



Junos[®] OS

User Access and Authentication Feature Guide for Routing Devices

Release

14.1



Modified: 2016-06-10

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 User Access and Authentication Feature Guide for Routing Devices

14.1

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

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

| | | |
|------------------|--|-----------|
| | About the Documentation | 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 |
| Chapter 1 | User Access and Authentication Overview | 23 |
| | Junos OS Login Classes Overview | 23 |
| | Junos OS User Accounts Overview | 24 |
| | Understanding Junos OS Access Privilege Levels | 26 |
| | Junos OS Login Class Permission Flags | 26 |
| | Allowing or Denying Individual Commands for Junos OS Login Classes | 29 |
| | Junos OS User Authentication Methods | 30 |
| | Understanding Remote Authentication Servers | 31 |
| | Junos OS Authentication Order for RADIUS, TACACS+, and Password | |
| | Authentication | 32 |
| | Using RADIUS or TACACS+ Authentication | 32 |
| | Using Local Password Authentication | 33 |
| | Order of Authentication Attempts | 33 |
| | Junos OS Authentication Methods for Routing Protocols | 36 |
| Chapter 2 | Configuring Junos OS Login Classes | 39 |
| | Defining Junos OS Login Classes | 39 |
| | Example: Creating Login Classes with Specific Privileges | 40 |
| | Configuring the Timeout Value for Idle Login Sessions | 40 |
| | Using Junos OS to Configure Logical System Administrators | 41 |
| | Configuring the Junos OS to Display a System Login Message | 42 |
| | Configuring the Junos OS to Display a System Login Announcement | 43 |
| | Examples: Configuring Time-Based User Access | 45 |
| | Configuring System Alarms to Appear Automatically Upon Login | 46 |
| | System Alarms on J Series Routers | 46 |

| | | |
|------------------|--|-----------|
| Chapter 3 | Configuring Junos OS User Accounts | 47 |
| | Junos-FIPS Crypto Officer and User Accounts Overview | 47 |
| | Crypto Officer User Configuration | 47 |
| | FIPS User Configuration | 48 |
| | Configuring Time-Based User Access | 48 |
| | Examples: Configuring Time-Based User Access | 49 |
| | Configuring Local User Template Accounts for User Authentication | 50 |
| | Configuring Remote Template Accounts for User Authentication | 52 |
| | Example: Configuring User Login Accounts | 52 |
| | Configuring Junos OS User Accounts | 53 |
| | Example: Configuring User Accounts | 56 |
| | Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 57 |
| | Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions | 58 |
| | Configuring Login Tips | 58 |
| | Handling Authorization Failure | 59 |
| | Example: Configuring System Retry Options | 59 |
| Chapter 4 | Configuring User Access Privileges | 63 |
| | Configuring Access Privilege Levels | 63 |
| | Example: Configuring Access Privilege Levels | 64 |
| | Specifying Access Privileges for Junos OS Operational Mode Commands | 64 |
| | Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands | 66 |
| | Example: Configuring Access Privileges for Operational Mode Commands | 67 |
| | Specifying Access Privileges for Junos OS Configuration Mode Hierarchies | 67 |
| | Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies | 68 |
| | Defining Access Privileges Using allow or deny configuration Statements | 69 |
| | Specifying Access Privileges Using allow/deny-configuration Statements | 70 |
| | Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements | 72 |
| Chapter 5 | Permission Flags for User Access Privileges | 77 |
| | Access Privilege User Permission Flags Overview | 78 |
| | access | 80 |
| | access-control | 81 |
| | admin | 81 |
| | admin-control | 82 |
| | all-control | 83 |
| | clear | 83 |
| | configure | 121 |
| | control | 122 |
| | field | 122 |
| | firewall | 123 |
| | firewall-control | 123 |
| | floppy | 124 |
| | flow-tap | 125 |
| | flow-tap-control | 125 |

| | | |
|------------------|---|------------|
| | flow-tap-operation | 125 |
| | idp-profiler-operation | 126 |
| | interface | 126 |
| | interface-control | 127 |
| | maintenance | 128 |
| | network | 135 |
| | pgcp-session-mirroring | 137 |
| | pgcp-session-mirroring-control | 137 |
| | reset | 138 |
| | rollback | 138 |
| | routing | 139 |
| | routing-control | 143 |
| | secret | 147 |
| | secret-control | 148 |
| | security | 150 |
| | security-control | 153 |
| | shell | 157 |
| | snmp | 157 |
| | snmp-control | 158 |
| | system | 158 |
| | system-control | 161 |
| | trace | 162 |
| | trace-control | 168 |
| | view | 173 |
| | view-configuration | 243 |
| Chapter 6 | Configuring Passwords for User Access | 245 |
| | Configuring the Root Password | 245 |
| | Example: Configuring the Root Password | 247 |
| | Example: Configuring a Plain-Text Password for Root Logins | 247 |
| | Example: Configuring SSH Authentication for Root Logins | 249 |
| | Recovering the Root Password | 250 |
| | Changing the Requirements for Junos OS Plain-Text Passwords | 252 |
| | Example: Changing the Requirements for Junos OS Plain-Text Passwords | 252 |
| | Configuring MS-CHAPv2 for Password-Change Support | 254 |
| Chapter 7 | Configuring Local Password Authentication | 257 |
| | Special Requirements for Junos OS Plain-Text Passwords | 257 |
| | Changing the Requirements for Junos OS Plain-Text Passwords | 259 |
| | Example: Changing the Requirements for Junos OS Plain-Text Passwords | 260 |
| | Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication | 262 |
| | Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication | 263 |

| | | |
|-------------------|---|------------|
| Chapter 8 | Configuring Radius Authentication | 267 |
| | Configuring RADIUS Authentication | 267 |
| | Configuring Authentication by a RADIUS Server | 267 |
| | Example: Configuring RADIUS Authentication | 272 |
| | Example: Configuring RADIUS Template Accounts | 273 |
| | Juniper Networks Vendor-Specific RADIUS Attributes | 274 |
| | Configuring RADIUS System Accounting | 276 |
| | Configuring Auditing of User Events on a RADIUS Server | 276 |
| | Specifying RADIUS Server Accounting and Auditing Events | 277 |
| | Configuring RADIUS Server Accounting | 277 |
| | Example: Configuring RADIUS System Accounting | 278 |
| | Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny | |
| | Access to Commands | 279 |
| | Overview of Template Accounts for RADIUS and TACACS+ Authentication | 280 |
| | Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local | |
| | Password Authentication | 281 |
| | Example: Configuring System Authentication for RADIUS, TACACS+, and | |
| | Password Authentication | 282 |
| Chapter 9 | Configuring TACACS+ Authentication | 285 |
| | Configuring TACACS+ Authentication | 285 |
| | Configuring Authentication by a TACACS+ Server | 285 |
| | Configuring the Same Authentication Service for Multiple TACACS+ | |
| | Servers | 291 |
| | Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny | |
| | Access to Commands | 291 |
| | Juniper Networks Vendor-Specific TACACS+ Attributes | 293 |
| | Configuring TACACS+ System Accounting | 295 |
| | Specifying TACACS+ Auditing and Accounting Events | 295 |
| | Configuring TACACS+ Server Accounting | 295 |
| | Configuring TACACS+ Accounting on a TX Matrix Router | 297 |
| | Overview of Template Accounts for RADIUS and TACACS+ Authentication | 297 |
| | Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local | |
| | Password Authentication | 297 |
| | Example: Configuring System Authentication for RADIUS, TACACS+, and | |
| | Password Authentication | 299 |
| Chapter 10 | Configuring DHCP Access Service for IP Address Management | 301 |
| | DHCP Access Service Overview | 302 |
| | Network Address Assignments (Allocating a New Address) | 303 |
| | Network Address Assignments (Reusing a Previously Assigned Address) | 304 |
| | Static and Dynamic Bindings | 305 |
| | Compatibility with Autoinstallation | 305 |
| | Conflict Detection and Resolution | 305 |
| | DHCP Statement Hierarchy and Inheritance | 305 |
| | Configuring Address Pools for DHCP Dynamic Bindings | 307 |
| | Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a | |
| | Client MAC Address | 308 |
| | Specifying DHCP Lease Times for IP Address Assignments | 310 |

| | |
|---|-----|
| Configuring a DHCP Boot File and DHCP Boot Server | 310 |
| Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication | 311 |
| Configuring a Static IP Address as DHCP Server Identifier | 312 |
| Configuring a Domain Name and Domain Search List for a DHCP Server Host . . | 312 |
| Configuring Routers Available to the DHCP Client | 313 |
| Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server | 314 |
| Example: Complete DHCP Server Configuration | 315 |
| Example: Viewing DHCP Bindings | 316 |
| Example: Viewing DHCP Address Pools | 317 |
| Example: Viewing and Clearing DHCP Conflicts | 317 |
| Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers | 317 |
| Configuring Tracing Operations for DHCP Processes | 318 |
| Configuring the DHCP Processes Log Filename | 319 |
| Configuring the Number and Size of DHCP Processes Log Files | 319 |
| Configuring Access to the DHCP Log File | 320 |
| Configuring a Regular Expression for Refining the Output of DHCP Logged Events | 320 |
| Configuring DHCP Trace Operation Events | 320 |
| DHCP Processes Tracing Flags | 321 |
| Configuring the Router as an Extended DHCP Local Server | 322 |
| Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 324 |
| Extended DHCP Local Server and Address-Assignment Pools | 324 |
| Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use | 325 |
| Matching the Client IP Address to the Address-Assignment Pool | 325 |
| Matching Option 82 Information to Named Address Ranges | 325 |
| Default Options Provided by the Extended DHCP Server for the DHCP Client . . | 326 |
| Using External AAA Authentication Services to Authenticate DHCP Clients . . | 326 |
| Configuring Authentication Support for an Extended DHCP Application . . . | 327 |
| Grouping Interfaces with Common DHCP Configurations | 328 |
| Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service | 329 |
| Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service | 329 |
| Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | 331 |
| Example: Configuring the Minimum Extended DHCP Local Server Configuration | 332 |
| Example: Extended DHCP Local Server Configuration with Optional Pool Matching | 332 |
| Verifying and Managing the DHCP Server Configuration | 332 |

| | | |
|-------------------|--|------------|
| | Tracing Extended DHCP Local Server Operations | 333 |
| | Configuring the Filename of the Extended DHCP Local Server Processes | |
| | Log | 334 |
| | Configuring the Number and Size of Extended DHCP Local Server Processes | |
| | Log Files | 334 |
| | Configuring Access to the Log File | 334 |
| | Configuring a Regular Expression for Lines to Be Logged | 334 |
| | Configuring Trace Option Flags | 335 |
| Chapter 11 | Configuring Remote Access to a Router or Switch | 337 |
| | System Services for Remote Access Overview | 337 |
| | Configuring Telnet Service for Remote Access to a Router or Switch | 338 |
| | Configuring FTP Service for Remote Access to the Router or Switch | 339 |
| | Configuring Finger Service for Remote Access to the Router | 339 |
| | Configuring SSH Service for Remote Access to the Router or Switch | 340 |
| | Configuring the Root Login Through SSH | 341 |
| | Configuring the SSH Protocol Version | 341 |
| | Configuring the Client Alive Mechanism | 342 |
| | Configuring Outbound SSH Service | 342 |
| | Configuring the Device Identifier for Outbound SSH Connections | 343 |
| | Sending the Public SSH Host Key to the Outbound SSH Client | 344 |
| | Configuring Keepalive Messages for Outbound SSH Connections | 345 |
| | Configuring a New Outbound SSH Connection | 345 |
| | Configuring the Outbound SSH Client to Accept NETCONF as an Available | |
| | Service | 346 |
| | Configuring Outbound SSH Clients | 346 |
| | Configuring DTCP-over-SSH Service for the Flow-Tap Application | 346 |
| | Configuring NETCONF-Over-SSH Connections on a Specified TCP Port | 348 |
| | Configuring clear-text or SSL Service for Junos XML Protocol Client | |
| | Applications | 348 |
| | Configuring clear-text Service for Junos XML Protocol Client | |
| | Applications | 348 |
| | Configuring SSL Service for Junos XML Protocol Client Applications | 349 |
| | Configuring the Junos OS to Work with SRC Software | 350 |
| Chapter 12 | Configuring Authentication for Routing Protocols | 351 |
| | Example: Configuring the BGP and IS-IS Routing Protocols | 351 |
| | Configuring BGP | 351 |
| | Configuring IS-IS | 352 |
| | Configuring the Authentication Key Update Mechanism for BGP and LDP Routing | |
| | Protocols | 353 |
| | Configuring Authentication Key Updates | 353 |
| | Configuring BGP and LDP for Authentication Key Updates | 354 |
| Chapter 13 | Configuration Statements | 355 |
| | System Management Configuration Statements | 358 |
| | accounting | 366 |
| | access-end | 367 |
| | access-start | 367 |
| | accounting-port (RADIUS Server) | 368 |

| | |
|---|-----|
| allow-commands | 368 |
| allow-configuration | 369 |
| allow-configuration-regexps | 370 |
| allowed-days | 370 |
| authentication (DHCP Local Server) | 371 |
| authentication (Login) | 372 |
| authentication-order | 373 |
| backoff-factor | 374 |
| backoff-threshold | 374 |
| boot-file | 375 |
| boot-server (DHCP) | 376 |
| change-type | 377 |
| ciphers | 378 |
| circuit-type | 379 |
| class (Assigning a Class to an Individual User) | 380 |
| class (Defining Login Classes) | 381 |
| client-alive-count-max | 382 |
| client-alive-interval | 382 |
| client-identifier | 383 |
| connection-limit | 384 |
| default-lease-time | 385 |
| delimiter (DHCP Local Server) | 386 |
| deny-commands | 387 |
| deny-configuration | 388 |
| deny-configuration-regexps | 389 |
| destination (Accounting) | 390 |
| dhcp | 391 |
| dhcpv6 (DHCP Local Server) | 393 |
| dhcp-local-server | 396 |
| domain-name (DHCP) | 401 |
| domain-name (DHCP Local Server) | 402 |
| dynamic-profile-options | 403 |
| enhanced-accounting | 403 |
| enhanced-avs-max | 404 |
| finger | 404 |
| flow-tap-dtcp | 405 |
| format | 406 |
| ftp | 407 |
| full-name | 407 |
| group (DHCP Local Server) | 408 |
| http | 410 |
| https | 411 |
| hostkey-algorithm | 412 |
| idle-timeout (System-Login) | 413 |
| interface (DHCP Local Server) | 414 |
| ip-address-first | 415 |
| key-exchange | 416 |
| load-key-file | 417 |
| local-certificate | 418 |

| | |
|--|-----|
| lockout-period | 419 |
| logical-system-name (DHCP Local Server) | 420 |
| login | 421 |
| login-alarms | 422 |
| login-script (Login) | 422 |
| mac-address (DHCP Local Server) | 423 |
| macs | 424 |
| maximum-lease-time (DHCP) | 425 |
| maximum-length | 426 |
| max-sessions-per-connection | 426 |
| maximum-time | 427 |
| minimum-changes | 428 |
| minimum-length | 429 |
| minimum-lower-cases | 430 |
| minimum-numeric | 431 |
| minimum-punctuations | 432 |
| minimum-time | 433 |
| minimum-upper-cases | 434 |
| next-server | 435 |
| no-passwords | 435 |
| no-tcp-forwarding | 436 |
| option (DHCP server) | 437 |
| option-60 (DHCP Local Server) | 438 |
| option-82 (DHCP Local Server Authentication) | 439 |
| option-82 (DHCP Local Server Pool Matching) | 440 |
| outbound-ssh | 441 |
| password (DHCP Local Server) | 444 |
| password (Login) | 445 |
| permissions | 446 |
| pool (System) | 447 |
| pool-match-order | 448 |
| port (HTTP/HTTPS) | 449 |
| port (NETCONF Server) | 450 |
| port (RADIUS Server) | 451 |
| port (SRC Server) | 451 |
| port (TACACS+ Server) | 452 |
| protocol-version | 452 |
| radius (System) | 453 |
| radius-options (edit system) | 454 |
| radius-server (System) | 455 |
| rate-limit | 456 |
| retry (RADIUS) | 457 |
| retry-options | 458 |
| root-login | 459 |
| router | 460 |
| routing-instance-name (DHCP Local Server) | 461 |
| secret | 462 |
| server (RADIUS Accounting) | 463 |
| server (TACACS+ Accounting) | 463 |

| | |
|--|------------|
| servers | 464 |
| server-identifier | 465 |
| service-deployment | 466 |
| services (System Services) | 467 |
| session (Time-out) | 469 |
| single-connection | 470 |
| source-address (NTP, RADIUS, System Logging, or TACACS+) | 471 |
| source-address (SRC Software) | 472 |
| source-port (Port Addresses) | 472 |
| ssh | 473 |
| ssl-renegotiation | 474 |
| static-binding | 475 |
| system | 476 |
| tacplus | 476 |
| tacplus-options | 477 |
| tacplus-server | 478 |
| telnet | 478 |
| timeout (System) | 479 |
| traceoptions (Address-Assignment Pool) | 480 |
| traceoptions (DHCP) | 482 |
| traceoptions (DHCP Server) | 485 |
| traceoptions (SBC Configuration Process) | 488 |
| tries-before-disconnect | 490 |
| uid | 490 |
| user (Access) | 491 |
| username-include (DHCP Local Server) | 492 |
| user-prefix (DHCP Local Server) | 493 |
| versioning | 494 |
| web-management | 495 |
| wins-server (System) | 496 |
| xnm-clear-text | 497 |
| xnm-ssl | 497 |
| Chapter 14 | |
| Operational Commands | 499 |
| show cli authorization | 500 |
| clear system services dhcp binding | 502 |
| clear system services dhcp conflict | 503 |
| clear system services dhcp statistics | 504 |
| show system services dhcp binding | 505 |
| show system services dhcp conflict | 508 |
| show system services dhcp global | 509 |
| show system services dhcp pool | 511 |
| show system services dhcp statistics | 513 |
| show system services service-deployment | 516 |
| show system users | 517 |
| ssh | 522 |
| telnet | 524 |
| test access profile | 526 |
| test access radius-server | 530 |

Chapter 15 Index 533
 Index 535

List of Figures

| | | |
|-------------------|--|------------|
| Chapter 10 | Configuring DHCP Access Service for IP Address Management | 301 |
| | Figure 1: DHCP Discover | 303 |
| | Figure 2: DHCP Offer | 303 |
| | Figure 3: DHCP Request | 304 |
| | Figure 4: DHCP ACK | 304 |
| | Figure 5: DHCP Release | 304 |

List of Tables

| | | |
|-------------------|--|-------------|
| | About the Documentation | xvii |
| | Table 1: Notice Icons | xix |
| | Table 2: Text and Syntax Conventions | xx |
| Chapter 1 | User Access and Authentication Overview | 23 |
| | Table 3: Predefined System Login Classes | 23 |
| | Table 4: Login Class Permission Flags | 27 |
| | Table 5: Order of Authentication Attempts | 33 |
| Chapter 2 | Configuring Junos OS Login Classes | 39 |
| | Table 6: System Alarms on J Series Routers | 46 |
| Chapter 4 | Configuring User Access Privileges | 63 |
| | Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode Commands | 66 |
| | Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators | 68 |
| Chapter 7 | Configuring Local Password Authentication | 257 |
| | Table 9: Special Requirements for Plain-Text Passwords | 257 |
| Chapter 8 | Configuring Radius Authentication | 267 |
| | Table 10: Juniper Networks Vendor-Specific RADIUS Attributes | 274 |
| Chapter 9 | Configuring TACACS+ Authentication | 285 |
| | Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes | 293 |
| Chapter 10 | Configuring DHCP Access Service for IP Address Management | 301 |
| | Table 12: Pool and Binding Statements | 306 |
| | Table 13: Common Configuration Statements | 307 |
| | Table 14: DHCP Processes Tracing Flags | 321 |
| Chapter 14 | Operational Commands | 499 |
| | Table 15: show system services dhcp binding Output Fields | 505 |
| | Table 16: show system services dhcp conflict Output Fields | 508 |
| | Table 17: show system services dhcp global Output Fields | 509 |
| | Table 18: show system services dhcp pool Output Fields | 511 |
| | Table 19: show system services dhcp statistics Output Fields | 513 |
| | Table 20: show system services service-deployment Output Fields | 516 |
| | Table 21: show system users Output Fields | 519 |
| | Table 22: test access profile Output Fields | 526 |
| | Table 23: test access radius-server Output Fields | 530 |

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:

- [M Series](#)
- [MX Series](#)
- [T Series](#)
- [J Series](#)
- [PTX Series](#)

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming

configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
  scripts {
    commit {
      file ex-script.xsl;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page 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 xx defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

GUI Conventions

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

User Access and Authentication Overview

- [Junos OS Login Classes Overview on page 23](#)
- [Junos OS User Accounts Overview on page 24](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Junos OS User Authentication Methods on page 30](#)
- [Understanding Remote Authentication Servers on page 31](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)
- [Junos OS Authentication Methods for Routing Protocols on page 36](#)

Junos OS Login Classes Overview

All users who can log in to the router or switch must be in a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the router or switch
- 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 out

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

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in [Table 3 on page 23](#). The predefined login classes cannot be modified.

Table 3: Predefined System Login Classes

| Login Class | Permission Flag Set |
|--------------------------------|--|
| operator | clear, network, reset, trace, and view |
| read-only | view |
| superuser or super-user | 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

**Related
Documentation**

- [Defining Junos OS Login Classes on page 39](#)
- [Defining Junos OS Login Classes](#)
- [Understanding QFabric System Login Classes](#)

Junos OS User Accounts Overview

User accounts provide one way for users to access the router. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers, as described in [“Junos OS User Authentication Methods” on page 30](#).) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the router. Do not include spaces, colons, or commas in the username. The username can be up to 64 characters long.
- User's full name—(Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
- User identifier (UID)—(Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the router. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- User's access privilege—(Required) One of the login classes you defined in the **class** statement at the **[edit system login]** hierarchy level, or one of the default classes listed in [“Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies” on page 68](#).

- Authentication method or methods and passwords that the user can use to access the router—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that the Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user's password. If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

```
[edit system login user username]
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long.
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Valid passwords must contain at least one change of case or character class.

Junos-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

For SSH authentication, you can copy the contents of an SSH key file into the configuration or directly configure SSH key information. Use the **load-key-file** *URL filename* command to load an SSH key file that was previously generated, e.g. by using **ssh-keygen**. The *URL filename* is the path to the file's location and name. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you enter the **load-key-file** statement. Optionally, you can use the **ssh-dsa public key <from hostname>** and the **ssh-rsa public key <from hostname>** statements to directly configure SSH keys.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them.

To view the SSH keys entries, use the configuration mode **show** command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host::ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
  ssh-rsa "1024 35 9727638204084251055468226757249864241630322
207404962528390382038690141584534964170019610608358722961563
475784918273603361276441874265946893207739108344813125957722
```

```
625461667999278316123500438660915866283822489746732605661192
181489539813862940327687806538169602027491641637359132693963
44008443 boojum@juniper.net"; # SECRET-DATA
}
```

An account for the user **root** is always present in the configuration. You configure the password for **root** using the *root-authentication* statement, as described in [“Configuring the Root Password” on page 245](#).

**Related
Documentation**

- [Configuring Junos OS User Accounts on page 53](#)
- [Junos OS Login Classes Overview on page 23](#)

Understanding Junos OS Access Privilege Levels

Each top-level command-line interface (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 26](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 29](#)

Junos OS Login Class Permission Flags

The **permissions** statement specifies one or more of the permission flags listed in [Table 4 on page 27](#). 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 4 on page 27](#) lists the Junos[®] operating system (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 4: 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. |
| flow-tap-operation | <p>Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must have flow-tap-operation permission to authenticate itself to the Junos OS as an administrative user.</p> <p>NOTE: The flow-tap-operation option is not included in the all-control permissions flag.</p> |
| idp-profiler-operation | Can view profiler data. |

Table 4: Login Class Permission Flags (*continued*)

| Permission Flag | Description |
|---------------------------------------|---|
| 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 and becoming the superuser in the shell by using the su root command, and can halt and reboot the router 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. |
| 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. |

Table 4: Login Class Permission Flags (*continued*)

| Permission Flag | Description |
|---------------------------|---|
| 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 | Can view all of the configuration excluding secrets, system scripts, and event options. NOTE: Only users with the maintenance permission can view commit script, op script, or event script configuration. |

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 issues **rollback** command with **rollback** permission flag enabled.
- 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**, **deny-configuration**, **allow-commands**, **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**.

**Related
Documentation**

- [Configuring Access Privilege Levels on page 63](#)
- [Access Privilege User Permission Flags Overview on page 78](#)

Junos OS User Authentication Methods

The 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 router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

**Related
Documentation**

- [Configuring RADIUS Authentication on page 267](#)
- [Configuring TACACS+ Authentication on page 285](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)
- *Configuring RADIUS Authentication (QFX Series or OCX Series)*
- *Configuring TACACS+ Authentication (QFX Series)*

Understanding Remote Authentication Servers

You probably already use a remote authentication server (or servers) in your network. It is a recommended best practice, because the servers allow you to centrally create a consistent set of user accounts for all devices in your network. There are many good reasons for implementing a authentication, authorization, and accountability (AAA) solution in your network, not the least of which is to make the management of user accounts easier.

There are two basic methods of remote authentication in use by most enterprises today—RADIUS and TACACS+. Junos OS supports both types and can be configured to query multiple remote authentication servers of both types. The idea behind a RADIUS or TACACS+ server is simple, a central authentication server that routers, switches, security devices, and even servers can use to authenticate users as they attempt to gain access to these systems. Think of the advantages that a central user directory brings for authentication auditing and access control in a client server model, and you have your justification for RADIUS or TACACS+ for your networks infrastructure.

Using a central server has multiple advantages over the alternative of creating local users on each device, a time-consuming and error-prone task. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks, in which someone uses a captured password to pose as a system administrator.

- **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+.
- TACACS+—You should use TACACS+ when your priorities are security and flexibility.
- Security—TACACS+ is more secure than RADIUS. Not only is the full session encrypted, but authorization and authentication are done separately to prevent someone from trying to force their way into your network.
- Flexibility—TCP is a more flexible transport protocol than UDP. You can do more with it in more advanced networks. In addition, TACACS+ supports more of the enterprise protocols like NetBios or Appletalk.

Related •
Documentation

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

If the **authentication-order** is remote-server then local, Junos OS will retry the local server if the remote-server is unreachable or has timed out. However, if the remote-server rejects the authentication, Junos OS will not retry the authentication.

If none of the configured authentication methods accept the login credentials and if a reject response is received, the login attempt fails. If no response is received from any configured authentication method, the Junos OS consults local password authentication as a last resort.

Using RADIUS or TACACS+ Authentication

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the **[authentication-order]** statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the **authentication-order** statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the **authentication-order** statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective **[edit system radius-server]** and **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the **[edit system radius-server]** or **[edit system tacplus-server]** hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.

Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the **[edit system login]** hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the **[authentication-order authentication-methods]** statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.
- The password authentication method is not explicitly configured as one of the authentication methods in the **authentication-order authentication-methods** statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

[Table 5 on page 33](#) describes how the **authentication-order** statement at the **[edit system]** hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 5: Order of Authentication Attempts

| Syntax | Order of Authentication Attempts |
|-------------------------------------|---|
| authentication-order radius; | <ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS server is available but authentication is rejected, deny access. 4. If RADIUS servers are not available, try password authentication. <p>NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p> |

Table 5: Order of Authentication Attempts (*continued*)

| Syntax | Order of Authentication Attempts |
|--|---|
| authentication-order [radius password]; | <ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order [radius tacplus]; | <ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ server is available but authentication is rejected, deny access. 6. If both RADIUS and TACACS+ servers are not available, try password authentication. <p>NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p> |
| authentication-order [radius tacplus password]; | <ol style="list-style-type: none"> 1. Try configured RADIUS authentication servers. 2. If RADIUS server is available and authentication is accepted, grant access. 3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers. 4. If TACACS+ server is available and authentication is accepted, grant access. 5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order tacplus; | <ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ server is available but authentication is rejected, deny access. 4. If TACACS+ servers are not available, try password authentication. <p>NOTE: If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p> |

Table 5: Order of Authentication Attempts (*continued*)

| Syntax | Order of Authentication Attempts |
|--|---|
| authentication-order [tacplus password]; | <ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order [tacplus radius]; | <ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS server is available but authentication is rejected, deny access. 6. If both TACACS+ and RADIUS servers are not available, try password authentication. <p>NOTE: If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</p> |
| authentication-order [tacplus radius password]; | <ol style="list-style-type: none"> 1. Try configured TACACS+ authentication servers. 2. If TACACS+ server is available and authentication is accepted, grant access. 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. 4. If RADIUS server is available and authentication is accepted, grant access. 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order password; | <ol style="list-style-type: none"> 1. Try to authenticate the user, using the password configured at the [edit system login] hierarchy level. 2. If the authentication is accepted, grant access. 3. If the authentication is rejected, deny access. |



NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the authentication-order statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups `re0` and `re1`. The authentication order must not be configured at the `[edit system]` hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the authentication-order statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the authentication-order statement.

Related Documentation

- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57](#)
- [*Limiting the Number of User Login Attempts for SSH and Telnet Sessions*](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)

Junos OS Authentication Methods for Routing Protocols

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- Simple authentication (IS-IS, OSPF, and RIP)—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you *not* use this authentication method.

- MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (" ").

Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

**Related
Documentation**

- [Example: Configuring the BGP and IS-IS Routing Protocols on page 351](#)
- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)

CHAPTER 2

Configuring Junos OS Login Classes

- [Defining Junos OS Login Classes on page 39](#)
- [Example: Creating Login Classes with Specific Privileges on page 40](#)
- [Configuring the Timeout Value for Idle Login Sessions on page 40](#)
- [Using Junos OS to Configure Logical System Administrators on page 41](#)
- [Configuring the Junos OS to Display a System Login Message on page 42](#)
- [Configuring the Junos OS to Display a System Login Announcement on page 43](#)
- [Examples: Configuring Time-Based User Access on page 45](#)
- [Configuring System Alarms to Appear Automatically Upon Login on page 46](#)
- [System Alarms on J Series Routers on page 46](#)

Defining Junos OS Login Classes

To define a login class and its access privileges, include the **class** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
class class-name {
  access-end;
  access-start;
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
  expression 2";
  allowed-days;
  configuration-breadcrumbs;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
  expression 2 ";
  idle-timeout minutes;
  login-script filename;
  login-tip;
  permissions [ permissions ];
}
```

Related Documentation

- [Junos OS Login Classes Overview on page 23](#)
- [Junos OS User Accounts Overview on page 24](#)
- [Example: Creating Login Classes with Specific Privileges on page 40](#)

- [Using Junos OS to Configure Logical System Administrators on page 41](#)

Example: Creating Login Classes with Specific Privileges

The following example shows how to create several user classes, each with specific privileges. In this example, you configure timeouts to disconnect the class members after a period of inactivity. Users' privilege levels, and therefore the classes of which they are members, should be dependent on their responsibilities within the organization, and the permissions shown here are only examples.

The first class of users (called "observation") can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users (called "operation") can view and modify the configuration. The third class of users (called "engineering") has unlimited access and control.

```
[edit]
system {
  login {
    class observation {
      idle-timeout 5;
      permissions [ view ];
    }
    class operation {
      idle-timeout 5;
      permissions [ admin clear configure interface interface-control network
        reset routing routing-control snmp snmp-control trace-control
        firewall-control rollback ];
    }
    class engineering {
      idle-timeout 5;
      permissions all;
    }
  }
}
```

Related Documentation • [Defining Junos OS Login Classes on page 39](#)

Configuring the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router or switch, even if that session is idle. To close idle sessions automatically, you must configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

To define the timeout value for idle login sessions, include the **idle-timeout** statement at the **[edit system login class *class-name*]** hierarchy level:

```
[edit system login class class-name]
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.

```
user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed, unless the user is running telnet or monitoring interfaces using the **monitor interface** or **monitor traffic** command.

- Related Documentation**
- [Defining Junos OS Login Classes on page 39](#)
 - [idle-timeout \(System-Login\) on page 413](#)

Using Junos OS to Configure Logical System Administrators

Using Junos OS, you can partition a single router or switch into multiple logical devices that perform independent routing or switching tasks. When creating logical systems, you must configure logical system administrators and interfaces, assign logical interfaces to logical systems, and configure various other logical system statements.

The master administrator can assign one or more logical system administrators to each logical system. Once assigned to a logical system, administrators are restricted to viewing only configurations of the logical system to which they are assigned and accessing only the operational commands that apply to that particular logical system. This restriction means that these administrators cannot access global configuration statements, and all command output is restricted to the logical system to which the administrators are assigned.

To configure logical system administrators, include the **logical-system *logical-system-name*** statement at the **[edit system login class *class-name*]** hierarchy level and apply the class to the user. For example:

```
[edit]
system {
  login {
    class admin1 {
      permissions all;
      logical-system logical-system-LS1;
    }
    class admin2 {
      permissions view; # Gives users assigned to class admin2 the ability to view
                        # but not to change the configuration.
      logical-system logical-system-LS2;
    }
    user user1 {
      class admin1;
    }
  }
}
```

```
user user2 {  
    class admin2;  
}  
}
```

Fully implementing logical systems requires that you also configure any protocols, routing statements, switching statements, and policy statements for the logical system.

- Related Documentation**
- [Defining Junos OS Login Classes on page 39](#)
 - *Defining Junos OS Login Classes*

Configuring the Junos OS to Display a System Login Message

You can create login banners for those who post messages and announcements to those who access the device. You might want to configure an initial login message now, before you create any user accounts.

A login message displays a banner to users when they access the device, before they log in. To display a message only after the user logs in, use a system login announcement instead of a system login message.

You can format the login message using the following special characters:

- `\n`—New line
- `\t`—Horizontal tab
- `\'`—Single quotation mark
- `\"`—Double quotation mark
- `\\`—Backslash

If the message text contains any spaces, enclose it in quotation marks.

To configure a login banner:

1. Include the **message** statement in the **[edit system login]** configuration.

