



Junos[®] OS

Administration Guide for Security Devices

Release

15.1X49-D70



Modified: 2016-11-22

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

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

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

Junos[®] OS Administration Guide for Security Devices
15.1X49-D70
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

| | | |
|------------------|--|-----------|
| | About the Documentation | xvii |
| | Documentation and Release Notes | xvii |
| | Supported Platforms | xvii |
| | Using the Examples in This Manual | xvii |
| | Merging a Full Example | xviii |
| | Merging a Snippet | xviii |
| | Documentation Conventions | xix |
| | Documentation Feedback | xxi |
| | Requesting Technical Support | xxi |
| | Self-Help Online Tools and Resources | xxi |
| | Opening a Case with JTAC | xxii |
| Part 1 | User Access and Authentication | |
| Chapter 1 | User Access and Authentication Overview | 3 |
| | Understanding Login Classes | 3 |
| | Permission Bits | 4 |
| | Denying or Allowing Individual Commands | 6 |
| | Understanding User Accounts | 6 |
| | Understanding Junos OS Access Privilege Levels | 7 |
| | Junos OS Login Class Permission Flags | 7 |
| | Allowing or Denying Individual Commands for Junos OS Login Classes | 11 |
| | Understanding User Authentication Methods | 12 |
| | Hardening Shared Secrets in Junos OS | 12 |
| | Understanding Hardening Shared Secrets | 12 |
| Chapter 2 | Configuring Junos OS User Accounts | 15 |
| | Example: Configuring New Users | 15 |
| | Understanding Template Accounts | 18 |
| | Example: Creating Template Accounts | 19 |
| | Understanding Administrative Roles | 21 |
| | Example: Configuring Administrative Roles | 24 |
| | Handling Authorization Failure | 30 |
| | Example: Configuring System Retry Options | 31 |

| | | |
|------------------|---|-----------|
| Chapter 3 | Configuring User Access Privileges | 37 |
| | Configuring Access Privilege Levels | 37 |
| | Example: Configuring User Permissions with Access Privilege Levels | 37 |
| | Specifying Access Privileges for Junos OS Operational Mode Commands | 38 |
| | Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 40 |
| | Specifying Access Privileges for Junos OS Configuration Mode Hierarchies | 42 |
| | Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements | 43 |
| Chapter 4 | Permissions Flags for User Access Privileges | 47 |
| | Access Privilege User Permission Flags Overview | 48 |
| | access | 50 |
| | access-control | 50 |
| | admin | 51 |
| | admin-control | 52 |
| | all-control | 53 |
| | clear | 53 |
| | configure | 104 |
| | control | 104 |
| | field | 104 |
| | firewall | 105 |
| | firewall-control | 106 |
| | floppy | 106 |
| | flow-tap | 107 |
| | flow-tap-control | 107 |
| | flow-tap-operation | 108 |
| | idp-profiler-operation | 108 |
| | interface | 108 |
| | interface-control | 109 |
| | maintenance | 110 |
| | network | 117 |
| | pgcp-session-mirroring | 119 |
| | pgcp-session-mirroring-control | 119 |
| | reset | 119 |
| | rollback | 120 |
| | secret | 121 |
| | secret-control | 122 |
| | security | 123 |
| | security-control | 126 |
| | shell | 130 |
| | snmp | 130 |
| | system | 130 |
| | system-control | 133 |
| | trace | 134 |
| | trace-control | 139 |
| | view | 144 |
| | view-configuration | 218 |

| | | |
|------------------|---|------------|
| Chapter 5 | Configuring Authentication Methods | 219 |
| | Configuring RADIUS Server Authentication | 219 |
| | Example: Configuring a RADIUS Server for System Authentication | 222 |
| | Configuring TACACS+ Authentication | 225 |
| | Configuring TACACS+ Server Details | 225 |
| | Specifying a Source Address for the Junos OS to Access External TACACS+ Servers | 226 |
| | Configuring the Same Authentication Service for Multiple TACACS+ Servers | 226 |
| | Configuring Juniper Networks Vendor-Specific TACACS+ Attributes | 227 |
| | Example: Configuring a TACACS+ Server for System Authentication | 227 |
| | Example: Configuring Authentication Order | 230 |
| Part 2 | Configuring Remote Access to an SRX Series Appliances | |
| Chapter 6 | Configuring Secure Web Access | 235 |
| | Secure Web Access Overview | 235 |
| | Generating an SSL Certificate Using the openssl Command | 236 |
| | Generating a Self-Signed SSL Certificate | 236 |
| | Manually Generating Self-Signed SSL Certificates | 237 |
| | Configuring Device Addresses | 237 |
| | Enabling Access Services | 238 |
| | Example: Configuring Secure Web Access | 239 |
| | Adding, Editing, and Deleting Certificates on the Device | 241 |
| Chapter 7 | Setting up USB Modems for Remote Management | 243 |
| | USB Modem Interface Overview | 243 |
| | USB Modem Interfaces | 244 |
| | Dialer Interface Rules | 244 |
| | How the Device Initializes USB Modems | 245 |
| | USB Modem Configuration Overview | 246 |
| | Example: Configuring a USB Modem Interface | 248 |
| | Example: Configuring a Dialer Interface | 250 |
| | Example: Configuring a Dialer Interface for USB Modem Dial-In | 254 |
| | Configuring a Dial-Up Modem Connection Remotely | 256 |
| | Connecting to the Device Remotely | 257 |
| | Modifying USB Modem Initialization Commands | 257 |
| | Resetting USB Modems | 258 |
| Chapter 8 | Configuring Telnet and SSH Access to an SRX Series Appliance | 259 |
| | Securing the Console Port Configuration Overview | 259 |
| | Configuring Password Retry Limits for Telnet and SSH Access | 260 |
| | Configuring Reverse Telnet and Reverse SSH | 261 |
| | Example: Controlling Management Access on SRX Series Devices | 262 |
| | Example: Configuring a Filter to Block Telnet and SSH Access | 265 |
| | The telnet Command | 270 |
| | The ssh Command | 271 |
| | Configuring Outbound SSH Service | 272 |
| | Configuring the Device Identifier for Outbound SSH Connections | 273 |
| | Sending the Public SSH Host Key to the Outbound SSH Client | 274 |

| | | |
|-------------------|--|------------|
| | Configuring Keepalive Messages for Outbound SSH Connections | 275 |
| | Configuring a New Outbound SSH Connection | 275 |
| | Configuring the Outbound SSH Client to Accept NETCONF as an Available Service | 275 |
| | Configuring Outbound SSH Clients | 275 |
| Part 3 | Configuring DNS | |
| Chapter 9 | Configuring DNS Server Caching, DNSSEC, and DNS Proxy | 279 |
| | DNS Overview | 279 |
| | DNS Components | 279 |
| | DNS Server Caching | 280 |
| | Example: Configuring the TTL Value for DNS Server Caching | 280 |
| | DNSSEC Overview | 281 |
| | Example: Configuring DNSSEC | 281 |
| | Example: Configuring Keys for DNSSEC | 282 |
| | Example: Configuring Secure Domains and Trusted Keys for DNSSEC | 282 |
| | DNS Proxy Overview | 284 |
| | DNS Proxy Cache | 284 |
| | DNS Proxy with Split DNS | 284 |
| | Dynamic Domain Name System Client | 287 |
| | Configuring the Device as a DNS Proxy | 289 |
| Part 4 | Configuring DHCP Access Service for IP Address Management | |
| Chapter 10 | Understanding DHCP Services | 293 |
| | DHCP Overview | 293 |
| | DHCP Local Server | 293 |
| | DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction | 293 |
| | DHCP Local Server and Address-Assignment Pools | 294 |
| | DHCP Client | 294 |
| | DHCP Relay Agent | 294 |
| | DHCP Client, DHCP Relay Agent, and DHCP Local Servers | 295 |
| | Considerations | 295 |
| | DHCP Server, Client, and Relay Agent Overview | 296 |
| | DHCP Settings and Restrictions Overview | 297 |
| | Propagation of TCP/IP Settings for DHCP | 297 |
| | DHCP Conflict Detection and Resolution | 298 |
| | DHCP Interface Restrictions | 298 |
| | Understanding Cascaded DHCPv6 Prefix Delegating | 298 |
| Chapter 11 | Configuring a DHCP Local Server | 301 |
| | Understanding DHCP Server Operation | 301 |
| | DHCP Options | 301 |
| | Compatibility with Autoinstallation | 302 |
| | Chassis Cluster Support | 302 |
| | DHCP Server Configuration Overview | 302 |
| | Minimum DHCP Local Server Configuration | 303 |
| | Configuring Address-Assignment Pools | 304 |

| | | |
|-------------------|---|------------|
| | Configuring an Address-Assignment Pool Name and Addresses | 305 |
| | Configuring a Named Address Range for Dynamic Address Assignment | 305 |
| | Configuring Static Address Assignments | 306 |
| | Enabling TCP/IP Propagation on a DHCP Local Server | 306 |
| | Verifying and Managing DHCP Local Server Configuration | 307 |
| | Example: Configuring the Device as a DHCP Server | 308 |
| Chapter 12 | Configuring a DHCP Client | 315 |
| | Understanding DHCP Client Operation | 315 |
| | Minimum DHCP Client Configuration | 315 |
| | Configuring DHCP Client-Specific Attributes for Address-Assignment Pools . . . | 316 |
| | Configuring Optional DHCP Client Attributes | 317 |
| | Verifying and Managing DHCP Client Configuration | 318 |
| | Example: Configuring the Device as a DHCP Client | 318 |
| Chapter 13 | Configuring a DHCP Relay Agent | 323 |
| | Understanding DHCP Relay Agent Operation | 323 |
| | Minimum DHCP Relay Agent Configuration | 323 |
| | Verifying and Managing DHCP Relay Configuration | 324 |
| Chapter 14 | Configuring a DHCPv6 Local Server | 327 |
| | DHCPv6 Server Overview | 327 |
| | Creating a Security Policy for DHCPv6 | 328 |
| | Example: Configuring DHCPv6 Server Options | 329 |
| | Example: Configuring an Address-Assignment Pool | 332 |
| | Configuring a Named Address Range for Dynamic Address Assignment | 334 |
| | Configuring Address-Assignment Pool Linking | 335 |
| | Configuring DHCP Client-Specific Attributes | 335 |
| | Configuring an Address-Assignment Pool for Router Advertisement | 336 |
| | Understanding DHCPv6 Client and Server Identification | 336 |
| Chapter 15 | Configuring a DHCPv6 Client | 339 |
| | DHCPv6 Client Overview | 339 |
| | Minimum DHCPv6 Client Configuration | 340 |
| | Configuring Optional DHCPv6 Client Attributes | 341 |
| | Configuring Nontemporary Address Assignment | 343 |
| | Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 343 |
| | Configuring Auto-Prefix Delegation | 344 |
| | Configuring the DHCPv6 Client Rapid Commit Option | 345 |
| | Configuring a DHCPv6 Client in Autoconfig Mode | 345 |
| | Configuring TCP/IP Propagation on a DHCPv6 Client | 346 |
| Part 5 | Managing System Files | |
| Chapter 16 | Performing File Management Tasks | 351 |
| | File Management Overview | 351 |
| | Decrypting Configuration Files | 352 |
| | Encrypting Configuration Files | 352 |

| | | |
|-------------------|---|------------|
| | Modifying the Encryption Key | 354 |
| | Cleaning Up Files in J-Web | 354 |
| | Cleaning Up Files with the CLI | 355 |
| | Deleting Files | 356 |
| | Deleting the Backup Software Image | 357 |
| | Downloading Files | 357 |
| | Configuring RADIUS System Accounting | 358 |
| | Configuring Auditing of User Events on a RADIUS Server | 358 |
| | Specifying RADIUS Server Accounting and Auditing Events | 359 |
| | Configuring RADIUS Server Accounting | 359 |
| | Managing Accounting Files | 361 |
| Part 6 | Working with Junos OS Licenses | |
| Chapter 17 | Managing Junos OS Licenses | 365 |
| | Junos OS Feature License Keys | 365 |
| | License Key Components | 365 |
| | License Management Fields Summary | 366 |
| | Software Feature Licenses for SRX Series Devices | 367 |
| | Displaying License Keys in J-Web | 372 |
| | Downloading License Keys | 372 |
| | Generating a License Key | 372 |
| | Saving License Keys | 373 |
| | Updating License Keys | 373 |
| | Example: Adding a New License Key | 374 |
| | Example: Deleting a License Key | 377 |
| Part 7 | Configuration Statements and Operational Commands | |
| Chapter 18 | Configuration Statements | 381 |
| | [edit security certificates] Hierarchy Level | 383 |
| | [edit security ssh-known-hosts] Hierarchy Level | 384 |
| | Groups Configuration Statement Hierarchy | 384 |
| | System Configuration Statement Hierarchy | 385 |
| | address-assignment (Access) | 416 |
| | address-pool (Access) | 419 |
| | allow-configuration | 420 |
| | allow-configuration-regexps | 420 |
| | authentication-key | 421 |
| | authentication-order | 422 |
| | boot-server (NTP) | 423 |
| | broadcast | 424 |
| | broadcast-client | 425 |
| | ciphers | 426 |
| | connection-limit | 427 |
| | client-ia-type | 428 |
| | client-identifier (dhcp-client) | 428 |
| | client-identifier (dhcpv6-client) | 429 |
| | client-list-name (SNMP) | 429 |

| | |
|--|-----|
| client-type | 430 |
| deny-configuration | 430 |
| deny-configuration-regexps | 431 |
| destination (Accounting) | 432 |
| dhcp-attributes (Access IPv4 Address Pools) | 433 |
| dhcp-attributes (Access IPv6 Address Pools) | 435 |
| dhcp-client | 436 |
| dhcp-local-server (System Services) | 437 |
| dhcpv6 (System Services) | 441 |
| dhcpv6-client | 444 |
| disable (System Services) | 445 |
| dlv | 445 |
| dynamic-pool | 446 |
| dynamic-server | 447 |
| family (Security Forwarding Options) | 448 |
| file (System Logging) | 449 |
| forwarding-options (Security) | 452 |
| group (System Services DHCP) | 453 |
| host (SSH Known Hosts) | 456 |
| hostkey-algorithm | 457 |
| idle-timeout (System) | 458 |
| interface (System Services DHCP) | 459 |
| interfaces (ARP) | 460 |
| interfaces (Security Zones) | 461 |
| interface-traceoptions (System Services DHCP) | 462 |
| internet-options | 464 |
| kernel-replication (System) | 465 |
| lease-time (dhcp-client) | 465 |
| location | 466 |
| lockout-period | 467 |
| macs | 468 |
| max-pre-authentication-packets | 469 |
| multicast-client | 469 |
| name-server (Access) | 470 |
| neighbor-discovery-router-advertisement (Access) | 470 |
| ntp | 471 |
| outbound-ssh | 472 |
| overrides (System Services DHCP) | 474 |
| peer (NTP) | 475 |
| prefix | 476 |
| profiller | 477 |
| proxy | 478 |
| radius-options | 479 |
| radius-server | 480 |
| rapid-commit | 481 |
| reconfigure (System Services DHCP) | 482 |
| req-option | 483 |
| retransmission-attempt (dhcp-client) | 484 |
| retransmission-attempt (dhcpv6-client) | 484 |

| | |
|--|------------|
| retransmission-interval (dhcp-client) | 485 |
| root-authentication | 486 |
| single-connection | 487 |
| server (NTP) | 488 |
| server-address (dhcp-client) | 489 |
| source-address (NTP, RADIUS, System Logging, or TACACS+) | 489 |
| ssh-known-hosts | 490 |
| static-subscribers | 491 |
| statistics-service | 491 |
| subscriber-management | 492 |
| subscriber-management-helper | 493 |
| system master password | 494 |
| tacplus | 495 |
| tacplus-options | 496 |
| tacplus-server | 497 |
| traceoptions (Outbound SSH) | 499 |
| traceoptions (System Services DHCP) | 501 |
| trusted-key | 503 |
| uac-service | 504 |
| update-router-advertisement | 505 |
| update-server (dhcp-client) | 505 |
| update-server (dhcpv6-client) | 506 |
| usb-control | 506 |
| use-interface | 507 |
| user-id | 507 |
| vendor-id | 508 |
| vpn (Forwarding Options) | 508 |
| watchdog | 509 |
| web-management | 510 |
| web-management (System Services) | 511 |
| Chapter 19 | |
| Operational Commands | 515 |
| clear dhcp client binding | 517 |
| clear dhcp client statistics | 518 |
| clear dhcp relay binding | 519 |
| clear dhcp relay statistics | 520 |
| clear dhcp server binding | 521 |
| clear dhcp server statistics | 522 |
| clear dhcpv6 client binding | 523 |
| clear dhcpv6 client statistics | 524 |
| clear dhcpv6 server binding (Local Server) | 525 |
| clear dhcpv6 server statistics (Local Server) | 526 |
| clear system login lockout | 527 |
| file archive | 528 |
| file checksum md5 | 530 |
| file checksum sha1 | 531 |
| file checksum sha-256 | 532 |
| file compare | 533 |
| file copy | 536 |

| | |
|--|-----|
| file delete | 538 |
| file list | 539 |
| file rename | 540 |
| file show | 541 |
| request dhcp client renew | 542 |
| request dhcpv6 client renew | 543 |
| request system autorecovery state | 544 |
| request system decrypt password | 546 |
| request system download abort | 547 |
| request system download clear | 548 |
| request system download pause | 549 |
| request system download resume | 550 |
| request system download start | 551 |
| request system firmware upgrade | 552 |
| request system license update | 553 |
| request system power-off fpc | 554 |
| request system services dhcp | 555 |
| request system snapshot (SRX Series) | 556 |
| request system software abort in-service-upgrade (ICU) | 558 |
| request system software add (Maintenance) | 559 |
| request system reboot | 560 |
| request system software rollback (SRX Series) | 561 |
| request system zeroize | 562 |
| restart (Reset) | 564 |
| Restart Commands Overview | 568 |
| show chassis routing-engine (View) | 569 |
| show cli authorization | 572 |
| show dhcp client binding | 573 |
| show dhcp client statistics | 576 |
| show dhcp relay binding | 578 |
| show dhcp relay statistics | 580 |
| show dhcp server binding | 582 |
| show dhcp server statistics | 584 |
| show dhcpv6 client binding | 586 |
| show dhcpv6 client statistics | 588 |
| show dhcpv6 server binding (View) | 590 |
| show dhcpv6 server statistics (View) | 594 |
| show firewall (View) | 597 |
| show system autorecovery state | 599 |
| show system download | 601 |
| show system license (View) | 603 |
| show system login lockout | 606 |
| show system services dhcp client | 607 |
| show system services dhcp relay-statistics | 610 |
| show system snapshot media | 612 |
| show system storage partitions (View SRX Series) | 613 |

List of Figures

| | | |
|-------------------|--|------------|
| Part 1 | User Access and Authentication | |
| Chapter 1 | User Access and Authentication Overview | 3 |
| | Figure 1: Master Password Encryption | 13 |
| Part 3 | Configuring DNS | |
| Chapter 9 | Configuring DNS Server Caching, DNSSEC, and DNS Proxy | 279 |
| | Figure 2: DNS Proxy with Split DNS | 286 |
| | Figure 3: Dynamic DNS | 288 |
| Part 4 | Configuring DHCP Access Service for IP Address Management | |
| Chapter 10 | Understanding DHCP Services | 293 |
| | Figure 4: IPv6 Prefix Delegation | 299 |
| | Figure 5: Sub-prefix Delegation | 299 |

List of Tables

| | | |
|-------------------|---|-------------|
| | About the Documentation | xvii |
| | Table 1: Notice Icons | xix |
| | Table 2: Text and Syntax Conventions | xix |
| Part 1 | User Access and Authentication | |
| Chapter 1 | User Access and Authentication Overview | 3 |
| | Table 3: Predefined Login Classes | 3 |
| | Table 4: Permission Bits for Login Classes | 4 |
| | Table 5: Login Class Permission Flags | 8 |
| | Table 6: \$8\$-encrypted Password Format | 13 |
| Part 2 | Configuring Remote Access to an SRX Series Appliances | |
| Chapter 7 | Setting up USB Modems for Remote Management | 243 |
| | Table 7: Default Modem Initialization Commands | 245 |
| | Table 8: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity | 247 |
| | Table 9: Incoming Map Options | 247 |
| Chapter 8 | Configuring Telnet and SSH Access to an SRX Series Appliance | 259 |
| | Table 10: CLI telnet Command Options | 271 |
| | Table 11: CLI ssh Command Options | 272 |
| Part 4 | Configuring DHCP Access Service for IP Address Management | |
| Chapter 11 | Configuring a DHCP Local Server | 301 |
| | Table 12: Sample DHCP Server Configuration Settings | 302 |
| Chapter 14 | Configuring a DHCPv6 Local Server | 327 |
| | Table 13: DHCPv6 Attributes | 336 |
| Part 5 | Managing System Files | |
| Chapter 16 | Performing File Management Tasks | 351 |
| | Table 14: request system set-encryption-key Commands | 353 |
| Part 6 | Working with Junos OS Licenses | |
| Chapter 17 | Managing Junos OS Licenses | 365 |
| | Table 15: Summary of License Management Fields | 366 |
| | Table 16: Junos OS Feature Licenses | 367 |

| | |
|--|-----|
| Table 17: Junos OS Feature License Model Number for SRX Series Devices | 368 |
|--|-----|

Part 7

Chapter 19

Configuration Statements and Operational Commands

| | |
|--|------------|
| Operational Commands | 515 |
| Table 18: show chassis routing-engine Output Fields | 569 |
| Table 19: show dhcp client binding Output Fields | 573 |
| Table 20: show dhcp client statistics | 576 |
| Table 21: show dhcp relay binding Output Fields | 578 |
| Table 22: show dhcp relay statistics | 580 |
| Table 23: show dhcp server binding Output Fields | 582 |
| Table 24: show dhcp server statistics | 584 |
| Table 25: show dhcpv6 client binding Output Fields | 586 |
| Table 26: show dhcpv6 client statistics Output Fields | 588 |
| Table 27: show dhc6p server binding Output Fields | 590 |
| Table 28: show dhcpv6 server statistics Output Fields | 595 |
| Table 29: show firewall Output Fields | 597 |
| Table 30: show system autorecovery state Output Fields | 599 |
| Table 31: show system download Output Fields | 601 |
| Table 32: show system license Output Fields | 603 |
| Table 33: show system login lockout | 606 |
| Table 34: show system services dhcp client Output Fields | 607 |
| Table 35: show system services dhcp relay-statistics Output Fields | 610 |

About the Documentation

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

Documentation and Release Notes

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

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

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

Supported Platforms

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

- SRX Series
- vSRX

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 xix](#) 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 xix](#) 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 |

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

| Convention | Description | Examples |
|--------------------------------|---|--|
| Fixed-width text like this | Represents output that appears on the terminal screen. | <code>user@host> show chassis alarms</code> <code>No alarms currently active</code> |
| <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 | | |
| 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. |

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

| Convention | Description | Examples |
|------------------------------|---|--|
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select Protocols>Ospf . |

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

User Access and Authentication

- [User Access and Authentication Overview on page 3](#)
- [Configuring Junos OS User Accounts on page 15](#)
- [Configuring User Access Privileges on page 37](#)
- [Permissions Flags for User Access Privileges on page 47](#)
- [Configuring Authentication Methods on page 219](#)

CHAPTER 1

User Access and Authentication Overview

- [Understanding Login Classes on page 3](#)
- [Understanding User Accounts on page 6](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Understanding User Authentication Methods on page 12](#)
- [Hardening Shared Secrets in Junos OS on page 12](#)

Understanding Login Classes

Supported Platforms [SRX Series, vSRX](#)

All users who log in to the device must be in a login class. You can define any number of login classes. You then apply one login class to an individual user account. With login classes, you define the following:

- Access privileges users have when they are logged in to the device.
- Commands and statements that users can and cannot specify.
- How long a login session can be idle before it times out and the user is logged off.

You can define any number of login classes and then apply one login class to an individual user account.

[Table 3 on page 3](#) contains a few predefined login classes. The predefined login classes cannot be modified.

Table 3: Predefined Login Classes

| Login Class | Permission Bits Set |
|--------------------------|------------------------------------|
| operator | clear, network, reset, trace, view |
| read-only | view |
| super-user and superuser | all |
| unauthorized | None |

**NOTE:**

- You cannot modify a predefined login class name. If you issue the `set` command on a predefined class name, the Junos OS appends `-local` to the login class name. The following message also appears:

warning: '<class-name>' is a predefined class name; changing to '<class-name>-local'

- You cannot issue the `rename` or `copy` command on a predefined login class. Doing so results in the following error message:

error: target '<class-name>' is a predefined class

This section contains the following topics:

- [Permission Bits on page 4](#)
- [Denying or Allowing Individual Commands on page 6](#)

Permission Bits

Each top-level CLI command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission bits (see [Table 4 on page 4](#)).

Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 4: Permission Bits for Login Classes

| Permission Bit | Access |
|-----------------------|--|
| admin | Can view user account information in configuration mode and with the show configuration command. |
| admin-control | Can view user accounts and configure them (at the [edit system login] hierarchy level). |
| access | Can view the access configuration in configuration mode and with the show configuration operational mode command. |
| access-control | Can view and configure access information (at the [edit access] hierarchy level). |
| all | Has all permissions. |
| clear | Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands). |

Table 4: Permission Bits for Login Classes (*continued*)

| Permission Bit | Access |
|--------------------------|--|
| configure | Can enter configuration mode (using the configure command) and commit configurations (using the commit command). |
| control | Can perform all control-level operations (all operations configured with the -control permission bits). |
| field | Reserved for field (debugging) support. |
| firewall | Can view the firewall filter configuration in configuration mode. |
| firewall-control | Can view and configure firewall filter information (at the [edit firewall] hierarchy level). |
| floppy | Can read from and write to the removable media. |
| interface | Can view the interface configuration in configuration mode and with the show configuration operational mode command. |
| interface-control | Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the [edit] hierarchy). |
| maintenance | Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the device (using the request system commands). |
| network | Can access the network by entering the ping , ssh , telnet , and traceroute commands. |
| reset | Can restart software processes using the restart command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level). |
| rollback | Can use the rollback command to return to a previously committed configuration other than the most recently committed one. |
| routing | Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes. |
| routing-control | Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level). |
| secret | Can view passwords and other authentication keys in the configuration. |
| secret-control | Can view passwords and other authentication keys in the configuration and can modify them in configuration mode. |
| security | Can view security configuration in configuration mode and with the show configuration operational mode command. |

Table 4: Permission Bits for Login Classes (*continued*)

| Permission Bit | Access |
|-------------------------|--|
| security-control | Can view and configure security information (at the [edit security] hierarchy level). |
| shell | Can start a local shell on the device by entering the start shell command. |
| snmp | Can view SNMP configuration information in configuration and operational modes. |
| snmp-control | Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level). |
| system | Can view system-level information in configuration and operational modes. |
| system-control | Can view system-level configuration information and configure it (at the [edit system] hierarchy level). |
| trace | Can view trace file settings in configuration and operational modes. |
| trace-control | Can view trace file settings and configure trace file properties. |
| view | Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. |

Denying or Allowing Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that are otherwise permitted or not allowed by a permission bit.

Related Documentation

- [Understanding User Authentication Methods on page 12](#)
- [Understanding User Accounts on page 6](#)
- [Understanding Template Accounts on page 18](#)
- [Example: Configuring New Users on page 15](#)

Understanding User Accounts

Supported Platforms [SRX Series, vSRX](#)

User accounts provide one way for users to access the device. Users can access the device without accounts if you configured RADIUS or TACACS+ servers. After you have created an account, the device creates a home directory for the user. An account for the user **root** is always present in the configuration. For each user account, you can define the following:

- **Username**—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username.
- **User's full name**—If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- **User identifier (UID)**—Numeric identifier that is associated with the user account name. The identifier range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- **User's access privilege**—You can create login classes with specific permission bits or use one of the predefined classes.
- **Authentication method or methods and passwords** that the user can use to access the device—You can use SSH or an MD5 password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. If you configure the plain-text-password option, you are prompted to enter and confirm the password.

Related Documentation

- [Understanding User Authentication Methods on page 12](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 222](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)
- [Example: Configuring Authentication Order on page 230](#)

Understanding Junos OS Access Privilege Levels

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [QFX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Each top-level CLI command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more *permission flags*.

For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

The following sections provide additional information about permissions:

- [Junos OS Login Class Permission Flags on page 7](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 11](#)

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in [Table 5 on page 8](#). Permission flags are not cumulative, so for each class you must list all the permission flags needed, including **view** to display information and **configure** to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Table 5 on page 8 lists the Junos OS login class permission flags that you can configure by including the **permissions** statement at the **[edit system login class class-name]** hierarchy level.

Table 5: Login Class Permission Flags

| Permission Flag | Description |
|-------------------------|--|
| access | Can view the access configuration in configuration mode and with the show configuration operational mode command. |
| access-control | Can view and configure access information at the [edit access] hierarchy level. |
| admin | Can view user account information in configuration mode and with the show configuration operational mode command. |
| admin-control | Can view user accounts and configure them at the [edit system login] hierarchy level. |
| all-control | Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels. |
| clear | Can clear (delete) information learned from the network that is stored in various network databases by using the clear commands. |
| configure | Can enter configuration mode by using the configure command. |
| control | Can perform all control-level operations—all operations configured with the -control permission flags. |
| field | Can view field debug commands. Reserved for debugging support. |
| firewall | Can view the firewall filter configuration in configuration mode. |
| firewall-control | Can view and configure firewall filter information at the [edit firewall] hierarchy level. |
| floppy | Can read from and write to the removable media. |
| flow-tap | Can view the flow-tap configuration in configuration mode. |
| flow-tap-control | Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap] hierarchy level. |

Table 5: Login Class Permission Flags (*continued*)

| Permission Flag | Description |
|---------------------------------------|---|
| flow-tap-operation | Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must authenticate itself to the Junos OS as an administrative user. That account must have flow-tap-operation permission. NOTE: The flow-tap-operation option is not included in the all-control permissions flag. |
| idp-profiler-operation | Can view profiler data. |
| interface | Can view the interface configuration in configuration mode and with the show configuration operational mode command. |
| interface-control | Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels: <ul style="list-style-type: none"> • [edit chassis] • [edit class-of-service] • [edit groups] • [edit forwarding-options] • [edit interfaces] |
| maintenance | Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the su root command, and can halt and reboot the router or switch by using the request system commands. |
| network | Can access the network by using the ping , ssh , telnet , and traceroute commands. |
| pgcp-session-mirroring | Can view the pgcp session mirroring configuration. |
| pgcp-session-mirroring-control | Can modify the pgcp session mirroring configuration. |
| reset | Can restart software processes by using the restart command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level. |
| rollback | Can use the rollback command to return to a previously committed configuration other than the most recently committed one. |
| routing | Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes. |

Table 5: Login Class Permission Flags (*continued*)

| Permission Flag | Description |
|---------------------------|--|
| routing-control | Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level. |
| secret | Can view passwords and other authentication keys in the configuration. |
| secret-control | Can view passwords and other authentication keys in the configuration and can modify them in configuration mode. |
| security | Can view security configuration in configuration mode and with the show configuration operational mode command. |
| security-control | Can view and configure security information at the [edit security] hierarchy level. |
| shell | Can start a local shell on the router or switch by using the start shell command. |
| snmp | Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes. |
| snmp-control | Can view SNMP configuration information and can modify SNMP configuration at the [edit snmp] hierarchy level. |
| system | Can view system-level information in configuration and operational modes. |
| system-control | Can view system-level configuration information and configure it at the [edit system] hierarchy level. |
| trace | Can view trace file settings and configure trace file properties. |
| trace-control | Can modify trace file settings and configure trace file properties. |
| view | Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration. |
| view-configuration | <p>Can view all of the configuration excluding secrets, system scripts, and event options.</p> <p>NOTE: Only users with the maintenance permission can view commit script, op script, or event script configuration.</p> |

Allowing or Denying Individual Commands for Junos OS Login Classes

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the **permissions** statement.

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag. For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

- The **all** login class permission bits take precedence over extended regular expressions when a user with **rollback** permission issues the **rollback** command.
- Expressions used to allow and deny commands for users on RADIUS and TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (**allow-commands=cmd1 cmd2 ... cmdn**), you can specify each command as a separate expression. This new syntax is valid for **allow-configuration-regexps** and **deny-configuration-regexps**, **allow-commands** and **deny-commands**, and all user permission bits.
- Users cannot issue the **load override** command when specifying an extended regular expression. Users can only issue the **merge**, **replace**, and **patch** configuration commands.
- If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by the **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.
- Regular expressions for **allow-commands** and **deny-commands** can also include the **commit**, **load**, **rollback**, **save**, **status**, and **update** commands.
- If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize** and it is specified for **deny-commands**.

- Related Documentation**
- [Configuring Access Privilege Levels on page 37](#)
 - [Access Privilege User Permission Flags Overview on page 48](#)

Understanding User Authentication Methods

Supported Platforms [SRX Series, vSRX](#)

Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the device.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the device using Telnet. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the device, and the server runs on a remote network system.

You can configure the device to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the device. If you set up both authentication methods, you also can configure which method the device will try first.

- Related Documentation**
- [Understanding User Accounts on page 6](#)
 - [Understanding Login Classes on page 3](#)
 - [Understanding Template Accounts on page 18](#)
 - [Example: Configuring Authentication Order on page 230](#)
 - [Example: Configuring a RADIUS Server for System Authentication on page 222](#)
 - [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)

Hardening Shared Secrets in Junos OS

Supported Platforms [SRX Series](#)

- [Understanding Hardening Shared Secrets on page 12](#)

Understanding Hardening Shared Secrets

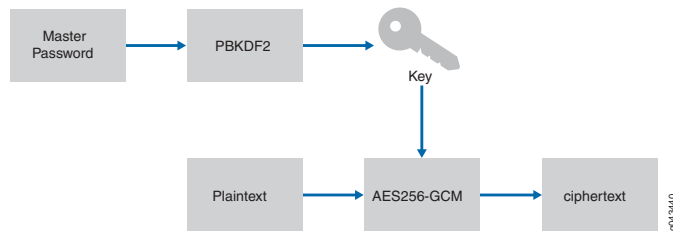
Existing shared secrets (\$9\$ format) in Junos OS currently use an obfuscation algorithm, which is not a very strong encryption for configuration secrets. If you want a strong

encryption for your configuration secrets, you can configure a master password. The master password is used to derive an encryption key that is used with AES256-GCM to encrypt configuration secrets. This new encryption method uses the \$8\$ formatted strings.

Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password. The master password encrypts secrets like the RADIUS password, IKE preshared keys, and other shared secrets in the Junos OS management process (mgd) configuration. The master password itself is not saved as part of the configuration. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. the key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text). See [Figure 1 on page 13](#)

Figure 1: Master Password Encryption



The \$8\$ configuration secrets can only be shared between devices using the same master password.

The \$8\$-encrypted passwords have the following format:

\$8\$crypt-algo\$hash-algo\$iterations\$salt\$iv\$tag\$encrypted. See [Table 6 on page 13](#) for the master password format details.

Table 6: \$8\$-encrypted Password Format

| Format | Description |
|------------|---|
| crypt-algo | Encryption/decryption algorithm to be used. Currently only AES256-GCM is supported. |
| hash-algo | Hash (prf) algorithm to be used for the PBKDF2 key derivation. |
| iterations | The number of iterations to use for the PBKDF2 hash function. Current iteration-count default is 100. The iteration count slows the hashing count, thus slowing attacker guesses. |
| salt | Sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used to <i>salt</i> (a random, but known string) the password and input to the PBKDF2 key derivation. |
| iv | A sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used as initialization vector for the AES256-GCM encryption function. |

Table 6: \$8\$-encrypted Password Format (*continued*)

| Format | Description |
|-----------|---|
| tag | ASCII64-encoded representation of the tag. |
| encrypted | ASCII64-encoded representation of the encrypted password. |

The ASCII64 encoding is Base64 (RFC 4648) compatible, except no padding (character “=”) is used to keep the strings short. For example:

```
$8$aes256-gcm$Hmac-sha2-256$100$y/4YMC4YDLU$FzYDI4jjN6YCyQsYLSaf8A$llu4jLcZarD9YnyD
/Hejww$okhBlcOcGakSqYxKww
```

CHAPTER 2

Configuring Junos OS User Accounts

- [Example: Configuring New Users on page 15](#)
- [Understanding Template Accounts on page 18](#)
- [Example: Creating Template Accounts on page 19](#)
- [Understanding Administrative Roles on page 21](#)
- [Example: Configuring Administrative Roles on page 24](#)
- [Handling Authorization Failure on page 30](#)
- [Example: Configuring System Retry Options on page 31](#)

Example: Configuring New Users

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure new users.

- [Requirements on page 15](#)
- [Overview on page 15](#)
- [Configuration on page 16](#)
- [Verification on page 18](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can add new users to the device's local database. For each account, you define a login name and password for the user and specify a login class for access privileges. The login password must meet the following criteria:

- The password must be at least six characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), but not control characters.
- The password must contain at least one change of case or character class.

In this example, you create a login class named `operator-and-boot` and allow it to reboot the device. You can define any number of login classes. You then allow the `operator-and-boot` login class to use commands defined in the `clear`, `network`, `reset`, `trace`, and `view` permission bits.

Then you create user accounts. User accounts provide enable you to access the device. (You can access the device without accounts if you configured RADIUS or TACACS+ servers.) You set the username as `cmartin` and the login class as `superuser`. Finally, you define the encrypted password for the user.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class operator-and-boot allow-commands "request system reboot"
set class system login operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password
$1$ABC123
```

GUI Step-by-Step Procedure

To configure new users:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Users** tab.
4. Click **Add** to add a new user. The Add User dialog box appears.
5. In the User name box, type a unique name for the user.

Do not include spaces, colons, or commas in the username.

6. In the User ID box, type a unique ID for the user.
7. In the Full Name box, type the user's full name.

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.
9. From the Login Class list, select the user's access privilege:
 - **operator**
 - **read-only**
 - **unauthorized**

This list also includes any user-defined login classes.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.

11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the [CLI User Guide](#).

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

```
[edit system login]
user@host# set class operator-and-boot allow-commands "request system reboot"
```
2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace view]
```
3. Set the username, login class, and encrypted password for the user.

```
[edit system login]
user@host# set user cmartin class superuser authentication encrypted-password $1$ABC123
```

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

```
[edit]
user@host# show system login
class operator-and-boot {
  permissions [ clear network reset trace view ];
  allow-commands "request system reboot";
}
user cmartin {
  class superuser;
  authentication {
    encrypted-password "$1$ABC123";
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 222](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 227](#).
- Configure a user. See [“Example: Configuring New Users” on page 15](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 19](#).

Verification

Confirm that the configuration is working properly.

Verifying the New Users Configuration

| | |
|------------------------------|---|
| Purpose | Verify that the new users have been configured. |
| Action | From operational mode, enter the show system login command. |
| Related Documentation | <ul style="list-style-type: none">• Understanding User Authentication Methods on page 12• Understanding User Accounts on page 6• Understanding Template Accounts on page 18• Understanding Login Classes on page 3 |

Understanding Template Accounts

Supported Platforms [SRX Series, vSRX](#)

You use local user template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the device and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, Junos OS issues a request to the authentication server to authenticate the user's login name. If a user is authenticated, the server returns the local username to the device, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, the device selects the appropriate local user template locally configured on the device. If a local user template does not exist for the authenticated user, the device defaults to the **remote** template.

- Related Documentation**
- [Understanding User Authentication Methods on page 12](#)
 - [Understanding User Accounts on page 6](#)
 - [Understanding Login Classes on page 3](#)
 - [Example: Creating Template Accounts on page 19](#)

Example: Creating Template Accounts

Supported Platforms [SRX Series, vSRX](#)

This example shows how to create template accounts.

- [Requirements on page 19](#)
- [Overview on page 19](#)
- [Configuration on page 19](#)
- [Verification on page 21](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

By default, Junos OS uses the **remote** template account when:

- The authenticated user does not exist locally on the device.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

In this example, you create a remote template account and set the username to remote and the login class for the user as operator. You create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

Configuration

- [Creating a Remote Template Account on page 20](#)
- [Creating a Local Template Account on page 20](#)

Creating a Remote Template Account

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user remote class operator
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To create a remote template account:

- Set the username and the login class for the user.

```
[edit system login]
user@host# set user remote class operator
```

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

```
[edit]
user@host# show system login
user remote {
  class operator;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Creating a Local Template Account

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login user admin class superuser
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To create a local template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user admin class superuser
```

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

```
[edit]
user@host# show system login
user admin {
class super-user;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a system authentication order. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 222](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 227](#).
- Configure system authentication order. See [“Example: Configuring Authentication Order” on page 230](#).

Verification

Confirm that the configuration is working properly.

Verifying the Template Accounts Creation

Purpose Verify that the template accounts have been created.

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

Related Documentation

- [Understanding User Authentication Methods on page 12](#)
- [Understanding User Accounts on page 6](#)
- [Understanding Login Classes on page 3](#)
- [Understanding Template Accounts on page 18](#)

Understanding Administrative Roles

Supported Platforms [SRX Series](#), [vSRX](#)

A system user can be a member of a class that allows the user to act as a particular kind of administrator for the system. Requiring a specific role to view or modify an item restricts the extent of information a user can obtain from the system. It also limits how much of

the system is open to intentional or unintentional modification or observation by a user. We recommend that you use the following guidelines when you are designing administrative roles:

- Do not allow any user to log in to the system as **root**.
- Restrict each user to the smallest set of privileges needed to perform the user's duties.
- Do not allow any user to belong to a login class containing the **shell** permission flag. The **shell** permission flag allows users to run the **start shell** command from the CLI.
- Allow users to have rollback permissions. Rollback permissions allow users to undo an action performed by an administrator but does not allow them to commit the changes.

You can assign an administrative role to a user by configuring a login class to have the privileges required for that role. You can configure each class to allow or deny access to configuration statements and commands by name. These specific restrictions override and take precedence over any permission flags also configured in the class. You can assign one of the following role attributes to an administrative user.

- **Crypto-administrator**—Allows the user to configure and monitor cryptographic data.
- **Security-administrator**—Allows the user to configure and monitor security data.
- **Audit-administrator**—Allows the user to configure and monitor audit data.
- **IDS-administrator**—Allows the user to monitor and clear the intrusion detection service (IDS) security logs.

Each role can perform the following specific management functions:

- **Cryptographic Administrator**
 - Configures the cryptographic self-test.
 - Modifies the cryptographic security data parameters.
- **Audit Administrator**
 - Configures and deletes the audit review search and sort feature.
 - Searches and sorts audit records.
 - Configures search and sort parameters.
 - Manually deletes audit logs.
- **Security Administrator**
 - Invokes, determines, and modifies the cryptographic self-test behavior.
 - Enables, disables, determines, and modifies the audit analysis and audit selection functions and configures the device to automatically delete audit logs.
 - Enables or disables security alarms.
 - Specifies limits for quotas on Transport Layer connections.

- Specifies the limits, network identifiers, and time periods for quotas on controlled connection-oriented resources.
- Specifies the network addresses permitted to use Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP).
- Configures the time and date used in time stamps.
- Queries, modifies, deletes, and creates the information flow or access control rules and attributes for the unauthenticated information flow security function policy (SFP), the authenticated information flow SFP, the unauthenticated device services, and the discretionary access control policy.
- Specifies initial values that override default values when object information is created under unauthenticated information flow SFP, the authenticated information flow SFP, the unauthenticated target of evaluation (TOE) services, and the discretionary access control policy.
- Creates, deletes, or modifies the rules that control the address from which management sessions can be established.
- Specifies and revokes security attributes associated with the users, subjects, and objects.
- Specifies the percentage of audit storage capacity at which the device alerts administrators.
- Handles authentication failures and modifies the number of failed authentication attempts through SSH or from the CLI that can occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.
- Manages basic network configuration of the device.
- **IDS Administrator**—Specifies IDS security alarms, intrusion alarms, audit selections, and audit data.

You need to set the security-role attribute in the classes created for these administrative roles. This attribute restricts which users can show and clear the security logs, actions that cannot be performed through configuration alone.

For example, you need to set the security-role attribute in the **ids-admin** class created for the IDS administrator role if you want to restrict clearing and showing IDS logs to the IDS administrator role. Likewise, you need to set the security-role to one of the other admin values to restrict that class from being able to clear and show non-IDS logs only.



NOTE: When a user deletes an existing configuration, the configuration statements under the hierarchy level of the deleted configuration (that is, the child objects that the user does not have permission to modify), now remain in the device.

Related Documentation

- [Example: Configuring Administrative Roles on page 24](#)

Example: Configuring Administrative Roles

Supported Platforms [M Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

This example shows how to configure individual administrative roles for a distinct, unique set of privileges apart from all other administrative roles.

- [Requirements on page 24](#)
- [Overview on page 24](#)
- [Configuration on page 24](#)
- [Verification on page 29](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

This example configures four users:

- **audit-officer** of the class **audit-admin**
- **crypto-officer** of the class **crypto-admin**
- **security-officer** of the class **security-admin**
- **ids-officer** of the class **ids-admin**

When a **security-admin** class is configured, the privileges for creating administrators are revoked from the user who created the **security-admin** class. Creation of new users and logins is at the discretion of the **security-officer**.

In this example, you create audit admin, crypto admin, security admin, and ids admin with permission flags pertaining to this role. Then you allow or deny access to configuration statements and commands by name for each administrative role. These specific restrictions take precedence over the permission flags also configured in the class. For example, only the **crypto-admin** can run the **request system set-encryption-key** command, which requires having the **security** permission flag to access it. Only the **security-admin** can include the **system time-zone** statement in the configuration, which requires having the **system-control** permission flag.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login class audit-admin permissions security
set system login class audit-admin permissions trace
set system login class audit-admin permissions maintenance
set system login class audit-admin allow-commands "^clear (log|security log)"
```

```

set system login class audit-admin deny-commands "^clear (security alarms|system
login logout)|^file (copy|delete|rename)|^request (security|system
set-encryption-key)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell";
set system login class audit-admin security-role audit-administrator
set system login class crypto-admin permissions admin-control
set system login class crypto-admin permissions configure
set system login class crypto-admin permissions maintenance
set system login class crypto-admin permissions security-control
set system login class crypto-admin permissions system-control
set system login class crypto-admin permissions trace
set system login class crypto-admin allow-commands "^request system
set-encryption-key"
set system login class crypto-admin deny-commands "^clear (log|security alarms|security
log|system login logout)|^file (copy|delete|rename)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
set system login class crypto-admin allow-configuration-regexps "security (ike|ipsec)
(policy|proposal)" "security ipsec ^vpn$ .* manual
(authentication|encryption|protocol|spi)" "system fips self-test after-key-generation"
set system login class crypto-admin security-role crypto-administrator
set system login class security-admin permissions all
set system login class security-admin deny-commands "^clear (log|security
log)|^(clear|show) security alarms alarm-type idp|^request (security|system
set-encryption-key)|^rollback|^start shell"
set system login class security-admin deny-configuration-regexps "security alarms
potential-violation idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$
.* manual (authentication|encryption|protocol|spi)" "security log cache" "security log
exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
set system login class security-admin security-role security-administrator
set system login class ids-admin permissions configure
set system login class ids-admin permissions security-control
set system login class ids-admin permissions trace
set system login class ids-admin permissions maintenance
set system login class ids-admin allow-configuration-regexps "security alarms
potential-violation idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^(clear|show) security
alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show) security
alarms alarm-type
(authentication|cryptographic-self-test|decryption-failures|encryption-failures|
ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^file (copy|delete|rename)|^request
(security|system set-encryption-key)|^rollback|
^set date|^show security (dynamic-policies|match-policies|policies)|^start shell"
set system login class ids-admin deny-configuration-regexps "security alarms
potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
set system login class ids-admin security-role ids-admin
set system login user audit-officer class audit-admin
set system login user crypto-officer class crypto-admin
set system login user security-officer class security-admin
set system login user ids-officer class ids-admin
set system login user audit-officer authentication plain-text-password
set system login user crypto-officer authentication plain-text-password
set system login user security-officer authentication plain-text-password
set system login user ids-officer authentication plain-text-password

```

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 users in administrative roles:

1. Create the **audit-admin** login class.

```
[edit]
user@host# set system login class audit-admin
[edit system login class audit-admin]
user@host# set permissions security
user@host# set permissions trace
user@host# set permissions maintenance
```

2. Configure the **audit-admin** login class restrictions.

```
[edit system login class audit-admin]
user@host# set allow-commands "^clear (log|security log)"
user@host# set deny-commands "^clear (security alarms|system login logout)|^file
(copy|delete|rename)|^request (security|system
set-encryption-key)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set security-role audit-administrator
```

3. Create the **crypto-admin** login class.

```
[edit]
user@host# set system login class crypto-admin
```

```
[edit system login class crypto-admin]
user@host# set permissions admin-control
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions system-control
user@host# set permissions trace
```

4. Configure the **crypto-admin** login class restrictions.

```
[edit system login class crypto-admin]
user@host# set allow-commands "^request system set-encryption-key"
user@host# set deny-commands "^clear (log|security alarms|security log|system
login logout)|^file (copy|delete|rename)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set allow-configuration-regexps "security (ike|ipsec) (policy|proposal)"
"security ipsec ^vpn$. * manual (authentication|encryption|protocol|spi)" "system
fips self-test after-key-generation"
user@host# set security-role crypto-administrator
```

5. Create the **security-admin** login class.

```
[edit]
user@host# set system login class security-admin
```

```
[edit system login class security-admin]
user@host# set permissions all
```

6. Configure the **security-admin** login class restrictions.

```
[edit system login class security-admin]
user@host# set deny-commands "^clear (log|security log)|^(clear|show) security
alarms alarm-type idp|^request (security|system
set-encryption-key)|^rollback|^start shell"
user@host# set deny-configuration-regexps "security alarms potential-violation
idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .* manual
(authentication| encryption|protocol|spi)" "security log cache" "security log
exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
user@host# set security-role security-administrator
```

7. Create the **ids-admin** login class.

```
[edit]
user@host# set system login class ids-admin

[edit system login class ids-admin]
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the **ids-admin** login class restrictions.

```
[edit system login class ids-admin]
user@host# set allow-configuration-regexps "security alarms potential-violation
idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^(clear|show) security
alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show)
security alarms alarm-type
(authentication|cryptographic-self-test|decryption-failures|encryption-failures|
ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^file
(copy|delete|rename)|^request (security|system set-encryption-key)|
^rollback|^set date|^show security (dynamic-policies|match-policies|policies)|^start
shell"
set system login class ids-admin deny-configuration-regexps "security alarms
potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
user@host# set security-role ids-administrator
```

9. Assign users to the roles.

```
[edit]
user@host# set system login

[edit system login]
user@host# set user audit-officer class audit-admin
user@host# set user crypto-officer class crypto-admin
user@host# set user security-officer class security-admin
user@host# set user ids-officer class ids-admin
```

10. Configure passwords for the users.

```
[edit system login]
user@host# set user audit-officer authentication plain-text-password
```

```

user@host# set user crypto-officer authentication plain-text-password
user@host# set user security-officer authentication plain-text-password
user@host# set user ids-officer authentication plain-text-password

```

Results

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

```

[edit]
user@host# show system
system {
  login {
    class audit-admin {
      permissions [ maintenance security trace ];
      allow-commands "^clear (log|security log)";
      deny-commands "^clear (security alarms|system login logout)|^file
        (copy|delete|rename)|^request (security|system
          set-encryption-key)|^rollback|^set date|^show security
            (alarms|dynamic-policies|match-policies|policies)|^start shell";
      security-role audit-administrator;
    }
    class crypto-admin {
      permissions [ admin-control configure maintenance security-control system-control
        trace ];
      allow-commands "^request (system set-encryption-key)";
      deny-commands "^clear (log|security alarms|security log|system login logout)|^file
        (copy|delete|rename)|^rollback|^set date|^show security
          (alarms|dynamic-policies|match-policies|policies)|^start shell";
      allow-configuration-regexps "security (ike|ipsec) (policy|proposal)" "security ipsec
        ^vpn$.* manual (authentication|encryption|protocol|spi)" "system fips self-test
          after-key-generation";
      security-role crypto-administrator;
    }
    class security-admin {
      permissions [ all];
      deny-commands "^clear (log|security log)|^(clear|show) security alarms alarm-type
        idp|^request (security|system set-encryption-key)|^rollback|^start shell";
      deny-configuration-regexps "security alarms potential-violation idp" "security
        (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$.* manual
          (authentication|encryption|protocol|spi)" "security log exclude.* event-id IDP_.*"
            "system fips self-test after-key-generation";
      security-role security-administrator;
    }
  }
  class ids-admin {
    permissions [ configure maintenance security-control trace ];
    deny-commands "^clear log|^ (clear|show) security alarms
      (alarm-id|all|newer-than|older-than|process|severity)|^(clear|show) security
        alarms alarm-type
          (authentication | cryptographic-self-test | decryption-failures | encryption-failures
            | ike-phase1-failures | ike-phase2-failures|key-generation-self-test |
            non-cryptographic-self-test |policy | replay-attacks) | ^file (copy|delete|rename)
              |^request (security|system set-encryption-key) | ^rollback |
                ^set date | ^show security (dynamic-policies|match-policies|policies) |^start shell";
  }
}

```

```

allow-configuration-regexps "security alarms potential-violation idp" "security log
exclude .* event-id IDP_*";
deny-configuration-regexps "security alarms potential-violation
(authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
security-role ids-administrator;
}
user audit-officer {
class audit-admin;
authentication {
encrypted-password "$1$ABC123"; ## SECRET-DATA
}
}
user crypto-officer {
class crypto-admin;
authentication {
encrypted-password "$1$ABC123."; ## SECRET-DATA
}
}
user security-officer {
class security-admin;
authentication {
encrypted-password "$1$ABC123."; ##SECRET-DATA
}
}
user ids-officer {
class ids-admin;
authentication {
encrypted-password "$1$ABC123/"; ## SECRET-DATA
}
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Login Permissions

Purpose Verify the login permissions for the current user.

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

```

user@host>show cli authorization
Current user: 'example' class 'super-user'
Permissions:
admin          -- Can view user accounts
admin-control  -- Can modify user accounts
clear          -- Can clear learned network info
configure      -- Can enter configuration mode
control        -- Can modify any config
edit           -- Can edit full files

```

```
field      -- Can use field debug commands
floppy     -- Can read and write the floppy
interface  -- Can view interface configuration
interface-control-- Can modify interface configuration
network    -- Can access the network
reset      -- Can reset/restart interfaces and daemons
routing    -- Can view routing configuration
routing-control-- Can modify routing configuration
shell      -- Can start a local shell
snmp       -- Can view SNMP configuration
snmp-control-- Can modify SNMP configuration
system     -- Can view system configuration
system-control-- Can modify system configuration
trace      -- Can view trace file settings
trace-control-- Can modify trace file settings
view       -- Can view current values and statistics
maintenance -- Can become the super-user
firewall   -- Can view firewall configuration
firewall-control-- Can modify firewall configuration
secret     -- Can view secret statements
secret-control-- Can modify secret statements
rollback   -- Can rollback to previous configurations
security   -- Can view security configuration
security-control-- Can modify security configuration
access     -- Can view access configuration
access-control-- Can modify access configuration
view-configuration-- Can view all configuration (not including secrets)
flow-tap   -- Can view flow-tap configuration
flow-tap-control-- Can modify flow-tap configuration
idp-profiler-operation-- Can Profiler data
pgcp-session-mirroring-- Can view pgcp session mirroring configuration
pgcp-session-mirroring-control-- Can modify pgcp session mirroring configuration
tion
storage    -- Can view fibre channel storage protocol configuration
storage-control-- Can modify fibre channel storage protocol configuration
all-control -- Can modify any configuration
Individual command authorization:
Allow regular expression: none
Deny regular expression: none
Allow configuration regular expression: none
Deny configuration regular expression: none
```

This output summarizes the login permissions.

Related Documentation • [Understanding Administrative Roles on page 21](#)

Handling Authorization Failure

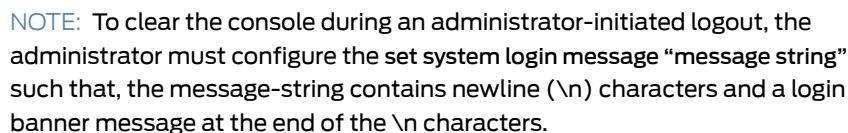
Supported Platforms [SRX Series, vSRX](#)

The system **lockout-period** defines the amount of time the device can be locked for a user account after a specified number of unsuccessful login attempts.

The system **idle-timeout** defines length of time the CLI operational mode prompt remains active before the session times out.

The system **message** defines the system login message. This message appears before a user logs in.

The number of reattempts the device allows is defined by the **tries-before-disconnect** option. The device allows 3 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console.

[illegible]

- [Example: Configuring System Retry Options on page 31](#)

Copyright © 2016, Juniper Networks, Inc. 31

This example shows how to configure system retry options to protect the device from malicious users.

- [Requirements on page 32](#)
- [Overview on page 32](#)
- [Configuration on page 34](#)
- [Verification on page 35](#)

Requirements

Before you begin, you should understand [“Handling Authorization Failure” on page 30](#).

No special configuration beyond device initialization is required before configuring this feature.

Overview

Malicious users sometimes try to log in to a secure device by guessing an authorized user account's password. Locking out a user account after a number of failed authentication attempts helps protect the device from malicious users.

Device lockout allows you to configure the number of failed attempts before the user account is locked out of the device and configure the amount of time before the user can attempt to log in to the device again. You can configure the amount of time in-between failed login attempts of a user account and can manually lock and unlock user accounts.



NOTE:

This example includes the following settings:

- **backoff-factor** — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the **backoff-threshold** statement. The default value for this statement is five seconds, with a range of five to ten seconds.
- **backoff-threshold** — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the **backoff-factor** statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.
- **lockout-period** — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the **tries-before-disconnect** statement. When a user fails to correctly login after the number of allowed attempts specified by the **tries-before-disconnect** statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.
- **tries-before-disconnect** — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH or Telnet. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the **lockout-period** statement before attempting to log back in to the device. The **tries-before-disconnect** statement must be set when the **lockout-period** statement is set; otherwise, the **lockout-period** statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

Once a user is locked out of the device, if you are the security administrator, you can manually remove the user from this state using the `clear system login lockout <username>` command. You can also use the `show system login lockout` command to view which users are currently locked out, when the lockout period began for each user, and when the lockout period ends for each user.

If the security administrator is locked out of the device, he can log in to the device from the console port, which ignores any user locks. This provides a way for the administrator to remove the user lock on their own user account.

In this example the user waits for the **backoff-threshold** multiplied by the **backoff-factor** interval, in seconds, to get the login prompt. In this example, the user must wait 5 seconds after the first failed login attempt and 10 seconds after the second failed login attempt to get the login prompt. The user gets disconnected after 15 seconds after the third failed attempt because the **tries-before-disconnect** option is configured as 3.

The user cannot attempt another login until 120 minutes has elapsed, unless a security administrator manually clears the lock sooner.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system login retry-options backoff-factor 5
set system login retry-options backoff-threshold 1
set system login retry-options lockout-period 120
set system login retry-options tries-before-disconnect 3
```

Step-by-Step Procedure To configure system retry-options:

1. Configure the backoff factor.

```
[edit]
user@host# set system login retry-options backoff-factor 5
```
2. Configure the backoff threshold.

```
[edit]
user@host# set system login retry-options backoff-threshold 1
```
3. Configure the amount of time the device gets locked after failed attempts.

```
[edit]
user@host# set system login retry-options lockout-period 5
```
4. Configure the number of unsuccessful attempts during which, the device can remain unlocked.

```
[edit]
user@host# set system login retry-options tries-before-disconnect 3
```

Results From configuration mode, confirm your configuration by entering the **show system login retry-options** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 5;
tries-before-disconnect 3;
```

Confirm that the configuration is working properly.

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Displaying the Locked User Logins

Purpose Verify that the login lockout configuration is enabled.

Action Attempt three unsuccessful logins for a particular username. The device will be locked for that username; then log in to the device with a different username. From operational mode, enter the **show system login lockout** command.

Meaning When you perform three unsuccessful login attempts with a particular username, the device is locked for that user for five minutes, as configured in the example. You can verify that the device is locked for that user by logging in to the device with a different username and entering the **show system login lockout** command.

Related Documentation

- [Handling Authorization Failure on page 30](#)

CHAPTER 3

Configuring User Access Privileges

- [Configuring Access Privilege Levels on page 37](#)
- [Example: Configuring User Permissions with Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 40](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 43](#)

Configuring Access Privilege Levels

Supported Platforms [EX Series, M Series, MX Series, OCX1100, PTX Series, QFabric System, QFX Series standalone switches, T Series](#)

Each top-level CLI command and each configuration statement have an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges.

To configure access privilege levels, include the **permissions** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]  
permissions [ permissions ];
```

**Related
Documentation**

- [Example: Configuring User Permissions with Access Privilege Levels on page 37](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [*permissions*](#)

Example: Configuring User Permissions with Access Privilege Levels

Supported Platforms [EX Series, M Series, MX Series, PTX Series, QFX Series, SRX Series, T Series, vSRX](#)

Create two access privilege classes on the router or switch, one for configuring and viewing user accounts only and the second for configuring and viewing SNMP parameters only:

In this example, you create two custom login classes on the router or switch and assign access privileges to each class through permission flags. The first custom login class is called **user-accounts** and it only includes access privileges for configuring and viewing user accounts. The second custom login class is called **network-mgmt** and only includes access privileges for configuring SNMP parameters.

```
[edit]
system {
  login {
    class user-accounts {
      permissions [ configure admin admin-control ];
    }
    class network-mgmt {
      permissions [ configure snmp snmp-control ];
    }
  }
}
```

1. Create the **user-accounts** custom login class and give it control over user accounts with the **configure admin admin-control** permission flag.

```
[edit system login]
user@router# set class user-accounts permissions configure admin admin-control
```

2. Create the **network-mgmt** custom login class and use the **configure snmp snmp-control** permission flag to assign it SNMP configuration privileges.

```
[edit system login]
user@router# set class network-mgmt permissions configure snmp snmp-control
```

3. Check your configuration by using the **show system login** command.

```
user@router# show system login
class user-accounts {
  permissions [ configure admin admin-control ];
}
class network-mgmt {
  permissions [ configure snmp snmp-control ];
}
```

Related Documentation

- [Configuring Access Privilege Levels on page 37](#)

Specifying Access Privileges for Junos OS Operational Mode Commands

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [OCX1100](#), [PTX Series](#), [QFabric System](#), [QFX Series standalone switches](#), [T Series](#)

You can specify extended regular expressions by using the **allow-commands** and **deny-commands** statements to define a user's access privileges to individual operational mode commands. Doing so takes precedence over a login class permissions bit set for a user. You can include one **deny-commands** and one **allow-commands** statement in each login class.

To explicitly provide use of an individual operational mode command that would otherwise be denied, include the **allow-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
  allow-commands "regular-expression";
```

To explicitly deny access to an individual operational mode command that would otherwise be supported, include the **deny-commands** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
  deny-commands "regular-expression";
```



NOTE: The regular expression to allow/deny commands for any login class is supported at the command level but not at the argument level. For example, you can completely block ping but not ping *argument1*.

If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive.

```
allow-commands "show interfaces";
```



NOTE: Modifiers are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

For example, the deny command **set protocols** does not match anything, whereas **protocols** matches *protocols*.

Explicitly providing access to operational mode commands using the **allow-commands** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying access to operational mode commands using the **deny-commands** statement removes permissions for the specified commands from the default permissions provided by the **permissions** statement.

For example, if a login class has the permission **view** and the **allow-commands** statement includes the **request system software add** command, the specified login class user can install software, in addition to the permissions specified by the **view** permissions flag. Likewise, if a login class has the permission **all** and the **deny-commands** statement includes the **request system software add** command, the specified login class user can perform all operations allowed by the **all** permissions flag, except installing software using the **request system software add** command.

If you allow and deny the same commands, the **allow-commands** permissions take precedence over the permissions specified by **deny-commands**. For example, if you include **allow-commands "request system software add"** and **deny-commands "request system software add"**, the login class user is allowed to install software using the **request system software add** command.

If you specify a regular expression for **allow-commands** and **deny-commands** with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for **allow-commands** with the **commit-synchronize** command and a regular expression for **deny-commands** with the **commit** command, users assigned to such a login class would be able to issue the **commit synchronize** command, but not the **commit** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **allow-commands**.

Likewise, if you specify a regular expression for **allow-commands** with the **commit** command and a regular expression for **deny-commands** with the **commit-synchronize** command, users assigned to such a login class would be able to issue the **commit** command, but not the **commit-synchronize** command. This is because **commit-synchronize** is the longest match between **commit** and **commit-synchronize**, and it is specified for **deny-commands**.

Anchors are required when specifying complex regular expressions with **allow-commands** or **deny-commands** statements. For example, when specifying multiple commands using the pipe (|) symbol for **allow-commands**, the following syntax is incorrect:

allow-commands = "(monitor.*)"|(ping.*)"|(show.*)"|(exit)" . Instead, you must specify the expression using the following syntax: **allow-commands = "^(^monitor) | (^ping) | (^show) | (^exit)"** OR **allow-commands = "^(monitor | ping | show | exit)"**

**Related
Documentation**

- [Example: Configuring User Permissions with Access Privileges for Operational Mode Commands on page 40](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands](#)
- [allow-commands](#)
- [deny-commands](#)

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands

Supported Platforms EX Series, M Series, MX Series, OCX1100, PTX Series, QFabric System, QFX Series standalone switches, T Series

Each operational mode command has an access privilege level associated with it. Access privileges control the commands that each custom login class can execute, configure, and view. Custom login classes are groups of users who are assigned with customized levels of access to different commands and statements. This ensures that each group of users can only use commands appropriate to their function, preventing unauthorized users from executing sensitive commands that could potentially cause damage to the network.

In this example, you create three custom login classes on the router or switch and assign access privileges for operational mode commands through the **allow-commands** and **deny-commands** settings. Each custom login class uses the same set of permission flags as the default login class **operator**, but the login class is allowed or denied certain operational mode commands. The first custom login class is called **operator-and-boot** and it has access to the **request system reboot** operational mode command. The second custom login class is called **operator-no-set** and it is denied access to any **set** commands. The third login class is called **operator-and-install-but-no-bgp** and it has access to the **request system software add** and **show route** operational mode commands, but it is denied access to the **show bgp** command.

```
[edit]
system {
  login {
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    class operator-no-set {
      permissions [ clear network reset trace view ];
      deny-commands "set";
    }
    class operator-and-install-but-no-bgp {
      permissions [ clear network reset trace view ];
      allow-commands "(request system software add)|(show route$)";
      deny-commands "show bgp";
    }
  }
}
```

1. Create the **operator-and-boot** custom login class, give it **operator** level permission flags, and authorize it to use the **request system reboot** command.

```
[edit system login]
user@router# set class operator-and-boot permissions clear network reset trace view
user@router# set class operator-and-boot allow-commands request system reboot
```

2. Create the **operator-no-set** custom login class, give it **operator** level permission flags, and deny it access to the **set** command.

```
[edit system login]
user@router# set class operator-no-set clear network reset trace view
user@router# set class operator-no-set deny-commands set
```

3. Create the **operator-and-install-but-no-bgp** custom login class, give it **operator** level permission flags, authorize it to use the **request system software add** and **show route** commands, and deny it access to the **show bgp** command.

```
[edit system login]
```

```

user@router# set class operator-and-install-but-no-bgp clear network reset trace
view
user@router# set class operator-and-install-but-no-bgp request system software
add show route
user@router# set class operator-and-install-but-no-bgp show bgp

```

4. Check your configuration by using the **show system login** command.

```

user@router# show system login
class operator-and-boot {
  permissions [ clear network reset trace view ];
  allow-commands "request system reboot";
}
class operator-no-set {
  permissions [ clear network reset trace view ];
  deny-commands "set";
}
class operator-and-install-but-no-bgp {
  permissions [ clear network reset trace view ];
  allow-commands "(request system software add)|(show route$)";
  deny-commands "show bgp";
}

```

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)

Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

The **allow/deny-configuration** and **allow/deny-configuration-regexps** statements let you explicitly allow or deny users access privileges to portions of the configuration hierarchy. Each of these statements is added to named login classes and configured with one or more regular expressions to be allowed or denied. Each login class is assigned to specific users or user IDs.

The search and match methods differ in the two forms of these statements. You must select which form to use within a login class—you cannot configure **allow-configuration** and **allow-configuration-regexps** together in the same login class. You must select just one. If you have existing configurations using the **allow/deny-configuration** form of the statements, using the same configuration options with the **allow/deny-configuration-regexps** form of the statements might not produce the same results.

- **Allow/deny-configuration** statements perform slower matching, with more flexibility, especially in wildcard matching. However, it can take a very long time to evaluate all of the possible statements if a great number of full path regular expressions or wildcard expressions are configured, possibly impacting performance. These statements were introduced before Junos OS Release 7.4.
- **Allow/deny-configuration-regexps** statements perform faster matching, with less flexibility. You configure a set of strings in which each string is a regular expression, with spaces between the terms of the string. This provides very fast matching. However,

it is more tedious to use wildcard expressions in this form of the statement, because you must set up wildcards for each token (term) of the space-delimited string you want to match. These statements were introduced in Junos OS Release 11.2.

- Related Documentation**
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Example: Configuring User Permissions with Access Privilege Levels on page 37](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)

Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

This example shows how to set up configuration access privileges using the **allow-configuration-regexps** and **deny-configuration-regexps** statements.

- [Requirements on page 43](#)
- [Overview on page 43](#)
- [Configuration on page 44](#)
- [Examples Using Allow or Deny Configurations with Regular Expressions on page 44](#)

Requirements

This example uses the following hardware and software components:

- One Juniper Networks M Series, MX Series, or T Series device
- Junos OS Release 11.2 or later
 - There must be at least one user assigned to a login class.
 - There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

The **allow-configuration-regexps** and **deny-configuration-regexps** statements let you explicitly allow or deny users assigned to named user classes access privileges to portions of the configuration hierarchy, giving the system administrator precision control over who can change specific configurations in the system.



NOTE: The statements **allow-configuration-regexps** and **deny-configuration-regexps** perform similar functions as the statements **allow-configuration** and **deny-configuration**, except you can configure sets of strings in which the strings include spaces when using the first set of statements. You cannot use the two kinds of statements together.

Configuration

To set up configuration access privileges:

1. To explicitly allow one or more individual configuration mode hierarchies that would otherwise be denied, include the **allow-configuration-regexps** statement at the **[edit system login class class-name]** hierarchy level, configured with the regular expressions to be allowed.

```
[edit system login class class-name]
user@host# set allow-configuration-regexps "regular expression 1" "regular expression
2" "regular expression 3" "regular expression 4" ...
```

2. To explicitly deny one or more individual configuration hierarchies that would otherwise be allowed, include the **deny-configuration-regexps** statement at the **[edit system login class class-name]** hierarchy level, configured with the regular expressions to be denied.

```
[edit system login class class-name]
user@host# set deny-configuration-regexps "regular expression 1" "regular-expression
2" "regular expression 3" "regular expression 4"...
```

3. Assign the login class to one or more users.

```
[edit system login]
user@host# set user username class class-name
```

4. Commit your changes.

Users assigned this login class have the permissions you have set for the class.

Examples Using Allow or Deny Configurations with Regular Expressions

Purpose This section provides examples of access privilege configurations to give you ideas for creating configurations appropriate for your system. You can use combinations of privilege statements for configuration access and for operational mode commands to give precise control over classes of access privileges.

Allow Configuration Changes The following example login class lets the user make changes at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to the permissions specified by the **configure** permissions flag, which allows the user to enter configuration mode using the **configure** command.

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "system services"
```

Deny Configuration Changes The following example login class lets the user perform all operations allowed by the **all** permissions flag. However, it denies modifying the configuration at the **[edit system services]** hierarchy level.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set deny-configuration-regexps "system services"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot configure telnet parameters:

```
[edit system login class class-name]
user@host# set deny-configuration "system services telnet"
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot issue login class commands within any login class whose name begins with "m":

```
[edit system login class class-name]
user@host# set deny-configuration "system login class m ."
```

If the following statement is included in the configuration and the user's login class permission bit is set to **all**, the user cannot edit the configuration or issue commands (such as **commit**) at the **[edit system login class]** or the **[edit system services]** hierarchy levels:

```
[edit system login class class-name]
user@host# set deny-configuration "system login class" "system services"
```

Allow and Deny Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to **[system "interfaces .*" unit .*" family inet address .*" protocols]**. However, the user is denied configuration access to the SNMP hierarchy level.



NOTE: You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use [*] or [.*] alone.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps system "interfaces .* unit .* family inet
address ." protocols
user@host# set deny-configuration-regexps snmp
```

Allow and Deny Multiple Configuration Changes

The following example login class lets the user perform all operations allowed by the **all** permissions flag, and explicitly grants configuration access to multiple hierarchy levels for interfaces. It denies configuration access to the **[edit system]** and **[edit protocols]** hierarchy levels.



NOTE: You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

```
[edit system login class class-name]
user@host# set permissions all configure view view-configuration
user@host# set allow-configuration-regexps "interfaces .* description ." "interfaces .*
unit .* description ." "interfaces .* unit .* family inet address ." "interfaces .* disable"
user@host# set deny-configuration-regexps "system" "protocols"
```

Allow Configuration Changes and Deny Operations Commands

You can combine allow and deny configuration statements with allow and deny operational commands statements to fine-tune access privileges. The following example login class uses a combination of the **deny-commands** operational permissions statement and the **allow-configuration-regexps** configuration permissions statement to let the user configure and commit changes to the OSPF and BGP protocols. However, this class of user cannot issue the **show system statistics** or the **show bgp summary** commands.

```
[edit system login class class-name]  
user@host# set permissions all configure view view-configuration  
user@host# set deny-commands "(show system statistics)|(show bgp summary)"  
user@host# set allow-configuration-regexps "protocols ospf|bgp"
```

The following shows permissions set for individual configuration mode hierarchies:

```
[edit]  
system {  
  login { # This login class has operator privileges and the additional ability to edit  
    # configuration at the system services hierarchy level.  
    class only-system-services {  
      permissions [ configure ];  
      allow-configuration "system services";  
    }  
    # services commands.  
    class all-except-system-services { # This login class has operator privileges but  
      # cannot edit any system services configuration.  
      permissions [ all ];  
      deny-configuration "system services";  
    }  
  }  
}
```

Verification To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.
2. Assign the login class to a *username*.
3. Log in as the *username* assigned with the new login class.
4. Attempt to perform the configurations that have been allowed or denied.
 - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
 - You should not be able to perform configuration changes to hierarchy levels and regular expressions that have been denied.
 - Denied expressions should take precedence over allowed expressions.
 - Any allowed or denied expressions should take precedence over any permissions granted with the **permissions** statement.

Related Documentation

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Example: Configuring User Permissions with Access Privilege Levels on page 37](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)

CHAPTER 4

Permissions Flags for User Access Privileges

- [Access Privilege User Permission Flags Overview on page 48](#)
- [access on page 50](#)
- [access-control on page 50](#)
- [admin on page 51](#)
- [admin-control on page 52](#)
- [all-control on page 53](#)
- [clear on page 53](#)
- [configure on page 104](#)
- [control on page 104](#)
- [field on page 104](#)
- [firewall on page 105](#)
- [firewall-control on page 106](#)
- [floppy on page 106](#)
- [flow-tap on page 107](#)
- [flow-tap-control on page 107](#)
- [flow-tap-operation on page 108](#)
- [idp-profiler-operation on page 108](#)
- [interface on page 108](#)
- [interface-control on page 109](#)
- [maintenance on page 110](#)
- [network on page 117](#)
- [pgcp-session-mirroring on page 119](#)
- [pgcp-session-mirroring-control on page 119](#)
- [reset on page 119](#)
- [rollback on page 120](#)
- [secret on page 121](#)

- [secret-control on page 122](#)
- [security on page 123](#)
- [security-control on page 126](#)
- [shell on page 130](#)
- [snmp on page 130](#)
- [system on page 130](#)
- [system-control on page 133](#)
- [trace on page 134](#)
- [trace-control on page 139](#)
- [view on page 144](#)
- [view-configuration on page 218](#)

Access Privilege User Permission Flags Overview

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the **[edit system login class]** hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the **all** permissions flag.

For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the **interface** permissions flag grants read-only access to the **[edit interfaces]** hierarchy level. The **-control** form of the flag grants read-write access to that configuration. Using the preceding example, **interface-control** grants read-write access to the **[edit interfaces]** hierarchy level.

The permission flags listed in "Related Documentation" grant a specific set of access privileges. Each permission flag is listed with the operational mode commands and configuration hierarchy levels and statements for which that flag grants access.



NOTE: Each command listed represents that command and all subcommands with that command as a prefix. Each configuration statement listed represents the top of the configuration hierarchy to which that flag grants access.

**Related
Documentation**

- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [access on page 50](#)
- [access-control on page 50](#)
- [admin on page 51](#)
- [admin-control on page 52](#)

- [all-control on page 53](#)
- [clear on page 53](#)
- [configure on page 104](#)
- [control on page 104](#)
- [field on page 104](#)
- [firewall on page 105](#)
- [firewall-control on page 106](#)
- [floppy on page 106](#)
- [flow-tap on page 107](#)
- [flow-tap-operation on page 108](#)
- [idp-profiler-operation on page 108](#)
- [interface on page 108](#)
- [interface-control on page 109](#)
- [maintenance on page 110](#)
- [network on page 117](#)
- [pgcp-session-mirroring on page 119](#)
- [pgcp-session-mirroring-control on page 119](#)
- [reset on page 119](#)
- [rollback on page 120](#)
- [secret on page 121](#)
- [secret-control on page 122](#)
- [security on page 123](#)
- [security-control on page 126](#)
- [shell on page 130](#)
- [snmp on page 130](#)
- [system on page 130](#)
- [system-control on page 133](#)
- [trace on page 134](#)
- [trace-control on page 139](#)
- [view on page 144](#)
- [view-configuration on page 218](#)

access

Supported Platforms EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX

Can view the access configuration in configuration mode.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit access]
[edit access diameter]
[edit access ppp-options]
[edit access radius]
[edit dynamic-profile]
[edit logical-systems access]
[edit logical-systems routing-instances instance system services
static-subscribers access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
dynamic-profile]
[edit routing-instances instance system services static-subscribers group
access-profile]
[edit routing-instances instance system services static-subscribers group
dynamic-profile]
[edit system services extensible-subscriber-services access-profile]
[edit system services static-subscribers access-profile]
[edit system services static-subscribers dynamic-profile]
[edit system services static-subscribers group access-profile]
[edit system services static-subscribers group dynamic-profile]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
 - [access-control on page 50](#)

access-control

Supported Platforms EX Series, M Series, MX Series, SRX Series, T Series, vSRX

Can view access configuration information. Can edit access configuration at the **[edit access]**, **[edit logical-systems]**, **[edit routing-instances]**, and **[edit system services]** hierarchy levels.

**Configuration
Hierarchy Levels**

```
[edit access]
[edit access ppp-options]
[edit dynamic-profile]
[edit logical-systems access]
[edit logical-systems routing-instances instance system services
static-subscribers access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
dynamic-profile]
[edit routing-instances instance system services static-subscribers group
access-profile]
[edit routing-instances instance system services static-subscribers group
dynamic-profile]
[edit system services static-subscribers access-profile]
[edit system services static-subscribers dynamic-profile]
[edit system services static-subscribers group access-profile]
[edit system services static-subscribers group dynamic-profile]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [access on page 50](#)

admin

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view user account information in configuration mode.

Commands

```
show system audit
```

**Configuration
Hierarchy Levels**

```
[edit protocols uplink-failure-detection]
[edit system]
[edit system accounting]
[edit system diag-port-authentication]
```

```

[edit system extensions]
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh ciphers]
[edit system services ssh client-alive-count-max]
[edit system services ssh client-alive-interval]]
[edit system services ssh hostkey-algorithm]
[edit system services ssh key-exchange]
[edit system services ssh macs]
[edit system services ssh max-sessions-per-connection]
[edit system services ssh no-tcp-fowarding]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
[edit system services ssh tcp-fowarding]

```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
 - [admin-control on page 52](#)

admin-control

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view user account information and configure it at the **[edit system]** hierarchy level.

Commands `show system audit`

Configuration Hierarchy Levels

```

[edit protocols uplink-failure-detection]
[edit system]
[edit system accounting]
[edit system diag-port-authentication]
[edit system extensions]
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh ciphers]
[edit system services ssh hostkey-algorithm]
[edit system services ssh key-exchange]
[edit system services ssh macs]
[edit system services ssh protocol-version]
[edit system services ssh root-login]

```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [admin on page 51](#)

all-control

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.

Commands All CLI commands.

Configuration Hierarchy Levels All CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

clear

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can clear (delete) information learned from the network that is stored in various network databases.

Commands

```
clear
clear amt
clear amt statistics
<clear-amt-statistics>
clear amt tunnel
clear-amt-tunnel
clear amt tunnel gateway-address
<clear amt tunnel gateway-address>
clear amt tunnel statistics
<clear-amt-tunnel-statistics>
clear amt tunnel statistics gateway-address
<clear-amt-tunnel-gateway-address-statistics>
clear amt tunnel statistics tunnel-interface
<clear-amt-tunnel-interface-statistics>
clear amt tunnel tunnel-interface
<clear-amt-tunnel-interface>
clear ancp
clear ancp neighbor
<clear-ancp-neighbor-connection>
clear ancp statistics
<clear-ancp-statistics>
clear ancp subscriber
<clear-ancp-subscriber-connection>
clear-appqos-counter
```

```
clear-appqos-rate-limiter-statistics
clear-appqos-rule-statistics
clear arp
  <clear-arp-table>
clear auto-configuration
clear auto-configuration interfaces
<clear-auto-configuration-interfaces>
clear bfd
clear bfd adaptation
<clear-bfd-adaptation-information>
clear bfd adaptation address
<clear-bfd-adaptation-address>
clear bfd adaptation discriminator
<clear-bfd-adaptation-discriminator>
clear bfd session
<clear-bfd-session-information>
clear bfd session address
<clear-bfd-session-address>
clear bfd session discriminator
<clear-bfd-session-discriminator>
clear bgp
clear bgp damping
  <clear-bgp-damping>
clear bgp neighbor
  <clear-bgp-neighbor>
clear bgp table
  <clear-bgp-table>
clear bridge
clear bridge evpn
clear bridge evpn arp-table
<clear-bridge-evpn-arp-table>
clear bridge mac-table
  <clear-bridge-mac-table>
clear bridge mac-table interface
  <clear-bridge-interface-mac-table>
clear bridge recovery-timeout
<clear-bridge-recovery>
clear bridge recovery-timeout interface
<clear-bridge-recovery-interface>
clear captive-portal
clear captive-portal firewall
<clear-captive-portal-firewall>
clear captive-portal firewall interface
<clear-captive-portal-firewall-interface>
clear captive-portal interface
<clear-captive-portal-interface-session>
clear captive-portal mac-address
<clear-captive-portal-mac-session>
clear cli
clear cli logical-system
<clear-cli-logical-system>
clear database-replication
clear database-replication statistics
<clear-database-replication-statistics-information>
clear ddos-protection
clear ddos-protection protocols
clear ddos-protection protocols amtv4
clear ddos-protection protocols amtv4 aggregate
clear ddos-protection protocols amtv4 aggregate culprit-flows
clear ddos-protection protocols amtv4 aggregate states
clear ddos-protection protocols amtv4 aggregate statistics
```

```
clear ddos-protection protocols amtv4 culprit-flows
clear ddos-protection protocols amtv4 states
clear ddos-protection protocols amtv4 statistics
clear ddos-protection protocols amtv6
clear ddos-protection protocols amtv6 aggregate
clear ddos-protection protocols amtv6 aggregate culprit-flows
<clear-ddos-amtv6-aggregate-flows>
clear ddos-protection protocols amtv6 aggregate states
<clear-ddos-amtv6-aggregate-states>
clear ddos-protection protocols amtv6 aggregate statistics
<clear-ddos-amtv6-aggregate-statistics>
clear ddos-protection protocols amtv6 culprit-flows
<clear-ddos-amtv6-flows>
clear ddos-protection protocols amtv6 states
<clear-ddos-amtv6-states>
clear ddos-protection protocols amtv6 statistics
<clear-ddos-amtv6-statistics>
clear ddos-protection protocols ancp aggregate culprit-flows
<clear-ddos-ancp-aggregate-flows>
clear ddos-protection protocols ancp culprit-flows
clear ddos-protection protocols ancp
clear ddos-protection protocols ancp aggregate
clear ddos-protection protocols ancp aggregate states
clear ddos-protection protocols ancp aggregate statistics
<clear-ddos-ancp-aggregate-statistics>
clear ddos-protection protocols ancp states
<clear-ddos-ancp-states>
clear ddos-protection protocols ancp statistics
<clear-ddos-ancp-statistics>
clear ddos-protection protocols ancpv6
clear ddos-protection protocols ancpv6 aggregate
clear ddos-protection protocols ancpv6 aggregate states

clear ddos-protection protocols ancpv6 aggregate culprit-flows
clear ddos-protection protocols arp aggregate statistics
clear-ddos-arp-aggregate-statistics
clear ddos-protection protocols arp aggregate culprit-flows
clear ddos-protection protocols arp states
clear-ddos-arp-states
clear ddos-protection protocols arp statistics
<clear-ddos-arp-statistics>
clear ddos-protection protocols arp culprit-flows
clear ddos-protection protocols atm
clear ddos-protection protocols atm aggregate
clear ddos-protection protocols atm aggregate culprit-flows
clear ddos-protection protocols atm aggregate states
<clear-ddos-atm-aggregate-states>
clear ddos-protection protocols atm aggregate statistics
<clear-ddos-atm-aggregate-statistics>
clear ddos-protection protocols atm culprit-flows
clear ddos-protection protocols bfd aggregate culprit-flows
clear ddos-protection protocols atm states
clear-ddos-atm-states
clear ddos-protection protocols atm statistics
clear-ddos-atm-statistics
clear ddos-protection protocols bfd
clear ddos-protection protocols bfd aggregate
clear ddos-protection protocols bfd culprit-flows
clear ddos-protection protocols bfd aggregate states
clear-ddos-bfd-aggregate-states
clear ddos-protection protocols bfd aggregate statistics
```

```
clear-ddos-bfd-aggregate-statistics
  clear ddos-protection protocols bfd states
clear-ddos-bfd-states
clear ddos-protection protocols bfd statistics
clear-ddos-bfd-statistics
clear ddos-protection protocols bfdv6
clear ddos-protection protocols bfdv6 aggregate
clear ddos-protection protocols bfdv6 culprit-flows
clear ddos-protection protocols bfdv6 aggregate states
clear-ddos-bfdv6-aggregate-states
clear ddos-protection protocols bfdv6 aggregate statistics
clear-ddos-bfdv6-aggregate-statistics
clear ddos-protection protocols bfdv6 states
clear-ddos-bfdv6-states
clear ddos-protection protocols bfdv6 statistics
clear-ddos-bfdv6-statistics
clear ddos-protection protocols bgp
clear ddos-protection protocols bgp aggregate
clear ddos-protection protocols bgp aggregate culprit-flows
clear ddos-protection protocols bgp aggregate states
clear-ddos-bgp-aggregate-states
clear ddos-protection protocols bgp aggregate statistics
clear ddos-protection protocols bgp culprit-flows
clear ddos-protection protocols bgp states
clear-ddos-bgp-states
clear ddos-protection protocols bgp statistics
clear-ddos-bgp-statistics
clear ddos-protection protocols bgpv6
clear ddos-protection protocols bgpv6 aggregate
clear ddos-protection protocols bgpv6 aggregate culprit-flows
clear ddos-protection protocols bgpv6 aggregate states
clear-ddos-bgpv6-aggregate-states
clear ddos-protection protocols bgpv6 aggregate statistics
clear-ddos-bgpv6-aggregate-statistics
clear ddos-protection protocols bgpv6 states
clear-ddos-bgp-aggregate-states
clear-ddos-bgp-aggregate-statistics
clear-ddos-bgp-states
clear-ddos-bgp-statistics
clear-ddos-bgpv6-aggregate-states
clear-ddos-bgpv6-aggregate-statistics
clear-ddos-bgpv6-states
clear ddos-protection protocols bgpv6 statistics
<clear-ddos-bgpv6-statistics>
clear ddos-protection protocols culprit-flows
clear ddos-protection protocols demux-autosense
clear ddos-protection protocols demux-autosense aggregate
clear ddos-protection protocols demux-autosense aggregate culprit-flows
clear ddos-protection protocols demux-autosense aggregate states
clear-ddos-demuxauto-aggregate-states
clear ddos-protection protocols demux-autosense aggregate statistics
clear ddos-protection protocols demux-autosense culprit-flows
clear ddos-protection protocols demux-autosense states
clear-ddos-demuxauto-states
clear ddos-protection protocols demux-autosense statistics
clear-ddos-demuxauto-statistics
clear ddos-protection protocols dhcpv4
clear ddos-protection protocols dhcpv4 ack
clear ddos-protection protocols dhcpv4 ack culprit-flows
clear ddos-protection protocols dhcpv4 ack states
clear ddos-protection protocols dhcpv4 ack statistics
```

```

clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4v6
clear ddos-protection protocols dhcpv4v6 aggregate
clear ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<clear-ddos-dhcpv4v6-aggregate-flows>
clear ddos-protection protocols dhcpv4v6 aggregate states
<clear-ddos-dhcpv4v6-aggregate-states>
clear ddos-protection protocols dhcpv4v6 aggregate statistics
<clear-ddos-dhcpv4v6-aggregate-statistics>
clear ddos-protection protocols dhcpv4v6 culprit-flows
<clear-ddos-dhcpv4v6-flows>
clear ddos-protection protocols dhcpv4v6 states
<clear-ddos-dhcpv4v6-states>
clear ddos-protection protocols dhcpv4v6 statistics
<clear-ddos-dhcpv4v6-statistics>
clear-ddos-demuxauto-aggregate-states
clear-ddos-demuxauto-aggregate-statistics
clear-ddos-demuxauto-states
clear-ddos-demuxauto-statistics
clear-ddos-dhcpv4-ack-states
clear ddos-protection protocols dhcpv4 ack statistics
clear-ddos-dhcpv4-ack-statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4 aggregate states
clear-ddos-dhcpv4-aggregate-states
clear ddos-protection protocols dhcpv4 aggregate statistics
clear-ddos-dhcpv4-aggregate-statistics
clear ddos-protection protocols dhcpv4 bad-packets
clear ddos-protection protocols dhcpv4 bad-packets states
clear-ddos-dhcpv4-bad-pack-states
clear ddos-protection protocols dhcpv4 bad-packets statistics
clear-ddos-dhcpv4-bad-pack-statistics
clear ddos-protection protocols dhcpv4 bootp
clear ddos-protection protocols dhcpv4 bootp states
clear-ddos-dhcpv4-bootp-states
clear ddos-protection protocols dhcpv4 bootp statistics
clear-ddos-dhcpv4-bootp-statistics
clear ddos-protection protocols dhcpv4 decline
clear ddos-protection protocols dhcpv4 decline culprit-flows
clear ddos-protection protocols dhcpv4 decline states
clear-ddos-dhcpv4-decline-states
clear ddos-protection protocols dhcpv4 decline statistics
clear-ddos-dhcpv4-decline-statistics
clear ddos-protection protocols dhcpv4 discover
clear ddos-protection protocols dhcpv4 discover states
clear-ddos-dhcpv4-discover-states
clear ddos-protection protocols dhcpv4 discover statistics
clear-ddos-dhcpv4-discover-statistics
clear ddos-protection protocols dhcpv4 force-renew
clear ddos-protection protocols dhcpv4 force-renew culprit-flows
clear ddos-protection protocols dhcpv4 force-renew states
clear-ddos-dhcpv4-forcerenew-states
clear ddos-protection protocols dhcpv4 force-renew statistics
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 inform
clear ddos-protection protocols dhcpv4 inform culprit-flows
clear ddos-protection protocols dhcpv4 inform states
clear-ddos-dhcpv4-decline-states
clear-ddos-dhcpv4-decline-statistics
clear-ddos-dhcpv4-discover-states
clear-ddos-dhcpv4-discover-statistics

```

```
clear-ddos-dhcpv4-forcerenew-states
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 unclassified culprit-flows
clear ddos-protection protocols dhcpv4 unclassified states
clear-ddos-dhcpv4-unclass-states
clear ddos-protection protocols dhcpv4 unclassified statistics
clear-ddos-dhcpv4-unclass-statistics
clear ddos-protection protocols dhcpv6
clear ddos-protection protocols dhcpv6 advertise
clear ddos-protection protocols dhcpv6 advertise culprit-flows
clear ddos-protection protocols dhcpv6 advertise states
clear-ddos-dhcpv6-advertise-states
clear ddos-protection protocols dhcpv6 advertise statistics
clear-ddos-dhcpv6-advertise-statistics
clear ddos-protection protocols dhcpv6 aggregate
clear ddos-protection protocols dhcpv6 aggregate states
clear-ddos-dhcpv6-aggregate-states
clear ddos-protection protocols dhcpv6 aggregate statistics
clear-ddos-dhcpv6-aggregate-statistics
clear ddos-protection protocols dhcpv6 confirm
clear ddos-protection protocols dhcpv6 confirm culprit-flows
clear ddos-protection protocols dhcpv6 confirm states
clear-ddos-dhcpv6-confirm-states
clear ddos-protection protocols dhcpv6 confirm statistics
clear-ddos-dhcpv6-confirm-statistics
clear ddos-protection protocols dhcpv6 decline
clear ddos-protection protocols dhcpv6 decline states
clear-ddos-dhcpv6-decline-states
clear ddos-protection protocols dhcpv6 decline statistics
clear-ddos-dhcpv6-decline-statistics
clear ddos-protection protocols dhcpv6 information-request
clear ddos-protection protocols dhcpv6 information-request states
clear-ddos-dhcpv6-info-req-states
clear ddos-protection protocols dhcpv6 information-request statistics
clear-ddos-dhcpv6-info-req-statistics
clear ddos-protection protocols dhcpv6 leasequery
clear ddos-protection protocols dhcpv6 leasequery states
clear-ddos-dhcpv6-leasequery-states
clear ddos-protection protocols dhcpv6 leasequery statistics
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-data
clear ddos-protection protocols dhcpv6 leasequery-data states
clear ddos-protection protocols dhcpv6 leasequery-data statistics
clear ddos-protection protocols garp-reply
clear ddos-protection protocols garp-reply aggregate
clear ddos-protection protocols garp-reply aggregate culprit-flows
<clear-ddos-garp-reply-aggregate-flows>
clear ddos-protection protocols garp-reply aggregate states
<clear-ddos-garp-reply-aggregate-states>
clear ddos-protection protocols garp-reply aggregate statistics
<clear-ddos-garp-reply-aggregate-statistics>
clear ddos-protection protocols garp-reply culprit-flows
<clear-ddos-garp-reply-flows>
clear ddos-protection protocols garp-reply states
<clear-ddos-garp-reply-states>
clear ddos-protection protocols garp-reply statistics
<clear-ddos-garp-reply-statistics>
clear ddos-protection protocols gre hbc
clear ddos-protection protocols gre hbc culprit-flows
<clear-ddos-gre-hbc-flows>
clear ddos-protection protocols gre hbc states
```

```

<clear-ddos-gre-hbc-states>
clear ddos-protection protocols gre hbc statistics
<clear-ddos-gre-hbc-statistics>
clear ddos-protection protocols gre punt
clear ddos-protection protocols gre punt culprit-flows
<clear-ddos-gre-punt-flows>
clear ddos-protection protocols gre punt states
<clear-ddos-gre-punt-states>
clear ddos-protection protocols gre punt statistics
<clear-ddos-gre-punt-statistics>
clear ddos-protection protocols ipmc-reserved
clear ddos-protection protocols ipmc-reserved aggregate
clear ddos-protection protocols ipmc-reserved aggregate culprit-flows
<clear-ddos-ipmc-reserved-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate states
<clear-ddos-ipmc-reserved-aggregate-states>
clear ddos-protection protocols ipmc-reserved aggregate statistics
<clear-ddos-ipmc-reserved-aggregate-statistics>
clear ddos-protection protocols ipmc-reserved culprit-flows
<clear-ddos-ipmc-reserved-flows>
clear ddos-protection protocols ipmc-reserved states
<clear-ddos-ipmc-reserved-states>
clear ddos-protection protocols ipmc-reserved statistics
<clear-ddos-ipmc-reserved-statistics>
clear ddos-protection protocols ipmcast-miss
clear ddos-protection protocols ipmcast-miss aggregate
clear ddos-protection protocols ipmcast-miss aggregate culprit-flows
<clear-ddos-ipmcast-miss-aggregate-flows>
clear ddos-protection protocols ipmcast-miss aggregate states
<clear-ddos-ipmcast-miss-aggregate-states>
clear ddos-protection protocols ipmcast-miss aggregate statistics
<clear-ddos-ipmcast-miss-aggregate-statistics>
clear ddos-protection protocols ipmcast-miss culprit-flows
<clear-ddos-ipmcast-miss-flows>
clear ddos-protection protocols ipmcast-miss states
<clear-ddos-ipmcast-miss-states>
clear ddos-protection protocols ipmcast-miss statistics
<clear-ddos-ipmcast-miss-statistics>
clear ddos-protection protocols l3dest-miss
clear ddos-protection protocols l3dest-miss aggregate
clear ddos-protection protocols l3dest-miss aggregate culprit-flows
<clear-ddos-l3dest-miss-aggregate-flows>
clear ddos-protection protocols l3dest-miss aggregate states
<clear-ddos-l3dest-miss-aggregate-states>
clear ddos-protection protocols l3dest-miss aggregate statistics
<clear-ddos-l3dest-miss-aggregate-statistics>
clear ddos-protection protocols l3dest-miss culprit-flows
<clear-ddos-l3dest-miss-flows>
clear ddos-protection protocols l3dest-miss states
<clear-ddos-l3dest-miss-states>
clear ddos-protection protocols l3dest-miss statistics
<clear-ddos-l3dest-miss-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-aggregate-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate states
<clear-ddos-l3mc-sgv-hit-icl-aggregate-states>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate statistics
<clear-ddos-l3mc-sgv-hit-icl-aggregate-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
clear

```

```
ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl states
<clear-ddos-l3mc-sgv-hit-icl-states>
clear ddos-protection protocols l3mc-sgv-hit-icl statistics
<clear-ddos-l3mc-sgv-hit-icl-statistics>
clear ddos-protection protocols l3mtu-fail
clear ddos-protection protocols l3mtu-fail aggregate
clear ddos-protection protocols l3mtu-fail aggregate culprit-flows
<clear-ddos-l3mtu-fail-aggregate-flows>
clear ddos-protection protocols l3mtu-fail aggregate states
<clear-ddos-l3mtu-fail-aggregate-states>
clear ddos-protection protocols l3mtu-fail aggregate statistics
<clear-ddos-l3mtu-fail-aggregate-statistics>
clear ddos-protection protocols l3mtu-fail culprit-flows
<clear-ddos-l3mtu-fail-flows>
clear ddos-protection protocols l3mtu-fail states
<clear-ddos-l3mtu-fail-states>
clear ddos-protection protocols l3mtu-fail statistics
<clear-ddos-l3mtu-fail-statistics>
clear ddos-protection protocols l3nhop
clear ddos-protection protocols l3nhop aggregate
clear ddos-protection protocols l3nhop aggregate culprit-flows
<clear-ddos-l3nhop-aggregate-flows>
clear ddos-protection protocols l3nhop aggregate states
<clear-ddos-l3nhop-aggregate-states>
clear ddos-protection protocols l3nhop aggregate statistics
<clear-ddos-l3nhop-aggregate-statistics>
clear ddos-protection protocols l3nhop culprit-flows
<clear-ddos-l3nhop-flows>
clear ddos-protection protocols l3nhop states
<clear-ddos-l3nhop-states>
clear ddos-protection protocols l3nhop statistics
<clear-ddos-l3nhop-statistics>
clear ddos-protection protocols localnh
clear ddos-protection protocols localnh aggregate
clear ddos-protection protocols localnh aggregate culprit-flows
<clear-ddos-localnh-aggregate-flows>
clear ddos-protection protocols localnh aggregate states
<clear-ddos-localnh-aggregate-states>
clear ddos-protection protocols localnh aggregate statistics
<clear-ddos-localnh-aggregate-statistics>
clear ddos-protection protocols localnh culprit-flows
<clear-ddos-localnh-flows>
clear ddos-protection protocols localnh states
<clear-ddos-localnh-states>
clear ddos-protection protocols localnh statistics
<clear-ddos-localnh-statistics>
clear-ddos-dhcpv4-unclass-states
clear-ddos-dhcpv4-unclass-statistics
clear-ddos-dhcpv6-advertise-states
clear-ddos-dhcpv6-advertise-statistics
clear-ddos-dhcpv6-aggregate-states
clear-ddos-dhcpv6-aggregate-statistics
clear-ddos-dhcpv6-confirm-states
clear-ddos-dhcpv6-confirm-statistics
clear-ddos-dhcpv6-decline-states
clear-ddos-dhcpv6-decline-statistics
clear-ddos-dhcpv6-info-req-states
clear-ddos-dhcpv6-info-req-statistics
clear-ddos-dhcpv6-leasdaq-states
```

```
clear-ddos-dhcpv6-leasequery-states
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-done
clear ddos-protection protocols dhcpv6 leasequery-done states
clear-ddos-dhcpv6-leaseq-do-states
clear ddos-protection protocols dhcpv6 leasequery-done statistics
clear-ddos-dhcpv6-leaseq-do-statistics
clear ddos-protection protocols dhcpv6 leasequery-reply
clear ddos-protection protocols dhcpv6 leasequery-reply states
clear-ddos-dhcpv6-leaseq-re-states
clear ddos-protection protocols dhcpv6 leasequery-reply statistics
clear-ddos-dhcpv6-leaseq-re-statistics
clear ddos-protection protocols dhcpv6 rebind
clear ddos-protection protocols dhcpv6 rebind states
clear-ddos-dhcpv6-rebind-states
clear ddos-protection protocols dhcpv6 rebind statistics
clear-ddos-dhcpv6-rebind-statistics
clear ddos-protection protocols dhcpv6 reconfigure
clear ddos-protection protocols dhcpv6 reconfigure states
clear-ddos-dhcpv6-reconfig-states
clear ddos-protection protocols dhcpv6 reconfigure statistics
clear-ddos-dhcpv6-reconfig-statistics
clear ddos-protection protocols dhcpv6 relay-forward
clear ddos-protection protocols dhcpv6 relay-forward states
clear-ddos-dhcpv6-relay-for-states
clear ddos-protection protocols dhcpv6 relay-forward statistics
clear-ddos-dhcpv6-relay-for-statistics
clear ddos-protection protocols dhcpv6 relay-reply
clear ddos-protection protocols dhcpv6 relay-reply states
clear-ddos-dhcpv6-relay-rep-states
clear ddos-protection protocols dhcpv6 relay-reply statistics
clear-ddos-dhcpv6-relay-rep-statistics
clear ddos-protection protocols dhcpv6 release
clear ddos-protection protocols dhcpv6 release states
clear-ddos-dhcpv6-release-states
clear ddos-protection protocols dhcpv6 release statistics
clear-ddos-dhcpv6-release-statistics
clear ddos-protection protocols dhcpv6 renew
clear ddos-protection protocols dhcpv6 renew states
clear-ddos-dhcpv6-renew-states
clear ddos-protection protocols dhcpv6 renew statistics
clear-ddos-dhcpv6-renew-statistics
clear ddos-protection protocols dhcpv6 reply
clear ddos-protection protocols dhcpv6 reply states
clear-ddos-dhcpv6-reply-states
clear ddos-protection protocols dhcpv6 reply statistics
clear-ddos-dhcpv6-reply-statistics
clear ddos-protection protocols dhcpv6 request
clear ddos-protection protocols dhcpv6 request culprit-flows
clear ddos-protection protocols dhcpv6 request states
clear-ddos-dhcpv6-request-states
clear ddos-protection protocols dhcpv6 request statistics
clear-ddos-dhcpv6-request-statistics
clear ddos-protection protocols dhcpv6 solicit
clear ddos-protection protocols dhcpv6 solicit culprit-flows
clear ddos-protection protocols dhcpv6 solicit states
clear-ddos-dhcpv6-solicit-states
clear ddos-protection protocols dhcpv6 solicit statistics
clear-ddos-dhcpv6-solicit-statistics
clear ddos-protection protocols dhcpv6 states
clear-ddos-dhcpv6-states
```

```
clear ddos-protection protocols dhcpv6 statistics
clear-ddos-dhcpv6-statistics
clear ddos-protection protocols dhcpv6 unclassified
clear ddos-protection protocols dhcpv6 unclassified culprit-flows
clear ddos-protection protocols dhcpv6 unclassified states
clear-ddos-dhcpv6-unclass-states
clear ddos-protection protocols dhcpv6 unclassified statistics
clear-ddos-dhcpv6-unclass-statistics
clear ddos-protection protocols diameter
clear ddos-protection protocols diameter aggregate
clear ddos-protection protocols diameter aggregate culprit-flows
clear ddos-protection protocols diameter aggregate states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-dhcpv6-leaseq-da-statistics
clear-ddos-dhcpv6-leaseq-do-states
clear-ddos-dhcpv6-leaseq-do-statistics
clear-ddos-dhcpv6-leaseq-re-states
clear-ddos-dhcpv6-leaseq-re-statistics
clear-ddos-dhcpv6-rebind-states
clear-ddos-dhcpv6-rebind-statistics
clear-ddos-dhcpv6-reconfig-states
clear-ddos-dhcpv6-reconfig-statistics
clear-ddos-dhcpv6-relay-for-states
clear-ddos-dhcpv6-relay-for-statistics
clear-ddos-dhcpv6-relay-rep-states
clear-ddos-dhcpv6-relay-rep-statistics
clear-ddos-dhcpv6-release-states
clear-ddos-dhcpv6-release-statistics
clear-ddos-dhcpv6-renew-states
clear-ddos-dhcpv6-renew-statistics
clear-ddos-dhcpv6-reply-states
clear-ddos-dhcpv6-reply-statistics
clear-ddos-dhcpv6-request-states
clear-ddos-dhcpv6-request-statistics
clear-ddos-dhcpv6-solicit-states
clear-ddos-dhcpv6-solicit-statistics
clear-ddos-dhcpv6-states
clear-ddos-dhcpv6-statistics
clear-ddos-dhcpv6-unclass-states
clear-ddos-dhcpv6-unclass-statistics
clear-ddos-diameter-aggregate-states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-diameter-aggregate-statistics
clear ddos-protection protocols diameter states
clear-ddos-diameter-states
clear ddos-protection protocols diameter statistics
clear-ddos-diameter-statistics
clear ddos-protection protocols dns
clear ddos-protection protocols dns aggregate
clear ddos-protection protocols dns aggregate states
clear-ddos-dns-aggregate-states
clear ddos-protection protocols dns aggregate statistics
clear-ddos-dns-aggregate-statistics
clear ddos-protection protocols dns states
clear-ddos-dns-states
clear ddos-protection protocols dns statistics
clear-ddos-dns-statistics
clear ddos-protection protocols dtcp
clear ddos-protection protocols dtcp aggregate
clear ddos-protection protocols dtcp aggregate culprit-flows
clear ddos-protection protocols dtcp aggregate states
```

```
clear-ddos-dtcp-aggregate-states
clear ddos-protection protocols dtcp aggregate statistics
clear ddos-protection protocols dtcp culprit-flows
clear ddos-protection protocols dtcp states
clear-ddos-dtcp-states
clear ddos-protection protocols dtcp statistics
clear-ddos-dtcp-statistics
clear ddos-protection protocols dynamic-vlan
clear ddos-protection protocols dynamic-vlan aggregate
clear ddos-protection protocols dynamic-vlan aggregate culprit-flows
clear ddos-protection protocols dynamic-vlan aggregate states
clear-ddos-dynvlan-aggregate-states
clear ddos-protection protocols dynamic-vlan aggregate statistics
clear-ddos-dynvlan-aggregate-statistics
clear ddos-protection protocols dynamic-vlan states
clear-ddos-dynvlan-states
clear ddos-protection protocols dynamic-vlan statistics
clear-ddos-dynvlan-statistics
clear ddos-protection protocols egpv6
clear ddos-protection protocols egpv6 aggregate
clear ddos-protection protocols egpv6 aggregate culprit-flows
clear ddos-protection protocols egpv6 aggregate states
clear-ddos-egpv6-aggregate-states
clear ddos-protection protocols egpv6 aggregate statistics
clear-ddos-egpv6-aggregate-statistics
clear ddos-protection protocols egpv6 states
clear-ddos-egpv6-states
clear ddos-protection protocols egpv6 statistics
clear-ddos-egpv6-statistics
clear ddos-protection protocols eoam
clear ddos-protection protocols eoam aggregate
clear ddos-protection protocols eoam aggregate culprit-flows
clear ddos-protection protocols eoam aggregate states
clear-ddos-eoam-aggregate-states
clear ddos-protection protocols eoam aggregate statistics
clear-ddos-eoam-aggregate-statistics
clear ddos-protection protocols eoam states
clear-ddos-eoam-states
clear ddos-protection protocols eoam statistics
clear-ddos-eoam-statistics
clear ddos-protection protocols esmc
clear ddos-protection protocols esmc aggregate
clear ddos-protection protocols esmc aggregate culprit-flows
clear ddos-protection protocols esmc aggregate states
clear-ddos-esmc-aggregate-states
clear ddos-protection protocols esmc aggregate statistics
clear ddos-protection protocols esmc culprit-flows
clear ddos-protection protocols esmc states
clear-ddos-esmc-states
clear ddos-protection protocols esmc statistics
clear ddos-protection protocols fab-probe
clear ddos-protection protocols fab-probe aggregate
clear ddos-protection protocols fab-probe aggregate states
clear ddos-protection protocols fab-probe aggregate statistics
<clear-ddos-fab-probe-aggregate-statistics>
clear ddos-protection protocols martian-address
clear ddos-protection protocols martian-address aggregate
clear ddos-protection protocols martian-address aggregate culprit-flows
<clear-ddos-martian-address-aggregate-flows>
clear ddos-protection protocols martian-address aggregate states
<clear-ddos-martian-address-aggregate-states>
```

```
clear ddos-protection protocols martian-address aggregate statistics
<clear-ddos-martian-address-aggregate-statistics>
clear ddos-protection protocols martian-address culprit-flows
<clear-ddos-martian-address-flows>
clear ddos-protection protocols martian-address states
<clear-ddos-martian-address-states>
clear ddos-protection protocols martian-address statistics
<clear-ddos-martian-address-statistics>
clear-ddos-diameter-statistics
clear-ddos-dns-aggregate-states
clear-ddos-dns-aggregate-statistics
clear-ddos-dns-states
clear-ddos-dns-statistics
clear-ddos-dtcp-aggregate-states
clear-ddos-dtcp-aggregate-statistics
clear-ddos-dtcp-states
clear-ddos-dtcp-statistics
clear-ddos-dynvlan-aggregate-states
clear-ddos-dynvlan-aggregate-statistics
clear-ddos-dynvlan-states
clear-ddos-dynvlan-statistics
clear-ddos-egpv6-aggregate-states
clear-ddos-egpv6-aggregate-statistics
clear-ddos-egpv6-states
clear-ddos-egpv6-statistics
clear-ddos-eoam-aggregate-states
clear-ddos-eoam-aggregate-statistics
clear-ddos-eoam-states
clear-ddos-eoam-statistics
clear-ddos-esmc-aggregate-states
clear-ddos-esmc-aggregate-statistics
clear-ddos-esmc-states
clear ddos-protection protocols fab-probe states
<clear-ddos-fab-probe-states>
clear ddos-protection protocols fab-probe statistics
<clear-ddos-fab-probe-statistics>
clear-ddos-esmc-statistics
clear ddos-protection protocols firewall-host
clear ddos-protection protocols firewall-host aggregate
clear ddos-protection protocols firewall-host aggregate culprit-flows
clear ddos-protection protocols firewall-host aggregate states
clear-ddos-fw-host-aggregate-states
clear ddos-protection protocols firewall-host aggregate statistics
clear ddos-protection protocols firewall-host states
clear ddos-protection protocols firewall-host statistics
clear-ddos-esmc-statistics
clear-ddos-fw-host-aggregate-states
clear-ddos-fw-host-aggregate-statistics
<clear-ddos-fw-host-statistics>
clear-ddos-fw-host-states
clear ddos-protection protocols frame-relay
clear ddos-protection protocols frame-relay aggregate
clear ddos-protection protocols frame-relay aggregate culprit-flows
clear ddos-protection protocols frame-relay aggregate states
clear ddos-protection protocols frame-relay aggregate statistics
clear ddos-protection protocols frame-relay culprit-flows
clear ddos-protection protocols frame-relay frf15
clear ddos-protection protocols frame-relay frf15 culprit-flows
clear ddos-protection protocols frame-relay frf15 states
clear ddos-protection protocols frame-relay frf15 statistics
clear ddos-protection protocols frame-relay frf16
```

```

clear ddos-protection protocols frame-relay frf16 culprit-flows
clear ddos-protection protocols frame-relay frf16 states
clear ddos-protection protocols frame-relay frf16 statistics
clear ddos-protection protocols frame-relay states
clear ddos-protection protocols frame-relay statistics
clear ddos-protection protocols ftp
clear ddos-protection protocols ftp aggregate
clear ddos-protection protocols ftp aggregate culprit-flows
clear ddos-protection protocols ftp aggregate states
clear-ddos-ftp-aggregate-states
clear ddos-protection protocols ftp aggregate statistics
clear-ddos-ftp-aggregate-statistics
clear ddos-protection protocols ftp states
clear-ddos-ftp-states
clear ddos-protection protocols ftp statistics
clear-ddos-ftp-statistics
clear ddos-protection protocols ftpv6
clear ddos-protection protocols ftpv6 aggregate
clear ddos-protection protocols ftpv6 aggregate culprit-flows
clear ddos-protection protocols ftpv6 aggregate states
clear-ddos-ftp6-aggregate-states
clear ddos-protection protocols ftpv6 aggregate statistics
clear-ddos-ftp6-aggregate-statistics
clear ddos-protection protocols ftpv6 states
clear-ddos-ftp6-states
clear ddos-protection protocols ftpv6 statistics
clear-ddos-ftp6-statistics
clear ddos-protection protocols gre
clear ddos-protection protocols gre aggregate
clear ddos-protection protocols gre aggregate culprit-flow
clear ddos-protection protocols gre aggregate states
clear ddos-protection protocols gre culprit-flows
clear-ddos-ftp-statistics
clear-ddos-ftp6-aggregate-states
clear-ddos-ftp6-aggregate-statistics
clear-ddos-ftp6-states
clear-ddos-ftp6-statistics
clear-ddos-gre-aggregate-states
clear ddos-protection protocols gre aggregate statistics
clear-ddos-gre-aggregate-statistics
clear ddos-protection protocols gre states
clear-ddos-gre-states
clear ddos-protection protocols gre statistics
clear-ddos-gre-statistics
clear ddos-protection protocols icmp
clear ddos-protection protocols icmp aggregate
clear ddos-protection protocols icmp aggregate states
clear-ddos-icmp-aggregate-states
clear ddos-protection protocols icmp aggregate statistics
clear-ddos-icmp-aggregate-statistics
clear ddos-protection protocols icmp states
clear-ddos-icmp-states
clear ddos-protection protocols icmp statistics
clear-ddos-icmp-statistics
clear ddos-protection protocols icmpv6
clear ddos-protection protocols icmpv6 aggregate
clear ddos-protection protocols icmpv6 aggregate culprit-flows
clear ddos-protection protocols icmpv6 aggregate states
<clear-ddos-icmpv6-aggregate-states>
clear ddos-protection protocols icmpv6 aggregate statistics
<clear-ddos-icmp-aggregate-statistics>

```

```
<clear-ddos-icmpv6-aggregate-statistics>
clear ddos-protection protocols icmpv6 states
<clear-ddos-icmpv6-states>
clear ddos-protection protocols icmpv6 statistics
<clear-ddos-icmpv6-statistics>
clear ddos-protection protocols igmp
clear ddos-protection protocols igmp aggregate
clear ddos-protection protocols igmp aggregate culprit-flows
clear ddos-protection protocols igmp aggregate states
clear-ddos-igmp-aggregate-states
clear ddos-protection protocols igmp aggregate statistics
clear-ddos-igmp-aggregate-statistics
clear ddos-protection protocols igmp states
clear-ddos-igmp-states
clear ddos-protection protocols igmp statistics
clear-ddos-igmp-statistics
clear ddos-protection protocols igmp-snoop
clear ddos-protection protocols igmp-snoop aggregate
clear ddos-protection protocols igmp-snoop aggregate states
clear-ddos-igmp-snoop-aggregate-states
clear ddos-protection protocols igmp-snoop aggregate statistics
clear-ddos-igmp-snoop-aggregate-statistics
clear ddos-protection protocols igmp-snoop states
clear-ddos-igmp-snoop-states
clear ddos-protection protocols igmp-snoop statistics
clear-ddos-igmp-snoop-statistics
clear ddos-protection protocols igmpv4v6
clear ddos-protection protocols igmpv4v6 aggregate
clear ddos-protection protocols igmpv4v6 aggregate states
clear-ddos-igmpv4v6-aggregate-states
clear ddos-protection protocols igmpv4v6 aggregate statistics
clear ddos-protection protocols igmpv4v6 culprit-flows
clear ddos-protection protocols igmpv4v6 states
clear-ddos-igmpv4v6-states
clear ddos-protection protocols igmpv4v6 statistics
clear-ddos-igmpv4v6-statistics
clear ddos-protection protocols igmpv6
clear ddos-protection protocols igmpv6 aggregate
clear ddos-protection protocols igmpv6 aggregate culprit-flows
clear ddos-protection protocols igmpv6 aggregate states
clear ddos-protection protocols igmpv6 aggregate statistics
clear ddos-protection protocols igmpv6 states
clear ddos-protection protocols igmpv6 statistics
<clear-ddos-igmpv6-statistics>clear-ddos-igmp-snoop-states
clear-ddos-igmp-snoop-statistics
clear-ddos-igmp-statistics
clear-ddos-igmpv4v6-aggregate-states
clear-ddos-igmpv4v6-aggregate-statistics
clear-ddos-igmpv4v6-states
clear-ddos-igmpv4v6-statistics
clear-ddos-igmpv6-aggregate-states
clear ddos-protection protocols igmpv6 aggregate statistics
clear-ddos-igmpv6-aggregate-statistics
clear ddos-protection protocols igmpv6 states
clear-ddos-igmpv6-states
clear ddos-protection protocols inline-ka
clear ddos-protection protocols inline-ka aggregate
clear ddos-protection protocols inline-ka aggregate culprit-flows
clear ddos-protection protocols inline-ka aggregate states
clear ddos-protection protocols inline-ka aggregate statistics
clear ddos-protection protocols inline-ka culprit-flows
```

```

clear ddos-protection protocols inline-ka states
clear ddos-protection protocols inline-ka statistics
clear ddos-protection protocols inline-svcs
clear ddos-protection protocols inline-svcs aggregate
clear ddos-protection protocols inline-svcs aggregate culprit-flows
clear ddos-protection protocols inline-svcs aggregate states
clear ddos-protection protocols inline-svcs aggregate statistics
clear ddos-protection protocols inline-svcs culprit-flows
clear ddos-protection protocols inline-svcs states
clear ddos-protection protocols inline-svcs statistics
clear ddos-protection protocols ip-fragments
clear ddos-protection protocols ip-fragments aggregate
clear ddos-protection protocols ip-fragments aggregate states
clear-ddos-ip-frag-aggregate-states
clear ddos-protection protocols ip-fragments aggregate statistics
clear ddos-protection protocols ip-fragments culprit-flows
clear ddos-protection protocols ip-fragments first-fragment
clear ddos-protection protocols ip-fragments first-fragment states
clear-ddos-ip-frag-first-frag-states
clear ddos-protection protocols ip-fragments first-fragment statistics
clear-ddos-ip-frag-first-frag-statistics
clear ddos-protection protocols ip-fragments states
clear-ddos-ip-frag-states
clear ddos-protection protocols ip-fragments statistics
clear-ddos-ip-frag-statistics
clear ddos-protection protocols ip-fragments trail-fragment
clear ddos-protection protocols ip-fragments trail-fragment culprit-flows
clear ddos-protection protocols ip-fragments trail-fragment states
clear-ddos-ip-frag-trail-frag-states
clear ddos-protection protocols ip-fragments trail-fragment statistics
clear-ddos-ip-frag-trail-frag-statistics
clear ddos-protection protocols ip-options
clear ddos-protection protocols ip-options aggregate
clear ddos-protection protocols ip-options aggregate states
clear-ddos-ip-opt-aggregate-states
clear ddos-protection protocols ip-options aggregate statistics
clear-ddos-ip-opt-aggregate-statistics
clear ddos-protection protocols ip-options non-v4v6
clear ddos-protection protocols ip-options non-v4v6 states
<clear-ddos-ip-opt-non-v4v6-states>
clear-ddos-ip-frag-aggregate-states
clear-ddos-ip-frag-aggregate-statistics
clear-ddos-ip-frag-first-frag-states
clear-ddos-ip-frag-first-frag-statistics
clear-ddos-ip-frag-states
clear-ddos-ip-frag-statistics
clear-ddos-ip-frag-trail-frag-states
clear-ddos-ip-frag-trail-frag-statistics
clear-ddos-ip-opt-aggregate-states
clear-ddos-ip-opt-aggregate-statistics
clear ddos-protection protocols ip-options non-v4v6 statistics
<clear-ddos-ip-opt-non-v4v6-statistics>
clear ddos-protection protocols ip-options router-alert
clear ddos-protection protocols ip-options router-alert culprit-flows
clear ddos-protection protocols ip-options router-alert states
clear-ddos-ip-opt-rt-alert-states
clear ddos-protection protocols ip-options router-alert statistics
clear-ddos-ip-opt-rt-alert-statistics
clear ddos-protection protocols ip-options states
clear-ddos-ip-opt-states
clear ddos-protection protocols ip-options statistics

```

```
clear-ddos-ip-opt-statistics
clear ddos-protection protocols ip-options unclassified
clear ddos-protection protocols ip-options unclassified culprit-flows
clear ddos-protection protocols ip-options unclassified states
clear ddos-protection protocols ip-options unclassified statistics
clear-ddos-ip-opt-unclass-statistics
clear ddos-protection protocols ipv4-unclassified
clear ddos-protection protocols ipv4-unclassified aggregate
clear ddos-protection protocols ipv4-unclassified aggregate states
clear-ddos-ipv4-uncls-aggregate-states
clear ddos-protection protocols ipv4-unclassified aggregate statistics
clear-ddos-ipv4-uncls-aggregate-statistics
clear ddos-protection protocols ipv4-unclassified states
clear-ddos-ipv4-uncls-states
clear ddos-protection protocols ipv4-unclassified statistics
clear-ddos-ipv4-uncls-statistics
clear ddos-protection protocols ipv6-unclassified
clear ddos-protection protocols ipv6-unclassified aggregate
clear ddos-protection protocols ipv6-unclassified aggregate states
clear-ddos-ipv6-uncls-aggregate-states
clear ddos-protection protocols ipv6-unclassified aggregate statistics
clear-ddos-ipv6-uncls-aggregate-statistics
clear ddos-protection protocols ipv6-unclassified states
clear-ddos-ipv6-uncls-states
clear ddos-protection protocols ipv6-unclassified statistics
clear-ddos-ipv6-uncls-statistics
clear ddos-protection protocols isis
clear ddos-protection protocols isis aggregate
clear ddos-protection protocols isis aggregate culprit-flows
clear ddos-protection protocols isis aggregate states
clear-ddos-ip-opt-rt-alert-states
clear-ddos-ip-opt-rt-alert-statistics
clear-ddos-ip-opt-states
clear-ddos-ip-opt-statistics
clear-ddos-ip-opt-unclass-states
clear-ddos-ip-opt-unclass-statistics
clear-ddos-ipv4-uncls-aggregate-states
clear-ddos-isis-aggregate-states
clear ddos-protection protocols isis aggregate statistics
<clear-ddos-isis-aggregate-statistics>
clear ddos-protection protocols isis culprit-flows
clear ddos-protection protocols isis states
clear-ddos-isis-states
clear ddos-protection protocols isis statistics
clear-ddos-isis-statistics
clear ddos-protection protocols jfm
clear ddos-protection protocols jfm aggregate
clear ddos-protection protocols jfm aggregate culprit-flows
clear ddos-protection protocols jfm aggregate states
clear-ddos-jfm-aggregate-states
clear ddos-protection protocols jfm aggregate statistics
clear-ddos-jfm-aggregate-statistics
clear ddos-protection protocols jfm states
clear-ddos-jfm-states
clear ddos-protection protocols jfm statistics
<clear-ddos-jfm-statistics>
clear ddos-protection protocols keepalive
clear ddos-protection protocols keepalive aggregate
clear ddos-protection protocols keepalive aggregate culprit-flows
clear ddos-protection protocols keepalive aggregate states
clear ddos-protection protocols keepalive aggregate statistics
```

```
clear ddos-protection protocols keepalive culprit-flows
clear ddos-protection protocols keepalive states
clear ddos-protection protocols keepalive statistics
clear ddos-protection protocols l2pt
clear ddos-protection protocols l2pt aggregate
clear ddos-protection protocols l2pt aggregate states
clear ddos-protection protocols l2pt aggregate statistics
clear ddos-protection protocols l2pt culprit-flows
clear ddos-protection protocols l2pt states
clear ddos-protection protocols l2pt statistics
clear ddos-protection protocols l2tp
clear ddos-protection protocols l2tp aggregate
clear ddos-protection protocols l2tp aggregate culprit-flows
clear ddos-protection protocols l2tp aggregate states
clear-ddos-l2tp-aggregate-states
clear ddos-protection protocols l2tp aggregate statistics
clear-ddos-l2tp-aggregate-statistics
clear ddos-protection protocols l2tp states
clear-ddos-l2tp-states
clear ddos-protection protocols l2tp statistics
clear-ddos-l2tp-statistics
clear ddos-protection protocols lacp
clear ddos-protection protocols lacp aggregate
clear ddos-protection protocols lacp aggregate culprit-flows
clear ddos-protection protocols lacp aggregate states
clear-ddos-lacp-aggregate-states
clear ddos-protection protocols lacp aggregate statistics
clear-ddos-lacp-aggregate-statistics
clear ddos-protection protocols lacp states
clear-ddos-lacp-states
clear ddos-protection protocols lacp statistics
clear-ddos-lacp-statistics
clear ddos-protection protocols ldp
clear ddos-protection protocols ldp aggregate
clear ddos-protection protocols ldp aggregate culprit-flows
clear ddos-protection protocols ldp aggregate states
clear-ddos-isis-states
clear-ddos-isis-statistics
clear-ddos-jfm-aggregate-states
clear-ddos-jfm-aggregate-statistics
clear-ddos-jfm-states
clear-ddos-l2tp-aggregate-states
clear-ddos-l2tp-aggregate-statistics
clear-ddos-l2tp-states
clear-ddos-l2tp-statistics
clear-ddos-lacp-aggregate-states
clear-ddos-lacp-aggregate-statistics
clear-ddos-lacp-states
clear-ddos-lacp-statistics
clear-ddos-ldp-aggregate-states
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp statistics
clear ddos-protection protocols ldp statistics
clear-ddos-ldp-statistics
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6
```

```
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate statistics
clear ddos-protection protocols ldpv6 aggregate statistics
clear-ddos-ldpv6-aggregate-statistics
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp states
clear ddos-protection protocols lldp states
clear-ddos-lddp-states
clear ddos-protection protocols lldp statistics
clear ddos-protection protocols lldp statistics
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp states
clear ddos-protection protocols lmp states
clear ddos-protection protocols lmp statistics
clear ddos-protection protocols lmp statistics
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 culprit-flows
clear ddos-protection protocols lmpv6 states
clear-ddos-lmpv6-states
clear ddos-protection protocols lmpv6 statistics
clear-ddos-lmpv6-statistics
clear ddos-protection protocols mac-host
clear ddos-protection protocols mac-host aggregate
clear ddos-protection protocols mac-host aggregate culprit-flows
clear ddos-protection protocols mac-host aggregate states
```

```

clear-ddos-mac-host-aggregate-states
clear ddos-protection protocols mac-host aggregate statistics
clear-ddos-mac-host-aggregate-statistics
clear ddos-protection protocols mac-host states
clear-ddos-mac-host-states
clear ddos-protection protocols mac-host statistics
clear ddos-protection protocols mcast-snoop
clear ddos-protection protocols mcast-snoop aggregate
clear ddos-protection protocols mcast-snoop aggregate culprit-flows
clear ddos-protection protocols mcast-snoop aggregate states
clear ddos-protection protocols mcast-snoop aggregate statistics
clear ddos-protection protocols mcast-snoop culprit-flows
clear ddos-protection protocols mcast-snoop igmp
clear ddos-protection protocols mlp
clear ddos-protection protocols mlp add
clear ddos-protection protocols mlp add culprit-flows
<clear-ddos-mlp-add-flows>
clear ddos-protection protocols mlp add states
<clear-ddos-mlp-add-states>
clear ddos-protection protocols mlp add statistics
<clear-ddos-mlp-add-statistics>
clear ddos-protection protocols mlp aggregate
clear ddos-protection protocols mlp aggregate culprit-flows
clear ddos-protection protocols mlp aggregate states
clear-ddos-mlp-aggregate-states
clear ddos-protection protocols mlp aggregate statistics
clear-ddos-mlp-aggregate-statistics
clear ddos-protection protocols mlp aging-exception
clear ddos-protection protocols mlp aging-exception culprit-flows
clear ddos-protection protocols mlp aging-exception states
clear-ddos-mlp-aging-exc-states
clear ddos-protection protocols mlp aging-exception statistics
clear-ddos-mlp-aging-exc-statistics
clear ddos-protection protocols mlp packets
clear ddos-protection protocols mlp packets states
clear-ddos-mlp-packets-states
clear ddos-protection protocols mlp packets statistics
clear-ddos-mlp-packets-statistics
clear ddos-protection protocols mlp states
clear-ddos-mlp-states
clear ddos-protection protocols mlp statistics
clear-ddos-mlp-statistics
clear ddos-protection protocols mlp unclassified
clear ddos-protection protocols mlp unclassified states
clear-ddos-mlp-unclass-states
clear ddos-protection protocols mlp unclassified statistics
clear-ddos-mlp-unclass-statistics
clear ddos-protection protocols msdp
clear ddos-protection protocols msdp aggregate
clear ddos-protection protocols msdp aggregate states
clear-ddos-msdp-aggregate-states
clear ddos-protection protocols msdp aggregate statistics
clear ddos-protection protocols msdp culprit-flows
clear ddos-protection protocols msdp states
clear-ddos-msdp-states
clear ddos-protection protocols msdp statistics
clear-ddos-msdp-statistics
clear ddos-protection protocols msdpv6
clear ddos-protection protocols msdpv6 aggregate
clear ddos-protection protocols msdpv6 aggregate culprit-flows
clear ddos-protection protocols msdpv6 aggregate states

```

```
clear-ddos-msdpv6-aggregate-states
clear ddos-protection protocols msdpv6 aggregate statistics
clear-ddos-msdpv6-aggregate-statistics
clear ddos-protection protocols msdpv6 states
clear-ddos-msdpv6-states
clear ddos-protection protocols msdpv6 statistics
clear-ddos-msdpv6-statistics
clear ddos-protection protocols multicast-copy
clear ddos-protection protocols multicast-copy aggregate
clear ddos-protection protocols multicast-copy aggregate states
clear-ddos-mcast-copy-aggregate-states
clear ddos-protection protocols multicast-copy aggregate statistics
clear-ddos-mcast-copy-aggregate-statistics
clear ddos-protection protocols multicast-copy states
clear-ddos-mcast-copy-states
clear ddos-protection protocols multicast-copy statistics
clear-ddos-mcast-copy-statistics
clear ddos-protection protocols mvrp
clear ddos-protection protocols mvrp aggregate
clear ddos-protection protocols mvrp aggregate states
clear-ddos-mvrp-aggregate-states
clear ddos-protection protocols mvrp aggregate statistics
clear ddos-protection protocols mvrp culprit-flows
clear ddos-protection protocols mvrp states
clear-ddos-mvrp-states
clear ddos-protection protocols mvrp statistics
clear-ddos-mvrp-statistics
clear ddos-protection protocols ndpv6
clear ddos-protection protocols ndpv6 aggregate
clear ddos-protection protocols ndpv6 aggregate states
clear ddos-protection protocols ndpv6 aggregate statistics
clear ddos-protection protocols ndpv6 states
clear ddos-protection protocols ndpv6 statistics
clear ddos-protection protocols nonucast-switch
clear ddos-protection protocols nonucast-switch aggregate
clear ddos-protection protocols nonucast-switch aggregate culprit-flows
<clear-ddos-nonucast-switch-aggregate-flows>
clear ddos-protection protocols nonucast-switch aggregate states
<clear-ddos-nonucast-switch-aggregate-states>
clear ddos-protection protocols nonucast-switch aggregate statistics
<clear-ddos-nonucast-switch-aggregate-statistics>
clear ddos-protection protocols nonucast-switch culprit-flows
<clear-ddos-nonucast-switch-flows>
clear ddos-protection protocols nonucast-switch states
<clear-ddos-nonucast-switch-states>
clear ddos-protection protocols nonucast-switch statistics
<clear-ddos-nonucast-switch-statistics>
clear ddos-protection protocols ntp aggregate
clear ddos-protection protocols ntp aggregate states
clear-ddos-ntp-aggregate-states
clear ddos-protection protocols ntp aggregate statistics
clear ddos-protection protocols ntp culprit-flows
clear ddos-protection protocols ntp states
clear-ddos-ntp-states
clear ddos-protection protocols ntp statistics
clear-ddos-ntp-statistics
clear ddos-protection protocols oam-lfm
clear ddos-protection protocols oam-lfm aggregate
clear ddos-protection protocols oam-lfm aggregate states
clear-ddos-oam-lfm-aggregate-states
clear ddos-protection protocols oam-lfm aggregate statistics
```

```
clear-ddos-oam-lfm-aggregate-statistics
clear ddos-protection protocols oam-lfm states
clear-ddos-oam-lfm-states
clear ddos-protection protocols oam-lfm statistics
clear-ddos-oam-lfm-statistics
clear ddos-protection protocols ospf
clear ddos-protection protocols ospf aggregate
clear ddos-protection protocols ospf aggregate culprit-flows
clear ddos-protection protocols ospf aggregate states
clear-ddos-ospf-aggregate-states
clear ddos-protection protocols ospf aggregate statistics
clear-ddos-ospf-aggregate-statistics
clear ddos-protection protocols ospf states
clear ddos-protection protocols ospf statistics
clear ddos-protection protocols ospf-hello
clear ddos-protection protocols ospf-hello aggregate
clear ddos-protection protocols ospf-hello aggregate culprit-flows
<clear-ddos-ospf-hello-aggregate-flows>
clear ddos-protection protocols ospf-hello aggregate states
<clear-ddos-ospf-hello-aggregate-states>
clear ddos-protection protocols ospf-hello aggregate statistics
<clear-ddos-ospf-hello-aggregate-statistics>
clear ddos-protection protocols ospf-hello culprit-flows
<clear-ddos-ospf-hello-flows>
clear ddos-protection protocols ospf-hello states
<clear-ddos-ospf-hello-states>
clear ddos-protection protocols ospf-hello statistics
<clear-ddos-ospf-hello-statistics>
clear ddos-protection protocols ospfv3v6
clear ddos-protection protocols ospfv3v6 aggregate
clear ddos-protection protocols ospfv3v6 aggregate culprit-flows
clear ddos-protection protocols ospfv3v6 aggregate states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear ddos-protection protocols ospfv3v6 states
clear ddos-protection protocols ospfv3v6 statistics
clear-ddos-ldp-states
clear-ddos-ldp-states
clear-ddos-ldp-statistics
clear-ddos-ldp-statistics
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-states
clear-ddos-ldpv6-states
clear-ddos-ldpv6-statistics
clear-ddos-ldpv6-statistics
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-states
clear-ddos-lldp-states
clear-ddos-lldp-statistics
clear-ddos-lldp-statistics
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-states
clear-ddos-lmp-states
```

```
clear-ddos-lmp-statistics
clear-ddos-lmp-statistics
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-states
clear-ddos-lmpv6-statistics
clear-ddos-mac-host-aggregate-states
clear-ddos-mac-host-aggregate-statistics
clear-ddos-mac-host-states
clear-ddos-mac-host-statistics
clear-ddos-mcast-copy-aggregate-states
clear-ddos-mcast-copy-aggregate-statistics
clear-ddos-mcast-copy-states
clear-ddos-mcast-copy-statistics
clear-ddos-mlp-aggregate-states
clear-ddos-mlp-aggregate-statistics
clear-ddos-mlp-aging-exc-states
clear-ddos-mlp-aging-exc-statistics
clear-ddos-mlp-packets-states
clear-ddos-mlp-packets-statistics
clear-ddos-mlp-states
clear-ddos-mlp-statistics
clear-ddos-mlp-unclass-states
clear-ddos-mlp-unclass-statistics
clear-ddos-msdp-aggregate-states
clear-ddos-msdp-aggregate-statistics
clear-ddos-msdp-states
clear-ddos-msdp-statistics
clear-ddos-msdpv6-aggregate-states
clear-ddos-msdpv6-aggregate-statistics
clear-ddos-msdpv6-states
clear-ddos-msdpv6-statistics
clear-ddos-mvrp-aggregate-states
clear-ddos-mvrp-aggregate-statistics
clear-ddos-mvrp-states
clear-ddos-mvrp-statistics
clear-ddos-ntp-aggregate-states
clear-ddos-ntp-aggregate-statistics
clear-ddos-ntp-states
clear-ddos-ntp-statistics
clear-ddos-oam-lfm-aggregate-states
clear-ddos-oam-lfm-aggregate-statistics
clear-ddos-oam-lfm-states
clear-ddos-oam-lfm-statistics
clear-ddos-ospf-aggregate-states
clear-ddos-ospf-aggregate-statistics
clear-ddos-ospf-states
clear-ddos-ospf-statistics
clear-ddos-ospfv3v6-aggregate-states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear-ddos-ospfv3v6-aggregate-statistics
clear ddos-protection protocols ospfv3v6 states
clear-ddos-ospfv3v6-states
clear ddos-protection protocols pimv6
clear-ddos-pim-statistics
clear ddos-protection protocols pim-ctrl
clear ddos-protection protocols pim-ctrl aggregate
clear ddos-protection protocols pim-ctrl aggregate culprit-flows
<clear-ddos-pim-ctrl-aggregate-flows>
clear ddos-protection protocols pim-ctrl aggregate states
<clear-ddos-pim-ctrl-aggregate-states>
```

```

clear ddos-protection protocols pim-ctrl aggregate statistics
<clear-ddos-pim-ctrl-aggregate-statistics>
clear ddos-protection protocols pim-ctrl culprit-flows
<clear-ddos-pim-ctrl-flows>
clear ddos-protection protocols pim-ctrl states
<clear-ddos-pim-ctrl-states>
clear ddos-protection protocols pim-ctrl statistics
<clear-ddos-pim-ctrl-statistics>
clear ddos-protection protocols pim-data
clear ddos-protection protocols pim-data aggregate
clear ddos-protection protocols pim-data aggregate culprit-flows
<clear-ddos-pim-data-aggregate-flows>
clear ddos-protection protocols pim-data aggregate states
<clear-ddos-pim-data-aggregate-states>
clear ddos-protection protocols pim-data aggregate statistics
<clear-ddos-pim-data-aggregate-statistics>
clear ddos-protection protocols pim-data culprit-flows
<clear-ddos-pim-data-flows>
clear ddos-protection protocols pim-data states
<clear-ddos-pim-data-states>
clear ddos-protection protocols pim-data statistics
<clear-ddos-pim-data-statistics>
clear ddos-protection protocols pfe-alive
clear ddos-protection protocols pfe-alive aggregate
clear ddos-protection protocols pfe-alive aggregate states
clear-ddos-pfe-alive-aggregate-states
clear ddos-protection protocols pfe-alive aggregate statistics
clear ddos-protection protocols pfe-alive culprit-flows
clear ddos-protection protocols pfe-alive states
clear-ddos-pfe-alive-states
clear ddos-protection protocols pfe-alive statistics
clear-ddos-pfe-alive-statistics
clear ddos-protection protocols pim
clear ddos-protection protocols pim aggregate
clear ddos-protection protocols pim aggregate states
clear-ddos-pim-aggregate-states
clear ddos-protection protocols pim aggregate statistics
clear ddos-protection protocols pim culprit-flows
clear ddos-protection protocols pim states
clear-ddos-pim-states
clear ddos-protection protocols pim statistics
clear-ddos-pim-statistics
clear ddos-protection protocols pimv6
clear ddos-protection protocols pimv6 aggregate
clear ddos-protection protocols pimv6 aggregate culprit-flows
clear ddos-protection protocols pimv6 aggregate states
clear ddos-protection protocols pimv6 aggregate statistics
clear ddos-protection protocols pimv6 states
clear ddos-protection protocols pimv6 statistics
clear ddos-protection protocols pmvrp
clear ddos-protection protocols pmvrp aggregate
clear ddos-protection protocols pmvrp aggregate states
clear-ddos-pmvrp-aggregate-states
clear ddos-protection protocols pmvrp aggregate statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows

```

```
clear ddos-protection protocols pmvrp states
clear-ddos-pmvrp-states
clear ddos-protection protocols pmvrp statistics
clear-ddos-pmvrp-statistics
clear ddos-protection protocols pos
clear ddos-protection protocols pos aggregate
clear ddos-protection protocols pos aggregate states
clear-ddos-pos-aggregate-states
clear ddos-protection protocols pos aggregate statistics
clear-ddos-pos-aggregate-statistics
clear ddos-protection protocols pos states
clear-ddos-pos-states
clear ddos-protection protocols pos statistics
clear-ddos-pos-statistics
clear ddos-protection protocols ppp
clear ddos-protection protocols ppp aggregate
clear ddos-protection protocols ppp aggregate states
clear-ddos-ppp-aggregate-states
clear ddos-protection protocols ppp aggregate statistics
clear-ddos-ppp-aggregate-statistics
clear ddos-protection protocols ppp authentication
clear ddos-protection protocols ppp authentication states
clear-ddos-ppp-auth-states
clear ddos-protection protocols ppp authentication statistics
clear-ddos-ppp-auth-statistics
clear ddos-protection protocols ppp ipcp
clear ddos-protection protocols ppp ipcp states
clear-ddos-ppp-ipcp-states
clear ddos-protection protocols ppp ipcp statistics
clear-ddos-ppp-ipcp-statistics
clear ddos-protection protocols ppp ipv6cp
clear ddos-protection protocols ppp ipv6cp states
clear-ddos-ppp-ipv6cp-states
clear ddos-protection protocols ppp ipv6cp statistics
clear-ddos-ppp-ipv6cp-statistics
clear ddos-protection protocols ppp isis
clear ddos-protection protocols ppp isis states
clear-ddos-ppp-isis-states
clear ddos-protection protocols ppp isis statistics
clear-ddos-ppp-isis-statistics
clear ddos-protection protocols ppp lcp
clear ddos-protection protocols ppp lcp states
clear-ddos-ppp-lcp-states
clear ddos-protection protocols ppp lcp statistics
clear-ddos-ppp-lcp-statistics
clear ddos-protection protocols ppp mplsdp
clear ddos-protection protocols ppp mplsdp states
clear-ddos-ppp-mplsdp-states
clear ddos-protection protocols ppp mplsdp statistics
clear-ddos-ppp-mplsdp-statistics
clear ddos-protection protocols ppp states
clear-ddos-ppp-states
clear ddos-protection protocols ppp statistics
clear-ddos-ppp-statistics
clear ddos-protection protocols ppp unclassified
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
<clear-ddos-ppp-unclass-statistics>
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
clear ddos-protection protocols pppoe aggregate states
```

```
clear-ddos-pppoe-aggregate-states
clear ddos-protection protocols pppoe aggregate statistics
clear-ddos-pppoe-aggregate-statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear-ddos-pppoe-padi-states
clear ddos-protection protocols pppoe padi statistics
clear-ddos-pppoe-padi-statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear-ddos-pppoe-padm-states
clear ddos-protection protocols pppoe padm statistics
clear-ddos-pppoe-padm-statistics
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
clear-ddos-pppoe-padn-states
clear ddos-protection protocols pppoe padn statistics
clear-ddos-pppoe-padn-statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear-ddos-pppoe-pado-states
clear ddos-protection protocols pppoe pado statistics
clear-ddos-pppoe-pado-statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear-ddos-pppoe-padr-states
clear ddos-protection protocols pppoe padr statistics
clear-ddos-pppoe-padr-statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear-ddos-pppoe-pads-states
clear ddos-protection protocols pppoe pads statistics
clear-ddos-pppoe-pads-statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear-ddos-pppoe-padt-states
clear ddos-protection protocols pppoe padt statistics
clear-ddos-pppoe-padt-statistics
clear ddos-protection protocols pppoe states
clear-ddos-pppoe-states
clear ddos-protection protocols pppoe statistics
clear-ddos-pppoe-statistics
clear ddos-protection protocols ptp
clear ddos-protection protocols ptp aggregate
clear ddos-protection protocols ptp aggregate states
clear-ddos-ntp-aggregate-states
clear ddos-protection protocols ptp aggregate statistics
clear-ddos-ntp-aggregate-statistics
clear ddos-protection protocols ptp states
clear-ddos-ntp-states
clear ddos-protection protocols ptp statistics
clear-ddos-ntp-statistics
clear ddos-protection protocols pvstp
clear ddos-protection protocols pvstp aggregate
clear ddos-protection protocols pvstp aggregate states
clear-ddos-pvstp-aggregate-states
clear ddos-protection protocols pvstp aggregate statistics
clear-ddos-pvstp-aggregate-statistics
clear ddos-protection protocols pvstp states
clear-ddos-pvstp-states
clear ddos-protection protocols pvstp statistics
```

```
clear-ddos-pvstp-statistics
clear ddos-protection protocols radius
clear ddos-protection protocols radius accounting
clear ddos-protection protocols radius accounting states
clear-ddos-radius-account-states
clear ddos-protection protocols radius accounting statistics
clear-ddos-radius-account-statistics
clear ddos-protection protocols radius aggregate
clear ddos-protection protocols radius aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius aggregate statistics
clear-ddos-radius-aggregate-statistics
clear ddos-protection protocols radius authorization
clear ddos-protection protocols radius authorization states
clear ddos-protection protocols radius authorization statistics
clear-ddos-ospfv3v6-statistics
clear-ddos-pfe-alive-aggregate-states
clear-ddos-pfe-alive-aggregate-statistics
clear-ddos-pfe-alive-states
clear-ddos-pfe-alive-statistics
clear-ddos-pim-aggregate-states
clear-ddos-pim-aggregate-statistics
clear-ddos-pim-states
clear-ddos-pmvrp-aggregate-states
clear-ddos-pmvrp-aggregate-statistics
clear-ddos-pmvrp-states
clear-ddos-pmvrp-statistics
clear-ddos-pos-aggregate-states
clear-ddos-pos-aggregate-statistics
clear-ddos-pos-states
clear-ddos-pos-statistics
clear-ddos-ppp-aggregate-states
clear-ddos-ppp-aggregate-statistics
clear-ddos-ppp-auth-states
clear-ddos-ppp-ipcp-states
clear-ddos-ppp-ipcp-statistics
clear-ddos-ppp-ipv6cp-states
clear-ddos-ppp-ipv6cp-statistics
clear-ddos-ppp-isis-states
clear-ddos-ppp-isis-statistics
clear-ddos-ppp-lcp-states
clear-ddos-ppp-lcp-statistics
clear-ddos-ppp-mplscp-states
clear-ddos-ppp-mplscp-statistics
clear-ddos-pppoe-aggregate-states
clear-ddos-pppoe-aggregate-statistics
clear-ddos-pppoe-padi-states
clear-ddos-pppoe-padi-statistics
clear-ddos-pppoe-padm-states
clear-ddos-pppoe-padm-statistics
clear-ddos-pppoe-padn-states
clear-ddos-pppoe-padn-statistics
clear-ddos-pppoe-pado-states
clear-ddos-pppoe-pado-statistics
clear-ddos-pppoe-padr-states
clear-ddos-pppoe-padr-statistics
clear-ddos-pppoe-pads-states
clear-ddos-pppoe-pads-statistics
clear-ddos-pppoe-padt-states
clear-ddos-pppoe-padt-statistics
clear-ddos-pppoe-states
```

```
clear-ddos-pppoe-statistics
clear-ddos-ppp-states
clear-ddos-ppp-statistics
clear-ddos-ntp-aggregate-states
clear-ddos-ntp-aggregate-statistics
clear-ddos-ntp-states
clear-ddos-ntp-statistics
clear-ddos-pvstp-aggregate-states
clear-ddos-pvstp-aggregate-statistics
clear-ddos-pvstp-states
clear-ddos-pvstp-statistics
clear-ddos-radius-account-states
clear-ddos-radius-account-statistics
clear-ddos-radius-aggregate-states
clear-ddos-radius-aggregate-statistics
clear-ddos-radius-auth-states
clear ddos-protection protocols radius authorization statistics
clear-ddos-radius-auth-statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols radius server
clear ddos-protection protocols radius server states
clear-ddos-radius-server-states
clear ddos-protection protocols radius server statistics
clear-ddos-radius-server-statistics
clear ddos-protection protocols radius states
clear-ddos-radius-states
clear ddos-protection protocols radius statistics
clear-ddos-radius-statistics
clear ddos-protection protocols redirect
clear ddos-protection protocols redirect aggregate
clear ddos-protection protocols redirect aggregate states
clear-ddos-redirect-aggregate-states
clear ddos-protection protocols redirect aggregate statistics
clear-ddos-redirect-aggregate-statistics
clear ddos-protection protocols redirect states
clear-ddos-redirect-states
clear ddos-protection protocols redirect statistics
clear-ddos-redirect-statistics
clear ddos-protection protocols reject
clear ddos-protection protocols reject aggregate
clear ddos-protection protocols reject aggregate states
clear ddos-protection protocols reject aggregate statistics
clear ddos-protection protocols reject states
clear ddos-protection protocols reject statistics
clear ddos-protection protocols rip
clear ddos-protection protocols rip aggregate
clear ddos-protection protocols rip aggregate states
clear-ddos-rip-aggregate-states
clear ddos-protection protocols rip aggregate statistics
clear-ddos-rip-aggregate-statistics
clear ddos-protection protocols rip states
clear-ddos-rip-states
clear ddos-protection protocols rip statistics
clear-ddos-rip-statistics
clear ddos-protection protocols ripv6
clear ddos-protection protocols ripv6 aggregate
clear ddos-protection protocols ripv6 aggregate states
clear-ddos-ripv6-aggregate-states
clear ddos-protection protocols ripv6 aggregate statistics
clear-ddos-ripv6-aggregate-statistics
clear ddos-protection protocols ripv6 states
```

```
clear-ddos-ripv6-states
clear ddos-protection protocols ripv6 statistics
clear-ddos-ripv6-statistics
clear ddos-protection protocols rsvp
clear ddos-protection protocols rsvp aggregate
clear ddos-protection protocols rsvp aggregate states
clear-ddos-rsvp-aggregate-states
clear ddos-protection protocols rsvp aggregate statistics
clear-ddos-rsvp-aggregate-statistics
clear ddos-protection protocols rsvp states
clear-ddos-rsvp-states
clear ddos-protection protocols rsvp statistics
clear-ddos-rsvp-statistics
clear ddos-protection protocols rsvpv6
clear ddos-protection protocols rsvpv6 aggregate
clear ddos-protection protocols rsvpv6 aggregate states
clear-ddos-rsvpv6-aggregate-states
clear ddos-protection protocols rsvpv6 aggregate statistics
clear-ddos-rsvpv6-aggregate-statistics
clear ddos-protection protocols rsvpv6 states
clear-ddos-rsvpv6-states
clear ddos-protection protocols rsvpv6 statistics
clear-ddos-rsvpv6-statistics
clear ddos-protection protocols sample
clear ddos-protection protocols sample aggregate
clear ddos-protection protocols sample aggregate states
<clear-ddos-sample-aggregate-states>
clear ddos-protection protocols sample aggregate statistics
<clear-ddos-sample-aggregate-statistics>
clear ddos-protection protocols sample host
clear ddos-protection protocols sample host states
<clear-ddos-sample-host-states>
clear ddos-protection protocols sample host statistics
<clear-ddos-sample-host-statistics>
clear ddos-protection protocols sample pfe
clear ddos-protection protocols sample pfe culprit-flows
clear ddos-protection protocols sample pfe states
<clear-ddos-sample-pfe-states>
clear ddos-protection protocols sample pfe statistics
clear ddos-protection protocols sample sflow
clear ddos-protection protocols sample sflow culprit-flows
<clear-ddos-sample-sflow-flows>
clear ddos-protection protocols sample sflow states
<clear-ddos-sample-sflow-states>
clear ddos-protection protocols sample sflow statistics
<clear-ddos-sample-sflow-statistics>
clear ddos-protection protocols sample states
<clear-ddos-sample-states>
clear ddos-protection protocols sample statistics
<clear-ddos-sample-statistics>
clear ddos-protection protocols sample syslog
clear ddos-protection protocols sample syslog culprit-flows
clear ddos-protection protocols sample syslog states
<clear-ddos-sample-syslog-states>
clear ddos-protection protocols sample syslog statistics
<clear-ddos-sample-syslog-statistics>
clear ddos-protection protocols sample tap
clear ddos-protection protocols sample tap states
clear ddos-protection protocols sample-dest
clear ddos-protection protocols sample-dest aggregate
clear ddos-protection protocols sample-dest aggregate culprit-flows
```

```

<clear-ddos-sample-dest-aggregate-flows>
clear ddos-protection protocols sample-dest aggregate states
<clear-ddos-sample-dest-aggregate-states>
clear ddos-protection protocols sample-dest aggregate statistics
  <clear-ddos-sample-dest-aggregate-statistics>
clear ddos-protection protocols sample-dest culprit-flows
<clear-ddos-sample-dest-flows>
clear ddos-protection protocols sample-dest states
<clear-ddos-sample-dest-states>
clear ddos-protection protocols sample-dest statistics
<clear-ddos-sample-dest-statistics>
clear ddos-protection protocols sample-source
clear ddos-protection protocols sample-source aggregate
clear ddos-protection protocols sample-source aggregate culprit-flows
<clear-ddos-sample-source-aggregate-flows>
clear ddos-protection protocols sample-source aggregate states
<clear-ddos-sample-source-aggregate-states>
clear ddos-protection protocols sample-source aggregate statistics
<clear-ddos-sample-source-aggregate-statistics>
clear ddos-protection protocols sample-source culprit-flows
<clear-ddos-sample-source-flows>
clear ddos-protection protocols sample-source states
<clear-ddos-sample-source-states>
clear ddos-protection protocols sample-source statistics
  <clear-ddos-sample-source-statistics>
clear ddos-protection protocols sample tap statistics
<clear-ddos-sample-tap-statistics>
clear ddos-protection protocols services
clear ddos-protection protocols services aggregate
clear ddos-protection protocols services aggregate states
clear-ddos-services-aggregate-states
clear ddos-protection protocols services aggregate statistics
clear ddos-protection protocols services bsdt
clear ddos-protection protocols services bsdt culprit-flows
<clear-ddos-services-BSDT-flows>
clear ddos-protection protocols services bsdt states
<clear-ddos-services-BSDT-states>
clear ddos-protection protocols services bsdt statistics
<clear-ddos-services-BSDT-statistics>
clear ddos-protection protocols services culprit-flows
<clear-ddos-services-flows>
clear ddos-protection protocols services packet
clear ddos-protection protocols services packet culprit-flows
<clear-ddos-services-packet-flows>
clear ddos-protection protocols services packet states
<clear-ddos-services-packet-states>
clear ddos-protection protocols services packet statistics
<clear-ddos-services-packet-statistics>
clear ddos-protection protocols services states
clear-ddos-services-states
clear ddos-protection protocols services statistics
clear-ddos-services-statistics
clear ddos-protection protocols snmp
clear ddos-protection protocols snmp aggregate
clear ddos-protection protocols snmp aggregate states
clear-ddos-snmp-aggregate-states
clear ddos-protection protocols snmp aggregate statistics
clear ddos-protection protocols snmp culprit-flows
clear ddos-protection protocols snmp states
clear-ddos-snmp-states
clear ddos-protection protocols snmp statistics

```

```
clear-ddos-snmp-statistics
clear ddos-protection protocols snmpv6
clear ddos-protection protocols snmpv6 aggregate
clear ddos-protection protocols snmpv6 aggregate states
clear-ddos-snmpv6-aggregate-states
clear ddos-protection protocols snmpv6 aggregate statistics
clear-ddos-snmpv6-aggregate-statistics
clear ddos-protection protocols snmpv6 states
clear-ddos-snmpv6-states
clear ddos-protection protocols snmpv6 statistics
clear-ddos-snmpv6-statistics
clear ddos-protection protocols ssh
clear ddos-protection protocols ssh aggregate
clear ddos-protection protocols ssh aggregate states
clear-ddos-ssh-aggregate-states
clear ddos-protection protocols ssh aggregate statistics
clear-ddos-ssh-aggregate-statistics
clear ddos-protection protocols ssh states
clear-ddos-ssh-states
clear ddos-protection protocols ssh statistics
clear-ddos-ssh-statistics
clear ddos-protection protocols sshv6
clear ddos-protection protocols sshv6 aggregate
clear ddos-protection protocols sshv6 aggregate states
clear-ddos-sshv6-aggregate-states
clear ddos-protection protocols sshv6 aggregate statistics
clear ddos-protection protocols sshv6 culprit-flows
clear ddos-protection protocols sshv6 states
clear-ddos-sshv6-states
clear ddos-protection protocols sshv6 statistics
clear-ddos-sshv6-statistics
clear ddos-protection protocols states
clear-ddos-protocols-states
clear ddos-protection protocols statistics
clear-ddos-protocols-statistics
clear ddos-protection protocols stp
clear ddos-protection protocols stp aggregate
clear ddos-protection protocols stp aggregate states
clear-ddos-stp-aggregate-states
clear ddos-protection protocols stp aggregate statistics
clear-ddos-stp-aggregate-statistics
clear ddos-protection protocols stp states
clear-ddos-stp-states
clear ddos-protection protocols stp statistics
clear-ddos-stp-statistics
clear ddos-protection protocols tacacs
clear ddos-protection protocols tacacs aggregate
clear ddos-protection protocols tacacs aggregate states
clear-ddos-tacacs-aggregate-states
clear ddos-protection protocols tacacs aggregate statistics
clear-ddos-tacacs-aggregate-statistics
clear ddos-protection protocols tacacs states
clear-ddos-tacacs-states
clear ddos-protection protocols tacacs statistics
clear-ddos-tacacs-statistics
clear ddos-protection protocols tcp-flags
clear ddos-protection protocols tcp-flags aggregate
clear ddos-protection protocols tcp-flags aggregate states
clear-ddos-tcp-flags-aggregate-states
clear ddos-protection protocols tcp-flags aggregate statistics
clear-ddos-tcp-flags-aggregate-statistics
```

```
clear ddos-protection protocols tcp-flags established
clear ddos-protection protocols tcp-flags established states
clear-ddos-tcp-flags-establish-states
clear ddos-protection protocols tcp-flags established statistics
clear-ddos-tcp-flags-establish-statistics
clear ddos-protection protocols tcp-flags initial
clear ddos-protection protocols tcp-flags initial culprit-flows
clear ddos-protection protocols tcp-flags initial states
clear-ddos-tcp-flags-initial-states
clear ddos-protection protocols tcp-flags initial statistics
clear-ddos-tcp-flags-initial-statistics
clear ddos-protection protocols tcp-flags states
clear-ddos-tcp-flags-states
clear ddos-protection protocols tcp-flags statistics
clear-ddos-tcp-flags-statistics
clear ddos-protection protocols tcp-flags unclassified
clear ddos-protection protocols tcp-flags unclassified states
clear-ddos-tcp-flags-unclass-states
clear ddos-protection protocols tcp-flags unclassified statistics
clear-ddos-tcp-flags-unclass-statistics
clear ddos-protection protocols telnet
clear ddos-protection protocols telnet aggregate
clear ddos-protection protocols telnet aggregate culprit-flows
clear ddos-protection protocols telnet aggregate states
clear-ddos-telnet-aggregate-states
clear ddos-protection protocols telnet aggregate statistics
clear-ddos-telnet-aggregate-statistics
clear ddos-protection protocols telnet states
clear-ddos-telnet-states
clear ddos-protection protocols telnet statistics
clear-ddos-telnet-statistics
clear ddos-protection protocols telnetv6
clear ddos-protection protocols telnetv6 aggregate
clear ddos-protection protocols telnetv6 aggregate states
clear-ddos-telnetv6-aggregate-states
clear ddos-protection protocols telnetv6 aggregate statistics
clear-ddos-telnetv6-aggregate-statistics
clear ddos-protection protocols telnetv6 states
clear-ddos-telnetv6-states
clear ddos-protection protocols telnetv6 statistics
clear-ddos-telnetv6-statistics
clear ddos-protection protocols ttl
clear ddos-protection protocols ttl aggregate
clear ddos-protection protocols ttl aggregate culprit-flows
clear ddos-protection protocols ttl aggregate states
clear-ddos-ttl-aggregate-states
clear ddos-protection protocols ttl aggregate statistics
clear-ddos-ttl-aggregate-statistics
clear ddos-protection protocols ttl states
clear-ddos-ttl-states
clear ddos-protection protocols ttl statistics
clear-ddos-ttl-statistics
clear ddos-protection protocols tunnel-fragment
clear ddos-protection protocols tunnel-fragment aggregate
clear ddos-protection protocols tunnel-fragment aggregate states
clear-ddos-tun-frag-aggregate-states
clear ddos-protection protocols tunnel-fragment aggregate statistics
clear-ddos-tun-frag-aggregate-statistics
clear ddos-protection protocols tunnel-fragment states
clear-ddos-tun-frag-states
clear ddos-protection protocols tunnel-fragment statistics
```

```

clear-ddos-tun-frag-statistics
clear ddos-protection protocols unclassified
clear ddos-protection protocols unclassified aggregate
clear ddos-protection protocols unclassified aggregate states
clear ddos-protection protocols unclassified aggregate statistics
clear ddos-protection protocols unclassified control-layer2
clear ddos-protection protocols unclassified control-layer2 culprit-flows
clear ddos-protection protocols unclassified control-layer2 states
clear ddos-protection protocols unclassified control-layer2 statistics
clear ddos-protection protocols unclassified control-v4
clear ddos-protection protocols unclassified control-v4 culprit-flows
clear ddos-protection protocols unclassified control-v4 states
clear ddos-protection protocols unclassified control-v4 statistics
clear ddos-protection protocols unclassified control-v6
clear ddos-protection protocols unclassified control-v6 culprit-flows
clear ddos-protection protocols unclassified control-v6 states
clear ddos-protection protocols unclassified control-v6 statistics
clear ddos-protection protocols unclassified filter-v4 culprit-flows
clear ddos-protection protocols unclassified filter-v4 states
clear ddos-protection protocols unclassified filter-v4 statistics
clear ddos-protection protocols unclassified filter-v6
clear ddos-protection protocols unclassified filter-v6 culprit-flows
clear ddos-protection protocols unclassified filter-v6 states
clear ddos-protection protocols unclassified filter-v6 statistics
clear ddos-protection protocols unclassified fw-host
clear ddos-protection protocols unclassified fw-host culprit-flows
<clear-ddos-uncls-fw-host-flows>
clear ddos-protection protocols unclassified fw-host states
<clear-ddos-uncls-fw-host-states>
clear ddos-protection protocols unclassified fw-host statistics
<clear-ddos-uncls-fw-host-statistics>
clear ddos-protection protocols unclassified host-route-v4
clear ddos-protection protocols unclassified host-route-v4 culprit-flows
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 statistics
clear ddos-protection protocols unclassified host-route-v6
clear ddos-protection protocols unclassified host-route-v6 culprit-flows
clear ddos-protection protocols unclassified host-route-v6 states
clear ddos-protection protocols unclassified host-route-v6 statistics
clear ddos-protection protocols unclassified mcast-copy
clear ddos-protection protocols unclassified mcast-copy culprit-flows
<clear-ddos-uncls-mcast-copy-flows>
clear ddos-protection protocols unclassified mcast-copy states
<clear-ddos-uncls-mcast-copy-states>
clear ddos-protection protocols unclassified mcast-copy statistics
<clear-ddos-uncls-mcast-copy-statistics>
clear ddos-protection protocols unknown-l2mc
clear ddos-protection protocols unknown-l2mc aggregate
clear ddos-protection protocols unknown-l2mc aggregate culprit-flows
<clear-ddos-unknown-l2mc-aggregate-flows>
clear ddos-protection protocols unknown-l2mc aggregate states
<clear-ddos-unknown-l2mc-aggregate-states>
clear ddos-protection protocols unknown-l2mc aggregate statistics
<clear-ddos-unknown-l2mc-aggregate-statistics>
clear ddos-protection protocols unknown-l2mc culprit-flows
<clear-ddos-unknown-l2mc-flows>
clear ddos-protection protocols unknown-l2mc states
<clear-ddos-unknown-l2mc-states>
clear ddos-protection protocols unknown-l2mc statistics
<clear-ddos-unknown-l2mc-statistics>

```

```

clear ddos-protection protocols urpf-fail
clear ddos-protection protocols urpf-fail aggregate
clear ddos-protection protocols urpf-fail aggregate culprit-flows
<clear-ddos-urpf-fail-aggregate-flows>
clear ddos-protection protocols urpf-fail aggregate states
<clear-ddos-urpf-fail-aggregate-states>
clear ddos-protection protocols urpf-fail aggregate statistics
<clear-ddos-urpf-fail-aggregate-statistics>
clear ddos-protection protocols urpf-fail culprit-flows
<clear-ddos-urpf-fail-flows>
clear ddos-protection protocols urpf-fail states
<clear-ddos-urpf-fail-states>
clear ddos-protection protocols urpf-fail statistics
<clear-ddos-urpf-fail-statistics>
clear ddos-protection protocols vcipc-udp
clear ddos-protection protocols vcipc-udp aggregate
clear ddos-protection protocols vcipc-udp aggregate culprit-flows
<clear-ddos-vcipc-udp-aggregate-flows>
clear ddos-protection protocols vcipc-udp aggregate states
<clear-ddos-vcipc-udp-aggregate-states>
clear ddos-protection protocols vcipc-udp aggregate statistics
<clear-ddos-vcipc-udp-aggregate-statistics>
clear ddos-protection protocols vcipc-udp culprit-flows
<clear-ddos-vcipc-udp-flows>
clear ddos-protection protocols vcipc-udp states
<clear-ddos-vcipc-udp-states>
<clear-ddos-vcipc-udp-statistics>
clear ddos-protection protocols unclassified other
clear ddos-protection protocols unclassified other culprit-flows
clear ddos-protection protocols unclassified other states
clear ddos-protection protocols unclassified other statistics
clear ddos-protection protocols unclassified resolve-v4
clear ddos-protection protocols unclassified resolve-v4 culprit-flows
clear ddos-protection protocols unclassified resolve-v4 states
clear ddos-protection protocols unclassified resolve-v4 statistics
clear ddos-protection protocols unclassified resolve-v6
clear ddos-protection protocols unclassified resolve-v6 culprit-flows
clear ddos-protection protocols unclassified resolve-v6 states
clear ddos-protection protocols unclassified resolve-v6 statistics
clear ddos-protection protocols unclassified states
clear ddos-protection protocols unclassified statistics
<clear-ddos-uncls-statistics>
clear ddos-protection protocols virtual-chassis
clear ddos-protection protocols virtual-chassis aggregate
clear ddos-protection protocols virtual-chassis aggregate culprit-flows
clear ddos-protection protocols virtual-chassis aggregate states
clear-ddos-protocols-states
clear-ddos-protocols-statistics
clear-ddos-radius-server-states
clear-ddos-radius-server-statistics
clear-ddos-radius-states
clear-ddos-radius-statistics
clear ddos-protection protocols re-services
clear ddos-protection protocols re-services aggregate
clear ddos-protection protocols re-services aggregate culprit-flows
<clear-ddos-re-services-aggregate-flows>
clear ddos-protection protocols re-services aggregate states
<clear-ddos-re-services-aggregate-states>
clear ddos-protection protocols re-services aggregate statistics
<clear-ddos-re-services-aggregate-statistics>
clear ddos-protection protocols re-services captive-portal