```
[edit system login]  
message text;
```

For example:

```
system {  
    login {  
        message "\n\n\n\tUNAUTHORIZED USE OF THIS SYSTEM\n\tIS STRICTLY PROHIBITED!\n\n\tPlease contact  
\t'company-noc@company.com'\n\tto gain authorization  
to this equipment if you need access.\n\n\n";  
    }  
}
```

2. Commit the configuration.

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

3. Connect to the device in a new session to verify the presence of the new banner.

The preceding login message configuration example produces a login message similar to the following:

```
server% telnet router1
Trying 1.1.1.1...
Connected to router1.
Escape character is '^['.
```

```
UNAUTHORIZED USE OF THIS SYSTEM
IS STRICTLY PROHIBITED!
```

```
Please contact 'company-noc@company.com' to gain
authorization to this equipment if you need access.
```

```
router1 (tty0)
```

```
Login:
```



NOTE: On some platforms, when you log in from the console, the login banner message is not seen unless you press Ctrl-D at the login prompt.

Related Documentation

- [Configuring the Junos OS to Display a System Login Announcement on page 43](#)
- [Defining Junos OS Login Classes on page 39](#)
- [Configuring the Junos OS to Display a System Login Announcement on page 43](#)

Configuring the Junos OS to Display a System Login Announcement

Sometimes you want to make announcements only to authorized users after they have logged in. For example, you might want to announce an upcoming maintenance event.

You can format the announcement using the following special characters:

- \n—New line
- \t—Horizontal tab
- \'—Single quotation mark
- \"—Double quotation mark
- \\—Backslash

If the message text contains any spaces, enclose it in quotation marks.

By default, no login announcement is displayed.

To configure an announcement that can be seen only by authorized users:

1. Include the **announcement** statement in the **[edit system login]** configuration.

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

For example:

```
system {
  login {
    announcement "\tJuly 27th 1:00 AM to 8:00\n\nPlanned Network
    Maintenance\n\nAFFECTED LOCATIONS: Sunnyvale\n\nPLANNED ACTIVITY:
    Upgrade all 6200 switch firmware to the Enterprise TAC recommended firmware
    version\n\nPURPOSE: This activity will help to minimize the impact of unplanned
    power outages as well as address known issues within our currently installed
    firmware version(s)\n\nWHAT TO EXPECT: During the maintenance window for
    your site, the office network will not be available.\n\n";
    message "\n\n\tTPO - M7i - iX Router Lab\n\n\tUNAUTHORIZED USE OF THIS
    ROUTER\n\tIS STRICTLY PROHIBITED!\n\n\tPlease contact
    \\'astatti@juniper.net\' to gain\n\taccess to this equipment if you need
    authorization.\n\n\n"
  }
}
```

2. Commit the configuration.

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

3. Connect to the device in a new session to verify the presence of the new banner.

The preceding login message configuration example produces a login message similar to the following:

```
server% telnet host
Trying 203.0.113.0
Connected to host.example.net
Escape character is '^['.
```

```

TPO - M7i - iX Router Lab
```

```

UNAUTHORIZED USE OF THIS ROUTER
IS STRICTLY PROHIBITED!
```

```

Please contact 'astatti@juniper.net' to gain
access to this equipment if you need authorization
```

```

login: user
Password:
```

```

      July 27th 1:00 AM to 8:00
```

```

Planned Network Maintenance
```

```

AFFECTED LOCATIONS: Sunnyvale
```

PLANNED ACTIVITY: Upgrade all 6200 switch firmware to the Enterprise TAC recommended firmware version

PURPOSE: This activity will help to minimize the impact of unplanned power outages as well as address known issues within our currently installed firmware version(s)

WHAT TO EXPECT: During the maintenance window for your site, the office network will not be available.

Related Documentation

- [Configuring the Junos OS to Display a System Login Message on page 42](#)

Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the **operator-round-the-clock-access** login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
  class operator-round-the-clock-access {
    allowed-days [ monday tuesday wednesday thursday friday ];
  }
}
```

The following example shows how to configure user access for the **operator-day-shift** login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 0830;
    access-end 1630;
  }
}
```

Alternatively, you can also specify the login start time and end time for the **operator-day-shift** login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 08:30am;
    access-end 04:30pm;
  }
}
```

The following example shows how to configure user access for the **operator-day-shift-all-days-of-the-week** login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]
login {
```

```

class operator-day-shift-all-days-of-the-week {
  access-start 0830;
  access-end 1630;
}

```

Related Documentation

- [Configuring Time-Based User Access on page 48](#)

Configuring System Alarms to Appear Automatically Upon Login

You can configure Juniper Networks routers and switches to run the **show system alarms** command whenever a user with the login class **admin** logs in to the router or switch. To do so, include the **login-alarms** statement at the **[edit system login class admin]** hierarchy level.

```

[edit system login class admin]
login-alarms;

```

For more information on the **show system alarms** command, see the [CLI Explorer](#).

Related Documentation

- [System Alarms on J Series Routers on page 46](#)
- *show system alarms*

System Alarms on J Series Routers

[Table 6 on page 46](#) describes system alarms that may occur on J Series routers. These alarms are preset and cannot be modified.

Table 6: System Alarms on J Series Routers

| Alarm Type | Alarm Summary | Remedy |
|---------------|---|----------------------------------|
| Configuration | This alarm appears if you have not created a rescue configuration for the router. If you inadvertently commit a configuration that denies management access to the router, you must either connect a console to the router or invoke a rescue configuration. Using a rescue configuration is the recommended method. A rescue configuration is one that you know enables management access to the router. | Create the rescue configuration. |
| License | This alarm appears if you have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed. | Install a valid license key. |

Related Documentation

- [Configuring System Alarms to Appear Automatically Upon Login on page 46](#)

CHAPTER 3

Configuring Junos OS User Accounts

- [Junos-FIPS Crypto Officer and User Accounts Overview on page 47](#)
- [Configuring Time-Based User Access on page 48](#)
- [Examples: Configuring Time-Based User Access on page 49](#)
- [Configuring Local User Template Accounts for User Authentication on page 50](#)
- [Configuring Remote Template Accounts for User Authentication on page 52](#)
- [Example: Configuring User Login Accounts on page 52](#)
- [Configuring Junos OS User Accounts on page 53](#)
- [Example: Configuring User Accounts on page 56](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57](#)
- [Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 58](#)
- [Configuring Login Tips on page 58](#)
- [Handling Authorization Failure on page 59](#)
- [Example: Configuring System Retry Options on page 59](#)

Junos-FIPS Crypto Officer and User Accounts Overview

Junos-FIPS defines a restricted set of user roles. Unlike the Junos OS, which enables a wide range of capabilities to users, FIPS 140-2 defines specific types of users (Crypto Officer, User, and Maintenance). Crypto Officers and FIPS Users perform all FIPS-related configuration tasks and issue all FIPS-related commands. Crypto Officer and FIPS User configurations must follow FIPS 140-2 guidelines. Typically, no user besides a Crypto Officer can perform FIPS-related tasks.

Crypto Officer User Configuration

Junos-FIPS offers finer control of user permissions than those mandated by FIPS 140-2. For FIPS 140-2 conformance, any Junos-FIPS user with the **secret**, **security**, and **maintenance** permission bits set is a Crypto Officer. In most cases, the **super-user** class should be reserved for a Crypto Officer. A FIPS User can be defined as any Junos-FIPS user that does not have the **secret**, **security**, and **maintenance** bits set.

FIPS User Configuration

A Crypto Officer sets up FIPS Users. FIPS Users can be granted permissions normally reserved for a Crypto Officer; for example, permission to zeroize the system and individual AS-II FIPS PICs.

Related Documentation

- [Junos OS User Accounts Overview on page 24](#)

Configuring Time-Based User Access

The Junos OS enables you to configure time-based restrictions for user access to log in to a device. This is useful for restricting the time and duration of user logins for all users belonging to a login class. You can specify the days of the week when users can log in, the access start time, and the access end time.

- To configure user access on specific days of the week, without any restrictions on the duration of login, include the **allowed-days** statement only.

```
[edit system]
login {
  class class-name {
    allowed-days [ days-of-the-week ];
  }
}
```

- To configure user access on all the days of the week for a specific duration, include the **access-start** and **access-end** statements only.

```
[edit system]
login {
  class class-name {
    access-start HH:MM;
    access-end HH:MM;
  }
}
```

- To configure user access on specific days of the week for a specified duration, include the **allowed-days**, **access-start**, and **access-end** statements.

```
[edit system]
login {
  class class-name {
    allowed-days [ days-of-the-week ];
    access-start HH:MM;
    access-end HH:MM;
  }
}
```

Specify the start time and end time in **HH:MM** (24-hour) format, where **HH** represents the hours and **MM** represents the minutes.



NOTE: Access start time and end time that spans across 12:00 AM on a specified day results in the user having access until the next day, even if the access day is not explicitly configured. For instance, the following configuration results in the user having access until 6:00 AM on Tuesday and Thursday, although the `allowed-days` statement specifies access only on Monday and Wednesday:

```
[edit system]
login {
  class operator-night-shift {
    allowed-days [ monday wednesday ];
    access-start 2000;
    access-end 0600;
  }
}
```

Related Documentation

- [Examples: Configuring Time-Based User Access on page 45](#)
- [Defining Junos OS Login Classes on page 39](#)
- [access-end on page 367](#)
- [access-start on page 367](#)
- [allowed-days on page 370](#)
- *access-end*
- *access-start*
- *allowed-days*

Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the **operator-round-the-clock-access** login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
  class operator-round-the-clock-access {
    allowed-days [ monday tuesday wednesday thursday friday ];
  }
}
```

The following example shows how to configure user access for the **operator-day-shift** login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 0830;
    access-end 1630;
  }
}
```

```
}
```

Alternatively, you can also specify the login start time and end time for the **operator-day-shift** login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]
login {
  class operator-day-shift {
    allowed-days [ monday wednesday friday ];
    access-start 08:30am;
    access-end 04:30pm;
  }
}
```

The following example shows how to configure user access for the **operator-day-shift-all-days-of-the-week** login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]
login {
  class operator-day-shift-all-days-of-the-week {
    access-start 0830;
    access-end 1630;
  }
}
```

Related Documentation

- [Configuring Time-Based User Access on page 48](#)

Configuring Local User Template Accounts for User Authentication

You use local user template accounts when you need different types of templates for authentication. 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 router or switch 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 Junos OS, which then determines whether a local username is specified for that login name (**local-username** for TACACS+, **Juniper-Local-User** for RADIUS). If so, Junos OS selects the appropriate local user template locally configured on the router or switch. If a local user template does not exist for the authenticated user, the router or switch defaults to the **remote** template.

To configure different access privileges for users who share the local user template account, include the **allow-commands** and **deny-commands** commands in the authentication server configuration file.

To configure a local user template, include the **user local-username** statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to the local users to whom the template applies:

```
[edit system login]
user local-username {
```

```

    full-name "Local user account";
    uid uid-value;
    class class-name;
}

```

This example configures the **sales** and **engineering** local user templates:

```

[edit]
system {
  login {
    user sales {
      uid uid-value;
      class class-name;
    }
    user engineering {
      uid uid-value;
      class class-name;
    }
  }
}

user = simon {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "configure"
    deny-commands = "shutdown"
  }
}

user = rob {
  ...
  service = junos-exec {
    local-user-name = sales
    allow-commands = "(request system) | (show rip neighbor)"
    deny-commands = "clear"
  }
}

user = harold {
  ...
  service = junos-exec {
    local-user-name = engineering
    allow-commands = "monitor | help | show | ping | traceroute"
    deny-commands = "configure"
  }
}

user = jim {
  ...
  service = junos-exec {
    local-user-name = engineering
    allow-commands = "show bgp neighbor"
    deny-commands = "telnet | ssh"
  }
}

```

When the login users Simon and Rob are authenticated, the router or switch applies the sales local user template. When login users Harold and Jim are authenticated, the router or switch applies the engineering local user template.

- Related Documentation**
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
 - [user \(Access\) on page 491](#)
 - *user (Access)*

Configuring Remote Template Accounts for User Authentication

By default, the Junos OS uses remote template accounts for user authentication when:

- The authenticated user does not exist locally on the router or switch.
- The authenticated user's record in the authentication server specifies local user, or the specified local user does not exist locally on the router or switch.

To configure the remote template account, include the **user remote** statement at the **[edit system login]** hierarchy level and specify the privileges you want to grant to remote users:

```
[edit system login]
user remote {
  full-name "All remote users";
  uid uid-value;
  class class-name;
}
```

To configure different access privileges for users who share the remote template account, include the **allow-commands** and **deny-commands** statements in the authentication server configuration file.

- Related Documentation**
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
 - [user \(Access\) on page 491](#)
 - *user (Access)*

Example: Configuring User Login Accounts

The following example shows how to configure the local administrator account (**user admin**). If RADIUS fails or becomes unreachable, the login process reverts to password authentication on the local accounts on the router or switch.

```
[edit]
system {
  login {
    user admin {
      uid 1000;
      class engineering;
      authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
      }
    }
  }
}
```

Related Documentation • [Configuring Junos OS User Accounts on page 53](#)

Configuring Junos OS User Accounts

User accounts provide a way for users to access the router or switch. Junos OS requires that all users have a predefined account before they can log in to the device. For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

It is a common practice to use remote authentication servers to centrally store information about users. Even so, it is also a good practice to configure at least one non-root user directly on each device, in case access to the remote authentication server is disrupted. This one non-root user commonly has a generic name, such as **admin**.

Because user accounts are configured on multiple devices, they are commonly configured inside of a configuration group. As such, the examples shown here are in a configuration group called **global**. Using a configuration group for your user accounts is optional.

To create a user account:

1. Add a new user, using the user's assigned account login name.

```
[edit groups global]
user@host# edit system login user user username
```

2. (Optional) Configure a full descriptive name for the account.

If the full name includes spaces, enclose the entire name in quotation marks.

```
[edit groups global system login user user-name]
user@host# set full-name complete-name
```

For example:

```
user@host# show groups
global {
  system {
    login {
      user admin {
        full-name "general administrator";
      }
    }
  }
}
```

3. (Optional) Set the user identifier (UID) for the account.

As with UNIX systems, the UID enforces user permissions and file access. If you do not set the UID, Junos OS assigns one for you. The format of the UID is a number in the range of 100 to 64000.

```
[edit groups global system login user user-name]
user@host# set uid uid-value
```

For example:

```
user@host# show groups
global {
  system {
    login {
      user admin {
        uid 9999;
      }
    }
  }
}
```

4. Assign the user to a login class.

You can define your own login classes or assign one of the predefined Junos OS login classes.

The predefined login classes are as follows:

- super-user—all permissions
- operator—clear, network, reset, trace, and view permissions
- read-only— view permissions
- unauthorized—no permissions

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

For example:

```
user@host# show groups
global {
  system {
    login {
      user admin {
        class super-user;
      }
    }
  }
}
```

5. Use one of the following methods to configure the user password.

- To enter a clear-text password that the system encrypts for you, use the following command to set the user password:

```
[edit groups global system login user user-name]
user@host# set authentication plain-text-password password
New Password: type password here
Retype new password: retry password here
```

As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are therefore hidden and marked as ## SECRET-DATA in the configuration.

- To enter a password that is already encrypted, use the following command to set the user password:



CAUTION: Do not use the `encrypted-password` option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

If you accidentally configure the `encrypted-password` option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as this user.

```
[edit groups global system login user user-name]
user@host# set authentication encrypted-password "password"
New Password: type password here
Retype new password: retype password here
```

- To load previously generated public keys from a named file at a specified URL location, use the following command to set the user password:

```
[edit groups global system login user user-name]
user@host# set authentication load-key-file URL filename
```

- To enter an ssh public string, use the following command to set the user password:

```
[edit groups global system login user user-name]
user@host# set authentication (ssh-dsa | ssh-ecdsa | ssh-rsa) authorized-key
```

6. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

7. Commit the configuration.

```
user@host# commit
```

8. To verify the configuration, log out and log back in as the new user.

Related Documentation

- [Defining Junos OS Login Classes on page 39](#)
- [Example: Creating Login Classes with Specific Privileges on page 40](#)
- [Junos OS User Accounts Overview on page 24](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57](#)
- [User Access and Authentication Feature Guide for Routing Devices](#)

Example: Configuring User Accounts

The following example shows how to create accounts for four router or switch users, and create an account for the template user **remote**. All users use one of the default system login classes. User **alexander** also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
system {
  login {
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class super-user;
      authentication {
        encrypted-password "$1$poPPeY";
      }
    }
    user alexander {
      full-name "Alexander the Great";
      uid 1002;
      class view;
      authentication {
        encrypted-password "$1$14c5.$sBopasdFFdssdfFFdsdfs0";
        ssh-dsa "8924 37 5678 5678@gaugamela.per";
        ssh-dsa "6273 94 9283@boojum.per";
      }
    }
    user darius {
      full-name "Darius King of Persia";
      uid 1003;
      class operator;
      authentication {
        ssh-rsa "1024 37 12341234@ecbatana.per";
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Related Documentation

- [Junos OS User Accounts Overview on page 24](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57](#)

Limiting the Number of User Login Attempts for SSH and Telnet Sessions

You can limit the number of times a user can attempt to enter a password while logging in through SSH or Telnet. The connection is terminated if a user fails to log in after the number of attempts specified. You can also specify a delay, in seconds, before a user can try to enter a password after a failed attempt. In addition, you can specify the threshold for the number of failed attempts before the user experiences a delay in being able to enter a password again.

To specify the number of times a user can attempt to enter a password while logging in, include the **retry-options** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
retry-options {
  tries-before-disconnect number;
  backoff-threshold number;
  backoff-factor seconds;
  maximum-time seconds
  minimum-time seconds;
}
```

You can configure the following options:

- **tries-before-disconnect**—Number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default is 10.
- **backoff-threshold**—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the **backoff-factor** option to specify the length of the delay in seconds. The range is from 1 through 3, and the default is 2.
- **backoff-factor**—Length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default is 5 seconds.
- **maximum-time *seconds***—Maximum length of time, in seconds, that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed. The range is from 20 through 300 seconds, and the default is 120 seconds.
- **minimum-time**—Minimum length of time, in seconds, that a connection remains open while a user is attempting to enter a correct password. The range is from 20 through 60, and the default is 40.

Related Documentation

- [Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions on page 58](#)
- [Configuring Junos OS User Accounts on page 53](#)

Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions

The following example shows how to limit the user to four attempts when the user enters a password while logging in through SSH or Telnet. Set the **backoff-threshold** to 2, the **back-off-factor** to 5 seconds, and the **minimum-time** to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

The additional variables **maximum-time** and **lockout-period** are not set in this example.

```
[edit]
system {
  login {
    retry-options {
      backoff-threshold 2;
      backoff-factor 5;
      minimum-time 40;
      tries-before-disconnect 4;
    }
    password {
    }
  }
}
```



NOTE: This sample only shows the portion of the [edit system login] hierarchy level being modified.

Related Documentation

- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57](#)
- [login on page 421](#)
- *login*

Configuring Login Tips

The Junos OS CLI provides the option of configuring login tips for the user. By default, the **tip** command is not enabled when a user logs in.

- To enable tips, include the **login-tip** statement at the [edit system login class *class-name*] hierarchy level:

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

Adding this statement enables the **tip** command for the class specified, provided the user logs in using the CLI.

- Related Documentation**
- [CLI User Interface Overview](#)
 - [Defining Junos OS Login Classes on page 39](#)
 - [login-tip](#)

Handling Authorization Failure

The security administrator can configure the number of times a user can try to log in to the device with invalid login credentials. The device can be locked after the specified number of unsuccessful authentication attempts. This helps to protect the device from malicious users attempting to access the system by guessing an account's password. The security administrator can unlock the user account or define a time period for the user account to remain locked.

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

The security administrator can configure a period of time after which an inactive session will be locked and require re-authentication to be unlocked. This helps to protect the device from being idle for a long period before the session times out.

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

The security administrator can configure a banner with an advisory notice to be displayed before the identification and authentication screen.

The **message** system login option 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 three unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users from performing 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.

- Related Documentation**
- [Example: Configuring System Retry Options on page 59](#)
 - [Junos OS CLI Reference](#)

Example: Configuring System Retry Options

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

- [Requirements on page 60](#)
- [Overview on page 60](#)

- [Configuration on page 61](#)
- [Verification on page 62](#)

Requirements

Before you begin, you should understand [“Handling Authorization Failure” on page 59](#).

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 enables 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 between failed login attempts of a user account and can manually lock and unlock user accounts.

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 5 seconds, with a range of 5 to 10 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 log in 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 1 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 10, with a range of 1 through 10 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 his 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 have elapsed, unless a security administrator manually clears the lock sooner.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
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 120
```
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 instructions in this example to correct the configuration.

```
[edit]
user@host# show system login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 120;
tries-before-disconnect 3;
```

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

Verification

Confirm that the configuration is working properly.

Displaying the Locked User Logins

Purpose Verify that the login lockout configuration is enabled.

- Action**
1. Attempt three unsuccessful logins for a particular username. The username is locked out from accessing the device.
 2. Log in to the device with a different username.
 3. 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 120 minutes as configured in the example. You can verify that the user is locked out 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 59](#)

CHAPTER 4

Configuring User Access Privileges

- [Configuring Access Privilege Levels on page 63](#)
- [Example: Configuring Access Privilege Levels on page 64](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 66](#)
- [Example: Configuring Access Privileges for Operational Mode Commands on page 67](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68](#)
- [Defining Access Privileges Using allow or deny configuration Statements on page 69](#)
- [Specifying Access Privileges Using allow/deny-configuration Statements on page 70](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 72](#)

Configuring Access Privilege Levels

Each top-level command-line interface (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 Access Privilege Levels on page 64](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [permissions on page 446](#)

Example: Configuring Access Privilege Levels

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:

```
[edit]
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 63](#)

Specifying Access Privileges for Junos OS Operational Mode Commands

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";
```

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 Access Privileges for Operational Mode Commands on page 67](#)
 - [Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands on page 66](#)
 - [allow-commands on page 368](#)
 - [deny-commands on page 387](#)

Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands

Use extended regular expressions to specify which operational mode commands are denied or allowed. [Table 7 on page 66](#) lists common regular expression operators that can be used in the operational mode commands. Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2.

Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode Commands

| Operator | Match |
|----------|--|
| | One of two or more terms separated by the pipe () symbol. Each term must be a complete standalone expression enclosed in parentheses (), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms) (show system software). |
| ^ | At the beginning of an expression, used to denote where the command begins, and where there might be some ambiguity. |
| \$ | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces\$" means that the user can issue the show interfaces command but cannot issue the show interfaces detail or show interfaces extensive command. |
| [] | Range of letters or digits. To separate the start and end of a range, use a hyphen (-). |
| () | A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must always be used in conjunction with pipe operators as explained above. |

If a regular expression contains a syntax error, it becomes invalid, and although the user can log in, the permission granted or denied by the regular expression does not take effect. When regular expressions configured on TACACS+ or RADIUS servers merge with regular expressions configured on the router or switch, if the final expression has a syntax error, the overall result is an invalid regular expression. If a regular expression does not contain any operators, all varieties of the command are allowed. For example, if the following statement is included in the configuration, the user can issue the commands **show interfaces detail** and **show interfaces extensive** in addition to showing an individual interface:

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

Related Documentation • [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)

Example: Configuring Access Privileges for Operational Mode Commands

The following example shows how to configure access privileges for different login classes for individual operational mode commands:

```
[edit]
system {
  # This login class has operator privileges and the additional ability
  # to reboot the router.
  login {
    # This login class has operator privileges and the additional ability to reboot the
    # router or switch.
    class operator-and-boot {
      permissions [ clear network reset trace view ];
      allow-commands "request system reboot";
    }
    # This login class has operator privileges but can't use any commands beginning
    # with "set".
    # This login class has operator privileges
    # but cannot use any commands beginning with "set"
    class operator-no-set {
      permissions [ clear network reset trace view ];
      deny-commands "^set";
    }
    # This login class has operator privileges and can install software but not view
    # BGP information, and can issue the show route command, without specifying
    # commands or arguments under it.
    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 64](#)

Specifying Access Privileges for Junos OS Configuration Mode Hierarchies

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 64](#)
- [Example: Configuring Access Privilege Levels on page 64](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)

Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies

Use extended regular expressions to specify which configuration mode hierarchies are denied or allowed. You specify these regular expressions in the **allow/deny-configuration-regexps** and **allow/deny-configuration** statements at the **[edit system login class]** hierarchy level, or by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authentication server's configuration. If regular expressions are received during TACACS+ or RADIUS authentication, they merge with any regular expressions configured on the local router or switch.

[Table 8 on page 68](#) lists common regular expression operators that you can use for allowing or denying configuration mode .

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2.

Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators

| Operator | Match |
|----------|---|
| | One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses (), with no spaces between the pipe and the adjacent parentheses. For example, (show system alarms) (show system software) . |

Table 8: Configuration Mode Hierarchies—Common Regular Expression Operators (*continued*)

| Operator | Match |
|------------------|---|
| <code>^</code> | At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity. |
| <code>\$</code> | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, allow-commands "show interfaces\$" means that the user can issue the show interfaces command but cannot issue show interfaces detail or show interfaces extensive . |
| <code>[]</code> | Range of letters or digits. To separate the start and end of a range, use a hyphen (-). |
| <code>()</code> | A group of commands, indicating a complete, standalone expression to be evaluated; the result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators as explained. |
| <code>*</code> | Zero or more terms. |
| <code>+</code> | One or more terms. |
| <code>.</code> | Any character except for a space " ". |

Related Documentation

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies](#)

Defining Access Privileges Using `allow` or `deny` configuration Statements

The following examples show how to configure access privileges for individual configuration mode hierarchy levels.

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@switch# 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@switch# 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 a configuration or issue commands (such as **commit**) at the login class or system services hierarchy levels:

```
[edit system login class class-name]  
user@switch# set deny-configuration "(system login class) | (system services)"
```

The following example shows how to configure permissions 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";  
    }  
  }  
}
```

**Related
Documentation**

- [Specifying Access Privileges Using allow/deny-configuration Statements on page 70](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies](#)

Specifying Access Privileges Using allow/deny-configuration Statements

You can specify extended regular expressions by using the **allow-configuration** and **deny-configuration** statements to define user access privileges to parts of the configuration hierarchy. Doing so overrides login class permission bits set for a user. You can also use wildcards to restrict access. When you define access privileges to parts of the configuration hierarchy, do the following:

- Specify the full paths in the extended regular expressions with the **allow-configuration** and **deny-configuration** statements.
- Use parentheses around an extended regular expression that connects two or more expressions with the pipe | symbol. For example:

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



NOTE: Each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol. You cannot define access to keywords such as **set**, **edit**, or **activate**.

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

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

To explicitly deny an individual configuration hierarchy that would otherwise be allowed, include the **deny-configuration** statement at the **[edit system login class *class-name*]** hierarchy level:

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

You can include one **deny-configuration** and one **allow-configuration** statement in each login class.



NOTE:

- Explicitly allowing configuration mode hierarchies or regular expressions using the **allow-configuration** statement adds to the regular permissions set using the **permissions** statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the **deny-configuration** statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the **permissions** statement.

For example, if a login class has permissions **configure** and the **allow-configuration** statement includes the **system services** expression, the specified login class user can edit the configuration at the **[edit system services]** hierarchy level and issue configuration mode commands (such as **commit**), in addition to just entering the configuration mode using the **configure** command (the permissions specified by the **configure** permission flag). Likewise, if a login class has permissions **all** and the **deny-configuration** statement includes **system services**, the specified login class user can perform all operations allowed by the **all** permissions flag, except issuing configuration mode commands (such as **commit**) or modifying the configuration at the **[edit system services]** hierarchy level.

- If you allow and deny the same set of configuration hierarchy levels, regular expressions, or commands, the **allow-configuration** statement permissions take precedence over the permissions specified by the **deny-configuration** statement. For example, if you include **allow-configuration "system services";** and **deny-configuration "system services";**, the login class user can continue to edit the configuration or issue commands at the **[edit system services]** hierarchy level.

Related Documentation

- [Configuring Access Privilege Levels on page 63](#)
- [Defining Access Privileges Using allow or deny configuration Statements on page 69](#)

- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68](#)

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

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

- [Requirements on page 72](#)
- [Overview on page 72](#)
- [Configuration on page 72](#)
- [Examples on page 73](#)

Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, 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 64](#)
- [Example: Configuring Access Privilege Levels on page 64](#)
- [Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)

CHAPTER 5

Permission Flags for User Access Privileges

- [Access Privilege User Permission Flags Overview on page 78](#)
- [access on page 80](#)
- [access-control on page 81](#)
- [admin on page 81](#)
- [admin-control on page 82](#)
- [all-control on page 83](#)
- [clear on page 83](#)
- [configure on page 121](#)
- [control on page 122](#)
- [field on page 122](#)
- [firewall on page 123](#)
- [firewall-control on page 123](#)
- [floppy on page 124](#)
- [flow-tap on page 125](#)
- [flow-tap-control on page 125](#)
- [flow-tap-operation on page 125](#)
- [idp-profiler-operation on page 126](#)
- [interface on page 126](#)
- [interface-control on page 127](#)
- [maintenance on page 128](#)
- [network on page 135](#)
- [pgcp-session-mirroring on page 137](#)
- [pgcp-session-mirroring-control on page 137](#)
- [reset on page 138](#)
- [rollback on page 138](#)
- [routing on page 139](#)

- [routing-control](#) on page 143
- [secret](#) on page 147
- [secret-control](#) on page 148
- [security](#) on page 150
- [security-control](#) on page 153
- [shell](#) on page 157
- [snmp](#) on page 157
- [snmp-control](#) on page 158
- [system](#) on page 158
- [system-control](#) on page 161
- [trace](#) on page 162
- [trace-control](#) on page 168
- [view](#) on page 173
- [view-configuration](#) on page 243

Access Privilege User Permission Flags Overview

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 26
- [access](#) on page 80
- [access-control](#) on page 81

- [admin](#) on page 81
- [admin-control](#) on page 82
- [all-control](#) on page 83
- [clear](#) on page 83
- [configure](#) on page 121
- [control](#) on page 122
- [field](#) on page 122
- [firewall](#) on page 123
- [firewall-control](#) on page 123
- [floppy](#) on page 124
- [flow-tap](#) on page 125
- [flow-tap-operation](#) on page 125
- [idp-profiler-operation](#) on page 126
- [interface](#) on page 126
- [interface-control](#) on page 127
- [maintenance](#) on page 128
- [network](#) on page 135
- [pgcp-session-mirroring](#) on page 137
- [pgcp-session-mirroring-control](#) on page 137
- [reset](#) on page 138
- [rollback](#) on page 138
- [routing](#) on page 139
- [routing-control](#) on page 143
- [secret](#) on page 147
- [secret-control](#) on page 148
- [security](#) on page 150
- [security-control](#) on page 153
- [shell](#) on page 157
- [snmp](#) on page 157
- [system](#) on page 158
- [system-control](#) on page 161
- [trace](#) on page 162
- [trace-control](#) on page 168

- [view on page 173](#)
- [view-configuration on page 243](#)

access

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 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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [access-control on page 81](#)

access-control

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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [access on page 80](#)

admin

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-forwarding]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
[edit system services ssh tcp-forwarding]
```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [admin-control on page 82](#)

admin-control

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

| | |
|---------------------------------------|--|
| Commands | show system audit |
| Configuration Hierarchy Levels | <pre>[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]</pre> |

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [admin on page 81](#)

all-control

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 | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

clear

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

| | |
|-----------------|---|
| Commands | <pre> 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> </pre> |
|-----------------|---|

```
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-protection protocols bgp aggregate statistics
clear ddos-protection protocols bgp culprit-flows
clear ddos-protection protocols bgp states
clear ddos-protection protocols 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-protection protocols bgpv6 aggregate statistics
clear ddos-protection protocols bgpv6 culprit-flows
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-protection protocols demux-autosense aggregate statistics
clear ddos-protection protocols demux-autosense culprit-flows
clear ddos-protection protocols demux-autosense states
clear ddos-protection protocols demux-autosense 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-demuxauto-aggregate-states
clear-ddos-demuxauto-aggregate-statistics
clear-ddos-demuxauto-states
clear-ddos-demuxauto-statistics
clear-ddos-dhcpv4-ack-states
clear-ddos-dhcpv4-ack-statistics
<clear-ddos-dhcpv4-bootp-statistics>
clear ddos-protection protocols dhcpv4 culprit-flows
clear ddos-protection protocols dhcpv4 decline
clear ddos-protection protocols dhcpv4 decline culprit-flows
clear ddos-protection protocols dhcpv4 decline states
clear ddos-protection protocols dhcpv4 decline statistics
clear ddos-protection protocols dhcpv4 discover
clear ddos-protection protocols dhcpv4 discover states
clear ddos-protection protocols 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-protection protocols dhcpv4 force-renew 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-protection protocols dhcpv4 unclassified 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-protection protocols dhcpv6 advertise statistics
clear ddos-protection protocols dhcpv6 aggregate
clear ddos-protection protocols dhcpv6 aggregate states
clear ddos-protection protocols 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-protection protocols dhcpv6 confirm statistics
clear ddos-protection protocols dhcpv6 decline
clear ddos-protection protocols dhcpv6 decline states
clear ddos-protection protocols dhcpv6 decline statistics
```

```
clear ddos-protection protocols dhcpv6 information-request
clear ddos-protection protocols dhcpv6 information-request states
clear ddos-protection protocols dhcpv6 information-request statistics
clear ddos-protection protocols dhcpv6 leasequery
clear ddos-protection protocols dhcpv6 leasequery states
clear ddos-protection protocols 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-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-leaseq-da-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-protection protocols dhcpv6 leasequery-done statistics
clear ddos-protection protocols dhcpv6 leasequery-reply
clear ddos-protection protocols dhcpv6 leasequery-reply states
clear ddos-protection protocols dhcpv6 leasequery-reply statistics
clear ddos-protection protocols dhcpv6 rebind
clear ddos-protection protocols dhcpv6 rebind states
clear ddos-protection protocols dhcpv6 rebind statistics
clear ddos-protection protocols dhcpv6 reconfigure
clear ddos-protection protocols dhcpv6 reconfigure states
clear ddos-protection protocols dhcpv6 reconfigure statistics
clear ddos-protection protocols dhcpv6 relay-forward
clear ddos-protection protocols dhcpv6 relay-forward states
clear ddos-protection protocols dhcpv6 relay-forward statistics
clear ddos-protection protocols dhcpv6 relay-reply
clear ddos-protection protocols dhcpv6 relay-reply states
clear ddos-protection protocols dhcpv6 relay-reply statistics
clear ddos-protection protocols dhcpv6 release
clear ddos-protection protocols dhcpv6 release states
clear ddos-protection protocols dhcpv6 release statistics
clear ddos-protection protocols dhcpv6 renew
clear ddos-protection protocols dhcpv6 renew states
clear ddos-protection protocols dhcpv6 renew statistics
clear ddos-protection protocols dhcpv6 reply
clear ddos-protection protocols dhcpv6 reply states
clear ddos-protection protocols 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-protection protocols 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-protection protocols dhcpv6 solicit statistics
clear ddos-protection protocols dhcpv6 states
clear ddos-protection protocols 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-protection protocols dhcpv6 unclassified 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-diameter-aggregate-statistics>
clear ddos-protection protocols diameter culprit-flows
clear ddos-protection protocols diameter states
<clear-ddos-diameter-states>
clear ddos-protection protocols diameter statistics
clear ddos-protection protocols dns
clear ddos-protection protocols dns aggregate
clear ddos-protection protocols dns aggregate states
clear ddos-protection protocols dns aggregate statistics
clear ddos-protection protocols dns states
clear ddos-protection protocols 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-protection protocols dtcp aggregate statistics
clear ddos-protection protocols dtcp culprit-flows
clear ddos-protection protocols dtcp states
clear ddos-protection protocols 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-protection protocols dynamic-vlan aggregate statistics
clear ddos-protection protocols dynamic-vlan states
clear ddos-protection protocols dynamic-vlan 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-protection protocols egpv6 aggregate statistics
clear ddos-protection protocols egpv6 states
clear ddos-protection protocols 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-protection protocols eoam aggregate statistics
clear ddos-protection protocols eoam states
clear ddos-protection protocols 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-protection protocols esmc aggregate statistics
clear ddos-protection protocols esmc culprit-flows
clear ddos-protection protocols 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-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-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-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-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-protection protocols ftpv6 aggregate statistics
clear ddos-protection protocols ftpv6 culprit-flows
clear ddos-protection protocols ftpv6 states
```

```
clear ddos-protection protocols ftpv6 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-ftpv6-aggregate-states
clear-ddos-ftpv6-aggregate-statistics
clear-ddos-ftpv6-states
clear-ddos-ftpv6-statistics
clear-ddos-gre-aggregate-states
clear ddos-protection protocols icmp culprit-flows
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-protection protocols igmp-snoop states
clear ddos-protection protocols igmp-snoop statistics
clear ddos-protection protocols igmpv4v6
clear ddos-protection protocols igmpv4v6 aggregate
clear ddos-protection protocols 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-protection protocols 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-igmpv6-aggregate-statistics
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-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-protection protocols ip-fragments first-fragment statistics
clear ddos-protection protocols ip-fragments states
clear ddos-protection protocols ip-fragments 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-protection protocols ip-fragments trail-fragment statistics
clear ddos-protection protocols ip-options
clear ddos-protection protocols ip-options aggregate
clear ddos-protection protocols ip-options aggregate states
clear ddos-protection protocols ip-options 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-protection protocols ip-options router-alert statistics
clear ddos-protection protocols ip-options states
clear ddos-protection protocols ip-options 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-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-protection protocols 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-protection protocols jfm aggregate statistics
clear ddos-protection protocols 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-protection protocols l2tp aggregate statistics
clear ddos-protection protocols l2tp states
clear ddos-protection protocols 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-protection protocols lacp aggregate statistics
clear ddos-protection protocols lacp states
clear ddos-protection protocols 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-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-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-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-protection protocols 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-protection protocols mac-host aggregate statistics
clear ddos-protection protocols 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 aggregate
clear ddos-protection protocols mlp aggregate culprit-flows
clear ddos-protection protocols mlp aggregate states
clear ddos-protection protocols 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-protection protocols mlp aging-exception statistics
clear ddos-protection protocols mlp packets
clear ddos-protection protocols mlp packets states
clear ddos-protection protocols mlp packets statistics
clear ddos-protection protocols mlp states
clear ddos-protection protocols mlp statistics
clear ddos-protection protocols mlp unclassified
clear ddos-protection protocols mlp unclassified states
clear ddos-protection protocols mlp unclassified statistics
clear ddos-protection protocols msdp
clear ddos-protection protocols msdp aggregate
clear ddos-protection protocols 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-protection protocols 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-protection protocols msdpv6 aggregate statistics
clear ddos-protection protocols msdpv6 states
clear ddos-protection protocols 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-protection protocols multicast-copy aggregate statistics
clear ddos-protection protocols multicast-copy states
clear ddos-protection protocols multicast-copy statistics
clear ddos-protection protocols mvrp
clear ddos-protection protocols mvrp aggregate
clear ddos-protection protocols 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-protection protocols 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 ntp aggregate
clear ddos-protection protocols 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-protection protocols 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-protection protocols oam-lfm aggregate statistics
clear ddos-protection protocols oam-lfm states
clear ddos-protection protocols 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-protection protocols ospf aggregate statistics
clear ddos-protection protocols ospf states
clear ddos-protection protocols ospf 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-ospfv3v6-aggregate-statistics
clear-ddos-ospfv3v6-states
clear ddos-protection protocols pimv6
clear-ddos-pim-statistics
clear ddos-protection protocols pfe-alive
clear ddos-protection protocols pfe-alive aggregate
clear ddos-protection protocols 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-protection protocols pfe-alive statistics
clear ddos-protection protocols pim
clear ddos-protection protocols pim aggregate
clear ddos-protection protocols 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-protection protocols pim statistics
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-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 states
clear ddos-protection protocols pmvrp statistics
clear ddos-protection protocols pos
clear ddos-protection protocols pos aggregate
clear ddos-protection protocols pos aggregate states
clear ddos-protection protocols pos aggregate statistics
clear ddos-protection protocols pos states
clear ddos-protection protocols pos statistics
clear ddos-protection protocols ppp
clear ddos-protection protocols ppp aggregate
clear ddos-protection protocols ppp aggregate states
clear ddos-protection protocols ppp aggregate statistics
clear ddos-protection protocols ppp authentication
clear ddos-protection protocols ppp authentication states
clear ddos-protection protocols ppp authentication statistics
clear ddos-protection protocols ppp ipcp
clear ddos-protection protocols ppp ipcp states
clear ddos-protection protocols ppp ipcp statistics
clear ddos-protection protocols ppp ipv6cp
clear ddos-protection protocols ppp ipv6cp states
clear ddos-protection protocols ppp ipv6cp statistics
clear ddos-protection protocols ppp isis
clear ddos-protection protocols ppp isis states
clear ddos-protection protocols ppp isis statistics
clear ddos-protection protocols ppp lcp
clear ddos-protection protocols ppp lcp states
clear ddos-protection protocols ppp lcp statistics
clear ddos-protection protocols ppp mplsdp
clear ddos-protection protocols ppp mplsdp states
clear ddos-protection protocols ppp mplsdp statistics
clear ddos-protection protocols ppp states
clear ddos-protection protocols ppp statistics
clear ddos-protection protocols ppp unclassified
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
clear ddos-protection protocols pppoe aggregate states
clear ddos-protection protocols pppoe aggregate statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear ddos-protection protocols pppoe padi statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear ddos-protection protocols pppoe padm statistics
```

```
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
clear ddos-protection protocols pppoe padn statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear ddos-protection protocols pppoe pado statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear ddos-protection protocols pppoe padr statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear ddos-protection protocols pppoe pads statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear ddos-protection protocols pppoe padt statistics
clear ddos-protection protocols pppoe states
clear ddos-protection protocols pppoe statistics
clear ddos-protection protocols ptp
clear ddos-protection protocols ptp aggregate
clear ddos-protection protocols ptp aggregate states
clear ddos-protection protocols ptp aggregate statistics
clear ddos-protection protocols ptp states
clear ddos-protection protocols ptp statistics
clear ddos-protection protocols pvstp
clear ddos-protection protocols pvstp aggregate
clear ddos-protection protocols pvstp aggregate states
clear ddos-protection protocols pvstp aggregate statistics
clear ddos-protection protocols pvstp states
clear ddos-protection protocols pvstp statistics
clear ddos-protection protocols radius
clear ddos-protection protocols radius accounting
clear ddos-protection protocols radius accounting states
clear ddos-protection protocols radius accounting statistics
clear ddos-protection protocols radius aggregate
clear ddos-protection protocols radius aggregate states
clear ddos-protection protocols 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-ptp-aggregate-states
clear-ddos-ptp-aggregate-statistics
clear-ddos-ptp-states
clear-ddos-ptp-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-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-protection protocols radius server statistics
clear ddos-protection protocols radius states
clear ddos-protection protocols radius statistics
clear ddos-protection protocols redirect
clear ddos-protection protocols redirect aggregate
clear ddos-protection protocols redirect aggregate states
clear ddos-protection protocols redirect aggregate statistics

```
clear ddos-protection protocols redirect states
clear ddos-protection protocols 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-protection protocols rip aggregate statistics
clear ddos-protection protocols rip states
clear ddos-protection protocols rip statistics
clear ddos-protection protocols ripv6
clear ddos-protection protocols ripv6 aggregate
clear ddos-protection protocols ripv6 aggregate states
clear ddos-protection protocols ripv6 aggregate statistics
clear ddos-protection protocols ripv6 states
clear ddos-protection protocols ripv6 statistics
clear ddos-protection protocols rsvp
clear ddos-protection protocols rsvp aggregate
clear ddos-protection protocols rsvp aggregate states
clear ddos-protection protocols rsvp aggregate statistics
clear ddos-protection protocols rsvp states
clear ddos-protection protocols rsvp statistics
clear ddos-protection protocols rsvpv6
clear ddos-protection protocols rsvpv6 aggregate
clear ddos-protection protocols rsvpv6 aggregate states
clear ddos-protection protocols rsvpv6 aggregate statistics
clear ddos-protection protocols rsvpv6 states
clear ddos-protection protocols rsvpv6 statistics
clear ddos-protection protocols sample
clear ddos-protection protocols sample aggregate
clear ddos-protection protocols sample aggregate states
clear ddos-protection protocols sample aggregate statistics
clear ddos-protection protocols sample host
clear ddos-protection protocols sample host states
clear ddos-protection protocols 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-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-protection protocols 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-protection protocols sample syslog statistics
```

```
clear ddos-protection protocols sample tap
clear ddos-protection protocols sample tap states
clear ddos-protection protocols sample tap statistics
clear ddos-protection protocols services
clear ddos-protection protocols services aggregate
clear ddos-protection protocols 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-protection protocols services statistics
clear ddos-protection protocols snmp
clear ddos-protection protocols snmp aggregate
clear ddos-protection protocols 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-protection protocols snmp statistics
clear ddos-protection protocols snmpv6
clear ddos-protection protocols snmpv6 aggregate
clear ddos-protection protocols snmpv6 aggregate states
clear ddos-protection protocols snmpv6 aggregate statistics
clear ddos-protection protocols snmpv6 states
clear ddos-protection protocols snmpv6 statistics
clear ddos-protection protocols ssh
clear ddos-protection protocols ssh aggregate
clear ddos-protection protocols ssh aggregate states
clear ddos-protection protocols ssh aggregate statistics
clear ddos-protection protocols ssh states
clear ddos-protection protocols ssh statistics
clear ddos-protection protocols sshv6
clear ddos-protection protocols sshv6 aggregate
clear ddos-protection protocols 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-protection protocols sshv6 statistics
clear ddos-protection protocols states
clear ddos-protection protocols statistics
clear ddos-protection protocols stp
clear ddos-protection protocols stp aggregate
clear ddos-protection protocols stp aggregate states
```

```
clear ddos-protection protocols stp aggregate statistics
clear ddos-protection protocols stp states
clear ddos-protection protocols stp statistics
clear ddos-protection protocols tacacs
clear ddos-protection protocols tacacs aggregate
clear ddos-protection protocols tacacs aggregate states
clear ddos-protection protocols tacacs aggregate statistics
clear ddos-protection protocols tacacs states
clear ddos-protection protocols 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-protection protocols tcp-flags aggregate statistics
clear ddos-protection protocols tcp-flags established
clear ddos-protection protocols tcp-flags established states
clear ddos-protection protocols tcp-flags established 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-protection protocols tcp-flags initial statistics
clear ddos-protection protocols tcp-flags states
clear ddos-protection protocols tcp-flags statistics
clear ddos-protection protocols tcp-flags unclassified
clear ddos-protection protocols tcp-flags unclassified states
clear ddos-protection protocols tcp-flags unclassified 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-protection protocols telnet aggregate statistics
clear ddos-protection protocols telnet states
clear ddos-protection protocols telnet statistics
clear ddos-protection protocols telnetv6
clear ddos-protection protocols telnetv6 aggregate
clear ddos-protection protocols telnetv6 aggregate states
clear ddos-protection protocols telnetv6 aggregate statistics
clear ddos-protection protocols telnetv6 states
clear ddos-protection protocols 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-protection protocols ttl aggregate statistics
clear ddos-protection protocols ttl states
clear ddos-protection protocols 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-protection protocols tunnel-fragment aggregate statistics
clear ddos-protection protocols tunnel-fragment states
clear ddos-protection protocols tunnel-fragment 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 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-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-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-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-vchassis-aggregate-states
clear ddos-protection protocols virtual-chassis aggregate statistics
clear ddos-protection protocols virtual-chassis control-high
clear ddos-protection protocols virtual-chassis control-high states
clear ddos-protection protocols virtual-chassis control-high statistics
clear ddos-protection protocols virtual-chassis control-low
clear ddos-protection protocols virtual-chassis control-low states
clear ddos-protection protocols virtual-chassis control-low statistics
clear ddos-protection protocols virtual-chassis states
clear ddos-protection protocols virtual-chassis 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-protection protocols virtual-chassis unclassified statistics
clear ddos-protection protocols virtual-chassis vc-packets
clear ddos-protection protocols virtual-chassis vc-packets states
clear ddos-protection protocols virtual-chassis vc-packets statistics
clear ddos-protection protocols virtual-chassis vc-ttl-errors
clear ddos-protection protocols virtual-chassis vc-ttl-errors states
clear ddos-protection protocols virtual-chassis vc-ttl-errors statistics
clear ddos-protection protocols vrrp
clear ddos-protection protocols vrrp aggregate
clear ddos-protection protocols 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-protection protocols vrrpv6
clear ddos-protection protocols vrrpv6 aggregate
clear ddos-protection protocols vrrpv6 aggregate states
clear ddos-protection protocols vrrpv6 aggregate statistics

```
clear ddos-protection protocols 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 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 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 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 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 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 bpd
clear error bpd interface
<clear-bpd-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 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 fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-conters>
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 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 pfe
clear pfe statistics
clear pfe statistics fabric
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 lockout
<clear-pppoe-lockout-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 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 software
clear services inline software statistics
<clear-inline-software-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 errors
<clear-service-video-monitoring-mdi-errors>
clear services video-monitoring mdi statistics
<clear-service-video-monitoring-mdi-statistics>
clear services software
clear services software statistics
<clear-services-software-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 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 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>
request services ipsec-vpn ipsec
request services ipsec-vpn ipsec switch
request services ipsec-vpn ipsec switch tunnel

```

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

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

configure

Can enter configuration mode.

| | |
|---------------------------------------|--|
| Commands | <code>configure</code> <code>request snmp</code> <code>request-snmp-utility-mib-clear</code> <code>request-snmp-utility-mib-set</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 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

control

| | |
|---------------------------------------|--|
| | Can perform all control-level operations; can modify any configuration. |
| Commands | <code>test configuration</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 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

field

| | |
|---------------------------------------|--|
| | 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 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

firewall

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 policer show firewall policer counters <get-firewall-policer-counter-information> show firewall policer counters counter-id <get-firewall-policer-per-counter-information> show firewall templates-in-use 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 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 • firewall-control on page 123 |

firewall-control

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

| | |
|-----------------|---|
| Commands | <pre>show firewall <get-firewall-information></pre> |
|-----------------|---|

| | |
|---|---|
| | <code>show firewall counter</code> <code><get-firewall-counter-information></code> |
| | <code>show firewall filter</code> <code><get-firewall-filter-information></code> |
| | <code>show firewall filter version</code> <code><get-filter-version></code> |
| | <code>show firewall log</code> <code><get-firewall-log-information></code> |
| | <code>show firewall prefix-action-stats</code> <code><get-firewall-prefix-action-information></code> |
| | <code>show policer</code> |
| Configuration Hierarchy Levels | <code>[edit dynamic-profiles firewall]</code> <code>[edit firewall]</code> <code>[edit logical-systems firewall]</code> |
| Related Documentation | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67• firewall on page 123 |

floppy

| | |
|---|--|
| | 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 | <ul style="list-style-type: none">• Access Privilege User Permission Flags Overview on page 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

flow-tap

| | |
|---------------------------------------|--|
| | Can view the flow-tap configuration in configuration mode. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | [edit services flow-tap] [edit services radius-flow-tap] [edit system services flow-tap-dtcp] |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 • flow-tap-control on page 125 |

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], [edit services radius-flow-tap], and [edit system services flow-tap-dtcp] hierarchy levels. |
| Commands | No associated CLI commands. |
| Configuration Hierarchy Levels | [edit services flow-tap] [edit services radius-flow-tap] [edit system services flow-tap-dtcp] |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 • flow-tap on page 125 |

flow-tap-operation

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 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

idp-profiler-operation

| | |
|---|--|
| | Can view profiler data. |
| Commands | No associated CLI commands. |
| CLI Configuration Hierarchy Levels | No associated CLI configuration hierarchy levels and statements. |

interface

| | |
|---------------------------------------|--|
| | Can view the interface configuration in configuration mode. |
| Commands | <ul style="list-style-type: none"><test-rfc2544-benchmarking><test-rfc2544-benchmarking-test><test-rfc2544-benchmarking-test-id> |
| 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][edit logical-systems routing-instances instance system services dhcp-local-server][edit logical-systems routing-instances instance system services dhcp-proxy-client]][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 dhcp-proxy-client]
[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 dhcp-proxy-client]
[edit system services static-subscribers group]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [interface-control on page 127](#)

interface-control

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 switch-options redundant-trunk-group group preempt-cutover-timer]
[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 switch-options redundant-trunk-group group preempt-cutover-timer]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [interface on page 126](#)

maintenance

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 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-eedebug-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 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 zeroize
request vpls-switchover
set date
set date ntp
show chassis usb
show chassis usb storage
  <get-usb-storage-status>
show services fips
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]
```

Related Documentation

- [Access Privilege User Permission Flags Overview on page 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

network

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 clns
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 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 mrinfo
ssh
telnet
traceroute
    <traceroute>

traceroute clns
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>

```

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

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

pgcp-session-mirroring

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 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [pgcp-session-mirroring-control on page 137](#)

pgcp-session-mirroring-control

Can modify the 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 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [pgcp-session-mirroring on page 137](#)

reset

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 78• Understanding Junos OS Access Privilege Levels on page 26• Configuring Access Privilege Levels on page 63• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |
|------------------------------|--|

rollback

Can roll back to previous configurations.

| | |
|---------------------------------------|--|
| Commands | rollback |
| Configuration Hierarchy Levels | [edit] |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 |

routing

Can view general routing, routing protocol, and routing policy configuration information.

| | |
|---------------------------------------|--|
| Commands | request mpls request mpls lsp request mpls lsp adjust-autobandwidth <request-mpls-lsp-autobandwidth-adjust> |
| Configuration Hierarchy Levels | [edit bridge-domains] [edit bridge-domains domain multicast-snooping-options] [edit bridge-domains domain multicast-snooping-options traceoptions] [edit dynamic-profiles protocols igmp traceoptions] [edit dynamic-profiles protocols mld traceoptions] [edit dynamic-profiles protocols router-advertisement traceoptions] [edit dynamic-profiles routing-instances] [edit dynamic-profiles routing-instances instance bridge-domains] [edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options] [edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions] [edit dynamic-profiles routing-instances instance multicast-snooping-options] [edit dynamic-profiles routing-instances instance multicast-snooping-options traceoptions] [edit dynamic-profiles routing-instances instance pbb-options] [edit dynamic-profiles routing-instances instance protocols] [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 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]
[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 service-groups]
[edit dynamic-profiles routing-instances instance switch-options]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit jnx-example]
[edit fabric protocols]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[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 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 isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host 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 mvpn traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim 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]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain

```
multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance igmp-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[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 evpn 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]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options validation group session
traceoptions]
[edit logical-systems routing-instances instance routing-options validation traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-options validation group session traceoptions]
[edit logical-systems routing-instances instance service-groups]
[edit logical-systems routing-instances instance switch-options]
[edit logical-systems routing-instances instance vlans]
[edit logical-systems routing-instances instance vlans vlan multicast-snooping-options]
[edit logical-systems routing-instances instance vlans vlan multicast-snooping-options
traceoptions]
[edit logical-systems routing-options]
[edit logical-systems routing-options validation group session traceoptions]
[edit logical-systems routing-options validation traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
[edit logical-systems vlans]
[edit logical-systems vlans vlan multicast-snooping-options]
[edit logical-systems vlans vlan multicast-snooping-options traceoptions]
[edit multicast-snooping-options]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
```

```
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections]
[edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2lw traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvrp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance multicast-snooping-options]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[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 evpn 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 mld-snooping traceoptions]
[edit routing-instances instance protocols mld-snooping vlan 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]
[edit routing-instances instance routing-options validation group session traceoptions]
[edit routing-instances instance routing-options validation traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-instances instance vlans]
[edit routing-instances instance vlans vlan multicast-snooping-options]
[edit routing-instances instance vlans vlan multicast-snooping-options traceoptions]
[edit routing-options]
[edit routing-options validation group session]
[edit routing-options multicast traceoptions]
[edit routing-options validation]
[edit routing-options traceoptions]
[edit switch-options]
[edit vlans]
[edit vlans vlan multicast-snooping-options]
[edit vlans vlan multicast-snooping-options traceoptions]

```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [routing-control on page 143](#)

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.

Commands No associated CLI commands.

Configuration Hierarchy Levels

```

[edit bridge-domains]
[edit bridge-domains domain multicast-snooping-options]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]

```

[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles routing-instances]
[edit dynamic-profiles routing-instances instance bridge-domains]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options]
[edit dynamic-profiles routing-instances instance multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance pbb-options]
[edit dynamic-profiles routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit dynamic-profiles routing-instances instance switch-options]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit jnx-example]
[edit fabric protocols]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[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 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 isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host 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 mvpn traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim 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]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance igmp-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[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 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]
[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 service-groups]
[edit logical-systems routing-instances instance switch-options]
[edit logical-systems routing-options]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
[edit multicast-snooping-options]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections][edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvpn traceoptions]
[edit protocols mvrp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ptp]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit routing-instances instance igmp-snooping-options]
[edit routing-instances instance multicast-snooping-options]

```

[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[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 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]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-options]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit switch-options]

```

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [routing on page 139](#)

secret

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 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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [secret-control on page 148](#)

secret-control

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 | <pre> [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 servers accounting-secret] [edit access radius servers dynamic-request-secret] [edit access radius servers 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] </pre> |
| Related Documentation | <ul style="list-style-type: none"> • Access Privilege User Permission Flags Overview on page 78 • Understanding Junos OS Access Privilege Levels on page 26 • Configuring Access Privilege Levels on page 63 |

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [secret on page 147](#)

security

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 ike

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 ca-profile-group
request security pki ca-certificate ca-profile-group load
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 export
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 group-vpn
show security group-vpn member
show security group-vpn member ike
show security group-vpn member ike security-associations
<get-gvpn-ike-security-associations-information>
show security group-vpn member ipsec
show security group-vpn member ipsec inactive-tunnels
<get-gvpn-inactive-tunnels>
show security group-vpn member ipsec security-associations
<get-gvpn-security-associations-information>
show security group-vpn member ipsec statistics
<get-gvpn-ipsec-statistics-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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [security-control on page 153](#)

security-control

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 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [security on page 150](#)

shell

Can start a local shell on the router.

Commands

```
request routing-engine
request routing-engine execute
<request-shell-execute>
start shell
start shell user
```

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

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

snmp

Can view Simple Network Management Protocol (SNMP) configuration.

Commands No associated CLI commands.

Configuration Hierarchy Levels [edit snmp]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
 - [snmp-control on page 158](#)

snmp-control

Can view SNMP configuration information and can modify SNMP configuration at the **[edit snmp]** hierarchy level.

Commands No associated CLI commands.

Configuration Hierarchy Levels [edit snmp]

Related Documentation

- [Access Privilege User Permission Flags Overview on page 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [snmp on page 157](#)

system

Can view system-level configuration information.

Commands

- 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 virtual-chassis
- 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 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-rollbacks]
[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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [system-control on page 161](#)

system-control

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

| | |
|-------------------------|---|
| Configuration | [edit applications] |
| Hierarchy Levels | [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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [system on page 158](#)

trace

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 access radius traceoptions]
 [edit bridge-domains domain multicast-snooping-options traceoptions]
 [edit bridge-domains domain protocols igmp-snooping]
 [edit bridge-domains domain forwarding-options dhcp-relay traceoptions]
 [edit bridge-domains domain protocols igmp-snooping traceoptions]
 [edit bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
 [edit bridge-domains domain multicast-snooping-options traceoptions]
 [edit bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay traceoptions]
 [edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
 [edit dynamic-profiles routing-instances instance bridge-domains 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 pim-snooping 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 bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems bridge-domains 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 igmp-snooping 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 mld-snooping vlan 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 mvpn 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 openflow traceoptions]
[edit logical-systems protocols pcep pce traceoptions]
[edit logical-systems protocols pcep pce-group traceoptions]
[edit logical-systems protocols pcep traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols pim-snooping 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 bridge-domains domain
multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance bridge-domains 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 mld-snooping traceoptions]
[edit logical-systems routing-instances instance protocols mld-snooping vlan
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 validation group session]
[edit logical-systems routing-instances instance routing-options validation 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 igmp-snooping 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 mld-snooping vlan 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 mvpn 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 bridge-domains domain multicast-snooping-options traceoptions]
[edit routing-instances instance bridge-domains 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 pim-snooping 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 group-vpn member ike 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 app-engine-management-service traceoptions]
[edit system processes app-engine-virtual-machine-management-service 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]
[edit unified-edge aaa]
[edit unified-edge gateways ggsn-pgw charging local-persistent-storage-options]
[edit unified-edge gateways ggsn-pgw charging traceoptions]
[edit unified-edge gateways ggsn-pgw gtp traceoptions]
[edit unified-edge gateways ggsn-pgw traceoptions]

[edit unified-edge gateways sgw charging local-persistent-storage-options traceoptions]
[edit unified-edge gateways sgw charging traceoptions]
[edit unified-edge gateways sgw gtp traceoptions]
[edit unified-edge gateways sgw traceoptions]
[edit unified-edge mobile-options traceoptions]
[edit unified-edge resource-management client traceoptions]
[edit unified-edge resource-management server traceoptions]

**Related
Documentation**

- [Access Privilege User Permission Flags Overview on page 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [trace-control on page 168](#)

trace-control

Can modify trace file settings and configure trace file properties.

**Configuration
Hierarchy Levels**

[edit bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
[edit bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems bridge-domains domain forwarding-options dhcp-relay
traceoptions]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay interface-traceoptions]
[edit logical-systems routing-instances instance bridge-domains domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance bridge-domains 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 bridge-domains domain forwarding-options dhcp-relay
interface-traceoptions]
[edit routing-instances instance bridge-domains domain forwarding-options dhcp-relay
traceoptions]
[edit routing-instances instance bridge-domains domain multicast-snooping-options
traceoptions]
[edit routing-instances instance bridge-domains 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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)
- [trace on page 162](#)

view

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 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
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 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 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 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 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 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 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 gre
  get-ddos-gre-information
show ddos-protection protocols gre aggregate
  get-ddos-gre-aggregate
show ddos-protection protocols gre parameters
  get-ddos-gre-parameters
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
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 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 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-lddp-information
show ddos-protection protocols lldp aggregate
  get-ddos-lddp-aggregate
show ddos-protection protocols lldp parameters
  get-ddos-lddp-parameters
show ddos-protection protocols lldp statistics
  get-ddos-lddp-statistics
show ddos-protection protocols lldp violations
  get-ddos-lddp-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 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 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 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 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 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 mplscp
  get-ddos-ppp-mplscp
show ddos-protection protocols ppp mplscp 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 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 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 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 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
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 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 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 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 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 statistics
  <get-dhcpv6-service-statistics-information>
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 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 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 forwarding-options
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 hfrf
show hfrf 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 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 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 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 pfe
show pfe cfeb
show pfe feb
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 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 statistics ip6
show pfe statistics traffic
  <get-pfe-statistics>

show pfe statistics traffic cpu
show pfe statistics traffic cpu fpe
show pfe statistics traffic egress-queues
show pfe statistics traffic egress-queues fpc
show pfe statistics traffic multicast
show pfe statistics traffic multicast fpcshow 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-ntp-clock>
show ptp global-information
  get-ntp-global-information>
show ptp hybrid
show ptp hybrid config
  <get-ntp-hybrid-mapping>
show ptp hybrid status
  <get-ntp-hybrid-status>
show ptp last-tod-update
  <get-last-tod-update>
show ptp lock-status
  get-ntp-lock-status>
show ptp master
  <get-ntp-master>
show ptp path-trace
  <get-ntp-path-trace>
show ptp port
  <get-ntp-port>
show ptp quality-level-mapping
  <get-ntp-quality-level-mapping>
show ptp slave
  <get-ntp-slave>
show ptp stateful
  <get-ntp-stateful>
show ptp statistics
  <get-ntp-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-rtexport-table-information>

show route export instance
  <get-rtexport-instance-information>

show route localization
  <get-fib-localization-information>
show route export vrf-target
  <get-rtexport-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 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

show 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 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 pool
  <get-inline-nat-pool-information>
show services inline nat statistics
  <get-inline-nat-statistics-information>
show services inline softwire
show services inline softwire statistics
  <get-inline-service-sw-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 lockdown
  <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 pcp
show services nat mappings summary
  <get-service-nat-mapping-summary>
show services nat pool
  <get-service-nat-pool-information>
show services pcp
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 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 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 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 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 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>

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 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 fdl-line-loop
test interface fdl-line-loop ansi
test interface fdl-line-loop ansi initiate
test interface fdl-line-loop ansi terminate
test interface fdl-line-loop bellcore
test interface fdl-line-loop bellcore initiate
test interface fdl-line-loop bellcore terminate
test interface fdl-payload-loop
```

```

test interface fdl-payload-loop ansi
test interface fdl-payload-loop ansi initiate
test interface fdl-payload-loop ansi terminate
test interface fdl-payload-loop bellcore
test interface fdl-payload-loop bellcore initiate
test interface fdl-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 78](#)
- [Understanding Junos OS Access Privilege Levels on page 26](#)
- [Configuring Access Privilege Levels on page 63](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

view-configuration

Can view all of the configuration excluding secrets, system scripts, and event options.



NOTE: Only users with the maintenance permission can view commit script, op script, or event script configuration.

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 78](#)
 - [Understanding Junos OS Access Privilege Levels on page 26](#)
 - [Configuring Access Privilege Levels on page 63](#)
 - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 64](#)
 - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67](#)

CHAPTER 6

Configuring Passwords for User Access

- [Configuring the Root Password on page 245](#)
- [Example: Configuring the Root Password on page 247](#)
- [Example: Configuring a Plain-Text Password for Root Logins on page 247](#)
- [Example: Configuring SSH Authentication for Root Logins on page 249](#)
- [Recovering the Root Password on page 250](#)
- [Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)
- [Configuring MS-CHAPv2 for Password-Change Support on page 254](#)

Configuring the Root Password

The Junos OS is preinstalled on the router or switch. When the router or switch is powered on, it is ready to be configured. Initially, you log in as the user **root** with no password. The root directory of a UNIX device is the entry point to all other folders and files on that device. As a result, access to the root directory is restricted by default to a predefined user account known as the *root user*. The root user (also referred to as *superuser*) has unrestricted access and full permissions within the system. The expression “log in as root” is commonly used when an action requires the user to log into the device as the root user.



NOTE: If you configure a blank password using the **encrypted-password** statement at the **[edit system root-authentication]** hierarchy level for root authentication, you can commit a configuration but you *cannot* log in as the root user and gain root level access to the router or switch.