```

```
clear ddos-protection protocols re-services captive-portal culprit-flows
<clear-ddos-re-services-captive-portal-flows>
clear ddos-protection protocols re-services captive-portal states
<clear-ddos-re-services-captive-portal-states>
clear ddos-protection protocols re-services captive-portal statistics
<clear-ddos-re-services-captive-portal-statistics>
clear ddos-protection protocols re-services culprit-flows
<clear-ddos-re-services-flows>
clear ddos-protection protocols re-services states
<clear-ddos-re-services-states>
clear ddos-protection protocols re-services statistics
<clear-ddos-re-services-statistics>
clear ddos-protection protocols re-services-v6
clear ddos-protection protocols re-services-v6 aggregate
clear ddos-protection protocols re-services-v6 aggregate culprit-flows
<clear-ddos-re-services-v6-aggregate-flows>
clear ddos-protection protocols re-services-v6 aggregate states
<clear-ddos-re-services-v6-aggregate-states>
clear ddos-protection protocols re-services-v6 aggregate statistics
<clear-ddos-re-services-v6-aggregate-statistics>
clear ddos-protection protocols re-services-v6 captive-portal
clear ddos-protection protocols re-services-v6 captive-portal culprit-flows
<clear-ddos-re-services-v6-captive-portal-v6-flows>
clear ddos-protection protocols re-services-v6 captive-portal states
<clear-ddos-re-services-v6-captive-portal-v6-states>
clear ddos-protection protocols re-services-v6 captive-portal statistics
<clear-ddos-re-services-v6-captive-portal-v6-statistics>
clear ddos-protection protocols re-services-v6 culprit-flows
<clear-ddos-re-services-v6-flows>
clear ddos-protection protocols re-services-v6 states
<clear-ddos-re-services-v6-states>
clear ddos-protection protocols re-services-v6 statistics
<clear-ddos-re-services-v6-statistics>
clear-ddos-redirect-aggregate-states
clear-ddos-redirect-states
clear-ddos-redirect-statistics
clear-ddos-rip-aggregate-states
clear-ddos-rip-aggregate-statistics
clear-ddos-rip-states
clear-ddos-rip-statistics
clear-ddos-ripv6-aggregate-states
clear-ddos-ripv6-aggregate-statistics
clear-ddos-ripv6-states
clear-ddos-ripv6-statistics
clear-ddos-rsvp-aggregate-states
clear-ddos-rsvp-aggregate-statistics
clear-ddos-rsvp-states
clear-ddos-rsvp-statistics
clear-ddos-rsvpv6-aggregate-states
clear-ddos-rsvpv6-aggregate-statistics
clear-ddos-rsvpv6-states
clear-ddos-rsvpv6-statistics
clear-ddos-services-aggregate-states
clear-ddos-services-aggregate-statistics
clear-ddos-services-states
clear-ddos-services-statistics
clear-ddos-snmp-aggregate-states
clear-ddos-snmp-aggregate-statistics
clear-ddos-snmp-states
clear-ddos-snmp-statistics
clear-ddos-snmpv6-aggregate-states
```

```
clear-ddos-snmpv6-aggregate-statistics
clear-ddos-snmpv6-states
clear-ddos-snmpv6-statistics
clear-ddos-ssh-aggregate-states
clear-ddos-ssh-aggregate-statistics
clear-ddos-ssh-states
clear-ddos-ssh-statistics
clear-ddos-sshv6-aggregate-states
clear-ddos-sshv6-aggregate-statistics
clear-ddos-sshv6-states
clear-ddos-sshv6-statistics
clear-ddos-stp-aggregate-states
clear-ddos-stp-aggregate-statistics
clear-ddos-stp-states
clear-ddos-stp-statistics
clear ddos-protection protocols syslog
clear ddos-protection protocols syslog aggregate
clear ddos-protection protocols syslog aggregate culprit-flows
<clear-ddos-syslog-aggregate-flows>
clear ddos-protection protocols syslog aggregate states
<clear-ddos-syslog-aggregate-states>
clear ddos-protection protocols syslog aggregate statistics
<clear-ddos-syslog-aggregate-statistics>
clear ddos-protection protocols syslog culprit-flows
<clear-ddos-syslog-flows>
clear ddos-protection protocols syslog states
<clear-ddos-syslog-states>
clear ddos-protection protocols syslog statistics
<clear-ddos-syslog-statistics>
clear-ddos-tacacs-aggregate-states
clear-ddos-tacacs-aggregate-statistics
clear-ddos-tacacs-states
clear-ddos-tacacs-statistics
clear-ddos-tcp-flags-aggregate-states
clear-ddos-tcp-flags-aggregate-statistics
clear-ddos-tcp-flags-establish-states
clear-ddos-tcp-flags-establish-statistics
clear-ddos-tcp-flags-initial-states
clear-ddos-tcp-flags-initial-statistics
clear-ddos-tcp-flags-states
clear-ddos-tcp-flags-statistics
clear-ddos-tcp-flags-unclass-states
clear-ddos-tcp-flags-unclass-statistics
clear-ddos-telnet-aggregate-states
clear-ddos-telnet-aggregate-statistics
clear-ddos-telnet-states
clear-ddos-telnet-statistics
clear-ddos-telnetv6-aggregate-states
clear-ddos-telnetv6-aggregate-statistics
clear-ddos-telnetv6-states
clear-ddos-telnetv6-statistics
clear-ddos-ttl-aggregate-states
clear-ddos-ttl-aggregate-statistics
clear-ddos-ttl-states
clear-ddos-ttl-statistics
clear-ddos-tun-frag-aggregate-states
clear-ddos-tun-frag-aggregate-statistics
clear-ddos-tun-frag-states
clear-ddos-tun-frag-statistics
clear ddos-protection protocols tunnel-ka
clear ddos-protection protocols tunnel-ka aggregate
```

```
clear ddos-protection protocols tunnel-ka aggregate culprit-flows
<clear-ddos-tunnel-ka-aggregate-flows>
clear ddos-protection protocols tunnel-ka aggregate states
<clear-ddos-tunnel-ka-aggregate-states>
clear ddos-protection protocols tunnel-ka aggregate statistics
<clear-ddos-tunnel-ka-aggregate-statistics>
clear ddos-protection protocols tunnel-ka culprit-flows
<clear-ddos-tunnel-ka-flows>
clear ddos-protection protocols tunnel-ka states
<clear-ddos-tunnel-ka-states>
clear ddos-protection protocols tunnel-ka statistics
<clear-ddos-tunnel-ka-statistics>
clear-ddos-vchassis-aggregate-states
clear ddos-protection protocols virtual-chassis aggregate statistics
clear-ddos-vchassis-aggregate-statistics
clear ddos-protection protocols virtual-chassis control-high
clear ddos-protection protocols virtual-chassis control-high states
clear-ddos-vchassis-control-hi-states
clear ddos-protection protocols virtual-chassis control-high statistics
clear-ddos-vchassis-control-hi-statistics
clear ddos-protection protocols virtual-chassis control-low
clear ddos-protection protocols virtual-chassis control-low states
clear-ddos-vchassis-control-lo-states
clear ddos-protection protocols virtual-chassis control-low statistics
clear-ddos-vchassis-control-lo-statistics
clear ddos-protection protocols virtual-chassis states
clear-ddos-vchassis-states
clear ddos-protection protocols virtual-chassis statistics
clear-ddos-vchassis-statistics
clear ddos-protection protocols virtual-chassis unclassified
clear ddos-protection protocols virtual-chassis unclassified culprit-flows
clear ddos-protection protocols virtual-chassis unclassified states
clear-ddos-vchassis-unclass-states
clear ddos-protection protocols virtual-chassis unclassified statistics
clear-ddos-vchassis-unclass-statistics
clear ddos-protection protocols virtual-chassis vc-packets
clear ddos-protection protocols virtual-chassis vc-packets states
clear-ddos-vchassis-vc-packets-states
clear ddos-protection protocols virtual-chassis vc-packets statistics
clear-ddos-vchassis-vc-packets-statistics
clear ddos-protection protocols virtual-chassis vc-ttl-errors
clear ddos-protection protocols virtual-chassis vc-ttl-errors states
clear-ddos-vchassis-vc-ttl-err-states
clear ddos-protection protocols virtual-chassis vc-ttl-errors statistics
clear-ddos-vchassis-vc-ttl-err-statistics
clear ddos-protection protocols vrrp
clear ddos-protection protocols vrrp aggregate
clear ddos-protection protocols vrrp aggregate states
clear-ddos-vrrp-aggregate-states
clear ddos-protection protocols vrrp aggregate statistics
clear ddos-protection protocols vrrp culprit-flows
clear ddos-protection protocols vrrp statistics
clear-ddos-vrrp-statistics
clear ddos-protection protocols vrrpv6
clear ddos-protection protocols vrrpv6 aggregate
clear ddos-protection protocols vrrpv6 aggregate states
clear-ddos-vrrpv6-aggregate-states
clear ddos-protection protocols vrrpv6 aggregate statistics
clear-ddos-vrrpv6-aggregate-statistics
clear ddos-protection protocols vrrpv6 states
clear-ddos-vrrpv6-states
```

```
clear ddos-protection protocols vrrpv6 statistics
clear-ddos-uncls-host-rt-v4-flows
clear-ddos-vchassis-aggregate-statistics
clear-ddos-vchassis-control-hi-states
clear-ddos-vchassis-control-hi-statistics
clear-ddos-vchassis-control-lo-states
clear-ddos-vchassis-control-lo-statistics
clear-ddos-vchassis-states
clear-ddos-vchassis-statistics
clear-ddos-vchassis-unclass-states
clear-ddos-vchassis-unclass-statistics
clear-ddos-vchassis-vc-packets-states
clear-ddos-vchassis-vc-packets-statistics
clear-ddos-vchassis-vc-ttl-err-states
clear-ddos-vchassis-vc-ttl-err-statistics
clear-ddos-vrrp-aggregate-states
clear-ddos-vrrp-aggregate-statistics
clear-ddos-vrrp-states
clear-ddos-vrrp-statistics
clear-ddos-vrrpv6-aggregate-states
clear-ddos-vrrpv6-aggregate-statistics
clear-ddos-vrrpv6-states
clear-ddos-vrrpv6-statistics
clear ddos-protection protocols vxlan
clear ddos-protection protocols vxlan aggregate
clear ddos-protection protocols vxlan aggregate culprit-flows
clear-ddos-vxlan-aggregate-flows
clear ddos-protection protocols vxlan aggregate states
<clear-ddos-vxlan-aggregate-states>
clear ddos-protection protocols vxlan aggregate statistics
<clear-ddos-vxlan-aggregate-statistics>
clear ddos-protection protocols vxlan culprit-flows
<clear-ddos-vxlan-flows>
clear ddos-protection protocols vxlan states
<clear-ddos-vxlan-states>
clear ddos-protection protocols vxlan statistics
<clear-ddos-vxlan-statistics>
clear dhcp
clear dhcp client
clear dhcp client binding
<clear-dhcp-client-binding-information>
clear dhcp client statistics
<clear-client-statistics-information>
clear dhcp proxy-client
clear dhcp proxy-client statistics
clear dhcp relay
clear dhcp relay binding
<clear-dhcp-relay-binding-information>
clear dhcp relay binding interface
<clear-dhcp-interface-bindings>
clear dhcp relay statistics
<clear-dhcp-relay-statistics-information>
<clear-dhcp-security-binding>
<clear-dhcp-security-binding-interface>
<clear-dhcp-security-binding-ip-address>
<clear-dhcp-security-binding-statistics>
<clear-dhcp-security-binding-vlan>
clear dhcp relay statistics bulk-leasequery-connections
<clear-dhcp-relay-bulk-leasequery-conn-statistics>
clear dhcp relay statistics leasequery
<clear-dhcp-relay-leasequery-statistics>
```

```
clear dhcp server
clear dhcp server binding
  <clear-dhcp-server-binding-information>
clear dhcp server binding interface
<clear-dhcp-server-binding-interface>
clear dhcp server statistics
  <clear-server-statistics-information>
clear dhcp statistics
<clear-dhcp-service-statistics-information>
clear dhcpv6
clear dhcpv6 proxy-client
clear dhcpv6 proxy-client statistics
  <clear-dhcpv6-proxy-client-statistics-information>
clear dhcpv6 relay
clear dhcpv6 relay binding
clear dhcpv6 relay binding interface
clear dhcpv6 relay statistics
<clear-dhcpv6-relay-statistics-information>
clear dhcpv6 relay statistics bulk-leasequery-connections
<clear-dhcpv6-relay-bulk-leasequery-conn-statistics>
clear dhcpv6 relay statistics leasequery
<clear-dhcpv6-relay-leasequery-statistics>
clear dhcpv6 server
clear dhcpv6 server binding
<clear-dhcpv6-server-binding-information>
clear dhcpv6 server binding interface
<clear-dhcpv6-server-binding-interface>
clear dhcpv6 server statistics
<clear-dhcpv6-server-statistics-information>
clear dhcpv6 server statistics bulk-leasequery-connections
<clear-dhcpv6-server-bulk-leasequery-statistics>
clear dhcpv6 statistics
<clear-dhcpv6-service-statistics-information>
clear diameter
clear diameter function
  <clear-diameter-function>
clear diameter peer
  <clear-diameter-peer>
<clear-dhcp-binding-information>
<clear-dhcp-conflict-information>
<clear-dhcp-statistics-information>
clear system subscriber-management
clear system subscriber-management statistics
<clear-subscriber-management-statistics>
clear dot1x
clear dot1x firewall
<clear-dot1x-firewall>
clear dot1x firewall interface
<clear-dot1x-firewall-interface>
clear dot1x interface
  <clear-dot1x-interface-session>
clear dot1x mac-address
  <clear-dot1x-mac-session>
clear dot1x statistics
<clear-dot1x-statistics>
clear dot1x statistics interface
<clear-dot1x-statistics-interface>
clear error
clear error bpdu
clear error bpdu interface
<clear-bpdu-error>
```

```
clear error mac-rewrite
clear error mac-rewrite interface
  <clear-mac-rewrite-error>
clear esis
clear esis adjacency
<clear-esis-adjacency>
clear esis statistics
<clear-esis-statistics>
clear ethernet-switching
clear ethernet-switching evpn
clear ethernet-switching evpn arp-table
<clear-ethernet-switching-evpn-arp-table>
clear ethernet-switching mac-learning-log
<clear-ethernet-switching-mac-learning-log>
clear ethernet-switching recovery-timeout
<clear-ethernet-switching-recovery>
clear ethernet-switching recovery-timeout interface
<clear-ethernet-switching-recovery-interface>
clear ethernet-switching table
<clear-ethernet-switching-table>
clear ethernet-switching table interface
<clear-ethernet-switching-interface-table>
clear ethernet-switching table persistent-learning
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning interface
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning mac
<clear-ethernet-switching-table-persistent-learning-mac>
clear evpn
clear evpn arp-table
<clear-evpn-arp-table>
clear evpn mac-table
<clear-evpn-mac-table>
clear evpn mac-table interface
<clear-evpn-interface-mac-table>
clear extensible-subscriber-services
clear extensible-subscriber-services counters
<clear-extensible-subscriber-services-counters>
clear extensible-subscriber-services sessions
<clear-extensible-subscriber-services-sessions>
clear fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-counters>
clear firewall log
<clear-firewall-log>
clear firewall policer
clear firewall policer counter
clear firewall policer counter all
<clear-interface-aggregate-fwd-options>
<clear-interface-aggregate-fwd-options-all>
clear helper
clear helper statistics
  <clear-helper-statistics-information>
clear igmp
clear igmp membership
<clear-igmp-membership>
```

```
clear igmp snooping
clear igmp snooping membership
<clear-igmp-snooping-membership>
clear igmp snooping membership bridge-domain
<clear-igmp-snooping-bridge-domain-membership>
clear igmp snooping membership vlan
<clear-igmp-snooping-vlan-membership>
clear igmp snooping statistics
<clear-igmp-snooping-statistics>
clear igmp snooping statistics bridge-domain
<clear-igmp-snooping-bridge-domain-statistics>
clear igmp snooping statistics vlan
<clear-igmp-snooping-vlan-statistics>
clear igmp statistics
<clear-igmp-statistics>
clear ike
clear ike security-associations
<clear-ike-security-associations>
clear ike statistics
<clear-ike-statistics>
clear ilmi
clear ilmi statistics
<clear-ilmi-statistics>
clear interfaces
clear interfaces interface-set
clear interfaces interface-set statistics
<clear-interface-set-statistics>
clear interfaces interface-set statistics all
<clear-interface-set-statistics-all>
clear interfaces interval
<clear-interfaces-interval>
clear interfaces mac-database
<clear-interfaces-mac-database>
clear interfaces mac-database statistics
<clear-interface-mac-database-statistics>
clear interfaces mac-database statistics all
<clear-interface-mac-database-statistics-all>
clear interfaces statistics
<clear-interfaces-statistics>
clear interfaces statistics all
<clear-interfaces-statistics-all>
clear interfaces transport
<clear-interface-transport-information>
clear interfaces transport optics
<clear-interface-transport-optics-information>
clear interfaces transport optics interval
<clear-interface-transport-optics-interval-information>
clear ipsec
clear ipsec security-associations
<clear-ipsec-security-associations>
clear ipv6
clear ipv6 neighbors
<clear-ipv6-nd-information>
clear ipv6 neighbors all
<clear-ipv6-all-neighbors>
clear isis
clear isis adjacency
<clear-isis-adjacency-information>
clear isis database
<clear-isis-database-information>
clear isis overload
```

```
<clear-isis-overload-information>
clear isis statistics
<clear-isis-statistics-information>
clear ipv6 router-advertisement
clear lacp
clear lacp statistics
clear l2-learning
clear l2-learning evpn
clear l2-learning evpn arp-statistics
<clear-evpn-arp-statistics>
clear l2-learning evpn arp-statistics interface
<clear-evpn-arp-statistics-interface>
clear l2-learning mac-move-buffer
<clear-l2-learning-mac-move-buffer>
clear l2-learning mac-move-buffer active
<clear-l2-learning-mac-move-buffer-active>
clear-l2-learning-redundancy-group
<clear-l2-learning-redundancy-group-statistics>
clear l2-learning remote-backbone-edge-bridges
<clear-l2-learning-remote-backbone-edge-bridges>
clear ldp
clear ldp statistics
<clear-ldp-statistics>
clear ldp statistics interface
<clear-ldp-interface-hello-statistics>
clear ldp neighbor
<clear-ldp-neighbors>
clear ldp session
<clear-ldp-sessions>
clear lldp
clear lldp neighbors
<clear-lldp-neighbors>
clear lldp neighbors interface
<clear-lldp-interface-neighbors>
clear lldp statistics
<clear-lldp-statistics>
clear lldp statistics interface
<clear-lldp-interface-statistics>
clear mld
clear mld membership
<clear-mld-membership>
clear mld snooping
clear mld snooping membership
<clear-mld-snooping-membership>
clear mld snooping membership bridge-domain
<clear-mld-snooping-bridge-domain-membership>
clear mld snooping membership vlan
<clear-mld-snooping-vlan-membership>
clear mld snooping statistics
<clear-mld-snooping-statistics>
clear mld snooping statistics bridge-domain
<clear-mld-snooping-bridge-domain-statistics>
clear mld snooping statistics vlan
<clear-mld-snooping-vlan-statistics>
clear mld statistics
<clear-mld-statistics>
clear mobile-ip
clear mobile-ip binding
clear mobile-ip binding all
<clear-binding-all>
clear mobile-ip binding ip-address
```

```
<clear-binding-ip>
clear mobile-ip binding nai
<clear-binding-nai>
clear mobile-ip visitor
clear mobile-ip visitor all
<clear-visitor-all>
clear mobile-ip visitor ip-address
<clear-visitor-ip>
clear mobile-ip visitor nai
<clear-visitor-nai>
clear mpls
clear mpls lsp
<clear-mpls-lsp-information>
clear mpls static-lsp
<clear-mpls-static-lsp-information>
clear mpls traceroute
clear mpls traceroute database
clear mpls traceroute database ldp
<clear-mpls-traceroute-database-ldp>
clear msdp
clear msdp cache
<clear-msdp-cache>
clear msdp statistics
<clear-msdp-statistics>
clear multicast
clear multicast bandwidth-admission
<clear-multicast-bandwidth-admission>
clear multicast forwarding-cache
clear multicast scope
<clear-multicast-scope-statistics>
clear multicast sessions
<clear-multicast-sessions>
clear multicast statistics
<clear-multicast-statistics>
clear mvrp
clear mvrp statistics
<clear-mvrp-interface-statistics>
clear network-access
clear network-access aaa
clear network-access aaa statistics
<clear-aaa-statistics-table>
clear network-access aaa statistics address-assignment
clear network-access aaa statistics address-assignment client
<clear-aaa-address-assignment-client-statistics>
clear network-access aaa statistics address-assignment pool
<clear-aaa-address-assignment-pool-statistics>
clear network-access aaa subscriber
<clear-aaa-subscriber-table>
clear network-access aaa subscriber statistics
<clear-aaa-subscriber-table-specific-statistics>
clear network-access requests
clear network-access requests pending
<clear-authentication-pending-table>
clear network-access requests statistics
<clear-authentication-statistics>
clear network-access securid-node-secret-file
<clear-node-secret-file>
clear oam
clear oam ethernet
clear oam ethernet connectivity-fault-management
clear oam ethernet connectivity-fault-management continuity-measurement
```

```

    <clear-cfm-continuity-measurement>
clear oam ethernet connectivity-fault-management delay-statistics
    <clear-cfm-delay-statistics>
clear oam ethernet connectivity-fault-management event
<clear-cfm-action-profile-event>
clear oam ethernet connectivity-fault-management loss-statistics
    <clear-cfm-loss-statistics>
clear oam ethernet connectivity-fault-management path-database
    <clear-cfm-linktrace-path-database>
clear oam ethernet connectivity-fault-management policer
<clear-cfm-policer-statistics>
clear oam ethernet connectivity-fault-management sla-iterator-statistics
    <clear-cfm-iterator-statistics>
clear oam ethernet connectivity-fault-management statistics
    <clear-cfm-statistics>
clear oam ethernet connectivity-fault-management synthetic-loss-statistics
<clear-cfm-slm-statistics>
clear oam ethernet link-fault-management
clear oam ethernet link-fault-management state
    <clear-lfmd-state>
clear oam ethernet link-fault-management statistics
    <clear-lfmd-statistics>
clear oam ethernet link-fault-management statistics action-profile
    <clear-lfmd-action-profile-statistics>
clear oam ethernet lmi
clear oam ethernet lmi statistics
    <clear-elmi-statistics>
clear ospf
clear ospf database
    <clear-ospf-database-information>
clear ospf database-protection
<clear-ospf-database-protection>
clear ospf io-statistics
    <clear-ospf-io-statistics-information>
clear ospf neighbor
    <clear-ospf-neighbor-information>
clear ospf overload
<clear-ospf-overload-information>
clear ospf statistics
<clear-ospf-statistics-information>
clear ospf3
clear ospf3 database
<clear-ospf3-database-information>
clear ospf3 database-protection
<clear-ospf3-database-protection>
clear ospf3 io-statistics
    <clear-ospf3-io-statistics-information>
clear ospf3 neighbor
    <clear-ospf3-neighbor-information>
clear ospf3 overload
    <clear-ospf3-overload-information>
clear ospf3 statistics
    <clear-ospf3-io-statistics-information>
clear ovsdb statistics interface all
<clear-ovsdb-interfaces-statistics-all>
clear performance-monitoring
clear performance-monitoring mpls
clear performance-monitoring mpls lsp
<clear-pm-mpls-lsp-information>
clear pfe
clear pfe statistics

```

```
clear pfe statistics fabric
clear pfe statistics traffic detail
clear passive-monitoring
  <clear-passive-monitoring>
clear passive-monitoring statistics
  <clear-passive-monitoring-statistics>
clear pgm
clear pgm negative-acknowledgments
  <clear-pgm-negative-acknowledgments>
clear pgm source-path-messages
  <clear-pgm-source-path-messages>
clear pgm statistics
  <clear-pgm-statistics>
clear pim
clear pim join
  <clear-pim-join-state>
clear pim join-distribution
  <clear-pim-join-distribution>
clear pim register
  <clear-pim-register-state>
clear pim snooping
clear pim snooping join
clear pim snooping statistics
clear pim statistics
  <clear-pim-statistics>
clear ppp
clear ppp statistics
  <clear-ppp-statistics-information>
clear pppoe
clear pppoe logout
  <clear-pppoe-logout-timers>
clear pppoe sessions
  <clear-pppoe-sessions-information>
clear pppoe statistics
  <clear-pppoe-statistics-information>
clear pppoe statistics interfaces
  <clear-pppoe-statistics-interface-information>
clear protection-group
  <clear-protection-group>
clear protection-group ethernet-ring
  <clear-ethernet-ring-information>
clear protection-group ethernet-ring statistics
  <clear-ethernet-ring-information>
clear r2cp
clear r2cp radio
  <clear-r2cp-radio>
clear r2cp session
  <clear-r2cp-session>
clear r2cp statistics
  <clear-r2cp-statistics>
clear r2cp statistics radio
clear r2cp statistics session
clear rip
clear rip general-statistics
  <clear-rip-general-statistics>
clear rip statistics
  <clear-rip-statistics>
clear rip statistics peer
  <clear-rip-peer-statistics>
clear ripng
clear ripng general-statistics
```

```

<clear-ripng-general-statistic>
clear ripng statistics
<clear-ripng-statistics>
clear rsvp
clear rsvp session
  <clear-rsvp-session-information>
clear rsvp statistics
  < clear-rsvp-counters-information>
clear security group-vpn
clear security group-vpn member
clear security group-vpn member ike
clear security group-vpn member ike security-associations
<clear-group-vpn-ike-security-associations>
clear security group-vpn member ipsec
clear security group-vpn member ipsec security-associations
<clear-gvpn-ipsec-security-association>
clear security group-vpn member ipsec security-associations statistics
<clear-gvpn-ipsec-security-association-statistics>
clear security group-vpn member ipsec statistics
<clear-gvpn-ipsec-statistics>
clear services
clear services alg
clear services alg statistics
<clear-services-alg-statistics>
clear services application-aware-access-list
clear services application-aware-access-list statistics
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics interface
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics subscriber
<clear-application-aware-access-list-statistics-subscriber>
clear services application-identification
clear services application-identification application-system-cache
  <clear-appid-application-system-cache>
clear services application-identification counter
  <clear-appid-counter>
clear services application-identification counter ssl-encrypted-sessions
<clear-appid-counter-encrypted>
clear services application-identification statistics
<clear-appid-application-statistics>
clear services application-identification statistics cumulative
<clear-appid-application-statistics-cumulative>
clear services application-identification statistics interval
<clear-appid-application-statistics-interval>
clear services border-signaling-gateway
clear services border-signaling-gateway denied-messages
  <clear-service-bsg-denied-messages>
clear services border-signaling-gateway name-resolution-cache
clear services border-signaling-gateway name-resolution-cache all
  <clear-service-border-signaling-gateway-name-resolution-cache-all>
clear services border-signaling-gateway name-resolution-cache by-fqdn
<clear-border-signaling-gateway-name-resolution-cache-by-fqdn>
clear services border-signaling-gateway statistics
  <clear-service-border-signaling-gateway-statistics>
clear services captive-portal-content-delivery
clear services captive-portal-content-delivery statistics
clear services captive-portal-content-delivery statistics interface
<clear-cpcdd-interface-statistics>
clear services cos
clear services cos statistics
<clear-services-cos-statistics>

```

```
clear services crtp
clear services crtp statistics
<clear-services-crtp-statistics>
clear services dynamic-flow-capture
clear services dynamic-flow-capture criteria
<clear-services-dynamic-flow-capture-criteria>
clear services dynamic-flow-capture sequence-number
clear services flow-collector
<clear-services-flow-collector-information>
clear services flow-collector statistics
<clear-services-flow-collector-statistics>
clear service-msp-flow-ipaction-table
clear services ids
<clear-services-ids-tables>
clear services ids destination-table
<clear-services-ids-destination-table>
clear services ids pair-table
<clear-services-ids-pair-table>
clear services ids source-table
<clear-services-ids-source-table>
clear services inline
clear services inline nat
clear services inline nat pool
<clear-inline-nat-pool-information>
clear services inline nat statistics
<clear-inline-nat-statistics>
clear services inline softwire
clear services inline softwire statistics
<clear-inline-softwire-statistics>
clear services ipsec-vpn
clear services ipsec-vpn ipsec
clear services ipsec-vpn ipsec security-associations
<clear-services-ipsec-vpn-security-associations>
clear services ipsec-vpn ike
clear services ipsec-vpn ike security-associations
<clear-services-ike-security-associations>
clear services ipsec-vpn ike statistics
<clear-services-ike-statistics>
clear services pcp
clear services pcp epoch
clear services pcp statistics
clear services ipsec-vpn ipsec statistics
<clear-ipsec-vpn-statistics>
clear services l2tp
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp multilink
<clear-l2tp-multilink-information>
clear services l2tp session
<clear-l2tp-session-information>
clear services l2tp destination
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp tunnel
<clear-l2tp-tunnel-information>
clear services l2tp user
<clear-l2tp-user-session-information>
clear services local-policy-decision-function
clear services local-policy-decision-function statistics
```

```
clear services local-policy-decision-function statistics interface
<clear-local-policy-decision-function-statistics-interface>
clear services local-policy-decision-function statistics subscriber
<clear-local-policy-decision-function-statistics-subscriber>
clear services server-load-balance
  clear services server-load-balance external-manager-statistics
  <clear-external-manager-statistics>
  clear services server-load-balance hash-table
  <clear-hash-table-information>
clear services server-load-balance health-monitor-statistics
<clear-health-monitor-statistics>
clear services server-load-balance real-server-group-statistics
<clear-real-server-group-statistics>
clear services server-load-balance real-server-statistics
<clear-real-server-statistics>
clear services server-load-balance sticky
<clear-sticky-table>
clear services server-load-balance virtual-server-statistics
<clear-virtual-server-statistics>
clear services service-sets statistics integrity-drops
clear services service-sets statistics syslog
  <clear-service-set-syslog-statistics>
clear services stateful-firewall flow-analysis
  <clear-service-flow-analysis>
clear services stateful-firewall flows
  <clear-service-sfw-flow-table-information>
clear services stateful-firewall sip-call
  <clear-service-sfw-sip-call-information>
clear services stateful-firewall sip-register
  <clear-service-sfw-sip-register-information>
clear services stateful-firewall statistics
  <clear-stateful-firewall-statistics>
clear services stateful-firewall subscriber-analysis
  <clear-service-subs-analysis>
clear services subscriber
clear services subscriber sessions
  <get-services-subscriber-sessions>
clear services video-monitoring
  <clear-service-video-monitoring-information>
clear services video-monitoring mdi
  <clear-service-video-monitoring-mdi-information>
clear services video-monitoring mdi alarm
  <clear-service-video-monitoring-mdi-alarm-information>
clear services video-monitoring mdi alarm errors
  <clear-services-video-monitoring-mdi-alarm-errors>
clear services video-monitoring mdi alarm stats
  <clear-services-video-monitoring-mdi-alarm-statistics>
clear services video-monitoring mdi errors
  <clear-service-video-monitoring-mdi-errors>
clear services video-monitoring mdi statistics
  <clear-service-video-monitoring-mdi-statistics>
clear services softwire
clear services softwire statistics
  <clear-services-softwire-statistics>
clear services stateful-firewall
clear services stateful-firewall flow-analysis
  <clear-service-flow-analysis>
clear services stateful-firewall flows
  <clear-service-sfw-flow-table-information>
clear services pgcp
clear services pgcp gates
```

```
<clear-service-pgcp-gates>
clear services pgcp gates gateway
<clear-service-pgcp-gates-gateway>
clear services pgcp statistics
<clear-service-pgcp-statistics>
clear services pgcp statistics gateway
<clear-service-pgcp-statistics-gateway>
<clear-rfc2544-information>
<clear-aborted-tests-information>
<clear-active-tests-information>
<clear-completed-tests-information>
clear sflow
clear sflow collector
clear sflow collector statistics
<clear-sflow-collector-statistics>
clear snmp
clear snmp history
<clear-snmp-history>
clear snmp statistics
<clear-snmp-statistics>
clear spanning-tree
clear spanning-tree protocol-migration
clear spanning-tree protocol-migration interface
<clear-interface-stp-protocol-migration>
clear spanning-tree statistics
<clear-stp-interface-statistics>
clear spanning-tree statistics bridge
clear spanning-tree statistics interface
clear spanning-tree statistics routing-instance
<clear-stp-routing-instance-statistics>
clear spanning-tree stp-buffer
clear spanning-tree topology-change-counter
<clear-stp-topology-change-counter>
clear synchronous-ethernet
clear synchronous-ethernet esmc
clear synchronous-ethernet esmc statistics
clear system
clear system boot-media
<clear-boot-media>
clear system login
clear system login lockout
<clear-system-login-lockout>
clear-twamp-information
clear-twamp-server-information
clear-twamp-server-connection-information
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
```

```
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
```

```
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear validation
clear validation database
<clear-validation-database>
clear validation session
<clear-validation-session>
clear validation statistics
<clear-validation-statistics>
clear virtual-chassis
clear virtual-chassis heartbeat
<clear-virtual-chassis-heartbeat-statistics>
<clear virtual-chassis protocol>
clear virtual-chassis protocol statistics
<clear-virtual-chassis-statistics>
<clear-virtual-chassis-port-statistics>
clear vpls
clear vpls mac-address
<clear-vpls-mac-address>
clear vpls mac-table
<clear-vpls-mac-table>
clear vpls mac-table interface
<clear-vpls-interface-mac-table>
request interface rebalance
request pppoe
request pppoe connect
request pppoe disconnect
request security ike debug-disable
<get-disable-ike-debug>
request security ike debug-enable
<get-enable-ike-debug>
request services rpm twamp start
request services rpm twamp start client
<twamp-test-start>
request services rpm twamp stop
  request services rpm twamp stop client
<twamp-test-stop>
request snmp
<request-snmp-utility-mib-clear>
<request-snmp-utility-mib-set>
clear vpls statistics
```

```

<clear-vpls-statistics>
clear vrrp
<clear-vrrp-information>
clear vrrp interface
<clear-vrrp-interface-statistics>
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
clear services inline stateful-firewall
clear services inline stateful-firewall flows
<clear-service-inline-sfw-flow-table-information>
clear services inline stateful-firewall statistics
<clear-inline-stateful-firewall-statistics>
clear services service-sets statistics drop-flow-limit>
<clear-service-set-drop-flow-statistics>
clear services service-sets statistics jflow-log
<clear-service-set-jflow-log-statistics>
request services ipsec-vpn ipsec
request services ipsec-vpn ipsec switch
request services ipsec-vpn ipsec switch tunnel
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>

```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

configure

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can enter configuration mode.

Commands

```
configure
request snmp
request-snmp-utility-mib-clear
request-snmp-utility-mib-set
```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

control

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can perform all control-level operations; can modify any configuration.

Commands

```
request jnu
request jnu role
request jnu schema
request jnu schema add
request jnu schema delete
```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

field

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view field debug commands.

| | |
|---------------------------------------|---|
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 48 • Understanding Junos OS Access Privilege Levels on page 7 • Configuring Access Privilege Levels on page 37 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 38 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |

firewall

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view the firewall filter configuration in configuration mode.

| | |
|---------------------------------------|---|
| Commands | <pre>show firewall <get-firewall-information> show firewall counter <get-firewall-counter-information> show firewall filter <get-firewall-filter-information> show firewall filter version <get-filter-version> show firewall log <get-firewall-log-information> show firewall prefix-action-stats <get-firewall-prefix-action-information> show policer <get-policer-information></pre> |
| Configuration Hierarchy Levels | <pre>[edit dynamic-profiles firewall] [edit firewall] [edit logical-systems firewall]</pre> |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 48 • Understanding Junos OS Access Privilege Levels on page 7 • Configuring Access Privilege Levels on page 37 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 38 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 • firewall-control on page 106 |

firewall-control

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view and configure firewall filter information at the [\[edit dynamic-profiles firewall\]](#), [\[edit firewall\]](#), and [\[edit logical-systems firewall\]](#) hierarchy levels.

Commands

```
show firewall
  <get-firewall-information>

show firewall counter
  <get-firewall-counter-information>

show firewall filter
  <get-firewall-filter-information>

show firewall filter version
  <get-filter-version>

show firewall log
  <get-firewall-log-information>

show firewall prefix-action-stats
  <get-firewall-prefix-action-information>

show policer
```

Configuration Hierarchy Levels

```
[edit dynamic-profiles firewall]
[edit firewall]
[edit logical-systems firewall]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
 - [firewall on page 105](#)

floppy

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can read from and write to the removable media.

Commands No associated CLI commands.

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)

- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

flow-tap

| | |
|---------------------------------------|---|
| Supported Platforms | M Series, MX Series, SRX Series, T Series, vSRX |
| | Can view the flow-tap configuration in configuration mode. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | <pre>[edit services flow-tap] [edit services radius-flow-tap] [edit system services flow-tap-dtcp]</pre> |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 48 • Understanding Junos OS Access Privilege Levels on page 7 • Configuring Access Privilege Levels on page 37 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 38 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 • flow-tap-control on page 107 |

flow-tap-control

| | |
|---------------------------------------|---|
| Supported Platforms | M Series, MX Series, SRX Series, T Series, vSRX |
| | Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the <code>[edit services flow-tap]</code> , <code>[edit services radius-flow-tap]</code> , and <code>[edit system services flow-tap-dtcp]</code> hierarchy levels. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | <pre>[edit services flow-tap] [edit services radius-flow-tap] [edit system services flow-tap-dtcp]</pre> |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 48 • Understanding Junos OS Access Privilege Levels on page 7 • Configuring Access Privilege Levels on page 37 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 38 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |

- [flow-tap on page 107](#)

flow-tap-operation

| | |
|---------------------------------------|---|
| Supported Platforms | M Series, MX Series, PTX Series, SRX Series, T Series, vSRX |
| | Can make flow-tap requests to the router. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 48• Understanding Junos OS Access Privilege Levels on page 7• Configuring Access Privilege Levels on page 37• Specifying Access Privileges for Junos OS Operational Mode Commands on page 38• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |

idp-profiler-operation

| | |
|---|--|
| Supported Platforms | M Series, MX Series, SRX Series, T Series, vSRX |
| | Can view profiler data. |
| Commands | No associated CLI commands. |
| CLI Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |

interface

| | |
|---------------------------------------|--|
| Supported Platforms | EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX |
| | Can view the interface configuration in configuration mode. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | <ul style="list-style-type: none">[edit accounting-options][edit chassis][edit class-of-service][edit class-of-service interfaces][edit dynamic-profiles class-of-service][edit dynamic-profiles class-of-service interfaces][edit dynamic-profiles interfaces][edit dynamic-profiles routing-instances instance system services dhcp-local-server][edit dynamic-profiles routing-instances instance system services static-subscribers group][edit forwarding-options][edit interfaces] |

```
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services
dhcp-local-server]
[edit logical-systems routing-instances instance system services
static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
[edit services radius-flow-tap interfaces]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [interface-control on page 109](#)

interface-control

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the **[edit chassis]**, **[edit class-of-service]**, **[edit groups]**, **[edit forwarding-options]**, and **[edit interfaces]** hierarchy levels.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit accounting-options]
[edit chassis]
[edit class-of-service]
[edit class-of-service interfaces]
[edit dynamic-profiles class-of-service]
[edit dynamic-profiles class-of-service interfaces]
[edit dynamic-profiles interfaces]
[edit dynamic-profiles routing-instances instance system services
dhcp-local-server]
[edit dynamic-profiles routing-instances instance system services
static-subscribers group]
[edit forwarding-options]
[edit interfaces]
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services
dhcp-local-server]
```

```
[edit logical-systems routing-instances instance system services
static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
[edit services radius-flow-tap interfaces]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
 - [interface on page 108](#)

maintenance

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell, and can halt and reboot the router.

Commands

```
clear system reboot
<clear-reboot>

clear-system-services-reverse-information
file archive
<file-archive>
file change-owner
<file-change-owner>
<extract-file>
monitor traffic
request chassis afeb
request chassis beacon
<request-chassis-beacon>
request chassis cb
<request-chassis-cb>
request chassis ccg
<request-chassis-ccg>

request chassis cfeb
request chassis cfeb master
request chassis cip
request chassis fabric
request chassis fabric device
request chassis fabric guided-cabling
request chassis fabric plane
request chassis fabric upgrade-bandwidth
request chassis fabric upgrade-bandwidth fpc
request chassis fabric upgrade-bandwidth info
```

```

request chassis feb
  <request-feb>

request chassis fpc
<request-chassis-fpc>
request chassis mcs
request chassis mic
request chassis optics
request chassis pcg
request chassis pic
<request-chassis-pic>
request chassis redundancy
request chassis redundancy feb
  <request-redundancy-feb>
request chassis routing-engine
<request-chassis-routing-engine>
request chassis routing-engine hard-disk-test
request chassis routing-engine master
request chassis scg
request chassis sfb
request chassis sfm
request chassis sfm master
request chassis sib
<request-chassis-sib>
request chassis sib f13

request chassis sib f2s
request chassis sib optics
request chassis spmb
<request-chassis-spmb>
request chassis ssb
request chassis ssb master
request chassis synchronization
request chassis synchronization force
request chassis synchronization force automatic-switching
request chassis synchronization force mark-failed
request chassis synchronization force unmark-failed
request chassis synchronization switch
request chassis tfeb
request chassis vcpu
request chassis vnpu
request diagnostics
request diagnostics tdr
request diagnostics tdr abort
request diagnostics tdr abort interface
<abort-tdr-interface-diagnostics>
request diagnostics tdr start
request diagnostics tdr start interface
<request-tdr-interface-diagnostics>
request l2circuit-switchover
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
  <reload-eedebg-action-profile>

```

```
request security idp
  <request-idp-security-policy-load>

request security idp security-package
request security idp security-package download
  <request-idp-security-package-download>

request security idp security-package download version
  <request-idp-security-package-download-version>

request security idp security-package install
  <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
  <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
  <request-idp-ssl-key-delete>
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security ike
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate ca-profile-group
request security pki ca-certificate ca-profile-group load
request security pki ca-certificate enroll
request security pki local-certificate export
request security pki ca-certificate load
  <load-pki-ca-certificate>
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki crl
request security pki crl load
  <load-pki-crl>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki verify-integrity-status
<verify-integrity-status>
request services fips
request services fips authorize
request services fips authorize pic
request services fips zeroize
request services fips zeroize pic
request services flow-collector
request services flow-collector change-destination
  <request-services-flow-collector-destination>
```

```
request services ggsn
request services ggsn pdp
request services ggsn pdp terminate
request services ggsn pdp terminate apn
    <request-ggsn-terminate-contexts-apn>

request services ggsn pdp terminate context
    <request-ggsn-terminate-context>

request services ggsn pdp terminate context msisdn
    <request-ggsn-terminate-msisdn-context>

request services ggsn restart
request services ggsn restart interface
    <request-ggsn-restart-interface>

request services ggsn restart node
    <request-ggsn-restart-node>

request services ggsn start
request services ggsn start interface
request services ggsn stop
request services ggsn stop interface
    <request-ggsn-stop-interface>

request services ggsn stop node
    <request-ggsn-stop-node>

request services ggsn trace
request services ggsn trace software
request services ggsn trace software update
    <request-ggsn-software-update>

request services ggsn trace start
request services ggsn trace start imsi
    <request-ggsn-start-imsi-trace>

request services ggsn trace start msisdn
    <request-ggsn-start-msisdn-trace>

request services ggsn trace stop
request services ggsn trace stop all
    <request-ggsn-stop-trace-activity>

request services ggsn trace stop imsi
    <request-ggsn-stop-imsi-trace>

request services ggsn trace stop msisdn
    <request-ggsn-stop-msisdn-trace>

request support
request support information
request system
request system boot-media
    <request-boot-media>
request system certificate
request system certificate add
request system commit
request system commit server
request system commit server pause
    <request-commit-server-pause>
```

```
request system commit server queue
request system commit server queue cleanup
<request-commit-server-cleanup>
request system commit server start
<request-commit-server-start>
request system configuration
request system configuration rescue
request system configuration rescue delete
  <request-delete-rescue-configuration>

request system configuration rescue save
  <request-save-rescue-configuration>
request system diagnostics
request system diagnostics log-archive
<request-log>
request system diagnostics transfer-control
<transfer-control>
request system firmware
request system firmware downgrade
request system firmware downgrade feb
request system firmware downgrade fpc
request system firmware downgrade pic
request system firmware downgrade poe
request system firmware downgrade re
request system firmware downgrade scb
request system firmware downgrade sfm
request system firmware downgrade spmb
request system firmware downgrade ssb
request system firmware downgrade vcpu
request system firmware upgrade
request system firmware upgrade feb
request system firmware upgrade fpc
request system firmware upgrade fpga
request system firmware upgrade fpga fpc
request system firmware upgrade fpga scb
<request-scb-fpga-upgrade>
request system firmware upgrade pic
request system firmware upgrade poe
request system firmware upgrade re
request system firmware upgrade re bios
request system firmware upgrade scb
request system firmware upgrade sfm
request system firmware upgrade spmb
request system firmware upgrade ssb
request system firmware upgrade vcpu
request system halt
  <request-halt>

request system keep-alive
request system license
request system license add
request system license delete
  <request-license-delete>
request system license revoke-licenses
<license-revoke-licenses>

request system license save
request system license update
  <request-license-update>
request system logout
request system partition
```

```
request system partition abort
request system partition compact-flash
request system partition hard-disk
request system power-off
    <request-power-off>

request system power-on
<request-power-on-other-re>
request system process
request system process terminate
<request-process-terminate>
request system reboot
    <request-reboot>
request system recover

request system scripts
request system scripts add
    <request-scripts-package-add>

request system scripts convert
request system scripts convert slax-to-xslt
request system scripts convert xslt-to-slax
request system scripts delete
    <request-scripts-package-delete>

request system scripts event-scripts
request system scripts event-scripts reload
    <reload-event-scripts>

request system scripts refresh-from
    <request-script-refresh-from>

request system scripts rollback
    <request-scripts-package-rollback>

request system scripts synchronize
<request-scripts-synchronize>

request system snapshot
    <request-snapshot>

request system software
request system software abort
request system software abort in-service-upgrade
    <abort-in-service-upgrade>

request system software add
    <request-package-add>

request system software delete
    <request-package-delete>

request system software delete-backup
    <request-package-delete-backup>

request system software in-service-upgrade
    <request-package-in-service-upgrade>

request system software nonstop-upgrade
    <request-package-nonstop-upgrade>
request system software recovery-package
```

```

request system software recovery-package add
request system software recovery-package delete
request system software recovery-package extract
request system software recovery-package extract ex-8200-package
request system software recovery-package extract ex-xre200-package
request system software rollback
    <request-package-rollback>

request system software validate
    <request-package-validate>
request system software validate in-service-upgrade
    <check-in-service-upgrade>

request system storage
request system storage cleanup
    <request-system-storage-cleanup>
request system storage cleanup qfabric
    <remove-qfabric-repository-contents>
request system storage mount
<request-mount>
request system storage unified-edge
request system storage unified-edge charging
request system storage unified-edge charging media
request system storage unified-edge media
request system storage unified-edge media eject
request system storage unified-edge media prepare
request system storage unmount
<request-unmount>
request system subscriber-management
request system subscriber-management new-sessions-disable
<request-sm-new-sessions-disable>
request system subscriber-management new-sessions-enable
<request-sm-new-sessions-enable>
request system zeroize
request vpls-switchover
set date
set date ntp
show chassis usb
show chassis usb storage
<get-usb-storage-status>
show services fips
show system configuration database
show system configuration database usage
<get-database-usage>
start shell
start shell user
test access
test access profile
    <get-radius-profile-access-test-result>

test access radius-server
    <get-radius-server-access-test-result>
get-test-services-l2tp-tunnel-result

```

Configuration Hierarchy Levels

```

[edit event-options]
[edit security ipsec internal]
[edit security ipsec trusted-channel]
[edit services dynamic-flow-capture traceoptions]
[edit services ggsn]
[edit system fips]

```

```
[edit services ggsn rule-space]
[edit system processes daemon-process command]
[edit system scripts]
[edit system scripts commit]
[edit system scripts op]
[edit system scripts snmp]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

network

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.

Commands

```
mtrace
mtrace from-source
mtrace monitor
mtrace to-gateway
ping
    <ping>

ping atm
ping cls
ping ethernet
    <request-ping-ethernet>
ping fibre-channel
ping mpls
ping mpls bgp
    <request-ping-bgp-lsp>
ping mpls l2circuit
ping mpls l2circuit interface
    <request-ping-l2circuit-interface>

ping mpls l2circuit virtual-circuit
    <request-ping-l2circuit-virtual-circuit>

ping mpls l2vpn
ping mpls l2vpn fec129
ping mpls l2vpn fec129 interface
    <request-ping-l2vpn-fec129-interface>
ping mpls l2vpn instance
    <request-ping-l2vpn-instance>

ping mpls l2vpn interface
    <request-ping-l2vpn-interface>

ping mpls l3vpn
    <request-ping-l3vpn>

ping mpls ldp
```

```
<request-ping-ldp-lsp>

ping mpls ldp p2mp
  <request-ping-ldp-p2mp-lsp>

ping mpls lsp-end-point
  <request-ping-lsp-end-point>

ping mpls rsvp
  <request-ping-rsvp-lsp>

ping overlay
  <request-ping-overlay>
ping vpls
ping vpls instance
  <request-ping-vpls-instance>

request routing-engine
request routing-engine login
  <request-routing-engine-login>
request routing-engine login other-routing-engine
  <request-login-to-other-routing-engine>
request services flow-collector
request services flow-collector test-file-transfer
  <request-services-flow-collector-test-file-transfer>

show host
show interfaces level-extra descriptions
show multicast minfo
ssh
telnet
traceroute
  <traceroute>

traceroute cpls
traceroute ethernet
  <request-traceroute-ethernet>

traceroute monitor
traceroute mpls
traceroute mpls l2vpn
  <traceroute-mpls-l2vpn>
traceroute mpls l2vpn fec129
  <traceroute-mpls-mspw>
traceroute mpls ldp
  <traceroute-mpls-ldp>
traceroute mpls rsvp
  <traceroute-mpls-rsvp>
traceroute overlay
  <request-traceroute-overlay>
```

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

pgcp-session-mirroring

Supported Platforms [M Series, MX Series, PTX Series, SRX Series, T Series, vSRX](#)

Can view session mirroring configuration by using the **pgcp** command.

Commands `show services pgcp gates gate-way display session-mirroring`

**Configuration
Hierarchy Levels** `[edit services pgcp gateway session-mirroring]`
 `[edit services pgcp session-mirroring]`

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [pgcp-session-mirroring-control on page 119](#)

pgcp-session-mirroring-control

Supported Platforms [M Series, MX Series, SRX Series, T Series, vSRX](#)

Can modify PGCP session mirroring configuration

Commands `show services pgcp gates gate-way display session-mirroring`

**Configuration
Hierarchy Levels** `[edit services pgcp gateway session-mirroring]`
 `[edit services pgcp session-mirroring]`

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [pgcp-session-mirroring on page 119](#)

reset

Supported Platforms [EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX](#)

Can restart software processes by using the **restart** command and can configure whether software processes configured at the **[edit system processes]** hierarchy level are enabled or disabled.

| | |
|-----------------|--|
| Commands | <pre>request chassis cfeb master switch request chassis cfeb master switch no-confirm request chassis routing-engine master acquire request chassis routing-engine master acquire force request chassis routing-engine master acquire force no-confirm request chassis routing-engine master acquire no-confirm request chassis routing-engine master release request chassis routing-engine master release no-confirm request chassis routing-engine master switch request chassis routing-engine master switch no-confirm request chassis sfm master switch request chassis sfm master switch no-confirm request chassis ssb master switch request chassis ssb master switch no-confirm restart restart kernel-replication <restart-kernel-replication> restart-named-service restart routing <routing-restart> restart services restart services border-signaling-gateway <restart-border-signaling-gateway-service> restart services pgcp <restart-pgcp-service> restart web-management <restart-web-management></pre> |
|-----------------|--|

| | |
|---------------------------------------|--|
| Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |
|---------------------------------------|--|

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 48• Understanding Junos OS Access Privilege Levels on page 7• Configuring Access Privilege Levels on page 37• Specifying Access Privileges for Junos OS Operational Mode Commands on page 38• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |
|------------------------------|---|

rollback

| | |
|----------------------------|--|
| Supported Platforms | EX Series , M Series , MX Series , PTX Series , SRX Series , T Series , vSRX |
|----------------------------|--|

Can roll back to previous configurations.

| | |
|-----------------|----------|
| Commands | rollback |
|-----------------|----------|

| | |
|---------------------------------------|--------|
| Configuration Hierarchy Levels | [edit] |
|---------------------------------------|--------|

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

secret

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view passwords and other authentication keys in the configuration.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius-disconnect preauthentication-secret]
[edit access radius-disconnect secret]
[edit access radius-server preauthentication-secret]
[edit access radius-server secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
[edit dynamic-profiles interfaces interface unit ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap
default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap]
[edit logical-systems interfaces interface unit ppp-options pap
default-password]
[edit logical-systems interfaces interface unit ppp-options pap local-password]
[edit logical-systems routing-instances instance system services
static-subscribers authentication password]
[edit logical-systems routing-instances instance system services
static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication
password]
[edit logical-systems system services static-subscribers group authentication
password]
[edit routing-instances instance system services static-subscribers
authentication password]
[edit routing-instances instance system services static-subscribers group
authentication password]
[edit services ggsn apn radius accounting server secret]
```

```
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server preauthentication-secret]
[edit system accounting destination radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server preauthentication-secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius
accounting-shared-secret]
[edit system services static-subscribers authentication password]
[edit system services static-subscribers group authentication password]
[edit system tacplus-server secret]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 48](#)
 - [Understanding Junos OS Access Privilege Levels on page 7](#)
 - [Configuring Access Privilege Levels on page 37](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
 - [secret-control on page 122](#)

secret-control

Supported Platforms EX Series, M Series, MX Series, SRX Series, T Series, vSRX

Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```
[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius-disconnect secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
[edit dynamic-profiles interfaces interface unit ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap
default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap]
```

```
[edit logical-systems interfaces interface unit ppp-options pap
default-password]
[edit logical-systems interfaces interface unit ppp-options pap local-password]
[edit logical-systems routing-instances instance system services
static-subscribers authentication password]
[edit logical-systems routing-instances instance system services
static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication
password]
[edit logical-systems system services static-subscribers group authentication
password]
[edit routing-instances instance system services static-subscribers
authentication password]
[edit routing-instances instance system services static-subscribers group
authentication password]
[edit services ggsn apn radius accounting server secret]
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius
accounting-shared-secret]
[edit system services static-subscribers authentication password]
[edit system services static-subscribers group authentication password]
[edit system tacplus-server secret]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [secret on page 121](#)

security

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view security configuration.

Commands

```
clear security
clear security alarms
  <clear-security-alarm-information>
clear security idp
clear security idp application-ddos
clear security idp application-ddos cache
  <clear-idp-appddos-cache>

clear security idp application-identification
clear security idp application-identification application-system-cache
  <clear-idp-application-system-cache>

clear security idp application-statistics
```

```
<clear-idp-applications-information>

clear security idp attack
clear security idp attack table
  <clear-idp-attack-table>

clear security idp counters
  <clear-idp-counters-by-counter-class>

clear security idp ssl-inspection
clear security idp ssl-inspection session-id-cache
  <clear-idp-ssl-session-cache-information>
clear security idp status
  <clear-idp-status-information>
clear security log
  <clear-security-log-information>
clear security pki
clear security pki ca-certificate
  <clear-pki-ca-certificate>
clear security pki certificate-request
  <clear-pki-certificate-request>
clear security pki crl
  <clear-pki-crl>
clear security pki key-pair
  <clear-pki-key-pair>
clear security pki local-certificate
  <clear-pki-local-certificate>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
  <request-idp-policy-load>
request security idp security-package
request security idp security-package download
  <request-idp-security-package-download>

request security idp security-package download version
  <request-idp-security-package-download-version>

request security idp security-package install
  <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
  <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
  <request-idp-ssl-key-delete>
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
```

```

    <load-pki-ca-certificate>
request security pki crl
request security pki crl load
    <request security pki crl load>
request security pki generate-certificate-request
    <generate-pki-certificate-request>
request security pki generate-key-pair
    <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
    <verify-pki-local-certificate>
request security pki verify-integrity-status
<verify-integrity-status>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
    <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
    <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
    <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
    <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
    <get-idp-application-system-cache>

show security idp application-statistics
    <get-idp-applications-information>

show security idp attack
show security idp attack description
    <get-idp-attack-description-information>
show security idp attack detail
    <get-idp-attack-detail-information>
show security idp attack table
    <get-idp-attack-table-information>

show security idp counters
    <get-idp-counter-information>

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
    <get-idp-memory-information>

show security idp policies
    <get-idp-subscriber-policy-list>

show security idp policy-templates-list
    <get-idp-policy-template-information>
    <get-idp-predefined-attack-groups>
    <get-idp-predefined-attack-group-filters>
    <get-idp-predefined-attacks>
    <get-idp-predefined-attack-filters>
    <get-idp-recent-security-package-information>
show security idp policy-commit-status

```

```
<get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp security-package-version
  <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
  <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>
```

**Configuration
Hierarchy Levels**

```
[edit security]
[edit security alarms]
[edit security log]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [security-control on page 126](#)

security-control

Supported Platforms

[EX Series](#), [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view and configure security information at the **[edit security]** hierarchy level.

Commands

```
clear security
clear security alarms
```

```

    <clear-security-alarm-information>
clear security idp
clear security idp application-ddos
clear security idp application-ddos cache
    <clear-idp-appddos-cache>

clear security idp application-identification
clear security idp application-identification application-system-cache
    <clear-idp-application-system-cache>

clear security idp application-statistics
    <clear-idp-applications-information>

clear security idp attack
clear security idp attack table
    <clear-idp-attack-table>

clear security idp counters
    <clear-idp-counters-by-counter-class>

clear security idp ssl-inspection
clear security idp ssl-inspection session-id-cache
    <clear-idp-ssl-session-cache-information>
clear security idp status
    <clear-idp-status-information>
clear security log
    <clear-security-log-information>
clear security pki
clear security pki ca-certificate
    <clear-pki-ca-certificate>
clear security pki certificate-request
    <clear-pki-certificate-request>
clear security pki crl
    <clear-pki-crl>
clear security pki key-pair
    <clear-pki-key-pair>
clear security pki local-certificate
    <clear-pki-local-certificate>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
    <request-idp-policy-load>
request security idp security-package
request security idp security-package download
    <request-idp-security-package-download>

request security idp security-package download version
    <request-idp-security-package-download-version>

request security idp security-package install
    <request-idp-security-package-install>

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
    <request-idp-ssl-key-add>

```

```
request security idp ssl-inspection key delete
    <request-idp-ssl-key-delete>
request security idp storage-cleanup
    <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
    <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
    <load-pki-ca-certificate>
request security pki crl
request security pki crl load
    <request security pki crl load>
request security pki generate-certificate-request
    <generate-pki-certificate-request>
request security pki generate-key-pair
    <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
    <verify-pki-local-certificate>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
    <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
    <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
    <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
    <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
    <get-idp-application-system-cache>

show security idp application-statistics
    <get-idp-applications-information>

show security idp attack
show security idp attack description
    <get-idp-attack-description-information>
show security idp attack detail
    <get-idp-attack-detail-information>
show security idp attack table
    <get-idp-attack-table-information>

show security idp counters
    <get-idp-counter-information>

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
    <get-idp-memory-information>

show security idp policies
    <get-idp-subscriber-policy-list>
```

```

show security idp policy-templates-list
  <get-idp-policy-template-information>
  <get-idp-predefined-attack-groups>
  <get-idp-predefined-attack-group-filters>
  <get-idp-predefined-attacks>
  <get-idp-predefined-attack-filters>
  <get-idp-recent-security-package-information>
show security idp policy-commit-status
  <get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp security-package-version
  <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
  <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>

```

**Configuration
Hierarchy Levels**

```

[edit security]
[edit security alarms]
[edit security log]

```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [security on page 123](#)

shell

| | |
|---------------------------------------|---|
| Supported Platforms | EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX |
| | Can start a local shell on the router. |
| Commands | <code>start shell</code> <code>start shell user</code> |
| Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 48• Understanding Junos OS Access Privilege Levels on page 7• Configuring Access Privilege Levels on page 37• Specifying Access Privileges for Junos OS Operational Mode Commands on page 38• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |

snmp

| | |
|---------------------------------------|---|
| Supported Platforms | EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX |
| | Can view Simple Network Management Protocol (SNMP) configuration. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | <code>[edit snmp]</code> |
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 48• Understanding Junos OS Access Privilege Levels on page 7• Configuring Access Privilege Levels on page 37• Specifying Access Privileges for Junos OS Operational Mode Commands on page 38• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42 |

system

| | |
|----------------------------|---|
| Supported Platforms | EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX |
| | Can view system-level configuration information. |
| Commands | <code>request chassis synchronization</code> <code>request chassis synchronization force</code> <code>request chassis synchronization force automatic-switching</code> <code>request chassis synchronization force mark-failed</code> <code>request chassis synchronization force unmark-failed</code> <code>request chassis synchronization switch</code> <code>request virtual-chassis</code> |

```

request virtual-chassis device-reachability
<get-virtual-chassis-diagnostic-information>
request virtual-chassis member-id
request virtual-chassis member-id delete
delete-virtual-chassis-member-id
request virtual-chassis member-id set
<set-virtual-chassis-member-id>
request virtual-chassis mode
request virtual-chassis mode mixed
<request-virtual-chassis-mode-mixed>
request virtual-chassis reactivate
<request-virtual-chassis-reactivate>
request virtual-chassis recycle
<request-virtual-chassis-recycle>
request virtual-chassis renumber
<request-virtual-chassis-renumber>
request virtual-chassis routing-engine
request virtual-chassis routing-engine master
request virtual-chassis routing-engine master switch
<switch-vc-routing-engine-protocol-master>
request virtual-chassis vc-port
request virtual-chassis vc-port delete
request virtual-chassis vc-port delete fpc-slot
<request-virtual-chassis-vc-port-delete-fpc-slot>
request virtual-chassis vc-port delete pic-slot
<request-virtual-chassis-vc-port-delete-pic-slot>
request virtual-chassis vc-port set
request virtual-chassis vc-port set fpc-slot
<request-virtual-chassis-vc-port-set-fpc-slot>
request virtual-chassis vc-port set interface
<request-virtual-chassis-vc-port-set-interface>
request virtual-chassis vc-port set pic-slot
<request-virtual-chassis-vc-port-set-pic-slot>
<set-virtual-chassis-mode>

```

Configuration Hierarchy Levels

```

[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers
  tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit fabric virtual-chassis]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems protocols uplink-failure-detection]
[edit logical-systems routing-instances instance forwarding-options helpers
  bootp]
[edit logical-systems routing-instances instance forwarding-options helpers
  domain]
[edit logical-systems routing-instances instance forwarding-options helpers
  port]
[edit logical-systems routing-instances instance forwarding-options helpers
  tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit logical-systems system syslog]

```

```
[edit poe]
[edit protocols uplink-failure-detection]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system boot loader authentication]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system no-debugger-on-alt-break]
[edit system no-redirects-ipv6]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports auxiliary silent-with-modem]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system ports console silent-with-modem]
[edit system processes]
[edit system proxy]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
```

```
[edit virtual-chassis locality-bias]
[edit vlans]
```

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [system-control on page 133](#)

system-control

Supported Platforms EX Series, M Series, MX Series, SRX Series, T Series, vSRX

Can view system-level configuration information and configure it at the **[edit system]** hierarchy level.

**Configuration
Hierarchy Levels**

```
[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers
tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems routing-instances instance forwarding-options helpers
bootp]
[edit logical-systems routing-instances instance forwarding-options helpers
domain]
[edit logical-systems routing-instances instance forwarding-options helpers
port]
[edit logical-systems routing-instances instance forwarding-options helpers
tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit poe]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
```

```
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system processes]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
[edit vlans]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [system on page 130](#)

trace**Supported Platforms**

[EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view trace file settings and configure trace file properties.

Commands

```
clear log
```

```

    <clear-log>
monitor
request-monitor-ethernet-delay-measurement
    <request-monitor-ethernet-loss-measurement>
monitor interface
monitor interface traffic
monitor label-switched-path
monitor list
monitor start
monitor static-lsp
monitor stop
show log
<get-log>
show log user
    <get-syslog-events>

```

Configuration Hierarchy Levels

```

[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit class-of-service application-traffic-control traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles class-of-service application-traffic-control
traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management
traceoptions]
[dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols oam gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping
traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer

```

```
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery
  traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[edit dynamic-profiles routing-instances instance routing-options multicast
  traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance services mobile-ip
  traceoptions]
[edit dynamic-profiles routing-instances instance system services
  dhcp-local-server traceoptions]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options traceoptions]
[edit jnx-example traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay
  interface-traceoptions]
[edit logical-systems vlans domain multicast-snooping-options traceoptions]
[edit logical-systems vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems forwarding-options dhcp-relay traceoptions]
[edit logical-systems protocols ancp traceoptions]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dot1x traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols ilmi traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols lacp traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet fnp traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam
  traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam
  traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet fnp traceoptions]
```

```

[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp lsp-set traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group
traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp group
traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery
traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast
traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip
traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server interface-traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]

```

```
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols protocols oam ethernet fnp]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp lsp-set traceoptions]
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
```

```

[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit services l2tp traceoptions]
[edit services server-load-balance traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system ddos-protection traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes dhcp-service interface-traceoptions]
[edit system processes dhcp-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes mag-service traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [trace-control on page 139](#)

trace-control

Supported Platforms EX Series, M Series, MX Series, SRX Series, T Series, vSRX

Can modify trace file settings and configure trace file properties.

Configuration Hierarchy Levels

```
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management
traceoptions]
[edit dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols oam gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols
igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping
traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer
traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery
traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[edit dynamic-profiles routing-instances instance routing-options multicast
traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance services mobile-ip
traceoptions]
[edit dynamic-profiles routing-instances instance system services
dhcp-local-server traceoptions]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
```

```

[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options traceoptions]
[edit forwarding-options dhcp-relay interface-traceoptions]
[edit forwarding-options dhcp-relay traceoptions]
[edit jnx-example traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems vlans domain multicast-snooping-options traceoptions]
[edit logical-systems vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems forwarding-options dhcp-relay traceoptions]
[edit logical-systems protocols ancp traceoptions]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dot1x traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols ilmi traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols lacp traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam
traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam
traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options
dhcp-relay interface-traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options
dhcp-relay traceoptions]
[edit logical-systems routing-instances instance vlans domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols

```

```
igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay
traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor
traceoptions]
[edit logical-systems routing-instances instance protocols bgp group
traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp group
traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer
traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery
traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast
traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip
traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server interface-traceoptions]
[edit logical-systems routing-instances instance system services
dhcp-local-server traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
```

```
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay
traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance system services dhcp-local-server
interface-traceoptions]
```

```

[edit routing-instances instance system services dhcp-local-server traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit system ddos-protection traceoptions]
[edit services l2tp traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services server-load-balance traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services dhcp-local-server traceoptions]
[edit system services dhcp-local-server interface-traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)
- [trace on page 134](#)

view

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#), [vSRX](#)

Can view current system-wide, routing table, and protocol-specific values and statistics.

Commands

```

clear ipv6 router-advertisement
<clear-ipv6-router-advertisement-information>
<request-validation-policy>
show
show accounting

show accounting profile

```

```
<get-accounting-profile-information>

show accounting records
  <get-accounting-record-information>

show amt
show amt statistics
  <get-amt-statistics>
show amt summary
  <get-amt-summary>
show amt tunnel
  <get-amt-tunnel-information>
show amt tunnel gateway-address
  <get-amt-tunnel-gateway-address>
show amt tunnel tunnel-interface
  <get-amt-tunnel-interface>
show analytics collector
  <get-analytics-collector>
show ancp
show ancp cos
  <get-ancp-cos-information>
show ancp cos last-update
  <get-ancp-cos-last-update-information>

show ancp cos pending-update
  <get-ancp-cos-pending-information>

show ancp neighbor
  <get-ancp-neighbor-information>
show ancp statistics
  <get-ancp-stats-information>
show ancp subscriber
  <get-ancp-subscriber-information>

show ancp subscriber identifier
  <get-ancp-subscriber-identifier-information>
show ancp subscriber neighbor
show app-engine
show app-engine information
show app-engine packages
show app-engine packages remote
  <get-virtual-machine-package-remote>
show app-engine packages system
  <get-virtual-machine-package-system>
show app-engine processes
show app-engine resource-usage
show app-engine route-table
show app-engine routing-instance
show app-engine routing-instance compute-clusters
show app-engine routing-instance virtual-machines
show app-engine status
show app-engine virtual-machine package
  <get-virtual-machine-package-information>
show app-engine virtual-machine vm-instance
show aps
  <get-aps-information>

show aps group
  <get-aps-group-information>
show aps interface
  <get-aps-interface-information>
```

```
show arp
    <get-arp-table-information>

show as-path
    <get-as-path>
show as-path domain
    <get-as-path-domain>
show auto-configuration
show auto-configuration interfaces
show backup-selection
    <get-backup-selection>
show backup-selection instance
    <get-backup-selection-instance>
show bfd
show bfd session
    <get-bfd-session-information>

show bfd session address
    <get-bfd-session-address>
show bfd session client
    <get-bfd-session-client>
show bfd session client rsvp-oam
    <get-bfd-session-client-rsvp>
show bfd session client vpls-oam
    <get-bfd-session-client-vpls>
show bfd session client vpls-oam instance
    <get-bfd-session-client-vpls-instance>
show bfd session discriminator
    <get-bfd-session-discriminator>
show bfd session prefix
    <get-bfd-session-prefix>
show bfd subscriber
show bfd subscriber session
    <get-bfd-subscriber-session>
show bgp
show bgp bmp
    <get-bgp-monitoring-protocol-statistics>
show bgp group
    <get-bgp-group-information>

show bgp group rtf
    <get-bgp-rtf-information>

show bgp group traffic-statistics
    <get-bgp-traffic-statistics-information>

show bgp neighbor
    <get-bgp-neighbor-information>

show bgp neighbor orf
    <get-bgp-orf-information>

show bgp replication
    <get-bgp-replication-information>
show bgp summary
    <get-bgp-summary-information>

show bridge
show bridge domain
    <get-bridge-instance-information>
```

```
show bridge domain operational
<get-operational-bridge-instance-information>
show bridge evpn
show bridge evpn arp-table
<get-bridge-evpn-arp-table>
show bridge evpn peer-gateway-macs
<get-bridge-peer-gateway-mac>
<get-bridge-flood-information>
show bridge flood
show bridge flood event-queue
<get-bridge-domain-event-queue-information>

show bridge flood route
show bridge flood route all-ce-flood
<get-show-bridge-domain-all-ce-flood-route-information>

show bridge flood route all-ve-flood
<get-show-bridge-domain-ve-flood-route-information>
show bridge flood route alt-root-flood
<get-bridge-domain-alt-root-flood-route-information>
show bridge flood route bd-flood
<get-bridge-domain-bd-flood-route-information>
show bridge flood route mlp-flood
<get-bridge-domain-mlp-flood-route-information>
show bridge flood route re-flood
<get-bridge-domain-re-flood-route-information>
show bridge mac-table
<get-bridge-mac-table>
show bridge mac-table interface
<get-bridge-interface-mac-table>
show bridge statistics
<get-bridge-statistics-information>
show chassis
show chassis adc
show chassis alarms
<get-alarm-information>
show chassis alarms fpc
<get-fpc-alarm-information>
show chassis beacon
<get-chassis-beacon-information>
show chassis beacon cb
<get-chassis-cb-beacon-information>
show chassis environment adc
show chassis environment ccg
<get-environment-ccg-information>
show chassis cfeb
<get-cfeb-information>
show chassis cip
show chassis craft-interface
<get-craft-information>
show chassis environment
<get-environment-information>
show chassis environment cb
<get-environment-cb-information>
show chassis environment cip
<get-environment-cip-information>
show chassis environment feb
<get-environment-feb-information>
show chassis environment fan
show chassis environment fpc
<get-environment-fpc-information>
```

```
show chassis environment fpm
    <get-environment-fpm-information>
show chassis environment mcs
    <get-environment-mcs-information>
show chassis environment pcg
    <get-environment-pcg-information>
show chassis environment pdu
    <get-environment-pdu-information>
show chassis environment pem
    <get-environment-pem-information>
show chassis environment psm
show chassis environment psu
    <get-environment-psu-information>
show chassis environment routing-engine
    <get-environment-re-information>
show chassis environment scg
    <get-environment-scg-information>
show chassis environment service-node
    <get-environment-service-node-information>
show chassis environment sfb
show chassis environment sfm
    <get-environment-sfm-information>

show chassis environment sib
    <get-environment-sib-information>

show chassis environment sib f13
show chassis environment sib f2s
show chassis ethernet-switch
show chassis ethernet-switch errors
show chassis ethernet-switch statistics
show chassis ethernet-switch temperature
show chassis fabric
show chassis fabric degraded-fabric-reachability
show chassis fabric device
    <get-chassis-fabric-information-device>
show chassis fabric connectivity
    <get-chassis-fabric-connectivity-information>
show chassis fabric degradation
    <get-fm-degradation-information>
show chassis fabric degradation actions
    <get-fm-degradation-information-details>
show chassis fabric destinations
    <get-fm-fabric-destinations-state>
show chassis fabric errors
show chassis fabric errors autoheal
    <get-fm-plane-autoheal-errors>
show chassis fabric errors fpc
    <get-fm-fpc-errors>

show chassis fabric errors sib
    <get-fm-sib-errors>

show chassis fabric errors sib f13
show chassis fabric errors sib f2s
show chassis fabric feb
show chassis fabric fpcs
    <get-fm-fpc-state-information>

show chassis fabric links
    <get-chassis-fabric-link-information>
```

```
show chassis fabric map
show chassis fabric plane
    <get-fm-plane-state-information>

show chassis fabric plane-location
show chassis fabric reachability
    <get-fm-fabric-reachability-information>
show chassis fabric sibs
    <get-fm-sib-state-information>
show chassis fabric spray-weights
    <get-chassis-fabric-spray-weight-information>
show chassis fabric spray-weights from
show chassis fabric spray-weights to
show chassis fabric summary
    <get-fm-state-information>

show chassis fabric topology
    <get-chassis-fabric-topology-information>
show chassis fabric unreachable-destinations
    <get-fm-unreachable-dest-information>
show chassis fan
show chassis feb
    <get-feb-brief-information>

show chassis feb detail
    <get-feb-information>

show chassis firmware
    <get-firmware-information>

show chassis firmware detail
    <get-firmware-information-detail>
show chassis forwarding
    <get-fwdd-information>

show chassis fpc
    <get-fpc-information>

show chassis fpc errors
    <get-fpc-error-information>

show chassis fpc pic-status
    <get-pic-information>

show chassis fpc-feb-connectivity
    <get-fpc-feb-connectivity-information>

show chassis hardware
    <get-chassis-inventory>
show chassis hss
show chassis hss link-quality
show chassis in-service-upgrade
show chassis ioc-npc-connectivity
    <get-ioc-npc-connectivity-information>

show chassis lccs
    <get-fru-information>

show chassis location
    <get-chassis-location>
```

```
show chassis location fpc
show chassis location interface
show chassis location interface by-name
    <get-interface-location-name-information>

show chassis location interface by-slot
    <get-interface-location-information>
show chassis mac-addresses
show chassis multicast-loadbalance
<get-chassis-ae-lb-information>

show chassis network-services
    <network-services>

show chassis nonstop-upgrade
show chassis pic
    <get-pic-detail>

show chassis power
    <get-power-usage-information>

show chassis power detail
<get-power-usage-information-detail>
show chassis power sequence
show chassis power upgrade

show chassis power-ratings
    <get-power-management>

show chassis psd
    <get-psd-information>

show chassis redundancy
show chassis redundancy feb
    <get-feb-redundancy-information>

show chassis redundancy feb errors
    <get-feb-redundancy-error-information>

show chassis redundancy feb redundancy-group
    <get-feb-redundancy-group-information>

show chassis redundant-power-system
    <get-rps-chassis-information>

show chassis routing-engine
    <get-route-engine-information>

show chassis routing-engine bios
    <get-bios-version-information>
show chassis scb
    <get-scb-information>

show chassis service-node
    <get-service-node-information>

show chassis sfm
    <get-sfm-information>

show chassis sfm detail
show chassis sibs
```

```
<get-sib-information>

show chassis spmb
  <get-spmb-information>

show chassis spmb sibs
  <get-spmb-sib-information>

show chassis ssb
  <get-ssb-information>

show chassis synchronization
  <get-clock-synchronization-information>

show chassis synchronization backup
show chassis synchronization master
show chassis system-mode
  <get-system-mode-information>
show chassis temperature-thresholds
  <get-temperature-threshold-information>
show chassis vcpu
show chassis zones
  <get-chassis-zones-information>
show class-of-service
  <get-cos-information>

show class-of-service adaptive-shaper
  <get-cos-adaptive-shaper-information>

show class-of-service application-traffic-control
show class-of-service application-traffic-control counter
show class-of-service application-traffic-control statistics
show class-of-service application-traffic-control statistics rate-limiter
show class-of-service application-traffic-control statistics rule
  <get-appqos-rule-statistics>
show class-of-service classifier
  <get-cos-classifier-information>

show class-of-service code-point-aliases
  <get-cos-code-point-map-information>

show class-of-service congestion-notification
  <get-cos-congestion-notification-information>
show class-of-service drop-profile
  <get-cos-drop-profile-information>

show class-of-service fabric
show class-of-service fabric scheduler-map
  <get-cos-fabric-scheduler-map-information>

show class-of-service fabric statistics
  <get-fabric-queue-information>

show class-of-service fabric statistics detail
  <get-fabric-queue-detailed-information>

show class-of-service forwarding-class
  <get-cos-forwarding-class-information>

show class-of-service forwarding-class-set
  <get-cos-forwarding-class-set-information>
```

```
show class-of-service forwarding-table
  <get-cos-table-information>

show class-of-service forwarding-table classifier
  <get-cos-classifier-table-information>

show class-of-service forwarding-table classifier mapping
  <get-cos-classifier-table-map-information>

show class-of-service forwarding-table drop-profile
  <get-cos-red-information>

show class-of-service forwarding-table fabric
show class-of-service forwarding-table fabric scheduler-map
  <get-cos-fwtab-fabric-scheduler-map-information>

show class-of-service forwarding-table forwarding-class-map
  <get-cos-forwarding-class-map-table-information>

show class-of-service forwarding-table forwarding-class-map mapping
  <get-cos-forwarding-class-map-interface-table-information>

show class-of-service forwarding-table loss-priority-map
  <get-cos-loss-priority-map-table-information>

show class-of-service forwarding-table loss-priority-map mapping
  <get-cos-loss-priority-map-table-binding-information>

show class-of-service forwarding-table loss-priority-rewrite
  <get-cos-loss-priority-rewrite-table-information>
show class-of-service forwarding-table loss-priority-rewrite mapping
  <get-cos-loss-priority-rewrite-table-binding-information>
show class-of-service forwarding-table policer
  <get-cos-policer-table-map-information>

show class-of-service forwarding-table rewrite-rule
  <get-cos-rewrite-table-information>

show class-of-service forwarding-table rewrite-rule mapping
  <get-cos-rewrite-table-map-information>

show class-of-service forwarding-table scheduler-map
  <get-cos-scheduler-map-table-information>

show class-of-service forwarding-table shaper
  <get-cos-shaper-table-map-information>

show class-of-service forwarding-table translation-table
  <get-cos-translation-table-information>

show class-of-service forwarding-table translation-table mapping
  <get-cos-translation-table-mapping-information>

show class-of-service fragmentation-map
  <get-cos-fragmentation-map-information>

show class-of-service interface
  <get-cos-interface-map-information>

show class-of-service interface-set
  <get-cos-interface-set-map-information>
```

```
show class-of-service l2tp-session
  <get-cos-l2tp-session-map-information>

show class-of-service loss-priority-map
  <get-cos-loss-priority-map-information>

show class-of-service loss-priority-rewrite
  <get-cos-loss-priority-rewrite-information>
show class-of-service multi-destination
  <get-cos-multi-destination-information>

show class-of-service packet-buffer
  <get-cos-packet-buffer-information>
show class-of-service packet-buffer usage
  <get-cos-packet-buffer-usage-information>

show class-of-service rewrite-rule
  <get-cos-rewrite-information>

show class-of-service routing-instance
  <get-cos-routing-instance-map-information>

show class-of-service scheduler-hierarchy
show class-of-service scheduler-hierarchy interface
  <get-interface-scheduler-hierarchy-information>

show class-of-service scheduler-hierarchy interface-set
  <get-interface-set-scheduler-hierarchy-information>

show class-of-service scheduler-map
  <get-cos-scheduler-map-information>

show class-of-service traffic-control-profile
  <get-cos-traffic-control-profile-information>

show class-of-service translation-table
  <get-cos-translation-table-map-information>

show class-of-service virtual-channel
  <get-cos-virtual-channel-information>

show class-of-service virtual-channel-group
  <get-cos-virtual-channel-group-information>

show cli
show cli authorization
  <get-authorization-information>

show cli directory
  <get-current-working-directory>
show cli history
show configuration
show connections
  <get-ccc-information>
show database-replication
show database-replication statistics
  <get-database-replication-statistics-information>

show database-replication summary
  <get-database-replication-summary-information>
```

```
show ddos-protection
show ddos-protection protocols
  <get-ddos-protocols-information>
show ddos-protection protocols amtv4
show ddos-protection protocols amtv4 aggregate
show ddos-protection protocols amtv4 aggregate culprit-flows
show ddos-protection protocols amtv4 culprit-flows
show ddos-protection protocols amtv4 flow-detection
show ddos-protection protocols amtv4 parameters
show ddos-protection protocols amtv4 statistics
show ddos-protection protocols amtv4 violations
show ddos-protection protocols amtv6
show ddos-protection protocols amtv6 aggregate
show ddos-protection protocols amtv6 aggregate culprit-flows
show ddos-protection protocols amtv6 culprit-flows
show ddos-protection protocols amtv6 flow-detection
show ddos-protection protocols amtv6 statistics
show ddos-protection protocols amtv6 violations

show ddos-protection protocols ancp
  <get-ddos-ancp-information>

show ddos-protection protocols ancp aggregate
  <get-ddos-ancp-aggregate>
show ddos-protection protocols ancp parameters
  <get-ddos-ancp-parameters>

show ddos-protection protocols ancp statistics
  <get-ddos-ancp-statistics>
show ddos-protection protocols ancp violations
  <get-ddos-ancp-violations>
show ddos-protection protocols ancpv6
  <get-ddos-ancpv6-information>
show ddos-protection protocols ancpv6 aggregate
  get-ddos-ancpv6-aggregate
show ddos-protection protocols ancpv6 parameters
  get-ddos-ancpv6-parameters
show ddos-protection protocols ancpv6 statistics
  get-ddos-ancpv6-statistics
show ddos-protection protocols ancpv6 violations
  get-ddos-ancpv6-violations
show ddos-protection protocols arp
  get-ddos-arp-information
show ddos-protection protocols arp aggregate
  get-ddos-arp-aggregate
show ddos-protection protocols arp parameters
  get-ddos-arp-parameters
show ddos-protection protocols arp statistics
  get-ddos-arp-statistics
show ddos-protection protocols arp violations
  get-ddos-arp-violations
show ddos-protection protocols atm
  get-ddos-atm-information
show ddos-protection protocols atm aggregate
  get-ddos-atm-aggregate
show ddos-protection protocols atm parameters
  get-ddos-atm-parameters
show ddos-protection protocols atm statistics
  get-ddos-atm-statistics
show ddos-protection protocols atm violations
```

```

    get-ddos-atm-violations
show ddos-protection protocols bfd
    get-ddos-bfd-information
show ddos-protection protocols bfd aggregate
    get-ddos-bfd-aggregate
show ddos-protection protocols bfd parameters
    get-ddos-bfd-parameters
show ddos-protection protocols bfd statistics
    get-ddos-bfd-statistics
show ddos-protection protocols bfd violations
    get-ddos-bfd-violations
show ddos-protection protocols bfdv6
    get-ddos-bfdv6-information
show ddos-protection protocols bfdv6 aggregate
    get-ddos-bfdv6-aggregate
show ddos-protection protocols bfdv6 parameters
    get-ddos-bfdv6-parameters
show ddos-protection protocols bfdv6 statistics
    get-ddos-bfdv6-statistics
show ddos-protection protocols bfdv6 violations
    get-ddos-bfdv6-violations
show ddos-protection protocols bgp
    get-ddos-bgp-information
show ddos-protection protocols bgp aggregate
    get-ddos-bgp-aggregate
show ddos-protection protocols bgp parameters
    get-ddos-bgp-parameters
show ddos-protection protocols bgp statistics
    get-ddos-bgp-statistics
show ddos-protection protocols bgp violations
    get-ddos-bgp-violations
show ddos-protection protocols bgpv6
    get-ddos-bgpv6-information
show ddos-protection protocols bgpv6 aggregate
    get-ddos-bgpv6-aggregate
show ddos-protection protocols bgpv6 parameters
    get-ddos-bgpv6-parameters
show ddos-protection protocols bgpv6 statistics
    get-ddos-bgpv6-statistics
show ddos-protection protocols bgpv6 violations
    get-ddos-bgpv6-violations
show ddos-protection protocols demux-autosense
    get-ddos-demuxauto-information
show ddos-protection protocols demux-autosense aggregate
    get-ddos-demuxauto-aggregate
show ddos-protection protocols demux-autosense parameters
    get-ddos-demuxauto-parameters
show ddos-protection protocols demux-autosense statistics
    get-ddos-demuxauto-statistics
show ddos-protection protocols demux-autosense violations
    get-ddos-demuxauto-violations
show ddos-protection protocols dhcpv4
    get-ddos-dhcpv4-information
show ddos-protection protocols dhcpv4 ack
    get-ddos-dhcpv4-ack
show ddos-protection protocols dhcpv4 aggregate
    get-ddos-dhcpv4-aggregate
show ddos-protection protocols dhcpv4 bad-packets
    get-ddos-dhcpv4-bad-pack
show ddos-protection protocols dhcpv4 bootp
    get-ddos-dhcpv4-bootp

```

```
show ddos-protection protocols dhcpv4 decline
  get-ddos-dhcpv4-decline
show ddos-protection protocols dhcpv4 discover
  get-ddos-dhcpv4-discover
show ddos-protection protocols dhcpv4 force-renew
  get-ddos-dhcpv4-forcerenew
show ddos-protection protocols dhcpv4 inform
  get-ddos-dhcpv4-inform
show ddos-protection protocols dhcpv4 lease-active
  get-ddos-dhcpv4-leaseact
show ddos-protection protocols dhcpv4 lease-query
  get-ddos-dhcpv4-leasequery
show ddos-protection protocols dhcpv4 lease-unassigned
  get-ddos-dhcpv4-leaseuna
show ddos-protection protocols dhcpv4 lease-unknown
  get-ddos-dhcpv4-leaseunk
show ddos-protection protocols dhcpv4 nak
  get-ddos-dhcpv4-nak
show ddos-protection protocols dhcpv4 no-message-type
  get-ddos-dhcpv4-no-msgtype
show ddos-protection protocols dhcpv4 offer
  get-ddos-dhcpv4-offer
show ddos-protection protocols dhcpv4 offer culprit-flows
show ddos-protection protocols dhcpv4 parameters
  get-ddos-dhcpv4-parameters
show ddos-protection protocols dhcpv4 release
  get-ddos-dhcpv4-release
show ddos-protection protocols dhcpv4 renew
  get-ddos-dhcpv4-renew
show ddos-protection protocols dhcpv4 request
  get-ddos-dhcpv4-request
show ddos-protection protocols dhcpv4 statistics
  get-ddos-dhcpv4-statistics
show ddos-protection protocols dhcpv4 unclassified
  get-ddos-dhcpv4-unclass
show ddos-protection protocols dhcpv4 violations
  get-ddos-dhcpv4-violations
show ddos-protection protocols dhcpv4v6
  <get-ddos-dhcpv4v6-information>
show ddos-protection protocols dhcpv4v6 aggregate
  <get-ddos-dhcpv4v6-aggregate>
show ddos-protection protocols dhcpv4v6 aggregate culprit-flows
  <get-ddos-dhcpv4v6-aggregate-flows>
show ddos-protection protocols dhcpv4v6 culprit-flows
  <get-ddos-dhcpv4v6-flows>
show ddos-protection protocols dhcpv4v6 flow-detection
  <get-ddos-dhcpv4v6-flow-parameters>
show ddos-protection protocols dhcpv4v6 parameters
  <get-ddos-dhcpv4v6-parameters>
show ddos-protection protocols dhcpv4v6 statistics
  <get-ddos-dhcpv4v6-statistics>
show ddos-protection protocols dhcpv4v6 violations
  <get-ddos-dhcpv4v6-violations>
show ddos-protection protocols dhcpv6
  get-ddos-dhcpv6-information
show ddos-protection protocols dhcpv6 advertise
  get-ddos-dhcpv6-advertise
show ddos-protection protocols dhcpv6 advertise culprit-flows
show ddos-protection protocols dhcpv6 aggregate
  get-ddos-dhcpv6-aggregate
show ddos-protection protocols dhcpv6 confirm
```

```
get-ddos-dhcpv6-confirm
show ddos-protection protocols dhcpv6 decline
get-ddos-dhcpv6-decline
show ddos-protection protocols dhcpv6 information-request
get-ddos-dhcpv6-info-req
show ddos-protection protocols dhcpv6 leasequery
get-ddos-dhcpv6-leasequery
show ddos-protection protocols dhcpv6 leasequery culprit-flows
show ddos-protection protocols dhcpv6 leasequery-data
get-ddos-dhcpv6-leaseq-da
show ddos-protection protocols dhcpv6 leasequery-done
get-ddos-dhcpv6-leaseq-do
show ddos-protection protocols dhcpv6 leasequery-reply
get-ddos-dhcpv6-leaseq-re
show ddos-protection protocols dhcpv6 parameters
get-ddos-dhcpv6-parameters
show ddos-protection protocols dhcpv6 rebind
get-ddos-dhcpv6-rebind
show ddos-protection protocols dhcpv6 reconfigure
get-ddos-dhcpv6-reconfig
show ddos-protection protocols dhcpv6 relay-forward
get-ddos-dhcpv6-relay-for
show ddos-protection protocols dhcpv6 relay-reply
get-ddos-dhcpv6-relay-rep
show ddos-protection protocols dhcpv6 release
get-ddos-dhcpv6-release
show ddos-protection protocols dhcpv6 renew
get-ddos-dhcpv6-renew
show ddos-protection protocols dhcpv6 reply
get-ddos-dhcpv6-reply
show ddos-protection protocols dhcpv6 request
get-ddos-dhcpv6-request
show ddos-protection protocols dhcpv6 solicit
get-ddos-dhcpv6-solicit
show ddos-protection protocols dhcpv6 statistics
get-ddos-dhcpv6-statistics
show ddos-protection protocols dhcpv6 unclassified
get-ddos-dhcpv6-unclass
show ddos-protection protocols dhcpv6 unclassified culprit-flows
show ddos-protection protocols dhcpv6 violations
get-ddos-dhcpv6-violations
show ddos-protection protocols diameter
get-ddos-diameter-information
show ddos-protection protocols diameter aggregate
get-ddos-diameter-aggregate
show ddos-protection protocols diameter parameters
get-ddos-diameter-parameters
show ddos-protection protocols diameter statistics
get-ddos-diameter-statistics
show ddos-protection protocols diameter violations
get-ddos-diameter-violations
show ddos-protection protocols dns
get-ddos-dns-information
show ddos-protection protocols dns aggregate
get-ddos-dns-aggregate
show ddos-protection protocols dns parameters
get-ddos-dns-parameters
show ddos-protection protocols dns statistics
get-ddos-dns-statistics
show ddos-protection protocols dns violations
get-ddos-dns-violations
```

```
show ddos-protection protocols dtcp
  get-ddos-dtcp-information
show ddos-protection protocols dtcp aggregate
  get-ddos-dtcp-aggregate
show ddos-protection protocols dtcp aggregate culprit-flows
show ddos-protection protocols dtcp parameters
  get-ddos-dtcp-parameters
show ddos-protection protocols dtcp statistics
  get-ddos-dtcp-statistics
show ddos-protection protocols dtcp violations
  get-ddos-dtcp-violations
show ddos-protection protocols dynamic-vlan
  get-ddos-dynvlan-information
show ddos-protection protocols dynamic-vlan aggregate
  get-ddos-dynvlan-aggregate
show ddos-protection protocols dynamic-vlan parameters
  get-ddos-dynvlan-parameters
show ddos-protection protocols dynamic-vlan statistics
  get-ddos-dynvlan-statistics
show ddos-protection protocols dynamic-vlan violations
  get-ddos-dynvlan-violations
show ddos-protection protocols egpv6
  get-ddos-egpv6-information
show ddos-protection protocols egpv6 aggregate
  get-ddos-egpv6-aggregate
show ddos-protection protocols egpv6 parameters
  get-ddos-egpv6-parameters
show ddos-protection protocols egpv6 statistics
  get-ddos-egpv6-statistics
show ddos-protection protocols egpv6 violations
  get-ddos-egpv6-violations
show ddos-protection protocols eoam
  get-ddos-eoam-information
show ddos-protection protocols eoam aggregate
  get-ddos-eoam-aggregate
show ddos-protection protocols eoam parameters
  get-ddos-eoam-parameters
show ddos-protection protocols eoam statistics
  get-ddos-eoam-statistics
show ddos-protection protocols eoam violations
  get-ddos-eoam-violations
show ddos-protection protocols esmc
  get-ddos-esmc-information
show ddos-protection protocols esmc aggregate
  get-ddos-esmc-aggregate
show ddos-protection protocols esmc parameters
  get-ddos-esmc-parameters
show ddos-protection protocols esmc statistics
  get-ddos-esmc-statistics
show ddos-protection protocols esmc violations
  get-ddos-esmc-violations
show ddos-protection protocols fab-probe
<get-ddos-fab-probe-information>
show ddos-protection protocols fab-probe aggregate
<get-ddos-fab-probe-aggregate>
show ddos-protection protocols fab-probe parameters
<get-ddos-fab-probe-parameters>
show ddos-protection protocols fab-probe statistics
<get-ddos-fab-probe-statistics>
show ddos-protection protocols fab-probe violations
<get-ddos-fab-probe-violations>
```

```

show ddos-protection protocols firewall-host
  get-ddos-fw-host-information
show ddos-protection protocols firewall-host aggregate
  get-ddos-fw-host-aggregate
show ddos-protection protocols firewall-host parameters
  get-ddos-fw-host-parameters
show ddos-protection protocols firewall-host statistics
  get-ddos-fw-host-statistics
show ddos-protection protocols firewall-host violations
  get-ddos-fw-host-violations

show ddos-protection protocols ftp
  get-ddos-ftp-information
show ddos-protection protocols ftp aggregate
  get-ddos-ftp-aggregate
show ddos-protection protocols ftp parameters
  get-ddos-ftp-parameters
show ddos-protection protocols ftp statistics
  get-ddos-ftp-statistics
show ddos-protection protocols ftp violations
  get-ddos-ftp-violations
show ddos-protection protocols ftpv6
  get-ddos-ftp6-information
show ddos-protection protocols ftpv6 aggregate
  get-ddos-ftp6-aggregate
show ddos-protection protocols ftpv6 parameters
  get-ddos-ftp6-parameters
show ddos-protection protocols ftpv6 statistics
  get-ddos-ftp6-statistics
show ddos-protection protocols ftpv6 violations
  get-ddos-ftp6-violations
show ddos-protection protocols garp-reply
  <get-ddos-garp-reply-information>
show ddos-protection protocols garp-reply aggregate
  <get-ddos-garp-reply-aggregate>
show ddos-protection protocols garp-reply aggregate culprit-flows
  <get-ddos-garp-reply-aggregate-flows>
show ddos-protection protocols garp-reply culprit-flows
  <get-ddos-garp-reply-flows>
show ddos-protection protocols garp-reply flow-detection
  <get-ddos-garp-reply-flow-parameters>
show ddos-protection protocols garp-reply parameters
  <get-ddos-garp-reply-parameters>
show ddos-protection protocols garp-reply statistics
  <get-ddos-garp-reply-statistics>
show ddos-protection protocols garp-reply violations
  <get-ddos-garp-reply-violations>
show ddos-protection protocols gre
  get-ddos-gre-information
show ddos-protection protocols gre aggregate
  get-ddos-gre-aggregate
show ddos-protection protocols gre hbc
  <get-ddos-gre-hbc>
show ddos-protection protocols gre hbc culprit-flows
  <get-ddos-gre-hbc-flows>
show ddos-protection protocols gre parameters
  get-ddos-gre-parameters
show ddos-protection protocols gre punt
  <get-ddos-gre-punt>
show ddos-protection protocols gre punt culprit-flows

```

```
<get-ddos-gre-punt-flows>
show ddos-protection protocols gre statistics
  get-ddos-gre-statistics
show ddos-protection protocols gre violations
  get-ddos-gre-violations
show ddos-protection protocols icmp
  get-ddos-icmp-information
show ddos-protection protocols icmp aggregate
  get-ddos-icmp-aggregate
show ddos-protection protocols icmp parameters
  get-ddos-icmp-parameters
show ddos-protection protocols icmp statistics
  get-ddos-icmp-statistics
show ddos-protection protocols icmp violations
  get-ddos-icmp-violations
show ddos-protection protocols icmpv6
<get-ddos-icmpv6-information>
show ddos-protection protocols icmpv6 aggregate
<get-ddos-icmpv6-aggregate>
show ddos-protection protocols icmpv6 aggregate culprit-flows
<get-ddos-icmpv6-aggregate-flows>
show ddos-protection protocols icmpv6 parameters
<get-ddos-icmpv6-parameters>
show ddos-protection protocols icmpv6 statistics
<get-ddos-icmpv6-statistics>
show ddos-protection protocols icmpv6 violations
<get-ddos-icmpv6-violations>
show ddos-protection protocols igmp
  get-ddos-igmp-information
show ddos-protection protocols igmp aggregate
  get-ddos-igmp-aggregate
show ddos-protection protocols igmp aggregate culprit-flows
show ddos-protection protocols igmp parameters
  get-ddos-igmp-parameters
show ddos-protection protocols igmp statistics
  get-ddos-igmp-statistics
show ddos-protection protocols igmp violations
  get-ddos-igmp-violations
show ddos-protection protocols igmp-snoop
  get-ddos-igmp-snoop-information
show ddos-protection protocols igmp-snoop aggregate
  get-ddos-igmp-snoop-aggregate
show ddos-protection protocols igmp-snoop parameters
  get-ddos-igmp-snoop-parameters
show ddos-protection protocols igmp-snoop statistics
  get-ddos-igmp-snoop-statistics
show ddos-protection protocols igmp-snoop violations
  get-ddos-igmp-snoop-violations
show ddos-protection protocols igmpv4v6
  get-ddos-igmpv4v6-information
show ddos-protection protocols igmpv4v6 aggregate
  get-ddos-igmpv4v6-aggregate
show ddos-protection protocols igmpv4v6 aggregate culprit-flows
show ddos-protection protocols igmpv4v6 parameters
  get-ddos-igmpv4v6-parameters
show ddos-protection protocols igmpv4v6 statistics
  get-ddos-igmpv4v6-statistics
show ddos-protection protocols igmpv4v6 violations
  get-ddos-igmpv4v6-violations
show ddos-protection protocols igmpv6
  get-ddos-igmpv6-information
```

```

show ddos-protection protocols igmpv6 aggregate
  get-ddos-igmpv6-aggregate
show ddos-protection protocols igmpv6 parameters
  get-ddos-igmpv6-parameters
show ddos-protection protocols igmpv6 statistics
  get-ddos-igmpv6-statistics
show ddos-protection protocols igmpv6 violations
  get-ddos-igmpv6-violations
show ddos-protection protocols ip-fragments
  get-ddos-ip-frag-information
show ddos-protection protocols ip-fragments aggregate
  get-ddos-ip-frag-aggregate
show ddos-protection protocols ip-fragments first-fragment
  get-ddos-ip-frag-first-frag
show ddos-protection protocols ip-fragments parameters
  get-ddos-ip-frag-parameters
show ddos-protection protocols ip-fragments statistics
  get-ddos-ip-frag-statistics
show ddos-protection protocols ip-fragments trail-fragment
  get-ddos-ip-frag-trail-frag
show ddos-protection protocols ip-fragments violations
  get-ddos-ip-frag-violations
show ddos-protection protocols ip-options
  get-ddos-ip-opt-information
show ddos-protection protocols ip-options aggregate
  get-ddos-ip-opt-aggregate
show ddos-protection protocols ip-options non-v4v6
  <get-ddos-ip-opt-non-v4v6>
show ddos-protection protocols ip-options parameters
  get-ddos-ip-opt-parameters
show ddos-protection protocols ip-options router-alert
  get-ddos-ip-opt-rt-alert
show ddos-protection protocols ip-options statistics
  get-ddos-ip-opt-statistics
show ddos-protection protocols ip-options unclassified
  get-ddos-ip-opt-unclass
show ddos-protection protocols ipmc-reserved culprit-flows
  <get-ddos-ipmc-reserved-flows>
show ddos-protection protocols ipmc-reserved flow-detection
  <get-ddos-ipmc-reserved-flow-parameters>
show ddos-protection protocols ipmc-reserved parameters
  <get-ddos-ipmc-reserved-parameters>
show ddos-protection protocols ipmc-reserved statistics
  <get-ddos-ipmc-reserved-statistics>
show ddos-protection protocols ipmc-reserved violations
  <get-ddos-ipmc-reserved-violations>
show ddos-protection protocols ipmcast-miss
  <get-ddos-ipmcast-miss-information>
show ddos-protection protocols ipmcast-miss aggregate
  <get-ddos-ipmcast-miss-aggregate>
show ddos-protection protocols ipmcast-miss aggregate culprit-flows
  <get-ddos-ipmcast-miss-aggregate-flows>
show ddos-protection protocols ipmcast-miss culprit-flows
  <get-ddos-ipmcast-miss-flows>
show ddos-protection protocols ipmcast-miss flow-detection
  <get-ddos-ipmcast-miss-flow-parameters>
show ddos-protection protocols ipmcast-miss parameters
  <get-ddos-ipmcast-miss-parameters>
show ddos-protection protocols ipmcast-miss statistics
  <get-ddos-ipmcast-miss-statistics>
show ddos-protection protocols ipmcast-miss violations

```

```
<get-ddos-ipmcast-miss-violations>
show ddos-protection protocols ip-options violations
  get-ddos-ip-opt-violations
show ddos-protection protocols ipv4-unclassified
  get-ddos-ipv4-uncls-information
show ddos-protection protocols ipv4-unclassified aggregate
  get-ddos-ipv4-uncls-aggregate
show ddos-protection protocols ipv4-unclassified parameters
  get-ddos-ipv4-uncls-parameters
show ddos-protection protocols ipv4-unclassified statistics
  get-ddos-ipv4-uncls-statistics
show ddos-protection protocols ipv4-unclassified violations
  get-ddos-ipv4-uncls-violations
show ddos-protection protocols ipv6-unclassified
  get-ddos-ipv6-uncls-information
show ddos-protection protocols ipv6-unclassified aggregate
  get-ddos-ipv6-uncls-aggregate
show ddos-protection protocols ipv6-unclassified parameters
  get-ddos-ipv6-uncls-parameters
show ddos-protection protocols ipv6-unclassified statistics
  get-ddos-ipv6-uncls-statistics
show ddos-protection protocols ipv6-unclassified violations
  get-ddos-ipv6-uncls-violations
show ddos-protection protocols isis
  get-ddos-isis-information
show ddos-protection protocols isis aggregate
  get-ddos-isis-aggregate
show ddos-protection protocols isis parameters
  get-ddos-isis-parameters
show ddos-protection protocols isis statistics
  get-ddos-isis-statistics
show ddos-protection protocols isis violations
  get-ddos-isis-violations
show ddos-protection protocols jfm
  get-ddos-jfm-information
show ddos-protection protocols jfm aggregate
  get-ddos-jfm-aggregate
show ddos-protection protocols jfm parameters
  get-ddos-jfm-parameters
show ddos-protection protocols jfm statistics
  get-ddos-jfm-statistics
show ddos-protection protocols jfm violations
  get-ddos-jfm-violations
show ddos-protection protocols l2tp
  get-ddos-l2tp-information
show ddos-protection protocols l2tp aggregate
  get-ddos-l2tp-aggregate
show ddos-protection protocols l2tp parameters
  get-ddos-l2tp-parameters
show ddos-protection protocols l2tp statistics
  get-ddos-l2tp-statistics
show ddos-protection protocols l2tp violations
  get-ddos-l2tp-violations
show ddos-protection protocols l3dest-miss
  <get-ddos-l3dest-miss-information>
show ddos-protection protocols l3dest-miss aggregate
  <get-ddos-l3dest-miss-aggregate>
show ddos-protection protocols l3dest-miss aggregate culprit-flows
  <get-ddos-l3dest-miss-aggregate-flows>
show ddos-protection protocols l3dest-miss culprit-flows
  <get-ddos-l3dest-miss-flows>
```

```
show ddos-protection protocols l3dest-miss flow-detection
  <get-ddos-l3dest-miss-flow-parameters>
show ddos-protection protocols l3dest-miss parameters
  <get-ddos-l3dest-miss-parameters>
show ddos-protection protocols l3dest-miss statistics
  <get-ddos-l3dest-miss-statistics>
show ddos-protection protocols l3dest-miss violations
  <get-ddos-l3dest-miss-violations>
show ddos-protection protocols l3mc-sgv-hit-icl
  <get-ddos-l3mc-sgv-hit-icl-information>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate
  <get-ddos-l3mc-sgv-hit-icl-aggregate>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
  <get-ddos-l3mc-sgv-hit-icl-aggregate-flows>
show ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
  <get-ddos-l3mc-sgv-hit-icl-flows>
show ddos-protection protocols l3mc-sgv-hit-icl flow-detection
  <get-ddos-l3mc-sgv-hit-icl-flow-parameters>
show ddos-protection protocols l3mc-sgv-hit-icl parameters
  <get-ddos-l3mc-sgv-hit-icl-parameters>
show ddos-protection protocols l3mc-sgv-hit-icl statistics
  <get-ddos-l3mc-sgv-hit-icl-statistics>
show ddos-protection protocols l3mc-sgv-hit-icl violations
  <get-ddos-l3mc-sgv-hit-icl-violations>
show ddos-protection protocols l3mtu-fail
  <get-ddos-l3mtu-fail-information>
show ddos-protection protocols l3mtu-fail aggregate
  <get-ddos-l3mtu-fail-aggregate>
show ddos-protection protocols l3mtu-fail aggregate culprit-flows
  <get-ddos-l3mtu-fail-aggregate-flows>
show ddos-protection protocols l3mtu-fail culprit-flows
  <get-ddos-l3mtu-fail-flows>
show ddos-protection protocols l3mtu-fail flow-detection
  <get-ddos-l3mtu-fail-flow-parameters>
show ddos-protection protocols l3mtu-fail parameters
  <get-ddos-l3mtu-fail-parameters>
show ddos-protection protocols l3mtu-fail statistics
  <get-ddos-l3mtu-fail-statistics>
show ddos-protection protocols l3mtu-fail violations
  <get-ddos-l3mtu-fail-violations>
show ddos-protection protocols l3nhop
  <get-ddos-l3nhop-information>
show ddos-protection protocols l3nhop aggregate
  <get-ddos-l3nhop-aggregate>
show ddos-protection protocols l3nhop aggregate culprit-flows
  <get-ddos-l3nhop-aggregate-flows>
show ddos-protection protocols l3nhop culprit-flows
  <get-ddos-l3nhop-flows>
show ddos-protection protocols l3nhop flow-detection
  <get-ddos-l3nhop-flow-parameters>
show ddos-protection protocols l3nhop parameters
  <get-ddos-l3nhop-parameters>
show ddos-protection protocols l3nhop statistics
  <get-ddos-l3nhop-statistics>
show ddos-protection protocols l3nhop violations
  <get-ddos-l3nhop-violations>
show ddos-protection protocols lacp
  <get-ddos-lacp-information>
show ddos-protection protocols lacp aggregate
  <get-ddos-lacp-aggregate>
show ddos-protection protocols lacp parameters
```

```
<get-ddos-lacp-parameters>
show ddos-protection protocols lacp statistics
<get-ddos-lacp-statistics>
show ddos-protection protocols lacp violations
<get-ddos-lacp-violations>
show ddos-protection protocols ldp
<get-ddos-ldp-information>
show ddos-protection protocols ldp aggregate
<get-ddos-ldp-aggregate>
show ddos-protection protocols ldp parameters
<get-ddos-ldp-parameters>
show ddos-protection protocols ldp statistics
<get-ddos-ldp-statistics>
show ddos-protection protocols ldp violations
<get-ddos-ldp-violations>
show ddos-protection protocols ldpv6
<get-ddos-ldpv6-information>
show ddos-protection protocols ldpv6 aggregate
<get-ddos-ldpv6-aggregate>
show ddos-protection protocols ldpv6 parameters
<get-ddos-ldpv6-parameters>
show ddos-protection protocols ldpv6 statistics
<get-ddos-ldpv6-statistics>
show ddos-protection protocols ldpv6 violations
<get-ddos-ldpv6-violations>
show ddos-protection protocols lldp
<get-ddos-lldp-information>
show ddos-protection protocols lldp aggregate
<get-ddos-lldp-aggregate>
show ddos-protection protocols lldp parameters
<get-ddos-lldp-parameters>
show ddos-protection protocols lldp statistics
<get-ddos-lldp-statistics>
show ddos-protection protocols lldp violations
<get-ddos-lldp-violations>
show ddos-protection protocols lmp
<get-ddos-lmp-information>
show ddos-protection protocols lmp aggregate
<get-ddos-lmp-aggregate>
show ddos-protection protocols lmp parameters
<get-ddos-lmp-parameters>
show ddos-protection protocols lmp statistics
<get-ddos-lmp-statistics>
show ddos-protection protocols lmp violations
<get-ddos-lmp-violations>
show ddos-protection protocols lmpv6
<get-ddos-lmpv6-information>
show ddos-protection protocols lmpv6 aggregate
<get-ddos-lmpv6-aggregate>
show ddos-protection protocols lmpv6 parameters
<get-ddos-lmpv6-parameters>
show ddos-protection protocols lmpv6 statistics
<get-ddos-lmpv6-statistics>
show ddos-protection protocols lmpv6 violations
<get-ddos-lmpv6-violations>
show ddos-protection protocols localnh
  <get-ddos-localnh-information>
show ddos-protection protocols localnh aggregate
  <get-ddos-localnh-aggregate>
show ddos-protection protocols localnh aggregate culprit-flows
  <get-ddos-localnh-aggregate-flows>
```

```
show ddos-protection protocols localnh culprit-flows
  <get-ddos-localnh-flows>
show ddos-protection protocols localnh flow-detection
  <get-ddos-localnh-flow-parameters>
show ddos-protection protocols localnh parameters
  <get-ddos-localnh-parameters>
show ddos-protection protocols localnh statistics
  <get-ddos-localnh-statistics>
show ddos-protection protocols localnh violations
  <get-ddos-localnh-violations>
show ddos-protection protocols mac-host
  <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
  <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host aggregate culprit-flows
  <get-ddos-mac-host-aggregate-flows>
show ddos-protection protocols mac-host culprit-flows
  <get-ddos-mac-host-flows>
show ddos-protection protocols mac-host flow-detection
  <get-ddos-mac-host-flow-parameters>
show ddos-protection protocols mac-host parameters
  <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
  <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
  <get-ddos-mac-host-violations>
show ddos-protection protocols martian-address
  <get-ddos-martian-address-information>
show ddos-protection protocols martian-address aggregate
  <get-ddos-martian-address-aggregate>
show ddos-protection protocols martian-address aggregate culprit-flows
  <get-ddos-martian-address-aggregate-flows>
show ddos-protection protocols martian-address culprit-flows
  <get-ddos-martian-address-flows>
show ddos-protection protocols martian-address flow-detection
  <get-ddos-martian-address-flow-parameters>
show ddos-protection protocols martian-address parameters
  <get-ddos-martian-address-parameters>
show ddos-protection protocols martian-address statistics
  <get-ddos-martian-address-statistics>
show ddos-protection protocols martian-address violations
  <get-ddos-martian-address-violations>
show ddos-protection protocols mac-host
  <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
  <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host parameters
  <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
  <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
  <get-ddos-mac-host-violations>
show ddos-protection protocols mlp
  <get-ddos-mlp-information>
show ddos-protection protocols mlp add
  <get-ddos-mlp-add>
show ddos-protection protocols mlp add culprit-flows
  <get-ddos-mlp-add-flows>
show ddos-protection protocols mlp aggregate
  <get-ddos-mlp-aggregate>
show ddos-protection protocols mlp aging-exception
```

```
<get-ddos-mlp-aging-exc>
show ddos-protection protocols mlp packets
<get-ddos-mlp-packets>
show ddos-protection protocols mlp parameters
get-ddos-mlp-parameters
show ddos-protection protocols mlp statistics
<get-ddos-mlp-statistics>
show ddos-protection protocols mlp unclassified
<get-ddos-mlp-unclass>
show ddos-protection protocols mlp violations
<get-ddos-mlp-violations>
show ddos-protection protocols msdp
<get-ddos-msdp-information>
show ddos-protection protocols msdp aggregate
<get-ddos-msdp-aggregate>
show ddos-protection protocols msdp parameters
<get-ddos-msdp-parameters>
show ddos-protection protocols msdp statistics
<get-ddos-msdp-statistics>
show ddos-protection protocols msdp violations
<get-ddos-msdp-violations>
show ddos-protection protocols msdpv6
<get-ddos-msdpv6-information>
show ddos-protection protocols msdpv6 aggregate
<get-ddos-msdpv6-aggregate>
show ddos-protection protocols msdpv6 parameters
<get-ddos-msdpv6-parameters>
show ddos-protection protocols msdpv6 statistics
<get-ddos-msdpv6-statistics>
show ddos-protection protocols msdpv6 violations
<get-ddos-msdpv6-violations>
show ddos-protection protocols multicast-copy
<get-ddos-mcast-copy-information>
show ddos-protection protocols multicast-copy aggregate
<get-ddos-mcast-copy-aggregate>
show ddos-protection protocols multicast-copy parameters
<get-ddos-mcast-copy-parameters>
show ddos-protection protocols multicast-copy statistics
<get-ddos-mcast-copy-statistics>
show ddos-protection protocols multicast-copy violations
<get-ddos-mcast-copy-violations>
show ddos-protection protocols mvrp
<get-ddos-mvrp-information>
show ddos-protection protocols mvrp aggregate
<get-ddos-mvrp-aggregate>
show ddos-protection protocols mvrp parameters
<get-ddos-mvrp-parameters>
show ddos-protection protocols mvrp statistics
<get-ddos-mvrp-statistics>
show ddos-protection protocols mvrp violations
<get-ddos-mvrp-violations>
show ddos-protection protocols nonucast-switch
<get-ddos-nonucast-switch-information>
show ddos-protection protocols nonucast-switch aggregate
<get-ddos-nonucast-switch-aggregate>
show ddos-protection protocols nonucast-switch aggregate culprit-flows
<get-ddos-nonucast-switch-aggregate-flows>
show ddos-protection protocols nonucast-switch culprit-flows
<get-ddos-nonucast-switch-flows>
show ddos-protection protocols nonucast-switch flow-detection
<get-ddos-nonucast-switch-flow-parameters>
```

```
show ddos-protection protocols nonucast-switch parameters
<get-ddos-nonucast-switch-parameters>
show ddos-protection protocols nonucast-switch statistics
<get-ddos-nonucast-switch-statistics>
show ddos-protection protocols nonucast-switch violations
<get-ddos-nonucast-switch-violations>
show ddos-protection protocols ntp
  get-ddos-ntp-information
show ddos-protection protocols ntp aggregate
  get-ddos-ntp-aggregate
show ddos-protection protocols ntp parameters
  get-ddos-ntp-parameters
show ddos-protection protocols ntp statistics
  get-ddos-ntp-statistics
show ddos-protection protocols ntp violations
  get-ddos-ntp-violations
show ddos-protection protocols oam-lfm
  get-ddos-oam-lfm-information
show ddos-protection protocols oam-lfm aggregate
  get-ddos-oam-lfm-aggregate
show ddos-protection protocols oam-lfm parameters
  get-ddos-oam-lfm-parameters
show ddos-protection protocols oam-lfm statistics
  get-ddos-oam-lfm-statistics
show ddos-protection protocols oam-lfm violations
  get-ddos-oam-lfm-violations
show ddos-protection protocols ospf
  get-ddos-ospf-information
show ddos-protection protocols ospf aggregate
  get-ddos-ospf-aggregate
show ddos-protection protocols ospf parameters
  get-ddos-ospf-parameters
show ddos-protection protocols ospf statistics
  get-ddos-ospf-statistics
show ddos-protection protocols ospf violations
  get-ddos-ospf-violations
show ddos-protection protocols ospf-hello
<get-ddos-ospf-hello-information>
show ddos-protection protocols ospf-hello aggregate
<get-ddos-ospf-hello-aggregate>
show ddos-protection protocols ospf-hello aggregate culprit-flows
<get-ddos-ospf-hello-aggregate-flows>
show ddos-protection protocols ospf-hello culprit-flows
<get-ddos-ospf-hello-flows>
show ddos-protection protocols ospf-hello flow-detection
<get-ddos-ospf-hello-flow-parameters>
show ddos-protection protocols ospf-hello parameters
<get-ddos-ospf-hello-parameters>
show ddos-protection protocols ospf-hello statistics
<get-ddos-ospf-hello-statistics>
show ddos-protection protocols ospf-hello violations
<get-ddos-ospf-hello-violations>
show ddos-protection protocols ospfv3v6
  get-ddos-ospfv3v6-information
show ddos-protection protocols ospfv3v6 aggregate
  get-ddos-ospfv3v6-aggregate
show ddos-protection protocols ospfv3v6 parameters
  get-ddos-ospfv3v6-parameters
show ddos-protection protocols ospfv3v6 statistics
  get-ddos-ospfv3v6-statistics
show ddos-protection protocols ospfv3v6 violations
```

```
get-ddos-ospfv3v6-violations
show ddos-protection protocols parameters
get-ddos-protocols-parameters
show ddos-protection protocols pfe-alive
get-ddos-pfe-alive-information
show ddos-protection protocols pfe-alive aggregate
get-ddos-pfe-alive-aggregate
show ddos-protection protocols pfe-alive parameters
get-ddos-pfe-alive-parameters
show ddos-protection protocols pfe-alive statistics
get-ddos-pfe-alive-statistics
show ddos-protection protocols pfe-alive violations
get-ddos-pfe-alive-violations
show ddos-protection protocols pim
get-ddos-pim-information
show ddos-protection protocols pim aggregate
get-ddos-pim-aggregate
show ddos-protection protocols pim aggregate culprit-flows
show ddos-protection protocols pim parameters
get-ddos-pim-parameters
show ddos-protection protocols pim statistics
get-ddos-pim-statistics
show ddos-protection protocols pim violations
get-ddos-pim-violations
show ddos-protection protocols pim-ctrl
  <get-ddos-pim-ctrl-information>
show ddos-protection protocols pim-ctrl aggregate
  <get-ddos-pim-ctrl-aggregate>
show ddos-protection protocols pim-ctrl aggregate culprit-flows
  <get-ddos-pim-ctrl-aggregate-flows>
show ddos-protection protocols pim-ctrl culprit-flows
  <get-ddos-pim-ctrl-flows>
show ddos-protection protocols pim-ctrl flow-detection
  <get-ddos-pim-ctrl-flow-parameters>
show ddos-protection protocols pim-ctrl parameters
  <get-ddos-pim-ctrl-parameters>
show ddos-protection protocols pim-ctrl statistics
  <get-ddos-pim-ctrl-statistics>
show ddos-protection protocols pim-ctrl violations
  <get-ddos-pim-ctrl-violations>
show ddos-protection protocols pim-data
  <get-ddos-pim-data-information>
show ddos-protection protocols pim-data aggregate
  <get-ddos-pim-data-aggregate>
show ddos-protection protocols pim-data aggregate culprit-flows
  <get-ddos-pim-data-aggregate-flows>
show ddos-protection protocols pim-data culprit-flows
  <get-ddos-pim-data-flows>
show ddos-protection protocols pim-data flow-detection
  <get-ddos-pim-data-flow-parameters>
show ddos-protection protocols pim-data parameters
  <get-ddos-pim-data-parameters>
show ddos-protection protocols pim-data statistics
  <get-ddos-pim-data-statistics>
show ddos-protection protocols pim-data violations
  <get-ddos-pim-data-violations>
show ddos-protection protocols pimv6
  <get-ddos-pimv6-information>
show ddos-protection protocols pimv6 aggregate
  <get-ddos-pimv6-aggregate>
show ddos-protection protocols pimv6 aggregate culprit-flows
```

```

show ddos-protection protocols pimv6 parameters
  <get-ddos-pimv6-parameters>
show ddos-protection protocols pimv6 statistics
  <get-ddos-pimv6-statistics>
show ddos-protection protocols pimv6 violations
  <get-ddos-pimv6-violations>

show ddos-protection protocols pmvrp
  get-ddos-pmvrp-information
show ddos-protection protocols pmvrp aggregate
  get-ddos-pmvrp-aggregate
show ddos-protection protocols pmvrp parameters
  get-ddos-pmvrp-parameters
show ddos-protection protocols pmvrp statistics
  get-ddos-pmvrp-statistics
show ddos-protection protocols pmvrp violations
  get-ddos-pmvrp-violations
show ddos-protection protocols pos
  get-ddos-pos-information
show ddos-protection protocols pos aggregate
  get-ddos-pos-aggregate
show ddos-protection protocols pos aggregate culprit-flows
show ddos-protection protocols pos parameters
  get-ddos-pos-parameters
show ddos-protection protocols pos statistics
  get-ddos-pos-statistics
show ddos-protection protocols pos violations
  get-ddos-pos-violations
show ddos-protection protocols ppp
  get-ddos-ppp-information
show ddos-protection protocols ppp aggregate
  get-ddos-ppp-aggregate
show ddos-protection protocols ppp authentication
  get-ddos-ppp-auth
show ddos-protection protocols ppp authentication culprit-flows
show ddos-protection protocols ppp ipcp
  get-ddos-ppp-ipcp
show ddos-protection protocols ppp ipv6cp
  get-ddos-ppp-ipv6cp
show ddos-protection protocols ppp isis
  get-ddos-ppp-isis
show ddos-protection protocols ppp isis culprit-flows
show ddos-protection protocols ppp lcp
  get-ddos-ppp-lcp
show ddos-protection protocols ppp lcp culprit-flows
show ddos-protection protocols ppp mplsdp
  get-ddos-ppp-mplsdp
show ddos-protection protocols ppp mplsdp culprit-flows
show ddos-protection protocols ppp parameters
  get-ddos-ppp-parameters
show ddos-protection protocols ppp statistics
  get-ddos-ppp-statistics
show ddos-protection protocols ppp unclassified
  <get-ddos-ppp-unclass>
show ddos-protection protocols ppp violations
  get-ddos-ppp-violations
show ddos-protection protocols pppoe
  get-ddos-pppoe-information
show ddos-protection protocols pppoe aggregate
  get-ddos-pppoe-aggregate

```

```
show ddos-protection protocols pppoe padi
  get-ddos-pppoe-padi
show ddos-protection protocols pppoe padm
  get-ddos-pppoe-padm
show ddos-protection protocols pppoe padn
  get-ddos-pppoe-padn
show ddos-protection protocols pppoe pado
  get-ddos-pppoe-pado
show ddos-protection protocols pppoe padr
  get-ddos-pppoe-padr
show ddos-protection protocols pppoe pads
  get-ddos-pppoe-pads
show ddos-protection protocols pppoe padt
  get-ddos-pppoe-padt
show ddos-protection protocols pppoe parameters
  get-ddos-pppoe-parameters
show ddos-protection protocols pppoe statistics
  get-ddos-pppoe-statistics
show ddos-protection protocols pppoe violations
  get-ddos-pppoe-violations
show ddos-protection protocols ptp
  get-ddos-ntp-information
show ddos-protection protocols ptp aggregate
  get-ddos-ntp-aggregate
show ddos-protection protocols ptp aggregate culprit-flows
show ddos-protection protocols ptp parameters
  get-ddos-ntp-parameters
show ddos-protection protocols ptp statistics
  get-ddos-ntp-statistics
show ddos-protection protocols ptp violations
  get-ddos-ntp-violations
show ddos-protection protocols pvstp
  get-ddos-pvstp-information
show ddos-protection protocols pvstp aggregate
  get-ddos-pvstp-aggregate
show ddos-protection protocols pvstp parameters
  get-ddos-pvstp-parameters
show ddos-protection protocols pvstp statistics
  get-ddos-pvstp-statistics
show ddos-protection protocols pvstp violations
  get-ddos-pvstp-violations
show ddos-protection protocols radius
  get-ddos-radius-information
show ddos-protection protocols radius accounting
  get-ddos-radius-account
show ddos-protection protocols radius aggregate
  get-ddos-radius-aggregate
show ddos-protection protocols radius accounting culprit-flows
show ddos-protection protocols radius authorization
  get-ddos-radius-auth
show ddos-protection protocols radius parameters
  get-ddos-radius-parameters
show ddos-protection protocols radius server
  get-ddos-radius-server
show ddos-protection protocols radius statistics
  get-ddos-radius-statistics
show ddos-protection protocols radius violations
  get-ddos-radius-violations
show ddos-protection protocols re-services
  <get-ddos-re-services-information>
show ddos-protection protocols re-services aggregate
```

```

    <get-ddos-re-services-aggregate>
show ddos-protection protocols re-services aggregate culprit-flows
    <get-ddos-re-services-aggregate-flows>
show ddos-protection protocols re-services captive-portal
    <get-ddos-re-services-captive-portal>
show ddos-protection protocols re-services captive-portal culprit-flows
    <get-ddos-re-services-captive-portal-flows>
show ddos-protection protocols re-services culprit-flows
    <get-ddos-re-services-flows>
show ddos-protection protocols re-services flow-detection
    <get-ddos-re-services-flow-parameters>
show ddos-protection protocols re-services parameters
    <get-ddos-re-services-parameters>
show ddos-protection protocols re-services statistics
    <get-ddos-re-services-statistics>
show ddos-protection protocols re-services violations
    <get-ddos-re-services-violations>
show ddos-protection protocols re-services-v6
    <get-ddos-re-services-v6-information>
show ddos-protection protocols re-services-v6 aggregate
    <get-ddos-re-services-v6-aggregate>
show ddos-protection protocols re-services-v6 aggregate culprit-flows
    <get-ddos-re-services-v6-aggregate-flows>
show ddos-protection protocols re-services-v6 captive-portal
    <get-ddos-re-services-v6-captive-portal-v6>
show ddos-protection protocols re-services-v6 captive-portal culprit-flows
    <get-ddos-re-services-v6-captive-portal-v6-flows>
show ddos-protection protocols re-services-v6 culprit-flows
    <get-ddos-re-services-v6-flows>
show ddos-protection protocols re-services-v6 flow-detection
    <get-ddos-re-services-v6-flow-parameters>
show ddos-protection protocols re-services-v6 parameters
    <get-ddos-re-services-v6-parameters>
show ddos-protection protocols re-services-v6 statistics
    <get-ddos-re-services-v6-statistics>
show ddos-protection protocols re-services-v6 violations
    <get-ddos-re-services-v6-violations>
show ddos-protection protocols redirect
    get-ddos-redirect-information
show ddos-protection protocols redirect aggregate
    get-ddos-redirect-aggregate
show ddos-protection protocols redirect parameters
    get-ddos-redirect-parameters
show ddos-protection protocols redirect statistics
    get-ddos-redirect-statistics
show ddos-protection protocols redirect violations
    get-ddos-redirect-violations

show ddos-protection protocols reject
    <get-ddos-reject-information>
show ddos-protection protocols reject aggregate
    <get-ddos-reject-aggregate>
show ddos-protection protocols reject parameters
    <get-ddos-reject-parameters>
show ddos-protection protocols reject statistics
    <get-ddos-reject-statistics>
show ddos-protection protocols reject violations
    <get-ddos-reject-violations>
show ddos-protection protocols rejectv6show ddos-protection protocols rejectv6
aggregate

```

```
show ddos-protection protocols rejectv6 aggregate culprit-flows
show ddos-protection protocols rejectv6 flow-detection
show ddos-protection protocols rejectv6 parameters
show ddos-protection protocols rejectv6 statistics
show ddos-protection protocols rejectv6 violations
show ddos-protection protocols rip
    get-ddos-rip-information
show ddos-protection protocols rip aggregate
    get-ddos-rip-aggregate
show ddos-protection protocols rip aggregate culprit-flows
show ddos-protection protocols rip culprit-flows
show ddos-protection protocols rip parameters
    get-ddos-rip-parameters
show ddos-protection protocols rip statistics
    get-ddos-rip-statistics
show ddos-protection protocols rip violations
    get-ddos-rip-violations
show ddos-protection protocols ripv6
    get-ddos-ripv6-information
show ddos-protection protocols ripv6 aggregate
    get-ddos-ripv6-aggregate
show ddos-protection protocols ripv6 aggregate culprit-flows
show ddos-protection protocols ripv6 parameters
    get-ddos-ripv6-parameters
show ddos-protection protocols ripv6 statistics
    get-ddos-ripv6-statistics
show ddos-protection protocols ripv6 violations
    get-ddos-ripv6-violations
show ddos-protection protocols rsvp
    get-ddos-rsvp-information
show ddos-protection protocols rsvp aggregate
    get-ddos-rsvp-aggregate
show ddos-protection protocols rsvp aggregate culprit-flows
show ddos-protection protocols rsvp parameters
    get-ddos-rsvp-parameters
show ddos-protection protocols rsvp statistics
    get-ddos-rsvp-statistics
show ddos-protection protocols rsvp violations
    get-ddos-rsvp-violations
show ddos-protection protocols rsvpv6
    get-ddos-rsvpv6-information
show ddos-protection protocols rsvpv6 aggregate
    get-ddos-rsvpv6-aggregate
show ddos-protection protocols rsvpv6 aggregate culprit-flows
show ddos-protection protocols rsvpv6 parameters
    get-ddos-rsvpv6-parameters
show ddos-protection protocols rsvpv6 statistics
    get-ddos-rsvpv6-statistics
show ddos-protection protocols rsvpv6 violations
    get-ddos-rsvpv6-violations
show ddos-protection protocols sample
<get-ddos-sample-information>
show ddos-protection protocols sample aggregate
<get-ddos-sample-aggregate>
show ddos-protection protocols sample aggregate culprit-flows
show ddos-protection protocols sample host
<get-ddos-sample-host>
show ddos-protection protocols sample parameters
<get-ddos-sample-parameters>
show ddos-protection protocols sample pfe
<get-ddos-sample-pfe>
```

```
show ddos-protection protocols sample pfe culprit-flows
show ddos-protection protocols sample sflow
<get-ddos-sample-sflow>
show ddos-protection protocols sample sflow culprit-flows
<get-ddos-sample-sflow-flows>
show ddos-protection protocols sample statistics
<get-ddos-sample-statistics>
show ddos-protection protocols sample syslog
show ddos-protection protocols sample tap
<get-ddos-sample-tap>
show ddos-protection protocols sample tap culprit-flows
show ddos-protection protocols sample violations
<get-ddos-sample-violations>
show ddos-protection protocols services
    get-ddos-services-information
show ddos-protection protocols sample-dest
<get-ddos-sample-dest-information>
show ddos-protection protocols sample-dest aggregate
<get-ddos-sample-dest-aggregate>
show ddos-protection protocols sample-dest aggregate culprit-flows
<get-ddos-sample-dest-aggregate-flows>
show ddos-protection protocols sample-dest culprit-flows
<get-ddos-sample-dest-flows>
show ddos-protection protocols sample-dest flow-detection
<get-ddos-sample-dest-flow-parameters>
show ddos-protection protocols sample-dest parameters
<get-ddos-sample-dest-parameters>
show ddos-protection protocols sample-dest statistics
<get-ddos-sample-dest-statistics>
show ddos-protection protocols sample-dest violations
<get-ddos-sample-dest-violations>
show ddos-protection protocols sample-source
<get-ddos-sample-source-information>
show ddos-protection protocols sample-source aggregate
<get-ddos-sample-source-aggregate>
show ddos-protection protocols sample-source aggregate culprit-flows
<get-ddos-sample-source-aggregate-flows>
show ddos-protection protocols sample-source culprit-flows
<get-ddos-sample-source-flows>
show ddos-protection protocols sample-source flow-detection
<get-ddos-sample-source-flow-parameters>
show ddos-protection protocols sample-source parameters
<get-ddos-sample-source-parameters>
show ddos-protection protocols sample-source statistics
<get-ddos-sample-source-statistics>
show ddos-protection protocols sample-source violations
<get-ddos-sample-source-violations>
show ddos-protection protocols services aggregate
    <get-ddos-services-aggregate>
show ddos-protection protocols services parameters
    <get-ddos-services-parameters>
show ddos-protection protocols services statistics
    <get-ddos-services-statistics>
show ddos-protection protocols syslog
    <get-ddos-syslog-information>
show ddos-protection protocols syslog aggregate
    <get-ddos-syslog-aggregate>
show ddos-protection protocols syslog aggregate culprit-flows
    <get-ddos-syslog-aggregate-flows>
show ddos-protection protocols syslog culprit-flows
    <get-ddos-syslog-flows>
```

```
show ddos-protection protocols syslog flow-detection
    <get-ddos-syslog-flow-parameters>
show ddos-protection protocols syslog parameters
    <get-ddos-syslog-parameters>
show ddos-protection protocols syslog statistics
    <get-ddos-syslog-statistics>
show ddos-protection protocols syslog violations
    <get-ddos-syslog-violations>
show ddos-protection protocols services violations
    get-ddos-services-violations
show ddos-protection protocols snmp
    get-ddos-snmp-information
show ddos-protection protocols snmp aggregate
    get-ddos-snmp-aggregate
show ddos-protection protocols snmp aggregate culprit-flows
show ddos-protection protocols snmp parameters
    get-ddos-snmp-parameters
show ddos-protection protocols snmp statistics
    get-ddos-snmp-statistics
show ddos-protection protocols snmp violations
    get-ddos-snmp-violations
show ddos-protection protocols snmpv6
    get-ddos-snmpv6-information
show ddos-protection protocols snmpv6 aggregate
    get-ddos-snmpv6-aggregate
show ddos-protection protocols snmpv6 aggregate culprit-flows
show ddos-protection protocols snmpv6 parameters
    get-ddos-snmpv6-parameters
show ddos-protection protocols snmpv6 statistics
    get-ddos-snmpv6-statistics
show ddos-protection protocols snmpv6 violations
    get-ddos-snmpv6-violations
show ddos-protection protocols ssh
    get-ddos-ssh-information
show ddos-protection protocols ssh aggregate
    get-ddos-ssh-aggregate
show ddos-protection protocols ssh parameters
    get-ddos-ssh-parameters
show ddos-protection protocols ssh statistics
    get-ddos-ssh-statistics
show ddos-protection protocols ssh violations
    get-ddos-ssh-violations
show ddos-protection protocols sshv6
    get-ddos-sshv6-information
show ddos-protection protocols sshv6 aggregate
    get-ddos-sshv6-aggregate
show ddos-protection protocols sshv6 parameters
    get-ddos-sshv6-parameters
show ddos-protection protocols sshv6 statistics
    <get-ddos-sshv6-statistics>
show ddos-protection protocols sshv6 violations
    <get-ddos-sshv6-violations>
show ddos-protection protocols statistics
    <get-ddos-protocols-statistics>
show ddos-protection protocols stp
    <get-ddos-stp-information>
show ddos-protection protocols stp aggregate
    <get-ddos-stp-aggregate>
show ddos-protection protocols stp parameters
    <get-ddos-stp-parameters>
show ddos-protection protocols stp statistics
```

```
<get-ddos-stp-statistics>
show ddos-protection protocols stp violations
<get-ddos-stp-violations>
show ddos-protection protocols tacacs
<get-ddos-tacacs-information>
show ddos-protection protocols tacacs aggregate
<get-ddos-tacacs-aggregate>
show ddos-protection protocols tacacs parameters
<get-ddos-tacacs-parameters>
show ddos-protection protocols tacacs statistics
<get-ddos-tacacs-statistics>
show ddos-protection protocols tacacs violations
<get-ddos-tacacs-violations>
show ddos-protection protocols tcp-flags
<get-ddos-tcp-flags-information>
show ddos-protection protocols tcp-flags aggregate
<get-ddos-tcp-flags-aggregate>
show ddos-protection protocols tcp-flags established
<get-ddos-tcp-flags-establish>
show ddos-protection protocols tcp-flags initial
<get-ddos-tcp-flags-initial>
show ddos-protection protocols tcp-flags parameters
<get-ddos-tcp-flags-parameters>
show ddos-protection protocols tcp-flags statistics
<get-ddos-tcp-flags-statistics>
show ddos-protection protocols tcp-flags unclassified
<get-ddos-tcp-flags-unclass>
show ddos-protection protocols tcp-flags violations
<get-ddos-tcp-flags-violations>
show ddos-protection protocols telnet
<get-ddos-telnet-information>
show ddos-protection protocols telnet aggregate
<get-ddos-telnet-aggregate>
show ddos-protection protocols telnet aggregate culprit-flows
show ddos-protection protocols telnet parameters
<get-ddos-telnet-parameters>
show ddos-protection protocols telnet statistics
<get-ddos-telnet-statistics>
show ddos-protection protocols telnet violations
<get-ddos-telnet-violations>
show ddos-protection protocols telnetv6
<get-ddos-telnetv6-information>
show ddos-protection protocols telnetv6 aggregate
<get-ddos-telnetv6-aggregate>
show ddos-protection protocols telnetv6 aggregate culprit-flows
show ddos-protection protocols telnetv6 parameters
<get-ddos-telnetv6-parameters>
show ddos-protection protocols telnetv6 statistics
<get-ddos-telnetv6-statistics>
show ddos-protection protocols telnetv6 violations
<get-ddos-telnetv6-violations>
show ddos-protection protocols ttl
<get-ddos-ttl-information>
show ddos-protection protocols ttl aggregate
<get-ddos-ttl-aggregate>
show ddos-protection protocols ttl parameters
<get-ddos-ttl-parameters>
show ddos-protection protocols ttl statistics
<get-ddos-ttl-statistics>
show ddos-protection protocols ttl violations
<get-ddos-ttl-violations>
```

```
show ddos-protection protocols tunnel-fragment
  <get-ddos-tun-frag-information>
show ddos-protection protocols tunnel-fragment aggregate
  <get-ddos-tun-frag-aggregate>
show ddos-protection protocols tunnel-fragment aggregate culprit-flows
show ddos-protection protocols tunnel-fragment parameters
  <get-ddos-tun-frag-parameters>
show ddos-protection protocols tunnel-fragment statistics
  <get-ddos-tun-frag-statistics>
show ddos-protection protocols tunnel-fragment violations
  <get-ddos-tun-frag-violations>
show ddos-protection protocols tunnel-ka
  <get-ddos-tunnel-ka-information>
show ddos-protection protocols tunnel-ka aggregate
  <get-ddos-tunnel-ka-aggregate>
show ddos-protection protocols tunnel-ka aggregate culprit-flows
  <get-ddos-tunnel-ka-aggregate-flows>
show ddos-protection protocols tunnel-ka culprit-flows
  <get-ddos-tunnel-ka-flows>
show ddos-protection protocols tunnel-ka flow-detection
  <get-ddos-tunnel-ka-flow-parameters>
show ddos-protection protocols tunnel-ka parameters
  <get-ddos-tunnel-ka-parameters>
show ddos-protection protocols tunnel-ka statistics
  <get-ddos-tunnel-ka-statistics>
show ddos-protection protocols tunnel-ka violations
  <get-ddos-tunnel-ka-violations>
show ddos-protection protocols unknown-l2mc
  <get-ddos-unknown-l2mc-information>
show ddos-protection protocols unknown-l2mc aggregate
  <get-ddos-unknown-l2mc-aggregate>
show ddos-protection protocols unknown-l2mc aggregate culprit-flows
  <get-ddos-unknown-l2mc-aggregate-flows>
show ddos-protection protocols unknown-l2mc culprit-flows
  <get-ddos-unknown-l2mc-flows>
show ddos-protection protocols unknown-l2mc flow-detection
  <get-ddos-unknown-l2mc-flow-parameters>
show ddos-protection protocols unknown-l2mc parameters
  <get-ddos-unknown-l2mc-parameters>
show ddos-protection protocols unknown-l2mc statistics
  <get-ddos-unknown-l2mc-statistics>
show ddos-protection protocols unknown-l2mc violations
  <get-ddos-unknown-l2mc-violations>
show ddos-protection protocols unclassified
  <get-ddos-uncls-information>
show ddos-protection protocols unclassified aggregate
  <get-ddos-uncls-aggregate>
show ddos-protection protocols unclassified parameters
  <get-ddos-uncls-parameters>
show ddos-protection protocols unclassified resolve-v4
show ddos-protection protocols unclassified resolve-v4 culprit-flows
show ddos-protection protocols unclassified resolve-v6 culprit-flows
show ddos-protection protocols unclassified statistics
  <get-ddos-uncls-statistics>
show ddos-protection protocols unclassified violations
  <get-ddos-uncls-violations>
show ddos-protection protocols urpf-fail
  <get-ddos-urpf-fail-information>
show ddos-protection protocols urpf-fail aggregate
  <get-ddos-urpf-fail-aggregate>
```

```

show ddos-protection protocols urpf-fail aggregate culprit-flows
  <get-ddos-urpf-fail-aggregate-flows>
show ddos-protection protocols urpf-fail culprit-flows
  <get-ddos-urpf-fail-flows>
show ddos-protection protocols urpf-fail flow-detection
  <get-ddos-urpf-fail-flow-parameters>
show ddos-protection protocols urpf-fail parameters
  <get-ddos-urpf-fail-parameters>
show ddos-protection protocols urpf-fail statistics
  <get-ddos-urpf-fail-statistics>
show ddos-protection protocols urpf-fail violations
  <get-ddos-urpf-fail-violations>
show ddos-protection protocols vcipc-udp
  <get-ddos-vcipc-udp-information>
show ddos-protection protocols vcipc-udp aggregate
  <get-ddos-vcipc-udp-aggregate>
show ddos-protection protocols vcipc-udp aggregate culprit-flows
  <get-ddos-vcipc-udp-aggregate-flows>
show ddos-protection protocols vcipc-udp culprit-flows
  <get-ddos-vcipc-udp-flows>
show ddos-protection protocols vcipc-udp flow-detection
  <get-ddos-vcipc-udp-flow-parameters>
show ddos-protection protocols vcipc-udp parameters
  <get-ddos-vcipc-udp-parameters>
show ddos-protection protocols vcipc-udp statistics
  <get-ddos-vcipc-udp-statistics>
show ddos-protection protocols vcipc-udp violations
  <get-ddos-vcipc-udp-violations>
show ddos-protection protocols violations
  get-ddos-protocols-violations
show ddos-protection protocols virtual-chassis
  get-ddos-vchassis-information
show ddos-protection protocols virtual-chassis aggregate
  get-ddos-vchassis-aggregate
show ddos-protection protocols virtual-chassis aggregate culprit-flows
show ddos-protection protocols virtual-chassis control-high
  get-ddos-vchassis-control-hi
show ddos-protection protocols virtual-chassis control-low
  get-ddos-vchassis-control-lo
show ddos-protection protocols virtual-chassis parameters
  get-ddos-vchassis-parameters
show ddos-protection protocols virtual-chassis statistics
  get-ddos-vchassis-statistics
show ddos-protection protocols virtual-chassis unclassified
  get-ddos-vchassis-unclass
show ddos-protection protocols virtual-chassis vc-packets
  get-ddos-vchassis-vc-packets
show ddos-protection protocols virtual-chassis vc-ttl-errors
  get-ddos-vchassis-vc-ttl-err
show ddos-protection protocols virtual-chassis violations
  get-ddos-vchassis-violations
show ddos-protection protocols vrrp
  get-ddos-vrrp-information
show ddos-protection protocols vrrp aggregate
  get-ddos-vrrp-aggregate
show ddos-protection protocols vrrp aggregate culprit-flows
show ddos-protection protocols vrrp parameters
  get-ddos-vrrp-parameters
show ddos-protection protocols vrrp statistics
  get-ddos-vrrp-statistics
show ddos-protection protocols vrrp violations

```

```
get-ddos-vrrp-violations
show ddos-protection protocols vrrpv6
get-ddos-vrrpv6-information
show ddos-protection protocols vrrpv6 aggregate
get-ddos-vrrpv6-aggregate
show ddos-protection protocols vrrpv6 aggregate culprit-flows
show ddos-protection protocols vrrpv6 parameters
get-ddos-vrrpv6-parameters
show ddos-protection protocols vrrpv6 statistics
get-ddos-vrrpv6-statistics
show ddos-protection protocols vrrpv6 violations
get-ddos-vrrpv6-violations
show ddos-protection statistics
get-ddos-statistics-information
show ddos-protection version
get-ddos-version
show ddos-protection protocols vxlan
<get-ddos-vxlan-information>
show ddos-protection protocols vxlan aggregate
<get-ddos-vxlan-aggregate>
show ddos-protection protocols vxlan aggregate culprit-flows
<get-ddos-vxlan-aggregate-flows>
show ddos-protection protocols vxlan culprit-flows
<get-ddos-vxlan-flows>
show ddos-protection protocols vxlan flow-detection
<get-ddos-vxlan-flow-parameters>
show ddos-protection protocols vxlan parameters
<get-ddos-vxlan-parameters>
show ddos-protection protocols vxlan statistics
<get-ddos-vxlan-statistics>
show ddos-protection protocols vxlan violations
<get-ddos-vxlan-violations>
show dhcp
show dhcp proxy-client
show dhcp proxy-client binding
show dhcp proxy-client servers
show dhcp proxy-client statistics
<get-proxy-dhcp-client-statistics-information>
show dhcp relay
show dhcp relay binding
<get-dhcp-relay-binding-information>

show dhcp relay binding interface
<get-dhcp-relay-interface-bindings>
show dhcp relay binding lease-time-violation
<get-dhcp-relay-binding-ltv-information>
show dhcp relay statistics
<get-dhcp-relay-statistics-information>
show dhcp relay statistics bulk-leasequery-connections
<get-dhcp-relay-bulk-leasequery-conn-statistics>
show dhcp relay statistics leasequery
<get-dhcp-relay-leasequery-statistics>

show dhcp server
show dhcp server binding
<get-dhcp-server-binding-information>

show dhcp server binding interface
<get-dhcp-relay-binding-interface>
show dhcp server binding lease-time-violation
<get-dhcp-server-binding-ltv-information>
```

```
show dhcp server statistics
  <get-dhcp-server-statistics-information>
show dhcp statistics
  <get-dhcp-service-statistics-information>
show dhcpv6

show dhcpv6 proxy-client
show dhcpv6 proxy-client binding
show dhcpv6 proxy-client statistics
  <get-proxy-dhcpv6-client-statistics-information>
show dhcpv6 relay
show dhcpv6 relay binding
  <get-dhcpv6-relay-binding-information>
show dhcpv6 relay binding interface
  <get-dhcpv6-relay-binding-interface>
show dhcpv6 relay binding lease-time-violation
  <get-dhcpv6-relay-binding-ltv-information>
show dhcpv6 relay statistics
  <get-dhcpv6-relay-statistics-information>
show dhcpv6 relay statistics bulk-leasequery-connections
  <get-dhcpv6-relay-bulk-leasequery-conn-statistics>
show dhcpv6 relay statistics leasequery
  <get-dhcpv6-relay-leasequery-statistics>
show dhcpv6 server
show dhcpv6 server binding
  <get-dhcpv6-server-binding-information>

show dhcpv6 server binding interface
  <get-dhcpv6-server-binding-interface>
show dhcpv6 server binding lease-time-violation
  <get-dhcpv6-server-binding-ltv-information>
show dhcpv6 server statistics
  <get-dhcpv6-server-statistics-information>
show dhcpv6 server statistics bulk-leasequery-connections
  <get-dhcpv6-server-bulk-leasequery-conn-statistics>
show dhcpv6 statistics
  <get-dhcpv6-service-statistics-information>
show diagnostics
show diagnostics tdr
  <get-tdr-interface-information>
show diagnostics tdr interface
  <get-tdr-interface-status>
show diameter
  <get-diameter-information>
show diameter function
  <get-diameter-function-information>
show diameter function statistics
  <get-diameter-function-statistics>
show diameter instance
  <get-diameter-instance-information>
show diameter network-element
  <get-diameter-network-element-information>
show diameter network-element map
  <get-diameter-network-element-map-information>
show diameter peer
  <get-diameter-peer-information>
show diameter peer map
  <get-diameter-peer-map-information>
show diameter peer statistics
  <get-diameter-peer-statistics>
show diameter route
```

```
<get-diameter-route-information>
show dot1x
show dot1x authentication-failed-users
  <get-dot1x-authentication-failed-users>
show dot1x interface
  <get-dot1x-interface-information>
show dot1x static-mac-address
  <get-dot1x-static-mac-addresses>
show dot1x static-mac-address interface
  <get-dot1x-interface-mac-addresses>
show dvmrp
show dvmrp interfaces
  <get-dvmrp-interfaces-information>
show dvmrp neighbors
  <get-dvmrp-neighbors-information>
show dvmrp prefix
  <get-dvmrp-prefix-information>
show dvmrp prunes
  <get-dvmrp-prunes-information>
show dynamic-profile
  <get-dynamic-profile>
show dynamic-profile session
  <get-dynamic-profile-session-information>
show dynamic-tunnels
show dynamic-tunnels database
  <get-dynamic-tunnels-database>
show ethernet-switching mac-learning-log
  <get-ethernet-switching-log-information>
show ethernet-switching mac-notification
  <get-ethernet-switching-mac-notification-information>
show ethernet-switching vxlan-tunnel-end-point remote vtep-source-interface
  <get-ethernet-switching-vxlan-remote-svtep-ip-information>
show ethernet-switching vxlan-tunnel-end-point source ip
  <get-ethernet-switching-vxlan-svtep-ip-information>
show ephemeral-configuration
show esis
show esis adjacency
  <get-esis-adjacency-information>
show esis interface
  <get-esis-interface-information>
show esis statistics
  <get-esis-statistics-information>
show event-options
show event-options event-scripts
show event-options event-scripts policies
  <get-event-scripts-policies>
  <get-event-summary>
show evpn
show evpn arp-table
  <get-evpn-arp-table>
show evpn flood
  <get-evpn-flood-information>
show evpn flood event-queue
  <get-evpn-event-queue-information>
show evpn flood route
show evpn flood route all-ce-flood
  <get-evpn-all-ce-flood-route-information>
show evpn flood route all-flood
  <get-evpn-all-flood-route-information>
show evpn flood route alt-root-flood
  <get-evpn-alt-root-flood-route-information>
```

```

show evpn flood route ce-flood
<get-evpn-ce-flood-route-information>
show evpn flood route mlp-flood
<get-evpn-mlp-flood-route-information>
show evpn flood route re-flood
<get-evpn-re-flood-route-information>
show evpn instance
<get-evpn-instance-information>
show evpn mac-table
<get-evpn-mac-table>
show evpn mac-table interface
<get-evpn-interface-mac-table>
show evpn peer-gateway-macs
<get-evpn-peer-gateway-mac>
show evpn statistics
<get-evpn-statistics-information>
show extensible-subscriber-services
show extensible-subscriber-services accounting
<get-extensible-subscriber-services-accounting>
show extensible-subscriber-services counters
<get-extensible-subscriber-services-counters>
show extensible-subscriber-services dictionary
<get-extensible-subscriber-services-dictionary>
show extensible-subscriber-services services
<get-extensible-subscriber-services-services>
show extensible-subscriber-services sessions
<get-extensible-subscriber-services-sessions>
show extension-provider
show extension-provider system
show extension-provider system connections
<get-mspinfo-connections>
show extension-provider system packages
<get-mspinfo-packages>
show extension-provider system processes
<get-mspinfo-processes>
show extension-provider system processes brief
<get-mspinfo-processes-brief>
show extension-provider system processes extensive
<get-mspinfo-processes-extensive>
show extension-provider system uptime
<get-mspinfo-uptime>
show extension-provider system virtual-memory
<get-core-key-list>
<get-fabric-summary-information>
<get-key-vg-binding>
<get-mac-ip-binding-information>
<get-mc-ccpc-cache-ccpc-select>
<get-mc-ccpc-cache-root-candidates>
<get-mc-ccpc-cache-spf>
<get-mc-ccpc-src-mod-filters>
<get-mc-edge-cache-ccpc-select>
<get-mc-edge-map-to-key-binding>
<get-mc-edge-key-to-map-binding>
<get-mc-edge-vg-portmap>
<get-mc-nsf>
<get-mc-root-cache-trunk>
<get-mc-root-key-to-map-binding>
<get-layer2-group-membership-entries>
<get-layer3-group-membership-entries>
<get-layer3-multicast-pending-routes>
<get-layer3-multicast-receivers>

```

```
<get-mc-root-map-to-key-binding>
<get-mc-root-vg-pfemap>
<get-fabric-multicast-statistics>
<get-mc-vccpdf-adjacency-database>
<get-mspinfo-virtual-memory>
get-fabric-statistics
get-fabric-summary-information
  <get-vlan-domain-map-information>
show fabric multicast dirty-key-info
<get-mc-dirty-key-info>
show fabric multicast edge corekey-ifls-filters
<get-mc-edge-corekey-ifls-filters>
show fabric multicast edge ine-ifls-filters
<get-mc-edge-ine-ifls-filters>
show fabric multicast edge src-mod-filters
<get-mc-edge-src-mod-filters>
show fabric multicast graph
show fabric multicast graph core-tree
<get-fabric-multicast-graph>
show fabric multicast steal-key-info
<get-mc-steal-key-info>
show forwarding-options
show forwarding-options enhanced-hash-key
show forwarding-options enhanced-hash-key fpc
show forwarding-options hyper-mode
<get forwarding-options hyper-mode>
show forwarding-options next-hop-group
<get-forwarding-options-next-hop-group>
show forwarding-options port-mirroring
<get-forwarding-options-port-mirroring>
show helper
show helper statistics
  <get-helper-statistics-information>
show hfrr
show hfrr profiles
show iccp
  <get-inter-chassis-control-protocol-information>
show igmp
show igmp group
  <get-igmp-group-information>
show igmp interface
  <get-igmp-interface-information>
show igmp output-group
  <get-igmp-output-group-information>
show igmp snooping
show igmp snooping interface
  <get-igmp-snooping-interface-information>
show igmp snooping interface bridge-domain
  <get-igmp-snooping-bridge-domain-interface>
show igmp snooping membership
  <get-igmp-snooping-membership-information>
show igmp snooping membership bridge-domain
show igmp snooping options
  <get-igmp-snooping-options-information>
show igmp snooping options
get-igmp-snooping-options-information
show igmp snooping statistics
  <get-igmp-snooping-statistics-information>
show igmp snooping statistics bridge-domain
  <get-igmp-snooping-bridge-domain-membership>
show igmp statistics
```

```
<get-igmp-statistics-information>

show ike
show ike security-associations
  <get-ike-security-associations-information>

show ilmi
<get-ilmi-information>
show ilmi interface
<get-ilmi-interface-information>
show ilmi statistics
<get-ilmi-statistics>
show ingress-replication
  <get-ingress-replication-information>
show interfaces
  <get-interface-information>
show interfaces anchor-group
show interfaces controller
<get-interface-controller-information>
show interfaces destination-class
  <get-destination-class-statistics>

show interfaces destination-class all
<get-all-destination-class-statistics>
show interfaces diagnostics
show interfaces diagnostics optics
  <get-interface-optics-diagnostics-information>

show interfaces far-end-interval
  <show-interfaces-far-end-interval>
show interfaces filters
  <get-interface-filter-information>

show interfaces forwarding-class-counters
<get-interface-fc-counters-information>

show interfaces interface-set
<get-interface-set-information>
show interfaces interface-set queue
  <get-interface-set-queue-information>

show interfaces interval
  <show-interfaces-interval>
show interfaces load-balancing
  <interface-load-balancing>
show interfaces mac-database
  <get-mac-database>

show interfaces mc-ae
  <get-mc-ae-interface-information>
show interfaces mc-ae revertive-info
  <get-mc-ae-revertive-information>
show interfaces policers
  <get-interface-policer-information>

show interfaces queue
  <get-interface-queue-information>

show interfaces redundancy
  <get-redundancy-status>
show interfaces redundancy detail
```

```
<get-redundancy-status-details>
show interfaces routing
show interfaces source-class
  <get-source-class-statistics>

show interfaces source-class all
<get-all-source-class-statistics>
show interfaces targeting
  <get-targeting-information>
show interfaces transport
<get-interface-transport-information>
show interfaces transport optics
<get-interface-transport-optics-information>
show interfaces transport optics interval
<get-interface-transport-optics-interval-information>
show interfaces voq
<get-interface-voq-information>
show ipsec
show ipsec redundancy
show ipsec redundancy interface
  <get-ipsec-pic-redundancy-information>

show ipsec redundancy security-associations
  <get-ipsec-tunnel-redundancy-information>

show ipsec security-associations
  <get-security-associations-information>

show ipv6
show ipv6 neighbors
  <get-ipv6-nd-information>

show ipv6 router-advertisement
  <get-ipv6-ra-information>

show isis
show isis adjacency
  <get-isis-adjacency-information>

show isis authentication
  <get-isis-authentication-information>

show isis backup
show isis backup coverage
  <get-isis-backup-coverage-information>

show isis backup label-switched-path
  <get-isis-backup-lsp-information>

show isis backup spf

show isis backup spf results
  <get-isis-backup-spf-results-information>

show isis context-identifier
  <get-isis-context-identifier-information>

show isis context-identifier identifier
  <get-isis-context-identifier-origin-information>
show isis database
  <get-isis-database-information>
```

```
show isis hostname
  <get-isis-hostname-information>

show isis interface
  <get-isis-interface-information>

show isis overview
  <get-isis-overview-information>

show isis route
  <get-isis-route-information>

show isis spf
show isis spf brief
  <get-isis-spf-results-brief-information>

show isis spf log
  <get-isis-spf-log-information>

show isis spf results
  <get-isis-spf-results-information>

show isis statistics
  <get-isis-statistics-information>

show l2-learning
show l2-learning backbone-instance
  <get-l2-learning-backbone-instance>
show l2-learning evpn
show l2-learning evpn arp-statistics
  <get-evpn-arp-statistics>
show l2-learning evpn arp-statistics interface
  <get-evpn-arp-statistics-interface>
show l2-learning global-information
  <get-l2-learning-global-information>
show l2-learning global-mac-count
  <get-l2-learning-global-mac-count>
show l2-learning instance
  <get-l2-learning-routing-instances>
show l2-learning interface
  <get-l2-learning-interface-information>
show l2-learning mac-move-buffer
  <get-l2-learning-mac-move-buffer-information>
show l2-learning provider-instance
  <get-l2-learning-provider-instance>
show l2-learning redundancy-groups
  <get-l2-learning-redundancy-groups>
show l2-learning remote-backbone-edge-bridges
  <get-l2-learning-remote-backbone-edge-bridges>
show l2-learning vxlan-tunnel-end-point
show l2-learning vxlan-tunnel-end-point remote
  <get-l2-learning-vxlan-rvtep-info>
show l2-learning vxlan-tunnel-end-point remote ip
  <get-l2-learning-vxlan-rvtep-ip-information>
show l2-learning vxlan-tunnel-end-point remote mac-table
  <get-l2-learning-vxlan-rvtep-mactable-information>
show l2-learning vxlan-tunnel-end-point remote vtep-source-interface
  <get-l2-learning-vxlan-remote-svtep-ip-information>
show l2-learning vxlan-tunnel-end-point source
  <get-l2-learning-vxlan-svtep-info>
```

```
show l2-learning vxlan-tunnel-end-point source ip
<get-l2-learning-vxlan-svtep-ip-information>
show l2circuit
show l2circuit connections
  <get-l2ckt-connection-information>

show l2cpd
show l2cpd task
<get-l2cpd-task-information>
show l2cpd task io
  <get-l2cpd-tasks-io-statistics>
show l2cpd task memory
  <get-l2cpd-task-memory>
show l2cpd task replication
  <get-l2cpd-replication-information>
show l2vpn
show l2vpn connections
  <get-l2vpn-connection-information>

show lacp
show lacp interfaces
  <get-lacp-interface-information>
show lacp statistics
show lacp statistics interfaces
  <get-lacp-interface-statistics>
show lacp timeouts
show ldp
show ldp database
  <get-ldp-database-information>

show ldp fec-filters
  <get-ldp-fec-filters-information>

show ldp interface
  <get-ldp-interface-information>

show ldp neighbor
  <get-ldp-neighbor-information>

show ldp oam
<get-ldp-oam-information>
show ldp overview
  <get-ldp-overview-information>
show ldp p2mp
show ldp p2mp fec
  <get-ldp-p2mp-fec-information>
show ldp p2mp path
  <get-ldp-p2mp-path-information>
show ldp p2mp tunnel
  <get-ldp-p2mp-tunnel-information>
show ldp path
  <get-ldp-path-information>

show ldp rib-groups
<get-ldp-rib-groups-information>
show ldp route
  <get-ldp-route-information>

show ldp session
  <get-ldp-session-information>
```

```
show ldp statistics
  <get-ldp-statistics-information>

show ldp traffic-statistics
  <get-ldp-traffic-statistics-information>

show link-management
  <get-lm-information>

show link-management peer
  <get-lm-peer-information>

show link-management routing
  <get-lm-routing-information>

show link-management routing peer
  <get-lm-routing-peer-information>

show link-management routing resource
  <get-lm-routing-resource-information>

show link-management routing te-link
  <get-lm-routing-te-link-information>

show lldp
  <get-lldp-information>

show lldp detail
  <get-lldp-information-detail>

show lldp local-information
  <get-lldp-local-info>

show lldp neighbors
  <get-lldp-neighbors-information>

show lldp neighbors interface
  <get-lldp-interface-neighbors>
show lldp remote-global-statistics
  <get-lldp-remote-global-statistics>

show lldp statistics
  <get-lldp-statistics-information>

show lldp statistics interface
  <get-lldp-interface-statistics>
show link-management statistics
  <get-lm-statistics-information>

show link-management statistics peer
  <get-lm-peer-statistics>

show link-management te-link
  <get-lm-te-link-information>

show mac-rewrite
show mac-rewrite interface
  <get-mac-rewrite-interface-information>
show mld
show mld group
  <get-mld-group-information>
```

```
show mld interface
  <get-mld-interface-information>

show mld output-group
  <get-mld-output-group-information>

show mld snooping
show mld snooping interface
  <get-mld-snooping-interface-information>
show mld snooping interface bridge-domain
  <get-mld-snooping-bridge-domain-interface>
show mld snooping interface vlan
  <get-mld-snooping-vlan-interface>
show mld snooping membership
  <get-mld-snooping-membership-information>
show mld snooping membership bridge-domain
  <get-mld-snooping-bridge-domain-membership>
show mld snooping membership vlan
  <get-mld-snooping-vlan-membership>
show mld snooping statistics
  <get-mld-snooping-statistics-information>
show mld snooping statistics bridge-domain
  <get-mld-snooping-bridge-domain-statistics>
show mld snooping statistics vlan
  <get-mld-snooping-vlan-statistics>
show mld statistics
  <get-mld-statistics-information>

show mobile-ip
show mobile-ip home-agent
show mobile-ip home-agent binding
  <get-mip-binding-information>

show mobile-ip home-agent binding ip-address
  <get-ip-mip-binding-information>

show mobile-ip home-agent binding nai
  <get-nai-mip-binding-information>

show mobile-ip home-agent binding summary
  <get-summary-mip-binding-information>

show mobile-ip home-agent interface
  <get-mip-ha-interface-information>

show mobile-ip home-agent overview
  <get-mip-ha-overview-information>

show mobile-ip home-agent traffic
  <get-mip-ha-traffic-information>

show mobile-ip home-agent virtual-network
  <get-mip-ha-virtual-network-information>

show mobile-ip tunnel
  <get-mip-tunnel-information>
show mobile-ip wimax
show mobile-ip wimax release
  <get-mip-wimax-release-information>
```

```
show mpls
show mpls admin-groups
    <get-mpls-admin-group-information>

show mpls admin-groups-extended
    <get-mpls-admin-group-extended-information>
show mpls call-admission-control
    <get-mpls-call-admission-control-information>

show mpls context-identifier
    <get-mpls-context-identifier-information>

show network-access domain-map
show network-access domain-map statistics
    <get-domain-map-statistics>
show mpls cspf
    <get-mpls-cspf-information>

show mpls diffserv-te
    <get-mpls-diffserv-te-information>
show mpls egress-protection
show mpls interface
    <get-mpls-interface-information>
show mpls label
    <get mpls-label-space>
show mpls label usage
    <get mpls-label-space-usage>

show mpls lsp
    <get-mpls-lsp-information>

show mpls lsp autobandwidth
    <get-mpls-lsp-autobandwidth>
show mpls srlg
    <get-mpls-srlg-information>
show oam ethernet fnp
show oam ethernet fnp interface
show oam ethernet fnp messages
show oam ethernet fnp status
    <get-fnp-status>
show mpls lsp defaults
    <get-mpls-lsp-defaults-information>

show mpls path
    <get-mpls-path-information>

show mpls static-lsp
    <get-mpls-static-lsp-information>
show mpls traceroute
show mpls traceroute database
show mpls traceroute database ldp
    <get-mpls-traceroute-database-ldp>
show msdp
    <get-msdp-information>
show msdp source
    <get-msdp-source-information>

show msdp source-active
    <get-msdp-source-active-information>

show msdp statistics
```

```
<get-msdp-statistics-information>

show multicast
show multicast backup-pe-groups
  <get-multicast-backup-pe-groups-information>

show multicast backup-pe-groups address
  <get-multicast-backup-pe-address-information>

show multicast backup-pe-groups group
  <get-multicast-backup-pe-group-information>
show multicast flow-map
  <get-multicast-flow-maps-information>

show multicast interface
  <get-multicast-interface-information>

show multicast next-hops
  <get-multicast-next-hops-information>

show multicast pim-to-igmp-proxy
  <get-multicast-pim-to-igmp-proxy-information>

show multicast pim-to-mld-proxy
  <get-multicast-pim-to-mld-proxy-information>

show multicast route
  <get-multicast-route-information>

show multicast rpf
  <get-multicast-rpf-information>

show multicast scope
  <get-multicast-scope-information>

show multicast sessions
  <get-multicast-sessions-information>

show multicast snooping
show multicast snooping next-hops
  <get-multicast-snooping-next-hops-information>

show multicast snooping route
  <get-multicast-snooping-route-information>

show multicast statistics
  <get-multicast-statistics-information>

show multicast usage
  <get-multicast-usage-information>

show mvpn
show mvpn c-multicast
  <get-mvpn-c-multicast-route>
show mvpn instance
  <get-mvpn-instance-information>

show mvpn neighbor
  <get-mvpn-neighbor-information>
show mvrp
  <get-mvrp-information>
```

```
show mvrp applicant-state
  <get-mvrp-applicant-information>

show mvrp dynamic-vlan-memberships
  <get-mvrp-dynamic-vlan-memberships>

show mvrp interface
  <get-mvrp-interface-information>

show mvrp registration-state
  <get-mvrp-registration-state>

show mvrp statistics
  <get-mvrp-interface-statistics>

show network-access
show network-access aaa
show network-access aaa radius-servers
  <get-radius-servers-table>
show network-access aaa statistics
  <get-aaa-module-statistics>

show network-access aaa statistics address-assignment
show network-access aaa statistics address-assignment client
  <get-address-assignment-client-statistics>
show network-access aaa statistics address-assignment pool
  <get-address-assignment-pool-statistics>
show network-access aaa subscribers
  <get-aaa-subscriber-table>

show network-access aaa subscribers session-id

show network-access aaa subscribers statistics
  <get-aaa-subscriber-statistics>

show network-access aaa terminate-code
  <get-aaa-terminate-code>
show network-access aaa terminate-code aaa
  <get-aaa-terminate-code-aaa>
show network-access aaa terminate-code dhcp
  <get-aaa-terminate-code-dhcp>
show network-access aaa terminate-code l2tp
  <get-aaa-terminate-code-l2tp>
show network-access aaa terminate-code ppp
  <get-aaa-terminate-code-ppp>
show network-access aaa terminate-code reverse
  <get-aaa-terminate-code-reverse>
show network-access aaa terminate-code reverse aaa
  <get-aaa-terminate-code-reverse-aaa>
show network-access aaa terminate-code reverse dhcp
  <get-aaa-terminate-code-reverse-dhcp>
show network-access aaa terminate-code reverse l2tp
  <get-aaa-terminate-code-reverse-l2tp>
show network-access aaa terminate-code reverse ppp
  <get-aaa-terminate-code-reverse-ppp>
show network-access address-assignment
show network-access address-assignment pool
  <get-address-assignment-pool-table>

show network-access requests
```

```
show network-access requests pending
    <get-authentication-pending-table>

show network-access requests statistics
    <get-authentication-statistics>

show network-access securid-node-secret-file
    <get-node-secret-file-table>

show nonstop-routing
    <get-nonstop-routing-information>

show ntp
show ntp associations
show ntp status
show oam
show oam ethernet
show oam ethernet connectivity-fault-management
show oam ethernet connectivity-fault-management adjacencies
    <get-cfm-adjacency-information>
show oam ethernet connectivity-fault-management delay-statistics
    <get-cfm-delay-statistics>

show oam ethernet connectivity-fault-management forwarding-state
show oam ethernet connectivity-fault-management forwarding-state instance
    <get-cfm-forwarding-state-instance-information>

show oam ethernet connectivity-fault-management forwarding-state interface
    <get-cfm-forwarding-state-interface-information>

show oam ethernet connectivity-fault-management interfaces
    <get-cfm-interfaces-information>
show oam ethernet connectivity-fault-management loss-statistics
    <get-cfm-loss-statistics>
show oam ethernet connectivity-fault-management mep-database
    <get-cfm-mep-database>

show oam ethernet connectivity-fault-management mep-statistics
    <get-cfm-mep-statistics>

show oam ethernet connectivity-fault-management mip
    <get-cfm-mip-information>

show oam ethernet connectivity-fault-management path-database
    <get-cfm-linktrace-path-database>

show oam ethernet connectivity-fault-management policer
    <get-evc-information>

show oam ethernet connectivity-fault-management sla-iterator-statistics
    <get-cfm-iterator-statistics>
show oam ethernet evc
    <get-evc-information>
show oam ethernet link-fault-management
    <get-lfmd-information>

show oam ethernet lmi
    <get-elmi-information>

show oam ethernet lmi statistics
    <get-elmi-statistics>
```

```
show openflow
show openflow capability
show openflow controller
show openflow filters
show openflow flows
show openflow interfaces
show openflow statistics
show openflow statistics flows
show openflow statistics interfaces
show openflow statistics packet
show openflow statistics packet in
show openflow statistics packet out
show openflow statistics queue
show openflow statistics summary
show openflow statistics tables
show openflow summary
show openflow switch

show ospf
show ospf backup
show ospf backup coverage
    <get-ospf-backup-coverage-information>

show ospf backup lsp
    <get-ospf-backup-lsp-information>

show ospf backup neighbor
    <get-ospf-backup-neighbor-information>

show ospf backup spf
    <get-ospf-backup-spf-information>

show ospf context-identifier
    <get-ospf-context-id-information>

show ospf database
    <get-ospf-database-information>

show ospf interface
    <get-ospf-interface-information>

show ospf io-statistics
    <get-ospf-io-statistics-information>

show ospf log
    <get-ospf-log-information>

show ospf neighbor
    <get-ospf-neighbor-information>

show ospf overview
    <get-ospf-overview-information>

show ospf route
    <get-ospf-route-information>

show ospf statistics
    <get-ospf-statistics-information>

show ospf3
```

```
show ospf3 backup
show ospf3 backup coverage
  <get-ospf3-backup-coverage-information>

show ospf3 backup lsp
  <get-ospf3-backup-lsp-information>

show ospf3 backup neighbor
  <get-ospf3-backup-neighbor-information>

show ospf3 backup spf
  <get-ospf3-backup-spf-information>

show ospf3 database
  <get-ospf3-database-information>

show ospf3 interface
  <get-ospf3-interface-information>

show ospf3 io-statistics
  <get-ospf3-io-statistics-information>

show ospf3 log
  <get-ospf3-log-information>

show ospf3 neighbor
  <get-ospf3-neighbor-information>

show ospf3 overview
  <get-ospf3-overview-information>

show ospf3 route
  <get-ospf3-route-information>

show ospf3 statistics
  <get-ospf3-statistics-information>

show passive-monitoring
  <get-passive-monitoring-information>

show passive-monitoring error
  <get-passive-monitoring-error-information>

show passive-monitoring flow
  <get-passive-monitoring-flow-information>

show passive-monitoring memory
  <get-passive-monitoring-memory-information>

show passive-monitoring status
  <get-passive-monitoring-status-information>

show passive-monitoring usage
  <get-passive-monitoring-usage-information>
show path-computation-client
show path-computation-client active-pce
show path-computation-client statistics
show performance-monitoring
show performance-monitoring mpls
show performance-monitoring mpls lsp
  <get-pm-mpls-lsp-information>
```

```
show pfe
show pfe cfeb
show pfe feb
show pfe filter
show pfe filter hw
show pfe filter hw summary
show pfe fpc
show pfe fwdd
show pfe lcc
show pfe next-hop
show pfe pfem
show pfe pfem detail
show pfe pfem extensive
show pfe route
show pfe route clnp
show pfe route clnp table
show pfe route inet6
show pfe route inet6 hw
show pfe route inet6 hw host
show pfe route inet6 hw lpm
show pfe route inet6 hw multicast

show pfe route inet6 table
show pfe route ip
show pfe route ip table
show pfe route iso
show pfe route iso table
show pfe scb
show pfe sfm
show pfe ssb
show pfe statistics
show pfe statistics exceptions
show pfe statistics fabric
show pfe statistics ip
show pfe route ip hw
show pfe route ip hw host
show pfe route ip hw lpm
show pfe route ip hw multicast
show pfe route summary
show pfe route summary hw
show pfe statistics ip6
show pfe statistics traffic
    <get-pfe-statistics>

show pfe statistics traffic cpu
show pfe statistics traffic cpu fpe
show pfe statistics traffic detail
    <get-pfe-traffic-statistics>
show pfe statistics traffic egress-queues
show pfe statistics traffic egress-queues fpc
show pfe statistics traffic multicast
show pfe statistics traffic multicast fpc
show pfe statistics traffic protocol
show pfe terse
    <get-pfe-information>

show pfe version brief
show pfe version detail
show pgm
show pgm negative-acknowledgments
    <get-pgm-nak>
```

```
show pgm source-path-messages
    <get-pgm-source-path-messages>

show pgm statistics
    <get-pgm-statistics>

show pim
show pim bidirectional
show pim bidirectional df-election
    <get-pim-bidir-df-election-information>
show pim bidirectional df-election interface
    <get-pim-bidir-df-election-interface-information>
show pim bootstrap
    <get-pim-bootstrap-information>

show pim interfaces
    <get-pim-interfaces-information>

show pim join
    <get-pim-join-information>

show pim mdt
    <get-pim-mdt-information>

show pim mdt data-mdt-joins
    <get-pim-data-mdt-join-information>
show pim mvpn
    <get-pim-mvpn-information>

show pim neighbors
    <get-pim-neighbors-information>

show pim rps
    <get-pim-rps-information>
show pim snooping
show pim snooping interfaces
show pim snooping join
show pim snooping neighbors
show pim snooping statistics
show pim source
    <get-pim-source-information>

show pim statistics
    <get-pim-statistics-information>

show policy
show policy conditions
show policy damping
show ppp
show ppp address-pool
    <get-ppp-address-pool-information>

show ppp interface
    <get-ppp-interface-information>

show ppp statistics
    <get-ppp-statistics-information>

show ppp summary
    <get-ppp-summary-information>
```

```
show pppoe
show pppoe interfaces
  <get-pppoe-interface-information>
show pppoe lockout
  <get-pppoe-lockout-information>

show pppoe service-name-tables
  <get-pppoe-service-name-table-information>

show pppoe statistics
  <get-pppoe-statistics-information>

show pppoe underlying-interfaces
  <get-pppoe-underlying-interface-information>

show pppoe version
  <get-pppoe-version>

show protection-group
show protection-group ethernet-aps
  <show-protection-group-ethernet-aps>
show protection-group ethernet-ring
show protection-group ethernet-ring aps
  <get-raps-pdu-information>
show protection-group ethernet-ring data-channel
  <get-ring-data-channel-information>
show protection-group ethernet-ring interface
  <get-ring-interface-information>
show protection-group ethernet-ring node-state
  <get-raps-state-machine-information>
show protection-group ethernet-ring node-state
show protection-group ethernet-ring statistics
  <get-ring-tatistics>
show protection-group ethernet-ring vlan
  <get-ring-vlan-information>

show ptp
show ptp clock
  get-ptp-clock>
show ptp global-information
  get-ptp-global-information>
show ptp hybrid
show ptp hybrid config
  <get-ptp-hybrid-mapping>
show ptp hybrid status
  <get-ptp-hybrid-status>
show ptp last-tod-update
  <get-last-tod-update>
show ptp lock-status
  get-ptp-lock-status>
show ptp master
  <get-ptp-master>
show ptp path-trace
  <get-ptp-path-trace>
show ptp port
  <get-ptp-port>
show ptp quality-level-mapping
  <get-ptp-quality-level-mapping>
show ptp slave
  <get-ptp-slave>
show ptp stateful
  <get-ptp-stateful>
```

```
show ptp statistics
    <get-ptp-statistics>
show r2cp
show r2cp interfaces
    <get-r2cp-interface-information>
show r2cp radio
    <get-r2cp-radio-information>
show r2cp sessions
    <get-r2cp-session-information>
show r2cp statistics
    <get-r2cp-statistics>
show redundant-power-system
show redundant-power-system led
show redundant-power-system multi-backup
    <get-rps-scale-information>
show redundant-power-system network
    <get-rps-network-information>
show redundant-power-system power-supply
show redundant-power-system status
show redundant-power-system upgrade
    <get-rps-upgrade-information>
show redundant-power-system version
show rip
show rip general-statistics
    <get-rip-general-statistics-information>

show rip neighbor
    <get-rip-neighbor-information>

show rip statistics
    <get-rip-statistics-information>
show rip statistics peer
    <get-rip-peer-information>
show ripng
show ripng general-statistics
    <get-ripng-general-statistics-information>

show ripng neighbor
    <get-ripng-neighbor-information>
show ripng statistics
    <get-ripng-statistics-information>
show route
    <get-route-information>

show route cumulative
    <get-route-cumulative>

show route export
    <get-rteexport-table-information>

show route export instance
    <get-rteexport-instance-information>

show route localization
    <get-fib-localization-information>
show route export vrf-target
    <get-rteexport-target-information>

show route flow
show route flow validation
    <get-rtflow-dep-information>
```

```
show route forwarding-table
  <get-forwarding-table-information>

show route instance
  <get-instance-information>

show route instance operational
  <get-operational-routing-instance-information>

show route martians
  <get-route-martians>
show route resolution
  <get-route-resolution-information>
show route resolution summary
  <get-route-resolution-summary>
show route resolution unresolved
show route rib-groups
  <get-route-rib-groups>
show route snooping
  <get-route-snooping-information>
show route snooping summary
  <get-route-snooping-summary>
show route summary
  <get-route-summary-information>

show rsvp
show rsvp interface
  <get-rsvp-interface-information>

show rsvp neighbor
  <get-rsvp-neighbor-information>

show rsvp session
  <get-rsvp-session-information>

show rsvp statistics
  <get-rsvp-statistics-information>

show rsvp version
  <get-rsvp-version-information>

show sap
show sap listen
  <get-sap-listen-information>
show security group-vpn member kek
show security group-vpn member kek security-associations
  <get-gvpn-kek-security-associations-information>

show services
show services accounting
  <get-service-accounting-information>

show services accounting aggregation
  <get-service-accounting-aggregation-information>

show services accounting aggregation as
  <get-service-accounting-aggregation-as-information>

show services accounting aggregation destination-prefix
  <get-service-accounting-aggregation-destination-prefix-information>
```

```
show services accounting aggregation protocol-port
  <get-service-accounting-aggregation-protocol-port-information>

show services accounting aggregation source-destination-prefix
  <get-service-accounting-aggregation-source-destination-prefix-information>

show services accounting aggregation source-prefix
  <get-service-accounting-aggregation-source-prefix-information>

show services accounting aggregation template
  <get-service-accounting-aggregation-template-information>

show services accounting errors
  <get-service-accounting-errors-information>

show services accounting flow
  <get-service-accounting-flow-information>

show services accounting flow-detail
  <get-service-accounting-flow-detail>

show services accounting memory
  <get-service-accounting-memory-information>

show services accounting packet-size-distribution
  <get-packet-distribution-information>

show services accounting status
  <get-service-accounting-status-information>

show services accounting usage
  <get-service-accounting-usage-information>

show services alg
show services alg conversations
  <get-service-msp-alg-conversation-information>
show services alg sip-globals
  <get-service-msp-alg-sip-globals-information>
show services alg statistics
show services application-aware-access-list
show services application-aware-access-list flows
show services application-aware-access-list flows interface
  <get-application-aware-access-list-flows-interface>
show services application-aware-access-list flows subscriber
  <get-application-aware-access-list-flows-subscriber>
show services application-aware-access-list statistics
show services application-aware-access-list statistics interface
  <get-application-aware-access-list-statistics-interface>
show services application-aware-access-list statistics subscriber
  <get-application-aware-access-list-statistics-subscriber>
show services application-identification
show services application-identification application
show services application-identification application detail
  <get-appid-application-signature-detail>
show services application-identification application summary
  <get-appid-application-signature-summary>
show services application-identification application-system-cache
  <get-appid-application-system-cache>

show services application-identification counter
```

```

    <get-appid-counter>
show services application-identification counter ssl-encrypted-sessions
<get-appid-counter-encrypted>
show services application-identification group
show services application-identification group detail