After you log in, you should configure the root (superuser) password by including the **root-authentication** statement at the **[edit system]** hierarchy level and configuring one of the password options:

```
[edit system]
root-authentication {
  (encrypted-password "password"| plain-text-password);
  load-key-file URL filename;
  ssh-dsa "public-key" <from hostname>;
```

```
ssh-ecdsa "public-key" <from hostname>;  
ssh-rsa "public-key" <from hostname>;  
}
```

If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

```
[edit system]  
user@host# set root-authentication plain-text-password  
New password: type password here  
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long
 - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
 - Valid passwords must contain at least one change of case or character class.

You can use the **load-key-file** *URL filename* statement to load an SSH key file that was previously generated using **ssh-keygen**. The *URL filename* is the path to the file's location and name. When using this option, the contents of the key file are copied into the configuration immediately after entering the **load-key-file** *URL* statement. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

Optionally, you can use the **ssh-dsa**, **ssh-ecdsa**, or **ssh-rsa** statements to directly configure SSH RSA, DSA, or ECDSA keys to authenticate root logins. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them.

To view the SSH keys entries, use the configuration mode **show** command. For example:

```
[edit system]  
user@host# set root-authentication load-key-file my-host:.ssh/id_dsa.pub  
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%  
[edit system]  
user@host# show  
root-authentication {  
  ssh-rsa "1024 35 9727638204084251055468226757249864241630322  
    20740496252839038203869014158453496417001961060835872296  
    15634757491827360336127644187426594689320773910834481012  
    68312595772262546166799927831612350043866091586628382248  
    97467326056611921489539813965561563786211940327687806538  
    16960202749164163735913269396344008443 boojum@juniper.net"; #  
    SECRET-DATA  
  }  
}
```

Junos-FIPS software has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router or switch, you cannot

configure passwords unless they meet this standard. If you use the **encrypted-password** option, then a null-password (empty) is not permitted.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

Related Documentation

- [Configuring the Root Password](#)
- [Example: Configuring a Plain-Text Password for Root Logins on page 247](#)
- [Example: Configuring SSH Authentication for Root Logins on page 249](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)
- [Recovering the Root Password on page 250](#)

Example: Configuring the Root Password

The following example shows how to configure the root password:

```
[edit]
user@switch# set system root-authentication encrypted-password
"$1$14c5.$sBopasddsdfs0"
[edit]
user@switch# show
system {
  root-authentication {
    encrypted-password "$1$14c5.$sBopasddsdfs0";
  }
}
```

Related Documentation

- [Configuring the Root Password on page 245](#)
- [Example: Configuring a Plain-Text Password for Root Logins on page 247](#)
- [Configuring the Root Password](#)

Example: Configuring a Plain-Text Password for Root Logins

This example shows how to configure the authentication methods for the root-level user, whose username is "root".

- [Requirements on page 247](#)
- [Overview on page 248](#)
- [Configuration on page 248](#)
- [Verification on page 249](#)

Requirements

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

Make sure you understand the requirements for a valid plain-text password. For Junos OS, the The default requirements for plain-text passwords are as follow:

- The password must be between 6 and 128 characters long.
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Valid passwords must contain at least one change of case or character class.

Overview

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the user “root” with no password. To set the root password, you have several options. This example shows you how to enter a plain-text password that Junos OS then encrypts for you.

Configuration

CLI Quick Configuration

```
[edit system]
set root-authentication plain-text-password
New password: new-password
Retype new password: new-password
```

Configuring [item]

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

To configure a plain-text password:

1. Type the set command for plain-text password and press Enter.

```
[edit]
user@host# set system root-authentication plain-text-password
New password:
```
2. Type the new password next to the **New password:** prompt and press Enter.

```
user@host# new-password
Retype new password:
```
3. Retype the same password next to the next prompt and press Enter.

Results

From configuration mode, confirm your configuration by entering the **show** command. It should look something like this:

```
root-authentication {
  encrypted-password "$1$ASwBkGYd$YUcEwgd0IO4QkRzzlQdmT/"; ## SECRET-DATA
}
```

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

After you have confirmed that the interfaces are configured, enter the **commit** command in configuration mode.

Verification

- [Verifying the Configuration of a Plain-Text Password for Root Logins on page 249](#)

Verifying the Configuration of a Plain-Text Password for Root Logins

Purpose Verify the configuration of a plain-text password.

Action From operational mode, confirm your configuration by entering the **show configuration system** command.

```
user@host> show configuration system
root-authentication {
  encrypted-password "$1$ASwBkGYd$YUcEwgd0IO4QkRzzlQdmT/"; ## SECRET-DATA
}
```

Meaning If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

- Related Documentation**
- *root-authentication*
 - [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
 - *Configuring Special Requirements for Plain-Text Passwords*
 - [Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)

Example: Configuring SSH Authentication for Root Logins

The following example shows how to configure two public DSA keys for SSH authentication of root logins:

```
[edit system]
root-authentication {
  encrypted-password "$1$1wp5tqMX$uy/u5H7OdXTwfWTmeJWXe/";
  ## SECRET-DATA;
  ssh-dsa "2354 95 9304@boojum.per";
  ssh-dsa "0483 02 8362@ecbatana.per";
}
```

- Related Documentation**
- [Configuring the Root Password on page 245](#)
 - [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)

Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.



NOTE: You need console access to recover the root password.



Video: [Recovering the Root Password](#)

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45-to-DB-9 serial port adapter supplied with the router.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the router.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
9. Power on the router by pressing the power button on the front panel.

Verify that the POWER LED on the front panel turns green.

The terminal emulation screen on your management device displays the router's boot sequence.
10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

Depending on your device hardware, the bootstrap loader might proceed quite quickly at this step without pausing for input. Therefore, you might need to press the spacebar multiple times at the beginning of the boot sequence.

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...

11. At the following prompt, type **boot -s** to start the system in single-user mode.

ok **boot -s**

12. At the following prompt, type **recovery** to start the root password recovery procedure.

Enter full pathname of shell or 'recovery' for root password recovery or RETURN
for /bin/sh: **recovery**

13. Enter configuration mode in the CLI.

14. Set the root password.

When you configure a plain-text password, Junos OS encrypts the password for you.



CAUTION: Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password. If you commit the **encrypted-password** option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to repeat this password recovery process.

Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the root password.

For example:

```
user@host# set groups global system root-authentication plain-text-password
```

15. At the following prompt, enter the new root password, for example:

New password: **password**
Retype new password:

16. At the second prompt, reenter the new root password.

17. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

18. After you have finished configuring the password, commit the configuration.

```
root@host# commit
commit complete
```

19. Exit configuration mode in the CLI.

20. Exit operational mode in the CLI.

21. At the prompt, type **y** to reboot the router.

Reboot the system? [y/n] **y**

- Related Documentation**
- [Configuring the Root Password on page 245](#)

Changing the Requirements for Junos OS Plain-Text Passwords

To change the requirements for plain-text passwords, include the **password** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
password {
  change-type (set-transitions | character-set);
  format (md5 | sha1);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
  minimum-lower-cases number;
  minimum-numeric number;
  minimum-punctuations number;
  minimum-upper-cases number;
}
```



NOTE: These statements apply to plain-text passwords only, not encrypted passwords.

- Related Documentation**
- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
 - [Configuring the Root Password on page 245](#)
 - [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)

Example: Changing the Requirements for Junos OS Plain-Text Passwords

This example shows how to set various maximum and minimum requirements for plain-text passwords to increase password strength.

- [Requirements on page 253](#)
- [Overview on page 253](#)
- [Configuration on page 253](#)

Requirements

This example requires a device running Junos 12.2 or greater. The **minimum-length** and **maximum-length** password requirements statements are available in earlier releases, however, you must have Junos OS Release 12.2 or greater to configure **minimum-lower-cases**, **minimum-numeric**s, **minimum-punctuations**, or **minimum-upper-cases**.

Overview

You can use a variety of requirements to strengthen plain-text passwords for greater security. Junos OS provides a number of possible configurations at the **[edit system login password]** hierarchy level that allow you to require users to create plain-text passwords that conform to a particular set of requirements that may include such things as length, number of changes, type of characters, numbers, or letter case.

Configuration

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

```
set system login password minimum-length 12
set system login password maximum-length 22
set system login password minimum-numeric 1
set system login password minimum-upper-cases 1
set system login password minimum-lower-cases 1
set system login password minimum-punctuations 1
```

Configuring Requirements for Plain-Text Passwords

Step-by-Step Procedure This example configures password requirements that require the user to create a password that has a minimum length of 12 characters, a maximum length of 22 characters, and that includes at least one lower-case letter, at least one upper-case letter, at least one punctuation character, and at least one numeric character.

1. Navigate to configuration mode in the **[system login password]** hierarchy level.

```
user@host> edit
[edit]
user@host# edit system login password
```
2. Set a minimum length requirement of 12 characters and a maximum length requirement of 22 characters for user passwords.

```
[edit system login password]
user@host# set minimum-length 12
[edit system login password]
user@host# set maximum-length 22
```
3. Require users to set a password that has at least one lower-case letter and at least one upper-case letter.

```
[edit system login password]
```

```
user@host# set minimum-lower-cases 1
[edit system login password]
user@host# set minimum-upper-cases 1
```

4. Require users to set a password that has at least one punctuation-class character and at least one number.

```
[edit system login password]
user@host# set minimum-punctuations 1
[edit system login password]
user@host# set minimum-numeric 1
```

Results

From configuration mode, confirm your configuration by entering the show command at the edit system login password hierarchy level. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit system login password]
user@host# show
  minimum-length 12;
  maximum-length 22;
  minimum-numeric 1;
  minimum-upper-cases 1;
  minimum-lower-cases 1;
```

- Related Documentation**
- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
 - [password \(Login\) on page 445](#)

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at next logon.

Before you configure MS-CHAPv2 for password-change support, ensure that you have done the following:

- Configured RADIUS server authentication parameters.
- Set the first tried option in the authentication order to RADIUS server.

To configure MS-CHAP-v2, include the following statements at the **[edit system radius-options]** hierarchy level:

```
[edit system radius-options]
  password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
  authentication-order [ radius password ];
  radius-server {
    192.168.69.149 secret "$9$G-j.5Qz6tpBk.1hrlXxUj1q5Qn/C"; ## SECRET-DATA
  }
  radius-options {
    password-protocol mschap-v2;
  }
  login {
    user bob {
      class operator;
    }
  }
}
```

Related Documentation

- *Configuring Access Profiles for L2TP or PPP Parameters*

CHAPTER 7

Configuring Local Password Authentication

- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
- [Changing the Requirements for Junos OS Plain-Text Passwords on page 259](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 260](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)

Special Requirements for Junos OS Plain-Text Passwords

Junos OS has special requirements when you create plain-text passwords on a router or switch. [Table 9 on page 257](#) shows the default requirements.

Table 9: Special Requirements for Plain-Text Passwords

| Junos OS | Junos-FIPS |
|--|--|
| The password must be between 6 and 128 characters long. | FIPS passwords must be between 10 and 20 characters long |
| You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. | You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended. |
| Valid passwords must contain at least one change of case or character class. | Passwords must use at least three of the five defined character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). |

You can change the requirements for plain-text passwords.

Junos OS supports the following five character classes for plain-text passwords:

- Lowercase letters
- Uppercase letters
- Numbers
- Punctuation
- Special characters: ! @ # \$ % ^ & * , + < > ; ;

Control characters are not recommended.

You can include the **plain-text-password** statement at the following hierarchy levels:

- [edit system diag-port-authentication]
- [edit system pic-console-authentication]
- [edit system root-authentication]
- [edit system login user *username* authentication]

The **change-type** statement specifies whether the password is checked for the following:

- The total number of character sets used (**character-set**)
- The total number of character set changes (**set-transitions**)

For example, the following password:

MyPassWd@2

has four character sets (uppercase letters, lowercase letters, special characters, and numbers) and seven character set changes (**M**–**y**, **y**–**P**, **P**–**a**, **s**–**W**, **W**–**d**, **d**–**@**, and **@**–**2**).

The **change-type** statement is optional. If you omit the **change-type** option, Junos-FIPS plain-text passwords are checked for character sets, and Junos OS plain-text passwords are checked for character set changes.

The **minimum-changes** statement specifies how many character sets or character set changes are required for the password. This statement is optional. If you do not use the **minimum-changes** statement, character sets are not checked for Junos OS. If the **change-type** statement is configured for the **character-set** option, then the **minimum-changes** value must be 5 or less, because Junos OS only supports five character sets.

The **format** statement specifies the hash algorithm (**md5**, **sha1**, **sha256**, **sha512** or **des**) for authenticating plain-text passwords. This statement is optional. For Junos OS, the default format is **md5**. For Junos-FIPS, only **sha1** is supported.



NOTE: Starting with Junos OS Release 13.3, the sha1 does not enable secure, protected specification of passwords and we recommend that you do not use the sha1 algorithm to configure passwords. Instead, you can use the sha256 or sha512 to specify passwords by using the 256-bit and 512-bit cryptographic hash algorithm respectively for a robust and reliable operation.

The **maximum-length** statement specifies the maximum number of characters allowed in a password. This statement is optional. By default, Junos OS passwords have no maximum; however, only the first 128 characters are significant. Junos-FIPS passwords must be 20 characters or less. The range for Junos OS maximum-length passwords is from 20 to 128 characters.

The **minimum-length** statement specifies the minimum number of characters required for a password. This statement is optional. By default, Junos OS passwords must be at least 6 characters long, and Junos-FIPS passwords must be at least 10 characters long. The range is from 6 to 20 characters.

Changes to password requirements do not take effect until the configuration is committed. When requirements change, only newly created, plain-text passwords are checked; existing passwords are not checked against the new requirements.

The default configuration for Junos OS plain-text passwords is:

```
[edit system login]
passwords {
  change-type character-sets;
  format md5;
  minimum-changes 1;
  minimum-length 6;
}
```

The default configuration for Junos-FIPS plain-text passwords is:

```
[edit system login]
passwords {
  change-type set-transitions;
  format sha1;
  maximum-length 20;
  minimum-changes 3;
  minimum-length 10;
}
```

- Related Documentation**
- [Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)
 - [Configuring the Root Password on page 245](#)
 - *Changing the Requirements for Junos OS Plain-Text Passwords*
 - *Configuring the Root Password*

Changing the Requirements for Junos OS Plain-Text Passwords

To change the requirements for plain-text passwords, include the **password** statement at the **[edit system login]** hierarchy level:

```
[edit system login]
password {
  change-type (set-transitions | character-set);
  format (md5 | sha1);
  maximum-length length;
  minimum-changes number;
```

```
minimum-length length;  
minimum-lower-cases number;  
minimum-numeric number;  
minimum-punctuations number;  
minimum-upper-cases number;  
}
```



NOTE: These statements apply to plain-text passwords only, not encrypted passwords.

Related Documentation

- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
- [Configuring the Root Password on page 245](#)
- [Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252](#)

Example: Changing the Requirements for Junos OS Plain-Text Passwords

This example shows how to set various maximum and minimum requirements for plain-text passwords to increase password strength.

- [Requirements on page 260](#)
- [Overview on page 260](#)
- [Configuration on page 260](#)

Requirements

This example requires a device running Junos 12.2 or greater. The **minimum-length** and **maximum-length** password requirements statements are available in earlier releases, however, you must have Junos OS Release 12.2 or greater to configure **minimum-lower-cases**, **minimum-numeric**, **minimum-punctuations**, or **minimum-upper-cases**.

Overview

You can use a variety of requirements to strengthen plain-text passwords for greater security. Junos OS provides a number of possible configurations at the **[edit system login password]** hierarchy level that allow you to require users to create plain-text passwords that conform to a particular set of requirements that may include such things as length, number of changes, type of characters, numbers, or letter case.

Configuration

CLI Quick Configuration

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

```
set system login password minimum-length 12  
sset system login password maximum-length 22  
set system login password minimum-numeric 1
```

```
set system login password minimum-upper-cases 1
set system login password minimum-lower-cases 1
set system login password minimum-punctuations 1
```

Configuring Requirements for Plain-Text Passwords

Step-by-Step Procedure

This example configures password requirements that require the user to create a password that has a minimum length of 12 characters, a maximum length of 22 characters, and that includes at least one lower-case letter, at least one upper-case letter, at least one punctuation character, and at least one numeric character.

1. Navigate to configuration mode in the [system login password] hierarchy level.

```
user@host> edit
[edit]
user@host# edit system login password
```
2. Set a minimum length requirement of 12 characters and a maximum length requirement of 22 characters for user passwords.

```
[edit system login password]
user@host# set minimum-length 12
[edit system login password]
user@host# set maximum-length 22
```
3. Require users to set a password that has at least one lower-case letter and at least one upper-case letter.

```
[edit system login password]
user@host# set minimum-lower-cases 1
[edit system login password]
user@host# set minimum-upper-cases 1
```
4. Require users to set a password that has at least one punctuation-class character and at least one number.

```
[edit system login password]
user@host# set minimum-punctuations 1
[edit system login password]
user@host# set minimum-numeric 1
```

Results

From configuration mode, confirm your configuration by entering the show command at the edit system login password hierarchy level. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit system login password]
user@host# show
minimum-length 12;
maximum-length 22;
minimum-numeric 1;
minimum-upper-cases 1;
minimum-lower-cases 1;
```

- Related Documentation**
- [Special Requirements for Junos OS Plain-Text Passwords on page 257](#)
 - [password \(Login\) on page 445](#)

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

To configure the authentication order, include the **authentication-order** statement at the **[edit system]** hierarchy level:

```
[edit system]
authentication-order [ authentication-methods ];
```

Specify one or more of the following authentication methods in the preferred order, from first tried to last tried:

- **radius**—Verify the user using RADIUS authentication services
- **tacplus**—Verify the user using TACACS+ authentication services.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the **[edit system login user]** hierarchy level.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router or switch attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

```
[edit system]
```

```
user@switch# delete authentication-order radius
```

The following example shows how to insert the **tacplus** statement after the **radius** statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

Related Documentation

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)
- [authentication-order on page 373](#)

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see ["Using Local Password Authentication" on page 33](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```



NOTE: For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 280](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class operator;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

- Related Documentation**
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262](#)

CHAPTER 8

Configuring Radius Authentication

- [Configuring RADIUS Authentication on page 267](#)
- [Example: Configuring RADIUS Authentication on page 272](#)
- [Example: Configuring RADIUS Template Accounts on page 273](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 274](#)
- [Configuring RADIUS System Accounting on page 276](#)
- [Example: Configuring RADIUS System Accounting on page 278](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 281](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 282](#)

Configuring RADIUS Authentication

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. As such, the examples shown here are in a configuration group called **global**. Using a configuration group is optional.

- [Configuring Authentication by a RADIUS Server on page 267](#)

Configuring Authentication by a RADIUS Server

To use RADIUS authentication on the router or switch, 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:

To configure authentication by a RADIUS server:

1. Add a server address.
[edit groups global]

```
user@host# edit system radius-server server-address
```

For example:

```
user@host# show groups
global {
  system {
    radius-server {
      192.168.69.162;
    }
  }
}
```

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:

```
user@host# show groups
global {
  system {
    radius-server {
      192.168.69.162 secret "$9$gQ4UHf5F36CiH.5Tz9CuOIhreM8xw2oIENVwgZG";
      ## SECRET-DATA
    }
  }
}
```

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:

```
user@host# show groups
global {
  system {
    radius-server {
      192.168.69.162 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:

```
user@host# show groups
global {
  system {
    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 system user remote class class
```

For example:

```
user@host# show groups
global {
  system {
    user remote {
      class super-user;
    }
  }
}
```

- To have different login classes be used for different RADIUS-authenticated users, granting them different permissions:

1. Create multiple user templates in the Junos OS configuration.

Every user template can be assigned a different login class.

For example:

```
user@host# show groups
global {
  system {
    user RO {
      class read-only;
    }
    user OP {
      class operator;
    }
    user SU {
      class super-user;
    }
    user remote {
      class read-only;
      full-name "default remote access user template";
    }
  }
}
```

2. 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” on page 274](#).

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 login. 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 above 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, *Steel-Belted Radius (SBR) Enterprise*. For information on using FreeRADIUS, <http://kb.juniper.net/InfoCenter/index?page=content&id=KB19446>.

6. If the Junos OS device has several interfaces that can reach the RADIUS server, assign an IP address that the Junos OS can use for all its communication with the RADIUS server. In this example, you choose the address 192.168.0.1:

```
[edit groups global system radius-server server-address]
user@host# set source-address source-address
```

source-address is a valid IP address configured on one of the router or switch interfaces. This sets a fixed address as the source address for locally generated IP packets.

For example:

```
user@host# show groups
global {
  system {
    radius-server {
      192.168.69.162 source-address 196.168.0.1
    }
  }
}
```

7. (Optional) Specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the **timeout** statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the **retry** statement).

By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server 3 times. You can configure this to be a value from 1 through 10 times.

```
[edit groups global system radius-server server-address]
user@host# set retry number
user@host# set timeout seconds
```

For example:

```
user@host# show groups
global {
  system {
    radius-server {
      192.168.68.162 {
        timeout 5;
        retry 4;
      }
    }
  }
}
```

8. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

9. Commit the configuration.

```
user@host# commit
```

10. Verify the configuration of remote authentication server.

If all is correct on the server, you should see the following messages in the system log message file. To use this verification method, you need to first configure system logging.

```
user@host> show log messages
Apr 22 13:38:58 juniper1 sshd[17859]: Accepted password for adminjlk from
172.30.48.10
port 61729 ssh2
```

If the user has no login on the RADIUS server, the message logs include a message that is similar to the following error message:

```
user@host> show log messages
Apr 22 13:40:57 juniper1 sshd[17873]: Failed password for username from
172.30.48.10
port 64844 ssh2
```

You can also show the session connections.

```
user@host> show system connections
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 48 172.16.53.101.22 172.16.48.10.61729 ESTABLISHED
```

Related Documentation

- [Example: Configuring RADIUS Authentication on page 272](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)
- [Juniper Networks Vendor-Specific RADIUS Attributes on page 274](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
- [Example: Configuring RADIUS Template Accounts on page 273](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Junos OS User Authentication Methods on page 30](#)
- [Example: Configuring RADIUS System Accounting on page 278](#)

Example: Configuring RADIUS Authentication

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 all vendors of these systems support RADIUS.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
system {
  authentication-order [ radius password ];
  root-authentication {
```

```

        encrypted-password "$9$aHlj8gqQ1gjyjjhgjgiiii"; # SECRET-DATA
    }
    name-server {
        10.1.1.1;
        10.1.1.2;
    }
}

```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```

[edit]
system {
    radius-server {
        10.1.2.1 {
            secret "$9$aHlj8gqQ1sdjerrhser"; # SECRET-DATA
            timeout 5;
        }
        10.1.2.2 {
            secret "$9$aHlj8gqQ1csdoiuardwefoiud"; # SECRET-DATA
            timeout 5;
        }
    }
}

```

Related Documentation • [Configuring RADIUS Authentication on page 267](#)

Example: Configuring RADIUS Template Accounts

The following example shows how to configure RADIUS template accounts for different users or groups of users:

```

[edit]
system {
    login {
        user observation {
            uid 1001;
            class observation;
        }
        user operation {
            uid 1002;
            class operation;
        }
        user engineering {
            uid 1003;
            class engineering;
        }
    }
}

```

Related Documentation • [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)

Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 10 on page 274](#) lists the Juniper Networks VSAs you can configure.

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes

| Name | Description | Type | Length | String |
|-----------------------------|--|------|--------|---|
| Juniper-Local-User-Name | Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets. | 1 | ≥3 | One or more octets containing printable ASCII characters. |
| Juniper-Allow-Commands | Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 2 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands" on page 66. |
| Juniper-Deny-Commands | Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 3 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands" on page 66. |
| Juniper-Allow-Configuration | Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 4 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 68. |

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

| Name | Description | Type | Length | String |
|------------------------------|---|------|--------|---|
| Juniper-Deny-Configuration | Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets. | 5 | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 68. |
| Juniper-Interactive-Command | Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets. | 8 | ≥3 | One or more octets containing printable ASCII characters. |
| Juniper-Configuration-Change | Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets. | 9 | ≥3 | One or more octets containing printable ASCII characters. |
| Juniper-User-Permissions | <p>Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets.</p> <p>NOTE: When the Juniper-User-Permissions attribute is configured to grant the Junos OS maintenance or all permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p> | 10 | ≥3 | <p>One or more octets containing printable ASCII characters.</p> <p>The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See Table 4 on page 27.</p> |

Table 10: Juniper Networks Vendor-Specific RADIUS Attributes (*continued*)

| Name | Description | Type | Length | String |
|-----------------------------|---|------|-----------------|---|
| Juniper-Authentication-Type | Indicates the authentication method (local database, or RADIUS server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using RADIUS server, the attribute value shows 'remote'. | 11 | ≥5 | One or more octets containing printable ASCII characters. |
| Juniper-Session-Port | Indicates the source port number of the established session. | 12 | size of integer | Integer |

For more information about the VSAs, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.

Related Documentation

- [Configuring RADIUS Authentication on page 267](#)
- [Configuring RADIUS Authentication \(QFX Series or OCX Series\)](#)

Configuring RADIUS System Accounting

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 276](#)
2. [Specifying RADIUS Server Accounting and Auditing Events on page 277](#)
3. [Configuring RADIUS Server Accounting on page 277](#)

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]
events [ events ];
destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        secret password;
        source-address address;
```

```

        retry number;
        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;
    secret password;
    source-address address;
    retry number;
    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 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>;
```

Example: Configuring RADIUS System Accounting

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 $9$dkafeqwrew;
            source-address 10.1.1.1;
            retry 3;
            timeout 3;
          }
          10.6.6.6 secret $9$fe3erqwrez;
          10.7.7.7 secret $9$f34929ftby;
        }
      }
    }
  }
}
```

}

Related Documentation

- [Configuring RADIUS System Accounting on page 276](#)

Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+= "cmd1"
Juniper-Allow-Commands+= "cmd2"
Juniper-Allow-Commands+= "cmdn"
Juniper-Deny-Commands+= "cmd1"
Juniper-Deny-Commands+= "cmd2"
Juniper-Deny-Commands+= "cmdn"
Juniper-Allow-Configuration+= "regex1"
Juniper-Allow-Configuration+= "regex2"
Juniper-Allow-Configuration+= "regexn"
Juniper-Deny-Configuration+= "regex1"
Juniper-Deny-Configuration+= "regex2"
Juniper-Deny-Configuration+= "regexn"
Juniper-User-Permissions+= "permission-flag1"
Juniper-User-Permissions+= "permission-flag2"
Juniper-User-Permissions+= "permission-flagn"
```

For TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1= "cmd1"
allow-commands2= "cmd2"
allow-commandsn= "cmdn"
deny-commands1= "cmd1"
deny-commands2= "cmd2"
deny-commandsn= "cmdn"
allow-configuration1= "regex1"
allow-configuration2= "regex2"
allow-configurationn= "regexn"
```

```
deny-configuration1="regex1"
deny-configuration2="regex2"
deny-configurationn="regexn"
user-permissions1="permission-flag1"
user-permissions2="permission-flag2"
user-permissionsn="permission-flagn "
```

**NOTE:**

- Numeric values 1 to *n* in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```

- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the `show cli authorization` command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see [“Juniper Networks Vendor-Specific RADIUS Attributes” on page 274](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 293](#).



NOTE: When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the `allow-commands`, `deny-commands`, `allow-configuration`, `deny-configuration`, or `permissions` statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

**Related
Documentation**

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)

Overview of Template Accounts for RADIUS and TACACS+ Authentication

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

- Related Documentation**
- [Understanding Remote Authentication Servers on page 31](#)
 - [Configuring Remote Template Accounts for User Authentication on page 52](#)
 - [Configuring Local User Template Accounts for User Authentication on page 50](#)

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

To configure the authentication order, include the **authentication-order** statement at the **[edit system]** hierarchy level:

```
[edit system]
  authentication-order [ authentication-methods ];
```

Specify one or more of the following authentication methods in the preferred order, from first tried to last tried:

- **radius**—Verify the user using RADIUS authentication services
- **tacplus**—Verify the user using TACACS+ authentication services.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the **[edit system login user]** hierarchy level.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router or switch attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
  user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

```
[edit system]
user@switch# delete authentication-order radius
```

The following example shows how to insert the **tacplus** statement after the **radius** statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

Related Documentation

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)
- [authentication-order on page 373](#)

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 33](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
    }
  }
}
```

```

        class operator;
    }
}

```



NOTE: For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 280](#).

When a user logs in to a device, the user’s login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```

[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class operator;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}

```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”

- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

**Related
Documentation**

- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262](#)

CHAPTER 9

Configuring TACACS+ Authentication

- [Configuring TACACS+ Authentication on page 285](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 291](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 293](#)
- [Configuring TACACS+ System Accounting on page 295](#)
- [Configuring TACACS+ Accounting on a TX Matrix Router on page 297](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 297](#)
- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 297](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 299](#)

Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure TACACS+ configuration are:

- [Configuring Authentication by a TACACS+ Server on page 285](#)
- [Configuring the Same Authentication Service for Multiple TACACS+ Servers on page 291](#)

Configuring Authentication by a TACACS+ Server

To configure multiple TACACS+ servers, include multiple **tacplus-server** statements.

On a TX Matrix router, TACACS+ accounting should be configured only under the groups **re0** and **re1**.



NOTE: Accounting should not be configured at the **[edit system]** hierarchy level; on a TX Matrix router, control is done under the switch-card chassis only.

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” on page 280](#).

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including one **tacplus-server** statement at the **[edit system]** hierarchy level for each TACACS+ server:

To configure authentication by a TACACS+ server:

1. Add a server address.

```
[edit groups global]
user@host# edit system tacplus-server server-address
```

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      192.168.69.162;
    }
  }
}
```

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 TACACS+ server.

```
[edit groups global system tacplus-server server-address]
user@host# set secret password
```

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      192.168.69.162 secret "$9$gQ4UHf5F36CiH.5Tz9CuOIhreM8xw2oIENVwgZG";
      ## SECRET-DATA
    }
  }
}
```

3. If necessary, specify a port on which to contact the TACACS+ 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 tacplus-server server-address]
```

```
user@host# set port port-number
```

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      192.168.69.162 port 1845
    }
  }
}
```

4. (Optional) 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.



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.

```
[edit groups global system tacplus-server server-address]
```

```
user@host# set single-connection
```

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      single-connection;
    }
  }
}
```

5. 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:

```
user@host# show groups
global {
  system {
    authentication-order [ radius password tacplus ];
  }
}
```

```
}
```

6. Assign a login class to TACACS+-authenticated users.

You can assign different user templates and login classes to TACACS+-authenticated users. This allows TACACS+-authenticated users to be granted different administrative permissions on the Junos OS device. By default, TACACS+-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 TACACS+ server.

- To use the same permissions for all TACACS+-authenticated users:

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

For example:

```
user@host# show groups
global {
  system {
    user remote {
      class super-user;
    }
  }
}
```

- To have different login classes be used for different TACACS+-authenticated users, granting them different permissions:

1. Create multiple user templates in the Junos OS configuration.

Every user template can be assigned a different login class.

For example:

```
user@host# show groups
global {
  system {
    user RO {
      class read-only;
    }
    user OP {
      class operator;
    }
    user SU {
      class super-user;
    }
    user remote {
      class read-only;
    }
  }
}
```

```

        full-name "default remote access user template";
    }
}

```

2. Configure access privileges for users on a TACACS+ server.

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-configurations = <allow-configuration-regex>
    deny-commands = <deny-commands-regex>
    deny-configuration = <deny-configuration-regex>
    user-permissions = <permission bits in junos>
}

```

This **service** statement can appear in a **user** or **group** statement.

Have the TACACS+ server specify the name of the user template to be applied to the authenticated user.

For a TACACS+ 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 TACACS+ 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 TACACS+ VSAs, see ["Juniper Networks Vendor-Specific TACACS+ Attributes" on page 293](#).

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 login. However, the user inherits the user class from the assigned user template.

7. If the Junos OS device has several interfaces that can reach the TACACS+ server, assign an IP address that the Junos OS can use for all its communication with the TACACS+ server. In this example, you choose the address 192.168.0.1:

```

[edit groups global system tacplus-server server-address]
user@host# set source-address source-address

```

source-address is a valid IP address configured on one of the router or switch interfaces. This sets a fixed address as the source address for locally generated IP packets.

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      192.168.69.162 source-address 196.168.0.1
    }
  }
}
```

8. (Optional) Specify the amount of time that the local router or switch waits to receive a response from a TACACS+ server (in the **timeout** statement).

By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds.

```
[edit groups global system tacplus-server server-address]
user@host# set timeout seconds
```

For example:

```
user@host# show groups
global {
  system {
    tacplus-server {
      192.168.68.162 {
        timeout 5;
      }
    }
  }
}
```

9. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

10. Commit the configuration.

```
user@host# commit
```

11. Verify the configuration of remote authentication server.

If all is correct on the server, you should see the following messages in the system log message file. To use this verification method, you need to first configure system logging.

```
user@host> show log messages
Apr 22 13:38:58 juniper1 sshd[17859]: Accepted password for adminjlk from
172.30.48.10
port 61729 ssh2
```

If the user has no login on the TACACS+ server, the message logs include a message that is similar to the following error message:

```
user@host> show log messages
```

```
Apr 22 13:40:57 juniper1 sshd[17873]: Failed password for username from
172.30.48.10
port 64844 ssh2
```

You can also show the session connections.

```
user@host> show system connections
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 48 172.16.53.101.22 172.16.48.10.61729 ESTABLISHED
```

Configuring the Same Authentication Service for Multiple TACACS+ Servers

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.