    <get-appid-application-group-detail>
show services application-identification group summary
    <get-appid-application-group-summary>
show services application-identification statistics
show services application-identification statistics application-groups
    <get-appid-application-group-statistics>
show services application-identification statistics applications
    <get-appid-application-statistics>
show services application-identification version
    <get-appid-package-version>

show services border-signaling-gateway
show services border-signaling-gateway accounting
show services border-signaling-gateway accounting statistics
    <get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway accounting status
    <get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway admission-control
    <get-service-border-signaling-gateway-statistics-admission-control>

show services border-signaling-gateway by-call-context-id
    <get-service-bsg-information-by-call-context-id>

show services border-signaling-gateway by-contact
    <get-service-border-signaling-gateway-information-by-contact>

show services border-signaling-gateway by-request-uri
    <get-service-border-signaling-gateway-information-by-request-uri>

show services border-signaling-gateway calls
    <get-service-border-signaling-gateway-statistics-calls>

show services border-signaling-gateway calls-duration
    <get-service-border-signaling-gateway-calls-duration>

show services border-signaling-gateway calls-failed

how services border-signaling-gateway charging
show services border-signaling-gateway charging statistics
    <get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway charging status
    <get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway denied-messages
    <get-service-bsg-denied-messages>

show services border-signaling-gateway embedded-spdf
    <get-service-border-signaling-gateway-embedded-spdf>

show services border-signaling-gateway embedded-spdf status
    <get-service-border-signaling-gateway-embedded-spdf-status>

show services border-signaling-gateway name-resolution-cache

show services border-signaling-gateway name-resolution-cache all

```

```
<get-service-border-signaling-gateway-name-resolution-cache-all>

show services border-signaling-gateway name-resolution-cache by-fqdn
<get-border-signaling-gateway-name-resolution-cache-by-fqdn>
show services border-signaling-gateway status
  <get-service-bsg-status-information>
show services captive-portal-content-delivery
show services captive-portal-content-delivery pic
  <get-cpcd-pic-information>
show services captive-portal-content-delivery profile
  <get-cpcd-profile>
show services captive-portal-content-delivery rule
  <get-cpcd-rule>
show services captive-portal-content-delivery ruleset
  <get-cpcd-rule-set>
show services captive-portal-content-delivery sset
  <get-cpcd-service-set>
show services captive-portal-content-delivery statistics
  <get-cpcd-pic-statistics>
show services captive-portal-content-delivery statistics interface
show services capture
<get-service-capture>
show services cos
show services cos statistics
  <get-service-cos-statistics-information>

show services cos statistics diffserv
  <get-service-cos-diffserv-statistics>

show services cos statistics forwarding-class
  <get-service-cos-forwarding-class-statistics>

show services crtp
  <get-service-crtp-params-information>

show services crtp extensive
  <get-service-crtp-extensive-information>

show services crtp flows
  <get-service-crtp-flow-table-information>

show services dynamic-flow-capture
show services dynamic-flow-capture content-destination
  <get-services-dynamic-flow-capture-content-destination-information>

show services dynamic-flow-capture control-source
  <get-services-dynamic-flow-capture-control-source-information>

show services dynamic-flow-capture statistics
  <get-services-dfc-statistics-information>
show services fips
show services fips pic
show services fips pic status
  <get-fips-pic-status-information>

show services flow-collector
  <get-services-flow-collector-information>

show services flow-collector file
  <get-services-flow-collector-file-information>
```

```
show services flow-collector input
  <get-services-flow-collector-input-information>

show services flow-table
show services flow-table statistics
  <get-flow-table-statistics-information>

show services flows
  <get-service-msp-flow-table-information>

show services ggsn
show services ggsn diagnostics
show services ggsn diagnostics pdp
  <get-pdp-diagnostics-per-apn>

show services ggsn statistics
  <get-ggsn-statistics>

show services ggsn statistics apn
  <get-ggsn-apn-statistics-information>

show services ggsn statistics charging
  <get-ggsn-charging-statistics-information>

show services ggsn statistics gtp
  <get-ggsn-gtp-statistics-information>

show services ggsn statistics gtp-prime
  <get-ggsn-gtp-prime-statistics-information>

show services ggsn statistics imsi
  <get-ggsn-imsi-user-information>

show services ggsn statistics l2tp-tunnel
  <get-ggsn-l2tp-tunnel-statistics-information>

show services ggsn statistics msisdn
show services ggsn statistics radius
  <get-ggsn-radius-statistics-information>

show services ggsn statistics sgsn
  <get-ggsn-sgsn-statistics-information>

show services ggsn status
  <get-ggsn-interface-information>

show services ggsn trace
show services ggsn trace all
  <get-ggsn-trace>

show services ggsn trace imsi
  <get-ggsn-imsi-trace>

show services ggsn trace msisdn
  <get-ggsn-msisdn-trace>
show services hcm
show services hcm pic-statistics
  <get-service-hcm-pic-statistics-information>
show services ids
show services ids destination-table
  <get-service-ids-destination-table-information>
```

```
show services ids pair-table
  <get-service-ids-pair-table-information>

show services ids source-table
  <get-service-ids-source-table-information>

show services inline
show services inline ip-reassembly
show services inline ip-reassembly statistics
show services inline nat
show services inline nat mappings
show services inline nat mappings nptv6
<get-inline-nat-mapping-nptv6-information>
show services inline nat pool
  <get-inline-nat-pool-information>
show services inline nat statistics
  <get-inline-nat-statistics-information>
show services inline software
show services inline software statistics
<get-inline-service-sw-statistics-information>
show services inline stateful-firewall
show services inline stateful-firewall flows
<get-inline-sfw-flow-table-information>
show services inline stateful-firewall statistics
<get-inline-sfw-statistics-information>
show services ipsec-vpn
show services ipsec-vpn ike
show services ipsec-vpn ike security-associations
  <get-ike-services-security-associations-information>

show services ipsec-vpn ike statistics
<get-ike-services-statistics>
show services ipsec-vpn ipsec
show services ipsec-vpn ipsec security-associations
  <get-services-security-associations-information>

show services ipsec-vpn ipsec statistics
  <get-services-ipsec-statistics-information>

show services l2tp
show services l2tp destination
  <get-l2tp-destination-information>
show services l2tp destination lockout
  <get-services-l2tp-destination-lockout>
show services l2tp disconnect-cause-summary<
  <get-l2tp-disconnect-cause-summary>
show services l2tp multilink
  <get-l2tp-multilink-information>

show services l2tp radius
show services l2tp radius accounting
show services l2tp radius accounting servers
  <get-services-l2tp-radius-accounting-servers-information>

show services l2tp radius accounting statistics
  <get-services-l2tp-radius-accounting-statistics-information>

show services l2tp radius authentication
show services l2tp radius authentication servers
  <get-services-l2tp-radius-authentication-servers-information>
```

```
show services l2tp radius authentication statistics
  <get-services-l2tp-radius-authentication-statistics-information>

show services l2tp radius servers
  <get-services-l2tp-radius-authentication-accounting-servers-information>

show services l2tp radius statistics
  <get-services-l2tp-radius-authentication-accounting-statistics-information>

show services l2tp session
  <get-l2tp-session-information>

show services l2tp summary
  <get-l2tp-summary-information>

show services l2tp tunnel
  <get-l2tp-tunnel-information>

show services l2tp user
  <get-l2tp-user-information>
show services link-services
show services link-services cpu-usage
  <get-link-services-cpu-usage>

show services local-policy-decision-function
show services local-policy-decision-function flows
show services local-policy-decision-function flows interface
  <get-local-policy-decision-function-flows-interface>
show services local-policy-decision-function flows subscriber
  <get-local-policy-decision-function-flows-subscriber>
show services local-policy-decision-function statistics
show services local-policy-decision-function statistics interface
  <get-local-policy-decision-function-statistics-interface>
show services local-policy-decision-function statistics subscriber
  <get-local-policy-decision-function-statistics-subscriber>
show services logging
show services logging history
show services logging history client
show services logging logfiles
show services mobile
show services mobile hcm
show services mobile hcm statistics
show services nat
show services nat ipv6-multicast-interfaces
  <get-service-nat-ipv6-multicast-information>

show services nat deterministic-nat
show services nat deterministic-nat internal-host
show services nat deterministic-nat nat-port-block
show services nat mappings
  <get-service-nat-mapping-address-pooling-paired>
show services nat mappings brief
  <get-service-nat-mapping-brief>
show services nat mappings detail
show services nat mappings endpoint-independent
  <get-service-nat-mapping-endpoint-independent>
show services nat mappings brief
  <get-service-nat-mapping-brief>
show services nat mappings detail
  <get-service-nat-mapping-detail>
```

```
show services nat mappings pcg
show services nat mappings summary
  <get-service-nat-mapping-summary>
show services nat pool
  <get-service-nat-pool-information>
show services pcg
show services pgcp
show services pgcp active-configuration
  <get-pgcpd-active-configuration>

show services pgcp active-configuration gateway
  <get-service-pgcp-active-configuration-gateway>

show services pgcp conversations
  <get-service-pgcp-conversation-information>

show services pgcp conversations gateway
  <get-service-pgcp-conversation-information-gateway>

show services pgcp flows
  <get-service-pgcp-flow-table-information>

show services pgcp flows gateway
  <get-service-pgcp-flow-table-information-gateway>

show services pgcp gate
  <get-service-pgcp-gate>

show services pgcp gate gateway
  <get-service-pgcp-gate-gateway>

show services pgcp gates
  <get-service-pgcp-gates>

show services pgcp gates gateway
  <get-service-pgcp-gates-gateway>

show services pgcp root-termination
  <get-services-pgcpd-root-termination>

show services pgcp root-termination gateway
  <get-services-pgcpd-root-termination-gateway>

show services pgcp statistics
  <get-service-pgcp-statistics>

show services pgcp statistics gateway
  <get-service-pgcp-statistics-gateway>

show services pgcp terminations
  <get-service-pgcp-terminations>

show services pgcp terminations gateway
  <get-service-pgcp-terminations-gateway>

show services rpm
show services rpm active-servers
  <get-active-servers>

show services rpm history-results
  <get-history-results>
```

```

show services rpm probe-results
    <get-probe-results>

show services rpm twamp
    <twamp-information>
show services rpm twamp client
    <twamp-client-information>
show services rpm twamp client connection
    <twamp-client-connection-information>
show services rpm twamp client history-results
    <twamp-get-history-results>
show services rpm twamp client probe-results
    <twamp-get-probe-results>
show services rpm twamp client session
    <twamp-client-test-session>
show services rpm twamp server
    <twamp-server-information>
show services rpm twamp server connection
    <twamp-server-connection-information>
show services rpm twamp server session
    <twamp-server-session-information>
show services server-load-balance
show services server-load-balance external-manager
show services server-load-balance external-manager information
show services server-load-balance external-manager statistics
    <get-external-manager-statistics-information>
show services server-load-balance hash-table
    <get-hash-table-information>
show services server-load-balance health-monitor
show services server-load-balance health-monitor information
    <get-real-server-health-monitor-information>
show services server-load-balance health-monitor statistics
    <get-real-server-health-monitor-statistics-information>
show services server-load-balance real-server
show services server-load-balance real-server statistics
    <get-real-server-statistics-information>
show services server-load-balance real-server-group
show services server-load-balance real-server-group information
    <get-real-server-group-information>
show services server-load-balance real-server-group statistics
    <get-real-server-group-statistics-information>
show services server-load-balance sticky
    <get-sticky-table-information>
show services server-load-balance virtual-server
show services server-load-balance virtual-server information
    <get-virtual-server-information>
show services server-load-balance virtual-server statistics
    <get-virtual-server-statistics-information>
show services service-identification
show services service-identification header-redirect
show services service-identification header-redirect statistics
    <get-header-redirect-set-statistics-information>

show services service-identification statistics
    <get-service-identification-statistics-information>

show services service-identification uri-redirect
show services service-identification uri-redirect statistics
    <get-uri-redirect-set-statistics-information>

```

```
show services service-sets
show services service-sets cpu-usage
    <get-service-set-cpu-statistics>

show services service-sets memory-usage
    <get-service-set-memory-statistics>

show services service-sets memory-usage zone
show services service-sets plug-ins
    <get-service-set-plugin-summary>

show services service-sets statistics
show services service-sets statistics drop-flow-limit
    <get-service-set-drop-flow-statistics>
show services service-sets statistics jflow-log
    <get-service-set-jflow-log-statistics>
show services service-sets statistics packet-drops
    <get-service-set-packet-drop-statistics>

show services service-sets statistics syslog
    <get-service-set-syslog-statistics>
show services service-sets statistics tcp-mss
    <get-service-set-tcp-mss-statistics>

show services service-sets summary
    <get-service-set-summary-information>

show services sessions
    <get-msp-session-table>

show services softwire
    <get-service-softwire-table-information>

show services softwire flows
    <get-service-fwnat-flow-table-information>

show services softwire statistics
    <get-service-softwire-statistics-information>

show services stateful-firewall
show services stateful-firewall flow-analysis
    <get-service-flow-analysis-information>
show services stateful-firewall conversations
    <get-service-sfw-conversation-information>

show services stateful-firewall flows
    <get-service-sfw-flow-table-information>
show services stateful-firewall redundancy-statistics
    <get-service-sfw-redundancy-statistics>

show services stateful-firewall sip-call
    <get-service-sfw-sip-call-information>

show services stateful-firewall sip-register
    <get-service-sfw-sip-register-information>

show services stateful-firewall statistics
    <get-service-sfw-statistics-information>

show services stateful-firewall statistics application-protocol
```

```
<et-sfw-application-protocol-statistics>
show services stateful-firewall subscriber-analysis
<get-service-subs-analysis-information>
show services subscriber
show services subscriber bandwidth
show services subscriber bandwidth client-id
  <get-services-subscriber-bandwidth-by-session-id>
show services subscriber bandwidth interface
  <get-services-subscriber-bandwidth-by-interface>
show services subscriber bandwidth ip-address
  <get-services-subscriber-bandwidth-by-ip-address>
show services subscriber bandwidth service-interface
  <get-services-subscriber-bandwidth-by-service-interface>
show services subscriber dynamic-policies
  <get-services-subscriber-dynamic-policies>
show services subscriber flows
  <get-services-subscriber-flows>
show services subscriber sessions
  <get-services-subscriber-session>
show services subscriber statistics
  <get-services-subscriber-statistics>
show services unified-access-control
show services unified-access-control authentication-table
  <get-uac-auth-table>
show services unified-access-control policies
  <get-uac-policies>
show services unified-access-control roles
  <get-uac-role-entries>
show services unified-access-control status
  <get-uac-status>
show services video-monitoring
  <get-service-video-monitoring-information>
show services video-monitoring mdi
  <get-service-video-monitoring-mdi-information>
show services video-monitoring mdi alarms
  <get-services-video-monitoring-mdi-alarms-information>
show services video-monitoring mdi alarms errors
  <get-services-video-monitoring-mdi-alarms-errors-information>
show services video-monitoring mdi alarms stats
  <get-services-video-monitoring-mdi-alarms-stats-information>
show services video-monitoring mdi errors
  <get-service-video-monitoring-mdi-errors-information>
show services video-monitoring mdi flow
  <get-service-video-monitoring-mdi-flows-information>
show services video-monitoring mdi stats
  <get-service-video-monitoring-mdi-stats-information>
show snmp
show snmp health-monitor
  <get-health-monitor-information>

show snmp health-monitor alarms
  <get-health-monitor-alarm-information>

show snmp health-monitor logs
  <get-health-monitor-log-information>

show snmp inform-statistics
  <get-snmp-inform-statistics>

show snmp mib
show snmp mib get
```

```
<get-snmp-object>

show snmp mib get-next
  <get-next-snmp-object>

show snmp mib walk
  <get-walk-snmp-object>

show snmp proxy
show snmp rmon
  <get-rmon-information>

show snmp rmon alarms
  <get-rmon-alarm-information>

show snmp rmon events
  <get-rmon-event-information>

show snmp rmon history
  <get-rmon-history-information>

show snmp rmon logs
  <get-rmon-log-information>

show snmp statistics
  <get-snmp-information>

show snmp v3
  <get-snmp-v3-information>

show snmp v3 access
  <get-snmp-v3-access-information>

show snmp v3 community
  <get-snmp-v3-community-information>

show snmp v3 general
  <get-snmp-v3-general-information>

show snmp v3 groups
  <get-snmp-v3-group-information>

show snmp v3 notify
  <get-snmp-v3-notify-information>

show snmp v3 notify filter
  <get-snmp-v3-notify-filter-information>

show snmp v3 target
  <get-snmp-v3-target-information>

show snmp v3 target address
  <get-snmp-v3-target-address-information>

show snmp v3 target parameters
  <get-snmp-v3-target-parameters-information>

show snmp v3 users
  <get-snmp-v3-usm-user-information>

show spanning-tree
```

```
show spanning-tree bridge
    <get-stp-bridge-information>
show spanning-tree interface
    <get-stp-interface-information>
show spanning-tree mstp
show spanning-tree mstp configuration
    <get-mstp-configuration-information>
show spanning-tree statistics
    <get-stp-interface-statistics>
show spanning-tree statistics bridge
show spanning-tree statistics interface
show spanning-tree statistics routing-instance
    <get-stp-routing-instance-statistics>
show spanning-tree stp-buffer
show static-subscribers
show static-subscribers sessions
<show subscribers
    <get-subscribers>
show subscribers summary
    <get-subscribers-summary>
<get-syslog-filenames>

show synchronous-ethernet
show synchronous-ethernet esmc
show synchronous-ethernet esmc statistics
show synchronous-ethernet esmc transmit
show synchronous-ethernet global-information
show system
show system alarms
    <get-system-alarm-information>

show system auto-snapshot
show system boot-messages
show system buffers
show system certificate
show system commit
    <get-commit-information>
show system commit revision
    <get-commit-revision-information>
show system commit server
    <get-commit-server-information>
show system commit server queue
    <get-commit-server-queue-information>
show system configuration
show system configuration archival
    <get-system-archival>

show system configuration rescue
    <get-rescue-information>

show system connections
show system core-dumps
<get-system-core-dumps>
show system core-dumps core-file-info
    <get-core-file-information>

show system core-dumps kernel-crashinfo
show system core-dumps transfer-status
show system diagnostics
show system diagnostics inventory
show system diagnostics usage
```

```
show system directory-usage
    <get-directory-usage-information>

show system firmware
    <get-system-firmware-information>
show system khms-stats

show system license
    <get-license-summary-information>

show system license installed
    <get-license-information>
show system license key-content
show system license keys
    <get-license-key-information>

show system license usage
    <get-license-usage-summary>
show system login
show system login lockout
    <get-system-login-lockout-information>
show system memory
<show system processes
show system processes brief
show system processes esc-node
show system processes extensive
show system processes health
    <get-process-health-information>

show system processes providers
show system processes host-processes detail
show system processes resource-limits
    <get-system-process-resource-limits>
show system processes summary
show system queues
show system reboot
show system resource-cleanup
show system resource-cleanup processes
    <get-system-resource-cleanup-processes-information>
    <get-resource-monitor-fpc-information>
    <get-resource-monitor-fpc-slot-information>

show system rollback
    <get-rollback-information>

show system services
show system services dhcp
show system services dhcp binding
    <get-dhcp-binding-information>

show system services dhcp conflict
    <get-dhcp-conflict-information>

show system services dhcp global
    <get-dhcp-global-information>

show system services dhcp pool
    <get-dhcp-pool-information>

show system services dhcp statistics
```

```
<get-dhcp-statistics-information>

show system services reverse
<get-system-services-reverse-information>

show system services service-deployment
<get-service-deployment-service-information>

show system snapshot
<get-snapshot-information>

show system software
show system software backup
<get-package-backup-information>
<get-software-installation-status>
show system software recovery-package

show system statistics
<get-statistics-information>

show system statistics bridge
<get-system-bridge-statistics>
show system statistics extended
show system statistics vpls
show system storage
<get-system-storage>
show system storage partitions
<get-system-storage-partitions>
show system subscriber-management
show system subscriber-management route
<get-subscriber-management-route>
show system subscriber-management route next-hop
<get-subscriber-management-route-nh>
show system subscriber-management route summary
<get-subscriber-management-route-summary>
show system subscriber-management statistics
<get-subscriber-management-statistics>
show system subscriber-management summary
show system switchover
<get-switchover-information>

show system uptime
<get-system-uptime-information>

show system users
<get-system-users-information>

show system virtual-memory
show task
show task io
show task logical-system-mux
<get-lrmuxd-task-information>
show task logical-system-mux io
<get-lrmuxd-tasks-io-statistics>
show task logical-system-mux memory
<get-lrmuxd-task-memory>
show task memory
show task replication
<get-routing-task-replication-state>
show task snooping
show task snooping io
```

```
show task snooping memory
<get-snooping-task-memory-information>
show ted
show ted database
  <get-ted-database-information>

show ted link
  <get-ted-link-information>

show ted protocol
  <get-ted-protocol-information>
show unified-edge
show unified-edge gateways
show unified-edge ggsn-pgw
show unified-edge ggsn-pgw aaa
show unified-edge ggsn-pgw aaa network-element
show unified-edge ggsn-pgw aaa network-element status
show unified-edge ggsn-pgw aaa network-element-group
show unified-edge ggsn-pgw aaa network-element-group status
show unified-edge ggsn-pgw aaa radius
show unified-edge ggsn-pgw aaa radius statistics
show unified-edge ggsn-pgw aaa statistics
show unified-edge ggsn-pgw address-assignment
show unified-edge ggsn-pgw address-assignment group
show unified-edge ggsn-pgw address-assignment pool
show unified-edge ggsn-pgw address-assignment service-mode
show unified-edge ggsn-pgw address-assignment statistics
show unified-edge ggsn-pgw apn
show unified-edge ggsn-pgw apn service-mode
show unified-edge ggsn-pgw apn statistics
show unified-edge ggsn-pgw call-rate
show unified-edge ggsn-pgw call-rate statistics
show unified-edge ggsn-pgw charging
show unified-edge ggsn-pgw charging global
show unified-edge ggsn-pgw charging global statistics
show unified-edge ggsn-pgw charging local-persistent-storage
show unified-edge ggsn-pgw charging local-persistent-storage statistics
show unified-edge ggsn-pgw charging path
show unified-edge ggsn-pgw charging path statistics
show unified-edge ggsn-pgw charging path status
show unified-edge ggsn-pgw charging service-mode
show unified-edge ggsn-pgw charging transfer
show unified-edge ggsn-pgw charging transfer statistics
show unified-edge ggsn-pgw charging transfer status
show unified-edge ggsn-pgw charging trigger-profile
show unified-edge ggsn-pgw gtp
show unified-edge ggsn-pgw gtp peer
show unified-edge ggsn-pgw gtp peer count
show unified-edge ggsn-pgw gtp peer history
show unified-edge ggsn-pgw gtp peer statistics
show unified-edge ggsn-pgw gtp statistics
show unified-edge ggsn-pgw ip-reassembly
show unified-edge ggsn-pgw ip-reassembly statistics
show unified-edge ggsn-pgw resource-manager
show unified-edge ggsn-pgw resource-manager clients
show unified-edge ggsn-pgw service-mode
show unified-edge ggsn-pgw statistics
show unified-edge ggsn-pgw statistics traffic-class
show unified-edge ggsn-pgw status
show unified-edge ggsn-pgw status gtp-peer
show unified-edge ggsn-pgw status preemption-list
```

```

show unified-edge ggsn-pgw status session-state
show unified-edge ggsn-pgw subscribers
show unified-edge ggsn-pgw subscribers charging
show unified-edge ggsn-pgw subscribers traffic-class
show unified-edge ggsn-pgw system
show unified-edge ggsn-pgw system interfaces
show unified-edge ggsn-pgw system interfaces service-mode
show unified-edge sgw
show unified-edge sgw call-rate
show unified-edge sgw call-rate statistics
show unified-edge sgw charging
show unified-edge sgw charging global
show unified-edge sgw charging global statistics
show unified-edge sgw charging local-persistent-storage
show unified-edge sgw charging local-persistent-storage statistics
show unified-edge sgw charging path
show unified-edge sgw charging path statistics
show unified-edge sgw charging path status
show unified-edge sgw charging service-mode
show unified-edge sgw charging transfer
show unified-edge sgw charging transfer statistics
show unified-edge sgw charging transfer status
show unified-edge sgw charging trigger-profile
show unified-edge sgw gtp
show unified-edge sgw gtp peer
show unified-edge sgw gtp peer count
show unified-edge sgw gtp peer history
show unified-edge sgw gtp peer statistics
show unified-edge sgw gtp statistics
show unified-edge sgw idle-mode-buffering
show unified-edge sgw idle-mode-buffering statistics
show unified-edge sgw ip-reassembly
show unified-edge sgw ip-reassembly statistics
show unified-edge sgw resource-manager
show unified-edge sgw resource-manager clients
show unified-edge sgw service-mode
show unified-edge sgw statistics
show unified-edge sgw status
show unified-edge sgw status gtp-peer
show unified-edge sgw status preemption-list
show unified-edge sgw status session-state
show unified-edge sgw subscribers
show unified-edge sgw subscribers charging
show unified-edge sgw system
show unified-edge sgw system interfaces
show unified-edge sgw system interfaces service-mode
show version
    <get-software-information>

show virtual-chassis
show virtual-chassis active-topology
<get-virtual-chassis-active-topology>
show virtual-chassis device-topology
<get-virtual-chassis-device-topology>
show virtual-chassis fast-failover
<get-virtual-chassis-fast-failover>
show virtual-chassis heartbeat
<get-virtual-chassis-heartbeat-information>
show virtual-chassis login
<get-virtual-chassis-login>
show virtual-chassis mode

```

```
<get-virtual-chassis-mode-information>
show virtual-chassis protocol
show virtual-chassis protocol adjacency
<get-virtual-chassis-adjacency-information>
show virtual-chassis protocol database
<get-virtual-chassis-database-information>
show virtual-chassis protocol interface
<get-virtual-chassis-interface-information>
show virtual-chassis protocol route
<get-virtual-chassis-route-information>
show virtual-chassis protocol statistics
<get-virtual-chassis-statistics-information>
show virtual-chassis status
<get-virtual-chassis-information>
show virtual-chassis vc-path
<get-virtual-chassis-packet-path>
show virtual-chassis vc-port
<get-virtual-chassis-port-information>
show virtual-chassis vc-port diagnostics
show virtual-chassis vc-port diagnostics optics
<get-virtual-chassis-optics-diagnostics>
show virtual-chassis vc-port lag-hash
<get-virtual-chassis-port-lag-hash-information>
show virtual-chassis vc-port statistics
<get-virtual-chassis-port-statistics>
show vlans
<get-vlan-information>
show vlans operational
<get-operational-vlan-instance-information>

show vpls
show vpls connections
    <get-vpls-connection-information>

show vpls flood
show vpls flood event-queue
    <get-vpls-event-queue-information>

show vpls flood route
show vpls flood route all-ce-flood
    <get-vpls-all-ce-flood-route-information>

show vpls flood route all-flood
    <get-vpls-all-flood-route-information>

show vpls flood route alt-root-flood
    <get-vpls-alt-root-flood-route-information>

show vpls flood route ce-flood
    <get-vpls-ce-flood-route-information>

show vpls flood route mlp-flood
    <get-vpls-mlp-flood-route-information>

show vpls flood route re-flood
    <get-vpls-re-flood-route-information>

show vpls mac-table
    <get-vpls-mac-table>

show vpls mac-table interface
```

```

<get-vpls-interface-mac-table>

show vpls statistics
<get-vpls-statistics-information>

show vrrp
show vrrp interface
show vrrp track
test interface
test interface fd1-line-loop
test interface fd1-line-loop ansi
test interface fd1-line-loop ansi initiate
test interface fd1-line-loop ansi terminate
test interface fd1-line-loop bellcore
test interface fd1-line-loop bellcore initiate
test interface fd1-line-loop bellcore terminate
test interface fd1-payload-loop
test interface fd1-payload-loop ansi
test interface fd1-payload-loop ansi initiate
test interface fd1-payload-loop ansi terminate
test interface fd1-payload-loop bellcore
test interface fd1-payload-loop bellcore initiate
test interface fd1-payload-loop bellcore terminate
test interface inband-line-loop
test interface inband-line-loop ansi
test interface inband-line-loop ansi initiate
test interface inband-line-loop ansi terminate
test interface inband-line-loop bellcore
test interface inband-line-loop bellcore initiate
test interface inband-line-loop bellcore terminate
test interface inband-line-loop initiate
test interface inband-line-loop terminate
test interface inband-payload-loop
test interface inband-payload-loop ansi
test interface inband-payload-loop ansi initiate
test interface inband-payload-loop ansi terminate
test interface inband-payload-loop bellcore
test interface inband-payload-loop bellcore initiate
test interface inband-payload-loop bellcore terminate
test msdp
test msdp dependent-peers
test msdp rpf-peer
test policy
<

```

Configuration Hierarchy Levels

```

[edit dynamic-profiles routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems services mobile-ip home-agent enable-service]
[edit routing-instances instance services mobile-ip home-agent enable-service]
[edit services mobile-ip home-agent enable-service]

```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

[view-configuration](#)

Supported Platforms [EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX](#)

Can view all of the configuration (not including secrets).

Commands No associated CLI commands.

Configuration Hierarchy Levels No associated CLI configuration hierarchy levels and statements.

Related Documentation

- [Access Privilege User Permission Flags Overview on page 48](#)
- [Understanding Junos OS Access Privilege Levels on page 7](#)
- [Configuring Access Privilege Levels on page 37](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 38](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 42](#)

CHAPTER 5

Configuring Authentication Methods

- [Configuring RADIUS Server Authentication on page 219](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 222](#)
- [Configuring TACACS+ Authentication on page 225](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)
- [Example: Configuring Authentication Order on page 230](#)

Configuring RADIUS Server Authentication

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

RADIUS authentication is a method of authenticating users who attempt to access the router or switch.

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and that all vendors of these systems support RADIUS.

You should use RADIUS when your priorities are interoperability and performance:

- **Interoperability**—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
- **Performance**—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.

To use RADIUS authentication on the device, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server.

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. As such, the steps shown here are in a configuration group called **global**. Using a configuration group is optional.

To configure authentication by a RADIUS server:

1. Add an IPv4 or IPv6 server address.

- Configure an IPv4 source address and server address:

```
[edit groups global]
user@host# set system radius-server server-address source-address source-address
```

For example:

```
[edit groups global]
user@host# set system radius-server 192.168.17.28 source-address 192.168.17.1
```

- Configure an IPv6 source address and server address:

```
[edit groups global system radius-server server-address]
user@host# set server-address secret "secretkey" source-address source-address
```

For example:

```
[edit groups global system radius-server ::17.22.22.162]
user@host# set secret $9$ABC123 source-address ::17.22.22.1
```

The source address is a valid IPv4 or IPv6 address configured on one of the router or switch interfaces. This configuration sets a fixed address as the source address for locally generated IP packets.

Server address is a unique IPv4 or IPv6 address that is assigned to a particular server and used to route information to the server. If the Junos OS device has several interfaces that can reach the RADIUS server, assign an IP address that Junos OS can use for all its communication with the RADIUS server.

2. Include a shared secret password.

You must specify a password in the **secret password** statement. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router or switch must match that used by the server. The secret password configures the password that the Junos OS device uses to access the RADIUS server.

```
[edit groups global system radius-server server-address]
user@host# set secret password
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set secret $9$ABC123ABC123
```

3. If necessary, specify a port on which to contact the RADIUS server.

By default, port number 1812 is used (as specified in RFC 2865).



NOTE: You can also specify an accounting port to send accounting packets with the **accounting-port** statement. The default is 1813 (as specified in RFC 2866).

```
[edit groups global system radius-server server-address]
user@host# set port port-number
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set port 1845
```

4. Specify the order in which Junos OS attempts authentication.

You must include the **authentication-order** statement in your remote authentication configuration.

The example assumes your network includes both RADIUS and TACACS+ servers. In this example, whenever a user attempts to log in, Junos OS begins by querying the RADIUS server for authentication. If it fails, it next attempts authentication with locally configured user accounts. Finally the TACACS+ server is tried.

```
[edit groups global system]
user@host# set authentication-order [ authentication-methods ]
```

For example:

```
[edit groups global system]
user@host# set authentication-order [ radius password tacplus ]
```

5. Assign a login class to RADIUS-authenticated users.

You can assign different user templates and login classes to RADIUS-authenticated users. This allows RADIUS-authenticated users to be granted different administrative permissions on the Junos OS device. By default, RADIUS-authenticated users use the **remote** user template and are assigned to the associated class, which is specified in the **remote** user template, if the **remote** user template is configured. The username **remote** is a special case in Junos OS. It acts as a template for users who are authenticated by a remote server, but do not have a locally-configured user account on the device. In this method, Junos OS applies the permissions of the remote template to those authenticated users without a locally defined account. All users mapped to the remote template are of the same login class.

In the Junos OS configuration, a user template is configured in the same way as a regular local user account, except that no local authentication password is configured because the authentication is remotely performed on the RADIUS server.

- To use the same permissions for all RADIUS-authenticated users:

```
[edit groups global system login]
user@host# set user remote class class
```

For example:

```
[edit groups global system login]
user@host# set user remote class super-user
```

- To have different login classes be used for different RADIUS-authenticated users, granting them different permissions:
 - a. Create multiple user templates in the Junos OS configuration.

Every user template can be assigned a different login class.

For example:

```
[edit groups global system login]
```

```
set user RO class read-only
set user OP class operator
set user SU class super-user
set user remote full-name "default remote access user template"
set user remote class read-only
```

- b. Have the RADIUS server specify the name of the user template to be applied to the authenticated user.

For a RADIUS server to indicate which user template is to be applied, it needs to include the Juniper-Local-User-Name attribute (Vendor 2636, type 1, string) Juniper VSA (vendor-specific attribute) in the RADIUS Access-Accept message. The string value in the Juniper-Local-User-Name must correspond to the name of a configured user template on the device. For a list of relevant Juniper RADIUS VSAs, see [Juniper Networks Vendor-Specific RADIUS Attributes](#).

If the Juniper-Local-User-Name is not included in the Access-Accept message or the string contains a user template name that does not exist on the device, the user is assigned to the **remote** user template, if configured. If it is not configured, authentication fails for the user.

After logging in, the remotely authenticated user retains the same username that was used to log in. However, the user inherits the user class from the assigned user template.

In a RADIUS server, users can be assigned a Juniper-Local-User-Name string, which indicates the user template to be used in the Junos OS device. From the previous example, the string would be RO, OP, or SU.

Configuration of the RADIUS server depends on the server being used. For instructions for the Juniper Steel-Belted Radius server, see [Steel-Belted Radius \(SBR\) Enterprise](#). For information on using FreeRADIUS, see <http://kb.juniper.net/InfoCenter/index?page=content&id=KB19446>.

Example: Configuring a RADIUS Server for System Authentication

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure a RADIUS server for system authentication.

- [Requirements on page 222](#)
- [Overview on page 223](#)
- [Configuration on page 223](#)
- [Verification on page 224](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one RADIUS server. For more details, see [RADIUS Authentication and Accounting Servers Configuration Overview](#).

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1 and specify the shared secret password of the RADIUS server as Radiussecret1. The secret is stored as an encrypted value in the configuration database. Finally, you specify the source address to be included in the RADIUS server requests by the device. In most cases you can use the loopback address of the device, which in this example is 10.0.0.1.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system radius-server address 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the RADIUS section, click **Add**. The Add Radius Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the source IP address of the server.
9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.
[edit system]

```
user@host# set radius-server address 172.16.98.1
```

2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```

3. Specify the device's loopback address source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system radius-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system radius-server
radius-server 172.16.98.1 {
  secret Radiussecret1;
  source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 230](#).
 - Configure a user. See [“Example: Configuring New Users” on page 15](#).
 - Configure local user template accounts. See [“Example: Creating Template Accounts” on page 19](#).
-

Verification

Confirm that the configuration is working properly.

Verifying the RADIUS Server System Authentication Configuration

Purpose Verify that the RADIUS server has been configured for system authentication.

Action From operational mode, enter the **show system radius-server** command.

Related Documentation

- [Understanding User Authentication Methods on page 12](#)
- [Understanding User Accounts on page 6](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)

- [Understanding Login Classes on page 3](#)

Configuring TACACS+ Authentication

Supported Platforms [SRX Series, vSRX](#)

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

- [Configuring TACACS+ Server Details on page 225](#)
- [Specifying a Source Address for the Junos OS to Access External TACACS+ Servers on page 226](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 226](#)
- [Configuring Juniper Networks Vendor-Specific TACACS+ Attributes on page 227](#)

Configuring TACACS+ Server Details

Supported Platforms

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the **tacplus-server** statement at the **[edit system]** hierarchy level:

```
[edit system]
tacplus-server server-address {
  port port-number;
  secret password;
  single-connection;
  timeout seconds;
}
```

server-address is the address of the TACACS+ server.

port-number is the TACACS+ server port number.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the **secret** statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the **single-connection** statement.



NOTE: Early versions of the TACACS+ server do not support the **single-connection** option. If you specify this option and the server does not support it, the Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the **user** statement at the **[edit system login]** hierarchy level, as described in *Overview of Template Accounts for RADIUS and TACACS+ Authentication*.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

Supported Platforms

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the **source-address** statement at the **[edit system tacplus-server server-address]** hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the **source-address** statement at the **[edit system accounting destination tacplus server server-address]** hierarchy level:

```
[edit system accounting destination tacplus server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router or switch interfaces.

Configuring the Same Authentication Service for Multiple TACACS+ Servers

Supported Platforms **SRX Series, vSRX**

To configure the same authentication service for multiple TACACS+ servers, include statements at the **[edit system tacplus-server]** and **[edit system tacplus-options]** hierarchy levels. For information about how to configure a TACACS+ server at the **[edit system tacplus-server]** hierarchy level, see [“Configuring TACACS+ Authentication” on page 225](#).

To assign the same authentication service to multiple TACACS+ servers, include the **service-name** statement at the **[edit system tacplus-options]** hierarchy level:

```
[edit system tacplus-options]
```

```
service-name service-name;
```

service-name is the name of the authentication service. By default, the service name is set to **junos-exec**.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
  10.2.2.2 secret "$ABC123"; ## SECRET-DATA
  10.3.3.3 secret "$ABC123"; ## SECRET-DATA
}
tacplus-options {
  service-name bob;
}
```

Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

Supported Platforms [SRX Series, vSRX](#)

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the Junos OS with TACACS+.

To specify these attributes, include a **service** statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
  local-user-name = <username-local-to-router>
  allow-commands = "<allow-commands-regex>"
  allow-configuration-regexps = "<allow-configuration-regex>"
  deny-commands = "<deny-commands-regex>"
  deny-configuration-regexps = "<deny-configuration-regex>"
}
```

This **service** statement can appear in a **user** or **group** statement.

Related Documentation

- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)

Example: Configuring a TACACS+ Server for System Authentication

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure a TACACS+ server for system authentication.

- [Requirements on page 228](#)
- [Overview on page 228](#)
- [Configuration on page 228](#)
- [Verification on page 229](#)

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one TACACS+ server.

Overview

In this example, you set the IP address to 172.16.98.24 and the shared secret password of the TACACS+ server to Tacacssecret1. The secret password is stored as an encrypted value in the configuration database. You then set the loopback source address as 10.0.0.1

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system tacplus-server address 172.16.98.24
set system tacplus-server 172.16.98.24 secret Tacacssecret1
set system tacplus-server 172.16.98.24 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a TACACS+ server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. In the TACACS section, click **Add**. The Add TACACS Server dialog box appears.
5. In the IP Address box, type the server's 32-bit IP address.
6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.
7. In the Server Port box, type the appropriate port.
8. In the Source Address box, type the locally configured interface address, which is used as the source address for TACACS+ packets.



NOTE: The Source Address box can accept either a hostname or an IP address.

9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.
10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.

11. Click **OK** to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server address 172.16.98.24
```
2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 secret Tacacssecret1
```
3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 source-address 10.0.0.1
```

Results From configuration mode, confirm your configuration by entering the **show system tacplus-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system tacplus-server
tacplus-server 172.16.98.24 {
  secret Tacacssecret1;
  source-address 10.0.0.1;
}
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See [“Example: Configuring Authentication Order” on page 230](#).
- Configure a user. See [“Example: Configuring New Users” on page 15](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 19](#).

Verification

Confirm that the configuration is working properly.

[Verifying the TACACS+ Server System Authentication Configuration](#)

Purpose Verify that the TACACS+ server has been configured for system authentication.

Action From operational mode, enter the **show system tacplus-server** command.

Related Documentation

- [Understanding User Authentication Methods on page 12](#)
- [Understanding User Accounts on page 6](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 222](#)
- [Understanding Login Classes on page 3](#)

[Example: Configuring Authentication Order](#)

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure authentication order.

- [Requirements on page 230](#)
- [Overview on page 230](#)
- [Configuration on page 230](#)
- [Verification on page 232](#)

Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
 - RADIUS
 - TACACS+
 - Local Password

If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.

5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure authentication order:

1. Add RADIUS authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order radius after password
```
2. Add TACACS+ authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order tacplus after radius
```

Results

From configuration mode, confirm your configuration by entering the **show system authentication-order** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system authentication-order
authentication-order [password, radius, tacplus];
```

If you are done configuring the device, enter **commit** from configuration mode.



NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 222](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 227](#).
- Configure a user. See [“Example: Configuring New Users” on page 15](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 19](#).

Verification

Confirm that the configuration is working properly.

Verifying the Authentication Order Configuration

| | |
|------------------------------|--|
| Purpose | Verify that the authentication order has been configured. |
| Action | From operational mode, enter the show system authentication-order command. |
| Related Documentation | <ul style="list-style-type: none">• Understanding User Authentication Methods on page 12• Understanding User Accounts on page 6• Understanding Login Classes on page 3 |

PART 2

Configuring Remote Access to an SRX Series Appliances

- [Configuring Secure Web Access on page 235](#)
- [Setting up USB Modems for Remote Management on page 243](#)
- [Configuring Telnet and SSH Access to an SRX Series Appliance on page 259](#)

CHAPTER 6

Configuring Secure Web Access

- [Secure Web Access Overview on page 235](#)
- [Generating an SSL Certificate Using the openssl Command on page 236](#)
- [Generating a Self-Signed SSL Certificate on page 236](#)
- [Manually Generating Self-Signed SSL Certificates on page 237](#)
- [Configuring Device Addresses on page 237](#)
- [Enabling Access Services on page 238](#)
- [Example: Configuring Secure Web Access on page 239](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 241](#)

Secure Web Access Overview

Supported Platforms [SRX Series, vSRX](#)

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

Related Documentation

- [Generating an SSL Certificate Using the openssl Command on page 236](#)
- [Generating a Self-Signed SSL Certificate on page 236](#)
- [Configuring Device Addresses on page 237](#)
- [Example: Configuring Secure Web Access on page 239](#)

Generating an SSL Certificate Using the openssl Command

Supported Platforms [SRX Series, vSRX](#)

To generate an SSL certificate using the **openssl** command:

1. Enter **openssl** in the CLI. The **openssl** command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.



NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the **openssl** command.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
```

Replace **filename** with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file **new.pem**.

```
cat new.pem
```

Copy the contents of this file for installing the SSL certificate.

Related Documentation

- [Secure Web Access Overview on page 235](#)

Generating a Self-Signed SSL Certificate

Supported Platforms [SRX Series, vSRX](#)

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

```
user@host> request system reboot
```

Reboot the system ? [yes,no] yes

3. Specify **system-generated-certificate** under HTTPS Web management.

[edit]

```
user@host# show system services web-management https
system-generated-certificate
```

Related
Documentation

- [Generating an SSL Certificate Using the openssl Command on page 236](#)

Manually Generating Self-Signed SSL Certificates

Supported Platforms [SRX Series, vSRX](#)

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:

```
root@host> request security pki generate-size 512 certificate-id certname
```

Generated key pair sslcert, key size 512 bits

```
root@host> request security pki local-certificate generate-self-signed certificate-id
cert-name email email domain-name domain-name ip-address ip-address subject
"DC= Domain name, CN= Common-Name, OU= Organizational-Unit-name, O=
Organization-Name, ST= state, C= Country"
```

Self-signed certificate generated and loaded successfully



NOTE: When generating the certificate, you must specify the subject, e-mail address, and either domain-name or ip-address.

3. Specify **local-certificate** under HTTPS Web management.

[edit]

```
root@host# show system services web-management https local-certificate certname
```

Related
Documentation

- [Generating a Self-Signed SSL Certificate on page 236](#)

Configuring Device Addresses

Supported Platforms [SRX Series, vSRX](#)

You can use the Management tab to configure IPv4 and loopback addresses on the device.

To configure IPv4 and loopback addresses:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Management** tab.
4. If you want to enable a loopback address for the device, enter an address and corresponding subnet mask in the **Loopback address** section.
5. If you want to enable an IPv4 address for the device, select **IPv4 address** and enter a corresponding management port, subnet mask, and default gateway.
6. Click **OK** to save the configuration or **Cancel** to clear it.

Related Documentation

- [Enabling Access Services on page 238](#)

Enabling Access Services

Supported Platforms [SRX Series, vSRX](#)

You can use the Services tab to specify the type of connections that users can make to the device. For instance, you can enable secure HTTPS sessions to the device or enable access to the Junos XML protocol XML scripting API.

To enable access services:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.
3. Select the **Services** tab.
4. If you want to enable users to create secure Telnet or secure SSH connections to the device, select **Enable Telnet** or **Enable SSH**.
5. If you want to enable access to the Junos XML protocol XML scripting API, select **Enable Junos XML protocol over clear text** or **Enable Junos XML protocol over SSL**. If you enable Junos XML protocol over SSL, select the certificate you want to use for encryption from the **Junos XML protocol certificate** drop-down list.
6. Select **Enable HTTP** if you want users to connect to device interfaces over an HTTP connection. Then specify the interfaces that should use the HTTP connection:
 - **Enable on all interfaces**—Select this option if you want to enable HTTP on all device interfaces.
 - **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTP on only some of the device interfaces.
7. If you want users to connect to device interfaces over a secure HTTPS connection, select **Enable HTTPS**. Then select which certificate you want to use to secure the

connection from the **HTTPS certificates** list and specify the interfaces that should use the HTTPS connection:

- **Enable on all interfaces**—Select this option if you want to enable HTTPS on all device interfaces.
- **Selected interfaces**—Use the arrow buttons to populate this list with individual interfaces if you want to enable HTTPS on only some of the device interfaces.

8. Click **OK** to save the configuration or **Cancel** to clear it.

To verify that Web access is enabled correctly, connect to the device using one of the following methods:

- For HTTP access—In your Web browser, type **http://URL** or **http://IP address**.
- For HTTPS access—In your Web browser, type **https://URL** or **https://IP address**.
- For SSL Junos XML protocol access—A Junos XML protocol client such as Junos Scope is required.

Related Documentation

- [Configuring Device Addresses on page 237](#)

Example: Configuring Secure Web Access

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure secure Web access on your device.

- [Requirements on page 239](#)
- [Overview on page 239](#)
- [Configuration on page 240](#)
- [Verification on page 241](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.



NOTE: You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.

Overview

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

```
[edit security]
user@host# set certificates local new load-key-file /var/tmp/new.pem
```

2. Enable HTTPS access and specify the SSL certificate and port.

```
[edit system]
user@host# set services web-management https local-certificate new port 8443
```

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

```
[edit]
user@host# show security
certificates {
  local {
    new {
      "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQC/C5UI4frNqbi
      qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY
      Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
      ... KYiFf4CbBBbjlMQJOHFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
      eIQBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
      CERTIFICATE-----\nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
      FADCBkTElMAkGAIUEBhMCdXMx\nCzAJBgNVBAGTAzAmNhMRlWEAYDVQQHEWlzdW5ue
      HB1YnMxDTALBgNVBAMTBGpucHlXJDAiBgkqhkiG9w0BCQEFWF5iaGFyZ2F2YUB
      fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying an SSL Certificate Configuration on page 241](#)
- [Verifying a Secure Access Configuration on page 241](#)

Verifying an SSL Certificate Configuration

Purpose Verify the SSL certificate configuration.

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

Verifying a Secure Access Configuration

Purpose Verify the secure access configuration.

Action From operational mode, enter the **show system services** command. The following sample output displays the sample values for secure Web access:

```
[edit]
user@host# show system services
web-management {
  http;
  https {
    port 8443;
    local-certificate new;
  }
}
```

- Related Documentation**
- [Secure Web Access Overview on page 235](#)
 - [Generating an SSL Certificate Using the openssl Command on page 236](#)
 - [Generating a Self-Signed SSL Certificate on page 236](#)
 - [Configuring Device Addresses on page 237](#)

Adding, Editing, and Deleting Certificates on the Device

Supported Platforms [SRX Series, vSRX](#)

You can use the Certificates tab to upload SSL certificates to the device, edit existing certificates on the device, or delete certificates from the device. You can use the certificates to secure HTTPS and Junos XML protocol sessions.

To add, edit, or delete a certificate:

1. In the J-Web user interface, select **Configure>System Properties>Management Access**.
2. Click **Edit**. The Edit Management Access dialog box appears.

3. Select the **Certificates** tab.
4. Choose one of the following options:
 - If you want to add a new certificate, click **Add**. The Add Certificate section is expanded.
 - If you want to edit the information for an existing certificate, select it and click **Edit**. The Edit Certificate section is expanded.
 - If you want to delete an existing certificate, select it and click **Delete**. (You can skip the remaining steps in this section.)
5. In the **Certificate Name** box, type a name—for example, **new**.
6. In the **Certificate content** box, paste the generated certificate and RSA private key.
7. Click **Save**.
8. Click **OK** to save the configuration or **Cancel** to clear it.

**Related
Documentation**

- [Generating an SSL Certificate Using the openssl Command on page 236](#)

CHAPTER 7

Setting up USB Modems for Remote Management

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)
- [Example: Configuring a USB Modem Interface on page 248](#)
- [Example: Configuring a Dialer Interface on page 250](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 254](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 256](#)
- [Connecting to the Device Remotely on page 257](#)
- [Modifying USB Modem Initialization Commands on page 257](#)
- [Resetting USB Modems on page 258](#)

USB Modem Interface Overview

Supported Platforms [SRX300, SRX320, SRX340](#)

Juniper Networks devices support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

You can configure your device to fail over to a USB modem connection when the primary Internet connection experiences interruption.

A USB modem connects to a device through modem interfaces that you configure. The device applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the device and the modem at the user end of the network.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.



NOTE: Low-latency traffic such as VoIP traffic is not supported over USB modem connections.



NOTE: We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity:

- A physical interface which uses the naming convention **umd0**. The device creates this interface when a USB modem is connected to the USB port.
- A logical interface called the dialer interface. You use the dialer interface, **dln**, to configure dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP). You can configure multiple dialer interfaces for different functions on the device. After configuring the dialer interface, you must configure a backup method such as a dialer backup, a dialer filter, or a dialer watch.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface. Dialer pool priority has a range from 1 to 255, with 1 designating the lowest priority interfaces and 255 designating the highest priority interfaces.

Dialer Interface Rules

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- The dialer interface cannot be configured as a constituent link in a multilink bundle.
- The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
 - As a backup interface—for one primary interface
 - As a dialer filter
 - As a dialer watch interface

The backup dialer interfaces are activated only when the primary interface fails. USB modem backup connectivity is supported on all interfaces except `lsq-0/0/0`.

The dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed. You define an interesting packet using the dialer filter feature of the device. To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route. If the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

How the Device Initializes USB Modems

When you connect the USB modem to the USB port on the device, the device applies the modem AT commands configured in the **init-command-string** command to the initialization commands on the modem.

If you do not configure modem AT commands for the **init-command-string** command, the device applies the following default sequence of initialization commands to the modem: **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. [Table 7 on page 245](#) describes the commands. For more information about these commands, see the documentation for your modem.

Table 7: Default Modem Initialization Commands

| Modem Command | Description |
|----------------|--|
| AT | Attention. Informs the modem that a command follows. |
| S7=45 | Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call. |
| S0=0 | Disables the auto answer feature, whereby the modem automatically answers calls. |
| V1 | Displays result codes as words. |
| &C1 | Disables reset of the modem when it loses the carrier signal. |
| E0 | Disables the display on the local terminal of commands issued to the modem from the local terminal. |
| Q0 | Enables the display of result codes. |
| &Q8 | Enables Microcom Networking Protocol (MNP) error control mode. |
| %C0 | Disables data compression. |

When the device applies the modem AT commands in the **init-command-string** command or the default sequence of initialization commands to the modem, it compares them to the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include **S0=0** and the device's **init-command-string** command includes **S0=2**, the device applies **S0=2**.
- If the initialization commands on the modem do not include a command in the device's **init-command-string** command, the device adds it. For example, if the **init-command-string** command includes the command **L2**, but the modem commands do not include it, the device adds **L2** to the initialization commands configured on the modem.

**Related
Documentation**

- [USB Modem Configuration Overview on page 246](#)
- [Example: Configuring a USB Modem Interface on page 248](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 254](#)

USB Modem Configuration Overview

Supported Platforms [SRX300, SRX320, SRX340](#)

Before you begin:

1. Install device hardware. For more information, see the Getting Started Guide for your device.
2. Establish basic connectivity. For more information, see the Getting Started Guide for your device.
3. Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637 (<http://www.usr.com/>).
4. Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
5. Connect the USB modem to the device's USB port.



NOTE: When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

- a. Plug the modem into the USB port.
- b. Connect the modem to your telephone network.

Suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. This example shows you how to establish a backup

connection between the branch office and head office routers. See [Table 8 on page 247](#) for a summarized description of the procedure.

Table 8: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity

| Router Location | Configuration Requirement | Procedure |
|-----------------|---|---|
| Branch Office | Configure the logical dialer interface on the branch office router for USB modem dial backup. | To configure the logical dialer interface, see “Example: Configuring a USB Modem Interface” on page 248 . |
| | Configure the dialer interface dl0 on the branch office router using one of the following backup methods: <ul style="list-style-type: none"> Configure the dialer interface dl0 as the backup interface on the branch office router's primary T1 interface t1-1/0/0. Configure a dialer filter on the branch office router's dialer interface. Configure a dialer watch on the branch office router's dialer interface. | Configure the dialer interface using one of the following backup methods: <ul style="list-style-type: none"> To configure dl0 as a backup for t1-1/0/0 see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup. To configure a dialer filter on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup. To configure a dialer watch on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup. |
| Head Office | Configure dial-in on the dialer interface dl0 on the head office router. | To configure dial-in on the head office router, see “Example: Configuring a Dialer Interface for USB Modem Dial-In” on page 254 . |

If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085321091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

See [Table 9 on page 247](#) for a list of available incoming map options.

Table 9: Incoming Map Options

| Option | Description |
|-------------------|---|
| accept-all | Dialer interface accepts all incoming calls. You can configure the accept-all option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the accept-all option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces. |

Table 9: Incoming Map Options (*continued*)

| Option | Description |
|---------------|---|
| caller | <p>Dialer interface accepts calls from a specific caller ID. You can configure a maximum of 15 caller IDs per dialer interface.</p> <p>The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.</p> |

You configure dialer interfaces to support PAP. PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair are repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

**Related
Documentation**

- [USB Modem Interface Overview on page 243](#)
- [Example: Configuring a USB Modem Interface on page 248](#)

Example: Configuring a USB Modem Interface

Supported Platforms [SRX300, SRX320, SRX340](#)

This example shows how to configure a USB modem interface for dial backup.

- [Requirements on page 248](#)
- [Overview on page 248](#)
- [Configuration on page 248](#)
- [Verification on page 249](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you create an interface called as umd0 for USB modem connectivity and set the dialer pool priority to 25. You also configure a modem initialization string to autoanswer after a specified number of rings. The default modem initialization string is **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. The modem command **S0=0** disables the modem from autoanswering the calls. Finally, you set the modem to act as a dial-in WAN backup interface.

Configuration

**CLI Quick
Configuration**

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

```
set interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
set modem-options init-command-string "ATSO=2 \n" dialin routable
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a USB modem interface for dial backup:

1. Create an interface.

```
[edit]
user@host# edit interfaces umd0
```

2. Set the dialer options and priority.

```
[edit interfaces umd0]
user@host# set dialer-options pool usb-modem-dialer-pool priority 25
```

3. Specify the modem options.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "ATSO=2 \n"
```

4. Set the modem to act as a dial-in WAN backup interface.

```
[edit interfaces umd0]
user@host# set modem-options dialin routable
```

Results From configuration mode, confirm your configuration by entering the **show interface umd0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interface umd0
modem-options {
  init-command-string "ATSO=2 \n";
  dialin routable;
}
dialer-options {
  pool usb-modem-dialer-pool priority 25;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose Verify a USB modem interface for dial backup.

Action From configuration mode, enter the **show interfaces umd0 extensive** command. The output shows a summary of interface information and displays the modem status.

```
Physical interface:  umd0, Enabled, Physical link is Up
Interface index:    64, SNMP ifIndex: 33, Generation: 1
Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
Clocking: Unspecified, Speed: MODEM
Device flags      : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags       : None
Hold-times       : Up 0 ms, Down 0 ms
Last flapped     : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes  :          21672
  Output bytes :          22558
  Input packets:           1782
  Output packets:          1832
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
  Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
MODEM status:
  Modem type                : LT V.92 1.0 MT5634ZBA-USB-V92 Data/Fax Modem

(Dual Config) Version 2.27m
  Initialization command string : ATSO=2
  Initialization status         : Ok
  Call status                   : Connected to 4085551515
  Call duration                 : 13429 seconds
  Call direction               : Dialin
  Baud rate                    : 33600 bps
  Most recent error code       : NO CARRIER

Logical interface umd0.0 (Index 2) (SNMP ifIndex 34) (Generation 1)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP-Subordinate
```

- Related Documentation**
- [USB Modem Configuration Overview on page 246](#)
 - [USB Modem Interface Overview on page 243](#)
 - [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 254](#)

Example: Configuring a Dialer Interface

Supported Platforms [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [vSRX](#)

This example shows how to configure a logical dialer interface for the device.

- [Requirements on page 251](#)
- [Overview on page 251](#)
- [Configuration on page 251](#)
- [Verification on page 253](#)

Requirements

Before you begin:

- Install device hardware and establish basic connectivity. See the Getting Started Guide for your device.
- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637, from US Robotics (<http://www.usr.com/>).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the device.
- Order a PSTN line from your telecommunications service provider. Contact your service provider.

Overview

In this example, you configure a logical dialer interface called `dl0` to establish USB connectivity. You can configure multiple dialer interfaces for different functions on the device. You add a description to differentiate among different dialer interfaces. For example, this modem is called `USB-modem-remote-management`. Configure PPP encapsulation and set the logical unit as 0. You then specify the name of the dialer pool as `usb-modem-dialer-pool` and set the source and destination IP addresses as `172.20.10.2`, and `172.20.10.1`, respectively.



NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.



NOTE: If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.

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, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces dl0 description USB-modem-remote-management encapsulation ppp
set interfaces dl0 unit 0 dialer-options pool usb-modem-dialer-pool
set interfaces dl0 unit 0 family inet address 172.20.10.2 destination 172.20.10.1
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a logical dialer interface for the device:

1. Create an interface.

```
[edit]
user@host# set interfaces dl0
```

2. Add a description and configure PPP encapsulation.

```
[edit interfaces dl0]
user@host# set description USB-modem-remote-management
user@host# set encapsulation ppp
```

3. Create the logical unit.



NOTE: The logical unit number must be 0.

```
[edit interfaces dl0]
user@host# set unit 0
```

4. Configure the name of the dialer pool to use for USB modem connectivity.

```
[edit interfaces dl0 unit 0]
user@host# set dialer-options pool usb-modem-dialer-pool
```

5. Configure source and destination IP addresses for the dialer interface.

```
[edit interfaces dl0 unit 0]
user@host# set family inet address 172.20.10.2 destination 172.20.10.1
```

Results From configuration mode, confirm your configuration by entering the **show interfaces dl0** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces dl0
description USB-modem-remote-management;
encapsulation ppp;
unit 0 {
  family inet {
    address 172.20.10.2/32 {
      destination 172.20.10.1;
    }
  }
  dialer-options {
    pool usb-modem-dialer-pool;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying a Dialer Interface

Purpose Verify that the dialer interface has been configured.

Action From configuration mode, enter the **show interfaces d10 extensive** command. The output shows a summary of dialer interface information.

```
Physical interface: d10, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
  Device flags      : Present Running
  Interface flags:  SNMP-Traps
  Link type        : Full-Duplex
  Link flags       : Keepalives
  Physical info    : Unspecified
  Hold-times       : Up 0 ms, Down 0 ms
  Current address:  Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped     : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes  :                13859                0 bps
    Output bytes :                   0                0 bps
    Input packets:                 317                0 pps
    Output packets:                  0                0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
  Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0

Logical interface d10.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
  Description: USB-modem-remote-management
  Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
  Dialer:
    State: Active, Dial pool: usb-modem-dialer-pool
    Dial strings: 220
    Subordinate interfaces: umd0 (Index 64)
    Activation delay: 0, Deactivation delay: 0
    Initial route check delay: 120
    Redial delay: 3
    Callback wait period: 5
    Load threshold: 0, Load interval: 60
  Bandwidth: 115200
  Traffic statistics:
    Input bytes  :                24839
    Output bytes :                17792
    Input packets:                 489
    Output packets:                 340
  Local statistics:
    Input bytes  :                10980
    Output bytes :                17792
```

```
Input packets:          172
Output packets:         340
Transit statistics:
Input bytes  :          13859          0 bps
Output bytes :           0          0 bps
Input packets:         317          0 pps
Output packets:         0          0 pps
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mp1s: Not-configured
CHAP state: Success
  Protocol inet, MTU: 1500, Generation: 136, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 172.20.10.1, Local: 172.20.10.2, Broadcast: Unspecified,
  Generation: 134
```

**Related
Documentation**

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)
- [Example: Configuring a USB Modem Interface on page 248](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 254](#)

Example: Configuring a Dialer Interface for USB Modem Dial-In

Supported Platforms [SRX300, SRX320, SRX340](#)

This example shows how to configure a dialer interface for USB modem dial-in.

- [Requirements on page 254](#)
- [Overview on page 254](#)
- [Configuration on page 255](#)
- [Verification on page 255](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the system matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the system performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID

configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

You can configure the following incoming map options for the dialer interface:

- **accept-all**—Dialer interface accepts all incoming calls.

You can configure the **accept-all** option for only one of the dialer interfaces associated with a USB modem physical interface. The device uses the dialer interface with the **accept-all** option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

- **caller**—Dialer interface accepts calls from a specific caller ID—for example, **4085550115**. You can configure a maximum of 15 caller IDs per dialer interface.

The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.

In this example, you configure the incoming map option as caller 4085550115 for dialer interface d10.

Configuration

CLI Quick Configuration

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

```
set interfaces d10 unit 0 dialer-options incoming-map caller 4085550115
```

Step-by-Step Procedure

To configure a dialer interface for USB modem dial-in:

1. Select a dialer interface.

```
[edit]
user@host# edit interfaces d10
```
2. Configure the incoming map options.

```
[edit]
user@host# edit unit 0 dialer-options incoming-map caller 4085551515
```
3. If you are done configuring the device, commit the configuration.

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

Verification

To verify the configuration is working properly, enter the **show interface d10** command.

Related Documentation

- [USB Modem Configuration Overview on page 246](#)
- [Example: Configuring a USB Modem Interface on page 248](#)

Configuring a Dial-Up Modem Connection Remotely

Supported Platforms [SRX Series, vSRX](#)

To remotely connect to the USB modem connected to the USB port on the device, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection remotely:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. Connect the modem to your telephone network.
3. On the PC or laptop computer, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
4. Click **Create a new connection**. The New Connection Wizard appears.
5. Click **Next**. The New Connection Wizard: Network Connection Type page appears.
6. Select **Connect to the network at my workplace**, and then click **Next**.

The New Connection Wizard: Network Connection page appears.

7. Select **Dial-up connection**, and then click **Next**. The New Connection Wizard: Connection Name page appears.
8. In the Company Name box, type the dial-up connection name, for example **USB-modem-connect**. Then, click **Next**. The New Connection Wizard: Phone Number to Dial page appears.
9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the device end.
10. Click **Next** twice, and then click **Finish**. The Connect USB-modem-connect page appears.
11. If CHAP is configured on the dialer interface used for the USB modem interface at the device end, type the username and password configured in the CHAP configuration in the User name and Password boxes.
12. Click **Properties**. The USB-modem-connect Properties page appears.
13. In the Networking tab, select **Internet Protocol (TCP/IP)**, and then click **Properties**. The Internet Protocol (TCP/IP) Properties page appears.
14. Click **Advanced**. The Advanced TCP/IP Settings page appears.
15. Clear the **Use IP header compression** check box.

Related Documentation

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)

- [Connecting to the Device Remotely on page 257](#)

Connecting to the Device Remotely

Supported Platforms [SRX Series, vSRX](#)

To remotely connect to the device through a USB modem connected to the USB port on the device:

1. On the PC or laptop computer at your remote location, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.
2. Double-click the **USB-modem-connect** dial-up connection. The Connect USB-modem-connect page appears.
3. Click **Dial** to connect to the Juniper Networks device.

When the connection is complete, you can use Telnet or SSH to connect to the device.

Related Documentation

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 256](#)

Modifying USB Modem Initialization Commands

Supported Platforms [SRX300, SRX320, SRX340, SRX345](#)



NOTE: These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands.

You can use the CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.



NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.

You can configure the following modem AT commands to initialize the USB modem:

- The command **S0=2** configures the modem to automatically answer calls on the second ring.
- The command **L2** configures medium speaker volume on the modem.

You can insert spaces between commands.

When you configure modem commands in the CLI configuration editor, you must follow these conventions:

- Use the newline character `\n` to indicate the end of a command sequence.
- Enclose the command string in double quotation marks.

You can override the value of the **S0=0** command in the initialization sequence configured on the modem and add the **L2** command.

To modify the initialization commands on a USB modem:

1. Configure the modem AT commands to initialize the USB modem.

```
[edit interfaces umd0]
```

```
user@host# set modem-options init-command-string "AT S0=2 L2 \n"
```

2. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)
- [Resetting USB Modems on page 258](#)

Resetting USB Modems

Supported Platforms [SRX300, SRX320, SRX340, SRX345](#)

If the USB modem does not respond, you can reset the modem.



.....
CAUTION: If you reset the modem when a call is in progress, the call is terminated.
.....

To reset the USB modem, in operational mode, enter the following command:

```
user@host> request interface modem reset umd0
```

**Related
Documentation**

- [USB Modem Interface Overview on page 243](#)
- [USB Modem Configuration Overview on page 246](#)
- [Modifying USB Modem Initialization Commands on page 257](#)

CHAPTER 8

Configuring Telnet and SSH Access to an SRX Series Appliance

- [Securing the Console Port Configuration Overview on page 259](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 260](#)
- [Configuring Reverse Telnet and Reverse SSH on page 261](#)
- [Example: Controlling Management Access on SRX Series Devices on page 262](#)
- [Example: Configuring a Filter to Block Telnet and SSH Access on page 265](#)
- [The telnet Command on page 270](#)
- [The ssh Command on page 271](#)
- [Configuring Outbound SSH Service on page 272](#)

Securing the Console Port Configuration Overview

Supported Platforms [SRX Series, vSRX](#)

You can use the console port on the device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:

- Log out of the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to the console. This action prevents a non-root user from performing password recovery operation using the console.
- Disable the console port. We recommend disabling the console port to prevent unauthorized access to the device, especially when the device is used as customer premises equipment (CPE) and is forwarding sensitive traffic.



NOTE: It is not always possible to disable the console port, because console access is important during operations such as software upgrades.

To secure the console port:

1. Do one of the following:

- Disable the console port. Enter

```
[edit system ports console]  
user@host# set disable
```

- Disable root login connections to the console. Enter

```
[edit system ports console]  
user@host# set insecure
```



NOTE: After configuring the console port as insecure, if a user tries to perform password recovery operation by booting in single-user mode, the device will prompt for the root password. This way, the user will be unable to log in to single-user mode for password recovery unless the root password is known.

- Log out the console session when the serial cable connected to the console port is unplugged. Enter

```
[edit system ports console]  
user@host# set log-out-on-disconnect
```

2. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [The telnet Command on page 270](#)
- [The ssh Command on page 271](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 260](#)
- [Configuring Reverse Telnet and Reverse SSH on page 261](#)

Configuring Password Retry Limits for Telnet and SSH Access

Supported Platforms [SRX Series, vSRX](#)

To prevent brute force and dictionary attacks, the device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.

For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.

- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from

disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
- Enforce a minimum session time of 40 seconds during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is **10**, but you can set a number from 1 through **10**.

```
[edit system login retry-options]  
user@host# set tries-before-disconnect 4
```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is **2**, but you can specify a value from 1 through **3**.

```
[edit system login retry-options]  
user@host# set backoff-threshold 2
```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of **5** seconds, but you can specify a value from **5** through **10** seconds.

```
[edit system login retry-options]  
user@host# set backoff-factor 5
```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is **20** seconds, but you can specify an interval from **20** through **60** seconds.

```
[edit system login retry-options]  
user@host# set minimum-time 40
```

5. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [The telnet Command on page 270](#)
- [The ssh Command on page 271](#)
- [Configuring Reverse Telnet and Reverse SSH on page 261](#)

Configuring Reverse Telnet and Reverse SSH

Supported Platforms [SRX1500](#), [SRX5400](#), [SRX5600](#), [SRX5800](#)

To configure reverse telnet and reverse ssh:

1. Enable reverse telnet.

```
[edit]
user@host# set system services reverse telnet
```

2. Specify the port to be used for reverse telnet. If you do not specify a port, 2900 is the default port that is used.

```
[edit]
user@host# set system services reverse telnet port 5000
```

3. Enable reverse ssh to encrypt the connection between the device and the client.

```
[edit]
user@host# set system services reverse ssh
```

4. Specify the port for reverse ssh. If you do not specify a port, 2901 is the default port that is used.

```
[edit]
user@host# set system services reverse ssh port 6000
```

5. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [The telnet Command on page 270](#)
- [The ssh Command on page 271](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 260](#)

Example: Controlling Management Access on SRX Series Devices

Supported Platforms [SRX Series, vSRX](#)

This example shows how to control management access on SRX Series devices.

- [Requirements on page 262](#)
- [Overview on page 262](#)
- [Configuration on page 263](#)
- [Verification on page 265](#)

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

By default, any host on the trusted interface can manage a security device. To limit the IP addresses that can manage a device, you can configure a firewall filter to deny all, with the exception of the IP address or addresses to which you want to grant management access. This example shows how to limit management access to a specific IP addresses to allow it to manage SRX Series devices.

Configuration

- [Configuring an IP Address List to Restrict Management Access to a Device on page 263](#)

Configuring an IP Address List to Restrict Management Access to a Device

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set policy-options prefix-list manager-ip 192.168.4.254/32
set policy-options prefix-list manager-ip 10.0.0.0/8
set firewall filter manager-ip term block_non_manager from source-address 0.0.0.0/0
set firewall filter manager-ip term block_non_manager from source-prefix-list manager-ip
except
set firewall filter manager-ip term block_non_manager from protocol tcp
set firewall filter manager-ip term block_non_manager from destination-port ssh
set firewall filter manager-ip term block_non_manager from destination-port https
set firewall filter manager-ip term block_non_manager from destination-port telnet
set firewall filter manager-ip term block_non_manager from destination-port http
set firewall filter manager-ip term block_non_manager then discard
set firewall filter manager-ip term accept_everything_else then accept
set interfaces lo0 unit 0 family inet filter input manager-ip
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Define a set of host addresses, called "manager-ip", that are allowed to manage the device.

```
[edit policy-options]
user@host# set prefix-list manager-ip 192.168.4.254/32
user@host# set prefix-list manager-ip 10.0.0.0/8
```



NOTE: The configured list is referenced in the actual filter, where you can change your defined set of addresses.

2. Configure a firewall filter to deny traffic from all IP addresses except the IP addresses defined in the "manager-ip" list. Management traffic that uses any of the listed destination ports is rejected when the traffic comes from an address in the list.

```
[edit firewall filter]
user@host# set manager-ip term block_non_manager from source-address 0.0.0.0/0
user@host# set manager-ip term block_non_manager from source-prefix-list
manager-ip except
user@host# set manager-ip term block_non_manager from protocol tcp
user@host# set manager-ip term block_non_manager from destination-port ssh
user@host# set manager-ip term block_non_manager from destination-port https
user@host# set manager-ip term block_non_manager from destination-port telnet
user@host# set manager-ip term block_non_manager from destination-port http
```

```

user@host# set manager-ip term block_non_manager then discard
user@host# set manager-ip term accept_everything_else then accept

```

3. Apply stateless firewall filters to the loopback interface to filter the packets originating from the hosts to which you are granting management access.

```

[edit interfaces lo0 unit 0 ]
user@host# set family inet filter input manager-ip

```



NOTE: This configuration applies to traffic that terminates at the device. For traffic that terminates at the device interface (such as IPsec, OSPF, RIP, or BGP), you must also include the management IP addresses in the manager-ip prefix-list.

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

```

user@host# show configuration policy-options
  prefix-list manager-ip {
    10.0.0.0/8;
    192.168.4.254/32;
  }

user@host# show configuration firewall
  filter manager-ip {
    term block_non_manager {
      from {
        source-address {
          0.0.0.0/0;
        }
        source-prefix-list {
          manager-ip except;
        }
        protocol tcp;
        destination-port [ ssh https telnet http ];
      }
      then {
        discard;
      }
    }
    term accept_everything_else {
      then accept;
    }
  }

user@host# show configuration interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input manager-ip;
      }
    }
  }
}

```

```
    }  
  }  
}  
  
user@host# show configuration interfaces lo0  
unit 0 {  
  family inet {  
    filter {  
      input manager-ip;  
    }  
  }  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Interfaces

Purpose Verify if the interfaces are configured correctly.

Action From operational mode, enter the following commands:

- `show policy-options`
- `show firewall`
- `show interfaces`

Related Documentation

- [Securing the Console Port Configuration Overview on page 259](#)

Example: Configuring a Filter to Block Telnet and SSH Access

Supported Platforms [SRX Series, vSRX](#)

- [Requirements on page 265](#)
- [Overview on page 266](#)
- [Configuration on page 266](#)
- [Verification on page 268](#)

Requirements

You must have access to a remote host that has network connectivity with this device.

Overview

In this example, you create an IPv4 stateless firewall filter that logs and rejects Telnet or SSH access packets unless the packet is destined for or originates from the 192.168.1.0/24 subnet.

- To match packets destined for or originating from the **address 192.168.1.0/24** subnet, you use the **address 192.168.1.0/24** IPv4 match condition.
- To match packets destined for or originating from a TCP port, Telnet port, or SSH port, you use the **protocol tcp**, **port telnet**, and **telnet ssh** IPv4 match conditions.

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:

- [Configure the Stateless Firewall Filter on page 266](#)
- [Apply the Firewall Filter to the Loopback Interface on page 267](#)
- [Confirm and Commit Your Candidate Configuration on page 267](#)

CLI Quick Configuration

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

```
set firewall family inet filter local_acl term terminal_access from address 192.168.1.0/24
set firewall family inet filter local_acl term terminal_access from protocol tcp
set firewall family inet filter local_acl term terminal_access from port ssh
set firewall family inet filter local_acl term terminal_access from port telnet
set firewall family inet filter local_acl term terminal_access then accept
set firewall family inet filter local_acl term terminal_access_denied from protocol tcp
set firewall family inet filter local_acl term terminal_access_denied from port ssh
set firewall family inet filter local_acl term terminal_access_denied from port telnet
set firewall family inet filter local_acl term terminal_access_denied then log
set firewall family inet filter local_acl term terminal_access_denied then reject
set firewall family inet filter local_acl term default-term then accept
set interfaces lo0 unit 0 family inet filter input local_acl
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Configure the Stateless Firewall Filter

Step-by-Step Procedure

To configure the stateless firewall filter that selectively blocks Telnet and SSH access:

1. Create the stateless firewall filter **local_acl**.

```
[edit]
```

```
user@myhost# edit firewall family inet filter local_acl
```

2. Define the filter term **terminal_access**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access from address 192.168.1.0/24
user@myhost# set term terminal_access from protocol tcp
user@myhost# set term terminal_access from port ssh
user@myhost# set term terminal_access from port telnet
user@myhost# set term terminal_access then accept
```

3. Define the filter term **terminal_access_denied**.

```
[edit firewall family inet filter local_acl]
user@myhost# set term terminal_access_denied from protocol tcp
user@myhost# set term terminal_access_denied from port ssh
user@myhost# set term terminal_access_denied from port telnet
user@myhost# set term terminal_access_denied then log
user@myhost# set term terminal_access_denied then reject
user@myhost# set term default-term then accept
```

Apply the Firewall Filter to the Loopback Interface

Step-by-Step Procedure

- To apply the firewall filter to the loopback interface:

```
[edit]
user@myhost# set interfaces lo0 unit 0 family inet filter input local_acl
user@myhost# set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Confirm and Commit Your Candidate Configuration

Step-by-Step Procedure

To confirm and then commit your candidate configuration:

1. Confirm the configuration of the stateless firewall filter by entering the **show firewall** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show firewall
family inet {
  filter local_acl {
    term terminal_access {
      from {
        address {
          192.168.1.0/24;
        }
        protocol tcp;
        port [ssh telnet];
      }
      then accept;
    }
    term terminal_access_denied {
      from {
        protocol tcp;
        port [ssh telnet];
      }
      then {
        log;
      }
    }
  }
}
```

```
        reject;
      }
    }
    term default-term {
      then accept;
    }
  }
}
```

2. Confirm the configuration of the interface by entering the **show interfaces** configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input local_acl;
      }
      address 127.0.0.1/32;
    }
  }
}
```

3. If you are done configuring the device, commit your candidate configuration.

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

Verification

Confirm that the configuration is working properly.

- [Verifying Accepted Packets on page 268](#)
- [Verifying Logged and Rejected Packets on page 269](#)

Verifying Accepted Packets

Purpose Verify that the actions of the firewall filter terms are taken.

- Action**
1. Clear the firewall log on your router or switch.

```
user@myhost> clear firewall log
```

2. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **ssh hostname** command to verify that you can log in to the device using only SSH. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-A> ssh myhost
user@myhosts's password:
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
```

```
% cli
user@myhost>
```

3. From a host at an IP address *within* the 192.168.1.0/24 subnet, use the **telnet *hostname*** command to verify that you can log in to your router or switch using only Telnet. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-A> telnet myhost
Trying 192.168.249.71...
Connected to myhost-fxp0.acme.net.
Escape character is '^]'.

host (ttyp0)

login: user
Password:

--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC

% cli
user@myhost>
```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

```
user@myhost> show firewall log
```

Verifying Logged and Rejected Packets

Purpose Verify that the actions of the firewall filter terms are taken.

- Action** 1. Clear the firewall log on your router or switch.

```
user@myhost> clear firewall log
```

2. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **ssh hostname** command to verify that you cannot log in to the device using only SSH. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-B ssh myhost
ssh: connect to host sugar port 22: Connection refused
--- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
%
```

3. From a host at an IP address *outside of* the 192.168.1.0/24 subnet, use the **telnet hostname** command to verify that you can log in to the device using only Telnet. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the PFE.

```
user@host-B> telnet myhost
Trying 192.168.249.71...
telnet: connect to address 192.168.187.3: Connection refused
telnet: Unable to connect to remote host
%
```

4. Use the **show firewall log** command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

```
user@myhost> show firewall log
```

| Time | Filter | Action | Interface | Protocol | Src Addr | Dest Addr |
|----------|-----------|--------|-----------|----------|---------------|---------------|
| 18:41:25 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| 18:41:25 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| 18:41:25 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| ... | | | | | | |
| 18:43:06 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| 18:43:06 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| 18:43:06 | local_acl | R | fxp0.0 | TCP | 192.168.187.5 | 192.168.187.1 |
| ... | | | | | | |

- Related Documentation**
- [Example: Controlling Management Access on SRX Series Devices on page 262](#)

The telnet Command

Supported Platforms [SRX Series, vSRX](#)

You can use the CLI **telnet** command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name>
<no-resolve> <port port> <routing-instance routing-instance-name> <source address>
```



NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent Telnet sessions is as follows:

| SRX300 | SRX320 | SRX340 | SRX345 | SRX1500 |
|--------|--------|--------|--------|---------|
| 3 | 3 | 3 | 5 | 5 |

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter **quit**.

Table 10 on page 271 describes the **telnet** command options.

Table 10: CLI telnet Command Options

| Option | Description |
|--|---|
| 8bit | Use an 8-bit data path. |
| bypass-routing | Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. |
| host | Open a Telnet session to the specified hostname or IP address. |
| inet | Force the Telnet session to an IPv4 destination. |
| interface <i>source-interface</i> | Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used. |
| no-resolve | Suppress the display of symbolic names. |
| port <i>port</i> | Specify the port number or service name on the host. |
| routing-instance <i>routing-instance-name</i> | Use the specified routing instance for the Telnet session. |
| source <i>address</i> | Use the specified source address for the Telnet session. |

Related Documentation

- [The ssh Command on page 271](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 260](#)
- [Configuring Reverse Telnet and Reverse SSH on page 261](#)

The ssh Command

Supported Platforms [SRX Series, vSRX](#)

You can use the CLI **ssh** command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```



NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent SSH sessions is as follows:

| SRX300 | SRX320 | SRX340 | SRX345 | SRX1500 |
|--------|--------|--------|--------|---------|
| 3 | 3 | 3 | 5 | 5 |

Table 11 on page 272 describes the **ssh** command options.

Table 11: CLI ssh Command Options

| Option | Description |
|---|--|
| bypass-routing | Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. |
| host | Open an SSH connection to the specified hostname or IP address. |
| inet | Force the SSH connection to an IPv4 destination. |
| interface source-interface | Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used. |
| routing-instance routing-instance-name | Use the specified routing instance for the SSH connection. |
| source address | Use the specified source address for the SSH connection. |
| v1 | Force SSH to use version 1 for the connection. |
| v2 | Force SSH to use version 2 for the connection. |

Related Documentation

- [The telnet Command on page 270](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 260](#)
- [Configuring Reverse Telnet and Reverse SSH on page 261](#)

Configuring Outbound SSH Service

Supported Platforms [SRX Series](#)

You can configure a device running the Junos OS to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate

the connection (for example, if the device is behind a firewall). The **outbound-ssh** command instructs the device to create a TCP/IP connection with the client management application and to forward the identity of the device. Once the connection is established, the management application acts as the client and initiates the SSH sequence, and the device acts as the server and authenticates the client.



NOTE: There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the device begins to initiate an outbound SSH connection based on the committed configuration. The device repeatedly attempts to create this connection until successful. If the connection between the device and the client management application is dropped, the device again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the device for outbound SSH connections, include the **outbound-ssh** statement at the **[edit system services]** hierarchy level:

[edit system services outbound-ssh]

The following topics describe the tasks for configuring the outbound SSH service:

- [Configuring the Device Identifier for Outbound SSH Connections on page 273](#)
- [Sending the Public SSH Host Key to the Outbound SSH Client on page 274](#)
- [Configuring Keepalive Messages for Outbound SSH Connections on page 275](#)
- [Configuring a New Outbound SSH Connection on page 275](#)
- [Configuring the Outbound SSH Client to Accept NETCONF as an Available Service on page 275](#)
- [Configuring Outbound SSH Clients on page 275](#)

Configuring the Device Identifier for Outbound SSH Connections

Each time the device establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the device to the management client. Within this transmission is the value of **device-id**.

To configure the device identifier of the device, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

Sending the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the **device-id** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]  
device-id device-id;
```

The initiation sequence when **secret** is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n  
MSG-VER: V1\r\n  
DEVICE-ID: <device-id>\r\n
```

During the initialization of an SSH connection, the client authenticates the identity of the device using the public SSH host key of the device. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the device. When you configure the **secret** statement, the device passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the device establishes an outbound SSH connection, the device communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the **secret** statement. The value of the **secret** statement is shared between the device and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the device identified by the **device-id** statement.

Using the **secret** statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.



NOTE: Including the **secret** statement means that the device sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that device. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router's or switch's public SSH host key when the device connects to the client, include the **secret** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]  
secret password;
```

The following message is sent by the device when the **secret** attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-hot-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router's or switch's public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the device using its copy of the router's or switch's public host SSH key as part of that sequence. The device authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the device to send SSH protocol keepalive messages to the client application, configure the **keep-alive** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
    retry number;
    timeout seconds;
}
```

Configuring a New Outbound SSH Connection

When disconnected, the device begins to initiate a new outbound SSH connection. To specify how the device reconnects to the server after a connection is dropped, include the **reconnect-strategy** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See [“Configuring Keepalive Messages for Outbound SSH Connections” on page 275](#).

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

To configure the application to accept NETCONF as an available service, include the **services netconf** statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
    netconf;
}
```

Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the **[edit system services outbound-ssh client *client-id*]** hierarchy level:

```
[edit system services outbound-ssh client client-id]
```

```
address address {  
    retry number;  
    timeout seconds;  
    port port-number;  
}
```



NOTE: Outbound SSH connections support IPv4 and IPv6 address formats.

PART 3

Configuring DNS

- [Configuring DNS Server Caching, DNSSEC, and DNS Proxy on page 279](#)

CHAPTER 9

Configuring DNS Server Caching, DNSSEC, and DNS Proxy

- [DNS Overview on page 279](#)
- [Example: Configuring the TTL Value for DNS Server Caching on page 280](#)
- [DNSSEC Overview on page 281](#)
- [Example: Configuring DNSSEC on page 281](#)
- [Example: Configuring Keys for DNSSEC on page 282](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 282](#)
- [DNS Proxy Overview on page 284](#)
- [Configuring the Device as a DNS Proxy on page 289](#)

DNS Overview

Supported Platforms [SRX Series, vSRX](#)

A Domain Name System (DNS) is a distributed hierarchical system that converts hostnames to IP addresses. The DNS is divided into sections called zones. Each zone has name servers that respond to the queries belonging to their zones.

This topic includes the following sections:

- [DNS Components on page 279](#)
- [DNS Server Caching on page 280](#)

DNS Components

DNS includes three main components:

- **DNS resolver** — Resides on the client side of the DNS. When a user sends a hostname request, the resolver sends a DNS query request to the name servers to request the hostname's IP address.
- **Name servers** — Processes the DNS query requests received from the DNS resolver and returns the IP address to the resolver.
- **Resource records** — Data elements that define the basic structure and content of the DNS.

DNS Server Caching

DNS name servers are responsible for providing the hostname IP address to users. The TTL field in the resource record defines the period for which DNS query results are cached. When the TTL value expires, the name server sends a fresh DNS query and updates the cache.

Related Documentation

- [Example: Configuring the TTL Value for DNS Server Caching on page 280](#)
- [DNSSEC Overview on page 281](#)

Example: Configuring the TTL Value for DNS Server Caching

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

- [Requirements on page 280](#)
- [Overview on page 280](#)
- [Configuration on page 280](#)
- [Verification on page 281](#)

Requirements

No special configuration beyond device initialization is required before performing this task.

Overview

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

Configuration

Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds.

[edit]
user@host# **set system services dns max-cache-ttl 86400**
2. Specify the maximum TTL value for negative cached responses, in seconds.

[edit]
user@host# **set system services dns max-ncache-ttl 86400**
3. If you are done configuring the device, commit the configuration.

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

Verification

To verify the configuration is working properly, enter the **show system services** command.

Related Documentation

- [DNS Overview on page 279](#)

DNSSEC Overview

Supported Platforms [SRX Series, vSRX](#)

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

Related Documentation

- [DNS Overview on page 279](#)
- [Example: Configuring Keys for DNSSEC on page 282](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 282](#)

Example: Configuring DNSSEC

Supported Platforms [SRX Series, vSRX](#)

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]
set system services dns dnssec disable
```

Related Documentation

- [DNSSEC Overview on page 281](#)

Example: Configuring Keys for DNSSEC

Supported Platforms [SRX Series, vSRX](#)

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key "...pasted-text..."
```

If you are done loading the keys from the file or terminal, click **commit** in the CLI editor.

Related Documentation

- [DNSSEC Overview on page 281](#)
- [Example: Configuring Secure Domains and Trusted Keys for DNSSEC on page 282](#)

Example: Configuring Secure Domains and Trusted Keys for DNSSEC

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure secure domains and trusted keys for DNSSEC.

- [Requirements on page 282](#)
- [Overview on page 282](#)
- [Configuration on page 283](#)

Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See ["Example: Configuring DNSSEC" on page 281](#) for more information.

Overview

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to

the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.ABC123ABCh
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Step-by-Step Procedure To configure secure domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

```
[edit]
user@host# set system services dns dnssec secure-domains domain1.net
user@host# set system services dns dnssec secure-domains domain2.net
```

2. Configure trusted keys to domain1.net.

```
[edit]
user@host# set system services dns dnssec trusted-keys key
"domain1.net.ABC123ABCh"
```

3. Attach a root zone div.isc.org as a trusted anchor to a secure domain.

```
[edit]
user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor
dlv.isc.org
```

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

```
dns {
  dnssec {
    trusted-keys {
      key domain1.net.ABC123ABCh; ## SECRET-DATA
    }
  }
  dlv {
    domain domain2.net trusted-anchor dlv.isc.org;
```

```
    }  
    secure-domains {  
        domain1.net;  
        domain2.net;  
    }  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [DNSSEC Overview on page 281](#)
- [Example: Configuring Keys for DNSSEC on page 282](#)

DNS Proxy Overview

Supported Platforms [SRX1500](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#), [vSRX](#)

A dynamic name system (DNS) proxy allows clients to use a device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

- [DNS Proxy Cache on page 284](#)
- [DNS Proxy with Split DNS on page 284](#)
- [Dynamic Domain Name System Client on page 287](#)

DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.



NOTE: If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the **clear cache** command, or the cache will automatically expire along with TTL when it goes to zero.

DNS Proxy with Split DNS

The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

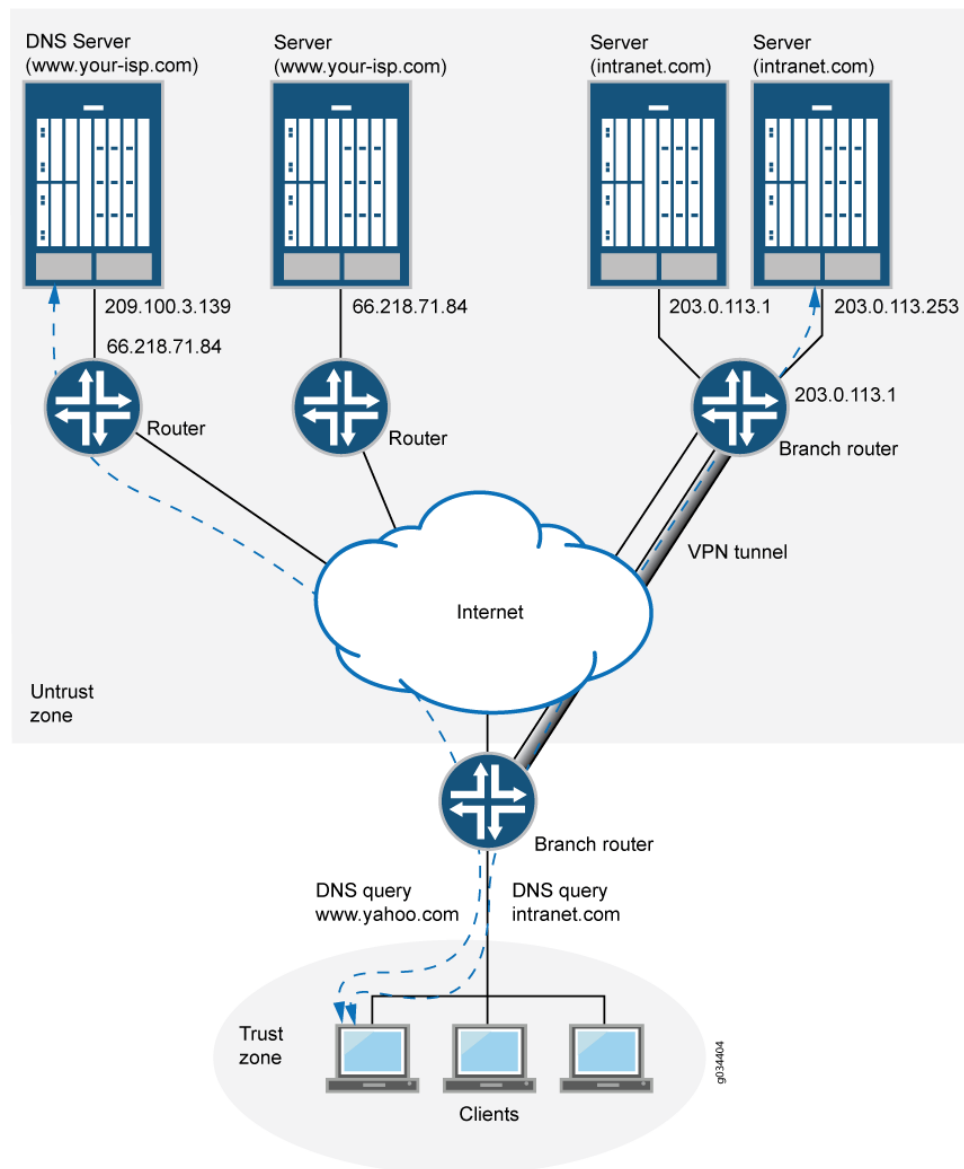
You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

[Figure 2 on page 286](#) shows how the split DNS proxy works in a corporate network.

Figure 2: DNS Proxy with Split DNS



In the corporate network shown in [Figure 2 on page 286](#), a PC client that points to the SRX Series device as its DNS server makes two queries—to `www.your-isp.com` and to `www.intranet.com`. The DNS proxy redirects the `www.intranet.com` query to the `www.intranet.com` DNS server (203.0.113.253), while the `www.your-isp.com` query is redirected to the ISP DNS server (209.100.3.130). Although the query for `www.your-isp.com` is sent to the ISP DNS server as a regular DNS query using clear text protocols (TCP/UDP), the query for the `www.intranet.com` domain goes to the intranet's DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as acme.com) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.
- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

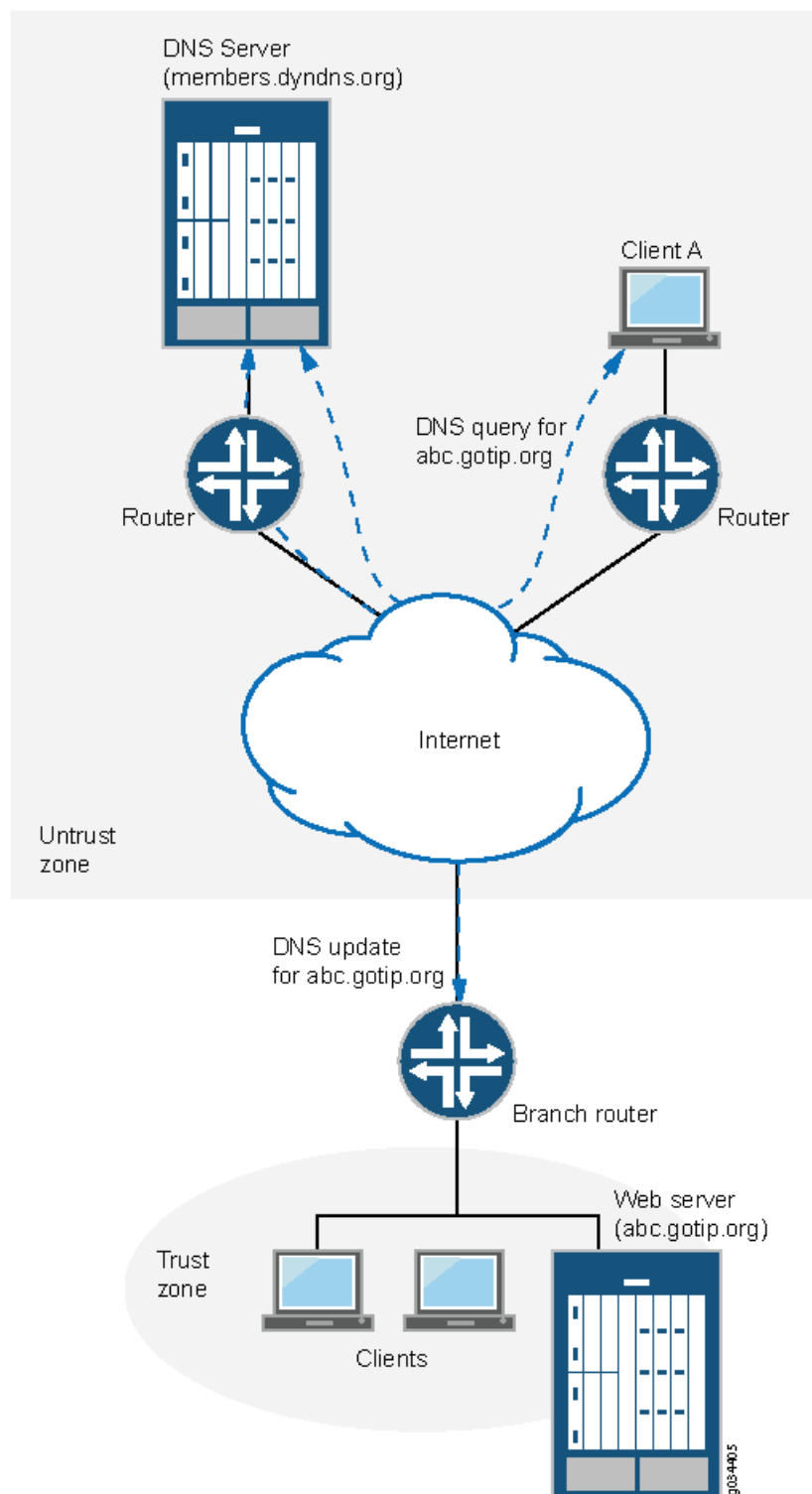
Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as dyndns.org and ddo.jp

[Figure 3 on page 288](#) illustrates how the DDNS client works.

Figure 3: Dynamic DNS



The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the untrust zone interface on the device. The hostname

abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in [Figure 3 on page 288](#) needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

Related Documentation

- [Configuring the Device as a DNS Proxy on page 289](#)

Configuring the Device as a DNS Proxy

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables a device to reference locations by domain name (such as www.example.net) in addition to using the routable IP address.

DNS features include:

- **DNS proxy**—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series device. DNS proxy improves domain lookup performance by using caching.
- **Split DNS**—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.
- **Dynamic DNS (DDNS) client**—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).

To configure the device as a DNS proxy, you enable DNS on a logical interface and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, ge-0/0/1.0—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

1. DNS proxy configuration

- Enable DNS proxy on a logical interface.

```
[edit system services]
user@host# set dns dns-proxy interface ge-0/0/1.0
```

- Set a default domain name, and specify global name servers according to their IP addresses.

```
[edit system services]
user@host# set dns dns-proxy default-domain * forwarders 172.17.28.100
```

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

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

To verify if the configuration is working properly, execute the show command.

```
user@hostshow system services dns dns-proxy
```

2. Dynamic DNS proxy configuration

- Enable client.

```
[edit system services]
user@host# set dynamic-dns client abc.com agent juniper interface ge-0/0/1.0
username test password test123
```

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

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

To verify if the configuration is working properly

```
user@hostshow system services dynamic-dns
```

**Related
Documentation**

- [Configuring the Device as a DNS Proxy on page 289](#)

PART 4

Configuring DHCP Access Service for IP Address Management

- [Understanding DHCP Services on page 293](#)
- [Configuring a DHCP Local Server on page 301](#)
- [Configuring a DHCP Client on page 315](#)
- [Configuring a DHCP Relay Agent on page 323](#)
- [Configuring a DHCPv6 Local Server on page 327](#)
- [Configuring a DHCPv6 Client on page 339](#)

CHAPTER 10

Understanding DHCP Services

- [DHCP Overview on page 293](#)
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [DHCP Settings and Restrictions Overview on page 297](#)
- [Understanding Cascaded DHCPv6 Prefix Delegating on page 298](#)

DHCP Overview

Supported Platforms [SRX Series, vSRX](#)

The Dynamic Host Configuration Protocol (DHCP) can serve as a DHCP local server, a DHCP client, or a DHCP relay agent.

DHCP Local Server

You can enable an SRX Series device to function as a DHCP local server, and then configure its options on the device. The DHCP local server provides an IP address and other configuration information in response to a client request.

To configure the DHCP local server on the device, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level.



NOTE: You cannot configure the DHCP local server and the DHCP relay agent on the same interface.

DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the device. The following steps provide a high-level description of the interaction among the DHCP client, DHCP local server, and address-assignment pools.

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local

server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server and client installs the host route and ARP entry, and then monitors the lease state.

DHCP Local Server and Address-Assignment Pools

In a DHCP local server operation, the client address and configuration information reside in centralized address-assignment pools, that are managed independently from the DHCP local server and they can be shared by different client applications.

Configuring a DHCP environment that includes a DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the DHCP local server on the device and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.



NOTE: The DHCP local server and the address-assignment pools used by the server must be configured in the same routing instance.

DHCP Client

DHCP configuration consists of configuring DHCP clients and a DHCP local server. A client configuration determines how clients send a message requesting an IP address, while a server configuration enables the server to send an IP address back to the client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval.

DHCP Relay Agent

You can configure DHCP relay options on the device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP local server.

To configure the DHCP relay agent on the router, include the **dhcp-relay** statement at the **[edit forwarding-options]** hierarchy level.

You can also include the **dhcp-relay** statement at the following hierarchy level:

[edit routing-instances routing-instance-name forwarding-options]

DHCP Client, DHCP Relay Agent, and DHCP Local Servers

In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the device between the DHCP client and one or more DHCP local servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP local server interact in a configuration that includes two DHCP local servers.

1. The DHCP client sends a discover packet to find a DHCP local server in the network from which to obtain configuration parameters for the subscriber, including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP local servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP local server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP local server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP local server from which to obtain configuration information.
6. The DHCP local server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
7. The DHCP relay agent receives the ACK packet and forwards it to the client.
8. The DHCP client receives the ACK packet and stores the configuration information.
9. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
10. After establishing the initial lease on the IP address, the DHCP client and the DHCP local server use unicast transmission to negotiate lease renewal or release.

Considerations

The following considerations apply when you enable a DHCP local server, DHCP relay agent, or DHCP client in a routing instance:

- The DHCP local server, DHCP relay agent, and DHCP client can be configured in one routing instance, but the functionality is mutually exclusive on one interface. If the DHCP client is enabled on one interface, the DHCP local server or the DHCP relay agent cannot be enabled on that interface.
- The DHCP client, DHCP relay agent and DHCP local server services act independently in their respective routing instance. The following features can function simultaneously on a device:

- DHCP client and DHCP local server
- DHCP client and DHCP relay agent
- Multiple routing instances. Each instance can have a DHCP local server, DHCP relay agent, or DHCP client, or each routing instance can have a DHCP client and DHCP local server or a DHCP client and DHCP relay agent.



NOTE: Before you enable DHCP services in a routing instance, you must remove all the configuration related to DHCP services that does not include routing instance support. If you do not do this, the old default routing instance configuration will override the new routing instance configuration.



NOTE: On all SRX Series devices, logical systems and routing instances are not supported for a DHCP client in chassis cluster mode.

**Related
Documentation**

- [Understanding DHCP Server Operation on page 301](#)
- [Understanding DHCP Client Operation on page 315](#)
- [Understanding DHCP Relay Agent Operation on page 323](#)

DHCP Server, Client, and Relay Agent Overview

Supported Platforms [SRX Series, vSRX](#)

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network. An IP address can be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.

The device can also operate as a DHCP client and DHCP relay agent.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.



NOTE: Although a Juniper Networks device can act as a DHCP server, a DHCP client, or DHCP relay agent at the same time, you cannot configure more than one DHCP role on a single interface.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.



NOTE: On all SRX Series devices, DHCPv4 is supported only in Layer 3 mode; the DHCP server and DHCP client are not supported in Layer 2 transparent mode.

Related Documentation

- [DHCP Server Configuration Overview on page 302](#)
- [Understanding DHCP Server Operation on page 301](#)
- [Understanding DHCP Client Operation on page 315](#)
- [Understanding DHCP Relay Agent Operation on page 323](#)
- [DHCP Settings and Restrictions Overview on page 297](#)

DHCP Settings and Restrictions Overview

Supported Platforms [SRX Series, vSRX](#)

This section contains the following topics:

- [Propagation of TCP/IP Settings for DHCP on page 297](#)
- [DHCP Conflict Detection and Resolution on page 298](#)
- [DHCP Interface Restrictions on page 298](#)

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP's DHCP name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device's internal network.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the **show system services dhcp conflict** command. The addresses in the conflicts list remain excluded until you use the **clear system services dhcp conflict** command to manually clear the list.

DHCP Interface Restrictions

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types.

DHCP is not supported on interfaces that are part of a virtual private network (VPN).

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [Understanding DHCP Server Operation on page 301](#)
- [Understanding DHCP Client Operation on page 315](#)
- [Understanding DHCP Relay Agent Operation on page 323](#)

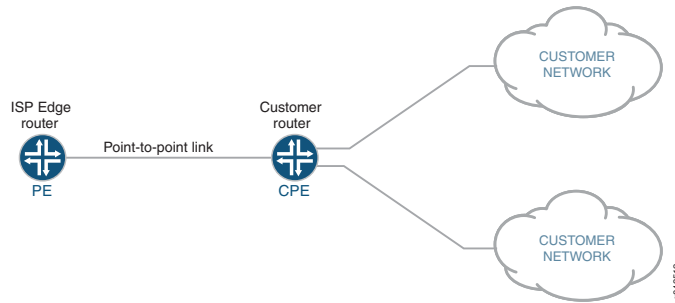
Understanding Cascaded DHCPv6 Prefix Delegating

Supported Platforms [SRX Series](#)

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating device delegates IPv6 prefixes to a requesting device. The requesting device then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting device can also assign subnet addresses to subnets on the LAN.

With cascaded prefix delegation, the IPv6 address block is delegated to a DHCPv6 client that is running on the WAN interface of a customer edge device. The identity association (IA) for the client is used for the identity association for prefix delegation (IA_PD). The CE device requests, through DHCPv6, an IPv6 address with the IA type of nontemporary addresses (IA_NA). Both IA_PD and IA_NA are requesting in the same DHCPv6 exchange.

Figure 4: IPv6 Prefix Delegation



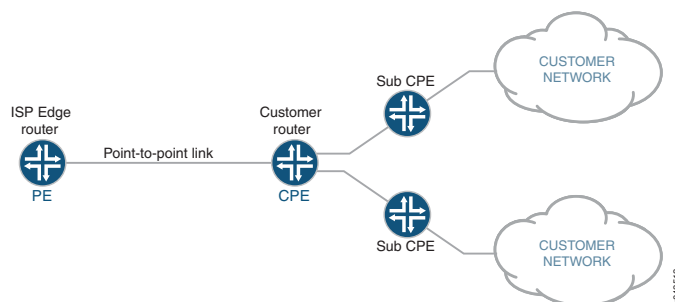
The topology in [Figure 4 on page 299](#) shows an SRX Series device acting as the CPE. The WAN interface links to the provider edge (PE) device and the LAN interfaces link to the customer networks. The service provider delegates a prefix (delegated-prefix) and an IPv6 address (cpe-wan-ipv6-address) to a DHCPv6 client. When a requesting device receives that IPv6 address through the DHCPv6 client, the device must install the IPv6 address on its WAN interface. The DHCPv6 client then divides the delegated prefix into sub-prefixes and subsequently assigns them to the connected LAN interfaces of the CPE device, making some subset of the remaining space available for sub-prefix delegation.

A CPE assigns sub-prefixes to its LAN interfaces and broadcasts the sub-prefixes through device advertisement. In this scenario, the CPE acts as a sub-PE and delegates sub-prefixes and assigns them to sub-CPEs.



NOTE: The requirements of sub-prefix delegation are the same as for the prefix delegation defined in RFC 3769.

Figure 5: Sub-prefix Delegation



There can be multi-level sub prefix delegations, see [Figure 5 on page 299](#). The top level CPE gets a delegated prefix from the PE and delegates the sub prefixes to second level sub-CPEs, then to the third level sub-CPEs, and finally to the end levels. The end level sub-CPEs assign the IPv6 address to end hosts through SLAAC, stateless DHCPv6 or stateful DHCPv6. This is called cascaded prefix delegating.

Related Documentation

CHAPTER 11

Configuring a DHCP Local Server

- [Understanding DHCP Server Operation on page 301](#)
- [DHCP Server Configuration Overview on page 302](#)
- [Minimum DHCP Local Server Configuration on page 303](#)
- [Configuring Address-Assignment Pools on page 304](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 305](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 305](#)
- [Configuring Static Address Assignments on page 306](#)
- [Enabling TCP/IP Propagation on a DHCP Local Server on page 306](#)
- [Verifying and Managing DHCP Local Server Configuration on page 307](#)
- [Example: Configuring the Device as a DHCP Server on page 308](#)

Understanding DHCP Server Operation

Supported Platforms [SRX Series, vSRX](#)

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. Juniper Networks devices can also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

This section contains the following topics:

- [DHCP Options on page 301](#)
- [Compatibility with Autoinstallation on page 302](#)
- [Chassis Cluster Support on page 302](#)

DHCP Options

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers

- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

Compatibility with Autoinstallation

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Chassis Cluster Support

DHCP server operations are supported on all SRX Series devices in chassis cluster mode.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [Example: Configuring the Device as a DHCP Server on page 308](#)
- [Understanding DHCP Client Operation on page 315](#)
- [Understanding DHCP Relay Agent Operation on page 323](#)

DHCP Server Configuration Overview

Supported Platforms [SRX Series, vSRX](#)

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device interface:

- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.
- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.
- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. [Table 12 on page 302](#) provides the settings and values for the sample DHCP server configuration.

Table 12: Sample DHCP Server Configuration Settings

| Setting | Sample Value |
|----------------------------------|----------------|
| DHCP Subnet Configuration | |
| Address pool subnet address | 192.168.2.0/24 |

Table 12: Sample DHCP Server Configuration Settings (*continued*)

| Setting | Sample Value |
|--|----------------------------|
| High address in the pool range | 192.168.2.254 |
| Low address in the pool range | 192.168.2.2 |
| Address pool default lease time, in seconds | 1,209,600 (14 days) |
| Address pool maximum lease time, in seconds | 2,419,200 (28 days) |
| Domain search suffixes | mycompany.net mylab.net |
| Address to exclude from the pool | 192.168.2.33 |
| DNS server address | 192.168.10.2 |
| Identifier code for router solicitation address option | 32 |
| Type choice for router solicitation address option | ip address |
| IP address for router solicitation address option | 192.168.2.33 |
| DHCP MAC Address Configuration | |
| Static binding MAC address | 01:03:05:07:09:0B |
| Fixed address | 192.168.2.50 |

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [Understanding DHCP Server Operation on page 301](#)
- [Understanding DHCP Client Operation on page 315](#)
- [Understanding DHCP Relay Agent Operation on page 323](#)
- [RFC 3397, *Dynamic Host Configuration Protocol \(DHCP\) Domain Search Option*](#)

Minimum DHCP Local Server Configuration

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP local server. In this output, the server group is named `mobileusers`, and the DHCP local server is enabled on interface `ge-1/0/1.0` within the group.

```
[edit access]
address-assignment {
```

```

    pool acmenetwork family inet {
        network 192.168.1.0/24;
    }
}

edit system services
dhcp-local-server {
    group mobileusers {
        interface ge-1/0/1.0
    }
}

edit interfaces ge-1/0/1 unit 0
family {
    inet {
        address 192.168.1.1/24
    }
}

```



NOTE: You can configure the DHCP local server in a routing instance by using the `dhcp-local-server`, `interface`, and `address-assignment` statements in the `[edit routing-instances]` hierarchy level.

Related Documentation

- [Configuring Address-Assignment Pools on page 304](#)

Configuring Address-Assignment Pools

Supported Platforms [SRX1500](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#), [vSRX](#)

The address-assignment pool feature enables you to create address pools that can be shared by different client applications.

To configure an address-assignment pool:

1. Configure the address-assignment pool name and specify the addresses for the pool.
See [“Configuring an Address-Assignment Pool Name and Addresses” on page 305](#).
2. (Optional) Configure named ranges (subsets) of addresses.
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 305](#).
3. (Optional;IPv4 only) Create static address bindings.
See [“Configuring Static Address Assignments” on page 306](#).
4. (Optional) Configure attributes for DHCP clients.
See [“Configuring DHCP Client-Specific Attributes for Address-Assignment Pools” on page 316](#).

Related Documentation

- [Configuring an Address-Assignment Pool Name and Addresses on page 305](#)

Configuring an Address-Assignment Pool Name and Addresses

Supported Platforms SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX

When configuring an address-assignment pool, you must specify the name of the pool and its addresses.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the network address and the prefix length of the addresses in the pool.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set network 192.168.0.0/16
```



NOTE: You can configure an IPv4 address-assignment pool in a routing instance by configuring the address-assignment statements in the `[edit routing-instances]` hierarchy level.

Related Documentation

- [Configuring Address-Assignment Pools on page 304](#)

Configuring a Named Address Range for Dynamic Address Assignment

Supported Platforms SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During a dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```



NOTE: To configure named address ranges in a routing instance, configure the address-assignment statements in the `[edit routing-instances]` hierarchy level.

Related Documentation • [Configuring Address-Assignment Pools on page 304](#)

Configuring Static Address Assignments

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address.

To configure a static IPv4 address binding:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 01:03:05:07:09:0b is always assigned IP address 192.168.10.2.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set host sva1e6_boston_net hardware-address 01:03:05:07:09:0b
ip-address 192.168.10.2
```



NOTE: To configure static binding for an IPv4 address in a routing instance, configure the address-assignment statements in the [edit routing-instances] hierarchy.

Related Documentation • [Configuring Address-Assignment Pools on page 304](#)

Enabling TCP/IP Propagation on a DHCP Local Server

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

This topic describes how to configure TCP/IP settings on a DHCP local server, which includes a DHCP client and a DHCP local server.

To enable TCP/IP setting propagation on a DHCP local server:

1. Configure the **update-server** option on the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp-client {
  update-server;
}
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

```
[edit access]
address-assignment {
  pool sprint family inet {
    network 192.168.2.0/24;
    dhcp-attributes {
      propagate-settings ge-0/0/1.0;
    }
  }
}
```

3. Configure the DHCP local server.

```
edit system services
dhcp-local-server {
  group bob {
    interface ge-1/0/1.0
  }
}
```

Related Documentation

- [Minimum DHCP Local Server Configuration on page 303](#)

Verifying and Managing DHCP Local Server Configuration

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Purpose View or clear information about client address bindings and statistics for the DHCP local server.

- Action**
- To display the address bindings in the client table on the DHCP local server:

```
user@host> show dhcp server binding
```
 - To display DHCP local server statistics:

```
user@host> show dhcp server statistics
```
 - To clear the binding state of a DHCP client from the client table on the DHCP local server:

```
user@host> clear dhcp server binding
```
 - To clear all DHCP local server statistics:

```
user@host> clear dhcp server statistics
```



NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp server binding routing instance <routing-instance name>`
- `show dhcp server statistics routing instance <routing-instance name>`
- `clear dhcp server binding routing instance <routing-instance name>`
- `clear dhcp server statistics routing instance <routing-instance name>`

Related Documentation

- [Minimum DHCP Local Server Configuration on page 303](#)

Example: Configuring the Device as a DHCP Server

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure the device as a DHCP server.

- [Requirements on page 308](#)
- [Overview on page 308](#)
- [Configuration on page 309](#)
- [Verification on page 311](#)

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the maximum-lease-time to 2,419,200. Then you specify the DNS server IP address as 192.168.10.2.



WARNING: Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated

and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

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, copy and paste the commands into the CLI at the **set access** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
set system services dhcp-local-server group g1 interface ge-0/0/2.0
set access address-assignment pool p1 family inet network 192.168.2.0/24
set access address-assignment pool p1 family inet range r1 low 192.168.2.2
set access address-assignment pool p1 family inet range r1 high 192.168.2.254
set access address-assignment pool p1 family inet dhcp-attributes maximum-lease-time
  2419200
set access address-assignment pool p1 family inet dhcp-attributes name-server
  192.168.10.2
```

GUI Step-by-Step Procedure

To configure the device as a DHCP server, specify the DHCP pool information, server information, lease time, and option information:

1. In the J-Web interface, select **Configure > DHCP > DHCP Services**.
2. Select DHCP Pools. Click **Add**.
3. Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
4. Specify the subnet information for the IPv4 address-assignment pool. Type **192.168.2.0/24**.
5. In the Address Range Low, type **192.168.2.2**.
6. In the Address Range High, type **192.168.2.254**.
7. In the Exclude Addresses box, type the addresses you want excluded from a DHCP address pool. Type **192.168.0.20**
8. Specify the server identifier to assign to any DHCP clients in this address pool. The identifier can be used to identify a DHCP server in a DHCP message.
9. Specify the domain name to assign to any DHCP clients in this address pool.
10. Specify the next server that DHCP clients need to contact. Type **192.168.10.2**

11. Define the maximum amount of time (in seconds) that DHCP should lease an address. Type **2419200**.
12. Define DHCP option 32, the device solicitation address option. You must enter a numeric value for option code. Select the option type from the list that corresponds to the option code.
13. Click **OK**.
14. If you are done configuring the device, click **Commit** > **Commit**.

**Step-by-Step
Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a DHCP server:

1. Configure an interface with an IP address on which the DHCP server will be reachable.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
```
2. Configure the DHCP server.

```
[edit]
user@host# set system services dhcp-local-server group g1 interface ge-0/0/2.0
```
3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]]
user@host# set access address-assignment pool p1 family inet network
192.168.2.0/24
```
4. (Optional) Specify the IP address pool range. Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit]]
user@host# set access address-assignment pool p1 192.168.2.0/24 address-range
low 192.168.2.2 high 192.168.2.254
```
5. (Optional) Configure one or more routers as the default gateway on the client's subnet.

```
[edit]
user@host# set access address-assignment pool p1 family inet dhcp-attributes
router 192.168.10.3
```
6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
```

```
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
server-identifier 192.168.10.1
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
maximum-lease-time 2419200
```

8. (Optional) Specify user-defined options to be included in DHCP packets

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes
option 98 string test98
```

9. Assign a fixed IP address with the MAC address of the client.

```
[edit]
user@host# set system services static-binding 01:03:05:07:09:0B
fixed-address 192.168.2.50
```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
pool 192.168.2.0/24 {
  address-range low 192.168.2.2 high 192.168.2.254;
  maximum-lease-time 2419200;
  name-server {
    192.168.10.2;
  }
  option 32 ip-address 192.168.2.33;
  }
  static-binding 01:03:05:07:09:0B {
    fixed-address {
      192.168.2.50;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the DHCP Binding Database on page 311](#)
- [Verifying DHCP Server Operation on page 312](#)

Verifying the DHCP Binding Database

Purpose Verify that the DHCP binding database reflects the DHCP server configuration.

Action From operational mode, enter these commands:

- **show dhcp server binding** command to display all active bindings in the database.
- **show dhcp server binding *address* detail** command (where *address* is the IP address of the client) to display more information about a client.

These commands produce following sample output:

```
user@host> show dhcp server binding

IP Address   Hardware Address   Type           Lease expires at
30.1.1.20    00:12:1e:a9:7b:81  dynamic       2007-05-11 11:14:43 PDT

user@host> show dhcp server binding address detail

IP address           192.0.2.2
Hardware address      00:a0:12:00:13:02
Pool                  192.0.2.0/24
Interface fe-0/0/0, relayed by 192.0.2.200

Lease information:
Type                 DHCP
Obtained at          2004-05-02 13:01:42 PDT
Expires at           2004-05-03 13:01:42 PDT
State                 active

DHCP options:
Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
Name: domain-name, Value: mydomain.tld
Code: 32, Type: ip-address, Value: 192.0.2.33
```

Verifying DHCP Server Operation

Purpose Verify that the DHCP server operation has been configured.

Action From operational mode, enter the following command:

- **show dhcp server statistics** command to verify the DHCP server statistics.

```
user@host> show dhcp server statistics

Packets dropped:
Total              0

Messages received:
BOOTREQUEST        45
DHCPDECLINE         0
DHCPDISCOVER        1
DHCPINFORM          39
DHCPRELEASE         0
DHCPREQUEST         5
DHCPLEASEQUERY      0
DHCPBULKLEASEQUERY  0

Messages sent:
BOOTREPLY           6
DHCPOFFER            1
DHCPACK              3
```

| | |
|---------------------|---|
| DHCPNAK | 2 |
| DHCPFORCERENEW | 0 |
| DHCPLEASEUNASSIGNED | 0 |
| DHCPLEASEUNKNOWN | 0 |
| DHCPLEASEACTIVE | 0 |
| DHCPLEASEQUERYDONE | 0 |

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
 - [Understanding DHCP Server Operation on page 301](#)
 - [Understanding DHCP Relay Agent Operation on page 323](#)
 - [DHCP Settings and Restrictions Overview on page 297](#)

CHAPTER 12

Configuring a DHCP Client

- [Understanding DHCP Client Operation on page 315](#)
- [Minimum DHCP Client Configuration on page 315](#)
- [Configuring DHCP Client-Specific Attributes for Address-Assignment Pools on page 316](#)
- [Configuring Optional DHCP Client Attributes on page 317](#)
- [Verifying and Managing DHCP Client Configuration on page 318](#)
- [Example: Configuring the Device as a DHCP Client on page 318](#)

Understanding DHCP Client Operation

Supported Platforms [SRX Series, vSRX](#)

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series devices in chassis cluster mode.

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
 - [Understanding DHCP Relay Agent Operation on page 323](#)
 - [DHCP Settings and Restrictions Overview on page 297](#)

Minimum DHCP Client Configuration

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
  ge-0/0/0 {
    unit 0 {
      family inet {
        dhcp-client
      }
    }
  }
```



NOTE: To configure a DHCP client in a routing instance, add the interface in a routing instance using the `[edit routing-instances]` hierarchy.

**Related
Documentation**

- [Configuring Optional DHCP Client Attributes on page 317](#)

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

Supported Platforms [SRX1500](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#), [vSRX](#)

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot file that the client uses, the DNS server, and the maximum lease time.

You use the **dhcp-attributes** statement to configure DHCP client-specific attributes for address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure optional DHCP client attributes.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set dhcp-attributes maximum-lease-time 2419200
user@host# set dhcp-attributes name-server 192.168.10.2
user@host# set dhcp-attributes boot-file boot-file.txt
user@host# set dhcp-attributes boot-file boot-server example.com
```



NOTE: To configure DHCP client-specific attributes in a routing instance, configure the `dhcp-attributes` statements in the `[edit routing-instances]` hierarchy.

Related Documentation

- [Configuring Address-Assignment Pools on page 304](#)

Configuring Optional DHCP Client Attributes

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```
2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```
3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```
4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```
5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```
6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```
7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```



NOTE: To configure the DHCP client in a routing instance, configure the interface in the [edit routing-instances] hierarchy.

Related Documentation

- [Minimum DHCP Client Configuration on page 315](#)

Verifying and Managing DHCP Client Configuration

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Purpose View or clear information about client address bindings and statistics for the DHCP client.

- Action**
- To display the address bindings in the client table on the DHCP client:
`user@host> show dhcp client binding`
 - To display DHCP client statistics:
`user@host> show dhcp client statistics`
 - To clear the binding state of a DHCP client from the client table on the DHCP client:
`user@host> clear dhcp client binding`
 - To clear all DHCP client statistics:
`user@host> clear dhcp client statistics`



NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp client binding routing instance <routing-instance name>`
- `show dhcp client statistics routing instance <routing-instance name>`
- `clear dhcp client binding routing instance <routing-instance name>`
- `clear dhcp client statistics routing instance <routing-instance name>`

Related Documentation

- [Example: Configuring the Device as a DHCP Client on page 318](#)

Example: Configuring the Device as a DHCP Client

Supported Platforms [SRX Series, vSRX](#)

This example shows how to configure the device as a DHCP client.

- [Requirements on page 319](#)
- [Overview on page 319](#)

- [Configuration on page 319](#)
- [Verification on page 321](#)

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. You can use the **show system services dhcp pool** CLI command to view information on DHCP address pools.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network. See *Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server*

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/2, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.



WARNING: Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet dhcp-client client-identifier prefix host-name
set interfaces ge-0/0/2 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/2 unit 0 family inet dhcp-client server-address 192.168.2.1
set interfaces ge-0/0/2 unit 0 family inet dhcp-client vendor-id ether
set interfaces ge-0/0/2 unit 0 family inet dhcp-client options no-hostname
```

GUI Step-by-Step Procedure

To configure the device as a DHCP client:

1. In the J-Web interface, select **Configure > Services > DHCP > DHCP Client**.
2. Under Interfaces, add **ge-0/0/2.0**.
3. Configure the DHCP client identifier as either an ASCII or hexadecimal value.
4. From the Client identifier choice list, select **hexadecimal**.
5. In the Hexadecimal box, type the client identifier—**00:0a:12:00:12:12**.
6. Set the DHCP lease time in seconds. This is the lease time in seconds requested in a DHCP client protocol packet; the range is 60 through 2,147,483,647. Type **86400**.
7. Set the retransmission number of attempts to 6. This is the number of attempts to retransmit the DHCP client protocol packet. The range is 0 through 6.
8. Set the retransmission interval in seconds to 5. This is the number of seconds between successive transmissions. The range is 4 through 64. The default is 4 seconds.
9. Set the IPv4 address of the preferred DHCP server. Type **192.168.2.1**.
10. Set the vendor class ID. This is the vendor class identification for the DHCP client. Type **ether**.
11. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).
12. Click **OK**.
13. If you are done configuring the device, click **Commit >**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/2 unit 0 family inet dhcp-client
```
2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```
4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```
5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```
6. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set server-address 192.168.2.1
```
7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```
8. Configure options no-hostname if you do not want the client to send the hostname in packets.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

Results From configuration mode, confirm your configuration by entering the **show interfaces ge-0/0/2 unit 0 family inet** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/2 unit 0 family inet
dhcp-client {
  client-identifier hexadecimal 00:0a:12:00:12:12;
  options no-hostname;
  lease-time 86400;
  retransmission-attempt 6;
  retransmission-interval 5;
  server-address 192.168.2.1;
  update-server;
  vendor-id ether;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying the DHCP Client on page 322](#)

Verifying the DHCP Client

Purpose Verify that the DHCP client information has been configured.

Action From operational mode, enter these commands:

- **show dhcp client binding** command to display the binding state of a Dynamic Host Configuration Protocol (DHCP) client.
- **show dhcp client statistics** command to display client statistics.

These commands produce the following sample output:

```
user@host> show dhcp client binding
```

| IP address | Hardware address | Expires | State | Interface |
|-------------|-------------------|---------|-------|-----------|
| 192.168.2.2 | 88:a2:5e:0a:d6:03 | 2419093 | BOUND | ge-0/0/2. |

```
user@host> show dhcp client statistics
```

Packets dropped:

| | |
|------------|---|
| Total | 2 |
| Send error | 2 |

Messages received:

| | |
|----------------|---|
| BOOTREPLY | 6 |
| DHCPOFFER | 4 |
| DHCPACK | 2 |
| DHCPNAK | 0 |
| DHCPFORCERENEW | 0 |

Messages sent:

| | |
|--------------|----|
| BOOTREQUEST | 39 |
| DHCPDECLINE | 0 |
| DHCPDISCOVER | 23 |
| DHCPREQUEST | 16 |
| DHCPINFORM | 0 |
| DHCPRELEASE | 0 |
| DHCPRENEW | 0 |
| DHCPREBIND | 0 |

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
 - [Understanding DHCP Server Operation on page 301](#)
 - [Understanding DHCP Client Operation on page 315](#)
 - [DHCP Settings and Restrictions Overview on page 297](#)

CHAPTER 13

Configuring a DHCP Relay Agent

- [Understanding DHCP Relay Agent Operation on page 323](#)
- [Minimum DHCP Relay Agent Configuration on page 323](#)
- [Verifying and Managing DHCP Relay Configuration on page 324](#)

Understanding DHCP Relay Agent Operation

Supported Platforms [SRX Series, vSRX](#)

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.



NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

**Related
Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [Understanding DHCP Server Operation on page 301](#)
- [DHCP Settings and Restrictions Overview on page 297](#)

Minimum DHCP Relay Agent Configuration

Supported Platforms [SRX Series, vSRX](#)

The following sample output shows the minimum configuration you must use to configure an SRX Series device as a DHCP relay agent. In this output, the active server group is named server-1 and its IP address is 203.0.113.1. The DHCP relay agent configuration is applied to a group named bob. Within this group, the DHCP relay agent is enabled on interface ge-1/0/1.0.

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    server-1 {
      203.0.113.1;
    }
  }
  active-server-group server-1;
  group bob {
    interface ge-1/0/1.0;
  }
}
```



NOTE: To configure the DHCP relay agent in a routing instance, configure the `dhcp-relay` statements in the `[edit routing-instances]` hierarchy level.

**Related
Documentation**

- [Verifying and Managing DHCP Relay Configuration on page 324](#)

Verifying and Managing DHCP Relay Configuration

Supported Platforms [SRX Series, vSRX](#)

Purpose View or clear address bindings or statistics for DHCP relay agent clients.

Action • To display the address bindings for DHCP relay agent clients:

```
user@host> show dhcp relay binding
```

- To display DHCP relay agent statistics:

```
user@host> show dhcp relay statistics
```

- To clear the binding state of DHCP relay agent clients:

```
user@host> clear dhcp relay binding
```

- To clear all DHCP relay agent statistics:

```
user@host> clear dhcp relay statistics
```

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp relay binding routing instance <routing-instance name>`
- `show dhcp relay statistics routing instance <routing-instance name>`

- clear dhcp relay binding routing instance <routing-instance name>
- clear dhcp relay statistics routing instance <routing-instance name>



NOTE: On all SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

**Related
Documentation**

- [Minimum DHCP Relay Agent Configuration on page 323](#)

Configuring a DHCPv6 Local Server

- [DHCPv6 Server Overview on page 327](#)
- [Creating a Security Policy for DHCPv6 on page 328](#)
- [Example: Configuring DHCPv6 Server Options on page 329](#)
- [Example: Configuring an Address-Assignment Pool on page 332](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)
- [Configuring Address-Assignment Pool Linking on page 335](#)
- [Configuring DHCP Client-Specific Attributes on page 335](#)
- [Configuring an Address-Assignment Pool for Router Advertisement on page 336](#)
- [Understanding DHCPv6 Client and Server Identification on page 336](#)

DHCPv6 Server Overview

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IP version 6 (IPv6) clients and deliver configuration settings to client hosts on a subnet or to requesting devices that need an IPv6 prefix. A DHCPv6 server lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network.



NOTE: SRX Series devices do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)
- Prefix delegation, including access-internal route installation
- DHCPv6 server groups

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the **[edit system services dhcp-local-server]** hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the **[edit access address-assignment pool]** hierarchy level using the **family inet6** statement.

You can also include the **dhcpv6** statement at the **[edit routing-instances routing-instance-name system services dhcp-local-server]** hierarchy.



NOTE: Existing DHCPv4 configurations in the **[edit system services dhcp]** hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

**Related
Documentation**

- [Example: Configuring DHCPv6 Server Options on page 329](#)
- [Example: Configuring an Address-Assignment Pool on page 332](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)
- [Creating a Security Policy for DHCPv6 on page 328](#)

Creating a Security Policy for DHCPv6

Supported Platforms [SRX1500](#), [SRX5400](#), [SRX5600](#), [SRX5800](#)

For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 2001:db8:3001::1.

To create a security zone policy to allow DHCPv6:

1. Create the zone and add an interface to that zone.

```
[edit security zones]  
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```
2. Configure host inbound traffic system services to allow DHCPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]  
user@host# set host-inbound-traffic system-services dhcpv6
```
3. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [DHCPv6 Server Overview on page 327](#)
- [Example: Configuring DHCPv6 Server Options on page 329](#)

- [Example: Configuring an Address-Assignment Pool on page 332](#)

Example: Configuring DHCPv6 Server Options

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

This example shows how to configure DHCPv6 server options.

- [Requirements on page 329](#)
- [Overview on page 329](#)
- [Configuration on page 329](#)
- [Verification on page 331](#)

Requirements

Before you begin:

- Determine the IPv6 address pool range.
- Determine the IPv6 prefix. See the *Understanding Address Books*.
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients.
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.

Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the upto command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 2001:db8:3001::1/64 and set router advertisement for interface ge-0/0/3.0. Starting with Junos OS Release 15.X49-D70, you can add the option **dynamic-server** to dynamically support prefix and attributes that are updated by the WAN server.



NOTE: A DHCPv6 group must contain at least one interface.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 dynamic-server
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
```

```

set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 upto
ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides
interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64

```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

```

[edit]
user@host# edit system services dhcp-local-server dhcpv6

```
2. Set a default limit for all DHCPv6 groups.

```

[edit system services dhcp-local-server dhcpv6]
user@host# set overrides interface-client-limit 100

```
3. Add a dynamic server that automatically adds prefix and attributes that are updated by the WAN server.

```

[edit]
user@host# edit system services dhcp-local-server dhcpv6 dynamic-server

```
4. Specify a group name and interface.

```

[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0

```
5. Set a range of interfaces.

```

[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0

```
6. Set a custom client limit for the group.

```

[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200

```
7. Configure an interface with an IPv6 address.

```

[edit interfaces]
user@host# set ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64

```
8. Set router advertisement for the interface.

```

[edit protocols]
user@host# set router-advertisement interface ge-0/0/3.0 prefix
2001:db8:3000::/64

```

Results From configuration mode, confirm your configuration by entering the **show system services dhcp-local-server**, **show interfaces ge-0/0/3**, and **show protocols** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
  dynamic-server
    overrides {
      interface-client-limit 100;
    }
  group my-group {
    overrides {
      interface-client-limit 200;
    }
    interface ge-0/0/3.0 {
      upto ge-0/0/6.0;
    }
  }
}
[edit]
user@host# show interfaces ge-0/0/3
unit 0 {
  family inet6 {
    address 2001:db8:3000::1/64;
  }
}
[edit]
user@host# show protocols
router-advertisement {
  interface ge-0/0/3.0 {
    prefix 2001:db8:3000::1/64;
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying DHCPv6 Local Server Configuration

- | | |
|----------------|---|
| Purpose | Verify that the client address bindings and statistics for the DHCPv6 local server have been configured |
| Action | <p>From operational mode, enter these commands:</p> <ul style="list-style-type: none"> • show dhcpv6 server binding command to display the address bindings in the client table on the DHCPv6 local server. • show dhcpv6 server statistics command to display the DHCPv6 local server statistics. • clear dhcpv6 server bindings all command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance. • clear dhcpv6 server statistics command to clear all DHCPv6 local server statistics. |

Release History Table

| Release | Description |
|-------------|--|
| 15.1X49-D70 | Starting with Junos OS Release 15.X49-D70, you can add the option dynamic-server to dynamically support prefix and attributes that are updated by the WAN server. |

Related Documentation

- [DHCPv6 Server Overview on page 327](#)
- [Example: Configuring an Address-Assignment Pool on page 332](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)
- [Creating a Security Policy for DHCPv6 on page 328](#)

Example: Configuring an Address-Assignment Pool

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

This example shows how to configure an address-assignment pool.

- [Requirements on page 332](#)
- [Overview on page 332](#)
- [Configuration on page 332](#)
- [Verification on page 334](#)

Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool.
- Set DHCPv6 attributes for the address-assignment pool.

Overview

In this example, you configure an address-pool called my-pool and specify the IPv6 family as inet6. You configure the IPv6 prefix as 2001:db8:3000:1::/64, the range name as range1, and the IPv6 range for DHCPv6 clients from a low of 2001:db8:3000:1::/64 to a high of 2001:db8:3000:200::/64. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as 2001:db8:3001::1, the grace period as 3600, and the maximum lease time as 120.

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```

set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low
  32001:db8:3000:1::/64 high 2001:db8:3000:200::/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
  2001:db8:3001::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period
  3600
set access address-assignment pool my-pool family inet6 dhcp-attributes
  maximum-lease-time 120

```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

```

[edit access]
user@host# edit address-assignment pool my-pool family inet6

```
2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.

```

[edit access address-assignment pool my-pool family inet6]
user@host# set prefix 2001:db8:3000:1::/64
user@host# set range range1 low 2001:db8:3000:1::/64 high
  2001:db8:3000:200::/64

```
3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```

[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:3001::1

```
4. Configure the DHCPv6 attribute for the grace period.

```

[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600

```
5. Configure the DHCPv6 attribute for the maximum lease time.

```

[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes maximum-lease-time 120

```

Results From configuration mode, confirm your configuration by entering the **show access address-assignment** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show access address-assignment
pool my-pool {
  family inet6 {
    prefix 2001:db8:3000:1::/64;
    range range1 {
      low 2001:db8:3000:1::/64 ;
      high 2001:db8:3000:200::/64;
    }
    dhcp-attributes {
      maximum-lease-time 120;
    }
  }
}

```

```
    grace-period 3600;
    dns-server {
        2001:db8:3001::1;
    }
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Configuration

Purpose Verify that the address-assignment pool has been configured.

Action From operational mode, enter the **show access address-assignment** command.

Related Documentation

- [DHCPv6 Server Overview on page 327](#)
- [Example: Configuring DHCPv6 Server Options on page 329](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)
- [Creating a Security Policy for DHCPv6 on page 328](#)

Configuring a Named Address Range for Dynamic Address Assignment

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool2 family inet6
```

2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 2001:db8:3000:5::/64
user@host# set range range2 low 2001:db8:3000:2::/64 high 2001:db8:3000:300::/64
```

3. Configure DHCPv6 attributes for the address pool.

```
[edit access address-assignment pool my-pool2 family inet6]
```

```
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600
maximum-lease-time 120
```

4. If you are done configuring the device, enter **commit** from configuration mode.

**Related
Documentation**

- [Configuring Address-Assignment Pool Linking on page 335](#)

Configuring Address-Assignment Pool Linking

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example, you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the device switches to pool B for addresses. When pool B is exhausted, the device switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool.

To link a primary address-assignment pool named `pool1` to a secondary pool named `pool2`:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```

**Related
Documentation**

- [Configuring a Named Address Range for Dynamic Address Assignment on page 305](#)

Configuring DHCP Client-Specific Attributes

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

You use the **dhcp-attributes** statement to configure DHCPv6 client-specific attributes for address-assignment pools at the **[edit access address-assignment pool *pool-name* family inet6]** hierarchy.

Table 13 on page 336 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 13: DHCPv6 Attributes

| Attribute | Description | DHCPv6 Option |
|-------------------------------|--|---------------|
| dns-server | IPv6 address of DNS server to which clients can send DNS queries | 23 |
| grace-period | Grace period offered with the lease | — |
| maximum-lease-time | Maximum lease time allowed by the DHCPv6 server | — |
| option | User-defined options | — |
| sip-server-address | IPv6 address of SIP outbound proxy server | 22 |
| sip-server-domain-name | Domain name of the SIP outbound proxy server | 21 |

Related Documentation

- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)

Configuring an Address-Assignment Pool for Router Advertisement

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

You can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:

1. Create the IPv6 address-assignment pool.
2. Specify that the address-assignment pool is used for router advertisement.

```
[edit access address-assignment]
user@host# set neighbor-discovery-router-advertisement router1
```
3. If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- [Configuring a Named Address Range for Dynamic Address Assignment on page 334](#)

Understanding DHCPv6 Client and Server Identification

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or

server. DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-llt)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Layer address (duid-ll)

The duid-llt DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

Related Documentation

- [DHCPv6 Client Overview on page 339](#)

CHAPTER 15

Configuring a DHCPv6 Client

- [DHCPv6 Client Overview on page 339](#)
- [Minimum DHCPv6 Client Configuration on page 340](#)
- [Configuring Optional DHCPv6 Client Attributes on page 341](#)
- [Configuring Nontemporary Address Assignment on page 343](#)
- [Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation on page 343](#)
- [Configuring Auto-Prefix Delegation on page 344](#)
- [Configuring the DHCPv6 Client Rapid Commit Option on page 345](#)
- [Configuring a DHCPv6 Client in Autoconfig Mode on page 345](#)
- [Configuring TCP/IP Propagation on a DHCPv6 Client on page 346](#)

DHCPv6 Client Overview

Supported Platforms SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the **dhcpv6-client** statement at the **[edit interfaces]** hierarchy level.



NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the **[edit routing-instances]** hierarchy.



NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.



NOTE: On all branch SRX Series devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

**Related
Documentation**

- [Minimum DHCPv6 Client Configuration on page 340](#)

Minimum DHCPv6 Client Configuration

Supported Platforms **SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M**

This topic describes the minimum configuration you must use to configure an SRX Series device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the DHCPv6 client type. The client type can be **autoconfig** or **statefull**.

- To enable DHCPv6 auto configuration mode, configure the client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

- For stateful address assignment, configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the identity association type.

- To configure identity association for nontemporary address (IA_NA) assignment, specify the **client-ia type** as **ia-na**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

- To configure identity association for prefix delegation (IA_PD), specify the **client-ia-type** as **ia-pd**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:

- Link Layer address (duid-ll)
- Link Layer address plus time (duid-llt)
- Vendor-assigned unique ID based on enterprise number (vendor)

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```



NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the `[edit routing-instances]` hierarchy.

Related Documentation

- [DHCPv6 Client Overview on page 339](#)

Configuring Optional DHCPv6 Client Attributes

Supported Platforms SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:

- dns-server
- domain
- ntp-server
- sip-domain
- sip-server

For example, to specify the DHCPv6 client requested option as **dns-server**:

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set req-option dns-server
```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set retransmission-attempt 6
```

3. Configure the **update-server** option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

4. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

5. Configure the two-message (rapid commit) exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```



NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [edit routing-instances] hierarchy.



NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.



NOTE: On all branch SRX Series devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 340](#)

Configuring Nontemporary Address Assignment

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

Nontemporary address assignment is also known as stateful address assignment. In the stateful address assignment mode, the DHCPv6 client requests global addresses from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the global addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

[edit]

```
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]

```
user@host# set client-type statefull
```

3. Specify the IA_NA assignment.

[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]

```
user@host# set client-ia-type ia-na
```

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 340](#)

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

The DHCPv6 client requests IPv6 addresses and prefixes from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the IPv6 addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure identity association for nontemporary addresses (IA_NA) and identity association for prefix delegation (IA_PD):

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

4. Specify the IA_PD.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

Related Documentation

- [Minimum DHCPv6 Client Configuration on page 340](#)

Configuring Auto-Prefix Delegation

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating router delegates IPv6 prefixes to a requesting router. The requesting router then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

To configure auto-prefix delegation:

1. Configure the DHCPv6 client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the identity association type as **ia-pd** for prefix delegation.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DUID type.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

5. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

**Related
Documentation**

- [Minimum DHCPv6 Client Configuration on page 340](#)
- [Configuring Optional DHCPv6 Client Attributes on page 341](#)

Configuring the DHCPv6 Client Rapid Commit Option

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

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:

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
```

**Related
Documentation**

- [DHCPv6 Client Overview on page 339](#)

Configuring a DHCPv6 Client in Autoconfig Mode

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

A DHCPv6 client configured in **autoconfig** mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in **autoconfig** mode:

1. Configure the DHCPv6 client type as **autoconfig**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

2. Specify the identity association type as **ia-na** for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the interface on which to configure router advertisement.

```
[edit protocols router-advertisement]
user@host# set interface ge-0/0/1.0
```

**Related
Documentation**

- [Minimum DHCPv6 Client Configuration on page 340](#)
- [Configuring Optional DHCPv6 Client Attributes on page 341](#)

Configuring TCP/IP Propagation on a DHCPv6 Client

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the **update-server** option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

2. Configure the address pool to specify the interface (where **update-server** is configured) from which TCP/IP settings can be propagated.

[edit access]

```
user@host# set address-assignment pool 2 family inet6 dhcp-attributes  
propagate-settings ge-0/0/0
```

**Related
Documentation**

- [DHCPv6 Client Overview on page 339](#)
- [Minimum DHCPv6 Client Configuration on page 340](#)

PART 5

Managing System Files

- [Performing File Management Tasks on page 351](#)

CHAPTER 16

Performing File Management Tasks

- [File Management Overview on page 351](#)
- [Decrypting Configuration Files on page 352](#)
- [Encrypting Configuration Files on page 352](#)
- [Modifying the Encryption Key on page 354](#)
- [Cleaning Up Files in J-Web on page 354](#)
- [Cleaning Up Files with the CLI on page 355](#)
- [Deleting Files on page 356](#)
- [Deleting the Backup Software Image on page 357](#)
- [Downloading Files on page 357](#)
- [Configuring RADIUS System Accounting on page 358](#)
- [Managing Accounting Files on page 361](#)

File Management Overview

Supported Platforms [SRX Series, vSRX](#)

You can use the J-Web user interface and the CLI to perform routine file management operations such as archiving log files and deleting unused log files, cleaning up temporary files and crash files, and downloading log files from the routing platform to your computer. You can also encrypt the configuration files with the CLI to prevent unauthorized users from viewing sensitive configuration information.

Before you perform any file management tasks, you must perform the initial device configuration described in the Getting Started Guide for your device.

**Related
Documentation**

- [Cleaning Up Files in J-Web on page 354](#)
- [Cleaning Up Files with the CLI on page 355](#)
- [Managing Accounting Files on page 361](#)
- [Encrypting Configuration Files on page 352](#)
- [Decrypting Configuration Files on page 352](#)

Decrypting Configuration Files

Supported Platforms [SRX Series, vSRX](#)

To disable the encryption of configuration files on a device and make them readable to all:

1. Enter operational mode in the CLI.
2. Verify your permission to decrypt configuration files on this device by entering the encryption key for the device.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
Verifying EEPROM stored encryption key:
```

3. At the second prompt, reenter the encryption key.
4. Enter configuration mode in the CLI.
5. Enable configuration file decryption.

```
[edit]
user@host# edit system
user@host# set no-encrypt-configuration-files
```

6. Begin the decryption process by committing the configuration.

```
[edit]
user@host# commit
commit complete
```

Related Documentation

- [Encrypting Configuration Files on page 352](#)

Encrypting Configuration Files

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

To configure an encryption key in EEPROM and determine the encryption process, enter one of the **request system set-encryption-key** commands in operational mode described in [Table 14 on page 353](#).



NOTE: The **request system set-encryption-key** command is not supported on high-end SRX Series devices; therefore, this task does not apply to such devices.

Table 14: request system set-encryption-key Commands

| CLI Command | Description |
|--|--|
| request system set-encryption-key | Sets the encryption key and enables default configuration file encryption: <ul style="list-style-type: none"> • AES encryption for the Canada and U.S. version of Junos OS • DES encryption for the international version of Junos OS |
| request system set-encryption-key algorithm des | Sets the encryption key and specifies configuration file encryption by DES. |
| request system set-encryption-key unique | Sets the encryption key and enables default configuration file encryption with a unique encryption key that includes the chassis serial number of the device. Configuration files encrypted with the unique key can be decrypted only on the current device. You cannot copy such configuration files to another device and decrypt them. |
| request system set-encryption-key des unique | Sets the encryption key and specifies configuration file encryption by DES with a unique encryption key. |

To encrypt configuration files on a device:

1. Enter operational mode in the CLI.
2. Configure an encryption key in EEPROM and determine the encryption process; for example, enter the **request system set-encryption-key** command.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
```

3. At the prompt, enter the encryption key. The encryption key must have at least six characters.

```
Enter EEPROM stored encryption key:juniper1
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the encryption key.
5. Enter configuration mode in the CLI.
6. Enable configuration file encryption to take place.

```
[edit]
user@host# edit system
user@host# set encrypt-configuration-files
```

7. Begin the encryption process by committing the configuration.

```
[edit]
user@host# commit
commit complete
```

Related Documentation

- [Managing Accounting Files on page 361](#)
- [Decrypting Configuration Files on page 352](#)

Modifying the Encryption Key

Supported Platforms [SRX Series, vSRX](#)

When you modify the encryption key, the configuration files are decrypted and then reencrypted with the new encryption key.

To modify the encryption key:

1. Enter operational mode in the CLI.
2. Configure a new encryption key in EEPROM and determine the encryption process; for example, enter the **request system set-encryption-key** command.

```
user@host> request system set-encryption-key
Enter EEPROM stored encryption key:
```

3. At the prompt, enter the new encryption key. The encryption key must have at least six characters.

```
Enter EEPROM stored encryption key:juniperone
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the new encryption key.

- Related Documentation**
- [Managing Accounting Files on page 361](#)
 - [Encrypting Configuration Files on page 352](#)
 - [Decrypting Configuration Files on page 352](#)

Cleaning Up Files in J-Web

Supported Platforms [SRX Series, vSRX](#)

You can use the J-Web user interface to rotate log files and delete unnecessary files on the device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives all information in the current log files and creates fresh log files.
- Deletes log files in **/var/log**—Deletes any files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes any files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes any core files that the device has written during an error.
- Deletes all software images (*.tgz files) in **/var/sw/pkg**—Deletes any software images copied to this directory during software upgrades.

To rotate log files and delete unnecessary files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The device rotates log files and identifies the files that can be safely deleted.

The J-Web user interface displays the files that you can delete and the amount of space that will be freed on the file system.

3. Click one of the following buttons on the confirmation page:
 - To delete the files and return to the Files page, click **OK**.
 - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation

- [Managing Accounting Files on page 361](#)
- [Encrypting Configuration Files on page 352](#)
- [Decrypting Configuration Files on page 352](#)
- [Cleaning Up Files with the CLI on page 355](#)

Cleaning Up Files with the CLI

Supported Platforms [SRX Series, vSRX](#)

You can use the CLI **request system storage cleanup** command to rotate log files and delete unnecessary files on the device. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives all information in the current log files, deletes old archives, and creates fresh log files.
- Deletes log files in **/var/log**—Deletes any files that are not currently being written to.
- Deletes temporary files in **/var/tmp**—Deletes any files that have not been accessed within two days.
- Deletes all crash files in **/var/crash**—Deletes any core files that the device has written during an error.
- Deletes all software images (***.tgz** files) in **/var/sw/pkg**—Deletes any software images copied to this directory during software upgrades.

To rotate log files and delete unnecessary files with the CLI:

1. Enter operational mode in the CLI.
2. Rotate log files and identify the files that can be safely deleted.

```
user@host> request system storage cleanup
```

The device rotates log files and displays the files that you can delete.

3. Enter **yes** at the prompt to delete the files.



NOTE: You can issue the `request system storage cleanup dry-run` command to review the list of files that can be deleted with the `request system storage cleanup` command, without actually deleting the files.



NOTE:

On SRX Series devices, the `/var` hierarchy is hosted in a separate partition (instead of the root partition). If Junos OS installation fails as a result of insufficient space:

- Use the `request system storage cleanup` command to delete temporary files.
- Delete any user-created files in both the root partition and under the `/var` hierarchy.

Related Documentation

- [Cleaning Up Files in J-Web on page 354](#)
- [Managing Accounting Files on page 361](#)
- [Encrypting Configuration Files on page 352](#)
- [Decrypting Configuration Files on page 352](#)

Deleting Files

Supported Platforms [SRX Series, vSRX](#)

You can use the J-Web user interface to delete an individual file from the device. When you delete the file, it is permanently removed from the file system.



CAUTION: If you are unsure whether to delete a file from the device, we recommend using the **Cleanup Files** tool. This tool determines which files can be safely deleted from the file system.

To delete files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Download and Delete Files section, click one of the following file types:
 - **Log Files**—Lists the log files located in the `/var/log` directory on the device.
 - **Temporary Files**—Lists the temporary files located in the `/var/tmp` directory on the device.

- **Old Junos OS**—Lists the software images in the (*.tgz files) in the /var/sw/pkg directory on the device.
- **Crash (Core) Files**—Lists the core files located in the /var/crash directory on the device.

The J-Web user interface displays the files located in the directory.

3. Check the box next to each file you plan to delete.
4. Click **Delete**.

The J-Web user interface displays the files you can delete and the amount of space that will be freed on the file system.

5. Click one of the following buttons on the confirmation page:
 - To delete the files and return to the Files page, click **OK**.
 - To cancel your entries and return to the list of files in the directory, click **Cancel**.

Related Documentation

- [Managing Accounting Files on page 361](#)

Deleting the Backup Software Image

Supported Platforms [SRX Series, vSRX](#)

Junos OS keeps a backup image of the software that was previously installed so that you can downgrade to that version of the software if necessary. You can use the J-Web user interface to delete this backup image. If you delete this image, you cannot downgrade to this particular version of the software.

To delete the backup software image:

1. In the J-Web user interface, select **Maintain > Files**.
2. Review the backup image information listed in the Delete Backup Junos Package section.
3. Click the **Delete backup Junos package** link to delete the backup image.
4. Click one of the following buttons on the confirmation page:
 - To delete the backup image and return to the Files page, click **OK**.
 - To cancel the deletion of the backup image and return to the Files page, click **Cancel**.

Related Documentation

- [Deleting Files on page 356](#)

Downloading Files

Supported Platforms [SRX Series, vSRX](#)

You can use the J-Web user interface to download a copy of an individual file from the device. When you download a file, it is not deleted from the file system.

To download files with the J-Web user interface:

1. In the J-Web user interface, select **Maintain>Files**.
2. In the Download and Delete Files section, click one of the following file types:
 - **Log Files**—Lists the log files located in the `/var/log` directory on the device.
 - **Temporary Files**—Lists the temporary files located in the `/var/tmp` directory on the device.
 - **Old Junos OS**—Lists the software images located in the (`*.tgz` files) in the `/var/sw/pkg` directory on the device.
 - **Crash (Core) Files**—Lists the core files located in the `/var/crash` directory on the device.

The J-Web user interface displays the files located in the directory.

3. Click **Download** to download an individual file.
4. Choose a location for the browser to save the file.

The file is downloaded.

**Related
Documentation**

- [Managing Accounting Files on page 361](#)

Configuring RADIUS System Accounting

Supported Platforms [EX Series, M Series, MX Series, OCX1100, PTX Series, QFX Series, SRX1500, SRX5400, SRX5600, SRX5800, T Series](#)

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

Tasks for configuring RADIUS system accounting are:

1. [Configuring Auditing of User Events on a RADIUS Server on page 358](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 359](#)
3. [Configuring RADIUS Server Accounting on page 359](#)

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the `[edit system accounting]` hierarchy level:

```
[edit system accounting]
destination {
  radius {
    server {
```

```

server-address {
    accounting-port port-number;
    max-outstanding-requests value;
    port port-number;
    retry value;
    secret password;
    source-address address;
    timeout seconds;
}
}
}
}

```

Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the **events** statement at the **[edit system accounting]** hierarchy level:

```

[edit system accounting]
events [ events ];

```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the **server** statement at the **[edit system accounting destination radius]** hierarchy level:

```

server {
    server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        secret password;
        source-address address;
        timeout seconds;
    }
}

```

server-address specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple **server** statements.



NOTE: If no RADIUS servers are configured at the **[edit system accounting destination radius]** statement hierarchy level, the Junos OS uses the RADIUS servers configured at the **[edit system radius-server]** hierarchy level.

accounting-port *port-number* specifies the RADIUS server accounting port number.

The default port number is 1813.



NOTE: If you enable RADIUS accounting at the `[edit access profile profile-name accounting-order]` hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the `accounting-port` statement.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the **secret** statement. If the password contains spaces, enclose the entire password in quotation marks (" ").

In the **source-address** statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address (in case if radius-server address is IPv4) or IPv6 address (in case if radius-server address is IPv6) configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the **retry** statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the **timeout** statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

If you use the **enhanced-accounting** statement at the `[edit system radius-options]` hierarchy level, the RADIUS attributes such as access method, remote port, and access privileges can be audited. You can limit the number of attribute values to be displayed for auditing by using the **enhanced-avs-max <number>** statement at the `[edit system accounting]` hierarchy level.

```
[edit system radius-options]
enhanced-accounting;

[edit system accounting]
enhanced-avs-max <number>;
```

When a Juniper Networks router or switch is configured with RADIUS accounting, it sends **Accounting-Start** and **Accounting-Stop** messages to the RADIUS server. These messages contain information about user activities such as software logins, configuration changes, and interactive commands. This information is typically used for monitoring a network, collecting usage statistics, and ensuring that users are billed properly.

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting:

```
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
```

```

server {
  10.5.5.5 {
    accounting-port 3333;
    secret $ABC123;
    source-address 10.1.1.1;
    retry 3;
    timeout 3;
  }
  10.6.6.6 secret $ABC123;
  10.7.7.7 secret $ABC123;
}
}
}
}
}

```

Managing Accounting Files

Supported Platforms [SRX1500](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [vSRX](#)

If you configure your system to capture accounting data in log files, set the location for your accounting files to the DRAM.

The default location for accounting files is the **cfs/var/log** directory on the CompactFlash (CF) card. The **nonpersistent** option minimizes the read/write traffic to your CF card. We recommend that you use the **nonpersistent** option for all accounting files configured on your system.

To store accounting log files in DRAM instead of the CF card:

1. Enter configuration mode in the CLI.
2. Create an accounting data log file in DRAM and replace *filename* with the name of the file.

```
[edit]
user@host# edit accounting-options file filename
```

3. Store accounting log files in the DRAM file.

```
[edit]
user@host# set file filename nonpersistent
```



CAUTION: If log files for accounting data are stored on DRAM, these files are lost when the device reboots. Therefore, we recommend that you back up these files periodically.

Related Documentation

- [Accounting Options Overview](#)

PART 6

Working with Junos OS Licenses

- [Managing Junos OS Licenses on page 365](#)

CHAPTER 17

Managing Junos OS Licenses

- [Junos OS Feature License Keys on page 365](#)
- [Software Feature Licenses for SRX Series Devices on page 367](#)
- [Displaying License Keys in J-Web on page 372](#)
- [Downloading License Keys on page 372](#)
- [Generating a License Key on page 372](#)
- [Saving License Keys on page 373](#)
- [Updating License Keys on page 373](#)
- [Example: Adding a New License Key on page 374](#)
- [Example: Deleting a License Key on page 377](#)

Junos OS Feature License Keys

Supported Platforms [SRX Series, vSRX](#)

This section contains the following topics:

- [License Key Components on page 365](#)
- [License Management Fields Summary on page 366](#)

License Key Components

A license key consists of two parts:

- **License ID**—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- **License data**—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string `XXXXXXXXXX` is the license ID, and the trailing block of data is the license data:

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx  
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx  
          xxxxxx xxxxxx xxx
```

The license data defines the device ID for which the license is valid and the version of the license.

License Management Fields Summary

The Licenses page displays a summary of licensed features that are configured on the device and a list of licenses that are installed on the device. The information on the license management page is summarized in [Table 15 on page 366](#).

Table 15: Summary of License Management Fields

| Field Name | Definition |
|---------------------------|--|
| Feature Summary | |
| Feature | Name of the licensed feature: <ul style="list-style-type: none"> • Features—Software feature licenses. • All features—All-inclusive licenses |
| Licenses Used | Number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used. |
| Licenses Installed | Number of licenses installed on the device for the particular feature. |
| Licenses Needed | Number of licenses required for legal use of the feature. Usage is determined by the configuration on the device: If a feature is configured and the license for that feature is not installed, a single license is needed. |
| Installed Licenses | |
| ID | Unique alphanumeric ID of the license. |
| State | Valid —The installed license key is valid. Invalid —The installed license key is not valid. |
| Version | Numeric version number of the license key. |
| Group | If the license defines a group license, this field displays the group definition. If the license requires a group license, this field displays the required group definition. NOTE: Because group licenses are currently unsupported, this field is always blank. |
| Enabled Features | Name of the feature that is enabled with the particular license. |
| Expiry | Verify that the expiration information for the license is correct. For Junos OS, only permanent licenses are supported. If a license has expired, it is shown as invalid. |

- Related Documentation**
- [Generating a License Key on page 372](#)
 - [Updating License Keys on page 373](#)
 - [Saving License Keys on page 373](#)

- [Downloading License Keys on page 372](#)

Software Feature Licenses for SRX Series Devices

Supported Platforms [SRX Series, vSRX](#)

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 16 on page 367](#) describes the Junos OS features that require licenses.

Table 16: Junos OS Feature Licenses

| Junos OS License Requirements | | | |
|--|---------|---------|--------------|
| Feature | SRX550M | SRX1500 | SRX5000 line |
| Access Manager | X | | |
| BGP Route Reflectors | | | |
| Dynamic VPN | X | | |
| IDP Signature Update* | X | X | X |
| Application Signature Update (Application Identification)* | X | | X |
| Juniper-Kaspersky Antivirus* | X | | |
| Juniper-Sophos Antivirus* | X | X | X |
| Juniper-Sophos Antispam* | X | X | X |
| Juniper-Enhanced Web filtering* | X | X | X |
| Juniper-Websense Web filtering* | X | | |
| Logical Systems | | | X |
| UTM | X | X | X |

* Indicates support on high-memory devices only.

[Table 17 on page 368](#) lists the licenses you can purchase for each SRX Series software feature. Each license allows you to run the specified advanced software features on a single device.

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Table 17: Junos OS Feature License Model Number for SRX Series Devices

| Licensed Software Feature | Supported Devices | Model Number |
|---|---------------------------|--------------------|
| Application Security and IDP updates (1 year, 3 years, and 5 years) | SRX550 | SRX550-APPSEC-A-1 |
| | | SRX550-APPSEC-A-3 |
| | | SRX550-APPSEC-A-5 |
| | SRX5400 | SRX5400-APPSEC-1 |
| | | SRX5400-APPSEC-3 |
| | | SRX5400-APPSEC-5 |
| | SRX5600 | SRX5600-APPSEC-A-1 |
| | | SRX5600-APPSEC-A-3 |
| | | SRX5600-APPSEC-A-5 |
| | SRX5800 | SRX5800-APPSEC-A-1 |
| | | SRX5800-APPSEC-A-3 |
| | | SRX5800-APPSEC-A-5 |
| IDP updates (1 year, 3 years, and 5 years) | SRX550 | SRX550-IDP |
| | | SRX550-IDP-3 |
| | | SRX550-IDP-5 |
| IDP subscription (1 year and 3 years) | SRX1500 | SRX1500-IPS-1 |
| | | SRX1500-IPS-3 |
| | SRX5400, SRX5600, SRX5800 | SRX5K-IDP |
| | | SRX5K-IDP-3 |
| | | SRX5K-IDP-3-R |
| | | SRX5K-IDP-R |
| Juniper-Kaspersky Antivirus updates (1 year, 3 years, and 5 years) | SRX550 | SRX550-K-AV |
| | | SRX550-K-AV-3 |
| | | SRX550-K-AV-5 |

Table 17: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|--|-------------------|-----------------|
| Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years) | SRX550 | SRX550-S-AV |
| | | SRX550-S-AV-3 |
| | | SRX550-S-AV-5 |
| Juniper-Sophos Antivirus updates (1 year, 3 years, and 5 years) | SRX5400 | SRX5400-S-AV-1 |
| | | SRX5400-S-AV-3 |
| | | SRX5400-S-AV-5 |
| Juniper-Sophos Antivirus updates (1 year) | SRX5600 | SRX5600-S-AV-1 |
| | SRX5800 | SRX5800-S-AV-1 |
| Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years) | SRX550 | SRX550-S2-AS |
| | | SRX550-S2-AS-3 |
| | | SRX550-S2-AS-5 |
| Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years) | SRX5400 | SRX5400-S-AV-1 |
| | | SRX5400-S-AV-3 |
| | | SRX5400-S-AV-5 |
| Juniper-Sophos Antispam updates (1 year, 3 years, and 5 years) | SRX5600 | SRX5600-S-AV-1 |
| | SRX5800 | SRX5800-S-AV-1 |
| Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years) | SRX550 | SRX550-W-EWF |
| | | SRX550-W-EWF-3 |
| | | SRX550-W-EWF-5 |
| Juniper-Enhanced Web filtering (1 year, 3 years, and 5 years) | SRX5400 | SRX5400-W-EWF-1 |
| | | SRX5400-W-EWF-3 |
| | | SRX5400-W-EWF-5 |
| Juniper-Enhanced Web filtering (1 year) | SRX5600 | SRX5600-W-EWF-1 |
| | SRX5800 | SRX5800-W-EWF-1 |

Table 17: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|---|-------------------|---------------------|
| Enterprise Bundle—Kaspersky Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years) | SRX550 | SRX550-SMB4-CS |
| | | SRX550-SMB4-CS-3 |
| | | SRX550-SMB4-CS-5 |
| Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years) | SRX550 | SRX550-S-SMB4- CS |
| | | SRX550-S-SMB4- CS-3 |
| | | SRX550-S-SMB4- CS-5 |
| Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years) | SRX1500 | SRX1500-CS-BUN-1 |
| | | SRX1500-CS-BUN-3 |
| Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year, 3 years, and 5 years) | SRX5400 | SRX5400-CS-BUN-1 |
| | | SRX5400-CS-BUN-3 |
| | | SRX5400-CS-BUN-5 |
| Enterprise Bundle—includes Sophos Antivirus, Enhanced Web Filtering, Sophos Antispam, AppSecure, and IDP (1 year) | SRX5600 | SRX5600-CS-BUN-1 |
| | SRX5800 | SRX5800-CS-BUN-1 |
| Dynamic VPN Client (5, 10, and 25 simultaneous users) | SRX550 | SRX-RAC-5-LTU |
| | | SRX-RAC-10-LTU |
| | | SRX-RAC-25-LTU |
| Dynamic VPN Service (5, 10, 25, and 50 simultaneous users) | SRX550 | SRX-RAC-5-LTU |
| | SRX550 | SRX-RAC-10-LTU |
| | SRX550 | SRX-RAC-25-LTU |
| | SRX550 | SRX-RAC-50-LTU |
| Dynamic VPN Service (100 and 150 simultaneous users) | SRX550 | SRX-RAC-100-LTU |
| | | SRX-RAC-150-LTU |
| Dynamic VPN Service (250 simultaneous users) | SRX550 | SRX-RAC-250-LTU |
| NOTE: Requires Junos OS 11.2R3 or later | | |

Table 17: Junos OS Feature License Model Number for SRX Series Devices (*continued*)

| Licensed Software Feature | Supported Devices | Model Number |
|---|--|------------------------------------|
| Dynamic VPN Service (500 simultaneous users) | SRX550 NOTE: Requires Junos OS 11.2R3 or later | SRX-RAC-500-LTU |
| Express Path License (formerly known as <i>services offloading</i>) NOTE: Prior to Junos OS Release 12.3X48-D10, Express Path was a licensed software feature. Starting with Junos OS Release 12.3X48-D10, the Express Path license is no longer required to enable this functionality. Your previously acquired Express Path license will not be effective anymore. | SRX5400, SRX5600, SRX5800 | SRX5K-SVCS-OFFLOAD-RTU |
| Logical Systems License (incremental 1, 5, and 25 numbers) | SRX5400 | SRX-5400-LSYS-1 |
| | | SRX-5400-LSYS-5 |
| | | SRX-5400-LSYS-25 |
| | SRX5600 | SRX-5600-LSYS-1 |
| | | SRX-5600-LSYS-5 |
| | | SRX-5600-LSYS-25 |
| | SRX5800 | SRX-5800-LSYS-1 |
| | | SRX-5800-LSYS-5 |
| | | SRX-5800-LSYS-25 |
| Sky Advanced Threat protection (1 year, 3 years) | SRX1500 | SRX1500-ATP-1 SRX1500-ATP-3 |
| Command and Control feeds (1 year, 3 years) | SRX1500 | SPOT-CC-1500-1Y SPOT-CC-1500-3Y |

- Related Documentation**
- *License Enforcement*
 - *Junos OS Feature License Keys*

Displaying License Keys in J-Web

Supported Platforms [SRX Series, vSRX](#)

To display license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the device.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

- Related Documentation**
- [Junos OS Feature License Keys on page 365](#)
 - [Generating a License Key on page 372](#)
 - [Example: Adding a New License Key on page 374](#)
 - [Example: Deleting a License Key on page 377](#)
 - [Downloading License Keys on page 372](#)

Downloading License Keys

Supported Platforms [SRX Series, vSRX](#)

To download license keys installed on the device:

1. In the J-Web interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the device to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written.

- Related Documentation**
- [Junos OS Feature License Keys on page 365](#)
 - [Generating a License Key on page 372](#)
 - [Example: Adding a New License Key on page 374](#)
 - [Example: Deleting a License Key on page 377](#)

Generating a License Key

Supported Platforms [SRX Series, vSRX](#)

To generate a license key:

1. Gather the authorization code that you received when you purchased your license as well as your device serial number.

2. Go to the Juniper Networks licensing page at:
<https://www.juniper.net/lcrs/generateLicense.do>
3. Enter the device serial number and authorization code in the webpage and click **Generate**. Depending on the type of license you purchased, you will receive one of the following responses:
 - License key—If you purchased a perpetual license, you will receive a license key from the licensing management system. You can enter this key directly into the system to activate the feature on your device.
 - License key entitlement—If you purchased a subscription-based license, you will receive a license key entitlement from the licensing management system. You can use this entitlement to validate your license on the Juniper Networks licensing server and download the feature license from the server to your device.

Related Documentation

- [Example: Adding a New License Key on page 374](#)
- [Example: Deleting a License Key on page 377](#)
- [Updating License Keys on page 373](#)
- [Downloading License Keys on page 372](#)

Saving License Keys

Supported Platforms [SRX Series, vSRX](#)

To save license keys installed on the device:

1. From operational mode, save the installed license keys to a file or URL.

```
user@host>request system license save filename | url
```

For example, the following command saves the installed license keys to a file named `license.config`:

```
request system license save ftp://user@host/license.conf
```

Related Documentation

- [Junos OS Feature License Keys on page 365](#)
- [Generating a License Key on page 372](#)
- [Example: Adding a New License Key on page 374](#)
- [Example: Deleting a License Key on page 377](#)
- [Downloading License Keys on page 372](#)

Updating License Keys

Supported Platforms [SRX Series, vSRX](#)

To update a license key from the device:

1. From operational mode, do one of the following tasks:

- Update the license keys automatically.

```
user@host> request system license update
```



NOTE: The `request system license update` command will always use the default Juniper license server <https://ae1.juniper.net>

You can only use this command to update subscription-based licenses (such as UTM).

- Update the trial license keys automatically.

```
user@host>request system license update trial
```

Related Documentation

- [Junos OS Feature License Keys on page 365](#)
- [Generating a License Key on page 372](#)
- [Example: Adding a New License Key on page 374](#)
- [Example: Deleting a License Key on page 377](#)
- [Downloading License Keys on page 372](#)

Example: Adding a New License Key

Supported Platforms [SRX Series, vSRX](#)

This example shows how to add a new license key.

- [Requirements on page 374](#)
- [Overview on page 374](#)
- [Configuration on page 375](#)
- [Verification on page 376](#)

Requirements

Before you begin, confirm that your Junos OS feature requires you to purchase, install, and manage a separate software license.

Overview

You can add a license key from a file or URL, from a terminal, or from the J-Web user interface. Use the ***filename*** option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.) Use the ***url*** to send a subscription-based license key entitlement (such as UTM) to the Juniper Networks licensing server for authorization. If authorized, the server downloads the license to the device and activates it.

In this example, the file name is `bgp-reflection`.

Configuration

CLI Quick Configuration To quickly configure this section of the example, 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.

From operational mode, you can add a license key in either way:

- From a file or URL:

```
user@hostname> request system license add bgp-reflection
```
- From the terminal:

```
user@hostname> request system license add terminal
```

GUI Step-by-Step Procedure To add a new license key:

1. In the J-Web user interface, select **Maintain>Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do one of the following, using a blank line to separate multiple license keys:
 - In the **License File URL** box, type the full URL to the destination file containing the license key to be added.
 - In the **License Key Text** box, paste the license key text, in plain-text format, for the license to be added.
4. Click **OK** to add the license key.
5. Click **OK** to check your configuration and save it as a candidate configuration.
6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure To add a new license key:

1. From operational mode, add a license key in either way:
 - From a file or URL:

```
user@host> request system license add bgp-reflection
```
 - From the terminal:

```
user@host>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 is generated when you press Ctrl-D to exit license entry mode.

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

```
user@hostname> show system license
```

License usage:

| Feature name | Licenses used | Licenses installed | Licenses needed | Expiry |
|----------------|------------------|-----------------------|--------------------|-----------|
| bgp-reflection | 0 | 1 | 0 | permanent |

Licenses installed:

License identifier: G0300000xxxx

License version: 2

Valid for device: JN001875AB

Features:

bgp-reflection - Border Gateway Protocol route reflection
permanent

License identifier: G0300000xxxx

License version: 2

Valid for device: JN001875AB

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying Installed Licenses

Purpose Verify that the expected licenses have been installed and are active on the device.

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

The output shows a list of the licenses used and a list of the licenses installed on the device and when they expire.

Verifying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From operational mode, enter the **show system license usage** command.

```
user@hostname> show system license usage
```

| Feature name | Licenses used | Licenses installed | Licenses needed | Expiry |
|----------------|------------------|-----------------------|--------------------|-----------|
| bgp-reflection | 1 | 1 | 0 | permanent |

The output shows a list of the licenses installed on the device and how they are used.

Verifying Installed License Keys

Purpose Verify that the license keys were installed on the device.

Action From operational mode, enter the **show system license keys** command.

```
user@hostname> show system license keys
```

```
XXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
          xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
```

The output shows a list of the license keys installed on the device. Verify that each expected license key is present.

Related Documentation

- [Junos OS Feature License Keys on page 365](#)
- [Generating a License Key on page 372](#)
- [Example: Deleting a License Key on page 377](#)
- [Updating License Keys on page 373](#)
- [Downloading License Keys on page 372](#)

Example: Deleting a License Key

Supported Platforms [SRX Series, vSRX](#)

This example shows how to delete a license key.

- [Requirements on page 377](#)
- [Overview on page 377](#)
- [Configuration on page 377](#)
- [Verification on page 378](#)

Requirements

Before you delete a license key, confirm that it is no longer needed.

Overview

You can delete a license key from the CLI or J-Web user interface. In this example, the license ID is G0300000xxxx.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, 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.