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 "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
  10.3.3.3 secret "$9$2dgoJGDiqP5ZG9A"; ## SECRET-DATA
}
tacplus-options {
  service-name bob;
}
```

Related Documentation

- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)
- [Juniper Networks Vendor-Specific TACACS+ Attributes on page 293](#)
- [Overview of Template Accounts for RADIUS and TACACS+ Authentication on page 280](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Junos OS User Authentication Methods on page 30](#)

Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication.

You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

You can specify **allow-configuration**, **deny-configuration**, **allow-commands**, or **deny-commands** in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple **allow-commands** parameters using: **allow-commands= (cmd1 | cmd2 | cmdn)**. You can specify **user-permissions** as a list of comma-separated values, and not as a regular expression.

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for **allow-commands**, **deny-commands**, **allow-configuration**, **deny-configuration**, and **permissions** vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

```
Juniper-Allow-Commands+= "cmd1"
Juniper-Allow-Commands+= "cmd2"
Juniper-Allow-Commands+= "cmdn"
Juniper-Deny-Commands+= "cmd1"
Juniper-Deny-Commands+= "cmd2"
Juniper-Deny-Commands+= "cmdn"
Juniper-Allow-Configuration+= "regex1"
Juniper-Allow-Configuration+= "regex2"
Juniper-Allow-Configuration+= "regexn"
Juniper-Deny-Configuration+= "regex1"
Juniper-Deny-Configuration+= "regex2"
Juniper-Deny-Configuration+= "regexn"
Juniper-User-Permissions+= "permission-flag1"
Juniper-User-Permissions+= "permission-flag2"
Juniper-User-Permissions+= "permission-flagn"
```

For TACACS+ server, specify the individual regular expressions using the following syntax:

```
allow-commands1= "cmd1"
allow-commands2= "cmd2"
allow-commandsn= "cmdn"
deny-commands1= "cmd1"
deny-commands2= "cmd2"
deny-commandsn= "cmdn"
allow-configuration1= "regex1"
allow-configuration2= "regex2"
allow-configurationn= "regexn"
deny-configuration1= "regex1"
deny-configuration2= "regex2"
deny-configurationn= "regexn"
user-permissions1= "permission-flag1"
user-permissions2= "permission-flag2"
user-permissionsn= "permission-flagn "
```

**NOTE:**

- Numeric values 1 to n in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

```
allow-commands1="cmd1"
allow-commands3="cmd3"
allow-commands2="cmd2"
deny-commands3="cmd3"
deny-commands2="cmd2"
deny-commands1="cmd1"
```
- The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.
- When you issue the `show cli authorization` command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see [“Juniper Networks Vendor-Specific RADIUS Attributes” on page 274](#) and [“Juniper Networks Vendor-Specific TACACS+ Attributes” on page 293](#).



NOTE: When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the `allow-commands`, `deny-commands`, `allow-configuration`, `deny-configuration`, or `permissions` statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

Related Documentation

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)

Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 11 on page 293](#) lists the Juniper Networks VSAs you can configure.

Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes

| Name | Description | Length | String |
|------------------------------|--|----------|---|
| <code>local-user-name</code> | Indicates the name of the user template used by this user when logging in to a device. | ≥ 3 | One or more octets containing printable ASCII characters. |

Table 11: Juniper Networks Vendor-Specific TACACS+ Attributes (*continued*)

| Name | Description | Length | String |
|----------------------------|--|-----------------|--|
| allow-commands | Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 7 on page 66 . |
| allow-configuration | Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See "Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies" on page 68 . |
| deny-commands | Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 7 on page 66 . |
| deny-configuration | Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user's login class permission bits. | ≥3 | One or more octets containing printable ASCII characters, in the form of an extended regular expression. See Table 8 on page 68 . |
| user-permissions | <p>Contains information the server uses to specify user permissions.</p> <p>NOTE: When the user-permissions attribute is configured to grant the Junos OS maintenance or all permissions on an IPv4 or IPv6 TACACS+ server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</p> | ≥3 | One or more octets containing printable ASCII characters. See Table 4 on page 27 . |
| authentication-type | Indicates the authentication method (local database, or TACACS+ server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using TACACS+ server, the attribute value shows 'remote'. | ≥5 | One or more octets containing printable ASCII characters. |
| session-port | Indicates the source port number of the established session. | size of integer | Integer |

- Related Documentation**
- [Configuring TACACS+ Authentication on page 285](#)
 - [Configuring TACACS+ Authentication \(QFX Series\)](#)

Configuring TACACS+ System Accounting

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the **[edit system accounting]** hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

Tasks for configuring TACACS+ system accounting are:

1. [Specifying TACACS+ Auditing and Accounting Events on page 295](#)
2. [Configuring TACACS+ Server Accounting on page 295](#)

Specifying TACACS+ Auditing and Accounting Events

To specify the events you want to audit when using a TACACS+ 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 TACACS+ Server Accounting

To configure TACACS+ server accounting, include the **server** statement at the **[edit system accounting destination tacplus]** hierarchy level:

```
[edit system accounting destination tacplus]
server {
  server-address {
    port port-number;
```

```
    secret password;  
    single-connection;  
    timeout seconds;  
  }  
}
```

server-address specifies the IPv4 or IPv6 address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple **server** statements.



NOTE: If no TACACS+ servers are configured at the [edit system accounting destination tacplus] statement hierarchy level, Junos OS uses the TACACS+ servers configured at the [edit system tacplus-server] hierarchy level.

port-number specifies 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 contains spaces, enclose the entire password in quotation marks (" "). The password 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 maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the **single-connection** statement.

To ensure that start and stop requests for accounting of login events are correctly logged in the Accounting file instead of the Administration log file on a TACACS+ server, include either the **no-cmd-attribute-value** statement or the **exclude-cmd-attribute** at the [edit system tacplus-options] hierarchy level.

If you use the **no-cmd-attribute-value** statement, the value of the **cmd** attribute is set to a null string in the start and stop requests. If you use the **exclude-cmd-attribute** statement, the **cmd** attribute is totally excluded from the start and stop requests. Both statements support the correct logging of accounting requests in the Accounting file, instead of the Administration file.

```
[edit system tacplus-options]  
(no-cmd-attribute-value | exclude-cmd-attribute);
```

If you use the **enhanced-accounting** statement at the [edit system tacplus-options] hierarchy level, the TACACS+ 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 tacplus-options]  
enhanced-accounting;
```

```
[edit system accounting]
enhanced-avs-max <number>;
```

- Related Documentation**
- [Configuring TACACS+ Accounting on a TX Matrix Router on page 297](#)
 - [Configuring TACACS+ Authentication on page 285](#)

Configuring TACACS+ Accounting on a TX Matrix Router

On a TX Matrix router, TACACS+ accounting should be configured only under the groups `re0` and `re1`.



NOTE: Accounting should *not* be configured at the `[edit system]` hierarchy; on a TX Matrix router, control is done under the switch-card chassis only.

- Related Documentation**
- [Configuring TACACS+ System Accounting on page 295](#)

Overview of Template Accounts for RADIUS and TACACS+ Authentication

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

- Related Documentation**
- [Understanding Remote Authentication Servers on page 31](#)
 - [Configuring Remote Template Accounts for User Authentication on page 52](#)
 - [Configuring Local User Template Accounts for User Authentication on page 50](#)

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the **authentication-order** statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

To configure the authentication order, include the **authentication-order** statement at the `[edit system]` hierarchy level:

```
[edit system]
authentication-order [ authentication-methods ];
```

Specify one or more of the following authentication methods in the preferred order, from first tried to last tried:

- **radius**—Verify the user using RADIUS authentication services
- **tacplus**—Verify the user using TACACS+ authentication services.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the **[edit system login user]** hierarchy level.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router or switch attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as **tacplus** or **password** are configured along with **radius**, the next authentication method is tried.

The following example shows how to configure **radius** and **password** authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the **radius** statement from the authentication order:

```
[edit system]
user@switch# delete authentication-order radius
```

The following example shows how to insert the **tacplus** statement after the **radius** statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

Related Documentation

- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32](#)
- [Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands on page 279](#)
- [Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication on page 263](#)
- [authentication-order on page 373](#)

Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication method and allowed access to the router or switch. For more information about the password authentication method, see [“Using Local Password Authentication” on page 33](#).

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```



NOTE: For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see [“Overview of Template Accounts for RADIUS and TACACS+ Authentication” on page 280](#).

When a user logs in to a device, the user's login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the **[edit system login user]** hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the **edit system login user remote** hierarchy level. The remote template account serves as a default template user account for all users that

are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user operator {
      full-name "All operators";
      uid 9990;
      class operator;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```

Assume your RADIUS server is configured with the following information:

- User Philip with password “olympia”
- User Alexander with password “bucephalus” and username “operator”
- User Darius with password “redhead” and username “operator”
- User Roxane with password “athena”

Philip would be given access as a superuser (**super-user**) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

**Related
Documentation**

- [Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262](#)

CHAPTER 10

Configuring DHCP Access Service for IP Address Management

- [DHCP Access Service Overview on page 302](#)
- [DHCP Statement Hierarchy and Inheritance on page 305](#)
- [Configuring Address Pools for DHCP Dynamic Bindings on page 307](#)
- [Configuring Manual \(Static\) DHCP Bindings Between a Fixed IP Address and a Client MAC Address on page 308](#)
- [Specifying DHCP Lease Times for IP Address Assignments on page 310](#)
- [Configuring a DHCP Boot File and DHCP Boot Server on page 310](#)
- [Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication on page 311](#)
- [Configuring a Static IP Address as DHCP Server Identifier on page 312](#)
- [Configuring a Domain Name and Domain Search List for a DHCP Server Host on page 312](#)
- [Configuring Routers Available to the DHCP Client on page 313](#)
- [Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server on page 314](#)
- [Example: Complete DHCP Server Configuration on page 315](#)
- [Example: Viewing DHCP Bindings on page 316](#)
- [Example: Viewing DHCP Address Pools on page 317](#)
- [Example: Viewing and Clearing DHCP Conflicts on page 317](#)
- [Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317](#)
- [Configuring Tracing Operations for DHCP Processes on page 318](#)
- [DHCP Processes Tracing Flags on page 321](#)
- [Configuring the Router as an Extended DHCP Local Server on page 322](#)
- [Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 324](#)
- [Extended DHCP Local Server and Address-Assignment Pools on page 324](#)
- [Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use on page 325](#)

- [Default Options Provided by the Extended DHCP Server for the DHCP Client on page 326](#)
- [Using External AAA Authentication Services to Authenticate DHCP Clients on page 326](#)
- [Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client on page 331](#)
- [Example: Configuring the Minimum Extended DHCP Local Server Configuration on page 332](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 332](#)
- [Verifying and Managing the DHCP Server Configuration on page 332](#)
- [Tracing Extended DHCP Local Server Operations on page 333](#)

DHCP Access Service Overview

DHCP access service consists of two components: a protocol for delivering host-specific configuration information from a server to a client host and a method for allocating network addresses to a client host. The client sends a message to request configuration information. A DHCP server sends the configuration information back to the client.

With DHCP, clients can be assigned a network address for a fixed *lease*, enabling serial reassignment of network addresses to different clients. A DHCP server leases IP addresses for specific times to various clients. If a client does not use its assigned address for some period of time, the DHCP server can assign that IP address to another host. When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The DHCP server includes IPv4 address assignment and commonly used DHCP options. The server is compatible with DHCP servers from other vendors on the network. The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The Junos-FIPS software does not support the DHCP server.



NOTE: You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.

The following topics describe these concepts in detail:

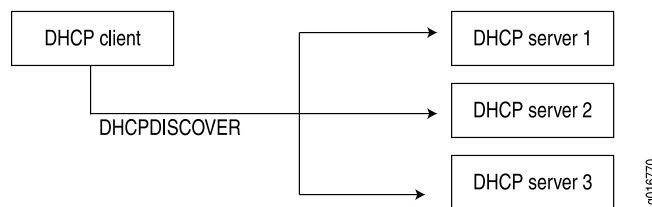
- [Network Address Assignments \(Allocating a New Address\) on page 303](#)
- [Network Address Assignments \(Reusing a Previously Assigned Address\) on page 304](#)
- [Static and Dynamic Bindings on page 305](#)
- [Compatibility with Autoinstallation on page 305](#)
- [Conflict Detection and Resolution on page 305](#)

Network Address Assignments (Allocating a New Address)

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.

1. When a client computer is started, it broadcasts a **DHCPDISCOVER** message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

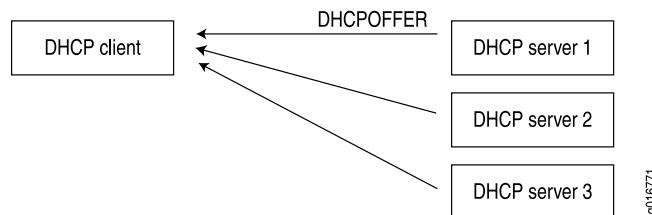
Figure 1: DHCP Discover



NOTE: For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes **DHCPDISCOVER** messages even if the overload options in the messages are not properly terminated with an end statement.

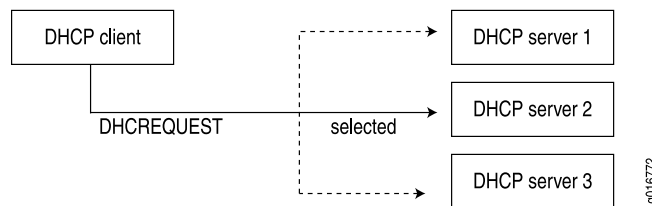
2. Each DHCP server receiving the broadcast sends a **DHCPOFFER** message to the client, offering an IP address for a set period of time, known as the lease period.

Figure 2: DHCP Offer



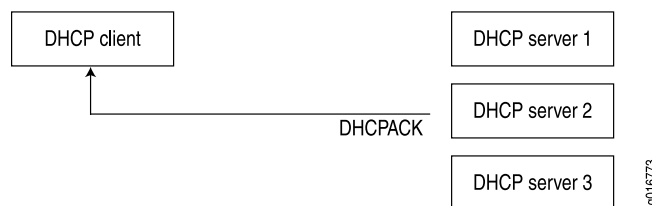
3. The client receives one or more **DHCPOFFER** messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.
4. The client broadcasts a **DHCPREQUEST** message indicating the client has selected an offered leased IP address and identifies the selected server.

Figure 3: DHCP Request



5. Those servers not selected by the **DHCPREQUEST** message return the unselected IP addresses to the pool of available addresses.
6. The selected DHCP server sends a **DHCPACK** acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

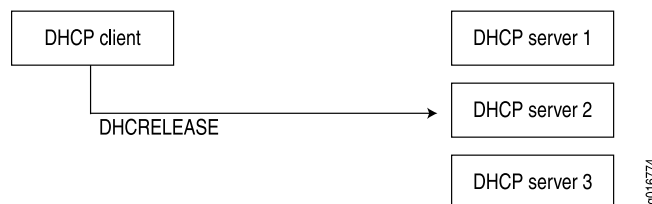
Figure 4: DHCP ACK



The information offered by the server is configurable.

7. The client receives the **DHCPACK** message with configuration information. The process is complete. The client is configured and has access to the network.
 - If the client receives a **DHCPNAK** message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.
 - The client can relinquish its lease on a network address by sending a **DHCPRELEASE** message to the server (for example, when the client is restarted). When the server receives the **DHCPRELEASE** message, it marks the lease as free and the IP address becomes available again.

Figure 5: DHCP Release



Network Address Assignments (Reusing a Previously Assigned Address)

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a **DHCPREQUEST** message on the local subnet.

2. The server with knowledge of the client's configuration responds with a **DHCPACK** message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.

Static and Dynamic Bindings

DHCP supports both dynamic and static bindings. For dynamic bindings, IP addresses are assigned to clients from a pool of addresses. Static bindings provide configuration information for a specific client and can include one or more fixed IP addresses for the client. You can configure a DHCP server to include both address pools and static bindings. For any individual client, static bindings take priority over address pools.

Compatibility with Autoinstallation

The DHCP server is compatible with the autoinstallation feature on J Series Services Routers. The server automatically checks autoinstallation settings for conflicts and gives autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes priority over an IP address set by the DHCP server.



NOTE: The autoinstallation feature includes a fixed address pool and a fixed lease time. With DHCP, you can create address pools and modify lease times.

Conflict Detection and Resolution

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the **clear system services dhcp conflict** command.

Related Documentation

- [DHCP Statement Hierarchy and Inheritance on page 305](#)

DHCP Statement Hierarchy and Inheritance

DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients. See [Table 12 on page 306](#).

The **pool** and **static-binding** statements appear at the **[edit system services dhcp]** hierarchy level. You can include the remaining statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
```

[edit system services dhcp static-binding]

Table 12: Pool and Binding Statements

| Statement | Description | Hierarchy Level |
|-----------------------------|---|-----------------------------|
| <code>pool</code> | Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool. | [edit system services dhcp] |
| <code>static-binding</code> | Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address. | |

To minimize configuration changes, include common configuration statements shown in [Table 13 on page 307](#) (for example, the **domain-name** statement) at the highest applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the [edit system services dhcp] and [edit system services dhcp pool] hierarchy levels, the value assigned to the statement at the [edit system services dhcp pool] level takes priority.

Table 13: Common Configuration Statements

| Statement | Description | Hierarchy Level |
|---------------------------------|---|---|
| <code>boot-file</code> | Set the boot filename advertised to clients. The client uses the boot image stored in the boot file to complete configuration. | [edit system services dhcp] [edit system services dhcp pool] [edit system services dhcp static-binding] |
| <code>boot-server</code> | Set the server that contains the boot file. | |
| <code>default-lease-time</code> | Set the default lease time assigned to any client that does not request a specific lease time. | |
| <code>domain-name</code> | Configure the name of the domain in which clients will search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. | |
| <code>domain-search</code> | Define a domain search list. | |
| <code>maximum-lease-time</code> | Set the maximum lease time allowed by the server. | |
| <code>name-server</code> | Specify the DNS server that maintains the database of client name to IP address mappings. | |
| <code>option</code> | Configure user-defined DHCP options. | |
| <code>router</code> | Specify IP address for routers on the client's subnetwork. Routers are listed in order of preference. | |
| <code>server-identifier</code> | Set the IP address of the DHCP server. | |

Related Documentation

- [DHCP Access Service Overview on page 302](#)

Configuring Address Pools for DHCP Dynamic Bindings

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet.

To configure an address pool, include the following statements at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
```

```
pool address</prefix-length> {  
    address-range {  
        low address;  
        high address;  
    }  
    exclude-address {  
        address;  
    }  
}
```

The pool definition must include the client subnet number and prefix length (in bits). Optionally, the definition can include an address range and a list of excluded addresses.

The **address-range** statement defines the lowest and highest IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

The **exclude-address** statement specifies addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit system services dhcp]  
pool 10.3.3.0/24 {  
    address-range low 10.3.3.2 high 10.3.3.254;  
    exclude-address {  
        10.3.3.33;  
    }  
}
```

For dynamic address assignment, configure an address pool for each client subnet the DHCP server supports. You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.

DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the **DHCPDISCOVER** packet is received. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

- Related Documentation**
- [DHCP Access Service Overview on page 302](#)
 - [Configuring Manual \(Static\) DHCP Bindings Between a Fixed IP Address and a Client MAC Address on page 308](#)

Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

To configure static bindings, include the following statements at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
static-binding mac-address {
  fixed-address {
    address;
  }
  host client-hostname;
  client-identifier (ascii client-id | hexadecimal client-id);
}
```

A static binding defines a mapping between a fixed IP address and the client's MAC address.

The *mac-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The **fixed-address** statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The **host** statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the **domain-name** statement.

The **client-identifier** statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.



NOTE: For each unique client-identifier *client-id* value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect client-identifier *client-id* value, the DHCP server did not issue a lease.

The following is an example of a static binding configuration:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
  fixed-address {
    10.5.5.5;
    10.6.6.6;
  }
  host-name "another-host.domain.tld";
  client-identifier hexadecimal 01001122aabbcc;
}
```

Related Documentation

- [DHCP Access Service Overview on page 302](#)
- [Specifying DHCP Lease Times for IP Address Assignments on page 310](#)

Specifying DHCP Lease Times for IP Address Assignments

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure lease times, include the **maximum-lease-time** and **default-lease-time** statements:

```
maximum-lease-time;  
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]  
[edit system services dhcp pool]  
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the **[edit system services dhcp]** hierarchy level.

The **maximum-lease-time** statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.



NOTE: Maximum lease times do not apply to dynamic BOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.

The following example shows a configuration for maximum and default lease times:

```
[edit system services dhcp]  
maximum-lease-time 7200;  
default-lease-time 3600;
```

Related Documentation

- [DHCP Access Service Overview on page 302](#)
- [Configuring a DHCP Boot File and DHCP Boot Server on page 310](#)

Configuring a DHCP Boot File and DHCP Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the **boot-file** and **boot-server** statements:

```
boot-file filename;  
boot-server (address | hostname);
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
```

```
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

After a client receives a **DHCPOFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnet.

The **boot-file** statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The **boot-server** statement configures the IP address of the TFTP server that contains the client's initial boot file. You must configure an IP address or a hostname for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the **[edit system services dhcp]** hierarchy level.

The following example specifies a boot file and server for an address pool:

```
[edit system services dhcp]
pool 10.4.4.0/24 {
  boot-file "boot.client";
  boot-server 10.4.4.1;
}
```

Related Documentation

- [DHCP Access Service Overview on page 302](#)
- [Configuring a Static IP Address as DHCP Server Identifier on page 312](#)

Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication

On J Series Services Routers, you can configure the next DHCP server to contact after a DHCP boot client establishes initial communication. You can use this option to specify the IP address of the DHCP server that is used as the "siaddr" in a DHCP protocol packet.

To configure the next server, include the **next-server** *next-server* statement at one of the following hierarchy levels:

- **[edit system services dhcp]**
- **[edit system services dhcp pool *pool-id*]**
- **[edit system services dhcp static-binding *mac-address*]**

```
[edit system services dhcp]
next-server next-server;
```

```
[edit system services dhcp pool pool-id]
next-server next-server;
```

```
[edit system services dhcp static-binding mac-address]  
next-server next-server;
```

Related Documentation

- [next-server on page 435](#)

Configuring a Static IP Address as DHCP Server Identifier

The host running the DHCP server must itself use a manually assigned, static IP address. It cannot send a request and receive an IP address from itself or another DHCP server.

To configure a DHCP server identifier, include the **server-identifier** statement:

```
server-identifier address;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]  
[edit system services dhcp pool]  
[edit system services dhcp static-binding]
```

The **server-identifier** statement specifies the IP address of the DHCP server. The host must be a TFTP server that is accessible by all clients served within a range of IP addresses (based on either an address pool or static binding).

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]  
pool 10.3.3.0/24 {  
  address-range low 10.3.3.2 high 10.3.3.254;  
  exclude-address {  
    10.3.3.33;  
  }  
  router {  
    10.3.3.1;  
  }  
  server-identifier 10.3.3.1;  
}
```

Related Documentation

- [DHCP Access Service Overview on page 302](#)

Configuring a Domain Name and Domain Search List for a DHCP Server Host

To configure the name of the domain in which clients search for a DHCP server host, include the **domain-name** statement:

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]  
[edit system services dhcp pool]  
[edit system services dhcp static-binding]
```

The **domain-name** statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

To configure a domain search list, include the **domain-search** statement:

```
domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **domain-search** statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The **domain-search** statement is optional, if you do not configure a domain search list, the default is the client's current domain.

Related Documentation

- [DHCP Access Service Overview on page 302](#)

Configuring Routers Available to the DHCP Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the **router** statement:

```
router {
  address;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The **router** statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the **[edit system services dhcp]** hierarchy level:

```
[edit system services dhcp]
router {
  10.6.6.1;
  10.7.7.1;
}
```

Related Documentation • [DHCP Access Service Overview on page 302](#)

Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the **option** statement:

```
option {  
  [ (id-number option-type option-value) | (id-number array option-type option-value) ];  
}
```

The **option** statement specifies the following values:

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: **byte**, **byte-stream**, **flag**, **integer**, **ip-address**, **short**, **string**, **unsigned-integer**, **unsigned-short**.
- *array*—An option can include an array of values.
- *option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an **On** or **Off** value for a **flag** type).

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]  
[edit system services dhcp pool]  
[edit system services dhcp static-binding]
```

The following example shows user-defined DHCP options:

```
[edit system services dhcp]  
option 19 flag off; # 19: "IP Forwarding" option  
option 40 string "domain.tld"; # 40: "NIS Domain" option  
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined **option 3 router** statement and uses the **router** statement instead:

```
[edit system services dhcp]  
option 3 router 10.7.7.2; # 3: "Default Router" option  
router {  
  10.7.7.1;  
}
```

Related Documentation • [DHCP Access Service Overview on page 302](#)

Example: Complete DHCP Server Configuration

This topic shows a complete DHCP server configuration with address pools, static bindings, and user-defined options.

The following example shows statements at the **[edit interfaces]** hierarchy level. The interface's primary address (10.3.3.1/24) has a corresponding address pool (10.3.3.0/24) defined at the **[edit system services]** hierarchy level.

```
[edit interfaces]
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.3.3.1/24;
    }
  }
}
```



NOTE: You can configure a DHCP server only on an interface's primary IP address.

Statements at the **[edit system services]** hierarchy level include the following:

```
[edit system services]
dhcp {
  domain-name "domain.tld";
  maximum-lease-time 7200;
  default-lease-time 3600;
  name-server {
    10.6.6.6;
    10.6.6.7;
  }
  domain-search [ subnet1.domain.tld subnet2.domain.tld ];
  wins-server {
    10.7.7.7;
    10.7.7.9;
  }
  router {
    10.6.6.1;
    10.7.7.1;
  }
  option 19 flag off; # 19: "IP Forwarding" option
  option 40 string "domain.tld"; # 40: "NIS Domain" option
  option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
  pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
    exclude-address {
      10.3.3.33;
    }
    router {
      10.3.3.1;
    }
  }
}
```

```
server-identifier 10.3.3.1;
}
pool 10.4.4.0/24 {
  boot-file "boot.client";
  boot-server 10.4.4.1;
}
static-binding 00:0d:56:f4:20:01 {
  fixed-address 10.4.4.4;
  host-name "host.domain.tld";
}
static-binding 00:0d:56:f4:01:ab {
  fixed-address {
    10.5.5.5;
    10.6.6.6;
  }
  host-name "another-host.domain.tld";
  client-identifier "01aa.001a.bc65.3e";
}
}
```

Example: Viewing DHCP Bindings

Use the CLI command **show system services dhcp binding** to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding
IP Address      Hardware Address    Type    Lease expires at
192.168.1.2     00:a0:12:00:12:ab   static   never
192.168.1.3     00:a0:12:00:13:02   dynamic  2004-05-03 13:01:42 PDT
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
IP address      192.168.1.3
Hardware address 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00
3a 31 33 3a 30 32
Lease information:
Type           dynamic
Obtained at    2004-05-02 13:01:42 PDT
Expires at     2004-05-03 13:01:42 PDT
```

Use the **detail** option to show detailed binding information:

```
user@host> show system services dhcp binding detail
DHCP binding information:
IP address      192.168.1.3
Hardware address 00:a0:12:00:12:ab
Pool            192.168.1.0/24
Interface       fe-0/0/0, relayed by 192.168.4.254
Lease information:
Type            dynamic
Obtained at     2004-05-02 13:01:42 PDT
```

```
Expires at                2004-05-03 13:01:42 PDT
DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off
```

Example: Viewing DHCP Address Pools

Use the CLI **show system services dhcp pool** command to view information about DHCP address pools.

The following example shows address pools configured on a DHCP server:

```
user@ host> show system services dhcp pool
Pool name      Low address    High address    Excluded addresses
10.40.1.0/24    10.40.1.1      10.40.1.254     10.40.1.254
```

Example: Viewing and Clearing DHCP Conflicts

When the DHCP server provides an IP address, the client performs an ARP check to make sure the address is not being used by another client and reports any conflicts back to the server. The server keeps track of addresses with conflicts and removes them from the address pool. Use the CLI command **show system services dhcp conflict** to show conflicts.

```
user@host> show system services dhcp conflict
Detection time      Detection method    Address
2004-08-03 19:04:00 PDT    client      192.168.1.5
2004-08-04 04:23:12 PDT    ping        192.168.1.8
```

Use the **clear system services dhcp conflicts** command to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```

For more information about CLI commands you can use with the DHCP server, see the [CLI Explorer](#).

Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers

The Dynamic Host Configuration Protocol (DHCP) server provides a framework for passing configuration information to client hosts (such as PCs) on a TCP/IP network. On J Series Services Routers and EX Series switches, a router, switch, or interface that acts as a DHCP server can allocate network IP addresses and deliver configuration settings to client hosts without user intervention. DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup. You do not have to manually create and maintain IP address assignments for clients. DHCP is defined in RFC 2131, *Dynamic Host Configuration Protocol*.

A J Series router or EX Series switch configured as a DHCP server is compatible with the autoinstallation feature.

To configure a J Series router or EX Series switch to accept DHCP as an access service, include the **dhcp** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
dhcp {
  boot-file filename;
  boot-server (address | hostname);
  domain-name domain-name;
  domain-search [domain-list];
  default-lease-time;
  maximum-lease-time;
  name-server {
    address;
  }
  option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
  }
  pool address/prefix-length {
    address-range {
      low address;
      high address;
    }
    exclude-address {
      address;
    }
  }
  router {
    address;
  }
  static-binding mac-address {
    fixed-address {
      address;
    }
    host-name hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
  }
  server-identifier address;
  wins-server {
    address;
  }
}
```

- Related Documentation**
- [DHCP Access Service Overview on page 302](#)
 - [DHCP Statement Hierarchy and Inheritance on page 305](#)

Configuring Tracing Operations for DHCP Processes

DHCP tracing operations track all DHCP operations and record them to a log file. By default, no DHCP processes are traced. If you include the **traceoptions** statement at the **[edit system services dhcp]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **dhcpcd** located in the **/var/log** directory.
- When the file **dhcpcd** reaches 128 kilobytes (KB), it is renamed **dhcpcd.0**, then **dhcpcd.1**, and so on, until there are three trace files. Then the oldest trace file (**dhcpcd.2** is

overwritten). For more information about how log files are created, see the *Junos OS System Log Messages Reference*.

- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable |
no-world-readable>;
flag {
  all;
}
```

Tasks for configuring DHCP tracing operations are:

1. [Configuring the DHCP Processes Log Filename on page 319](#)
2. [Configuring the Number and Size of DHCP Processes Log Files on page 319](#)
3. [Configuring Access to the DHCP Log File on page 320](#)
4. [Configuring a Regular Expression for Refining the Output of DHCP Logged Events on page 320](#)
5. [Configuring DHCP Trace Operation Events on page 320](#)

Configuring the DHCP Processes Log Filename

By default, the name of the file that records trace output is **dhcpd**. You can specify a different name by including the file statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file filename;
```

Configuring the Number and Size of DHCP Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **filename.0**, then **filename.1**, and so on, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**filename**) reaches 2 MB, **filename** is renamed **filename.0**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0** is renamed **filename.1** and **filename** is renamed **filename.0**. This process repeats until there are 20 trace files. Then the oldest file (**filename.19**) is overwritten by the newest file (**filename.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable** statement at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit system services dhcp traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Refining the Output of DHCP Logged Events

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the **[edit system services dhcp traceoptions file filename]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

Configuring DHCP Trace Operation Events

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the **[edit system services dhcp traceoptions]** hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
  all;
  binding;
  config;
  conflict;
  event;
  ifdb;
  io;
  lease;
  main;
  misc;
  packet;
  options;
  pool;
  protocol;
  rtsock;
  scope;
  signal;
  trace;
```

```

    ui;
}

```

DHCP Processes Tracing Flags

Table 14 on page 321 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

Table 14: DHCP Processes Tracing Flags

| Flag | Operation or Event |
|-----------------|---|
| all | All operations. |
| binding | Binding operations. |
| config | Logins to the configuration database. |
| conflict | Client-detected conflicts for IP addresses. |
| event | Important events. |
| ifdb | Interface database operations. |
| io | I/O operations. |
| lease | Lease operations. |
| main | Main loop operations. |
| misc | Miscellaneous operations. |
| packet | DHCP packets. |
| options | DHCP options. |
| pool | Address pool operations. |
| protocol | Protocol operations. |
| rtsock | Routing socket operations. |
| scope | Scope operations. |
| signal | DHCP signal operations. |
| trace | Tracing operations. |
| ui | User interface operations. |

Configuring the Router as an Extended DHCP Local Server

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router 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. See *Configuring Address-Assignment Pools* for details about creating and using address-assignment pools.



NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the **dhcp-local-server** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
```

```

    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
}
interface interface-name <upto upto-interface-name> <exclude>;
}
pool-match-order {
  ip-address-first;
  option-82;
}
}

```

You can also include these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* system services]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]
- [edit routing-instances *routing-instance-name* system services]

In addition, you can configure tracing for DHCP local server operations by including the **traceoptions** statement at the [edit system processes dhcp-service] hierarchy level:

```

[edit system processes]
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;
}

```



NOTE: The extended DHCP local server is incompatible with the J Series router DHCP server. As a result, the DHCP local server and the DHCP or BOOTP relay agent cannot both be enabled on the router at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

Related Documentation

- [Example: Configuring the Minimum Extended DHCP Local Server Configuration on page 332](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 332](#)

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, 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 that will 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 also installs the host route and ARP entry, and then monitors the lease state.

Extended DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router 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. See *Configuring Address-Assignment Pools* for details about creating and using address-assignment pools.



NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client. By default, the server matches the IP address in the client DHCP request to the address of the address-assignment pool.

The following sections describe the methods used by the DHCP local server to determine which address-assignment pool to use:

- [Matching the Client IP Address to the Address-Assignment Pool on page 325](#)
- [Matching Option 82 Information to Named Address Ranges on page 325](#)

Matching the Client IP Address to the Address-Assignment Pool

In the default configuration, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

Matching Option 82 Information to Named Address Ranges

You can also configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool. To use the DHCP local server option 82 matching feature, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.



NOTE: To enable the option 82 matching method, you must first specify the **ip-address-first** statement in the **pool-match-order** statement, and then specify the **option-82** statement.

Default Options Provided by the Extended DHCP Server for the DHCP Client

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

Using External AAA Authentication Services to Authenticate DHCP Clients

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.



NOTE: This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the **authentication-server** statement at the **[edit access profile profile-name]** hierarchy level.

Tasks for configuring External AAA authentication services are:

1. [Configuring Authentication Support for an Extended DHCP Application on page 327](#)
2. [Grouping Interfaces with Common DHCP Configurations on page 328](#)
3. [Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service on page 329](#)
4. [Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service on page 329](#)

Configuring Authentication Support for an Extended DHCP Application

To configure authentication support for an extended DHCP application, include the **authentication** statement at these hierarchy levels. You can configure either global authentication support or group-specific support.

You must configure the **username-include** statement to enable the use of authentication. The **password** statement is not required and does not cause DHCP to use authentication if the **username-include** statement is not included.

Extended DHCP local server hierarchies:

- [edit system services dhcp-local-server]
- [edit system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server]
- [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*]

Extended DHCP relay agent hierarchies:

- [edit forwarding-options dhcp-relay]
- [edit forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]
- [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name*]

```
authentication {  
  password password-string;  
  username-include {  
    circuit-type;  
    delimiter delimiter-character;  
    domain-name domain-name-string;  
    logical-system-name;  
    mac-address;  
    option-60;  
    option-82 <circuit-id> <remote-id>;  
    routing-instance-name;  
    user-prefix user-prefix-string;  
  }  
}
```

Grouping Interfaces with Common DHCP Configurations

The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

To configure an interface group, use the **group** statement.

```
group group-name {  
  authentication {  
    password password-string;  
    username-include {  
      circuit-type;  
      delimiter delimiter-character;  
      domain-name domain-name-string;  
      logical-system-name;  
      mac-address;  
      option-60;  
      option-82 <circuit-id> <remote-id>;  
      routing-instance-name;  
      user-prefix user-prefix-string;  
    }  
  }  
  interface interface-name <upto upto-interface-name> <exclude>;  
}
```

You can specify the names of one or more interfaces on which the extended DHCP application 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. For example:

```
group boston {  
  interface 192.168.10.1;  
  interface 192.168.15.5;  
}
```

You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
  interface 192.168.10.1 upto 192.168.10.255;
}
```

You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
  interface 192.168.100.1 exclude;
  interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username, use the **password** statement. See “[Special Requirements for Junos OS Plain-Text Passwords](#)” on page 257 for information about supported characters in passwords. For example:

```
authentication {
  password myPassword1234;
}
```

Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service

You can configure the extended DHCP application to include additional fields in the username passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.



NOTE: No authentication is performed if you do not include a username in the authentication configuration; however, the IP address is provided by the local pool if it is configured.

To configure unique usernames, use the **username-include** statement. You can include any or all of the additional statements.

```
authentication {
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
  }
}
```

```
    routing-instance-name;  
    user-prefix user-prefix-string;  
  }  
}
```

The following list describes the attributes that can be included as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as string. The router adds the @ delimiter to the username.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of format **xxxx.xxxx.xxxx**.
- **option-60**—The portion of the option 60 payload that follows the length field.
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload.
 - **circuit-id**—The payload of the agent circuit ID suboption.
 - **remote-id**—The payload of the Agent Remote ID suboption.
 - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
 - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter. The default delimiter is a period (.). You can specify a different delimiter; however, the semicolon character (;) is not allowed.

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]  
routing-instance-name[delimiter]circuit-type[delimiter]option-82[delimiter]  
option-60@domain-name
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {  
  username-include {  
    circuit-type;  
    domain-name isp55.com;  
    mac-address;  
    user-prefix wallybrown;  
  }  
}
```

The resulting unique username is:

wallybrown.0090.1a01.1234.enet@isp55.com

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following list shows the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

- Client IP address—RADIUS attribute 8, Framed-IP-Address
- Subnet mask for client IP address (DHCP option 1)—RADIUS attribute 9, Framed-IP-Netmask
- Primary domain server (DHCP option 6)—VSA 26-4, Primary-DNS
- Secondary domain server (DHCP option 6)—VSA 26-5 Secondary-DNS
- Primary WINS server (DHCP option 44)—VSA 26-6, Primary-WINS
- Secondary WINS server (DHCP option 44)—VSA 26-7, Secondary-WINS
- Address assignment pool name—RADIUS attribute 88, Framed-Pool
- Lease time—RADIUS attribute 27, Session-Timeout
- DHCP relay server—VSA 26-109, DHCP-Guided-Relay-Server

Example: Configuring the Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first**.

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
    interface fe-0/0/2.1;
  }
  group group_two {
    interface fe-0/0/3.0;
    interface fe-0/0/3.1;
  }
  pool-match-order {
    ip-address-first;
    option-82;
  }
}
```

Verifying and Managing the DHCP Server Configuration

To display the client address bindings for the extended DHCP local server, use the following operational commands:

- **show dhcp server binding**
- **show dhcp server statistics**

To clear client address bindings and DHCP local server statistics, use the following operational commands:

- **clear dhcp server binding**

- **clear dhcp server statistics**

For information about using these operations commands, see the *Junos System Basics and Services Reference*.

Tracing Extended DHCP Local Server Operations

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are traced. If you include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called **jdhcpd** located in the **/var/log** directory.
- When the file **jdhcpd** reaches 128 kilobytes (KB), it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten. For more information about how log files are created, see the *Junos System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.



NOTE: In software releases earlier than Junos OS 11.4, you configured tracing statements at the **[edit system services dhcp-local-server]** and **[edit forwarding-options dhcp-relay]** hierarchy levels. Starting in Junos OS Release 11.4, these statements have been deprecated and hidden in favor of a new statement at the **[edit system processes dhcp-service]** hierarchy level. The deprecated statements may be removed from a future release; we recommend that you transition to the new statement.

To trace DHCP local server operations, include the **traceoptions** statement at the **[edit system processes dhcp-service]** hierarchy level:

```
traceoptions {
  file filename <files number> <match regular-expression> <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

The following topics describe the tracing operation configuration statements:

1. [Configuring the Filename of the Extended DHCP Local Server Processes Log on page 334](#)
2. [Configuring the Number and Size of Extended DHCP Local Server Processes Log Files on page 334](#)
3. [Configuring Access to the Log File on page 334](#)
4. [Configuring a Regular Expression for Lines to Be Logged on page 334](#)
5. [Configuring Trace Option Flags on page 335](#)

Configuring the Filename of the Extended DHCP Local Server Processes Log

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the **file** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename;
```

Configuring the Number and Size of Extended DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**jdhcpd**) reaches 2 MB, **jdhcpd** is renamed **jdhcpd.0**, and a new file called **jdhcpd** is created. When the new **jdhcpd** reaches 2 MB, **jdhcpd.0** is renamed **jdhcpd.1** and **filename** is renamed **jdhcpd.0**. This process repeats until there are 20 trace files. Then the oldest file (**jdhcpd.19**) is overwritten by the newest file (**jdhcpd.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the **file no-world-readable** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit system processes dhcp-service traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes dhcp-service traceoptions]  
file filename match regex;
```

Configuring Trace Option Flags

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the **[edit system processes dhcp-service traceoptions]** hierarchy level:

```
[edit system processes dhcp-service traceoptions]  
flag flag;
```

You can configure the following tracing flags:

- **all**—Trace all operations.
- **auth**—Trace authentication operations.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **packet**—Trace packet decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

Configuring Remote Access to a Router or Switch

- [System Services for Remote Access Overview on page 337](#)
- [Configuring Telnet Service for Remote Access to a Router or Switch on page 338](#)
- [Configuring FTP Service for Remote Access to the Router or Switch on page 339](#)
- [Configuring Finger Service for Remote Access to the Router on page 339](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 340](#)
- [Configuring Outbound SSH Service on page 342](#)
- [Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 346](#)
- [Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 348](#)
- [Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348](#)
- [Configuring the Junos OS to Work with SRC Software on page 350](#)

System Services for Remote Access Overview

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the DHCP, finger, FTP, rlogin, SSH, and Telnet services. In addition, Junos XML protocol client applications can use Secure Sockets Layer (SSL) or the Junos XML protocol-specific clear-text service, among other services.



NOTE: To protect system resources, you can limit the number of simultaneous connections that a service accepts and the number of processes owned by a single user. If either limit is exceeded, connection attempts fail.

Related Documentation

- [Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348](#)
- [Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317](#)
- [DHCP Access Service Overview on page 302](#)

- [Configuring the Router as an Extended DHCP Local Server on page 322](#)
- [Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 324](#)
- [Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 346](#)
- [Configuring Finger Service for Remote Access to the Router on page 339](#)
- [Configuring FTP Service for Remote Access to the Router or Switch on page 339](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 340](#)
- [Configuring Outbound SSH Service on page 342](#)
- [Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 348](#)

Configuring Telnet Service for Remote Access to a Router or Switch

To configure the router or switch to accept Telnet as an access service, include the **telnet** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
telnet {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute.

Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of telnet sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 telnet sessions and 10 IPv4 telnet sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute (from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

You cannot include the **telnet** statement on devices that run the Junos-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

Related
Documentation

- [telnet on page 524](#)

Configuring FTP Service for Remote Access to the Router or Switch

To configure the router or switch to accept FTP as an access service, include the **ftp** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous FTP sessions and connection attempts per minute. You can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 FTP sessions and 10 IPv4 FTP sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 FTP session connection attempts and 10 IPv4 FTP session connection attempts.

You can use passive FTP to access devices that accept only passive FTP services. All commands and statements that use FTP also accept passive FTP. Include the **ftp** statement at the **[edit system services]** hierarchy level to use either active FTP or passive FTP.

To start a passive FTP session, use **pasvftp** (instead of **ftp**) in the standard FTP format (**ftp://*destination***). For example:

```
request system software add pasvftp://name.com/jinstall.tgz
```

You cannot include the **ftp** statement on routers or switches that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring Finger Service for Remote Access to the Router

To configure the router to accept finger as an access service, include the **finger** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
finger {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router supports a limited number of simultaneous finger sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the **finger** statement on routers that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch to accept SSH as an access service, include the **ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ssh {
  ciphers [ cipher-1 cipher-2 cipher-3 ...]
  client-alive-count-max number;
  client-alive-interval seconds;
  connection-limit limit;
  hostkey-algorithm <algorithm | no-algorithm>;
  key-exchange algorithm;
  macs algorithm;
  max-sessions-per-connection number;
  no-passwords;
  no-tcp-forwarding;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login <allow | deny | deny-password>;
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **max-sessions-per-connection *number***—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit

the number of cloned sessions tunneled within a single SSH connection. The default value is 10.

- **rate-limit *limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router. Use the **no-tcp-forwarding** option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

- [Configuring the Root Login Through SSH on page 341](#)
- [Configuring the SSH Protocol Version on page 341](#)
- [Configuring the Client Alive Mechanism on page 342](#)

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH. To control user access through SSH, include the **root-login** statement at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router or switch as root through SSH. The default is **allow**.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

Configuring the SSH Protocol Version

By default, both version 1 and version 2 of the SSH protocol are enabled. To configure the router or switch to use only version 1 of the SSH protocol, include the **protocol-version** statement and specify **v1** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 ];
```

To configure the router or switch to use only version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

To explicitly configure the router or switch to use version 1 and 2 of the SSH protocol, include the **protocol-version** statement and specify **v1** and **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 v2 ];
```

For J Series Services Routers, the export license software supports SSH version 1 only.

Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the **client-alive-count-max** and the **client-alive-interval**. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

Configuring Outbound SSH Service

You can configure a router or switch 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 router or switch is behind a firewall). A single **outbound-ssh** configuration statement instructs the router or switch to create a TCP/IP connection with the client management application and to forward the identity of the router or switch. Once the connection is established, the management application initiates the SSH sequence as the client and the router or switch as the server that authenticates the client.



NOTE: There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the router or switch begins to initiate an outbound SSH connection based on the committed configuration. It continues to attempt to create this connection until successful. If the connection between the router or switch and the client management application is broken, the router or switch 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 router or switch for outbound SSH connections, include the **outbound-ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
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;
}
}

```

The following topics describe the tasks for configuring the outbound-SSH service:

1. [Configuring the Device Identifier for Outbound SSH Connections on page 343](#)
2. [Sending the Public SSH Host Key to the Outbound SSH Client on page 344](#)
3. [Configuring Keepalive Messages for Outbound SSH Connections on page 345](#)
4. [Configuring a New Outbound SSH Connection on page 345](#)
5. [Configuring the Outbound SSH Client to Accept NETCONF as an Available Service on page 346](#)
6. [Configuring Outbound SSH Clients on page 346](#)

Configuring the Device Identifier for Outbound SSH Connections

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

```

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 router or switch using the public SSH host key of the router or switch. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the router or switch. When you configure the **secret** statement, the router or switch passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the **secret** statement is set and the router or switch establishes an outbound SSH connection, the router or switch 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 router or switch 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 router or switch 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 router or switch 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 router or switch. 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 router or switch 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 router or switch 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 router or switch using its copy of the router's or switch's public host SSH key as part of that sequence. The router or switch authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the router or switch 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;
}
```

The **timeout** statement specifies how long the router or switch 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 router or switch disconnects from the application, ending the outbound SSH connection. The default is three retries.

Configuring a New Outbound SSH Connection

When disconnected, the router or switch begins to initiate a new outbound SSH connection. To specify how the router or switch 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);
```

The **sticky** option configures the router or switch to reconnect to the server from which it disconnected.

The **in-order** option configures the router or switch to reconnect to the first configured server. If this server is unavailable, the router or switch tries to connect to the next configured server. This process repeats until a connection is completed.

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 345](#).

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;  
}
```

The **client *client-id*** value is not forwarded to the client management application. 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.

The **address *address*** statement is the IP address or host name of the client.

The **timeout** statement specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

The **retry** statement specifies how many connection attempts a router or switch can make to the specified IP address. The default is 3.

The **port** statement specifies the port at which a server listens for outbound SSH connection requests.

Configuring DTCP-over-SSH Service for the Flow-Tap Application

The active monitoring flow-tap application requires Dynamic Tasking Control Protocol, by configuring the flow-tap DTCP-over-SSH service. Flow-tap enables you to intercept IPv4 packets transiting an active monitoring router and send a copy of matching packets to one or more content destinations, for use in flexible trend analysis of security threats and in lawful intercept of data.



NOTE: The flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported.

To enable the flow-tap DTCP-over-SSH service, include the following statements at the **[edit system services]** hierarchy level:

```
flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
  }
}
```

By default, the router supports a limited number of simultaneous flow-tap DTCP-over-SSH sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You must also define user permissions that enable flow-tap users to configure flow-tap services. Specify a login class and access privileges for flow-tap users at the **[edit system login class *class-name* permissions]** hierarchy level:

```
[edit system login class class-name permissions]
(flow-tap | flow-tap-control | flow-tap-operation);
```

The permission bit for a flow-tap login class can be one of the following:

- **flow-tap**—Can view the flow-tap configuration in configuration mode.
- **flow-tap-control**—Can view the flow-tap configuration in configuration mode and configure flow-tap configuration information at the **[edit services flow-tap]** hierarchy level.
- **flow-tap-operation**—Can make flow-tap requests to the router from a remote location using a DTCP client.



NOTE: Only users with a configured access privilege of **flow-tap-operation** can initiate flow-tap requests.

You can also specify user permissions through the Juniper-User-Permissions RADIUS attribute.

To enable the flow-tap DTCP-over-SSH service, you must also include statements at the **[edit interfaces]** hierarchy level to specify an Adaptive Services PIC that runs the flow-tap service and conveys flow-tap filters from the mediation device to the router. In addition, you must include the **flow-tap** statement at the **[edit services]** hierarchy level.

Configuring NETCONF-Over-SSH Connections on a Specified TCP Port

The Junos OS enables you to restrict incoming NETCONF connections to a specified TCP port without configuring a firewall. To configure the TCP port used for NETCONF-over-SSH connections, include the **port** statement at the **[edit system services netconf ssh]** hierarchy level. The configured port accepts only NETCONF-over-SSH sessions. Regular SSH session requests for this port are rejected.

You can either configure the default port 830 for NETCONF connections over SSH, as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, or configure any port from 1 through 65535.



NOTE:

- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Related Documentation

- [port \(NETCONF Server\) on page 450](#)

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the clear-text or SSL protocol, you must include Junos XML protocol-specific statements in the router configuration.

For more information, see the following topics:

1. [Configuring clear-text Service for Junos XML Protocol Client Applications on page 348](#)
2. [Configuring SSL Service for Junos XML Protocol Client Applications on page 349](#)

Configuring clear-text Service for Junos XML Protocol Client Applications

To configure the router to accept clear-text connections from Junos XML protocol client applications on port 3221, include the **xnm-clear-text** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
xnm-clear-text {
```

```

    connection-limit limit;
    rate-limit limit;
}

```

By default, the Junos XML protocol server supports a limited number of simultaneous clear-text sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6) (a value from 1 through 250). The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per minute per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the **xnm-clear-text** statement on routers that run the Junos-FIPS software. We recommend that you do not use the clear-text protocol in a Common Criteria environment.

Configuring SSL Service for Junos XML Protocol Client Applications

To configure the router to accept SSL connections from Junos XML protocol client applications on port 3220, include the **xnm-ssl** statement at the **[edit system services]** hierarchy level:

```

[edit system services]
xnm-ssl {
    local-certificate name;
    connection-limit limit;
    rate-limit limit;
}

```

local-certificate is the name of the X.509 authentication certificate used to establish an SSL connection. You must obtain the certificate and copy it to the router before referencing it.

By default, the Junos XML protocol server supports a limited number of simultaneous SSL sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit *limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSL sessions and 10 IPv4 SSL sessions.
- **rate-limit *limit***—Maximum number of connection attempts accepted per protocol per minute. The range is a value from 1 through 250. The default is 150. When you

configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSL session connection attempts per minute and 10 IPv4 SSL session connection attempts per minute.

Configuring the Junos OS to Work with SRC Software

You can enable Junos OS to work with the Session and Resource Control (SRC) software. The SRC software supports dynamic service activation engine (SAE) functionality on routers and switches running under Junos OS. To do this, include the following statements at the **[edit system services service-deployment]** hierarchy level:

```
[edit system services service-deployment]
servers server-address {
  port port-number;
}
source-address source-address;
```

server-address is the IPv4 address of the SRC server.

By default, *port-number* is set to 3333 and is a TCP port number.

source-address is optional and is the local IP version 4 (IPv4) address to be used as the source address for traffic to the SRC server.



NOTE: By default, when a connection between SRC and a Juniper Networks router or switch is established, the SRC process (sdxd) starts a Junos XML protocol session as user root. You have the option of configuring user sdx with a different classification at the **[edit system login]** hierarchy level.

For more information about SRC software, see the SRC documentation set.

Related Documentation

- [Configuring Finger Service for Remote Access to the Router on page 339](#)
- [Configuring FTP Service for Remote Access to the Router or Switch on page 339](#)
- [Configuring SSH Service for Remote Access to the Router or Switch on page 340](#)
- [Configuring Outbound SSH Service on page 342](#)
- [Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 348](#)
- [Configuring Telnet Service for Remote Access to a Router or Switch on page 338](#)
- [Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348](#)

Configuring Authentication for Routing Protocols

- [Example: Configuring the BGP and IS-IS Routing Protocols on page 351](#)
- [Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 353](#)

Example: Configuring the BGP and IS-IS Routing Protocols

The main task of a router is to use its routing and forwarding tables to forward user traffic to its intended destination. Attackers can send forged routing protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn can degrade the functionality of the router and the network. To prevent such attacks, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. We strongly recommend using authentication when configuring routing protocols. The Junos OS supports HMAC-MD5 authentication for BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Resource Reservation Protocol (RSVP). HMAC-MD5 uses a secret key that is combined with the data being transmitted to compute a hash. The computed hash is transmitted along with the data. The receiver uses the matching key to recompute and validate the message hash. If an attacker has forged or modified the message, the hash will not match and the data will be discarded.

In the following examples, we configure BGP as the exterior gateway protocol (EGP) and IS-IS as the interior gateway protocol (IGP). If you use OSPF, configure it similarly to the IS-IS configuration shown.

Configuring BGP

The following example shows the configuration of a single authentication key for the BGP peer group internal peers. You can also configure BGP authentication at the neighbor or routing instance levels, or for all BGP sessions. As with any security configuration, there is a trade-off between the degree of granularity (and to some extent the degree of security) and the amount of management necessary to maintain the system. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or

otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
  bgp {
    group ibgp {
      type internal;
      traceoptions {
        file bgp-trace size 1m files 10;
        flag state;
        flag general;
      }
      local-address 10.10.5.1;
      log-updown;
      neighbor 10.2.1.1;
      authentication-key "$9$aH1j8gqQ1gjyjjhgjgiiiiii";
    }
    group ebgp {
      type external;
      traceoptions {
        file ebgp-trace size 10m files 10;
        flag state;
        flag general;
      }
      local-address 10.10.5.1;
      log-updown;
      peer-as 2;
      neighbor 10.2.1.2;
      authentication-key "$9$aH1j8gqQ1gjyjjhgjgiiiiii";
    }
  }
}
```

Configuring IS-IS

Although all IGPs supported by the Junos OS support authentication, some are inherently more secure than others. Most service providers use OSPF or IS-IS to allow fast internal convergence and scalability and to use traffic engineering capabilities with Multiprotocol Label Switching (MPLS). Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF, which is encapsulated in IP and is therefore subject to remote spoofing and DoS attacks.

The following example also shows how to configure a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
  isis {
    authentication-key "$9$aH1j8gqQ1gjyjjhgjgiiiiii"; # SECRET-DATA
    authentication-type md5;
    traceoptions {
```

```

        file isis-trace size 10m files 10;
        flag normal;
        flag error;
    }
    interface at-0/0/0.131 {
        lsp-interval 50;
        level 2 disable;
        level 1 {
            metric 3;
            hello-interval 5;
            hold-time 60;
        }
    }
    interface lo0.0 {
        passive;
    }
}

```

**Related
Documentation**

- [Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 353](#)

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols

You can configure an authentication key update mechanism for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. This mechanism allows you to update authentication keys without interrupting associated routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

To configure this feature, include the **authentication-key-chains** statement at the **[edit security]** level, and include the **authentication-key-chain** statement for the BGP or LDP routing protocols at the **[edit protocols]** level.

The following topics provide more details about configuring authentication key updates for BGP and LDP Routing Protocols:

1. [Configuring Authentication Key Updates on page 353](#)
2. [Configuring BGP and LDP for Authentication Key Updates on page 354](#)

Configuring Authentication Key Updates

To configure the authentication key update mechanism, include the **key-chain** statement at the **[edit security authentication-key-chains]** hierarchy level, and specify the **key** option to create a keychain consisting of several authentication keys.

```

[edit security authentication-key-chains]
key-chain key-chain-name {
    key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
    }
}

```

```
}
```

key-chain—Assigns a name to the keychain mechanism. This name is also configured at the **[edit protocols bgp]** or the **[edit protocols ldp]** hierarchy levels to associate unique **authentication key-chain** attributes as specified using the following options:

- **key**—Each key within a keychain is identified by a unique integer value. The range is from 0 through 63.
- **secret**—Each key must specify a secret in encrypted text or plain text format. Even if you enter the secret data in plain-text format, the secret always appears in encrypted format.
- **start-time**—Start times for authentication key updates are specified in UTC (Coordinated Universal Time), and must be unique within the keychain.

Configuring BGP and LDP for Authentication Key Updates

To configure the authentication key update mechanism for the BGP and LDP routing protocols, include the **authentication-key-chain** statement at the **[edit protocols (bgp | ldp)]** hierarchy level to associate each routing protocol with the **[edit security authentication-key-chains]** authentication keys.

```
[edit protocols (bgp | ldp)]
group group-name {
  neighbor address {
    authentication-key-chain key-chain-name;
  }
}
```



NOTE: When configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

For information about the BGP protocol, see the *Junos OS Routing Protocols Library for Routing Devices*.

Related Documentation

- [Example: Configuring the BGP and IS-IS Routing Protocols on page 351](#)

Configuration Statements

- [System Management Configuration Statements on page 358](#)
- [accounting on page 366](#)
- [access-end on page 367](#)
- [access-start on page 367](#)
- [accounting-port \(RADIUS Server\) on page 368](#)
- [allow-commands on page 368](#)
- [allow-configuration on page 369](#)
- [allow-configuration-regexps on page 370](#)
- [allowed-days on page 370](#)
- [authentication \(DHCP Local Server\) on page 371](#)
- [authentication \(Login\) on page 372](#)
- [authentication-order on page 373](#)
- [backoff-factor on page 374](#)
- [backoff-threshold on page 374](#)
- [boot-file on page 375](#)
- [boot-server \(DHCP\) on page 376](#)
- [change-type on page 377](#)
- [ciphers on page 378](#)
- [circuit-type on page 379](#)
- [class \(Assigning a Class to an Individual User\) on page 380](#)
- [class \(Defining Login Classes\) on page 381](#)
- [client-alive-count-max on page 382](#)
- [client-alive-interval on page 382](#)
- [client-identifier on page 383](#)
- [connection-limit on page 384](#)
- [default-lease-time on page 385](#)
- [delimiter \(DHCP Local Server\) on page 386](#)
- [deny-commands on page 387](#)

- [deny-configuration](#) on page 388
- [deny-configuration-regexps](#) on page 389
- [destination \(Accounting\)](#) on page 390
- [dhcp](#) on page 391
- [dhcpx6 \(DHCP Local Server\)](#) on page 393
- [dhcp-local-server](#) on page 396
- [domain-name \(DHCP\)](#) on page 401
- [domain-name \(DHCP Local Server\)](#) on page 402
- [dynamic-profile-options](#) on page 403
- [enhanced-accounting](#) on page 403
- [enhanced-avs-max](#) on page 404
- [finger](#) on page 404
- [flow-tap-dtcp](#) on page 405
- [format](#) on page 406
- [ftp](#) on page 407
- [full-name](#) on page 407
- [group \(DHCP Local Server\)](#) on page 408
- [http](#) on page 410
- [https](#) on page 411
- [hostkey-algorithm](#) on page 412
- [idle-timeout \(System-Login\)](#) on page 413
- [interface \(DHCP Local Server\)](#) on page 414
- [ip-address-first](#) on page 415
- [key-exchange](#) on page 416
- [load-key-file](#) on page 417
- [local-certificate](#) on page 418
- [lockout-period](#) on page 419
- [logical-system-name \(DHCP Local Server\)](#) on page 420
- [login](#) on page 421
- [login-alarms](#) on page 422
- [login-script \(Login\)](#) on page 422
- [mac-address \(DHCP Local Server\)](#) on page 423
- [macs](#) on page 424
- [maximum-lease-time \(DHCP\)](#) on page 425
- [maximum-length](#) on page 426
- [max-sessions-per-connection](#) on page 426
- [maximum-time](#) on page 427

- [minimum-changes on page 428](#)
- [minimum-length on page 429](#)
- [minimum-lower-cases on page 430](#)
- [minimum-numeric on page 431](#)
- [minimum-punctuations on page 432](#)
- [minimum-time on page 433](#)
- [minimum-upper-cases on page 434](#)
- [next-server on page 435](#)
- [no-passwords on page 435](#)
- [no-tcp-forwarding on page 436](#)
- [option \(DHCP server\) on page 437](#)
- [option-60 \(DHCP Local Server\) on page 438](#)
- [option-82 \(DHCP Local Server Authentication\) on page 439](#)
- [option-82 \(DHCP Local Server Pool Matching\) on page 440](#)
- [outbound-ssh on page 441](#)
- [password \(DHCP Local Server\) on page 444](#)
- [password \(Login\) on page 445](#)
- [permissions on page 446](#)
- [pool \(System\) on page 447](#)
- [pool-match-order on page 448](#)
- [port \(HTTP/HTTPS\) on page 449](#)
- [port \(NETCONF Server\) on page 450](#)
- [port \(RADIUS Server\) on page 451](#)
- [port \(SRC Server\) on page 451](#)
- [port \(TACACS+ Server\) on page 452](#)
- [protocol-version on page 452](#)
- [radius \(System\) on page 453](#)
- [radius-options \(edit system\) on page 454](#)
- [radius-server \(System\) on page 455](#)
- [rate-limit on page 456](#)
- [retry \(RADIUS\) on page 457](#)
- [retry-options on page 458](#)
- [root-login on page 459](#)
- [router on page 460](#)
- [routing-instance-name \(DHCP Local Server\) on page 461](#)
- [secret on page 462](#)
- [server \(RADIUS Accounting\) on page 463](#)

- [server \(TACACS+ Accounting\) on page 463](#)
- [servers on page 464](#)
- [server-identifier on page 465](#)
- [service-deployment on page 466](#)
- [services \(System Services\) on page 467](#)
- [session \(Time-out\) on page 469](#)
- [single-connection on page 470](#)
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\) on page 471](#)
- [source-address \(SRC Software\) on page 472](#)
- [source-port \(Port Addresses\) on page 472](#)
- [ssh on page 473](#)
- [ssl-renegotiation on page 474](#)
- [static-binding on page 475](#)
- [system on page 476](#)
- [tacplus on page 476](#)
- [tacplus-options on page 477](#)
- [tacplus-server on page 478](#)
- [telnet on page 478](#)
- [timeout \(System\) on page 479](#)
- [traceoptions \(Address-Assignment Pool\) on page 480](#)
- [traceoptions \(DHCP\) on page 482](#)
- [traceoptions \(DHCP Server\) on page 485](#)
- [traceoptions \(SBC Configuration Process\) on page 488](#)
- [tries-before-disconnect on page 490](#)
- [uid on page 490](#)
- [user \(Access\) on page 491](#)
- [username-include \(DHCP Local Server\) on page 492](#)
- [user-prefix \(DHCP Local Server\) on page 493](#)
- [versioning on page 494](#)
- [web-management on page 495](#)
- [wins-server \(System\) on page 496](#)
- [xnm-clear-text on page 497](#)
- [xnm-ssl on page 497](#)

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```

system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
  enhanced-avs-max;
  events [ login change-log interactive-commands ];
}
archival {
  configuration {
    archive-sites {
      ftp://<username>:<password>@<host>:<port>/<url-path>;
      ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
allow-v4mapped-packets;
arp {
  aging-timer minutes;
  gratuitous-arp-delay;
  gratuitous-arp-on-ifup;
  interfaces;
  passive-learning;
  purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit {
  fast-synchronize;
  persist-groups-inheritance ;
  server;
  synchronize
}
synchronize;

```

```
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
    icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
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;
        access-start;
        allow-commands "regular-expression";
        ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
        expression 2";
        allowed-days;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
        expression 2";
        idle-timeout minutes;
        login-script
        login-tip;
        permissions [ permissions ];
```

```

}
message text;
password {
  change-type (set-transitions | character-set);
  format (md5 | sha1 | des);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
}
retry-options {
  backoff-threshold number;
  backoff-factor seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}
user username {
  full-name complete-name;
  uid uid-value;
  class class-name;
  authentication {
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
}
login-tip number;
mirror-flash-on-disk;
name-server {
  address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
  authentication-key key-number type type value password;
  boot-server address;
  broadcast <address> <key key-number> <version value> <ttl value>;
  broadcast-client;
  multicast-client <address>;
  peer address <key key-number> <version value> <prefer>;
  source-address source-address;
  server address <key key-number> <version value> <prefer>;
  trusted-key [ key-numbers ];
}
ports {
  auxiliary {
    type terminal-type;
  }
  pic-console-authentication {
    encrypted-password encrypted-password;
    plain-text-password;
    console {
      insecure;
      log-out-on-disconnect;
    }
  }
}

```

```

        type terminal-type;
        disable;
    }
}
processes {
    process--name (enable | disable) failover (alternate-media | other-routing-engine);
    timeout seconds;
}
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
radius-options {
    attributes {
        nas-ip-address ip-address;
    }
    enhanced-accounting;
    password-protocol mschap-v2;
}
root-authentication {
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
    commit {
        allow-transients;
        file filename {
            optional;
            refresh;
            refresh-from url;
            source url;
        }
        traceoptions {
            file <filename> <files number> <size size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
    }
    op {
        file filename {
            arguments {
                argument-name {
                    description descriptive-text;
                }
            }
        }
        command filename-alias;
        description descriptive-text;
        refresh;
        refresh-from url;
    }
}

```

```

        source url;
    }
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
}
services {
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    flow-tap-dtcp {
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers server-address {
            port port-number;
        }
        source-address source-address;
    }
    ssh {
        root-login (allow | deny | deny-password);
        protocol-version [v1 v2];
        connection-limit limit;
        rate-limit limit;
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {
        http {
            interfaces [ interface-names ];
            port port;
        }
        https {
            interfaces [ interface-names ];
            local-certificate name;
            port port;
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ session-limit ];
        }
    }
}

```

```

}
xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
}
xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
}
}
static-host-mapping {
    hostname {
        alias [ alias ];
        inet [ address ];
        sysid system-identifier;
    }
}
syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url <password password>}> <files number> <size size>
            <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
            no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
}
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {
    facility severity;
    match "regular-expression";
}
}
tacplus-options {
    enhanced-accounting;
    service-name service-name;
    (no-cmd-attribute-value | exclude-cmd-attribute);
}

```

```
}
tacplus-server server-address {
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
time-zone (GMThour-offset | time-zone);
}
tracing {
  destination-override {
    syslog host;
  }
}
use-imported-time-zones;
}
```

accounting

```
Syntax  accounting {
        events [login change-log interactive-commands];
        destination {
            radius {
                server {
                    server-address {
                        accounting-port port-number;
                        secret password;
                        source-address address;
                        retry number;
                        timeout seconds;
                    }
                }
            }
            tacplus {
                server {
                    server-address {
                        port port-number;
                        secret password;
                        single-connection;
                        timeout seconds;
                    }
                }
            }
        }
        enhanced-avs-max <number>;
    }
```

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.
enhanced-avs-max statement introduced in Junos OS Release 14.1.