```
user@host> request system license delete G0300000xxxx
```

| | |
|-----------------------------------|---|
| GUI Step-by-Step Procedure | <p>To delete a license key:</p> <ol style="list-style-type: none">1. In the J-Web user interface, select Maintain>Licenses.2. Select the check box of the license or licenses you want to delete.3. Click Delete.4. Click OK to check your configuration and save it as a candidate configuration.5. If you are done configuring the device, click Commit Options>Commit. |
| Step-by-Step Procedure | <p>To delete a license key:</p> <ol style="list-style-type: none">1. From operational mode, for each license, enter the following command and specify the license ID. You can delete only one license at a time. user@host> request system license delete G0300000xxxx |
| Results | <p>From configuration mode, confirm your deletion by entering the show system license command. The license key you deleted will be removed. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.</p> <p>If you are done configuring the device, enter commit from configuration mode.</p> |

Verification

Confirm that the configuration is working properly.

- [Verifying Installed Licenses on page 378](#)

Verifying Installed Licenses

| | |
|------------------------------|---|
| Purpose | Verify that the expected licenses have been removed from the device. |
| Action | From operational mode, enter the show system license command. |
| Related Documentation | <ul style="list-style-type: none">• Generating a License Key on page 372• Example: Adding a New License Key on page 374• Updating License Keys on page 373• Downloading License Keys on page 372 |

PART 7

Configuration Statements and Operational Commands

- Configuration Statements on page 381
- Operational Commands on page 515

CHAPTER 18

Configuration Statements

- [\[edit security certificates\] Hierarchy Level on page 383](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 384](#)
- [Groups Configuration Statement Hierarchy on page 384](#)
- [System Configuration Statement Hierarchy on page 385](#)
- [address-assignment \(Access\) on page 416](#)
- [address-pool \(Access\) on page 419](#)
- [allow-configuration on page 420](#)
- [allow-configuration-regexps on page 420](#)
- [authentication-key on page 421](#)
- [authentication-order on page 422](#)
- [boot-server \(NTP\) on page 423](#)
- [broadcast on page 424](#)
- [broadcast-client on page 425](#)
- [ciphers on page 426](#)
- [connection-limit on page 427](#)
- [client-ia-type on page 428](#)
- [client-identifier \(dhcp-client\) on page 428](#)
- [client-identifier \(dhcpv6-client\) on page 429](#)
- [client-list-name \(SNMP\) on page 429](#)
- [client-type on page 430](#)
- [deny-configuration on page 430](#)
- [deny-configuration-regexps on page 431](#)
- [destination \(Accounting\) on page 432](#)
- [dhcp-attributes \(Access IPv4 Address Pools\) on page 433](#)
- [dhcp-attributes \(Access IPv6 Address Pools\) on page 435](#)
- [dhcp-client on page 436](#)
- [dhcp-local-server \(System Services\) on page 437](#)
- [dhcpv6 \(System Services\) on page 441](#)

- [dhcpv6-client](#) on page 444
- [disable \(System Services\)](#) on page 445
- [dlv](#) on page 445
- [dynamic-pool](#) on page 446
- [dynamic-server](#) on page 447
- [family \(Security Forwarding Options\)](#) on page 448
- [file \(System Logging\)](#) on page 449
- [forwarding-options \(Security\)](#) on page 452
- [group \(System Services DHCP\)](#) on page 453
- [host \(SSH Known Hosts\)](#) on page 456
- [hostkey-algorithm](#) on page 457
- [idle-timeout \(System\)](#) on page 458
- [interface \(System Services DHCP\)](#) on page 459
- [interfaces \(ARP\)](#) on page 460
- [interfaces \(Security Zones\)](#) on page 461
- [interface-traceoptions \(System Services DHCP\)](#) on page 462
- [internet-options](#) on page 464
- [kernel-replication \(System\)](#) on page 465
- [lease-time \(dhcp-client\)](#) on page 465
- [location](#) on page 466
- [lockout-period](#) on page 467
- [macs](#) on page 468
- [max-pre-authentication-packets](#) on page 469
- [multicast-client](#) on page 469
- [name-server \(Access\)](#) on page 470
- [neighbor-discovery-router-advertisement \(Access\)](#) on page 470
- [ntp](#) on page 471
- [outbound-ssh](#) on page 472
- [overrides \(System Services DHCP\)](#) on page 474
- [peer \(NTP\)](#) on page 475
- [prefix](#) on page 476
- [profilerd](#) on page 477
- [proxy](#) on page 478
- [radius-options](#) on page 479
- [radius-server](#) on page 480
- [rapid-commit](#) on page 481
- [reconfigure \(System Services DHCP\)](#) on page 482

- [req-option](#) on page 483
- [retransmission-attempt \(dhcp-client\)](#) on page 484
- [retransmission-attempt \(dhcpv6-client\)](#) on page 484
- [retransmission-interval \(dhcp-client\)](#) on page 485
- [root-authentication](#) on page 486
- [single-connection](#) on page 487
- [server \(NTP\)](#) on page 488
- [server-address \(dhcp-client\)](#) on page 489
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\)](#) on page 489
- [ssh-known-hosts](#) on page 490
- [static-subscribers](#) on page 491
- [statistics-service](#) on page 491
- [subscriber-management](#) on page 492
- [subscriber-management-helper](#) on page 493
- [system master password](#) on page 494
- [tacplus](#) on page 495
- [tacplus-options](#) on page 496
- [tacplus-server](#) on page 497
- [traceoptions \(Outbound SSH\)](#) on page 499
- [traceoptions \(System Services DHCP\)](#) on page 501
- [trusted-key](#) on page 503
- [uac-service](#) on page 504
- [update-router-advertisement](#) on page 505
- [update-server \(dhcp-client\)](#) on page 505
- [update-server \(dhcpv6-client\)](#) on page 506
- [usb-control](#) on page 506
- [use-interface](#) on page 507
- [user-id](#) on page 507
- [vendor-id](#) on page 508
- [vpn \(Forwarding Options\)](#) on page 508
- [watchdog](#) on page 509
- [web-management](#) on page 510
- [web-management \(System Services\)](#) on page 511

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

Supported Platforms [SRX Series, vSRX](#)

```
security {
```

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority profile-name {
    ca-name name;
    crl filename;
    encoding (binary | pem);
    enrollment-url url;
    file filename;
    ldap-url url;
  }
  enrollment-retry number;
  local name {
    certificate;
    load-key-file url;
  }
  maximum-certificates number;
  path-length length;
}
```

**Related
Documentation**

- [Security Configuration Statement Hierarchy](#)
- [Installation and Upgrade Guide](#)

[edit security ssh-known-hosts] Hierarchy Level

Supported Platforms [SRX Series, vSRX](#)

```
security {
  ssh-known-hosts {
    fetch-from-server server-name;
    host hostname {
      dsa-key dsa-key;
      ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
      ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
      ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
      rsa-key rsa-key;
      rsa1-key rsa1-key;
    }
    load-key-file key-file;
  }
}
```

**Related
Documentation**

- [Security Configuration Statement Hierarchy](#)

Groups Configuration Statement Hierarchy

Supported Platforms [SRX Series, vSRX](#)

Use the statements in the **groups** configuration hierarchy to configure information that can be dynamically updated in various parts of the device configuration.

```

groups {
  group-name {
    configuration-data ;
  }
}

```

**Related
Documentation**

- [Understanding Junos OS Configuration Groups](#)

System Configuration Statement Hierarchy

Supported Platforms [SRX Series, vSRX](#)

Use the statements in the **system** configuration hierarchy to configure system management functions including addresses of the Domain Name System (DNS) servers; device's hostname, address, and domain name; health monitoring; interface filtering; properties of the device's auxiliary and console ports; security profiles for logical systems; time zones and Network Time Protocol (NTP) properties; trace options; and user login accounts, including user authentication and the root-level user account. Statement descriptions that are exclusive to the SRX Series devices running Junos OS are described in this section.

```

system {
  accounting {
    destination {
      radius {
        server server-address {
          accounting-port port-number;
          max-outstanding-requests number;
          port number;
          retry number;
          secret password;
          source-address address;
          timeout seconds;
        }
      }
    }
    tacplus {
      server server-address {
        port port-number;
        secret password;
        single-connection;
        source-address source-address;
        timeout seconds;
      }
    }
  }
  events [change-log interactive-commands login];
  traceoptions {
    file {
      filename;
      files number;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
  }
}

```

```
        flag flag;  
        no-remote-trace;  
    }  
}  
allow-v4mapped-packets;  
archival {  
    configuration {  
        archive-sites url {  
            password password;  
        }  
        transfer-interval interval;  
        transfer-on-commit;  
    }  
}  
arp {  
    aging-timer minutes;  
    gratuitous-arp-delay seconds;  
    gratuitous-arp-on-ifup;  
    interfaces {  
        interface name {  
            aging-timer minutes;  
        }  
    }  
    passive-learning;  
    purging;  
}  
authentication-order [password radius tacplus];  
auto-configuration {  
    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;  
    }  
}  
auto-snapshot;  
autoinstallation {  
    configuration-servers {  
        url {  
            password password;  
        }  
    }  
    interfaces {  
        interface-name {  
            bootp;  
            rarp;  
        }  
    }  
}  
usb {  
    disable;
```

```

    }
  }
  auto-snapshot;
  backup-router {
    address;
    destination [network];
  }
  commit {
    server {
      commit-interval seconds;
      days-to-keep-error-logs days;
      maximum-aggregate-pool number;
      maximum entries number;
      traceoptions {
        file {
          filename;
          files number;
          microsecond-stamp;
          size maximum-file-size;
          (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
      }
    }
    synchronize;
  }
  compress-configuration-files;
  default-address-selection;
  diag-port-authentication {
    encrypted-password password;
    plain-text-password;
  }
  domain-name domain-name;
  domain-search [domain-list];
  donot-disable-ip6op-ondad;
  dump-device (boot-device | compact-flash | usb);
  dynamic-profile-options {
    versioning;
  }
  encrypt-configuration-files;
  extensions {
    providers {
      provider-id {
        license-type license deployment-scope [deployments];
      }
    }
    resource-limits {
      package package-name {
        resources {
          cpu {
            priority number;
            time seconds;
          }
          file {
            core-size bytes;

```

```

        open number;
        size bytes;
    }
    memory {
        data-size mbytes;
        locked-in mbytes;
        resident-set-size mbytes;
        socket-buffers mbytes;
        stack-size mbytes;
    }
}
}
process process-ui-name {
    resources {
        cpu {
            priority number;
            time seconds;
        }
        file {
            core-size bytes;
            open number;
            size bytes;
        }
        memory {
            data-size mbytes;
            locked-in mbytes;
            resident-set-size mbytes;
            socket-buffers mbytes;
            stack-size mbytes;
        }
    }
}
}
}
fips {
    level (0 | 1 | 2 | 3 | 4);
}
host-name hostname;
inet6-backup-router {
    address;
    destination destination;
}
internet-options {
    icmpv4-rate-limit {
        bucket-size seconds;
        packet-rate packets-per-second;
    }
    icmpv6-rate-limit {
        bucket-size seconds;
        packet-rate packets-per-second;
    }
}
(ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
ipv6-duplicate-addr-detection-transmits number;
(ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
ipv6-path-mtu-discovery-timeout minutes;
no-tcp-reset (drop-all-tcp | drop-tcp-with-syn-only);

```

```

no-tcp-rfc1323;
no-tcp-rfc1323-paws;
(path-mtu-discovery | no-path-mtu-discovery);
source-port upper-limit upper-limit;
(source-quench | no-source-quench);
tcp-drop-synfin-set;
tcp-mss bytes;
}
kernel-replication;
license {
  autoupdate {
    url url;
    password password;
  }
  renew {
    before-expiration number;
    interval interval-hours;
  }
  traceoptions {
    file {
      filename ;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
location {
  altitude feet;
  building name;
  country-code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
login {
  announcement text;
  class class-name {
    access-end hh:mm;
    access-start hh:mm;
    allow-commands regular-expression;
    allow-configuration regular-expression;
    allow-configuration-regexps [regular-expression];
    allowed-days [day];
    deny-commands regular-expression;
    deny-configuration regular-expression;
    deny-configuration-regexps [regular-expression];
  }
}

```

```
    idle-timeout minutes;  
    logical-system logical-system;  
    login-alarms;  
    login-script script;  
    login-tip;  
    permissions [permissions ];  
    security-role (audit-administrator | crypto-administrator | ids-administrator |  
        security-administrator);  
}  
deny-sources {  
    address [address-or-hostname];  
}  
message text;  
}  
password {  
    change-type (character-set | set-transitions);  
    format (des | md5 | sha1);  
    maximum-length length;  
    minimum-changes number;  
    minimum-length length;  
}  
retry-options {  
    backoff-factor seconds;  
    backoff-threshold number;  
    lockout-period time;  
    maximum-time seconds;  
    minimum-time seconds;  
    tries-before-disconnect number;  
}  
user username {  
    authentication {  
        encrypted-password password;  
        load-key-file url;  
        plain-text-password;  
        ssh-dsa public-key;  
        ssh-rsa public-key;  
    }  
    class class-name;  
    full-name complete-name;  
    uid uid-value;  
}  
}  
log-vital {  
    interval minutes;  
    files days;  
    storage-limit percentage;  
    file-size Mbytes;  
    add oid{  
        comment comment;  
    }  
}  
group {  
    operating;  
    idp;  
    storage;  
    cluster-counter;  
    screen zone-name;
```

```

    spu spu-name;
  }
}
max-configuration-rollback number;
max-configurations-on-flash number;
mirror-flash-on-disk;
name-server ip-address;
nd-maxmcast-solicit value;
nd-retransmit-timer value;
no-compress-configuration-files;
no-debugger-on-alt-break;
no-multicast-echo;
no-neighbor-learn;
no-ping-record-route;
no-ping-time-stamp;
no-redirects;
no-saved-core-context;
ntp {
  authentication-key key-number {
    type md5;
    value password;
  }
  boot-server address;
  broadcast broadcast-address {
    key key;
    ttl value;
    version version;
  }
  broadcast-client;
  multicast-client {
    address;
  }
  peer peer-address {
    key key;
    prefer;
    version version;
  }
  server server-address {
    key key;
    prefer;
    version version;
  }
  source-address source-address;
  trusted-key [key-number];
}
pic-console-authentication {
  encrypted-password password;
  plain-text-password;
}
ports {
  auxiliary {
    disable;
    insecure;
    type (ansi | small-xterm | vt100 | xterm);
  }
  console {

```

```
        disable;
        insecure;
        log-out-on-disconnect;
        type (ansi | small-xterm | vt100 | xterm);
    }
}
processes {
    802.1x-protocol-daemon {
        command binary-file-path;
        disable;
    }
    adaptive-services {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    alarm-control {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    application-identification {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    application-security {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    audit-process {
        command binary-file-path;
        disable;
    }
    auto-configuration {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    bootp {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    chassis-control {
        disable;
        failover alternate-media;
    }
    class-of-service {
        command binary-file-path;
        disable;
        failover (alternate-media | other-routing-engine);
    }
    craft-control {
        command binary-file-path;
```

```

    disable;
    failover (alternate-media | other-routing-engine);
}
database-replication {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
datapath-trace-service {
    disable;
    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;
    }
}
dhcp {
    command binary-file-path;
    disable;
}
dhcp-service {
    disable;
    failover (alternate-media | other-routing-engine);
    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;
    }
    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;
    }
}
dialer-services {

```

```
disable;
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
diameter-service {
  disable;
  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;
  }
}
}
disk-monitoring {
  command binary-file-path;
  disable;
}
dynamic-flow-capture {
  command binary-file-path;
  disable;
}
ecc-error-logging {
  command binary-file-path;
  disable;
}
ethernet-connectivity-fault-management {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ethernet-link-fault-management {
  command binary-file-path;
  disable;
}
ethernet-switching {
  command binary-file-path;
  disable;
}
event-processing {
  command binary-file-path;
  disable;
```

```

}
fipsd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
firewall-authentication-service {
    disable;
}
forwarding {
    command binary-file-path;
    disable;
}
general-authentication-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
gprs-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
group-key-member {
    disable;
}
group-key-server {
    disable;
}
idp-policy {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ilmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
inet-process {
    command binary-file-path;
    disable;
}

```

```
    failover (alternate-media | other-routing-engine);
}
init {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
interface-control {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ipmi {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
ipsec-key-management {
    (disable | enable);
}
jsrp-service {
    disable;
}
jtasktest {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
kernel-replication {
    command binary-file-path;
    disable;
}
l2-learning {
    command binary-file-path;
    disable;
}
l2cpd-service {
    command binary-file-path;
    disable;
}
lACP {
    command binary-file-path;
    disable;
}
lldpd-service {
    command binary-file-path;
    disable;
}
logical-system-mux {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
logical-system-service {
    disable;
    traceoptions {
```

```

    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
mib-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mobile-ip {
    command binary-file-path;
    disable;
}
mountd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
mspd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
multicast-snooping {
    command binary-file-path;
    disable;
}
named-service {
    disable;
    failover (alternate-media | other-routing-engine);
}
neighbor-liveness {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
network-security {
    disable;
}
network-security-trace {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
nfsd-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}

```

```
ntp {
  disable;
  failover (alternate-media | other-routing-engine);
}
ntpd-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
peer-selection-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
periodic-packet-services {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
pgcp-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
pgm {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
pic-services-logging {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
ppp {
  command binary-file-path;
  disable;
}
pppoe {
  command binary-file-path;
  disable;
}
process-monitor {
  disable;
  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;
  }
}
```

```

}
profilerd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
r2cp {
    command binary-file-path;
    disable;
}
redundancy-interface-process {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
remote-operations {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
resource-cleanup {
    disable;
    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;
    }
}
routing {
    disable;
    failover (alternate-media | other-routing-engine);
}
sampling {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
sbc-configuration-process {
    disable;
    failover (alternate-media | other-routing-engine);
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
    }
}

```

```
        no-remote-trace;
    }
}
sdk-service {
    disable;
    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;
    }
}
secure-neighbor-discovery {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
security-log {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
send {
    disable;
}
service-deployment {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
shm-rtssdbd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
simple-mail-client-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
smtpd-service {
    disable;
}
snmp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
static-subscribers {
    disable;
```

```

}
statistics-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
subscriber-management {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
subscriber-management-helper {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
system-health-management {
    disable;
}
system-log-vital {
    disable;
}
tunnel-oamd {
    command binary-file-path;
    disable;
}
uac-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
usb-control {
    command binary-file-path;
    disable;
}
virtualization-service {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
vrrp {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
wan-acceleration {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
    }
}

```

```
        no-remote-trace;
    }
}
watchdog {
    enable;
    disable;
    timeout value;
}
web-management {
    disable;
    failover (alternate media | other-routing-engine);
}
wireless-lan-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
wireless-wan-service {
    disable;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
proxy {
    password password;
    port port-number;
    server url;
    username user-name;
}
radius-options {
    attributes {
        nas-ip-address nas-ip-address;
    }
    password-protocol mschap-v2;
}
radius-server server-address {
    accounting-port number;
    max-outstanding-requests number;
    port number;
```

```

    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
root-authentication {
    encrypted-password password;
    load-key-file url;
    plain-text-password;
    ssh-dsa public-key {
        <from pattern-list>;
    }
    ssh-rsa public-key {
        <from pattern-list>;
    }
}
saved-core-context;
saved-core-files number;
scripts {
    commit {
        allow-transients;
        direct-access;
        file filename {
            checksum (md5 | sha-256 | sha1);
            optional;
            refresh;
            refresh-from url;
            source url;
        }
    }
    refresh;
    refresh-from url;
    traceoptions {
        file {
            filename;
            files number;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
load-scripts-from-flash;
op {
    file filename {
        arguments name {
            description text;
        }
        checksum (md5 | sha-256 | sha1);
        command filename-alias;
        description cli-help-text;
        refresh;
        refresh-from url;
        source url;
    }
    no-allow-url;
}

```

```
refresh;
refresh-from url;
traceoptions {
  file {
    filename;
    files number;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
}
security-profile security-profile-name {
  address-book {
    maximum amount;
    reserved amount;
  }
  appfw-profile {
    maximum amount;
    reserved amount;
  }
  appfw-rule {
    maximum amount;
    reserved amount;
  }
  appfw-rule-set {
    maximum amount;
    reserved amount;
  }
  auth-entry {
    maximum amount;
    reserved amount;
  }
  cpu {
    reserved percent;
  }
  dslite-software-initiator {
    maximum amount;
    reserved amount;
  }
  flow-gate {
    maximum amount;
    reserved amount;
  }
  flow-session {
    maximum amount;
    reserved amount;
  }
  idp-policy idp-policy-name;
  logical-system logical-system-name;
  nat-cone-binding {
    maximum amount;
    reserved amount;
  }
  nat-destination-pool {
```

```
    maximum amount;
    reserved amount;
}
nat-destination-rule {
    maximum amount;
    reserved amount;
}
nat-interface-port-ol {
    maximum amount;
    reserved amount;
}
nat-nopat-address {
    maximum amount;
    reserved amount;
}
nat-pat-address {
    maximum amount;
    reserved amount;
}
nat-pat-portnum {
    maximum amount
    reserved amount
}
nat-port-ol-ipnumber {
    maximum amount;
    reserved amount;
}
nat-rule-referenced-prefix {
    maximum amount;
    reserved amount;
}
nat-source-pool {
    maximum amount;
    reserved amount;
}
nat-source-rule {
    maximum amount;
    reserved amount;
}
nat-static-rule {
    maximum amount;
    reserved amount;
}
policy {
    maximum amount;
    reserved amount;
}
policy-with-count {
    maximum amount;
    reserved amount;
}
root-logical-system;
scheduler {
    maximum amount;
    reserved amount;
}
```

```

    zone {
        maximum amount;
        reserved amount;
    }
}
security-profile-resources {
    cpu-control;
    cpu-control-target percent;
}
services {
    database-replication {
        traceoptions {
            file {
                filename ;
                files number;
                match regular-expression;
                size maximum-file-size;
                (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
        }
    }
}
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time (infinite | seconds);
    domain-name domain-name;
    domain-search dns-search-suffix;
    maximum-lease-time (infinite | seconds);
    name-server ip-address;
    next-server ip-address;
    option option-identifier-code array type-name [ type-values ] | byte 8-bit-value | flag
        (false | off | on | true) | integer signed-32-bit-value | ip-address address | short
        signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
        unsigned-short 16-bit-value);
    pool subnet-ip-address/mask {
        address-range {
            high address;
            low address;
        }
        boot-file filename;
        boot-server (address | hostname);
        default-lease-time (infinite | seconds);
        domain-name domain-name;
        domain-search dns-search-suffix;
        exclude-address ip-address;
        maximum-lease-time (infinite | seconds);
        name-server ip-address;
        next-server ip-address;
        option option-identifier-code array type-name [ type-values ] | byte 8-bit-value |
            flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
            short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
            unsigned-short 16-bit-value);
        propagate-ppp-settings interface-name;
        propagate-settings interface-name;
    }
}

```

```

router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
wins-server ip-address;
}
propagate-ppp-settings interface-name;
propagate-settings interface-name;
router ip-address;
server-identifier dhcp-server;
sip-server {
    address ip-address;
    name sip-server-name;
}
static-binding mac-address;
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;
}
wins-server ip-address;
}
dhcp-local-server {
    dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
    }
    junos-default-profile;
}

```

```
    use-primary dynamic-profile-name;
}
group group-name {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix;
    }
  }
}
dynamic-profile {
  profile-name;
  aggregate-clients {
    merge;
    replace;
  }
  junos-default-profile;
  use-primary dynamic-profile;
}
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
  }
  junos-default-profile;
  use-primary dynamic-profile-name;
}
exclude;
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
service-profile service-profile-name
trace ;
upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
```

```

}
method {
  bfd {
    detection-time {
      threshold milliseconds;
    }
    holddown-interval interval;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    session-mode (automatic | multihop | single-hop);
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version (0 | 1 | automatic);
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
reconfigure {
  attempts number;
  clear-on-abort;
  strict;
  timeout number;
  token token-name;
  trigger {
    radius-disconnect;
  }
}
service-profile service-profile-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
}
method {
  bfd {
    detection-time {
      threshold milliseconds;
    }
    holddown-interval interval;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    session-mode (automatic | multihop | single-hop);
  }
}

```

```

        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
group group-name {
    interface interface-name {
        exclude;
        upto upto-interface-name;
    }
}
}
dns {
    dns-proxy {
        cache hostname inet ip-address;
        default-domain domain-name {
            forwarders ip-address;
        }
        interface interface-name;
        propogate-setting (enable | disable);
        view view-name {
            domain domain-name {
                forward-only;
                forwarders ip-address;
            }
            match-clients subnet-address;
        }
    }
}
}
dnssec {
    disable;
    dlv {
        domain-name domain-name trusted-anchor trusted-anchor;
    }
}

```

```

secure-domains domain-name;
  trusted-keys (key dns-key | load-key-file url);
forwarders {
  ip-address;
}
max-cache-ttl seconds;
max-ncache-ttl seconds;
traceoptions {
  category {
    category-type;
  }
  debug-level level;
  file {
    filename;
    files number;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
dynamic-dns {
  client hostname {
    agent agent-name;
    interface interface-name;
    password server-password;
    server server-name;
    username user-name;
  }
}
finger {
  connection-limit number;
  rate-limit number;
}
ftp {
  connection-limit number;
  rate-limit number;
}
netconf {
  ssh {
    connection-limit number;
    port port-number;
    rate-limit number;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}

```

```
        on-demand;
    }
}
outbound-ssh {
    client client-id {
        address {
            port port-number;
            retry number;
            timeout value;
        }
        device-id device-id;
        keep-alive {
            retry number;
            time-out value;
        }
        reconnect-strategy (in-order | sticky);
        secret secret;
        services {
            netconf;
        }
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
}
service-deployment {
    local-certificate certificate-name;
    servers server-address {
        port port-number;
        security-options {
            ssl3;
            tls;
        }
        user user-name;
    }
    source-address source-address;
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}
}
```

```

ssh {
  ciphers [cipher];
  client-alive-count-max number;
  client-alive-interval seconds;
  connection-limit number;
  hostkey-algorithm {
    (ssh-dss | no-ssh-dss);
    (ssh-ecdsa | no-ssh-ecdsa);
    (ssh-rsa | no-ssh-rsa);
  }
  key-exchange [algorithm];
  macs [algorithm];
  max-sessions-per-connection number;
  protocol-version {
    v1;
    v2;
  }
  rate-limit number;
  root-login (allow | deny | deny-password);
  (tcp-forwarding | no-tcp-forwarding);
}
subscriber-management {
  enforce-strict-scale-limit-license;
  gres-route-flush-delay;
  maintain-subscriber interface-delete;
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
subscriber-management-helper {
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
}
telnet {
  connection-limit number;
  rate-limit number;
}
web-management {
  control {

```

```

        max-threads number;
    }
    http {
        interface [interface-name];
        port port-number;
    }
    https {
        interface [interface-name];
        local-certificate name;
        pki-local-certificate name;
        port port-number;
        system-generated-certificate;
    }
    management-url url;
    session {
        idle-timeout minutes;
        session-limit number;
    }
    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;
    }
}
xnm-clear-text {
    connection-limit number;
    rate-limit number;
}
xnm-ssl {
    connection-limit number;
    local-certificate name;
    rate-limit number;
}
}
static-host-mapping hostname {
    alias [host-name-alias];
    inet [ip-address];
    inet6 [ipv6-address];
    sysid system-identifier;
}
syslog {
    allow-duplicates;
    archive {
        binary-data;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    console {

```

```

    (any | facility) severity;
}
file filename {
    allow-duplicates;
    archive {
        archive-sites url {
            password password;
        }
        (binary-data | no-binary-data);
        files number;
        size maximum-file-size;
        start-time "YYYY-MM-DD.hh:mm";
        transfer-interval minutes;
        (world-readable | no-world-readable);
    }
    structure-data {
        brief;
    }
    (any | facility) severity;
}
host (hostname | other-routing-engine) {
    (any | facility) severity;
}
log-rotate-frequency minutes;
source-address source-address;
time-format {
    millisecond;
    year;
}
user (username | *) {
    (any | facility) severity;
}
}
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    service-name service-name;
}
tacplus-server server-address {
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}
time-zone (GMThour-offset | time-zone);
tracing {
    destination-override {
        syslog {
            host address;
        }
    }
}
}
use-imported-time-zones;
}

```

address-assignment (Access)

Supported Platforms SRX300, SRX320, SRX340, SRX345, SRX550M

Syntax address-assignment {
 abated-utilization *percentage*;
 abated-utilization-v6 *percentage*;
 high-utilization *percentage*;
 high-utilization-v6 *percentage*;
 neighbor-discovery-router-advertisement *ndra-name*;
 pool *pool-name* {
 family {
 inet {
 dhcp-attributes {
 boot-file *boot-file-name*;
 boot-server *boot-server-name*;
 domain-name *domain-name*;
 grace-period *seconds*;
 maximum-lease-time (*seconds* | infinite);
 name-server *ipv4-address*;
 netbios-node-type (b-node | h-node | m-node | p-node);
 next-server *next-server-name*;
 option *dhcp-option-identifier-code* {
 array {
 byte [*8-bit-value*];
 flag [false | off | on | true];
 integer [*32-bit-numeric-values*];
 ip-address [*ip-address*];
 short [*signed-16-bit-numeric-value*];
 string [*character string value*];
 unsigned-integer [*unsigned-32-bit-numeric-value*];
 unsigned-short [*16-bit-numeric-value*];
 }
 byte *8-bit-value*;
 flag (false | off | on | true);
 integer *32-bit-numeric-values*;
 ip-address *ip-address*;
 short *signed-16-bit-numeric-value*;
 string *character string value*;
 unsigned-integer *unsigned-32-bit-numeric-value*;
 unsigned-short *16-bit-numeric-value*;
 }
 }
 option-match {
 option-82 {
 circuit-id *match-value* {
 range *range-name*;
 }
 remote-id *match-value*;
 range *range-name*;
 }
 }
 }
 }
 }
 propagate-ppp-settings [*interface-name*];
 propagate-settings *interface-name*;
 router *ipv4-address*;

```

server-identifier ip-address;
sip-server {
    ip-address ipv4-address;
    name sip-server-name;
}
tftp-server server-name;
wins-server ipv4-address;
}
host hostname {
    hardware-address mac-address;
    ip-address reserved-address;
}
network network address;
range range-name {
    high upper-limit;
    low lower-limit;
}
excluded-range range-name
    high upper-limit;
    low lower-limit;
}
xauth-attributes {
    primary-dns ip-address;
    primary-wins ip-address;
    secondary-dns ip-address;
    secondary-wins ip-address;
}
}
inet6 {
    dhcp-attributes {
        dns-server ipv6-address;
        grace-period seconds;
        maximum-lease-time (seconds | infinite);
        option dhcp-option-identifier-code {
            array {
                byte [8-bit-value];
                flag [ false | off | on | true];
                integer [32-bit-numeric-values];
                ip-address [ip-address];
                short [signed-16-bit-numeric-value];
                string [character string value];
                unsigned-integer [unsigned-32-bit-numeric-value];
                unsigned-short [16-bit-numeric-value];
            }
            byte 8-bit-value;
            flag (false | off | on | true);
            integer 32-bit-numeric-values;
            ip-address ip-address;
            short signed-16-bit-numeric-value;
            string character string value;
            unsigned-integer unsigned-32-bit-numeric-value;
            unsigned-short 16-bit-numeric-value;
        }
        propagate-ppp-settings [interface-name];
        sip-server-address ipv6-address;
        sip-server-domain-name domain-name;
    }
}

```

```
    }
    prefix ipv6-network-prefix;
    range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length delegated-prefix-length;
    }
    excluded-range range-name
        high upper-limit;
        low lower-limit;
    }
}
link pool-name;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- *Dynamic VPN Overview*

address-pool (Access)

Supported Platforms [M Series](#), [MX Series](#), [SRX Series](#), [T Series](#)

Syntax

```
address-pool pool-name {
    address address or address prefix;
    address-range {
        high upper-limit;
        low lower-limit;
        mask network-mask;
    }
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-wins IP address;
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description Create an address-pool for L2TP clients.

- Options**
- **pool-name**—Name assigned to the address-pool.
 - **address**—Configure subnet information for the address-pool.
 - **address-range**—Defines the address range available for clients.
 - **primary-dns**—Specify the primary-dns IP address.
 - **secondary-dns**—Specify the secondary-dns IP address.
 - **primary-wins**—Specify the primary-wins IP address.
 - **secondary-wins**—Specify the secondary-wins IP address.

Required Privilege Level

access—To view this statement in the configuration.
 access-control—To add this statement to the configuration.

Related Documentation

- [access-control on page 50](#)

allow-configuration

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | allow-configuration " <i>regular-expression</i> "; |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.2 for SRX Series devices. |
| Description | Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement do not grant such access by default. |
| Default | If you omit this statement and the deny-configuration statement, users can edit only those commands for which they have access privileges through the permissions statement. |
| Options | <i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |

allow-configuration-regexps

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | allow-configuration-regexps " <i>regular expression 1</i> " " <i>regular expression 2</i> "; |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced in Junos OS Release 11.2. |
| Description | Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access. The statement deny-configuration-regexps takes precedence if it is used in the same login class definition. |
| Default | If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement. |
| Options | <i>regular expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |

authentication-key

Supported Platforms [SRX Series](#)

Syntax `authentication-key key-number type md5 value <password>;`

Hierarchy Level [edit system *ntp*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Network Time Protocol (NTP) authentication keys so that the SRX Series device can send authenticated packets. If you configure the SRX Series device to operate in authenticated mode, you must configure a key.

Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.

Options *key-number*—Positive integer that identifies the key.

type md5—Authentication type. It can only be **md5**.

value password—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [ntp on page 471](#)

authentication-order

| | |
|---------------------------------|---|
| Supported Platforms | EX Series, M Series, SRX Series, T Series |
| Syntax | authentication-order [<i>authentication-methods</i>]; |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches. |
| Default | If you do not include the authentication-order statement, users are verified based on their configured passwords. |
| Options | <i>authentication-methods</i> —One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following: <ul style="list-style-type: none">• password—Use the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.• radius—Use RADIUS authentication services.• tacplus—Use TACACS+ authentication services. |
| 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 User Authentication Methods on page 12 |

boot-server (NTP)

Supported Platforms [SRX Series](#)

Syntax `boot-server (address | hostname);`

Hierarchy Level [edit system ntp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the server that NTP queries when the SRX Series device boots to determine the local date and time.

When you boot the SRX Series device, it issues an **ntpdate** request, which polls a network server to determine the local date and time. You need to configure a server that the SRX Series device uses to determine the time when the SRX Series device boots. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the **ntpdate** request resolves the hostname to an IP address when the SRX Series device boots up.

If you configure an NTP boot server, then when the SRX Series device boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.

- Options**
- **address**—The IP address of an NTP boot server.
 - **hostname**—The hostname of an NTP boot server.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation [• ntp on page 471](#)

broadcast

Supported Platforms [SRX Series](#)

Syntax `broadcast address <key key-number> <routing-instance-name routing-instance-name> <ttl value> <version value>;`

Hierarchy Level `[edit system ntp]`

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the SRX Series device to operate in broadcast mode with the remote system at the specified address. In this mode, the SRX Series device sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Normally, you include this statement only when the SRX Series device is operating as a transmitter.

Options **address**—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be **224.0.1.1**.

key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

Range: Any unsigned 32-bit integer

routing-instance-name routing-instance-name—(Optional) The routing instance name in which the interface has an address in the broadcast subnet.

Default: The default routing instance is used to broadcast packets.

ttl value—(Optional) Time-to-live (TTL) value to use.

Range: 1 through 255

Default: 1

version value—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege Level `system`—To view this statement in the configuration.
`system-control`—To add this statement to the configuration.

Related Documentation

- [ntp on page 471](#)

broadcast-client

| | |
|---------------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | <code>broadcast-client;</code> |
| Hierarchy Level | [edit system <i>ntp</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | Configure the SRX Series device to listen for broadcast messages on the local network to discover other servers on the same subnet. |
| 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">• ntp on page 471 |

ciphers

Supported Platforms [MX Series](#), [SRX Series](#)

Syntax `ciphers [cipher-1 cipher-2 cipher-3 ...]`

Hierarchy Level `[edit system services ssh]`

Release Information Statement introduced in Junos OS Release 11.2.

Description Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.

- Options**
- **3des-cbc**—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
 - **aes128-cbc**—128-bit Advanced Encryption Standard (AES) in CBC mode.
 - **aes256-cbc**—256-bit AES in CBC mode.
 - **aes128-ctr**—128-bit AES in CBC mode.
 - **aes192-ctr**—192-bit AES in counter mode.
 - **aes256-ctr**—256-bit AES in counter mode.
 - **aes128-gcm@openssh.com**—128-bit AES in Galois/Counter Mode.
 - **aes256-gcm@openssh.com**—256-bit AES in Galois/Counter Mode.
 - **arcfour128**—128-bit RC4-stream cipher in CBC mode.
 - **arcfour256**—256-bit RC4-stream cipher in CBC mode.
 - **blowfish128-cbc**—128-bit blowfish-symmetric block cipher in CBC mode.
 - **cast128-cbc**—128-bit cast in CBC mode.



NOTE: Ciphers represent a set. To configure SSH ciphers:

```
user@host#set system services ssh ciphers [ aes256-cbc aes192-cbc ]
```

Required Privilege Level

| | |
|----------------|--|
| system | To view this statement in the configuration. |
| system-control | To add this statement to the configuration. |

Related Documentation

- [Configuring SSH Service for Remote Access to the Router or Switch](#)

connection-limit

Supported Platforms SRX Series, vSRX

Syntax connection-limit *limit*;

Hierarchy Level [edit system services finger]
[edit system services ftp]
[edit system services netconf ssh]
[edit system services ssh]
[edit system services telnet]
[edit system services xnm-clear-text]
[edit system services xnm-ssl]

Release Information Statement introduced in Junos OS Release 11.4.

Description Configure the maximum number of connection sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options *limit*—Maximum number of established connections per protocol (either IPv6 or IPv4).

On all high-end SRX Series devices, the range and default value are as follows:

Range: 1 through 250

Default: 75

On all branch SRX Series devices, the range is as follows:

Range: 1 through 5



NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

client-ia-type

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | client-ia-type (ia-na ia-pd); |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Configure the DHCPv6 client identity association type. |
| Options | ia-na — Identity association for nontemporary address ia-pd —Identity association for prefix delegation |
| 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 Client Overview on page 339 |

client-identifier (dhcp-client)

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | client-identifier { user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i> ; use-interface-description {logical device}; prefix [host-name routing-instance-name]; } |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | The DHCP server identifies a client by a client-identifier value. |
| 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 | <ul style="list-style-type: none">• DHCPv6 Client Overview on page 339 |

client-identifier (dhcpv6-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | client-identifier duid-type (duid-ll duid-llt vendor); |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | The DHCPv6 server identifies a client by a client-identifier value. |
| Options | <p>duid-type—The DHCPv6 client is identified by a DHCP unique identifier (DUID).</p> <p>duid-ll—Link Layer address.</p> <p>duid-llt—Link Layer address plus time.</p> <p>vendor—Vendor-assigned unique ID based on the enterprise number.</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"> • DHCPv6 Client Overview on page 339 |

client-list-name (SNMP)

| | |
|---------------------------------|--|
| Syntax | client-list-name <i>client-list-name</i> ; |
| Hierarchy Level | [edit snmp community <i>community-name</i>] |
| Release Information | Statement introduced in Junos OS Release 8.5. |
| Description | Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration. |
| Options | client-list-name — Name of the client list. Client list is the list of IP address prefixes defined with the prefix-list statement in the policy-options hierarchy. |
| Required Privilege Level | <p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Understanding the SNMP Implementation in Junos OS • Standard SNMP MIBs Supported by Junos OS |

client-type

| | |
|--------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | client-type (autoconfig statefull); |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | The type of DHCPv6 client. |
| Options | <ul style="list-style-type: none">• autoconfig—Autoconfig client type for router advertisement• statefull— Stateful client type for address assignment |
| 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 Client Overview on page 339 |

deny-configuration

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | deny-configuration " <i>regular-expression</i> "; |
| Hierarchy Level | [edit system login class] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.2 for SRX Series devices. |
| Description | Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement grant such access by default. |
| Default | If you omit this statement and the allow-configuration statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the permissions statement. |
| Options | regular-expression —Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |

deny-configuration-regexps

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | deny-configuration-regexps " <i>regular expression 1</i> " " <i>regular expression 2</i> "; |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.2 for SRX Series devices. |
| Description | <p>Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access.</p> <p>Expressions configured with this statement take precedence over allow-configuration-regexps if the two statements are used in the same login class definition.</p> |
| Default | If you do not configure this statement or the deny-configuration-regexps statement, users can edit only those commands for which they have access privileges set with the permissions statement. |
| Options | <p><i>regular expression</i>—Extended (modern) regular expression as defined in POSIX 1003.2.</p> <p>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.</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> |

destination (Accounting)

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

Syntax

```
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        secret password;
        source-address source-address;
        timeout seconds;
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Hierarchy Level [edit system accounting]

Release Information Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4. Support for IPv6 source address added in Junos OS Release 12.1X47-D15.

Description Configure the authentication server.

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.

dhcp-attributes (Access IPv4 Address Pools)

Supported Platforms [SRX Series, vSRX](#)

Syntax `dhcp-attributes {`
 `boot-file` *boot-file-name*;
 `boot-server` *boot-server-name*;
 `domain-name` *domain-name*;
 `grace-period` *seconds*;
 `maximum-lease-time` (*seconds* | *infinite*);
 `name-server` *ipv4-address*;
 `netbios-node-type` (*b-node* | *h-node* | *m-node* | *p-node*);
 `next-server` *next-server-name*;
 `option` *dhcp-option-identifier-code* {
 `array` {
 `byte` [*8-bit-value*];
 `flag` [*false* | *off* | *on* | *true*];
 `integer` [*32-bit-numeric-values*];
 `ip-address` [*ip-address*];
 `short` [*signed-16-bit-numeric-value*];
 `string` [*character string value*];
 `unsigned-integer` [*unsigned-32-bit-numeric-value*];
 `unsigned-short` [*16-bit-numeric-value*];
 }
 `byte` *8-bit-value*;
 `flag` (*false* | *off* | *on* | *true*);
 `integer` *32-bit-numeric-values*;
 `ip-address` *ip-address*;
 `short` *signed-16-bit-numeric-value*;
 `string` *character string value*;
 `unsigned-integer` *unsigned-32-bit-numeric-value*;
 `unsigned-short` *16-bit-numeric-value*;
 }
 `option-match` {
 `option-82` {
 `circuit-id` *match-value* {
 `range` *range-name*;
 }
 `remote-id` *match-value*;
 `range` *range-name*;
 }
 }
 `propagate-ppp-settings` [*interface-name*];
 `propagate-settings` *interface-name*;
 `router` *ipv4-address*;
 `server-identifier` *ip-address*;
 `sip-server` {
 `ip-address` *ipv4-address*;
 `name` *sip-server-name*;
 }
 `tftp-server` *server-name*;
 `wins-server` *ipv4-address*;
 }

| | |
|---------------------------------|--|
| Hierarchy Level | [edit access address-assignment pool <i>pool-name</i> family inet] |
| Release Information | Statement introduced in Junos OS Release 10.4. |
| Description | Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options. |
| Required Privilege Level | access—To view this statement in the configuration. access-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• DHCP Server, Client, and Relay Agent Overview on page 296 |

dhcp-attributes (Access IPv6 Address Pools)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
dhcp-attributes {
  dns-server ipv6-address;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [ false | off | on | true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag ( false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  propagate-ppp-settings [interface-name];
  sip-server-address ipv6-address;
  sip-server-domain-name domain-name;
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet6]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure attributes for address pools that can be used by different clients.

- Options**
- **dns-server *IPv6-address***—Specify a DNS server to which clients can send DNS queries.
 - **grace-period *seconds*** —Specify the grace period offered with the lease.

Range: 0 through 4,294,967,295 seconds

Default: 0 (no grace period)

- **maximum-lease-time *seconds***—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

Range: 30 through 4,294,967,295 seconds

Default: 86,400 seconds (24 hours)

- **option *dhcp-option-identifier-code***—Specify the DHCP option identifier code.

- **propagate-ppp-settings** [*interface-name*—Specify PPP interface name for propagating DNS or WINS settings.
- **sip-server-address** *IPv6-address*—Specify the IPv6 address of the SIP outbound proxy server.
- **sip-server-domain-name** *domain-name*—Specify the domain name of the SIP outbound proxy server.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation [• DHCP Server, Client, and Relay Agent Overview on page 296](#)

dhcp-client

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax

```
dhcp-client {
  client-identifier {
    prefix {
      host-name;
      logical-system-name;
      routing-instance-name;
    }
    use-interface-description (device | logical);
    user-id (ascii string | hexadecimal string);
  }
  lease-time (length | infinite);
  retransmission-attempt value;
  retransmission-interval seconds;
  server-address server-address;
  update-server;
  vendor-id vendor-id;
}
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Configure the Dynamic Host Configuration Protocol (DHCP) client.

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 [• DHCP Server, Client, and Relay Agent Overview on page 296](#)

dhcp-local-server (System Services)

Supported Platforms [SRX Series](#)

```
Syntax  dhcp-local-server {
        dhcpv6 {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        group group-name {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
        }
    }
```

```

        use-primary dynamic-profile;
    }
    interface interface-name {
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        exclude;
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        service-profile service-profile-name
        trace ;
        upto interface-name;
    }
    liveness-detection {
        failure-action {
            clear-binding;
            clear-binding-if-interface-up;
            log-only;
        }
        method {
            bfd {
                detection-time {
                    threshold milliseconds;
                }
                holddown-interval interval;
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                session-mode (automatic | multihop | single-hop);
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
                version (0 | 1 | automatic);
            }
        }
    }
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }

```

```

    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;

```

```
    }  
    group group-name {  
        interface interface-name {  
            exclude;  
            upto upto-interface-name;  
        }  
    }  
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.



NOTE: SRX Series devices do not support client authentication.

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

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)

dhcpv6 (System Services)

Supported Platforms [SRX Series](#)

```
Syntax  dhcpv6 {
    authentication {
        password password;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name;
            interface-name;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile;
        }
    }
}
```

```
}
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
```

```

reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}

```

| | |
|----------------------------|---|
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced in Junos OS Release 10.4. |
| Description | Configure DHCPv6 server to provide IPv6 addresses to clients. |



NOTE: SRX Series devices do not support client authentication.

| | |
|---------------------------------|--|
| Options | <ul style="list-style-type: none"> duplicate-clients-on-interface—Allow duplicate clients on different interfaces in a subnet. <p>The remaining statements are explained separately. See CLI Explorer.</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"> DHCP Server, Client, and Relay Agent Overview on page 296 |

dhcpv6-client

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | <pre>dhcpv6-client { client-ia-type (ia-na ia-pd); client-identifier duid-type (duid-ll duid-llt vendor); client-type (autoconfig statefull); rapid-commit; req-option (dns-server domain fqdn nis-domain nis-server ntp-server sip-domain sip-server time-zone vendor-spec); retransmission-attempt <i>number</i>; update-router-advertisement { interface <i>interface-name</i>; } update-server; }</pre> |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Configure the Dynamic Host Configuration Protocol version 6 (DHCPv6) client. |
| 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 | <ul style="list-style-type: none"> DHCP Server, Client, and Relay Agent Overview on page 296 |

disable (System Services)

| | |
|---------------------------------|---|
| Supported Platforms | SRX Series, vSRX |
| Syntax | disable; |
| Hierarchy Level | [edit system services dns dnssec] |
| Release Information | Statement introduced in Junos OS Release 10.2 . |
| Description | Disables DNSSEC in the DNS 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"> • DHCP Server, Client, and Relay Agent Overview on page 296 |

dlv

| | |
|---------------------------------|---|
| Supported Platforms | SRX Series, vSRX |
| Syntax | <pre>dlv { domain-name <i>domain-name</i> trusted-anchor <i>trusted-anchor</i>; }</pre> |
| Hierarchy Level | [edit system services dns dnssec] |
| Release Information | Statement introduced in Junos OS Release 10.2 . |
| Description | Configure DNSSEC Lookaside Validation (DLV). |
| Options | <ul style="list-style-type: none"> • domain-name <i>domain-name</i>—Specify the secure domain server name. • trusted-anchor <i>trusted-anchor</i>—Specify the trusted DLV anchor. |
| 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"> • DHCP Server, Client, and Relay Agent Overview on page 296 |

dynamic-pool

Supported Platforms [SRX Series](#)

Syntax

```
address-assignment {
  dynamic-pool <dynamic-pool>{
    family {
      inet6 {
        from-interface <interface>;
        delegated-prefix-length <network-prefix-length>;
        range <range-name> {
          masked-low <masked-low>;
          masked-high <masked-high>;
          prefix-length <prefix-length>;
        }
        dhcp-attributes {
          dns-server <address>;
          t1-percentage <t1-percentage>;
          t2-percentage <t2-percentage>;
          preferred-lifetime <preferred-lifetime>;
          valid-lifetime <valid-lifetime>;
        }
      }
    }
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 15.1X49-D70.

Description Configure the dynamic pool updated by the client running on the WAN interface.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- [Configuring Address-Assignment Pools on page 304](#)
- [address-assignment \(Access\) on page 416](#)

dynamic-server

Supported Platforms [SRX Series](#)

Syntax

```

dhcpv6 {
  dynamic-server {
    group <group> {
      neighbor-discovery-router-advertisement <ndra-pool>;
      interface <interface> {
        overrides {
          delegated-pool <delegated-pool>;
          ia-na-pool <ia-na-pool>;
          process-inform {
            pool <pool>;
          }
        }
      }
    }
  }
}

```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 15.1X49-D70.

Description Configure the server running on a LAN interface.

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

- [dhcp-local-server \(System Services\) on page 437](#)
- [dhcp-client on page 436](#)

family (Security Forwarding Options)

Supported Platforms [SRX Series](#), [vSRX](#)

Syntax

```
family {  
  inet6 {  
    mode (drop | flow-based | packet-based);  
  }  
  iso {  
    mode packet-based;  
  }  
  mpls {  
    mode packet-based;  
  }  
}
```

Hierarchy Level [edit security forwarding-options]

Release Information Statement introduced in Junos OS Release 8.5.

Description Determine the protocol family to be used for packet forwarding.



NOTE: Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.

Options 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

- [MPLS Overview](#)

file (System Logging)

Supported Platforms M Series, MX Series, SRX Series, T Series

Syntax

```
file filename {
    allow-duplicates;
    any (alert | any | critical | emergency | error | info | none | notice | warning);
    archive {
        archive-sites {
            url password;
        }
        (binary-data | no-binary-data);
        files number;
        size size;
        start-time start-time;
        transfer-interval transfer-interval;
        (world-readable | no-world-readable);
    }
    authorization (alert | any | critical | emergency | error | info | none | notice | warning);
    change-log (alert | any | critical | emergency | error | info | none | notice | warning);
    conflict-log (alert | any | critical | emergency | error | info | none | notice | warning);
    daemon (alert | any | critical | emergency | error | info | none | notice | warning);
    dfc (alert | any | critical | emergency | error | info | none | notice | warning);
    explicit-priority;
    external (alert | any | critical | emergency | error | info | none | notice | warning);
    firewall (alert | any | critical | emergency | error | info | none | notice | warning);
    ftp (alert | any | critical | emergency | error | info | none | notice | warning);
    interactive-commands (alert | any | critical | emergency | error | info | none | notice | warning);
    kernel (alert | any | critical | emergency | error | info | none | notice | warning);
    match "regular-expression";
    ntp (alert | any | critical | emergency | error | info | none | notice | warning);
    pfe (alert | any | critical | emergency | error | info | none | notice | warning);
    security (alert | any | critical | emergency | error | info | none | notice | warning);
    structured-data {
        brief;
    }
    user (alert | any | critical | emergency | error | info | none | notice | warning);
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description Specify the file in which to log data.

- Options**
- *filename*—Specify the name of the file in which to log data.
 - *allow-duplicates*—Do not suppress the repeated messages.
 - *any*—Specify all facilities information.
 - *alert*—Specify the conditions that should be corrected immediately.
 - *critical*—Specify the critical conditions.
 - *emergency*—Specify the conditions that cause security functions to stop.

- *error*—Specify the general error conditions.
- *info*—Specify the information about normal security operations.
- *none*—Do not specify any messages.
- *notice*—Specify the conditions that should be handled specifically.
- *warning*—Specify the general warning conditions.
- *archive*—Specify the archive file information.
 - *archive-sites*—Specify a list of destination URLs for the archived log files.
 - *url*—Specify the primary and failover URLs to receive archive files.
 - *binary-data*—Mark file such that it contains binary data.
 - *no-binary-data*—Do not mark the file such that it contains binary data.
 - *files*—Specify the number of files to be archived. Range: 1 through 1000 files.
 - *size*—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
 - *world-readable*—Allow any user to read the log file.
 - *no-world-readable*—Do not allow any user to read the log file.
 - *start-time*—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
 - *transfer-interval*—Specify the frequency at which to transfer the files to archive sites.
- *authorization*—Specify the authorization system.
- *change-log*—Specify the configuration change log.
- *conflict-log*—Specify the configuration conflict log.
- *daemon*—Specify the various system processes.
- *dfc*—Specify the dynamic flow capture.
- *explicit-priority*—Include the priority and facility in messages.
- *external*—Specify the local external applications.
- *firewall*—Specify the firewall filtering system.
- *ftp*—Specify the FTP process.
- *interactive-commands*—Specify the commands executed by the UI.
- *kernel*—Specify the kernel information.
- *match*—Specify the regular expression for lines to be logged.
- *ntp*—Specify the NTP process.
- *pfe*—Specify the Packet Forwarding Engine.
- *security*—Specify the security-related information.

- *structured-data*—Log the messages in structured log format.
 - *brief*—Omit English language text from the end of the logged message.
- *user*—Specify the user processes.
 - *info*—Specify the informational messages.

| | |
|---------------------------|--|
| Required Privilege | system—To view this statement in the configuration. |
| Level | system-control—To add this statement to the configuration. |

forwarding-options (Security)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5 .

Description Determine how the **inet6**, **iso**, and **mpls** protocol families manage security forwarding options.



NOTE:

- Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.
- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the `set security forwarding-options family mpls mode packet-based` statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

Options 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

- *MPLS Overview*
- *Understanding Packet-Based Processing*
- *Juniper Networks Devices Processing Overview*

group (System Services DHCP)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
group group-name {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix;
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
  }
  interface interface-name {
    dynamic-profile {
      profile-name;
      aggregate-clients {
        merge;
        replace;
      }
      junos-default-profile;
      use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
      delegated-pool pool-name;
      interface-client-limit number;
      process-inform {
        pool pool-name;
      }
      rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
  }
  liveness-detection {
    failure-action {
```

```

clear-binding;
clear-binding-if-interface-up;
log-only;
}
method {
bfd {
detection-time {
threshold milliseconds;
}
holddown-interval interval;
minimum-interval milliseconds;
minimum-receive-interval milliseconds;
multiplier number;
no-adaptation;
session-mode (automatic | multihop | single-hop);
transmit-interval {
minimum-interval milliseconds;
threshold milliseconds;
}
}
version (0 | 1 | automatic);
}
}
overrides {
delegated-pool pool-name;
interface-client-limit number;
process-inform {
pool pool-name;
}
}
rapid-commit ;
}
reconfigure {
attempts number;
clear-on-abort;
strict;
timeout number;
token token-name;
trigger {
radius-disconnect;
}
}
}
service-profile service-profile-name;
}

```

Hierarchy Level [edit system services dhcp-local-server dhcpv6]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a group of interfaces that have a common configuration.

The remaining statements are explained separately. See [CLI Explorer](#).

- Options**
- *group-name*—Name of the group.



NOTE: SRX Series devices do not support DHCP client authentication.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

| | |
|----------------|---|
| access | —To view this statement in the configuration. |
| access-control | —To add this statement to the configuration. |

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
 - [DHCP Server Configuration Overview on page 302](#)

host (SSH Known Hosts)

Supported Platforms [SRX Series, vSRX](#)

Syntax `host hostname {
 dsa-key dsa-key;
 ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
 ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
 ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
 rsa-key rsa-key;
 rsa1-key rsa1-key;
}`

Hierarchy Level [edit security ssh-known-hosts]

Release Information Statement modified in Junos OS Release 8.5.


Description Configure the type of base-64 encoded host key.

- Options**
- ***hostname***—Name of the SSH known host.
 - ***dsa-key dsa-key***—Digital Signature Algorithm (DSA) for SSH version 2
 - ***ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
 - ***ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
 - ***ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key***—Elliptic Curve Digital Signature Algorithm (ECDSA)
 - ***rsa-key rsa-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2
 - ***rsa1-key rsa1-key***—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

- Related Documentation**
- [Generating an SSL Certificate Using the openssl Command on page 236](#)
 - [Generating a Self-Signed SSL Certificate on page 236](#)

hostkey-algorithm

| | |
|---------------------------------|--|
| Supported Platforms | M Series, MX Series, SRX Series, vSRX |
| Syntax | hostkey-algorithm <algorithm no-algorithm> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Junos OS Release 11.2. <algorithm no algorithm> statements introduced in Junos OS Release 12.2. |
| Description | Allow or disallow a host-key signature algorithm for the SSH host to use to authenticate another host. |
| Options | <ul style="list-style-type: none"> • no-ssh-dss—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key. • no-ssh-ecdsa—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key. • no-ssh-rsa—Do not allow generation of an RSA host-key. • ssh-ecdsa—Allow generation of an ECDSA host-key. • ssh-dss—Allow generation of a 1024-bit DSA host-key. |
| | <div>  <p>NOTE: DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode.</p> </div> |
| | <ul style="list-style-type: none"> • ssh-rsa—Allow generation of an RSA host-key. |
| 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"> • Generating an SSL Certificate Using the openssl Command on page 236 • Generating a Self-Signed SSL Certificate on page 236 |

idle-timeout (System)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, vSRX |
| Syntax | idle-timeout <i>idle-timeout</i> ; |
| Hierarchy Level | [edit system login] |
| Release Information | Statement introduced in Junos OS Release 15.1X49-D70 for the vSRX, SRX4100, SRX4200 and SRX1500 Series. |
| Description | Configure the maximum time for which the C shell or CLI console session can be idle. The user (including the root user) is logged out after the expiry of idle-timeout . |
| Options | <i>idle-timeout</i> — Maximum idle time before logout. Range: 1 through 60 minutes |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |

interface (System Services DHCP)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
interface interface-name {
    exclude;
    overrides {
        interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level [edit system services dhcp-local-server dhcpv6 group *group-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface *interface-name* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

- Options**
- *interface-name*—Name of the interface.
 - **trace**—Enable tracing of the interface specified by the *interface-name* argument.
 - **upto** *upto-interface-name*—The upper end of the range of interfaces; the lower end of the range is the *interface-name* entry. The interface device name of the *upto-interface-name* must be the same as the device name of the *interface-name*.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

- Related Documentation**
- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
 - [DHCP Server Configuration Overview on page 302](#)

interfaces (ARP)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
interfaces {  
  interface-name {  
    aging-timer minutes;  
  }  
}
```

Hierarchy Level [edit system arp]

Release Information Statement introduced before Junos OS Release 9.4.

Description Specify the Address Resolution Protocol (ARP) aging timer in minutes for a logical interface.

Options **aging-timer *minutes***—Time between ARP updates, in minutes.

Range: 1 through 240

Default: 20

Required Privilege Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [DHCP Server Configuration Overview on page 302](#)

interfaces (Security Zones)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```

interfaces interface-name {
  host-inbound-traffic {
    protocols protocol-name {
      except;
    }
  }
  system-services service-name {
    except;
  }
}

```

Hierarchy Level [edit security zones functional-zone management],
[edit security zones security-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the set of interfaces that are part of the zone.

Options *interface-name* —Name of the interface.

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 Security Zones](#)

interface-traceoptions (System Services DHCP)

Supported Platforms SRX Series, vSRX

Syntax

```
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;
}
```

Hierarchy Level [edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the **interface *interface-name* trace** statement at the [edit system services group *group-name*] hierarchy level to enable the tracing operation on the specific interfaces.

Options **file-name**—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files number—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **packet**—Trace packet decoding operations
- **packet-option**—Trace DHCP option decoding operations

- **state**—Trace changes in state

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 *size*—(Optional) Maximum size of each trace file, in 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: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

| | |
|---------------------------------|---|
| Required Privilege Level | interface—To view this statement in the configuration. |
| | interface-control—To add this statement to the configuration. |
| Related Documentation | • DHCP Server, Client, and Relay Agent Overview on page 296 |
| | • DHCP Server Configuration Overview on page 302 |

internet-options

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
internet-options {
  icmpv4-rate-limit {
    bucket size seconds;
    packet-rate packet-rate;
  }
  icmpv6-rate-limit {
    bucket size seconds;
    packet-rate packet-rate;
  }
  ipv6-duplicate-addr-detection-transmits number;
  no-path-mtu-discovery;
  no-source-quench;
  no-tcp-reset;
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  path-mtu-discovery;
  source-port {
    upper-limit range;
  }
  source-quench;
  tcp-drop-synfin-set;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure tunable options for Internet operations.

- Options**
- **icmpv4-rate-limit**—Configure rate-limiting parameters for Internet Control Message Protocol version 4 (ICMPv4) messages.
 - **bucket-size *seconds***—Set ICMP rate-limiting maximum bucket size in seconds.
 - **packet-rate *packet-rate***— Set ICMP rate-limiting packets earned per second.
 - **icmpv6-rate-limit**—Configure rate-limiting parameters for Internet Control Message Protocol version 6 (ICMPv6) messages.
 - **bucket-size *seconds***—Set ICMP rate-limiting maximum bucket size in seconds.
 - **packet-rate *packet-rate***— Set ICMP rate-limiting packets earned per second.
 - **ipv6-duplicate-addr-detection-transmits *number***—Control the number of attempts for IPv6 duplicate address detection.
 - **no-path-mtu-discovery**—Do not enable path maximum transmission unit (MTU) discovery on TCP connections.
 - **no-source-quench**—Do not react to incoming ICMP source quench messages.
 - **no-tcp-reset**—Do not send RST TCP packets for packets sent to non-listening ports.

- **no-tcp-rfc1323**—Disable RFC 1323 TCP extensions.
- **no-tcp-rfc1323-paws**—Disable RFC 1323 Protection Against Wrapped Sequence Number extension.
- **path-mtu-discovery**—Enable path MTU discovery on TCP connections.
- **source-port**—Configure source port selection parameters.
 - **upper-limit range**—Specify upper limit of source port selection range.
- **source-quench**—React to incoming ICMP source quench messages.
- **tcp-drop-synfin-set**—Drop TCP packets that have both SYN and FIN flags.

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

kernel-replication (System)

Supported Platforms [SRX Series](#), [vSRX](#)

Syntax kernel-replication;

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.1.

Description Configure kernel replication.

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

lease-time (dhcp-client)

Supported Platforms [SRX1500](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#), [vSRX](#)

Syntax lease-time *seconds*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options **seconds**— Request time to negotiate and exchange information.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)

location

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
location {  
    altitude feet;  
    building name;  
    country-code code;  
    floor number;  
    hcoord horizontal-coordinate;  
    lata service-area;  
    latitude degrees;  
    longitude degrees;  
    npa-nxx number;  
    postal-code postal-code;  
    rack number;  
    vcoord vertical-coordinate;  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure the physical location of the device.

- Options**
- **altitude *feet***—Number of feet above sea level.
 - **building *name***—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").
 - **country-code *code***—Two-letter country code.
 - **floor *number***—Floor number in the building.
 - **hcoord *horizontal-coordinate***—Bellcore Horizontal Coordinate.
 - **lata *service-area***—Long-distance service area.
 - **latitude *degrees***—Latitude in degree format.
 - **longitude *degrees***—Longitude in degree format.
 - **npa-nxx *number***—First six digits of the phone number (area code and exchange).
 - **postal-code *postal-code***—Zip code or Postal code.
 - **rack *number***—Rack number.
 - **vcoord *vertical-coordinate***—Bellcore Vertical Coordinate.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

lockout-period

| | |
|---------------------------------|--|
| Supported Platforms | M Series, MX Series, SRX Series, T Series |
| Syntax | lockout-period <i>minutes</i> ; |
| Hierarchy Level | [edit system login retry-options] |
| Release Information | Statement introduced in Junos OS Release 11.2. |
| Description | Configure the amount of time before the user can attempt to log in to the router after being locked out due to the number of failed login attempts specified in the tries-before-disconnect statement. |
| Options | <i>minutes</i> —Amount of time before the user can attempt to log in after being locked out. Default: Off Range: 1 through 43200 |
| 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">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions• Handling Authorization Failure on page 30• Example: Configuring System Retry Options on page 31• retry-options• clear system login lockout on page 527• show system login lockout on page 606 |

macs

Supported Platforms [SRX Series, vSRX](#)

Syntax `macs [algorithm]`

Hierarchy Level `[edit system services ssh]`

Release Information Statement introduced in Junos OS Release 11.2.
SHA-2 options introduced in Junos OS Release 12.1.

Description Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.

- Options**
- `hmac-md5`—Hash-based MAC using Message-Digest 5 (MD5).
 - `hmac-md5-96`—96-bits of Hash-based MAC using MD5.
 - `hmac-ripemd160`—Hash-based MAC using RIPEMD.
 - `hmac-sha1`—Hash-based MAC using Secure Hash Algorithm (SHA-1).
 - `hmac-sha1-96`—96-bits of Hash-based MAC using SHA-1.
 - `hmac-sha2-256`—256-bits of Hash-based MAC using SHA-2.
 - `hmac-sha2-256-96`—first 96-bits of hmac-sha2-256.
 - `hmac-sha2-512`—96-bits of Hash-based MAC using SHA-1.
 - `umac-64`—Message Authentication Code using Universal Hashing.



NOTE: The *macs* configuration statement represents a set. Therefore, it should be configured as in the following.

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [System Configuration Statement Hierarchy on page 385](#)

max-pre-authentication-packets

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series , vSRX |
| Syntax | max-pre-authentication-packets <i>value</i> ; |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Junos OS Release 12.3X48-D10. |
| Description | Define the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication. |
| Options | <i>value</i> —Maximum number of pre-authentication SSH packets that the server will accept. Range: 20 through 2147483647. Default: 128 |
| Required Privilege Level | admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • The ssh Command on page 271 |

multicast-client

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | multicast-client < <i>address</i> >; |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | For NTP, configure the SRX Series device to listen for multicast messages on the local network to discover other servers on the same subnet. |
| Options | <i>address</i> —(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups. Default: 224.0.1.1. |
| 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"> • ntp on page 471 |

name-server (Access)

| | |
|---------------------------------|---|
| Syntax | <code>name-server address</code> |
| Hierarchy Level | [edit access address-assignment pool <name> family (inet inet6) xauth-attributes] |
| Release Information | Statement introduced in Junos OS Release 10.4. |
| Description | Specify the DNS server IP address for an address-assignment pool. |
| Required Privilege Level | access—To view this statement in the configuration. access-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• address-assignment (Access) on page 416• <i>Access Configuration Statement Hierarchy</i> |

neighbor-discovery-router-advertisement (Access)

| | |
|---------------------------------|---|
| Supported Platforms | SRX Series , vSRX |
| Syntax | <code>neighbor-discovery-router-advertisement ndra-pool-name;</code> |
| Hierarchy Level | [edit access address-assignment] |
| Release Information | Statement introduced in Junos OS Release 10.4. |
| Description | Configure the name of the address-assignment pool used to assign the router advertisement prefix. |
| Options | <i>ndra-pool-name</i> —Name of the address assignment pool. |
| Required Privilege Level | access—To view this statement in the configuration. access-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Access Configuration Statement Hierarchy</i> |

ntp

Supported Platforms [SRX Series](#)

Syntax

```
ntp {
  authentication-key key-number type md5 value <password>;
  boot-server <address>;
  broadcast <address> <key key-number> <routing-instance routing-instance-name> <version value> <ttl value>;
  broadcast-client;
  multicast-client <address>;
  peer address <key key-number> <version value> <prefer>;
  server address <key key-number> <version value> <prefer>;
  source-address source-address <routing-instance routing-instance-name>;
  trusted-key [key-numbers];
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Network Time Protocol (NTP) on the SRX Series device.

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. |

outbound-ssh

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
outbound-ssh {
  client client-id {
    address address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.4.
Support for IPv6 address added in Junos OS Release 12.1X47-D15.

Description Initiate outbound SSH connections.

Options **client** *client-id*—Defines a device-initiated connection. This value serves to uniquely identify the outbound-ssh configuration stanza. Each outbound-ssh stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the client-id any meaningful unique value.

address *address*—Specifies the IPv4 or IPv6 address or hostname of the client.

port *port-number*—Specifies the port at which a server listens for outbound SSH connection requests.

retry *number*—Specifies the maximum number of connection attempts a device can make to the specified IP address. The default is three attempts.

timeout *seconds*—Specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

device *device-id*—Identifies the device to the management client. Each time the device establishes an outbound SSH connection, it first sends an initiation sequence (*device-id*) to the management client.

keep-alive—Enables the device to send SSH protocol keepalive messages to the client application. The **timeout** statement specifies how long the device waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds. The **retry** statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the device disconnects from the application, ending the outbound SSH connection. The default is three retries.

reconnect-strategy (in-order|sticky)—Specifies how the device reconnects to the server after a connection is dropped.

in-order—Configures the device to reconnect to the first configured server. If this server is unavailable, the device tries to connect to the next configured server. This process repeats until a connection is completed.

sticky—Configures the device to reconnect to the server from which it disconnected.

secret *password*—Sends the device's public SSH host key when the device connects to the client.

services *netconf*—Configures the application to accept NETCONF as an available service.

| | |
|---------------------------|--|
| Required Privilege | system—To view this statement in the configuration. |
| Level | system-control—To add this statement to the configuration. |

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none"> • traceoptions (Outbound SSH) on page 499 • Configuring Outbound SSH Service on page 272 |
|------------------------------|---|

overrides (System Services DHCP)

| | |
|--------------------------|---|
| Supported Platforms | SRX Series, vSRX |
| Syntax | <pre>overrides { interface-client-limit <i>number</i>; }</pre> |
| Hierarchy Level | <pre>[edit system services dhcp-local-server dhcpv6] [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>] [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>]</pre> |
| Release Information | Statement introduced in Junos OS Release 10.4. |
| Description | <p>Override the default configuration settings for the extended DHCP local server. Specifying the overrides statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.</p> <ul style="list-style-type: none"> To override global DHCP local server configuration options, include the overrides statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level. To override configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>] hierarchy level. To override configuration options for a specific interface within a named group of interfaces, include the statements at the [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>] hierarchy level. Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options. |
| Options | <p>interface-client-limit <i>number</i>—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.</p> <p>Range: 1 through 500,000</p> <p>Default: No limit</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"> DHCP Server, Client, and Relay Agent Overview on page 296 |

peer (NTP)

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | <code>peer address <key key-number> <version value> <prefer>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | For NTP, configure the SRX Series device to operate in symmetric active mode with the remote system at the specified address. In this mode, the SRX Series device and the remote system can synchronize with each other. This configuration is useful in a network in which either the SRX Series device or the remote system might be a better source of time. |
| Options | <p>address—Address of the remote system. You must specify an address, not a hostname.</p> <p>key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p>Range: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version value—(Optional) Specify the NTP version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</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"> • ntp on page 471 |

prefix

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | <pre>prefix { host-name; logical-system-name; routing-instance-name; }</pre> |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Specify a prefix as a client identifier. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

profilerd

Supported Platforms SRX Series, vSRX

Syntax

```
profilerd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the profiler process.

- Options**
- **command *binary-file-path***—Path to binary for process.
 - **disable**—Disable the profiler process.
 - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
 - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
 - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege system—To view this statement in the configuration.

Level system-control—To add this statement to the configuration.

proxy

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
proxy {  
    password password;  
    port port-number;  
    server url;  
    username user-name;  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the proxy information for the router.

- Options**
- **password *password***—Password configured in the proxy server.
 - **port *port number***—Proxy server port number.
Range: 0 through 65,535
 - **server *url***—URL or IP address of the proxy server host.
 - **username *username***—Username configured in the proxy server.

Required Privilege Level

| | |
|----------------|---|
| system | —To view this statement in the configuration. |
| system-control | —To add this statement to the configuration. |

radius-options

Supported Platforms [SRX1500, SRX5400, SRX5600, SRX5800](#)

Syntax

```
radius-options {
  attributes {
    nas-ip-address nas-ip-address;
  }
  password-protocol mschap-v2;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5. Support for network access server (NAS) IPv6 address added in Junos OS Release 12.1X47-D15.

Description Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

- Options**
- **attributes**—Configure RADIUS attributes.
 - **nas-ip-address *nas-ip-address***—Valid IPv4 or IPv6 address of the NAS requesting user authentication.
 - **password-protocol mschap-v2**—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

- [radius-server on page 480](#)

radius-server

Supported Platforms SRX1500, SRX5400, SRX5600, SRX5800

Syntax radius-server *server-address* {
 accounting-port *port-number*;
 max-outstanding-requests *value*;
 port *port-number*;
 retry *value*;
 secret *password*;
 source-address *source-address*;
 timeout *seconds*;
}

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5. Support for IPv6 source address added in Junos OS Release 12.1X47-D15.

Description Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP)).

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

- Options**
- *server-address*—Address of the RADIUS server.
 - **accounting-port** *port-number*—RADIUS server accounting port number.
Range: 1 through 65,335 files
Default: 1813
 - **port** *port-number*—RADIUS server authentication port number.
Range: 1 through 65,335 files
Default: 1812
 - **retry** *value*—Number of times that the router is allowed to attempt to contact a RADIUS server.
Range: 1 through 10
Default: 3
 - **secret** *password*—Password to use; it can include spaces if the character string is enclosed in quotation marks.
 - **max-outstanding-requests** *value*—Maximum number of outstanding requests in flight to server.
Range: 1 through 65,335 files
 - **source-address** *source-address*—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.

- **timeout *seconds***—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

rapid-commit

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax rapid-commit;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcpv6-client]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Used to signal the use of the two-message exchange for address assignment.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [DHCPv6 Client Overview on page 339](#)
- [Understanding DHCPv6 Client and Server Identification on page 336](#)

reconfigure (System Services DHCP)

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
reconfigure {
  attempts number;
  clear-on-abort;
  strict;
  timeout number;
  token token-name;
  trigger {
    radius-disconnect;
  }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server group group-name]
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Release Information Statement introduced in Junos OS Release 10.4.

Description Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.

Options **attempts *number***—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 attempts

Default: 8 attempts

clear-on-abort —Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

strict —Configure the system to only allow packets that contain the reconfigure accept option.

timeout *seconds*—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempts doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 seconds

Default: 2 seconds

token *token-name*—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

trigger — Specify DHCP reconfigure trigger.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [DHCP Server, Client, and Relay Agent Overview on page 296](#)
- [DHCP Server Configuration Overview on page 302](#)

req-option

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcpv6-client]

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description The configuration options requested by the DHCPv6 client.

Options

dns-server—Specify a DNS server.

domain—Specify a domain name.

fqdn—Specify a fully qualified domain name.

nis-domain—Specify a Network Information Service (NIS) domain.

nis-server—Specify a Network Information Service (NIS) server.

ntp-server—Specify a Network Time Protocol (NTP) server.

sip-domain—Specify a Session Initiation Protocol (SIP) domain.

sip-server—Specify a Session Initiation Protocol (SIP) server.

time-zone—Specify a time zone.

vendor-spec—Specify vendor specification.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

retransmission-attempt (dhcp-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | retransmission-attempts <i>number</i> ; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback. |
| Options | number —Number of attempts to retransmit the packet. Range: 0 through 6 |
| 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">• Understanding DHCP Client Operation on page 315• Minimum DHCP Client Configuration on page 315 |

retransmission-attempt (dhcpv6-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | retransmission-attempt <i>number</i> ; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made. |
| Options | number —Number of retransmit attempts |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

retransmission-interval (dhcp-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | retransmission-interval <i>seconds</i> ; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Specify the time between successive retransmission attempts. |
| Options | seconds —Number of seconds between successive retransmission attempts. Range: 4 through 64 seconds |
| 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">• Understanding DHCPv6 Client and Server Identification on page 336 |

root-authentication

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
root-authentication {  
  encrypted-password password;  
  load-key-file URL;  
  plain-text-password;  
  ssh-dsa public-key {  
    <from pattern-list>;  
  }  
  ssh-rsa public-key {  
    <from pattern-list>;  
  }  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify authentication information for the root login.

- Options**
- **encrypted-password *password***—Specify the encrypted authentication password. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.
 - **plain-text-password**—The CLI prompts you for a password encrypts it, and stores the encrypted version in its user database.
 - **load-key-file *URL***—File URL containing one or more SSH keys.
 - **ssh-dsa *public-key***—SSH DSA public key string.
 - **from *pattern-list***—Pattern list of allowed hosts.
 - **ssh-rsa *public-key***—SSH RSA public key string.
 - **from *pattern-list***—Pattern list of allowed hosts.

Required Privilege Level

| | |
|----------------|---|
| system | —To view this statement in the configuration. |
| system-control | —To add this statement to the configuration. |

single-connection

| | |
|---------------------------------|---|
| Supported Platforms | SRX Series, vSRX |
| Syntax | single-connection; |
| Hierarchy Level | [edit system accounting destination tacplus server <i>server-address</i>] [edit system tacplus-server <i>server-address</i>] |
| Release Information | Statement introduced in Junos OS Release 8.5. |
| Description | Optimize the attempt to connect to a TACACS+ server. Junos OS maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |

server (NTP)

Supported Platforms [SRX Series](#)

Syntax `server address <key key-number> <version value> <prefer>;`

Hierarchy Level [edit system ntp]

Release Information Statement introduced before Junos OS Release 7.4.

Description For NTP, configure the SRX Series device to operate in client mode with the remote system at the specified address. In this mode, the SRX Series device can be synchronized with the remote system, but the remote system can never be synchronized with the SRX Series device.

If the NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the client is automatically stepped back into synchronization. If the offset between the NTP client and server exceeds the 1000-second threshold, the client still synchronizes with the server, but it also generates a system log message noting that the threshold was exceeded.

Options **address**—Address of the remote system. You must specify an address, not a hostname.

key key-number—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.

Range: Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as the preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version value—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege system—To view this statement in the configuration.

Level system-control—To add this statement to the configuration.

Related Documentation

- [ntp on page 471](#)

server-address (dhcp-client)

| | |
|--------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | server address <i>ip-address</i> ; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Specify the preferred DHCP server address that is sent to DHCP clients. |
| Options | <i>ip-address</i> —DHCP server address. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

source-address (NTP, RADIUS, System Logging, or TACACS+)

| | |
|--------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | source-address <i>source-address</i> <routing-instance <i>routing-instance-name</i> >; |
| Hierarchy Level | [edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system ntp], [edit system radius-server <i>server-address</i>], [edit system syslog], [edit system tacplus-server <i>server-address</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | Specify a source address for each configured TACACS+ server, RADIUS server, or NTP server, or the source address to record in system log messages that are directed to a remote machine. |
| Options | <i>source-address</i> —A valid IP address configured on one of the SRX Series devices. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine. |
| 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"> • ntp on page 471 |

ssh-known-hosts

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
ssh-known-hosts {  
    fetch-from-server server-name;  
    host hostname {  
        dsa-key dsa-key;  
        ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;  
        ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;  
        ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;  
        rsa-key rsa-key;  
        rsa1-key rsa1-key;  
    }  
    load-key-file key-file;  
}
```

Hierarchy Level [edit security]

Release Information Statement modified in Junos OS Release 8.5.

Description Configure SSH support for known hosts and for administering SSH host key updates.

- Options**
- **fetch-from-server *server-name***—Retrieve SSH public host key information from a specified server.
 - **load-key-file *key-file***—Import SSH host-key information from the specified `/var/tmp/ssh-known-hosts` file.

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

- [\[edit security ssh-known-hosts\] Hierarchy Level on page 384](#)

static-subscribers

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series, vSRX |
| Syntax | static-subscribers { disable; } |
| Hierarchy Level | [edit system processes] |
| Release Information | Statement introduced in Junos OS Release 8.5. |
| Description | Associate subscribers with statically configured interfaces, and provide dynamic service activation for these subscribers. |
| Options | disable —Disable the static subscribers process. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |

statistics-service

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series, vSRX |
| Syntax | statistics-service { command <i>binary-file-path</i> ; disable; } |
| Hierarchy Level | [edit system processes] |
| Release Information | Statement introduced in Junos OS Release 8.5. |
| Description | Specify the Packet Forwarding Engine (PFE) statistics service management process. |
| Options | <ul style="list-style-type: none"> • command <i>binary-file-path</i>—Path to the binary process. • disable—Disable the Packet Forwarding Engine (PFE) statistics service management process. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |

subscriber-management

Supported Platforms [SRX Series, vSRX](#)

Syntax subscriber-management {
 command *binary-file-path*;
 disable;
}

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the subscriber management process.

- Options**
- **command *binary-file-path***—Path to the binary process.
 - **disable**—Disable the subscriber management process.

Required Privilege Level

| | |
|----------------|---|
| system | —To view this statement in the configuration. |
| system-control | —To add this statement to the configuration. |

subscriber-management-helper

Supported Platforms SRX Series, vSRX

Syntax subscriber-management-helper {
 command *binary-file-path*;
 disable;
 failover (alternate-media | other-routing-engine);
 }

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the subscriber management helper process.

- Options**
- **command *binary-file-path***—Path to the binary process.
 - **disable**—Disable the subscriber management helper process.
 - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
 - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
 - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege system—To view this statement in the configuration.

Level system-control—To add this statement to the configuration.

system master password

Supported Platforms [SRX Series](#)

Syntax set system master-password plain-text-password
Master password: ***
Repeat master password: ***

Hierarchy Level system

Release Information Statement introduced in Junos OS Release 15.1X49-D50.

Description Use to set a master password in a hidden configuration within the Junos OS configuration database.

Options set system master-password iteration-count—(Optional) The number of iterations to use for the PBKDF2 hash function. The range is 10 through 10000. Default value is 100. High iteration counts can impact system performance on systems with many secrets.

set system master-password pseudorandom-function (hmac-sha1 | hmac-sha2-256 | hmac-sha2-512); default hmac-sha2-256—(Optional) Hash (prf) algorithm to be used for the PBKDF2 key derivation.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- request system decrypt password

tacplus

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
tacplus {
  server server-address {
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
  }
}
```

Hierarchy Level [edit system accounting destination]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the TACACS+ accounting server.

- Options**
- ***server-address***—Specify the address of the TACACS+ authentication server.
 - ***port number***—Configure the port number on which to contact the TACACS+ server.
 - ***single-connection***—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
 - ***source-address address***—Configure a source address for each configured TACACS+ server.
 - ***timeout seconds***—Configure the amount of time that the local device waits to receive a response from a TACACS+ server.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)

tacplus-options

| | |
|--------------------------|--|
| Supported Platforms | EX Series, M Series, MX Series, OCX1100, PTX Series, QFabric System, QFX Series standalone switches, SRX Series, T Series |
| Syntax | <pre>tacplus-options { (exclude-cmd-attribute no-cmd-attribute-value); enhanced-accounting; service-name <i>service-name</i>; timestamp-and-timezone; }</pre> |
| Hierarchy Level | [edit system] |
| 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>no-cmd-attribute-value and exclude-cmd-attribute options introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 11.1 for QFX Series.</p> <p>timestamp-and-timezone option introduced in Junos OS Release 12.2.</p> <p>enhanced-accounting option introduced in Junos OS Release 14.1.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> |
| Description | Configure TACACS+ options for authentication and accounting. |
| Options | <p>enhanced-accounting—View the attribute values of a logged in user.</p> <p>exclude-cmd-attribute—Exclude the cmd attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>no-cmd-attribute-value—Set the cmd attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.</p> <p>service-name <i>service-name</i>—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.</p> <p>Default: junos-exec</p> <p>timestamp-and-timezone—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.</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 Same Authentication Service for Multiple TACACS+ Servers on page 226• Configuring TACACS+ System Accounting• Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication• enhanced-accounting |

tacplus-server

Supported Platforms EX Series, M Series, PTX Series, SRX Series, T Series, vSRX

Syntax `tacplus-server server-address {
port port-number;
secret password;
single-connection;
source-address source-address;
timeoutseconds;
}`

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the TACACS+ server.

Options • **server-address**—Address of the TACACS+ authentication server.



NOTE: Wildcard characters cannot be used in the TACACS server address or source address. This is because the TACACS server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

- **port**—Port number of TACACS+ authentication server.
- **secret**—Password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server. Password to use; can include spaces included in quotation marks.
- **single-connection**—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
- **source-address**—Source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. Configure a valid IP address on one of the device interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host hostname** statements at the **[edit system syslog]** hierarchy level.
- **timeout**—The amount of time that the local device waits to receive a response from a RADIUS or TACACS+ server. The timeout range is 1 through 90 seconds. The default is 3 seconds.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

- Related Documentation**
- [Example: Configuring a TACACS+ Server for System Authentication on page 227](#)

traceoptions (Outbound SSH)

Supported Platforms SRX Series, vSRX

Syntax

```
traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit system services outbound-ssh]

Release Information Statement introduced in Junos OS Release 10.4.

Description Set the trace options.

Options

- **file**—Configure the trace file information.

- **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
- **files *number***—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed to **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000 files

Default: 10 files

- **match *regular-expression***—Refine the output to include lines that contain the regular expression.
- **size *maximum-file-size***—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.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag**—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.
 - **all**—Trace all events.
 - **configuration**—Trace configuration events.
 - **connectivity**—Trace TCP connection handling.
- **no-remote-trace**—Disable remote tracing.

| | |
|---------------------------------|---|
| Required Privilege Level | trace—To view this statement in the configuration. trace-control—To add this statement to the configuration. |
|---------------------------------|---|

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• <i>Displaying Log and Trace Files</i> |
|------------------------------|---|

traceoptions (System Services DHCP)

Supported Platforms SRX Series, vSRX

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit routing-instances *routing-instance-name* system services dhcp-local-server],
[edit system services dhcp-local-server]
[edit system processes dhcp-service]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure extended DHCP local server tracing operations for DHCP processes.

- Options**
- **file-name**—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.
 - **files number**—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

- **match regular-expression**—(Optional) Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—(Optional) Maximum size of each trace file, in 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: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable**—(Optional) Enable unrestricted file access.
- **no-world-readable**—(Optional) Disable unrestricted file access.
- **flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events.
- **database**—Trace database operations.
- **dhcpv6-general**—Trace operations for DHCPv6.
- **dhcpv6-io**—Trace input/output operations for DHCPv6.
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-rpd**—Trace routing protocol process operations.
- **dhcpv6-session-db**—Trace session database operations for DHCPv6.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **fwd**—Trace firewall process operations.
- **general**—Trace miscellaneous general operations.
- **ha**—Trace high-availability related operations.
- **interface**—Trace interface operations.
- **io**—Trace input/output operations.
- **packet**—Trace packet decoding operations.
- **packet- option**—Trace DHCP option decoding operations.
- **performance**—Trace DHCP performance measurement operations.
- **profile**—Trace DHCP profile operations.
- **rpd**—Trace routing protocol process operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace changes in statistics.
- **ui**—Trace changes in user interface operations.
- **no remote-trace**—Disable remote tracing.

Required Privilege Level trace—To view this statement in the configuration.
 trace-control—To add this statement to the configuration.

Related Documentation • [System Configuration Statement Hierarchy on page 385](#)

trusted-key

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | trusted-key [<i>key-numbers</i>]; |
| Hierarchy Level | [edit system <i>ntp</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | For NTP, configure the keys you are allowed to use when you configure the SRX Series device to synchronize its time with other systems on the network. |
| Options | key-numbers —One or more key numbers. Each key can be any 32-bit unsigned integer except 0. |
| 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">• ntp on page 471 |

uac-service

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
uac-service {  
    command binary-file-path;  
    disable;  
    failover (alternate-media | other-routing-engine);  
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the unified access control daemon process.

- Options**
- **command *binary-file-path***—Path to the binary process.
 - **disable**—Disable the unified access control daemon process.
 - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
 - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
 - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Firewall User Authentication Overview](#)

update-router-advertisement

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | update-router-advertisement (interface <i>interface-name</i>); |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Specify the interface used to delegate prefixes. |
| Options | interface <i>interface-name</i> —Interface on which to delegate prefixes |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

update-server (dhcp-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | update-server; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Propagate DHCP options to a local DHCP server. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

update-server (dhcpv6-client)

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | update-server; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Propagate TCP/IP settings to the DHCPv6 server. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

usb-control

| | |
|---------------------------------|---|
| Supported Platforms | SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | usb-control { command <i>binary-file-path</i> ; disable; } |
| Hierarchy Level | [edit system processes] |
| Release Information | Statement introduced in Junos OS Release 8.5. |
| Description | Specify the universal serial bus (USB) supervise process. |
| Options | <ul style="list-style-type: none">• command <i>binary-file-path</i>—Path to the binary process.• disable—Disable the universal serial bus (USB) supervise process. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |

use-interface

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | use-interface-description {logical device}; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | The description configured at the physical or logical interface level is used for client identification. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

user-id

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i> }; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

vendor-id

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | vendor-id <i>vendor-id</i> ; |
| Hierarchy Level | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client. |
| Options | vendor-id —Vendor class ID. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |
| Related Documentation | |

vpn (Forwarding Options)

| | |
|---------------------------------|---|
| Syntax | vpn; |
| Hierarchy Level | [edit forwarding-options helpers bootp] |
| Release Information | Statement introduced in Junos OS Release 9.0. |
| Description | For Dynamic Host Configuration Protocol (DHCP) or BOOTP client request forwarding, enable virtual private network (VPN) encryption for a client request to pass through a VPN tunnel. |
| 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">• DHCP Server, Client, and Relay Agent Overview on page 296 |

watchdog

Supported Platforms [SRX Series, vSRX](#)

Syntax

```
watchdog {  
    disable;  
    enable;  
    timeout value;  
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Enable or disable the watchdog timer when Junos OS encounters a problem.

- Options**
- **disable**—Disable the watchdog timer.
 - **enable**—Enable the watchdog timer.
 - **timeout *value***—Specify amount of time to wait in seconds.
Range: 1 through 3600 seconds.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

web-management

Supported Platforms [SRX Series, vSRX](#)

Syntax `web-management {
 disable;
 failover (alternate-media | other-routing-engine);
}`

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the Web management process.

- Options**
- **disable**—Disable the Web management process.
 - **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
 - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
 - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege system—To view this statement in the configuration.

Level system-control—To add this statement to the configuration.

web-management (System Services)

Supported Platforms SRX Series, vSRX

Syntax

```
web-management {
  http {
    interfaces interface-names ;
    port port;
  }
  https {
    interfaces interface-names;
    local-certificate name;
    pki-local-certificate name;
    system-generated-certificate name;
    port port;
  }
  management url management url;
  session {
    idle-timeout minutes;
    session-limit number;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (no-world-readable | world-readable);
    }
    flag flag;
    level level;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 9.0.
Support for **https** introduced for high-end SRX Series Services Gateways starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways starting from Junos OS Release 15.1X49-D40.

Description Configure settings for HTTP or HTTPS access. HTTP access allows management of the device using the J-Web interface. HTTPS access allows secure management of the device using the J-Web interface. With HTTPS access, communication is encrypted between your browser and the webserver for your device.

Options **control**—Disable the SBC process.

- max-threads**—Maximum simultaneous threads to handle requests.
Range: 0 through 16

http—Configure HTTP.

- **interface** [*value*]—Interface value that accepts HTTP access.
- **port** *number*—TCP port for incoming HTTP connections.

Range: 1 through 65,535

https—Configure HTTPS.

- **interface** [*value*]—Interface value that accept HTTP access.
- **port** *number*—TCP port for incoming HTTP connections.

Range: 1 through 65,535

- **local-certificate**—X.509 certificate to use from the configuration.
- **pki-local-certificate**—X.509 certificate to use from the PKI local store.
- **system-generated-certificate**—X.509 certificate generated automatically by the system.

management url *management url*—URL path for Web management access.

session—Configure the Web-management session.

- **idle-timeout** *minutes*—Default timeout of Web-management sessions in minutes.
- **session-limit** *number*—Maximum number of Web-management sessions to allow.

traceoptions—Set the trace options.

- **file**—Configure the trace file information.
 - *filename*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
 - **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size maximum file-size** option.

Range: 2 through 1000 files

Default: 10 files

- **match regular-expression**—Refine the output to include lines that contain the regular expression.
- **size maximum-file-size**—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Range: 10 KB through 1 GB

Default: 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files number** option.

- **(world-readable | no-world-readable)**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.
- **flag flag**—Specify which tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags.
 - **all**—Trace all areas.
 - **configuration**—Trace configuration.
 - **dynamic-vpn**—Trace dynamic VPN events.
 - **init**—Trace the daemon init process.
 - **mgd**—Trace MGD requests.
 - **webauth**—Trace Web authentication requests.
- **level level**—Specify the level of debugging output.
 - **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**—Disable remote tracing.

| | |
|------------------------------|--|
| Required Privilege | system—To view this statement in the configuration. |
| Level | system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Firewall User Authentication Overview</i>• <i>Dynamic VPN Overview</i> |

CHAPTER 19

Operational Commands

- clear dhcp client binding
- clear dhcp client statistics
- clear dhcp relay binding
- clear dhcp relay statistics
- clear dhcp server binding
- clear dhcp server statistics
- clear dhcpv6 client binding
- clear dhcpv6 client statistics
- clear dhcpv6 server binding (Local Server)
- clear dhcpv6 server statistics (Local Server)
- clear system login lockout
- file archive
- file checksum md5
- file checksum sha1
- file checksum sha-256
- file compare
- file copy
- file delete
- file list
- file rename
- file show
- request dhcp client renew
- request dhcpv6 client renew
- request system autorecovery state
- request system decrypt password
- request system download abort
- request system download clear
- request system download pause

- [request system download resume](#)
- [request system download start](#)
- [request system firmware upgrade](#)
- [request system license update](#)
- [request system power-off fpc](#)
- [request system services dhcp](#)
- [request system snapshot \(SRX Series\)](#)
- [request system software abort in-service-upgrade \(ICU\)](#)
- [request system software add \(Maintenance\)](#)
- [request system reboot](#)
- [request system software rollback \(SRX Series\)](#)
- [request system zeroize](#)
- [restart \(Reset\)](#)
- [Restart Commands Overview on page 568](#)
- [show chassis routing-engine \(View\)](#)
- [show cli authorization](#)
- [show dhcp client binding](#)
- [show dhcp client statistics](#)
- [show dhcp relay binding](#)
- [show dhcp relay statistics](#)
- [show dhcp server binding](#)
- [show dhcp server statistics](#)
- [show dhcpv6 client binding](#)
- [show dhcpv6 client statistics](#)
- [show dhcpv6 server binding \(View\)](#)
- [show dhcpv6 server statistics \(View\)](#)
- [show firewall \(View\)](#)
- [show system autorecovery state](#)
- [show system download](#)
- [show system license \(View\)](#)
- [show system login logout](#)
- [show system services dhcp client](#)
- [show system services dhcp relay-statistics](#)
- [show system snapshot media](#)
- [show system storage partitions \(View SRX Series\)](#)

clear dhcp client binding

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | clear dhcp client binding [all interface <interface-name>] [routing-instance <routing-instance-name>] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table. |
| Options | <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>interface <interface-name>—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p>routing-instance <routing-instance-name>—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show dhcp client binding on page 573 |
| Output Fields | This command produces no output. |

clear dhcp client statistics

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax clear dhcp client statistics
<all>
<interface>
<routing-instance>

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.

Options **all**—(Optional) Clear all the DHCP client statistics.

interface—(Optional) Clear the statistics for DHCP clients on the specified interface.

routing-instance —(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- [show dhcp client statistics on page 576](#)

Output Fields This command produces no output.

clear dhcp relay binding

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | clear dhcp relay binding <all ip-address mac-address> <interface interface-name> <routing-instance routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table. |
| Options | <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p>mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show dhcp relay binding on page 578 |
| Output Fields | This command produces no output. |

clear dhcp relay statistics

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | clear dhcp relay statistics <routing-instance routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics. |
| Options | routing-instance routing-instance-name —(Optional) Clear the DHCP relay statistics on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show dhcp relay statistics on page 580 |
| Output Fields | This command produces no output. |

clear dhcp server binding

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | clear dhcp server binding <all ip-address mac-address> <interface interface-name> <routing-instance routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server. |
| Options | <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>ip-address— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p>mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show dhcp server binding on page 582 |
| Output Fields | This command produces no output. |

clear dhcp server statistics

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | clear dhcp server statistics <routing-instance routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics. |
| Options | routing-instance routing-instance-name —(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show dhcp server statistics on page 584 |
| Output Fields | This command produces no output. |

clear dhcpv6 client binding

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | clear dhcpv6 client binding [all interface <i>interface-name</i>] [routing-instance <i>routing-instance-name</i>] |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table. |
| Options | <p>all—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p>interface <i>interface-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for DHCPv6 clients on the default routing instance.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show dhcpv6 client binding on page 586 |
| Output Fields | This command produces no output. |

clear dhcpv6 client statistics

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | clear dhcpv6 client statistics routing-instance <i>routing-instance-name</i> |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Clear all DHCPv6 client statistics. |
| Options | routing-instance <i>routing-instance-name</i> —(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show dhcpv6 client statistics on page 588 |
| Output Fields | This command produces no output. |

clear dhcpv6 server binding (Local Server)

Supported Platforms [SRX Series](#)

Syntax `clear dhcpv6 server binding`
`<all | client-id | ip-address | session-id>`
`<interface interface-name>`
`<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 10.4.

Description Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

- Options**
- `all`—(Optional) Clear the binding state for all DHCPv6 clients.
 - `client-id`—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).
 - `ip-address`—(Optional) Clear the binding state for the DHCPv6 client with the specified address.
 - `session-id`—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.
 - `interface interface-name`—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
 - `routing-instance routing-instance-name`—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level `clear`

Related Documentation [• show dhcpv6 server binding \(View\) on page 590](#)

clear dhcpv6 server statistics (Local Server)

Supported Platforms [SRX Series](#)

Syntax `clear dhcpv6 server statistics`
`<logical-system logical-system-name>`
`<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 10.4.

Description Clear all DHCPv6 local server statistics.

Options `logical-system logical-system-name`—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

`routing-instance routing-instance-name`—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level clear

Related Documentation

- [show dhcpv6 server statistics \(View\) on page 594](#)

clear system login logout

| | |
|---------------------------------|---|
| Supported Platforms | EX Series, M Series, MX Series, PTX Series, T Series |
| Syntax | clear system login logout <all> <user <i>username</i> > |
| Release Information | Command introduced in Junos OS Release 11.2. |
| Description | Unlock the user account locked as a result of invalid login attempts. |
| Options | all —Clear all locked user accounts. user <i>username</i> —Clear the specified locked user account. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• lockout-period on page 467• show system login logout on page 606 |
| Output Fields | This command produces no output. |

file archive

| | |
|--------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | <code>file archive destination <i>destination</i> source <i>source</i> <compress></code> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location. |
| Options | destination <i>destination</i> —Name of the created archive. Specify the destination as a URL or filename. source <i>source</i> — Path of directory to archive. compress —(Optional) Compress the archived file with the GNU zip (gzip) compression utility. The compressed files have the suffix .tgz . |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• Administration Guide for Security Devices |
| List of Sample Output | file archive (Multiple Files) on page 528 file archive (Single File) on page 528 file archive (with Compression) on page 529 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file archive (Multiple Files)

The following sample command archives all message files in the local directory `/var/log/messages` as the single file **messages-archive.tar**.

```
user@host> file archive source /var/log/messages* destination /var/log/messages-archive.tar
/usr/bin/tar: Removing leading / from absolute path names in the archive.
```

file archive (Single File)

The following sample command archives one message file in the local directory `/var/log/messages` as the single file **messages-archive.tar**.

```
user@host> file archive source /var/log/messages destination /var/log/messages-archive.tar
/usr/bin/tar: Removing leading / from absolute path names in the archive.
user@host
```

file archive (with Compression)

The following sample command archives and compresses all message files in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive compress source /var/log/messages* destination  
/var/log/messages-archive.tgz  
/usr/bin/tar: Removing leading / from absolute path names in the archive.
```

file checksum md5

Supported Platforms [SRX Series](#)

Syntax `file checksum md5 path`

Release Information Command introduced before Junos OS Release 7.4.

Description Calculate the Message Digest 5 (MD5) checksum of a file.

Options *path*—(Optional) Path to a filename.

Required Privilege Level maintenance

Related Documentation

- *Administration Guide for Security Devices*
- [file checksum sha1 on page 531](#)
- [file checksum sha-256 on page 532](#)

List of Sample Output [file checksum md5 on page 530](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum md5

```
user@host> file checksum md5 jbundle-5.3R2.4-export-signed.tgz
MD5 (jbundle-5.3R2.4-export-signed.tgz) = 2a3b69e43f9bd4893729cc16f505a0f5
```

file checksum sha1

Supported Platforms [SRX Series](#)

Syntax `file checksum sha1 path`

Release Information Command introduced in Junos OS Release 9.5.

Description Calculate the Secure Hash Algorithm (SHA-1) checksum of a file.

Options *path*—(Optional) Path to a filename.

Required Privilege Level maintenance

Related Documentation

- *Administration Guide for Security Devices*
- [file checksum md5 on page 530](#)
- [file checksum sha-256 on page 532](#)

List of Sample Output [file checksum sha1 on page 531](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha1

```
user@host> file checksum sha1 /var/db/scripts/opscript.slax
```

```
SHA1 (/var/db/scripts/commitscript.slax) = ba9e47120c7ce55cff29afd73eacd370e162c676
```

file checksum sha-256

Supported Platforms [SRX Series](#)

Syntax `file checksum sha-256 path`

Release Information Command introduced in Junos OS Release 9.5.

Description Calculate the Secure Hash Algorithm 2 family (SHA-256) checksum of a file.

Options *path*—(Optional) Path to a filename.

Required Privilege Level
maintenance
view
view-configuration

Related Documentation

- [Administration Guide for Security Devices](#)
- [file checksum sha1 on page 531](#)
- [file checksum md5 on page 530](#)

List of Sample Output [file checksum sha-256 on page 532](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha-256

```
user@host> file checksum sha-256 /var/db/scripts/commitscript.slax

SHA256 (/var/db/scripts/commitscript.slax) =
94c2b061fb55399e15babd2529453815601a602b5c98e5c12ed929c9d343dd71
```

file compare

| | |
|--------------------------|---|
| Supported Platforms | SRX Series, vSRX |
| Syntax | <code>file compare (files <i>from-file to-file</i>) <context unified> <ignore-white-space></code> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | <p>Compare two local files and describe the differences between them in default, context, or unified output styles:</p> <ul style="list-style-type: none"> • default—In the first line of output, c means lines were changed between the two files, d means lines were deleted between the two files, and a means lines were added between the two files. The numbers preceding this alphabetical marker represent the first file, and the lines after the alphabetical marker represent the second file. A left angle bracket (<) in front of output lines refers to the first file. A right angle bracket (>) in front of output lines refers to the second file. • context—The display is divided into two parts. The first part is the first file; the second part is the second file. Output lines preceded by an exclamation point (!) have changed. Additions are marked with a plus sign (+), and deletions are marked with a minus sign (-). • unified—The display is preceded by the line number from the first and the second file (xx,xxx,x). Before the line number, additions to the file are marked with a plus sign (+), and deletions to the file are marked with a minus sign (-). The body of the output contains the affected lines. Changes are viewed as additions plus deletions. |
| Options | <p>files <i>from-file</i>—Names of files to compare.</p> <p>files <i>to-file</i>—Names of files to compare against.</p> <p>context—(Optional) Display output in context format.</p> <p>ignore-white-space—(Optional) Ignore changes in the amount of white space.</p> <p>unified—(Optional) Display output in unified format.</p> |
| Required Privilege Level | none |
| Related Documentation | <ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i> |
| List of Sample Output | <p>file compare files on page 534</p> <p>file compare files context on page 534</p> <p>file compare files unified on page 534</p> <p>file compare files unified ignore-white-space on page 534</p> |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file compare files

```
user@host> file compare files /tmp/one /tmp/two
100c100
<          full-name "File 1";
---
>          full-name "File 2";
102c102
<          class foo; # 'foo' is not defined
---
>          class super-user;
```

file compare files context

```
user@host> file compare files /tmp/one /tmp/two context
*** /tmp/one   Wed Dec  3 17:12:50 2003
--- /tmp/two   Wed Dec  3 09:13:14 2003
*****
*** 97,104 ****
        }
    }
    user bill {
!         full-name "Bill Smith";
!         class foo; # 'foo' is not defined
        authentication {
            encrypted-password SECRET;
        }
--- 97,105 ----
    }
    user bill {
!         full-name "Bill Smith";
!         uid 1089;
!         class super-user;
        authentication {
            encrypted-password SECRET;
        }
    }
```

file compare files unified

```
user@host> file compare files /tmp/one /tmp/two unified
--- /tmp/one   Wed Dec  3 17:12:50 2003
+++ /tmp/two   Wed Dec  3 09:13:14 2003
@@ -97,8 +97,9 @@
    }
}
user bill {
-     full-name "Bill Smith";
-     class foo; # 'foo' is not defined
+     full-name "Bill Smith";
+     uid 1089;
+     class super-user;
    authentication {
        encrypted-passwordSECRET;
    }
}
```

file compare files unified ignore-white-space

```
user@host> file compare files /tmp/one /tmp/two unified ignore-white-space
```

```
--- /tmp/one    Wed Dec  3 09:13:10 2003
+++ /tmp/two    Wed Dec  3 09:13:14 2003
@@ -99,7 +99,7 @@
     user bill {
         full-name "Bill Smith";
         uid 1089;
-        class foo; # 'foo' is not defined
+        class super-user;
         authentication {
             encrypted-password <SECRET>; # SECRET-DATA
         }
     }
```

file copy

Supported Platforms [SRX Series](#)

Syntax `file copy source destination`
`<source-address source-address>`

Release Information Command introduced before Junos OS Release 7.4.

Description Copy files from one location to another location on the local device or to a location on a remote device that is reachable by the local device.



WARNING: The `ssl3-support` option is not available for configuration with the `set system services xnm-ssl` and `file copy` commands. SSLv3 is no longer supported or available.

You can use the `set system services xnm-ssl ssl3-support` command to enable SSLv3 for a Junos XML protocol client application to use as the protocol to connect to the Junos XML protocol server on a device, and you can use the `file copy source destination ssl3-support` command to enable the copying of files from an SSLv3 URL.

Using SSLv3 presents a potential security vulnerability, and we recommend that you not use SSLv3. For more details about this security vulnerability, go to <http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10656>.

Required Privilege Level maintenance

Related Documentation

- *Administration Guide for Security Devices*

List of Sample Output

- [Copy a File from the Local Device to a Personal Computer on page 536](#)
- [Copy a Configuration File Between Routing Engines on page 537](#)
- [Copy a Log File Between Routing Engines on page 537](#)
- [Copy a File Using FTP on page 537](#)
- [Copy a File Using FTP and Requiring a Password on page 537](#)
- [Copy a File Using Secure Copy on page 537](#)

Sample Output

The following are examples of a variety of file copy scenarios.

Copy a File from the Local Device to a Personal Computer

```
user@host> file copy /var/tmp/rpd.core.4 mypc:/c/junipero/tmp
```

```
...transferring.file..... |          0 KB |    0.3 kB/s | ETA: 00:00:00 | 100%
```

Copy a Configuration File Between Routing Engines

The following sample command copies a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

Copy a Log File Between Routing Engines

The following sample command copies a log file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy lcc0-re0:/var/log/chassisd lcc0-re1:/var/tmp
```

Copy a File Using FTP

To use anonymous FTP to copy a local file to a remote system:

```
user@host> file copy filename ftp://hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
user@host> file copy /config/juniper.conf ftp://hostname/juniper.conf
Receiving ftp: //hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using FTP and Requiring a Password

To use FTP where you require more privacy and are prompted for a password:

```
root@host> file copy filename ftp://user@hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
root@host> file copy /config/juniper.conf ftp://user@hostname/juniper.conf
Password for user@hostname: *****
Receiving ftp: //user@hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using Secure Copy

To use scp to copy a local file to a remote system:

```
root@host> file copy filename scp://user@hostname/path/filename
```

In the following example, `/config/juniper.conf` is the local file, `user` is the username, and `ssh-host` is the scp server:

```
root@host> file copy /config/juniper.conf scp://user@ssh-host/tmp/juniper.conf
user@ssh-host's password: *****
juniper.conf          100%
| ***** |
2198          00:00
```

file delete

| | |
|--------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | <code>file delete path</code> <code><purge></code> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | Delete a path on the device. |
| Options | path —Name of the path to delete. purge —(Optional) Overwrite regular files before deleting them. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• <i>Administration Guide for Security Devices</i> |
| List of Sample Output | file delete on page 538 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file delete

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file delete /var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpd.core
```

file list

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | <code>file list path</code> <detail recursive> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | Display a list of paths on the device. |
| Options | <p>path—(Optional) Display a list of paths.</p> <p>detail recursive—(Optional) Display detailed output or descend recursively through the directory hierarchy, respectively.</p> |
| Additional Information | The default directory is the home directory of the user logged in to the device. To view available directories, enter a space and then a slash (/) after the file list command. To view files within a specific directory, include a slash followed by the directory and, optionally, subdirectory name after the file list command. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i> |
| List of Sample Output | file list on page 539 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file list

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core
```

file rename

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | <code>file rename <i>source destination</i></code> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | Rename a file on the device. |
| Options | <i>destination</i> —New name for the file. <i>source</i> —Original name of the file. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">Administration Guide for Security Devices |
| List of Sample Output | file rename on page 540 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file rename

The following example lists the files in `/var/tmp`, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file rename /var/tmp/dcd.core /var/tmp/dcd.core.990413
user@host> file list /var/tmp
dcd.core.990413
rpd.core
snmpd.core
```

file show

| | |
|--------------------------|--|
| Supported Platforms | SRX Series |
| Syntax | file show <i>filename</i> <encoding (base64 raw)> |
| Release Information | Command introduced before Junos OS Release 7.4. |
| Description | Display the contents of a file. |
| Options | <i>filename</i> —Name of a file. encoding (base64 raw)—(Optional) Encode file contents with base64 encoding or show raw text. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • <i>Administration Guide for Security Devices</i> |
| List of Sample Output | file show on page 541 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

file show

```
user@host> file show /var/log/messages
Apr 13 21:00:08 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:00:40 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:02:48 romney last message repeated 4 times
Apr 13 21:07:04 romney last message repeated 8 times
Apr 13 21:07:13 romney /kernel: so-1/1/0: Clearing SONET alarm(s) RDI-P
Apr 13 21:07:29 romney /kernel: so-1/1/0: Asserting SONET alarm(s) RDI-P
...
```

request dhcp client renew

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | <pre>request dhcp client renew [all interface <interface-name>] routing-instance <routing-instance-name></pre> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Initiates a renew request for the specified clients if they are in the bound state. |
| Options | <p>all—Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.</p> <p>interface <interface-name>—Initiate renew requests for DHCP clients on the specified interface.</p> <p>routing-instance <routing-instance-name>—Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none">• request dhcpv6 client renew on page 543 |
| Output Fields | This command produces no output. |

request dhcpv6 client renew

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | request dhcpv6 client renew [all interface <i>interface-name</i>] routing-instance < <i>routing-instance-name</i> > |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Initiate a renew request for the specified DHCPv6 clients if they are in the bound state. |
| Options | <p>all—Initiate renew requests for all DHCPv6 clients. If you specify a routing instance, renew requests are initiated for all DHCPv6 clients within that routing instance.</p> <p>interface-name <i>interface-name</i>—Initiate renew requests for DHCPv6 clients on the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate renew requests for DHCPv6 clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.</p> |
| Required Privilege Level | view |
| Output Fields | This command produces no output. |

request system autorecovery state

Supported Platforms [SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax `request system autorecovery state (save | recover | clear)`

Release Information Command introduced in Junos OS Release 11.2.

Description Prepare the system for autorecovery of configuration, licenses, and disk information.

Options **save**—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.

The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.



NOTE:

- Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.
- A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.

recover—Recover the disk partitioning, configuration, and licenses.

After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.

clear—Clear all saved autorecovery information.

Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.

Required Privilege Level maintenance

Related Documentation

- [show system autorecovery state on page 599](#)

List of Sample Output

- [request system autorecovery state save on page 545](#)
- [request system autorecovery state recover on page 545](#)
- [request system autorecovery state clear on page 545](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

```
user@host> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving bsdlablel recovery information
```

Sample Output

request system autorecovery state recover

```
user@host> request system autorecovery state recover

Configuration:
File           Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File           Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Saved                Failed           Recovered
BSD Labels:
Slice          Recovery Information  Integrity Check  Action / Status
s1             Saved                Passed           None
s2             Saved                Passed           None
s3             Saved                Passed           None
s4             Saved                Passed           None
```

Sample Output

request system autorecovery state clear

```
user@host> request system autorecovery state clear
Clearing config recovery information
Clearing license recovery information
Clearing bsdlablel recovery information
```

request system decrypt password

Supported Platforms [SRX Series](#)

Syntax request system decrypt password

Release Information Statement introduced in Junos OS Release 15.1X49-D50.

Description Use to display plain text versions of obfuscated (\$9) or encrypted (\$8) passwords. If the password was encrypted using the new \$8\$ method, you are prompted for the master password.

Options

- **decrypt**—Decrypt a \$8\$-encrypted or \$9\$-encrypted password.

Required Privilege Level system

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
// Decrypting a $9 password
user@host> request system decrypt password $9$ABC123
Plaintext password: mysecret
```

Sample Output

```
// Decrypting a $8 password
user@host> request system decrypt password $8$ABC123
Master password:
Plaintext password: mysecret
(Simple passwords like "mysecret" are discouraged. This is an example only.)
```

request system download abort

Supported Platforms [EX Series](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#), [vSRX](#)

Syntax request system download abort <download-id>

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the **show system download** command until a **request system download clear** operation is performed.



NOTE: Only downloads in the active, paused, and error states can be aborted.

Options download-id—(Required) The ID number of the download to be aborted.

Required Privilege Level maintenance

Related Documentation

- [request system download start on page 551](#)
- [request system download pause on page 549](#)
- [request system download resume on page 550](#)
- [request system download clear on page 548](#)

List of Sample Output [request system download abort on page 547](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download abort

```
user@host> request system download abort 1
Aborted download #1
```

request system download clear

Supported Platforms [EX Series, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax request system download clear

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Delete the history of completed and aborted downloads.

Required Privilege Level maintenance

Related Documentation

- [request system download start on page 551](#)
- [request system download pause on page 549](#)
- [request system download resume on page 550](#)
- [request system download abort on page 547](#)

List of Sample Output [request system download clear on page 548](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download clear

```
user@host> request system download clear
Cleared information on completed and aborted downloads
```

request system download pause

Supported Platforms [EX Series, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax `request system download pause <download-id>`

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Suspend a particular download instance.



NOTE: Only downloads in the active state can be paused.

Options `download-id`—(Required) The ID number of the download to be paused.

Required Privilege Level maintenance

Related Documentation

- [request system download start on page 551](#)
- [request system download resume on page 550](#)
- [request system download abort on page 547](#)
- [request system download clear on page 548](#)

List of Sample Output [request system download pause on page 549](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

`request system download pause`

```
user@host> request system download pause 1
Paused download #1
```

request system download resume

Supported Platforms [EX Series](#), [LN Series](#), [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), [SRX550M](#)

Syntax `request system download resume download-id <max-rate>`

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the **request system download start** command. The user can optionally specify a new (maximum) bandwidth with the **request system download resume** command.



NOTE: Only downloads in the paused and error states can be resumed.

Options **download-id**—(Required) The ID number of the download to be resumed.

max-rate—(Optional) The maximum bandwidth for the download.

Required Privilege Level maintenance

Related Documentation

- [request system download start on page 551](#)
- [request system download pause on page 549](#)
- [request system download abort on page 547](#)
- [request system download clear on page 548](#)

List of Sample Output [request system download resume on page 550](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download resume

```
user@host> request system download resume 1
Resumed download #1
```

request system download start

| | |
|---------------------------------|--|
| Supported Platforms | EX Series, LN Series, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | request system download start (<i>url</i> <i>max-rate</i> <i>save as</i> <i>login</i> <i>delay</i>) |
| Release Information | Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. |
| Description | Creates a new download instance and identifies it with a unique integer called the download ID. |
| Options | <p>url—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p>max-rate—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as kbps, mbps, or gbps, respectively.</p> <p>save-as—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p>login—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p>delay—(Optional) The number of hours after which the download should start.</p> |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • request system download pause on page 549 • request system download resume on page 550 • request system download abort on page 547 • request system download clear on page 548 |
| List of Sample Output | request system download start on page 551 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

request system download start

```
user@host> request system download start login user:passwd ftp://ftp-server/tftpboot/1m_file
max-rate 1k
Starting download #1
```

request system firmware upgrade

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series, vSRX |
| Syntax | request system firmware upgrade |
| Release Information | Command introduced in Junos OS Release 10.2. |
| Description | Upgrade firmware on a system. |
| Options | <p>fpc—Upgrade FPC ROM monitor.</p> <p>pic—Upgrade PIC firmware.</p> <p>re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p>vcpu—Upgrade VCPU ROM monitor.</p> |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> request system license update on page 553 |
| List of Sample Output | request system firmware upgrade on page 552 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

request system firmware upgrade

```

user@host> request system firmware upgrade re bios
Part          Type          Tag Current Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1   1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re bios backup
Part          Type          Tag Current Available Status
              version      version
Routing Engine 0 RE BIOS      0   1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1   1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

```

request system license update

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series, vSRX |
| Syntax | request system license update |
| Release Information | Command introduced in Junos OS Release 9.5. |
| Description | Start autoupdating license keys from the LMS server. |
| Options | trial —Starts autoupdating trial license keys from the LMS server. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • show system license (View) on page 603 |
| List of Sample Output | request system license update on page 553 request system license update trial on page 553 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

request system license update

```
user@host> request system license update
```

```
Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

request system power-off fpc

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | request system (halt power-off reboot) power-off fpc |
| Release Information | Command introduced in Junos OS Release 11.4. |
| Description | Bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down. |
| Options | <ul style="list-style-type: none">• halt—Bring FPC offline and then halt the system.• power-off—Bring FPC offline and then power off the system.• reboot—Bring FPC offline and then reboot the system. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• request system reboot on page 560 |
| List of Sample Output | request system halt power-off fpc on page 554 request system power-off power-off fpc on page 554 request system reboot power-off fpc on page 554 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

request system halt power-off fpc

```
user@host> request system halt power-off fpc
Halt the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system power-off power-off fpc

```
user@host> request system power-off power-off fpc
Power off the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system reboot power-off fpc

```
user@host> request system reboot power-off fpc
Reboot the system ? [yes,no] (no) yes

Offline fpc slot 0
```

request system services dhcp

Supported Platforms [SRX Series, vSRX](#)

Syntax request system services dhcp (release *interface-name* | renew *interface-name*)

Release Information Command introduced in Junos OS Release 8.5.

Description Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the **show system services dhcp client *interface-name*** command.

- Options**
- **release *interface-name*** —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.
 - **renew *interface-name*** —Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.

Required Privilege Level maintenance

- Related Documentation**
- [dhcp](#)
 - [show system services dhcp client on page 607](#)

Output Fields This command produces no output.

request system snapshot (SRX Series)

Supported Platforms SRX Series, vSRX

Syntax request system snapshot
 <factory>
 <media (compact-flash | hard-disk | internal | usb)>
 <node (all | local | node-id | primary)>
 <partition>
 <slice (alternate) >

Release Information Command introduced in Junos OS Release 10.2.

Description Back up the currently running and active file system partitions on the device.

- Options**
- **media—** (Optional) Specifies the media to be included in the snapshot:
 - compact-flash— Copies the snapshot to the CompactFlash card.
 - hard-disk— Copies the snapshot to the hard disk.
 - usb— Copies the snapshot to the USB storage device.
 - **node—** (Optional) Specifies the archive data and executable areas of a specific node.
 - node-id— Specifies for node(0, 1).
 - all— Specifies for all nodes.
 - local— Specifies for local nodes.
 - primary— Specifies for primary nodes.
 - **partition -** (Default) Specifies that the target media should be repartitioned before the backup is saved to it.



NOTE: The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

Example: request system snapshot media usb partition

Example: request system snapshot media usb partition factory

- **slice—** (Optional) Takes a snapshot of the root partition the system has currently booted from to another slice in the same media.
- **alternate—** (Optional) Stores the snapshot on the other root partition in the system.



NOTE: The slice option cannot be used along with the other request system snapshot options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

| | |
|---------------------------------|--|
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • <i>Example: Installing Junos OS on SRX Series Devices Using the Partition Option</i> |
| List of Sample Output | request system snapshot media hard-disk on page 557 request system snapshot media usb (when usb device is missing on page 557 request system snapshot media compact-flash on page 557 request system snapshot partition on page 557 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

[request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

[request system snapshot media usb \(when usb device is missing](#)

```
user@host> request system snapshot media usb
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

[request system snapshot media compact-flash](#)

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

[request system snapshot partition](#)

```
user@host> request system snapshot partition
Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

[request system software abort in-service-upgrade \(ICU\)](#)

Supported Platforms [SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax `request system software abort in-service-upgrade`

Release Information Command introduced in Junos OS Release 11.2.

Description Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the **request system in-service-upgrade** command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

Options This command has no options.

Required Privilege Level view

Related Documentation

- [request system software in-service-upgrade \(Maintenance\)](#)

List of Sample Output [request system software abort in-service-upgrade on page 558](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request system software abort in-service-upgrade](#)

```
user@host> request system software abort in-service-upgrade
In-Service-Upgrade aborted
```

request system software add (Maintenance)

| | |
|---------------------------------|--|
| Supported Platforms | SRX Series , vSRX |
| Syntax | <code>request system software add <i>package-name</i></code> |
| Release Information | Partition option introduced in the command in Junos OS Release 10.1. |
| Description | Install the new software package on the device. For example: request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot . |
| Options | <ul style="list-style-type: none"> • <code>delay-restart</code> — Installs the software package but does not restart the software process • <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors • <code>no-copy</code> — Installs the software package but does not saves the copies of package files • <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts • <code>partition</code> — Formats and re-partitions the media before installation • <code>reboot</code> — Reboots the device after installation is completed • <code>unlink</code> — Removes the software package after successful installation • <code>validate</code> — Checks the compatibility with current configuration before installation starts |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none"> • request system reboot on page 560 |

request system reboot

Supported Platforms [SRX Series, vSRX](#)

Syntax `request system reboot <at time> <in minutes> <media> <message 'text'>`

Release Information Command introduced in Junos OS Release 10.1.
Command **hypervisor** option introduced in Junos OS Release 15.1X49-D10 for vSRX.
Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.

Description Reboot the software.

- Options**
- *at time*— Specifies the time at which to reboot the device . You can specify time in one of the following ways:
 - *now*— Reboots the device immediately. This is the default.
 - *+minutes*— Reboots the device in the number of minutes from now that you specify.
 - *yymmddhhmm*— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
 - *hh:mm*— Reboots the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
 - *in minutes*— Specifies the number of minutes from now to reboot the device. This option is a synonym for the *at +minutes* option
 - *media type*— Specifies the boot device to boot the device from:
 - *disk/internal*— Reboots from the internal media. This is the default.
 - *usb*— Reboots from the USB storage device.
 - *compact flash*— Reboots from the external CompactFlash card.



NOTE: The **media** command option is not available on vSRX.

- *message text*— Provides a message to display to all system users before the device reboots.

Example: `request system reboot at 5 in 50 media internal message stop`

Required Privilege Level maintenance

Related Documentation

- [request system software rollback \(SRX Series\) on page 561](#)

request system software rollback (SRX Series)

| | |
|--------------------------|--|
| Supported Platforms | SRX Series , vSRX |
| Syntax | <code>request system software rollback</code> <code><node-id></code> |
| Release Information | Command introduced in Junos OS Release 10.1. Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices. |
| Description | Revert to the software that was loaded at the last successful request system software add command. Example: request system software rollback . |
| Options | <i>node-id</i> —Identification number of the chassis cluster node. It can be 0 or 1. |
| Required Privilege Level | maintenance |
| Related Documentation | <ul style="list-style-type: none">• request system reboot on page 560 |

request system zeroize

Supported Platforms [SRX Series](#)

Syntax `request system zeroize <media>`

Description Erases all configuration information and resets all key values. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories.

The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the Junos OS CLI by typing `cli` at the prompt.

Options **media**—(Optional) In addition to removing all configuration and log files, the media option causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and the like. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the request system zeroize media operation can take considerably more time than the request system zeroize operation. However, the critical security parameters are all removed at the beginning of the process.



NOTE: The media option is not supported on SRX5000 line devices.

Required Privilege Level Not applicable.

Related Documentation

- [request system reboot on page 560](#)
- [request system software rollback \(SRX Series\) on page 561](#)

List of Sample Output [request system zeroize on page 562](#)

Sample Output

`request system zeroize`

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no)  yes
```

```
warning: zeroizing re0
```

```
Loading /boot/loader  Consoles: serial port
BIOS driver C: is disk0
```

```
BIOS 607kB/2087552kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.1
(builder@youcompany.com, Mon Mar 28 20:49:26 UTC 2011)
Loading /boot/defaults/loader.config
/kernel text=0x837a60 data=0x46a78+0x9d44c syms=[0x4+0x8f38+0x4+0xca1ee]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
platform_early_bootinit: MAG Series Early Boot Initialization
GDB: debug ports: sio
GDB: current port: sio
KDB: debugger backends: ddb gdb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
...
output truncated
```

restart (Reset)

Supported Platforms SRX Series, vSRX

Syntax restart

```
<application-identification | application-security | audit-process | commitd-service
| chassis-control | class-of-service | database-replication | datapath-trace-service | ddns
| dhcp | dhcp-service | dynamic-flow-capture | disk-monitoring | event-processing |
ethernet-connectivity-fault-management | ethernet-link-fault-management
| extensible-subscriber-services | fipsd | firewall | firewall-authentication-service
| general-authentication-service | gracefully | gprs-process | idp-policy | immediately
| interface-control | ipmi | ipsec-key-management | jflow-service | jnu-management
| jnx-wmicd-service | jsrp-service | kernel-replication | l2-learning | l2cpd-service | lacp
| license-service | logical-system-service | mib-process | mountd-service | named-service
| network-security | network-security-trace | nfsd-service | ntpd-service | pgm
| pic-services-logging | profilerd | pki-service | remote-operations | rest-api | routing | sampling
| sampling-route-record | scc-chassisd | secure-neighbor-discovery | security-intelligence
| security-log | services | service-deployment | simple-mail-client-service | soft | snmp
| static-routed | statistics-service | subscriber-management | subscriber-management-helper
| system-log-vital | tunnel-oamd | uac-service | user-ad-authentication | vrrp
| web-management >
```

Release Information Command introduced before Junos OS Release 9.2

Description Restart a Junos OS process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

- Options**
- application-identification—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
 - application-security—(Optional) Restart the application security process.
 - audit-process—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, for analyzing and tracking usage patterns, and for billing a user based upon the amount of time used or the type of services accessed.
 - chassis-control—(Optional) Restart the chassis management process.
 - class-of-service—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.
 - commitd-service—(Optional) Restart the committed services.
 - database-replication—(Optional) Restart the database replication process.
 - datapath-trace-service—(Optional) Restart the Restart the packet path tracing process.

- `ddns`—(Optional) Restart the dynamic domain name system, which dynamically updates IP addresses for registered domain names.
- `dhcp`—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
- `dhcp-service`—(Optional) Restart the Dynamic Host Configuration Protocol process.
- `disk-monitoring`—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.
- `dynamic-flow-capture`—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on PIC3 monitoring services cards.
- `ethernet-connectivity-fault-management`—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.
- `ethernet-link-fault-management`—(Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.
- `event-processing`—(Optional) Restart the event process (`eventd`).
- `extensible-subscriber-services`—(Optional) Restart the extensible subscriber services process.
- `fipsd`—(Optional) Restart the `fipsd` services.
- `firewall`—(Optional) Restart the firewall management process, which manages the firewall configuration and accepts or rejects packets that are transiting an interface on a router or switch.
- `firewall-authentication-service`—(Optional) Restart the firewall authentication service process.
- `general-authentication-service`—(Optional) Restart the general authentication process.
- `gprs-process`—(Optional) Restart the General Packet Radio Service (GPRS) process.
- `gracefully`—(Optional) Restart the software process.
- `idp-policy`—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.
- `immediately`—(Optional) Immediately restart the software process.
- `interface-control`—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.
- `ipmi`—(Optional) Restart the intelligent platform management interface process.
- `ipsec-key-management`—(Optional) Restart the IPsec key management process.
- `jflow-service`—(Optional) Restart `jflow` service process.
- `jnu-management`—(Optional) Restart `jnu` management process.
- `jnx-wmicd-service`—(Optional) Restart `jnx wmicd` service process.

- `jsrp-service`—(Optional) Restart the Juniper Services Redundancy Protocol (jsrdp) process, which controls chassis clustering.
- `kernel-replication`—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.
- `lACP`—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link. The LACP process allows link aggregation control instances to reach agreement on the identity of the LAG to which a link belongs, moves the link to that LAG, and enables the transmission and reception processes for the link to function in an orderly manner.
- `l2cpd-service`—(High-end SRX Series only) (Optional) Restart the Layer 2 Control Protocol (L2CP) process, which enables features such as L2 protocol tunneling and nonstop bridging.
- `l2-learning`—(Optional) Restart the Layer 2 (L2) address flooding and learning process.
- `license-service`—(Optional) Restart the feature license management process.
- `logical-system-service`—(Optional) Restart the logical system service process.
- `mib-process`—(Optional) Restart the MIB version II process, which provides the router's MIB II agent.
- `mountd-service`—(Optional) Restart the service for Network File System (NFS) mount requests.
- `named-service`—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.
- `network-security`—(Optional) Restart the network security process.
- `network-security-trace`—(Optional) Restart the network security trace process.
- `nfsd-service`—(Optional) Restart the remote NFS server process, which provides remote file access for applications that need NFS-based transport.
- `ntpd-service`—(Optional) Restart the Network Time Protocol (NTP) process.
- `pgm`—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.
- `pic-services-logging`—(Optional) Restart the logging process for some PICs. With this process, also known as `fsad` (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.
- `pki-service`—(Optional) Restart the public key infrastructure (PKI) service process.
- `profillerd`—(Optional) Restart the profiler process.
- `remote-operations`—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
- `rest-api`—(Optional) Restart the rest api process.
- `routing`—(Optional) Restart the routing protocol process (`rpd`).

- **sampling**—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.
- **sampling-route-record**—(Optional) Restart the sampling route record process.
- **scc-chassisd**—(Optional) Restart the scc chassisd process.
- **secure-neighbor-discovery**—(Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.
- **security-intelligence**—(Optional) Restart security intelligence process.
- **security-log**—(Optional) Restart the security log process.
- **service-deployment**—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.
- **services**—(Optional) Restart a service.
- **simple-mail-client-service**—(Optional) Restart the simple mail client service process.
- **snmp**—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.
- **static-routed**—(Optional) Restart the static routed process.
- **soft**—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.
- **statistics-service**—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.
- **subscriber-management**—(Optional) Restart the subscriber management process.
- **subscriber-management-helper**—(Optional) Restart the subscriber management helper process.
- **system-log-vital**—(Optional) Restart system log vital process.
- **tunnel-oamd**—(Optional) Restart the tunnel OAM process for L2 tunneled networks.
- **uac-service**—(Optional) Restart the Unified Access Control (UAC) process.
- **user-ad-authentication**—(Optional) Restart User ad Authentication process
- **vrrp**—(Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.
- **web-management**—(Optional) Restart the Web management process.

Required Privilege Level reset

Related Documentation • [Restart Commands Overview on page 568](#)

List of Sample Output [restart interfaces on page 568](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

Restart Commands Overview

Supported Platforms [SRX Series, vSRX](#)

Use the **restart** operational commands to restart software processes on the device. Operational commands are organized alphabetically.

Related Documentation

- [restart](#)

show chassis routing-engine (View)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show chassis routing-engine`

Release Information Command introduced in Junos OS Release 9.5.

Description Display the Routing Engine status of the chassis cluster.

Required Privilege Level view

Related Documentation

- [cluster \(Chassis\)](#)
- [request system snapshot \(SRX Series\) on page 556](#)

List of Sample Output [show chassis routing-engine \(Sample 1 - SRX550M\) on page 570](#)
[show chassis routing-engine \(Sample 2- vSRX\) on page 570](#)

Output Fields [Table 18 on page 569](#) lists the output fields for the `show chassis routing-engine` command. Output fields are listed in the approximate order in which they appear.

Table 18: show chassis routing-engine Output Fields

| Field Name | Field Description |
|----------------------|--|
| Temperature | Routing Engine temperature. (Not available for vSRX deployments.) |
| CPU temperature | CPU temperature. (Not available for vSRX deployments.) |
| Total memory | Total memory available on the system. |
| Control plane memory | Memory available for the control plane. |
| Data plane memory | Memory reserved for data plane processing. |
| CPU utilization | Current CPU utilization statistics on the control plane core. |
| User | Current CPU utilization in user mode on the control plane core. |
| Background | Current CPU utilization in nice mode on the control plane core. |
| Kernel | Current CPU utilization in kernel mode on the control plane core. |
| Interrupt | Current CPU utilization in interrupt mode on the control plane core. |
| Idle | Current CPU utilization in idle mode on the control plane core. |
| Model | Routing Engine model. |

Table 18: show chassis routing-engine Output Fields (*continued*)

| Field Name | Field Description |
|--------------------|---|
| Start time | Routing Engine start time. |
| Uptime | Length of time the Routing Engine has been up (running) since the last start. |
| Last reboot reason | Reason for the last reboot of the Routing Engine. |
| Load averages | The average number of threads waiting in the run queue or currently executing over 1-, 5-, and 15-minute periods. |

Sample Output

show chassis routing-engine (Sample 1 - SRX550M)

```

user@host> show chassis routing-engine
Routing Engine status:
  Temperature          38 degrees C / 100 degrees F
  CPU temperature      36 degrees C / 96 degrees F
  Total memory         512 MB Max   435 MB used ( 85 percent)
    Control plane memory 344 MB Max   296 MB used ( 86 percent)
    Data plane memory   168 MB Max   138 MB used ( 82 percent)
  CPU utilization:
    User                8 percent
    Background          0 percent
    Kernel              4 percent
    Interrupt           0 percent
    Idle                88 percent
  Model                RE-SRX5500-LOWMEM
  Serial ID            AAP8652
  Start time           2009-09-21 00:04:54 PDT
  Uptime               52 minutes, 47 seconds
  Last reboot reason    0x200:chassis control reset
  Load averages:       1 minute   5 minute   15 minute
                       0.12       0.15       0.10

```

Sample Output

show chassis routing-engine (Sample 2- vSRX)

```

user@host> show chassis routing-engine
Routing Engine status:
  Total memory         1024 MB Max   358 MB used ( 35 percent)
  Control plane memory 1024 MB Max   358 MB used ( 35 percent)
  5 sec CPU utilization:
    User                2 percent
    Background          0 percent
    Kernel              4 percent
    Interrupt           6 percent
    Idle                88 percent
  Model                VSRX RE
  Start time           2015-03-03 07:04:18 UTC
  Uptime               2 days, 11 hours, 51 minutes, 11 seconds
  Last reboot reason    Router rebooted after a normal shutdown.
  Load averages:       1 minute   5 minute   15 minute
                       0.07       0.04       0.06

```


show cli authorization

Supported Platforms EX Series, M Series, MX Series, PTX Series, SRX Series, T Series, vSRX

Syntax show cli authorization

Release Information Command introduced before Junos OS Release 7.4.

Description Display the permissions for the current user.

```
user@host> show cli authorization
Current user: 'root' login: 'boojum' class '(root)'
Permissions:
Permissions:
  admin      -- Can view user accounts
  admin-control-- Can modify user accounts
  clear      -- Can clear learned network info
  configure  -- Can enter configuration mode
  control    -- Can modify any config
  edit       -- Can edit full files
  field      -- Can use field debug commands
  floppy     -- Can read and write the floppy
  interface  -- Can view interface configuration
  interface-control-- Can modify interface configuration
  network    -- Can access the network
  reset      -- Can reset/restart interfaces and daemons
  routing    -- Can view routing configuration
  routing-control-- Can modify routing configuration
  shell      -- Can start a local shell
  snmp       -- Can view SNMP configuration
  snmp-control-- Can modify SNMP configuration
  system     -- Can view system configuration
  system-control-- Can modify system configuration
  trace      -- Can view trace file settings
  trace-control-- Can modify trace file settings
  view       -- Can view current values and statistics
  maintenance -- Can become the super-user
  firewall   -- Can view firewall configuration
  firewall-control-- Can modify firewall configuration
  secret     -- Can view secret statements
  secret-control-- Can modify secret statements
  rollback   -- Can rollback to previous configurations
  security   -- Can view security configuration
  security-control-- Can modify security configuration
  access     -- Can view access configuration
  access-control-- Can modify access configuration
  view-configuration-- Can view all configuration (not including secrets)
  flow-tap    -- Can view flow-tap configuration
  flow-tap-control-- Can modify flow-tap configuration
  idp-profiler-operation-- Can Profiler data
  pgcp-session-mirroring-- Can view pgcp session mirroring configuration
  pgcp-session-mirroring-control-- Can modify pgcp session mirroring
  configuration
  storage     -- Can view fibre channel storage protocol configuration
  storage-control-- Can modify fibre channel storage protocol configuration
  all-control -- Can modify any configuration
```

Required Privilege Level view

show dhcp client binding

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax `show dhcp client binding`
`[<address> | interface <interface-name>]`
`routing-instance <routing-instance name>`
`[brief | detail | summary]`

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options **address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- **ip-address**—The specified IP address.
- **mac-address**—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level view

Related Documentation • [clear dhcp client binding on page 517](#)

List of Sample Output [show dhcp client binding on page 574](#)

Output Fields [Table 19 on page 573](#) lists the output fields for the **show dhcp client binding** command. Output fields are listed in the approximate order in which they appear.

Table 19: show dhcp client binding Output Fields

| Field Name | Field Description |
|------------------|--------------------------------------|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Server | IP address of the DHCP server. |

Table 19: show dhcp client binding Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|---|
| Expires | Number of seconds in which the lease expires. |
| State | State of the address binding table on the DHCP local server. |
| Interface | Interface on which the request was received. |
| Lease Expires | Date and time at which the client's IP address lease expires. |
| Lease Expires in | Number of seconds in which the lease expires. |
| Lease Start | Date and time at which the client's IP address lease started. |
| Vendor Identifier | Vendor identifier. |
| Server Identifier | IP address of the DHCP server. |
| Client IP Address | IP address of the DHCP client. |

Sample Output

show dhcp client binding

```

user@host> show dhcp client binding
2 clients, (2 bound, 0 init, 0 discover, 0 renew, 0 rebind)

      IP address      Hardware address      Server      Expires      State
Interface
  10.1.1.89          00:0a:12:00:12:12      10.1.1.1      348          BOUND
fe-0/0/1.0
  20.1.1.90          00:0a:12:00:12:34      20.1.1.1      568          BOUND
fe-0/0/2.0

user@host> show dhcp client binding interface fe-0/0/1.0 detail
Client Interface: fe-0/0/1.0
      Hardware address:      00:0a:12:00:12:12
      State:                  BOUND
      Lease Expires:          2010-09-16 14:45:41 UTC
      Lease Expires in:       528 seconds
      Lease Start:            2010-09-16 14:35:41 UTC
      Vendor Identifier:       ether
      Server Identifier:       10.1.1.1
      Client IP Address:       10.1.1.89
      update server            enabled

DHCP Options :
      Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3
]
      Name: server-identifier, Value: 10.1.1.1
      Name: router, Value: [ 10.1.1.80 ]
      Name: domain-name, Value: example-50

```

```
user@host> show dhcp client binding 10.1.1.89
```

| IP address | Hardware address | Server | Expires | State | Interface |
|------------|-------------------|----------|---------|-------|------------|
| 10.1.1.89 | 00:0a:12:00:12:12 | 10.1.1.1 | 348 | BOUND | fe-0/0/1.0 |

show dhcp client statistics

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | show dhcp client statistics <routing-instance <i>routing-instance-name</i> > |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Display Dynamic Host Configuration Protocol (DHCP) client statistics. |
| Options | routing-instance <i>routing-instance-name</i> —(Optional) Display the statistics for DHCP clients on the specified routing instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear dhcp client statistics on page 518 |
| List of Sample Output | show dhcp client statistics on page 577 |
| Output Fields | Table 20 on page 576 lists the output fields for the show dhcp client statistics command. Output fields are listed in the approximate order in which they appear. |

Table 20: show dhcp client statistics

| Field Name | Field Description |
|-------------------|---|
| Packets dropped | Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. |
| Messages received | Number of DHCP messages received. <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP protocol data units (PDUs) received • DHCPOFFER—Number of DHCP PDUs of type OFFER received • DHCPACK—Number of DHCP PDUs of type ACK received • DHCPNACK—Number of DHCP PDUs of type NACK received • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received |

Table 20: show dhcp client statistics (*continued*)

| Field Name | Field Description |
|---------------|--|
| Messages sent | <p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted • DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted • DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted • DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted • DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted • DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted • DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted |

Sample Output

show dhcp client statistics

```

user@host> show dhcp client statistics
Packets dropped:
  Total                0
Messages received:
  BOOTREPLY            0
  DHCPOFFER            0
  DHCPACK              0
  DHCPNAK              0
  DHCPFORCERENEW      0
Messages sent:
  BOOTREQUEST          0
  DHCPDECLINE          0
  DHCPDISCOVER         0
  DHCPREQUEST          0
  DHCPINFORM           0
  DHCPRELEASE          0
  DHCPRENEW            0
  DHCPREBIND           0

```

show dhcp relay binding

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax Show dhcp relay binding
 [<address> | interface <interface-name>]
 routing-instance <routing-instance name>
 [brief | detail | summary]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.

Options **address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- **ip-address**—The specified IP address.
- **mac-address**—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level view

Related Documentation • [clear dhcp relay binding on page 519](#)

List of Sample Output [show dhcp relay binding on page 579](#)

Output Fields [Table 21 on page 578](#) lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 21: show dhcp relay binding Output Fields

| Field Name | Field Description |
|---------------------|--|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Request received on | Interface on which the request was received. |

Table 21: show dhcp relay binding Output Fields (*continued*)

| Field Name | Field Description |
|-------------|---|
| Type | Type of DHCP packet processing performed on the device. |
| Obtained at | Date and time at which the client's IP address lease started. |
| Expires at | Date and time at which the client's IP address lease expires. |
| State | State of the address binding table on the DHCP local server. |

Sample Output

show dhcp relay binding

```

user@host> show dhcp relay binding detail
IP address      Hardware address  Type      Lease expires      State
100.20.32.1     90:00:00:01:00:01 active    2007-01-17 11:38:47 PST
rebind
100.20.32.3     90:00:00:02:00:01 active    2007-01-17 11:38:41 PST
rebind
100.20.32.4     90:00:00:03:00:01 active    2007-01-17 11:38:01 PST
rebind
100.20.32.5     90:00:00:04:00:01 active    2007-01-17 11:38:07 PST
rebind
100.20.32.6     90:00:00:05:00:01 active    2007-01-17 11:38:47 PST
rebind

```

```

user@host> show dhcp relay binding 100.20.32.1
Active binding information:
    IP address      100.20.32.1
    Hardware address 90:00:00:01:00:01

Lease information:
    Type      DHCP
    Obtained at 2007-01-17 11:28:47 PST
    Expires at 2007-01-17 11:38:47 PST

> show dhcp relay binding 100.20.32.1 detail
Active binding information:
    IP address      100.20.32.1
    Hardware address 90:00:00:01:00:01
    Request received on fe-0/0/2.0, relayed by 100.20.32.2

Lease information:
    Type      DHCP
    Obtained at 2007-01-17 11:28:47 PST
    Expires at 2007-01-17 11:38:47 PST
    State      rebind

```

show dhcp relay statistics

| | |
|---------------------------------|---|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | show dhcp relay statistics [<routing-instance>] |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Display Dynamic Host Configuration Protocol (DHCP) relay statistics. |
| Options | routing-instance —(Optional) Display the DHCP relay statistics on the specified routing instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear dhcp relay statistics on page 520 |
| List of Sample Output | show dhcp relay statistics on page 580 |
| Output Fields | Table 22 on page 580 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear. |

Table 22: show dhcp relay statistics

| Field Name | Field Description |
|-------------------|--|
| Messages received | <p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received |
| Messages sent | <p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted |

Sample Output

show dhcp relay statistics

```
user@host> show dhcp relay statistics
```

Messages received:

| | |
|--------------|---|
| BOOTREQUEST | 0 |
| DHCPDECLINE | 0 |
| DHCPDISCOVER | 0 |
| DHCPINFORM | 0 |
| DHCPRELEASE | 0 |
| DHCPREQUEST | 0 |

Messages sent:

| | |
|----------------|---|
| BOOTREPLY | 0 |
| DHCPOFFER | 0 |
| DHCPACK | 0 |
| DHCPNAK | 0 |
| DHCPFORCERENEW | 0 |

show dhcp server binding

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX](#)

Syntax `show dhcp server binding`
`[interface <interface name>]`
`<brief | detail | summary | verbose>`
`<ip-address | MAC address>`
`<routing-instance routing-instance-name>`

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.

Options `interface <interface name>`—(Optional) Display information about active client bindings on the specified interface.

`brief | detail | summary`—(Optional) Display the specified level of output about active client bindings. The default is `brief`, which produces the same output as **show dhcp server binding**.

`ip-address`—Display DHCP binding information for a specific client identified by the specified IP address.

`MAC address`—Display DHCP binding information for a specific client identified by the specified MAC address.

`routing-instance routing-instance-name`—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege Level `view`

Related Documentation

- [clear dhcp server binding on page 521](#)

List of Sample Output [show dhcp server binding on page 583](#)

Output Fields [Table 23 on page 582](#) lists the output fields for the `show dhcp server binding` command. Output fields are listed in the approximate order in which they appear.

Table 23: show dhcp server binding Output Fields

| Field Name | Field Description |
|---------------------|--|
| IP address | IP address of the DHCP client. |
| Hardware address | Hardware address of the DHCP client. |
| Request received on | Interface on which the request was received. |

Table 23: show dhcp server binding Output Fields (*continued*)

| Field Name | Field Description |
|-------------|---|
| Type | Type of DHCP packet processing performed on the device. |
| Obtained at | Date and time at which the client's IP address lease started. |
| Expires at | Date and time at which the client's IP address lease expires. |
| State | State of the address binding table on the DHCP local server. |

Sample Output

show dhcp server binding

```

user@host> show dhcp server binding 100.20.32.1 detail
Active binding information:
    IP address      100.20.32.1
    Hardware address 90:00:00:01:00:01
    Request received on fe-0/0/2.0, relayed by 100.20.32.2

Lease information:
    Type           DHCP
    Obtained at    2007-01-17 11:28:47 PST
    Expires at     2007-01-17 11:38:47 PST
    State          rebind

```

show dhcp server statistics

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | show dhcp server statistics <routing-instance> |
| Release Information | Statement introduced in Junos OS Release 12.1X44-D10. |
| Description | Display Dynamic Host Configuration Protocol (DHCP) local server statistics. |
| Options | routing-instance —(Optional) Display information about DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear dhcp server statistics on page 522 |
| List of Sample Output | show dhcp server statistics on page 585 |
| Output Fields | Table 24 on page 584 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear. |

Table 24: show dhcp server statistics

| Field Name | Field Description |
|-------------------|---|
| Packets dropped | Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. |
| Messages received | Number of DHCP messages sent. <ul style="list-style-type: none"> BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received DHCPDECLINE—Number of DHCP PDUs of type DECLINE received DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received DHCPREQUEST—Number of DHCP PDUs of type REQUEST received DHCPINFORM—Number of DHCP PDUs of type INFORM received DHCPRELEASE—Number of DHCP PDUs of type RELEASE received |
| Messages sent | Number of DHCP messages received. <ul style="list-style-type: none"> BOOTREPLY—Number of BOOTP PDUs transmitted DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted DHCPACK—Number of DHCP PDUs of type ACK transmitted DHCPNACK—Number of DHCP PDUs of type NACK transmitted DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted |

Sample Output

show dhcp server statistics

```
user@host> show dhcp server statistics
Packets dropped:
  Total                                0

Messages received:
  BOOTREQUEST                          0
  DHCPDECLINE                          0
  DHCPDISCOVER                         0
  DHCPINFORM                           0
  DHCPRELEASE                          0
  DHCPREQUEST                          0

Messages sent:
  BOOTREPLY                            0
  DHCPOFFER                            0
  DHCPACK                              0
  DHCPNAK                              0
  DHCPFORCERENEW                       0
```

show dhcpv6 client binding

Supported Platforms [SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M](#)

Syntax `show dhcpv6 client binding`
`interface interface-name`
`routing-instance <routing-instance-name>`
`[brief | detail | summary]`

Release Information Statement introduced in Junos OS Release 12.1X45-D10.

Description Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.

Options `interface interface-name`—(Optional) Perform this operation on the specified interface.

`routing-instance routing-instance-name`—(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.

`brief`—(Optional) Display brief information about the active client bindings.

`detail`—(Optional) Display detailed client binding information.

`summary`—(Optional) Display a summary of DHCPv6 client information.

Required Privilege Level view

Related Documentation

- [clear dhcpv6 client binding on page 523](#)

List of Sample Output [show dhcpv6 client binding on page 587](#)

Output Fields [Table 25 on page 586](#) lists the output fields for the `show dhcpv6 client binding` command. Output fields are listed in the approximate order in which they appear.

Table 25: show dhcpv6 client binding Output Fields

| Field Name | Field Description |
|------------------|--|
| Hardware Address | Hardware address of the DHCPv6 client. |
| State | State of the address-binding table on the DHCPv6 local server. |
| Lease Expires | Date and time at which the client's IP address lease expires. |
| Lease Expires in | Number of seconds until the lease expires. |
| Lease Start | Date and time at which the client's IP address lease started. |
| Client DUID | The DHCPv6 client's unique identifier. |
| Bind type | The bind type. |

Table 25: show dhcpv6 client binding Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|---|
| Client Type | The type of DHCPv6 client. The client type can be autoconfig or stateful. |
| Rapid Commit | Two-message exchange option for address assignment. |
| Server IP Address | IP address of the DHCPv6 server. |
| Client IP Address | IP address of the DHCPv6 client. |

Sample Output

show dhcpv6 client binding

```

user@host> show dhcpv6 client binding
IP prefix      Expires      ClientType  State  Interface  Client DUID
2001:db8::b2b7:8631:d968:8d5e/128 96          STATEFUL   BOUND  ge-0/0/1.0
LL_TIME0x3-0x0-2c:6b:f5:62:39:c1

```

show dhcpv6 client binding detail

```

Client Interface: ge-0/0/1.0
  Hardware Address:      2c:6b:f5:62:39:c1
  State:                  BOUND(DHCPV6_CLIENT_STATE_BOUND)
  Lease Expires:         2012-08-07 15:52:19 UTC
  Lease Expires in:      116 seconds
  Lease Start:           2012-08-07 15:50:19 UTC
  Client DUID             VENDOR0x00000583-0x3000103f
  Bind Type:              IA_NA
  ClientType :            STATEFUL
  Rapid Commit            Off
  Server Ip Address:      fe80::230:48ff:fe5d:5bf7
  Client IP Address:      2001:db8::655b:3c80:2deb:1a3/128

DHCP options:
Name: server-identifier, Value: LL_TIME0x1-0x17acddab-00:30:48:5d:5b:f7
Name: vendor-opts, Value: 000005830002aaaa
Name: sip-server-list, Value: 2000::300 2000::302 2000::303 2000::304
Name: dns-recursive-server, Value: 2000::ff2000::fe
Name: domain-search-list, Value: 076578616d706c6503636f6d00

```

show dhcpv6 client statistics

| | |
|---------------------------------|--|
| Supported Platforms | SRX1500, SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | show dhcpv6 client statistics routing-instance<routing-instance-name> |
| Release Information | Statement introduced in Junos OS Release 12.1X45-D10. |
| Description | Display Dynamic Host Configuration Protocol (DHCPv6) client statistics. |
| Options | routing-instance <routing-instance-name>—(Optional) Display the statistics for DHCPv6 clients on the specified routing instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear dhcpv6 client statistics on page 524 |
| List of Sample Output | show dhcpv6 client statistics on page 589 |
| Output Fields | Table 26 on page 588 lists the output fields for the show dhcpv6 client statistics command. Output fields are listed in the approximate order in which they appear. |

Table 26: show dhcpv6 client statistics Output Fields

| Field Name | Field Description |
|------------------------|---|
| Dhcpv6 Packets dropped | Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the DHCPv6 Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears. |
| Messages sent | <p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE transmitted • DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT transmitted • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted • DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE transmitted • DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST transmitted • DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM transmitted • DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW transmitted • DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND transmitted |

Table 26: show dhcpv6 client statistics Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|--|
| Messages received | <p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> DHCPV6_ADVERTISE—Number of DHCPv6 PDUs of type ADVERTISE received DHCPV6_REPLY—Number of DHCPv6 PDUs of type REPLY received DHCPV6_RECONFIGURE—Number of DHCPv6 PDUs of type RECONFIGURE received |

Sample Output

show dhcpv6 client statistics

```

user@host> show dhcpv6 client statistics
Dhcpv6 Packets dropped:
    Total                0

Messages sent:
    DHCPV6_DECLINE        0
    DHCPV6_SOLICIT        3
    DHCPV6_INFORMATION_REQUEST 6
    DHCPV6_RELEASE        1
    DHCPV6_REQUEST        2
    DHCPV6_CONFIRM        0
    DHCPV6_RENEW          0
    DHCPV6_REBIND         0

Messages received:
    DHCPV6_ADVERTISE      3
    DHCPV6_REPLY          3
    DHCPV6_RECONFIGURE    0

```

show dhcpv6 server binding (View)

Supported Platforms [SRX Series](#)

Syntax `show dhcpv6 server binding`
`<brief | detail | summary>`
`<interface interface-name>`
`<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 10.4.

Description Display the address bindings in the client table for DHCPv6 local server.

- Options**
- `brief | detail | summary`—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcpv6 server binding**.
 - `interface interface-name`—(Optional) Display information about active client bindings on the specified interface.
 - `routing-instance routing-instance-name`—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- [clear dhcpv6 server binding \(Local Server\) on page 525](#)

List of Sample Output

[show dhcpv6 server binding on page 591](#)
[show dhcpv6 server binding detail on page 592](#)
[show dhcpv6 server binding interface on page 592](#)
[show dhcpv6 server binding interface detail on page 592](#)
[show dhcpv6 server binding prefix on page 593](#)
[show dhcpv6 server binding session-id on page 593](#)
[show dhcpv6 server binding summary on page 593](#)

Output Fields [Table 27 on page 590](#) lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 27: show dhcpv6p server binding Output Fields

| Field Name | Field Description | Level of Output |
|---|--|-----------------|
| <i>number</i> clients, (<i>number</i> init, <i>number</i> bound, <i>number</i> selecting, <i>number</i> requesting, <i>number</i> renewing, <i>number</i> releasing) | Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state. | summary |

Table 27: show dhc6p server binding Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|----------------------------------|--|-------------------------------|
| Prefix | Client's DHCPv6 prefix. | brief detail |
| Session Id | Session ID of the subscriber session. | brief detail |
| Expires | Number of seconds in which lease expires. | brief detail |
| State | State of the address binding table on the DHCPv6 local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • INIT—Initial state. • RELEASE—Client is releasing IP address lease. • RECONFIGURE—Client has received reconfigure message from server. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCPv6 server. • SELECTING—Client receiving offers from DHCPv6 servers. | brief detail |
| Interface | Interface on which the DHCPv6 request was received. | brief |
| Client DUID | Client's DHCP Unique Identifier (DUID). | brief detail |
| Lease expires | Date and time at which the client's IP address lease expires. | detail |
| Lease expires in | Number of seconds in which lease expires. | detail |
| Lease Start | Date and time at which the client's address lease was obtained. | detail |
| Incoming Client Interface | Client's incoming interface. | detail |
| Server IP Address | IP address of DHCPv6 server. | detail |
| Server Interface | Interface of DHCPv6 server. | detail |
| Client Id length | Length of the DHCPv6 client ID, in bytes. | detail |
| Client Id | ID of the DHCPv6 client. | detail |

Sample Output

show dhc6p server binding

```
user@host> show dhc6p server binding
```

| Prefix | Session Id | Expires | State | Interface | Client DUID |
|----------------------------|--|---------|-------|------------|-------------|
| 2001:bd8:1111:2222::/64 6 | LL_TIME0x1-0x2e159c0-00:10:94:00:00:01 | 86321 | BOUND | ge-1/0/0.0 | |
| 2001:bd8:1111:2222::/64 7 | LL_TIME0x1-0x2e159c0-00:10:94:00:00:02 | 86321 | BOUND | ge-1/0/0.0 | |
| 2001:bd8:1111:2222::/64 8 | LL_TIME0x1-0x2e159c0-00:10:94:00:00:03 | 86321 | BOUND | ge-1/0/0.0 | |
| 2001:bd8:1111:2222::/64 9 | LL_TIME0x1-0x2e159c1-00:10:94:00:00:04 | 86321 | BOUND | ge-1/0/0.0 | |
| 2001:bd8:1111:2222::/64 10 | LL_TIME0x1-0x2e159c1-00:10:94:00:00:05 | 86321 | BOUND | ge-1/0/0.0 | |

show dhcpv6 server binding detail

```

user@host> show dhcpv6 server binding detail
Session Id: 6
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

  State:                   BOUND(bound)
  Lease Expires:           2009-07-21 10:41:15 PDT
  Lease Expires in:        86308 seconds
  Lease Start:             2009-07-20 10:41:15 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address:       0.0.0.0
  Server Interface:        none
  Client Id Length:        14
  Client Id:               /0x00010001/0x02e159c0/0x00109400/0x0001

Session Id: 7
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:                   BOUND(bound)
  Lease Expires:           2009-07-21 10:41:15 PDT
  Lease Expires in:        86308 seconds
  Lease Start:             2009-07-20 10:41:15 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address:       0.0.0.0
  Server Interface:        none
  Client Id Length:        14
  Client Id:               /0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding interface

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
Prefix      Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 1      86055  BOUND  ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01

```

show dhcpv6 server binding interface detail

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
Session Id: 7
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:                   BOUND(bound)
  Lease Expires:           2009-07-21 10:41:15 PDT

```

```

Lease Expires in:      86136 seconds
Lease Start:           2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:     0.0.0.0
Server Interface:      none
Client Id Length:      14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding prefix

```

user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id: 7
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:                   BOUND(bound)
  Lease Expires:           2009-07-21 10:41:15 PDT
  Lease Expires in:        86136 seconds
  Lease Start:             2009-07-20 10:41:15 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address:       0.0.0.0
  Server Interface:        none
  Client Id Length:        14
  Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding session-id

```

user@host> show dhcpv6 server binding 8
Prefix      Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 8      86235 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03

```

show dhcpv6 server binding summary

```

user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

```

show dhcpv6 server statistics (View)

| | |
|--------------------------|---|
| Supported Platforms | SRX Series |
| Syntax | show dhcpv6 server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>> |
| Release Information | Command introduced in Junos OS Release 10.4. |
| Description | Display DHCPv6 local server statistics. |
| Options | logical-system <i>logical-system-name</i> —(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system. routing-instance <i>routing-instance-name</i> —(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none">• clear dhcpv6 server statistics (Local Server) on page 526 |
| List of Sample Output | show dhcpv6 server statistics on page 596 |
| Output Fields | Table 28 on page 595 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear. |

Table 28: show dhcpv6 server statistics Output Fields

| Field Name | Field Description |
|-------------------------------|---|
| Dhcpv6 Packets dropped | <p>Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the DHCPv6 local server • Strict Reconfigure—Number of solicit messages discarded because the client does not support reconfiguration • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Invalid server address—Number of packets discarded because an invalid server address was specified • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the DHCPv6 local server could not send |
| Messages received | <p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> • DHCPV6_CONFIRM—Number of DHCPv6 CONFIRM PDUs received. • DHCPV6_DECLINE—Number of DHCPv6 DECLINE PDUs received. • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • DHCPV6_REBIND—Number of DHCPv6 REBIND PDUs received. • DHCPV6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the DHCPv6 server. • DHCPV6_RELEASE—Number of DHCPv6 RELEASE PDUs received. • DHCPV6_RENEW—Number of DHCPv6 RENEW PDUs received. • DHCPV6_REQUEST—Number of DHCPv6 REQUEST PDUs received. • DHCPV6_SOLICIT—Number of DHCPv6 SOLICIT PDUs received. |
| Messages sent | <p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_REPLY—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted. • DHCPV6_RELAY_REPL—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay. |

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
  Total          0

Messages received:
  DHCPV6_DECLINE          0
  DHCPV6_SOLICIT          9
  DHCPV6_INFORMATION_REQUEST 0
  DHCPV6_RELEASE          0
  DHCPV6_REQUEST          5
  DHCPV6_CONFIRM          0
  DHCPV6_RENEW            0
  DHCPV6_REBIND           0
  DHCPV6_RELAY_FORW       0
Messages sent:
  DHCPV6_ADVERTISE        9
  DHCPV6_REPLY             5
  DHCPV6_RECONFIGURE       0
  DHCPV6_RELAY_REPL        0
```

show firewall (View)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show firewall`
`<filter filter-name>`
`<counter counter-name>`
`<log>`
`<prefix-action-stats>`
`<terse>`

Release Information Command introduced before Junos OS Release 10.0 .

Description Display statistics about configured firewall filters.

Options `none`—Display statistics about configured firewall filters.

`filter filter-name`—Name of a configured filter.

`counter counter-name`—Name of a filter counter.

`log`—Display log entries for firewall filters.

`prefix-action-stats`—Display prefix action statistics for firewall filters.

`terse`—Display firewall filter names only.

Required Privilege Level view

Related Documentation

- [firewall on page 105](#)

List of Sample Output [show firewall on page 598](#)

Output Fields [Table 29 on page 597](#) lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

Table 29: show firewall Output Fields

| Field Name | Field Description |
|---------------|--|
| Filter | <p>Name of a filter that has been configured with the filter statement at the [edit firewall] hierarchy level.</p> <p>When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either -i for an input filter or -o for an output filter.</p> <p>When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either -in for an input filter or -out for an output filter. When a logical system-specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, <code>__ls1/filter1</code>).</p> |

Table 29: show firewall Output Fields (*continued*)

| Field Name | Field Description |
|-----------------|--|
| Counters | <p>Display filter counter information:</p> <ul style="list-style-type: none"> • Name—Name of a filter counter that has been configured with the counter firewall filter action. • Bytes—Number of bytes that match the filter term under which the counter action is specified. • Packets—Number of packets that matched the filter term under which the counter action is specified. |
| Policers | <p>Display policer information:</p> <ul style="list-style-type: none"> • Name—Name of policer. • Bytes—Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer. • Packets—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer. |

Sample Output

show firewall

```

user@host> show firewall
Filter: ef_path
Counters:
Name          Bytes          Packets
def-count     0              0
video-count   0              0
voice-count    0              0

Filter: __default_bpdu_filter__

Filter: deep
Counters:
Name          Bytes          Packets
deep2         302076         5031

Filter: deep-flood
Counters:
Name          Bytes          Packets
deep_flood_def 302136         5032
deep1         0              0
Policers:
Name          Packets
deep-pol-op-first 0

```

show system autorecovery state

| | |
|---------------------------------|---|
| Supported Platforms | SRX300, SRX320, SRX340, SRX345, SRX550M |
| Syntax | show system autorecovery state |
| Release Information | Command introduced in Junos OS Release 11.2. |
| Description | Perform checks and show status of all autorecovered items. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • request system autorecovery state on page 544 • <i>Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Devices</i> |
| List of Sample Output | show system autorecovery state on page 599 |
| Output Fields | Table 30 on page 599 lists the output fields for the show system autorecovery state command. Output fields are listed in the approximate order in which they appear. |

Table 30: show system autorecovery state Output Fields

| Field Name | Field Description |
|----------------------|--|
| File | The name of the file on which autorecovery checks are performed. |
| Slice | The disk partition on which autorecovery checks are performed. |
| Recovery Information | Indicates whether autorecovery information for the file or slice has been saved. |
| Integrity Check | Displays the status of the file's integrity check (passed or failed). |
| Action / Status | Displays the status of the item, or the action required to be taken for that item. |

Sample Output

show system autorecovery state

```
user@host> show system autorecovery state
```

```

Configuration:
File          Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed          None
Licenses:
File          Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed          None
JUNOS282737.lic Not Saved           Not checked     Requires save
BSD Labels:
Slice         Recovery Information  Integrity Check  Action / Status
s1            Saved                Passed          None

```

| | | | |
|----|-------|--------|------|
| s2 | Saved | Passed | None |
| s3 | Saved | Passed | None |
| s4 | Saved | Passed | None |

show system download

| | |
|---------------------------------|--|
| Supported Platforms | EX Series, LN Series, SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | show system download <download-id> |
| Release Information | Command introduced in Junos OS Release 11.2. Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches. |
| Description | Display a brief summary of all the download instances along with their current state and extent of progress. If a download-id is provided, the command displays a detailed report of the particular download instance. |
| Options | <ul style="list-style-type: none"> download-id—(Optional) The ID number of the download instance. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> request system download start on page 551 <i>Understanding Download Manager for SRX Series Devices</i> <i>Understanding Download Manager for EX Series Devices</i> |
| List of Sample Output | show system download on page 601 show system download 1 on page 602 |
| Output Fields | Table 31 on page 601 lists the output fields for the show system download command. Output fields are listed in the approximate order in which they appear. |

Table 31: show system download Output Fields

| Field Name | Field Description |
|------------|--|
| ID | Displays the download identification number. |
| Status | Displays the state of a particular download. |
| Start Time | Displays the start time of a particular download. |
| Progress | Displays the percentage of a download that has been completed. |
| URL | Displays the URL from which the file was downloaded. |

Sample Output

show system download

```

user@host> show system download
Download Status Information:
ID  Status      Start Time      Progress  URL
1   Active      May 4 06:28:36  5%        ftp://ftp-server//tftpboot/1m_file

```

| | | | | |
|---|-----------|----------------|---------|--------------------------------------|
| 2 | Active | May 4 06:29:07 | 3% | ftp://ftp-server//tftpboot/5m_file |
| 3 | Error | May 4 06:29:22 | Unknown | ftp://ftp-server//tftpboot/badfile |
| 4 | Completed | May 4 06:29:40 | 100% | ftp://ftp-server//tftpboot/smallfile |

show system download 1

```
user@host> show system download 1
```

```
Download ID      : 1
Status           : Active
Progress         : 6%
URL              : ftp://ftp-server//tftpboot/1m_file
Local Path       : /var/tmp/1m_file
Maximum Rate     : 1k
Creation Time    : May 4 06:28:36
Scheduled Time   : May 4 06:28:36
Start Time       : May 4 06:28:37
Error Count      : 0
```

show system license (View)

Supported Platforms [SRX Series, vSRX](#)

Syntax `show system license`
`<installed | keys | status | usage>`

Release Information Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.

Description Display licenses and information about how licenses are used.

Options **none**—Display all license information.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

status—(Optional) Display license status for a specified logical system or for all logical systems.

usage—(Optional) Display the state of licensed features.

Required Privilege Level view

Related Documentation

- [Verifying Junos OS License Installation](#)

List of Sample Output [show system license on page 604](#)
[show system license installed on page 604](#)
[show system license keys on page 605](#)
[show system license usage on page 605](#)
[show system license status logical-system all on page 605](#)

Output Fields [Table 32 on page 603](#) lists the output fields for the **show system license** command. Output fields are listed in the approximate order in which they appear.

Table 32: show system license Output Fields

| Field Name | Field Description |
|----------------------|--|
| Feature name | Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present. |
| Licenses used | Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used. |

Table 32: show system license Output Fields (*continued*)

| Field Name | Field Description |
|-------------------------------|--|
| Licenses installed | Information about the installed license key: <ul style="list-style-type: none"> • License identifier—Identifier associated with a license key. • License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key. • Valid for device—Device that can use a license key. • Features—Feature associated with a license. |
| Licenses needed | Number of licenses required for features being used but not yet properly licensed. |
| Expiry | Time remaining in the grace period before a license is required for a feature being used. |
| Logical system license status | Displays whether a license is enabled for a logical system. |

Sample Output

show system license

```
user@host> show system license
```

```
License usage:
```

| Feature name | Licenses used | Licenses installed | Licenses needed | Expiry |
|---|---------------|--------------------|-----------------|------------|
| av_key_kaspersky_engine 01:00:00 IST | 1 | 1 | 0 | 2012-03-30 |
| wf_key_surfcontrol_cpa 01:00:00 IST | 0 | 1 | 0 | 2012-03-30 |
| dynamic-vpn | 0 | 1 | 0 | permanent |
| ax411-wlan-ap | 0 | 2 | 0 | permanent |

```
Licenses installed:
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license installed

```
user@host> show system license installed
```

```
License identifier: JUNOS301998
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
av_key_kaspersky_engine - Kaspersky AV
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

```
License identifier: JUNOS302000
```

```
License version: 2
```

```
Valid for device: AG4909AA0080
```

```
Features:
```

```
wf_key_surfcontrol_cpa - Web Filtering
```

```
date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST
```

show system license keys

```
user@host> show system license keys
```

```
XXXXXXXXXX xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx xxxxxxx
xxxxxxx xxxxxxx xxx
```

show system license usage

```
user@host> show system license usage
```

| Feature name | Licenses used | Licenses installed | Licenses needed | Expiry |
|-------------------------|------------------|-----------------------|--------------------|------------|
| av_key_kaspersky_engine | 1 | 1 | 0 | 2012-03-30 |
| 01:00:00 IST | | | | |
| wf_key_surfcontrol_cpa | 0 | 1 | 0 | 2012-03-30 |
| 01:00:00 IST | | | | |
| dynamic-vpn | 0 | 1 | 0 | permanent |
| ax411-wlan-ap | 0 | 2 | 0 | permanent |

show system license status logical-system all

```
user@host> show system license status logical-system all
Logical system license status:
```

| logical system name | license status |
|---------------------|----------------|
| root-logical-system | enabled |
| LSYS0 | enabled |
| LSYS1 | enabled |
| LSYS2 | enabled |

show system login logout

Supported Platforms [EX Series](#), [M Series](#), [MX Series](#), [PTX Series](#), [SRX Series](#), [T Series](#)

Syntax show system login logout

Release Information Command introduced in Junos OS Release 11.2.

Description Display the usernames locked after unsuccessful login attempts.

Required Privilege Level view and system

Related Documentation

- [lockout-period on page 467](#)
- [clear system login logout on page 527](#)

List of Sample Output [show system login logout on page 606](#)

Output Fields [Table 33 on page 606](#) lists the output fields for the **show system login logout** command. Output fields are listed in the approximate order in which they appear.

Table 33: show system login logout

| Field Name | Field Description | Level of Output |
|---------------|---|-----------------|
| User | Username | All levels |
| Lockout start | Date and time the username was locked | All levels |
| Lockout end | Date and time the username was unlocked | All levels |

Sample Output

show system login logout

```
user@host> show system login logout
```

```
User          Lockout start      Lockout end
root          2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC
```

show system services dhcp client

| | |
|---------------------------------|--|
| Supported Platforms | EX Series, LN Series, SRX Series |
| Syntax | <pre>show system services dhcp client < interface-name > <statistics></pre> |
| Release Information | <p>Command introduced in Junos OS Release 8.5.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | Display information about DHCP clients. |
| Options | <ul style="list-style-type: none"> • none—Display DHCP information for all interfaces. • interface-name—(Optional) Display DHCP information for the specified interface. • statistics—(Optional) Display DHCP client statistics. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none"> • <i>dhcp (Interfaces)</i> • request system services dhcp on page 555 • <i>Administration Guide for Security Devices</i> |
| List of Sample Output | show system services dhcp client on page 608 show system services dhcp client ge-0/0/34.0 on page 609 show system services dhcp client statistics on page 609 |
| Output Fields | Table 34 on page 607 lists the output fields for the show system services dhcp client command. Output fields are listed in the approximate order in which they appear. |

Table 34: show system services dhcp client Output Fields

| Field Name | Field Description |
|------------------------|--|
| Logical Interface Name | Name of the logical interface. |
| Client Status | State of the client binding. |
| Vendor Identifier | Vendor ID. |
| Server Address | IP address of the DHCP server. |
| Address obtained | IP address obtained from the DHCP server. |
| Lease Obtained at | Date and time the lease was obtained. |
| Lease Expires in | (EX Series switches only) Time the current lease expires in (seconds). |

Table 34: show system services dhcp client Output Fields (*continued*)

| Field Name | Field Description |
|-------------------|---|
| Lease Expires at | Date and time the lease expires. |
| DHCP Options | <ul style="list-style-type: none"> • Name: server-identifier, Value: IP address of the name server. • Name: device, Value: IP address of the name device. • Name: domain-name, Value: Name of the domain. |
| Packets dropped | Total packets dropped. |
| Messages received | <p>Number of the following DHCP messages received:</p> <ul style="list-style-type: none"> • DHCPOFFER—First packet received on a logical interface when DHCP is enabled. • DHCPACK—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stops the earlier timer added for DHCPACK. • DHCPNAK—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet. |
| Messages sent | <p>Number of the following DHCP messages sent:</p> <ul style="list-style-type: none"> • DHCPDECLINE—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet. • DHCPDISCOVER—Packet sent on the interface for which the DHCP client is enabled. • DHCPREQUEST—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer. • DHCPINFORM—Packet sent to the DHCP server for local configuration parameters. • DHCPRELEASE—Packet sent to the DHCP server to relinquish network address and cancel remaining lease. • DHCPRENEW—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server. • DHCPREBIND—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast. |

Sample Output

show system services dhcp client

```

user@host> show system services dhcp client
Logical Interface name      ge-0/0/34.0
Hardware address           00:1f:12:38:5f:e5
Client status               bound
Address obtained            10.0.0.2
Update server               disabled
Lease obtained at           2013-12-23 08:11:40 UTC
Lease expires in            93
Lease expires at            2013-12-23 08:13:20 UTC

DHCP options:
  Name: server-identifier, Value: 10.0.0.1
  Code: 1, Type: ip-address, Value: 255.255.255.0

```

Sample Output

show system services dhcp client ge-0/0/34.0

```

user@host> show system services dhcp client ge-0/0/34.0
Logical Interface name      ge-0/0/34.0
Hardware address           00:1f:12:38:5f:e5
Client status              bound
Address obtained           10.0.0.2
Update server              disabled
Lease obtained at          2013-12-23 08:11:40 UTC
Lease expires in           87
Lease expires at           2013-12-23 08:13:20 UTC

DHCP options:
Name: server-identifier, Value: 10.0.0.1
Code: 1, Type: ip-address, Value: 255.255.255.0

```

Sample Output

show system services dhcp client statistics

```

user@host> show system services dhcp client statistics
Packets dropped:
  Total                0
Messages received:
  DHCPPOFFER           0
  DHCPACK              8
  DHCPNAK              0
Messages sent:
  DHCPDECLINE          0
  DHCPDISCOVER         0
  DHCPREQUEST          1
  DHCPINFORM           0
  DHCPRELEASE          0
  DHCPRENEW            7
  DHCPREBIND           0

```

show system services dhcp relay-statistics

Supported Platforms [SRX Series, vSRX](#)

Syntax `show system services dhcp relay-statistics`

Release Information Command introduced in Junos OS Release 8.5 .

Description Display information about the DHCP relay.

Required Privilege Level view and system

Related Documentation

- [dhcp](#)

List of Sample Output [show system services dhcp relay-statistics on page 610](#)

Output Fields [Table 35 on page 610](#) lists the output fields for the `show system services dhcp relay-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 35: show system services dhcp relay-statistics Output Fields

| Field Name | Field Description |
|-------------------|--|
| Received packets | Total DHCP packets received. |
| Forwarded packets | Total DHCP packet forwarded. |
| Dropped packets | <p>Total DHCP packets dropped for the following reasons:</p> <ul style="list-style-type: none"> • Due to a missing interface in the relay database—Number of packets discarded because they did not belong to a configured interface. • Due to a missing matching routing instance—Number of packets discarded because they did not belong to a configured routing instance. • Due to an error during packet read—Number of packets discarded because of a system read error. • Due to an error during packet send—Number of packets that the DHCP relay application could not send. • Due to an invalid server address—Number of packets discarded because an invalid server address was specified. • Due to a missing valid local address—Number of packets discarded because there was no valid local address. • Due to a missing route to the server or client—Number of packets discarded because there were no addresses available for assignment. |

Sample Output

show system services dhcp relay-statistics

```
user@host> show system services dhcp relay-statistics
```

```
Received packets: 4
Forwarded packets: 4
Dropped packets: 4
  Due to missing interface in relay database: 4
  Due to missing matching routing instance: 0
  Due to an error during packet read: 0
  Due to an error during packet send: 0
  Due to invalid server address: 0
  Due to missing valid local address: 0
  Due to missing route to server/client: 0
```

show system snapshot media

Supported Platforms [SRX Series, vSRX](#)

Syntax `show system snapshot media media-type`

Release Information Command introduced in Junos OS Release 10.2 .

Description Display the snapshot information for both root partitions on SRX Series devices

- Options**
- `internal`— Show snapshot information from internal media.
 - `usb`— Show snapshot information from device connected to USB port.
 - `external`— Show snapshot information from the external CompactFlash card.

Required Privilege Level View

Related Documentation

- [Example: Creating a Snapshot and Using It to Boot an SRX Series Device](#)

List of Sample Output [show system snapshot media internal on page 612](#)
[show system snapshot media usb on page 612](#)

Sample Output

show system snapshot media internal

```
show system snapshot media internal
Information for snapshot on      internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
  junos : 10.1B3-domestic
Information for snapshot on      internal (/dev/da0s2a) (backup)
Creation date: Jan 15 10:15:32 2010
JUNOS version on snapshot:
  junos : 10.2-20100112.0-domestic
```

show system snapshot media usb

```
show system snapshot media usb
Information for snapshot on      usb (/dev/da1s1a) (primary)
Creation date: Jul 24 16:16:01 2009
JUNOS version on snapshot:
  junos : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/da1s2a) (backup)
Creation date: Jul 24 16:17:13 2009
JUNOS version on snapshot:
  junos : 10.0I20090724_0719-domestic
```

show system storage partitions (View SRX Series)

| | |
|---------------------------------|---|
| Supported Platforms | SRX300, SRX320, SRX340, SRX345, SRX550M, vSRX |
| Syntax | show system storage partitions |
| Release Information | Command introduced in Junos OS Release 10.2. |
| Description | Display the partitioning scheme details on SRX Series devices. |
| Required Privilege Level | View |
| Related Documentation | <ul style="list-style-type: none"> • <i>Example: Installing Junos OS on SRX Series Devices Using the Partition Option</i> |
| List of Sample Output | show system storage partitions (single root partitioning) on page 613 show system storage partitions (USB) on page 613 |

show system storage partitions (dual root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)
```

```
Partitions Information:
Partition  Size  Mountpoint
s1a       293M  altroot
s2a       293M  /
s3e       24M   /config
s3f       342M  /var
s4a       30M   recovery
```

show system storage partitions (single root partitioning)

```
show system storage partitions
Boot Media: internal (da0)
Partitions Information:
Partition  Size  Mountpoint
s1a       898M  /
s1e       24M   /config
s1f       61M   /var
```

show system storage partitions (USB)

```
show system storage partitions
Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)
```

```
Partitions Information:
Partition  Size  Mountpoint
s1a       293M  /
s2a       293M  altroot
s3e       24M   /config
```

| | | |
|-----|------|----------|
| s3f | 342M | /var |
| s4a | 30M | recovery |