Description Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands. Auditing these factors helps you track network usage for auditing and billing purposes.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS System Accounting on page 276](#)
- [Configuring TACACS+ System Accounting on page 295](#)
- [enhanced-avs-max on page 404](#)

access-end

| | |
|---------------------------------|---|
| Syntax | access-end <i>HH:MM</i> ; |
| Hierarchy Level | [edit system login class] |
| Release Information | Statement introduced in Junos OS Release 10.1. |
| Description | Configure the end time for login access. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Time-Based User Access on page 48 |

access-start

| | |
|---------------------------------|---|
| Syntax | access-start <i>HH:MM</i> ; |
| Hierarchy Level | [edit system login class] |
| Release Information | Statement introduced in Junos OS Release 10.1. |
| Description | Configure the start time for login access. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Time-Based User Access on page 48 |

accounting-port (RADIUS Server)

| | |
|--------------------------|---|
| Syntax | accounting-port <i>port-number</i> ; |
| Hierarchy Level | [edit system accounting destination radius <i>server</i> <i>server-address</i>], [edit system <i>radius-server</i> <i>server-address</i>] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the accounting port number on which to contact the RADIUS server. |
| Options | <i>number</i> —Port number on which to contact the RADIUS server. Default: 1813 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring RADIUS Authentication on page 267• Configuring RADIUS System Accounting on page 276 |

allow-commands

| | |
|--------------------------|---|
| Syntax | allow-commands " <i>regular-expression</i> "; |
| Hierarchy Level | [edit system login <i>class</i> <i>class-name</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Specify the operational mode commands that members of a login class can use. |
| Default | If you omit this statement and the deny-commands statement, users can issue 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. |
| Related Documentation | <ul style="list-style-type: none">• Specifying Access Privileges for Junos OS Operational Mode Commands on page 64• deny-commands on page 387• user on page 491 |

allow-configuration

| | |
|---------------------------------|--|
| Syntax | <code>allow-configuration "regular-expression";</code> |
| 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 9.0 for EX Series switches. |
| 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 | 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. |
| Related Documentation | <ul style="list-style-type: none"> • Specifying Access Privileges Using allow/deny-configuration Statements on page 70 • Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68 • deny-configuration on page 388 • user on page 491 |

allow-configuration-regexps

| | |
|---------------------------------|---|
| Syntax | <code>allow-configuration-regexps "regular expression 1" "regular expression 2";</code> |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced in Junos OS Release 11.2. |
| Description | <p>Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the permissions statement allow that access. .</p> <p>The statement deny-configuration-regexps takes precedence if it is 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>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. Enter as many expressions as needed..</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67• Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies on page 68• deny-configuration-regexps on page 389• user on page 491 |

allowed-days

| | |
|---------------------------------|--|
| Syntax | <code>allowed-days [<i>days-of-the-week</i>];</code> |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced in Junos OS Release 10.1. |
| Description | Specify the days of the week when users can log in. |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Configuring Time-Based User Access on page 48 |

authentication (DHCP Local Server)

| | |
|---------------------------------|---|
| Syntax | <pre> authentication { password <i>password-string</i>; username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name ; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; } }</pre> |
| Hierarchy Level | <pre> [edit system services dhcp-local-server], [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 group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</pre> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | <p>Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Using External AAA Authentication Services with DHCP</i> |

authentication (Login)

| | |
|---------------------------------|---|
| Syntax | <pre>authentication { (encrypted-password "password" plain-text-password); load-key-file URL filename; ssh-dsa "public-key"; ssh-ecdsa "public-key"; ssh-rsa "public-key"; }</pre> |
| Hierarchy Level | [edit system login user <i>username</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user. |
| Options | <p>encrypted-password "password"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.</p> <p>You cannot configure a blank password for encrypted-password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.</p> <p>load-key-file URL filename—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.</p> <p>plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.</p> <p>ssh-dsa "public-key"—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.</p> <p>ssh-ecdsa "public-key"—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.</p> <p>ssh-rsa "public-key"—SSH version 1 and SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.</p> |
| Required Privilege Level | admin —To view this statement in the configuration. admin-control —To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Junos OS User Accounts on page 53• <i>root-authentication</i> |

authentication-order

| | |
|---------------------------------|--|
| Syntax | <code>authentication-order [<i>authentication-methods</i>];</code> |
| 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 | <p><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:</p> <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 | <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 Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication on page 262 • authentication on page 372 |

backoff-factor

| | |
|--------------------------|---|
| Syntax | <code>backoff-factor <i>seconds</i>;</code> |
| Hierarchy Level | <code>[edit system login retry-options]</code> |
| Release Information | Statement introduced in Junos OS Release 8.0. |
| Description | Configure the length of delay after each failed login attempt, which increases for each subsequent login attempt after the value specified in the backoff-threshold statement. |
| Options | <p><i>seconds</i>—Length of delay after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold option.</p> <p>Range: 5 through 10</p> <p>Default: 5</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57• retry-options on page 458 |

backoff-threshold

| | |
|--------------------------|--|
| Syntax | <code>backoff-threshold <i>number</i>;</code> |
| Hierarchy Level | <code>[edit system login retry-options]</code> |
| Release Information | Statement introduced in Junos OS Release 8.0. |
| Description | Configure the threshold for the number of failed login attempts on the router before the user experiences a delay when attempting to reenter a password. |
| Options | <p><i>number</i>—Threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Use the backoff-factor option to specify the length of delay, in seconds.</p> <p>Range: 1 through 3</p> <p>Default: 2</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57• retry-options on page 458 |

boot-file

| | |
|---------------------------------|--|
| Syntax | <code>boot-file <i>filename</i>;</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For J Series Services Routers and EX Series switches only. Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. |
| Options | <i>filename</i> —The location of the boot file on the boot server. The filename can include a pathname. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 • boot-server on page 376 |


boot-server (DHCP)

| | |
|---------------------------------|--|
| Syntax | <code>boot-server (address hostname);</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For J Series Services Routers and EX Series switches only. Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. |
| Options | <ul style="list-style-type: none">• address—IP address of a DHCP boot server.• hostname—Hostname of a DHCP boot 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">• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317• boot-file on page 375 |

change-type

| | |
|---------------------------------|---|
| Syntax | change-type (character-sets set-transitions); |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Set requirements for using character sets in plain-text passwords. When you combine this statement with the minimum-changes statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements. |
| Options | Specify one of the following: <ul style="list-style-type: none">• character-sets—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.• set-transitions—The number of transitions between character sets. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257• minimum-changes on page 428 |

ciphers

| | |
|--|--|
| Syntax | <code>ciphers [cipher-1 cipher-2 cipher-3 ...]</code> |
| Hierarchy Level | <code>[edit system services ssh]</code> |
| 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 | <ul style="list-style-type: none"> • 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. |
| <div>  <p>NOTE: Ciphers represent a set. To configure SSH ciphers:</p> <pre>user@host#set system services ssh ciphers [aes256-cbc aes192-cbc]</pre> </div> | |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring SSH Service for Remote Access to the Router or Switch on page 340 • <i>Junos OS Security Configuration Guide</i> |

circuit-type

| | |
|---------------------------------|--|
| Syntax | circuit-type; |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p> |
| Release Information | Statement introduced in Junos OS Release 9.1. |
| Description | Specify that the circuit type is concatenated with the username during the subscriber authentication process. |
| 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"> • Using External AAA Authentication Services to Authenticate DHCP Clients on page 326 |

class (Assigning a Class to an Individual User)

| | |
|---------------------------------|---|
| Syntax | <code>class <i>class-name</i>;</code> |
| Hierarchy Level | [edit system login user <i>username</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Assign a user to a login class. You must assign each user to a login class. |
| Options | <i>class-name</i> —One of the classes defined at the [edit system login class] hierarchy level. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Junos OS User Accounts on page 53 |

class (Defining Login Classes)

| | |
|---------------------------------|---|
| Syntax | <pre> class <i>class-name</i> { allow-commands "<i>regular-expression</i>"; (allow-configuration allow-configuration-regexps) "<i>regular expression 1</i>" "<i>regular expression 2</i>"; configuration-breadcrumbs; deny-commands "<i>regular-expression</i>"; (deny-configuration deny-configuration-regexps) "<i>regular expression 1</i>" "<i>regular expression 2</i>"; idle-timeout <i>minutes</i>; login-script <i>filename</i>; login-tip; permissions [<i>permissions</i>]; } </pre> |
| Hierarchy Level | [edit system login] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Define a login class. |
| Options | <p><i>class-name</i>—A name you choose for the login class.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Defining Junos OS Login Classes on page 39 • user on page 491 |

client-alive-count-max

| | |
|---------------------------------|---|
| Syntax | <code>client-alive-count-max <i>number</i>;</code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Junos OS Release 11.2. |
| Description | Configure the number of client alive messages that can be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. Client alive messages are sent through the encrypted channel. Use in conjunction with client-alive-interval to disconnect unresponsive SSH clients. |
| Default | 3 messages |
| Options | Range: 1 through 255 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340 |


client-alive-interval

| | |
|---------------------------------|---|
| Syntax | <code>client-alive-interval <i>seconds</i>;</code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Junos OS Release 12.1. |
| Description | Configure a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. This option applies to SSH protocol version 2 only. Use in conjunction with client-alive-count-max to disconnect unresponsive SSH clients. |
| Default | 0 seconds |
| Options | Range: 1 through 65535 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340 |

client-identifier

| | |
|---------------------------------|---|
| Syntax | <code>client-identifier (ascii <i>client-id</i> hexadecimal <i>client-id</i>);</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For J Series Services Routers and EX Series switches only. Configure the client's unique identifier. This identifier is used by the DHCP server to index its database of address bindings. Either a client identifier or the client's MAC address is required to uniquely identify the client on the network. |
| Options | <i>client-id</i> —A name or number that uniquely identifies the client on the network. The client identifier can be an ASCII string or hexadecimal digits. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i> |

connection-limit

| | |
|--|---|
| Syntax | connection-limit <i>limit</i> ; |
| 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 before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4). |
| Options | <i>limit</i> —(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4). Range: 1 through 250 Default: 75 |
| <div> 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.</div> | |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348• Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 346• Configuring Finger Service for Remote Access to the Router on page 339• Configuring FTP Service for Remote Access to the Router or Switch on page 339• Configuring SSH Service for Remote Access to the Router or Switch on page 340• Configuring Telnet Service for Remote Access to a Router or Switch on page 338 |

default-lease-time

| | |
|---------------------------------|--|
| Syntax | <code>default-lease-time <i>seconds</i>;</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For J Series Services Routers and EX Series switches only. Specify the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server. This setting is used if a lease time is not requested by the client. |
| Options | <i>seconds</i> —Number of seconds the lease can be held. Default: 86400 (1day) |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317• maximum-lease-time on page 425 |

delimiter (DHCP Local Server)

| | |
|---------------------------------|--|
| Syntax | <code>delimiter <i>delimiter-character</i>;</code> |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify the character used as the delimiter between the concatenated components of the username. |
| Options | <i>delimiter-character</i> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter. |
| 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**
- [Using External AAA Authentication Services with DHCP](#)

deny-commands

| | |
|---------------------------------|--|
| Syntax | <code>deny-commands "regular-expression";</code> |
| Hierarchy Level | [edit system login class] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Specify the operational mode commands that the user is denied permission to issue even though the permissions set with the permissions statement would allow it. |
| Default | If you omit this statement and the allow-commands statement, users can issue only those commands 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. |
| Related Documentation | <ul style="list-style-type: none"> • Specifying Access Privileges for Junos OS Operational Mode Commands on page 64 • allow-commands on page 368 • user on page 491 |

deny-configuration

| | |
|---------------------------------|---|
| Syntax | <code>deny-configuration "regular-expression";</code> |
| Hierarchy Level | [edit system login class] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| 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. Note that the user cannot view a particular hierarchy if configuration access is denied for that hierarchy. |
| 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. |
| Related Documentation | <ul style="list-style-type: none">• Specifying Access Privileges Using allow/deny-configuration Statements on page 70• allow-configuration on page 369• user on page 491 |

deny-configuration-regexps

| | |
|---------------------------------|--|
| Syntax | <code>deny-configuration-regexps "regular expression 1" "regular expression 2";</code> |
| Hierarchy Level | [edit system login class <i>class-name</i>] |
| Release Information | Statement introduced in Junos OS Release 11.2. |
| 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>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. Enter as many expressions as needed.</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 67 • allow-configuration-regexps on page 370 • user on page 491 |

destination (Accounting)

Syntax

```
destination {  
  radius {  
    server {  
      server-address {  
        accounting-port port-number;  
        secret password;  
        source-address address;  
        retry number;  
        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.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the authentication server.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS System Accounting on page 276](#)
- [Configuring TACACS+ System Accounting on page 295](#)

dhcp

```
Syntax  dhcp {
        boot-file filename;
        boot-server (address | hostname);
        default-lease-time seconds;
        domain-name domain-name;
        domain-search [domain-list];
        maximum-lease-time seconds;
        name-server {
            address;
        }
        next-server next-server
        option option-identifier-code ;
        pool address/prefix-length {
            address-range {
                low address;
                high address;
            }
            exclude-address {
                address;
            }
        }
        router {
            address;
        }
        static-binding mac-address {
            fixed-address {
                address;
            }
            host-name hostname;
            client-identifier (ascii client-id | hexadecimal client-id);
        }
        wins-server {
            address;
        }
    }
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.

Description For J Series Services Routers only. Configure a router, switch, or interface as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation • [Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317](#)

- [System Management Configuration Statements on page 358](#)

dhcpv6 (DHCP Local Server)

```
Syntax  dhcpv6 {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
        authentication {
            ...
        }
        interface interface-name {
            exclude;
            liveness-detection {
                failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                method {
                    bfd {
                        version (0 | 1 | automatic);
                        minimum-interval milliseconds;
                        minimum-receive-interval milliseconds;
                        multiplier number;
                        no-adaptation;
                        transmit-interval {
                            minimum-interval milliseconds;
                            threshold milliseconds;
                        }
                        detection-time {
                            threshold milliseconds;
                        }
                    }
                    session-mode (automatic | multihop | singlehop);
                    holddown-interval milliseconds;
                }
            }
        }
        overrides {
            include-option-82;
            interface-client-limit number;
            multi-address-embedded-option-response;
            process-inform {
                pool pool-name;
            }
            rapid-commit;
        }
        service-profile dynamic-profile-name;
    }
}
```

```
    trace;
    upto upto-interface-name;
}
overrides {
    delegated-pool;
    include-option-82;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    delegated-pool;
    include-option-82;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        strict;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
}
```

```

}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```

| | |
|---------------------------------|---|
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> |
| Description | <p>Configure DHCPv6 local server options on the router or switch and enable the router or switch to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.</p> <p>The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>DHCPv6 Local Server Overview</i> |

dhcp-local-server

```
Syntax  dhcp-local-server {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dhcpv6 {
            authentication {
                ...
            }
            group group-name {
                authentication {
                    ...
                }
                interface interface-name {
                    exclude;
                    liveness-detection {
                        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                        method {
                            bfd {
                                version (0 | 1 | automatic);
                                minimum-interval milliseconds;
                                minimum-receive-interval milliseconds;
                                multiplier number;
                                no-adaptation;
                                transmit-interval {
                                    minimum-interval milliseconds;
                                    threshold milliseconds;
                                }
                                detection-time {
                                    threshold milliseconds;
                                }
                            }
                            session-mode (automatic | multihop | singlehop);
                            holddown-interval milliseconds;
                        }
                    }
                }
            }
            overrides {
                interface-client-limit number;
                multi-address-embedded-option-response;
                process-inform {
                    pool pool-name;
                }
            }
        }
    }
```

```

    }
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}
overrides {
  delegated-pool;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
  }
}
}
overrides {
  delegated-pool;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {

```

```

        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    authentication {
        ...
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
        primary-profile-name>;
    interface interface-name {
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                    detection-time {
                        threshold milliseconds;
                    }
                    session-mode (automatic | multihop | singlehop);
                    holddown-interval milliseconds;
                }
            }
        }
    }
    overrides {
        client-discover-match (option60-and-option82 | incoming-interface);
        include-option-82 {
            forcerenew;
            nak;
        }
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
overrides {

```

```

    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
requested-ip-network-match subnet-mask
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
}

```

```

    token token-value;
    trigger {
        radius-disconnect;
    }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services],
 [edit logical-systems *logical-system-name* system services],
 [edit routing-instances *routing-instance-name* system services],
 [edit system services]

Release Information Statement introduced in Junos OS Release 9.0.
 Statement introduced in Junos OS Release 12.1 for EX Series switches.
 Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch and enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpx6** stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.



NOTE: When you configure the **dhcp-local-server** statement at the routing instance hierarchy level, you must use a routing instance type of **virtual-router**.

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

- *Extended DHCP Local Server Overview*
- *DHCPv6 Local Server Overview*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

domain-name (DHCP)

| | |
|---------------------------------|---|
| Syntax | <code>domain-name <i>domain-name</i>;</code> |
| Hierarchy Level | <code>[edit system services dhcp</code> <code>[edit system services dhcp],</code> <code>[edit system services dhcp pool],</code> <code>[edit system services dhcp static-binding]</code> |
| 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> |
| Description | For J Series Services Routers and EX Series switches only. Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. |
| Options | <i>domain-name</i> —Name of the domain. |
| 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 Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 • Configuring a DHCP Server on Switches (CLI Procedure) |

domain-name (DHCP Local Server)

| | |
|---------------------------------|--|
| Syntax | <code>domain-name <i>domain-name-string</i>;</code> |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process. |
| Options | <i>domain-name-string</i> —Domain name formatted string. |
| 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**
- *Using External AAA Authentication Services with DHCP*

dynamic-profile-options

| | |
|---------------------------------|---|
| Syntax | dynamic-profile-options { versioning ; } |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced in Junos OS Release 11.4. |
| Description | Configure global dynamic profile options. The remaining statement is explained separately. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • <i>Enabling Dynamic Profiles to Use Multiple Versions</i> |

enhanced-accounting

| | |
|---------------------------------|--|
| Syntax | enhanced-accounting; |
| Hierarchy Level | [edit system radius-options] [edit system tacplus-options], |
| Release Information | Statement introduced in Junos OS Release 14.1. |
| Description | Configure audit of TACACS+ or RADIUS authentication events such as access method, remote port, and access privileges. |
| 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"> • radius-options on page 454 • tacplus-options on page 477 • Configuring RADIUS System Accounting on page 276 • Configuring TACACS+ System Accounting on page 295 |

enhanced-avs-max

| | |
|---------------------------------|---|
| Syntax | enhanced-avs-max <i><number></i> ; |
| Hierarchy Level | [edit system accounting] |
| Release Information | Statement introduced in Junos OS Release 14.1. |
| Description | Configure the number of attribute values to be displayed. |
| Options | <i><number></i> —Number of attribute values. Range: 7 through 15 Default: 7 |
| 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">• accounting on page 366• enhanced-accounting on page 403• Configuring RADIUS System Accounting on page 276• Configuring TACACS+ System Accounting on page 295 |

finger

| | |
|---------------------------------|--|
| Syntax | finger { connection-limit <i>limit</i> ; rate-limit <i>limit</i> ; } |
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | Allow finger requests from remote systems to the local router. 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 | <ul style="list-style-type: none">• Configuring Finger Service for Remote Access to the Router on page 339 |

flow-tap-dtcp

| | |
|---------------------------------|---|
| Syntax | <pre> flow-tap-dtcp { ssh { connection-limit <i>limit</i>; rate-limit <i>limit</i>; } } </pre> |
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced in Junos OS Release 8.1. |
| Description | Configure Dynamic Tasking Control Protocol (DTCP) sessions to run over SSH in support of the flow-tap application. Note that the flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported. |
| Options | <p>connection-limit <i>limit</i>—(Optional) Maximum number of connections allowed. Range: 1 through 250 Default: 75</p> <p>rate-limit <i>limit</i>—(Optional) Maximum number of connection attempts allowed per minute. Range: 1 through 250 Default: 150</p> |
| Required Privilege Level | <p>flow-tap—To view this statement in the configuration.</p> <p>flow-tap-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring DTCP-over-SSH Service for the Flow-Tap Application on page 346 |

format

| | |
|---------------------------------|---|
| Syntax | format (md5 sha1 sha256 sha512); |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure the authentication algorithm for plain-text passwords. |
| Default | For Junos OS, the default encryption format is md5 . For Junos-FIPS software, the default encryption format is sha1 . |
| Options | <p>The hash algorithm that authenticates the password can be one of these algorithms:</p> <ul style="list-style-type: none">• Agreed technical requirements;• Layout of the proposed physical and logical network topology;• Protocols and equipment to be used;• CoS and QoS functionality;• Description of the devices and connectivity for End-User's sites;• Further Juniper Networks' findings and recommendations, if applicable; and• md5—Produces a 128-bit digest.• sha1—Produces a 160-bit digest.• sha256—Produces a 256-bit digest.• sha512—Produces a 512-bit digest. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257 |

ftp

| | |
|---------------------------------|---|
| Syntax | ftp { connection-limit <i>limit</i> ; rate-limit <i>limit</i> ; } |
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Allow FTP requests from remote systems to the local router or switch. |
| 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 | <ul style="list-style-type: none"> • Configuring FTP Service for Remote Access to the Router or Switch on page 339 |

full-name

| | |
|---------------------------------|---|
| Syntax | full-name <i>complete-name</i> ; |
| Hierarchy Level | [edit system login user] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| Description | Configure the complete name of a user. |
| Options | <i>complete-name</i> —Full name of the user. If the name contains spaces, 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. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring Junos OS User Accounts on page 53 • user on page 491 • <i>user</i> |

group (DHCP Local Server)

```
Syntax  group group-name {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name-string;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                relay-agent-interface-id
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
            primary-profile-name>;
        interface interface-name {
            exclude;
            overrides {
                client-discover-match (option60-and-option82 | incoming-interface);
                interface-client-limit number;
                process-inform {
                    pool pool-name;
                }
                rapid-commit;
            }
            service-profile dynamic-profile-name;
            trace;
            upto upto-interface-name;
        }
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                }
                detection-time {
                    threshold milliseconds;
                }
            }
            session-mode (automatic | multihop | singlehop);
        }
    }
```

```

        holddown-interval milliseconds;
    }
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    delegated-pool;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}

```

| | |
|---------------------------------|--|
| Hierarchy Level | <p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> |
| Description | Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface. |
| Options | <p><i>group-name</i>—Name of the group.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |

- Related Documentation**
- *Extended DHCP Local Server Overview*
 - *Grouping Interfaces with Common DHCP Configurations*
 - *Using External AAA Authentication Services with DHCP*
 - *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
 - *Configuring a DHCP Server on Switches (CLI Procedure)*


http

| | |
|---------------------------------|---|
| Syntax | <pre>http { interfaces [<i>interface-names</i>]; port <i>port</i>; }</pre> |
| Hierarchy Level | [edit system services web-management] |
| 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 port and interfaces for HTTP service, which is unencrypted. |
| Options | <p>interfaces [<i>interface-names</i>]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.</p> <p>The remaining statement is explained separately.</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">• <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i>• <i>J-Web Interface User Guide</i>• https on page 411• port on page 449• web-management on page 495 |

https

| | |
|---------------------------------|---|
| Syntax | <pre>https { interfaces [<i>interface-names</i>]; local-certificate <i>name</i>; port <i>port</i>; }</pre> |
| Hierarchy Level | [edit system services web-management] |
| 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> |
| Description | Configure the secure version of HTTP (HTTPS) service, which is encrypted. |
| Options | <p>interfaces [<i>interface-names</i>]—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.</p> <p>local-certificate <i>name</i>—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 410 • port on page 449 • web-management on page 495 |

hostkey-algorithm

| | |
|---------------------------------|--|
| 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 a 2048-bit RSA host key.• ssh-ecdsa—Allow generation of an ECDSA host key.• ssh-rsa—Allow generation of a 2048-bit RSA host key.• ssh-dss—Allow generation of a 1024-bit DSA host key. |
| | <div> NOTE: On systems operating in FIPS mode, host keys are regenerated to be of compliant size. However, DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode. RSA keys are also not supported in FIPS, so the ssh-rsa option is also not available. In FIPS mode, by default, ECDSA host keys of 256 bit length are generated.</div> |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340• <i>Junos OS Security Configuration Guide</i> |

idle-timeout (System-Login)

| | |
|----------------------------|--|
| Syntax | <code>idle-timeout <i>minutes</i>;</code> |
| 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 9.0 for EX Series switches. |
| Description | For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time. |
| Default | If you omit this statement, a user is never forced off the system after extended idle times. |
| Options | <i>minutes</i> —Maximum idle time. Range: 0 through 4294967295 minutes |



NOTE: The timeout feature is disabled if the value of *minutes* is set to 0.

| | |
|---------------------------------|--|
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Timeout Value for Idle Login Sessions on page 40 • user on page 491 |

interface (DHCP Local Server)

| | |
|----------------------------|---|
| Syntax | <pre> interface <i>interface-name</i> { exclude; overrides { client-discover-match (option60-and-option82 incoming-interface); interface-client-limit <i>number</i>; rapid-commit; } service-profile <i>dynamic-profile-name</i>; trace; upto <i>upto-interface-name</i>; } </pre> |
| Hierarchy Level | <pre> [edit system services dhcp-local-server <i>group group-name</i>], [edit system services dhcp-local-server <i>dhcpv6 group group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services <i>dhcp-local-server ...</i>], [edit logical-systems <i>logical-system-name</i> system services <i>dhcp-local-server ...</i>], [edit routing-instances <i>routing-instance-name</i> system services <i>dhcp-local-server ...</i>] </pre> |
| Release Information | <p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options upto and exclude introduced in Junos OS Release 9.1.</p> |
| Description | <p>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 <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.</p> |



NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see *Configuring Integrated Routing and Bridging for Bridge Domains*.

Options **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—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***.

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

- *Extended DHCP Local Server Overview*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*

ip-address-first

Syntax ip-address-first;

Hierarchy Level [edit logical-systems *logical-system-name* system services dhcp-local-server [pool-match-order](#)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server [pool-match-order](#)],
[edit routing-instances *routing-instance-name* system services dhcp-local-server [pool-match-order](#)],
[edit system services [dhcp-local-server pool-match-order](#)]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.



Description Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.


Related Documentation

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Extended DHCP Local Server Overview*
- *Address-Assignment Pools Overview*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

key-exchange

| | |
|---------------------------------|---|
| Syntax | <code>key-exchange <algorithm></code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Release 11.2 of Junos OS. |
| Description | Specify the set of Diffie-Hellman key exchange methods that the SSH server can use. |
| Options | <ul style="list-style-type: none">• ecdh-sha2-nistp256—The ECDH key exchange method with ephemeral keys generated on the nistp256 curve.• ecdh-sha2-nistp384—The ECDH key exchange method with ephemeral keys generated on the nistp384 curve.• ecdh-sha2-nistp521—The ECDH key exchange method with ephemeral keys generated on the nistp521 curve.• group-exchange-sha2—The group exchange algorithm using SHA-2.• group-exchange-sha1—The group exchange algorithm using SHA-1.• dh-group14-sha1—The Diffie-Hellman group14 algorithm using SHA-1.• dh-group1-sha1—The Diffie-Hellman group1 algorithm using SHA-1. |
| | <div> NOTE: The key-exchange represents a set. To configure key-exchange: <code>user@host#set system services ssh key-exchange</code></div> |
| | <div> NOTE: The following options are not available on systems operating in FIPS mode: group-exchange-sha1, dh-group14-sha1, and dh-group1-sha1.</div> |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340 |

load-key-file

| | |
|---------------------------------|--|
| Syntax | load-key-file <i>URL filename</i> ; |
| Hierarchy Level | [edit system root-authentication], [edit system login user <i>username</i> authentication] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <div>  NOTE: ECDSA is not supported on the QFabric system. </div> <p>Load RSA (SSH version 1 and SSH version 2) and DSA or ECDSA (SSH version 2) public keys from a previously-generated named file at a specified URL location or local path. The file contains one or more SSH keys that are copied into the configuration when the command is issued.</p> |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Root Password on page 245 • Configuring the Root Password • Configuring Junos OS User Accounts on page 53 • Configuring Junos OS User Accounts |

local-certificate

| | |
|---------------------------------|---|
| Syntax | local-certificate; |
| Hierarchy Level | [edit system services service-deployment], [edit system services web-management https], [edit system services xnm-ssl] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Import or reference an SSL certificate. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348• <i>Generating SSL Certificates to Be Used for Secure Web Access</i>• <i>Importing SSL Certificates for Junos XML Protocol Support</i> |

lockout-period

| | |
|---------------------------------|--|
| 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 on page 57 • Handling Authorization Failure on page 59 • Example: Configuring System Retry Options on page 59 • retry-options on page 458 • <i>clear system login lockout</i> • <i>show system login lockout</i> |

logical-system-name (DHCP Local Server)

| | |
|---------------------------------|---|
| Syntax | logical-system-name; |
| Hierarchy Level | <p>[edit system services dhcp-local-server authentication username-include], [edit system services dhcp-local-server dhcpv6 authentication username-include], [edit system services dhcp-local-server dhcpv6 group group-name authentication username-include], [edit system services dhcp-local-server group group-name authentication username-include] [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...] [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system. |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• <i>Using External AAA Authentication Services with DHCP</i> |

login

```
Syntax login {
    announcement text;
    class class-name {
        allow-commands "regular-expression";
        allow-configuration-regexps "regular expression 1" "regular expression 2";
        configuration-breadcrumbs;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
            expression 2 ";
        idle-timeout minutes;
        login-script filename;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

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 user access to the router or switch.



NOTE: The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Defining Junos OS Login Classes on page 39](#)

login-alarms

Syntax login-alarms;

Hierarchy Level [edit system login class *class-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Show system alarms automatically when an **admin** user logs in to the router or switch.

Options *class-name*—Login class name.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring System Alarms to Appear Automatically Upon Login on page 46](#)

login-script (Login)

Syntax login-script *filename*;

Hierarchy Level [edit system [login class](#) *class-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Execute the specified op script when a user belonging to the class logs in to the CLI. The script must be enabled in the configuration.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Executing an Op Script](#)

mac-address (DHCP Local Server)

| | |
|---------------------------------|---|
| Syntax | mac-address; |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process. |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Using External AAA Authentication Services with DHCP</i> |

macs

| | |
|----------------------------|--|
| Syntax | <code>macs [algorithm-1 algorithm-2 ...]</code> |
| Hierarchy Level | <code>[edit system services ssh]</code> |
| 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 | <ul style="list-style-type: none">• <code>hmac-md5</code>—Hash-based MAC using Message-Digest 5 (MD5).• <code>hmac-md5-96</code>—96-bits of Hash-based MAC using MD5.• <code>hmac-md5-96-etm@openssh.com</code>—96-bits of Hash-based Encrypt-then-MAC using MD5.• <code>hmac-md5-etm@openssh.com</code>—Hash-based Encrypt-then-MAC using MD5.• <code>hmac-ripemd160</code>—Hash-based MAC using RIPEMD.• <code>hmac-ripemd160-etm@openssh.com</code>—Hash-based Encrypt-then-MAC using RIPEMD.• <code>hmac-sha1</code>—Hash-based MAC using Secure Hash Algorithm (SHA-1).• <code>hmac-sha1-96</code>—96-bits of Hash-based MAC using SHA-1.• <code>hmac-sha1-96-etm@openssh.com</code>—96-bits of Hash-based Encrypt-then-MAC using SHA-1.• <code>hmac-sha1-etm@openssh.com</code>—Hash-based Encrypt-then-MAC using SHA-1.• <code>hmac-sha2-256</code>—256-bits of Hash-based MAC using Secure Hash Algorithm (SHA-2).• <code>hmac-sha2-256-96</code>—First 96-bits of <code>hmac-sha2-256</code>.• <code>hmac-sha2-256-etm@openssh.com</code>—256-bits of Hash-based Encrypt-then-Mac using SHA-2.• <code>hmac-sha2-512</code>—512-bits of Hash-based MAC using SHA-2.• <code>hmac-sha2-512-etm@openssh.com</code>—512-bits of Hash-based Encrypt-then-Mac using SHA-2.• <code>umac-64@openssh.com</code>—Message Authentication Code using Universal Hashing specified in RFC4418.• <code>umac-64-etm@openssh.com</code>—Encrypt-then-MAC using UMAC-64 algorithm specified in RFC4418.• <code>umac-128@openssh.com</code>—UMAC-128 algorithm specified in RFC4418.• <code>umac-128-etm@openssh.com</code>—Encrypt-then-MAC using UMAC-128 algorithm specified in RFC4418. |



NOTE: The `macs` configuration statement represents a set. To configure SSH MAC algorithms:

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```



NOTE: The following options are not available on systems operating in FIPS mode: `hmac-md5`, `hmac-md5-96`, `hmac-md5-96-etm@openssh.com`, `hmac-md5-etm@openssh.com`, `hmac-ripemd160`, `hmac-ripemd160-etm@openssh.com`, `umac-64@openssh.com`, `umac-64-etm@openssh.com`, `umac-128@openssh.com`, and `umac-128-etm@openssh.com`.

| | |
|---------------------------------|---|
| 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 SSH Service for Remote Access to the Router or Switch on page 340 • <i>Junos OS Security Configuration Guide</i> |

maximum-lease-time (DHCP)

| | |
|---------------------------------|---|
| Syntax | <code>maximum-lease-time seconds</code> ; |
| Hierarchy Level | [edit system services dhcp], |
| 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> |
| Description | <p>For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.</p> <p>An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.</p> |
| Options | seconds —The maximum number of seconds the lease can be held. |
| 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 Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 • default-lease-time on page 385 |

maximum-length

| | |
|---------------------------------|--|
| Syntax | <code>maximum-length <i>length</i>;</code> |
| Hierarchy Level | [edit system login passwords] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement. |
| Default | For Junos-FIPS software, the maximum number of characters for plain-text passwords is 20. For Junos OS, no maximum is set. |
| Options | length —The maximum number of characters the password can include. Range: 1 to 64 characters |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Special Requirements for Junos OS Plain-Text Passwords on page 257• Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252• password (Login) on page 445 |

max-sessions-per-connection

| | |
|---------------------------------|---|
| Syntax | <code>max-sessions-per-connection <i>number</i></code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Release 11.4 of Junos OS. |
| Description | Specify the maximum number of ssh sessions allowed per single SSH connection. |
| Options | Default: 10 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340• ssh on page 473• Junos OS Security Configuration Guide |

maximum-time

| | |
|---------------------------------|--|
| Syntax | <code>maximum-time <i>seconds</i>;</code> |
| Hierarchy Level | <code>[edit system login retry-options]</code> |
| Release Information | Statement introduced in Junos OS Release 9.6. |
| Description | Configure the maximum time available for the user to enter the username and password for logging on to a router before the connection is closed. |
| Options | <p><i>seconds</i>—Maximum length of time that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured maximum-time, the connection is closed.</p> <p>Range: 20 through 300</p> <p>Default: 120</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57• retry-options on page 458 |

minimum-changes

| | |
|---------------------------------|---|
| Syntax | <code>minimum-changes <i>number</i>;</code> |
| Hierarchy Level | [edit system login passwords] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement is used in combination with the change-type statement. If the change-type is character-sets, then the number of character sets included in the password is checked against the specified minimum. If change-type is set-transitions, then the number of character set changes in the password is checked against the specified minimum.</p> |
| Default | For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3. |
| Options | <i>number</i> —The minimum number of character sets (or character set changes) required for the password. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257• change-type on page 377 |

minimum-length

| | |
|---------------------------------|--|
| Syntax | minimum-length <i>length</i> ; |
| Hierarchy Level | [edit system login passwords] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-upper-cases, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> |
| Default | For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10. |
| Options | length —The minimum number of characters the password must include. Range: 6 to 20 characters |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 257 • Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252 • maximum-length on page 426 |

minimum-lower-cases

| | |
|---------------------------------|---|
| Syntax | <code>minimum-lower-cases <i>number</i>;</code> |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Specify the minimum number of lower-case letters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-upper-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> |
| Options | <i>number</i> —The minimum number of lower-case letters required for the password. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257• Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252• password (Login) on page 445 |

minimum-numeric

| | |
|---------------------------------|---|
| Syntax | <code>minimum-numeric <i>number</i>;</code> |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Specify the minimum number of numeric class characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> |
| Options | <i>number</i> —The minimum number of numeric class characters required for the password. |
| 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"> • Special Requirements for Junos OS Plain-Text Passwords on page 257 • Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252 • password (Login) on page 445 |

minimum-punctuations

| | |
|---------------------------------|--|
| Syntax | <code>minimum-punctuations <i>number</i>;</code> |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Specify the minimum number of punctuation class characters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-upper-cases, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> |
| Options | <i>number</i> —The minimum number of punctuation class characters required for the password. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257• Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252• password (Login) on page 445 |

minimum-time

| | |
|---------------------------------|---|
| Syntax | minimum-time <i>seconds</i> ; |
| Hierarchy Level | [edit system login retry-options] |
| Release Information | Statement introduced in Junos OS Release 8.0. |
| Description | Configure the minimum time available for the user to enter a password to log on to a router before the connection is closed. |
| Options | <p><i>seconds</i>—Minimum length of time that the connection remains open while the user is attempting to enter a password to log in.</p> <p>Range: 20 through 60</p> <p>Default: 20</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57• retry-options on page 458 |


minimum-upper-cases

| | |
|---------------------------------|---|
| Syntax | <code>minimum-upper-cases <i>number</i>;</code> |
| Hierarchy Level | [edit system login password] |
| Release Information | Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Specify the minimum number of upper-case letters required in plain-text passwords. Newly created passwords must meet this requirement.</p> <p>This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-lower-cases, and so on.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> |
| Options | <i>number</i> —The minimum number of upper-case letters required for the password. |
| 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">• Special Requirements for Junos OS Plain-Text Passwords on page 257• Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252• password (Login) on page 445 |

next-server

| | |
|---------------------------------|---|
| Syntax | <code>next-server <i>next-server</i>;</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp pool <i>pool-id</i>], [edit system services dhcp static-binding <i>mac-address</i>] |
| Release Information | Statement introduced in Junos OS Release 8.4. |
| Description | (J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact. |
| Options | <i>next-server</i> —The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Next DHCP Server to Contact After a Boot Client Establishes Initial Communication on page 311 • Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 |

no-passwords

| | |
|---|---|
| Syntax | <code>no-passwords;</code> |
| Hierarchy Level | [edit system services ssh] |
| Description | Disable ssh password based authentication. |
| <div style="display: flex; align-items: center;">  <div> <p>NOTE: Enabling this option under [edit system services ssh] applies to SSH login service and NETCONF running over ssh services.</p> </div> </div> | |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring SSH Service for Remote Access to the Router or Switch on page 340 |

no-tcp-forwarding

| | |
|---------------------------------|---|
| Syntax | no-tcp-forwarding |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced in Release 11.4 of Junos OS. |
| Description | Use this configuration option to prevent a user from creating an SSH tunnel over a CLI session to a Junos router via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring SSH Service for Remote Access to the Router or Switch on page 340• ssh on page 473• <i>Junos OS Security Configuration Guide</i> |

option (DHCP server)

| | |
|---------------------------------|---|
| Syntax | option { [(<i>id-number</i> <i>option-type</i> <i>option-value</i>) (<i>id-number</i> array <i>option-type</i> <i>option-value</i>)]; } |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request. |
| Options | <ul style="list-style-type: none"> • <i>id-number</i>—Any whole number. The ID number is used to index the option and must be unique across a DHCP server. • <i>option-type</i>—Any of the following types: byte, byte-stream, flag, integer, ip-address, short, string, unsigned-integer, unsigned-short. • array—An option can include an array of values. • <i>option-value</i>—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type). |
| 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"> • Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server on page 314 • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i> |

option-60 (DHCP Local Server)

| | |
|---------------------------------|--|
| Syntax | option-60; |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process. |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• <i>Using External AAA Authentication Services with DHCP</i> |

option-82 (DHCP Local Server Authentication)

| | |
|---------------------------------|--|
| Syntax | <code>option-82 <circuit-id> <remote-id>;</code> |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | <p>Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.</p> |
| Options | <p>circuit-id—(Optional) Agent Circuit ID suboption (suboption 1).</p> <p>remote-id—(Optional) Agent Remote ID suboption (suboption 2).</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"> • <i>Using External AAA Authentication Services with DHCP</i> |

option-82 (DHCP Local Server Pool Matching)

| | |
|---------------------------------|--|
| Syntax | option-82; |
| Hierarchy Level | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order] |
| Release Information | Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. |
| Description | Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the ip-address-first statement before configuring the option-82 statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use</i>• <i>Extended DHCP Local Server Overview</i>• <i>Address-Assignment Pools Overview</i> |

outbound-ssh

| | |
|----------------------------|---|
| Syntax | <pre> [edit system services] outbound-ssh { client <i>client-id</i> { address { port <i>port-number</i>; retry <i>number</i>; timeout <i>seconds</i>; } device-id <i>device-id</i>; keep-alive { retry <i>number</i>; timeout <i>seconds</i>; } reconnect-strategy (in-order sticky); secret <i>password</i>; services netconf; } traceoptions { file filename <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } } </pre> |
| Hierarchy Level | [edit system services] |
| Release Information | <p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall. |
| Default | To configure transmission of the router's or switch's device ID to the application, include the device-id statement at the [edit system services] hierarchy level. |
| Options | <p>client-id—Identifies the outbound-ssh configuration stanza on the router or switch. Each outbound-ssh stanza represents a single outbound SSH connection. This attribute is not sent to the client.</p> <p>device-id—Identifies the router or switch to the client during the initiation sequence.</p> <p>keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the timeout and retry attributes.</p> <p>reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:</p> |

- **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.
- **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

secret—(Optional) Router's or switch's public SSH host key. If added to the **outbound-ssh** statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

address—Hostname or the IPv4 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

- **port**—Outbound SSH port for the client. The default is port 22.
- **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
- **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

filename—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, **mib2d** or **snmpd**). Use this option to override the default value.

files—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

size—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to **=error**, the system only records lines to the trace file that include the string **error**.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (**no-world-readable**).

all | configuration | connectivity—(Optional) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

| | |
|---------------------------------|--|
| Required Privilege Level | interface —To view this statement in the configuration. |
| | interface-control —To add this statement to the configuration. |
| Related Documentation | • Configuring Outbound SSH Service on page 342 |
| | • System Management Configuration Statements on page 358 |

password (DHCP Local Server)

| | |
|---------------------------------|---|
| Syntax | <code>password password-string;</code> |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit system services dhcp-local-server authentication],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit system services dhcp-local-server group group-name authentication]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication. |
| Options | <i>password-string</i> —Authentication password. |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Using External AAA Authentication Services with DHCP</i> |

password (Login)

| | |
|---------------------------------|---|
| Syntax | <pre>password { change-type (set-transitions character-set); format (md5 sha1 sha256 sha512); maximum-length <i>length</i>; minimum-changes <i>number</i>; minimum-length <i>length</i>; minimum-lower-cases <i>number</i>; minimum-nums <i>number</i>; minimum-punctuations <i>number</i>; minimum-upper-cases <i>number</i>; }</pre> |
| Hierarchy Level | [edit system login] |
| Release Information | <p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | <p>Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.</p> <p>Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.</p> <p>The individual statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Special Requirements for Junos OS Plain-Text Passwords on page 257 • Example: Changing the Requirements for Junos OS Plain-Text Passwords on page 252 |

permissions

| | |
|---------------------------------|---|
| Syntax | <code>permissions [<i>permissions</i>];</code> |
| Hierarchy Level | [edit system login class] |
| 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 login access privileges to be provided on the router or switch. |
| Options | <i>permissions</i> —Privilege type. For a list of permission flag types, see Table 4 on page 27 . |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Access Privilege Levels on page 63• user on page 491 |

pool (System)

| | |
|---------------------------------|--|
| Syntax | <pre>pool address/prefix-length { address-range { low address; high address; } exclude-address { address; } }</pre> |
| Hierarchy Level | [edit system services dhcp], |
| 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> |
| Description | For J Series Services Routers and EX Series switches only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool. |
| Options | <p>address-range—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)</p> <p>exclude-address—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 |

pool-match-order

| | |
|---------------------------------|---|
| Syntax | <pre>pool-match-order { external-authority; ip-address-first; option-82; }</pre> |
| Hierarchy Level | [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server] |
| Release Information | Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.1. |
| Description | Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client. The remaining statements are explained separately. |
| Default | DHCP local server uses the ip-address-first method to determine which address pool to use. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use</i>• <i>Extended DHCP Local Server Overview</i>• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i> |

port (HTTP/HTTPS)

| | |
|---------------------------------|---|
| Syntax | <code>port <i>port-number</i>;</code> |
| Hierarchy Level | [edit system services web-management] |
| 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 port on which the HTTP or HTTPS service is connected. |
| Options | <i>port-number</i> —The TCP port number on which the specified service listens. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i>• <i>J-Web Interface User Guide</i>• http on page 410• https on page 411• web-management on page 495 |

port (NETCONF Server)

| | |
|----------------------------|---|
| Syntax | <code>port <i>port-number</i>;</code> |
| Hierarchy Level | [edit system services netconf] |
| Release Information | Statement introduced in Junos OS Release 10.0. |
| Description | Configure the TCP port used for NETCONF-over-SSH connections. |



NOTE:

- The configured port accepts only NETCONF-over-SSH connections. Regular SSH session requests for this port are rejected.
 - The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, you can specify this in the login event script.
 - We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.
-

| | |
|---------------------------------|--|
| Options | port <i>port-number</i> —Port number on which to enable incoming NETCONF connections over SSH. Default: 830 (as specified in RFC 4742, <i>Using the NETCONF Configuration Protocol over Secure Shell (SSH)</i>) Range: 1 through 65535 |
| 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">• NETCONF XML Management Protocol Guide• Configuring NETCONF-Over-SSH Connections on a Specified TCP Port on page 348 |

port (RADIUS Server)

| | |
|----------------------------|---|
| Syntax | <code>port <i>port-number</i>;</code> |
| Hierarchy Level | <code>[edit system radius-server <i>address</i>],</code> <code>[edit system accounting destination radius server <i>address</i>]</code> |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| Description | Configure the port number on which to contact the RADIUS server. |
| Options | <i>number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865) |



NOTE: The `[edit system accounting]` hierarchy is not available on QFabric systems.

| | |
|---------------------------------|---|
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring RADIUS Authentication on page 267 • Configuring RADIUS Authentication (QFX Series or OCX Series) |

port (SRC Server)

| | |
|---------------------------------|--|
| Syntax | <code>port <i>port-number</i>;</code> |
| Hierarchy Level | <code>[edit system services service-deployment servers <i>server-address</i>]</code> |
| 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 port number on which to contact the SRC server. |
| Options | <i>port-number</i> —(Optional) The TCP port number for the SRC server. Default: 3333 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Junos OS to Work with SRC Software on page 350 |

port (TACACS+ Server)

| | |
|---------------------------------|---|
| Syntax | <code>port port-number;</code> |
| Hierarchy Level | [edit system accounting destination tacplus server <i>server-address</i>] |
| 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 port number on which to contact the TACACS+ server. |
| Options | <i>number</i> —Port number on which to contact the TACACS+ server. Default: 49 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring TACACS+ System Accounting on page 295 |


protocol-version

| | |
|---------------------------------|--|
| Syntax | <code>protocol-version version;</code> |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Specify the secure shell (SSH) protocol version. |
| Default | v2—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4. |
| Options | <i>version</i> —SSH protocol version: v1, v2, or both. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the SSH Protocol Version on page 341 |

radius (System)

| | |
|---------------------------------|---|
| Syntax | <pre>radius { server { server-address { accounting-port port-number; secret password; source-address address; retry number; timeout seconds; } } }</pre> |
| Hierarchy Level | [edit system accounting destination] |
| Release Information | <p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| Description | Configure the RADIUS accounting server. |
| Options | <p>server-address—Address of the RADIUS accounting server.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring RADIUS System Accounting on page 276 |

radius-options (edit system)

| | |
|---|---|
| Syntax | <pre>radius-options { attributes { nas-ip-address <i>ip-address</i>; } enhanced-accounting; password-protocol <i>mschap-v2</i>; }</pre> |
| Hierarchy Level | [edit system] |
| Release Information | <p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.</p> <p>MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> |
| <hr/> | |
| <div> NOTE: The <code>radius-options</code> statement is not available on QFabric systems.</div> <hr/> | |
| <p>enhanced-accounting statement introduced in Junos OS Release 14.1.</p> | |
| Description | Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets. |
| Options | <p>enhanced-accounting—View the attribute values of a logged in user.</p> <p>nas-ip-address <i>ip-address</i>—IP address of the network access server (NAS) that requests user authentication.</p> <p>password-protocol <i>mschap-v2</i>—Protocol MS-CHAPv2, used for password authentication and password changing.</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">• <i>Configuring MS-CHAPv2 for Password-Change Support</i>• <i>Configuring RADIUS Authentication (QFX Series or OCX Series)</i>• Configuring RADIUS System Accounting on page 276• enhanced-accounting on page 403 |

radius-server (System)

| | |
|---------------------------------|---|
| Syntax | <pre>radius-server server-address { accounting-port port-number; port number; retry number; secret password; source-address source-address; timeout seconds; }</pre> |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | <p>Configure a RADIUS server for Point-to-Point Protocol (PPP).</p> <p>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.</p> |
| Options | <p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring RADIUS Authentication on page 267 |

rate-limit

| | |
|---------------------------------|--|
| Syntax | <code>rate-limit <i>limit</i>;</code> |
| 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 before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service. |
| Default | 150 connections |
| Options | rate-limit <i>limit</i> —(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6). Range: 1 through 250 Default: 150 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348 |

retry (RADIUS)

| | |
|---------------------------------|--|
| Syntax | <code>retry number;</code> |
| Hierarchy Level | [edit system radius-server <i>server-address</i>], [edit system accounting destination radius server <i>server-address</i>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server. |
| Options | number —Number of retries allowed for contacting a RADIUS server. Range: 1 through 10 Default: 3 |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring RADIUS Authentication on page 267• Configuring RADIUS System Accounting on page 276• timeout on page 479 |

retry-options

| | |
|---------------------------------|---|
| Syntax | <pre>retry-options { backoff-factor <i>seconds</i>; backoff-threshold <i>number</i>; maximum-time <i>seconds</i>; minimum-time <i>seconds</i>; tries-before-disconnect <i>number</i>; }</pre> |
| Hierarchy Level | [edit system login] |
| Release Information | <p>Statement introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>maximum-time option introduced in Junos OS Release 9.6.</p> <p>maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.</p> |
| Description | Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected. |
| 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 on page 57• rate-limit on page 456 |

root-login

| | |
|---------------------------------|--|
| Syntax | root-login (allow deny deny-password); |
| Hierarchy Level | [edit system services ssh] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| Description | Control user access through SSH. |
| Default | Allow user access through SSH. |
| Options | <p>allow—Allow users to log in to the router or switch as root through SSH.</p> <p>deny—Disable users from logging in to the router or switch as root through SSH.</p> <p>deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Root Login Through SSH on page 341 |

router

| | |
|---------------------------------|---|
| Syntax | <pre>router { address; }</pre> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp], [edit system services dhcp-service], [edit system services dhcp-service pool], [edit system services dhcp-service static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement for EX Series switches introduced in Junos OS Release 9.0. |
| Description | For J Series Services Routers and EX Series switches only, specify IPv4 addresses for one or more devices available to a DHCP client. List devices (switches or routers) in order of preference. |
| Options | address —IPv4 address of the router or switch. To configure multiple devices, include multiple address options. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i> |

routing-instance-name (DHCP Local Server)

| | |
|---------------------------------|--|
| Syntax | routing-instance-name; |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. |
| 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**
- *Using External AAA Authentication Services with DHCP*

secret

| | |
|---------------------------------|---|
| Syntax | <code>secret password;</code> |
| Hierarchy Level | [edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>] |
| 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 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. |
| Options | <i>password</i> —Password to use; can include spaces included 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 | <ul style="list-style-type: none">• Configuring RADIUS Authentication on page 267• Configuring TACACS+ Authentication on page 285• Configuring TACACS+ System Accounting on page 295• Configuring RADIUS System Accounting on page 276 |

server (RADIUS Accounting)

| | |
|---------------------------------|--|
| Syntax | <pre>server { server-address { accounting-port port-number; retry number secret password; source-address address; timeout seconds; } }</pre> |
| Hierarchy Level | [edit system accounting destination radius] |
| Release Information | Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure RADIUS logging. 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 | <ul style="list-style-type: none"> • Configuring RADIUS System Accounting on page 276 |

server (TACACS+ Accounting)

| | |
|---------------------------------|---|
| Syntax | <pre>server { server-address { port port-number; secret password; single-connection; timeout seconds; } }</pre> |
| Hierarchy Level | [edit system accounting destination tacplus] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure TACACS+ logging. 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 | <ul style="list-style-type: none"> • Configuring TACACS+ System Accounting on page 295 |

servers

| | |
|---------------------------------|--|
| Syntax | <code>servers server-address { port port-number; }</code> |
| Hierarchy Level | [edit system services service-deployment] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure an IPv4 address for the Session and Resource Control (SRC) server. |
| Options | server-address —The TCP port number. Default: 3333 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 | <ul style="list-style-type: none">• Configuring the Junos OS to Work with SRC Software on page 350 |

server-identifier

| | |
|---------------------------------|--|
| Syntax | <code>server-identifier <i>address</i>;</code> |
| Hierarchy Level | <code>[edit system services dhcp],</code> <code>[edit system services dhcp pool],</code> <code>[edit system services dhcp static-binding]</code> |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>For J Series Services Routers and EX Series switches only. Configure a server identifier. The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).</p> <p>Servers include the server identifier in DHCPOFFER messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in DHCPREQUEST messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.</p> <p>This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.</p> |
| Default | If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on fe-0/0/0 and the primary interface address is 1.1.1.1 , then the server identifier is set to 1.1.1.1 . |
| Options | address —IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding). |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 |

service-deployment

| | |
|---------------------------------|--|
| Syntax | <pre>service-deployment { servers <i>server-address</i> { port <i>port-number</i>; } source-address <i>source-address</i>; }</pre> |
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Enable Junos OS to work with the Session and Resource Control (SRC) software. 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 | <ul style="list-style-type: none">• Configuring the Junos OS to Work with SRC Software on page 350 |

services (System Services)

```
Syntax  services {
    dhcp { \* DHCP not supported on a DCF
        dhcp_services;
    }
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        connection-limit limit;
        protocol-version [v1 v2];
        rate-limit limit;
        root-login (allow | deny | deny-password);
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {
        http {
            interfaces [ names ];
            port port;
        }
        https {
            interfaces [ names ];
            local-certificate name;
            port port;
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ limit ];
        }
    }
    xnm-clear-text {
        connection-limit limit;
        rate-limit limit;
    }
    xnm-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
        ssl-renegotiation;
    }
}
```

```
}  
}
```

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 router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348](#)
- [Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317](#)
- [Configuring the Junos OS to Work with SRC Software on page 350](#)

session (Time-out)

| | |
|---------------------------------|--|
| Syntax | <pre>session { idle-timeout <i>minutes</i>; session-limit <i>session-limit</i>; }</pre> |
| Hierarchy Level | [edit system services web-management] |
| Release Information | <p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions. |
| Options | <p>idle-timeout <i>minutes</i>—Configure the number of minutes a session can be idle before it times out.</p> <p>Range: 1 through 1440</p> <p>Default: 1440</p> <p>session-limit <i>session-limit</i>—Configure the maximum number of simultaneous J-Web user login sessions.</p> <p>Range: 1 through 1024</p> <p>Default: Unlimited</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"> • <i>J-Web Interface User Guide</i> |

single-connection

| | |
|---------------------------------|--|
| 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 before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | 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. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring TACACS+ Authentication on page 285• Configuring TACACS+ System Accounting on page 295 |

source-address (NTP, RADIUS, System Logging, or TACACS+)

| | |
|---------------------------------|--|
| Syntax | <code>source-address <i>source-address</i> <routing-instance <i>routing-instance-name</i>>;</code> |
| Hierarchy Level | <p>[edit system accounting destination radius <i>server</i> <i>server-address</i>],</p> <p>[edit system accounting destination tacplus <i>server</i> <i>server-address</i>],</p> <p>[edit system ntp],</p> <p>[edit system <i>radius-server</i> <i>server-address</i>],</p> <p>[edit system syslog],</p> <p>[edit system <i>tacplus-server</i> <i>server-address</i>]</p> |
| 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>routing-instance option added in Junos OS Release 14.1</p> |
| Description | Specify a source address for each configured IPv4 or IPv6 TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. |
| Options | <p>source-address—A valid IP address configured on one of the router or switch interfaces. 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 or to the TX Matrix router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) The routing instance name in which the source address is defined.</p> <p>Default: The primary address of the interface</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring RADIUS Authentication on page 267 • <i>Synchronizing and Coordinating Time Distribution Using NTP</i> • <i>Specifying an Alternative Source Address for System Log Messages</i> |

source-address (SRC Software)

| | |
|---------------------------------|---|
| Syntax | <code>source-address <i>source-address</i>;</code> |
| Hierarchy Level | [edit system services service-deployment] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Enable Junos OS to work with the Session and Resource Control (SRC) software. |
| Options | <i>source-address</i> — Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Junos OS to Work with SRC Software on page 350 |

source-port (Port Addresses)

| | |
|---------------------------------|--|
| Syntax | <code>source-port upper-limit <<i>upper-limit</i>>;</code> |
| Hierarchy Level | [edit system internet-options] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the range of port addresses. |
| Options | <i>upper-limit upper-limit</i> —(Optional) The range of port addresses and can be a value from 5000 through 65,355. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Junos OS to Extend the Default Port Address Range |

ssh

| | |
|---------------------------------|---|
| Syntax | <pre>ssh { ciphers [cipher-1 cipher-2 cipher-3 ...]; client-alive-count-max seconds; client-alive-interval seconds; connection-limit limit; hostkey-algorithm <algorithm no-algorithm>; key-exchange <algorithm>; macs <algorithm>; max-sessions-per-connection <number>; no-passwords; no-tcp-forwarding; protocol-version [v1 v2]; rate-limit limit; root-login (allow deny deny-password); }</pre> |
| Hierarchy Level | [edit system services] |
| Release Information | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>client-alive-interval and client-alive-max-count statements introduced in Junos OS Release 12.2.</p> <p>no-passwords statement introduced in Junos OS Release 13.3.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| Description | <p>Allow SSH requests from remote systems to the local router or switch.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring SSH Service for Remote Access to the Router or Switch on page 340 |

ssl-renegotiation

| | |
|---------------------------------|--|
| Syntax | ssl-renegotiation; |
| Hierarchy Level | [edit system services xnm-ssl] |
| Release Information | Statement introduced in Junos OS Release 13.3. |
| Description | Enable or disable SSL re-negotiation for xnm-ssl service. |
| Default | SSL re-negotiation for xnm-ssl service is disabled by default. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348 |

static-binding

| | |
|---------------------------------|---|
| Syntax | <pre>static-binding mac-address { client-identifier (ascii <i>client-id</i> hexadecimal <i>client-id</i>); fixed-address { address; } host-name <i>client-hostname</i>; }</pre> |
| Hierarchy Level | <pre>[edit system services dhcp], [edit system services dhcp]</pre> |
| 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> |
| Description | <p>For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.</p> |
| Options | <p>mac-address—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.</p> <p>fixed-address <i>address</i>—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.</p> <p>host-name <i>client-hostname</i>—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the domain-name statement.</p> <p>client-identifier (ascii <i>client-id</i> hexadecimal <i>client-id</i>)—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, <i>Assigned Numbers</i>. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.</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 Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317 • Configuring a DHCP Server on Switches (CLI Procedure) |

system

| | |
|--------------------------|---|
| Syntax | system { ... } |
| Hierarchy Level | [edit] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure system management properties. Set values in the edit system hierarchy of the configuration. |
| 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">• System Management Configuration Statements on page 358 |

tacplus

| | |
|--------------------------|---|
| Syntax | <pre>tacplus { server { server-address { port port-number; secret password; single-connection; timeout seconds; } } }</pre> |
| Hierarchy Level | [edit system accounting destination] |
| 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 Terminal Access Controller Access Control System Plus (TACACS+). |
| Options | server-address —Address of the TACACS+ authentication server. 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 | <ul style="list-style-type: none">• Configuring TACACS+ System Accounting on page 295 |

tacplus-options

| | |
|---------------------------------|---|
| 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 291 • Configuring TACACS+ Server Accounting on page 295 • Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication on page 32 • enhanced-accounting on page 403 |

tacplus-server

| | |
|---------------------------------|--|
| Syntax | <pre>tacplus-server server-address { secret password; single-connection; source-address source-address; timeout seconds; }</pre> |
| 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 IPv4 or IPv6 TACACS+ server. |
| Options | server-address —Address of the IPv4 or IPv6 TACACS+ authentication server. 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 | <ul style="list-style-type: none">• Configuring TACACS+ Authentication on page 285 |

telnet

| | |
|---------------------------------|--|
| Syntax | <pre>telnet { connection-limit limit; rate-limit limit; }</pre> |
| Hierarchy Level | [edit system services] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Provide Telnet connections from remote systems to the local router or switch. 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 | <ul style="list-style-type: none">• Configuring Telnet Service for Remote Access to a Router or Switch on page 338 |

timeout (System)

| | |
|---------------------------------|---|
| Syntax | <code>timeout seconds;</code> |
| Hierarchy Level | [edit system radius-server server-address], [edit system tacplus-server server-address], [edit system accounting destination radius server server-address], [edit system accounting destination tacplus server server-address] |
| 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 amount of time that the local router or switch waits to receive a response from a RADIUS or TACACS+ server. |
| Options | 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. |
| Related Documentation | <ul style="list-style-type: none">• Configuring RADIUS Authentication on page 267• Configuring TACACS+ Authentication on page 285• retry on page 457 |

traceoptions (Address-Assignment Pool)

| | |
|----------------------------|--|
| Syntax | <pre>traceoptions { file <i>filename</i> { files <i>number</i>; size <i>maximum-file-size</i>; match <i>regex</i>; (world-readable no-world-readable); } flag address-assignment; flag all; flag configuration; flag framework; flag ldap; flag local-authentication; flag radius; }</pre> |
| Hierarchy Level | [edit system processes general-authentication-service] |
| Release Information | Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0. option-name option introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure tracing options. |
| Options | <p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• address-assignment—All address-assignment events• all—All tracing operations• configuration—Configuration events• framework—Authentication framework events• ldap—LDAP authentication events• local-authentication—Local authentication events |

- **radius**—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

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 and filename.

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 | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
|---------------------------------|---|

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring Address-Assignment Pools</i> |
|------------------------------|---|

traceoptions (DHCP)

| | |
|----------------------------|--|
| Syntax | <pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre> |
| Hierarchy Level | [edit system processes dhcp-service] |
| Release Information | Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches. |
| Description | <p>Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.</p> <p>Replaces deprecated traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p> |
| Options | <p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:</p> <ul style="list-style-type: none">• all—Trace all events.• auth—Trace authentication events.• database—Trace database events.• fwd—Trace firewall process events.• general—Trace miscellaneous events.• ha—Trace high availability-related events.• interface—Trace interface operations.• io—Trace I/O operations.• liveness-detection—Trace liveness detection operations.• packet—Trace packet and option decoding operations.• performance—Trace performance measurement operations.• profile—Trace profile operations. |

- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **security-persistence**—Trace security persistence events.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (***maximum-file-sizek***), megabytes (***maximum-file-sizem***), or gigabytes (***maximum-file-sizeg***). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Range: 10,240 through 1,073,741,824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

| | |
|---------------------------------|---|
| Required Privilege Level | trace —To view this statement in the configuration. trace-control —To add this statement to the configuration. |
|---------------------------------|---|

Related Documentation • *Tracing Extended DHCP Operations*

traceoptions (DHCP Server)

| | |
|----------------------------|---|
| Syntax | <pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre> |
| Hierarchy Level | [edit system services dhcp] |
| Release Information | <p>Statement for tracing J Series Services Router DHCP processes introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | Define tracing operations for DHCP processes for J Series Services Routers and EX Series switches. |
| Options | <p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory <i>/var/log</i>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—All tracing operations • binding—Trace binding operations • config—Log reading of configuration • conflict—Trace user-detected conflicts for IP addresses • event—Trace important events • ifdb—Trace interface database operations • io— Trace I/O operations • lease—Trace lease operations • main—Trace main loop operations • misc— Trace miscellaneous operations • packet—Trace DHCP packets |

- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**—Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**—Trace interface database operations
- **io**—Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **match *regex***—Refine the output to include lines that contain the regular expression.
- **misc**—Trace miscellaneous operations
- **packet**—Trace DHCP packets
- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

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). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

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 | system—To view this statement in the configuration. |
| | system-control—To add this statement to the configuration. |

| | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none"> • Configuring Tracing Operations for DHCP Processes on page 318 • System Management Configuration Statements on page 358 |
|------------------------------|---|

traceoptions (SBC Configuration Process)

| | |
|----------------------------|---|
| Syntax | <pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; }</pre> |
| Hierarchy Level | [edit system processes sbc-configuration-process] |
| Release Information | Statement introduced in Junos OS Release 9.5. Statement introduced in Junos OS Release 9.5 for EX Series switches. |
| Description | Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG). |
| Options | <p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory <code>/var/log</code>. You can include the following file options:</p> <ul style="list-style-type: none">• files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000 Default: 3 files</p> <ul style="list-style-type: none">• match <i>regex</i>—(Optional) Refine the output to include lines that contain the regular expression.• no-world-readable—(Optional) Disable unrestricted file access.• size <i>size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename. <p>Syntax: <i>xk</i> to specify KB, <i>xm</i> to specify MB, or <i>xg</i> to specify GB. Range: 10 KB through 1 GB Default: 128 KB</p> <ul style="list-style-type: none">• world-readable—(Optional) Enable 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-level**—Trace all SBC process operations.
- **common trace-level**—Trace common events.
- **configuration trace-level**—Trace configuration events.
- **device-monitor trace-level**—Trace device monitor events.
- **ipc trace-level**—Trace IPC events.
- **memory—pool trace-level**—Trace memory pool events.
- **trace-level**—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the **trace-level**:
 - **debug**—Log all code flow of control.
 - **error**—Log failures with a short-term effect.
 - **info**—Log summary for normal operations, such as the policy decisions made for a call.
 - **trace**—Log program trace START and EXIT macros.
 - **warning**—Log failure recovery events or failure of an external entity.
- **ui trace-level**—Trace user interface operations.

| | |
|---------------------------------|---|
| 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"> • See “Troubleshooting the IMSG” in the <i>Junos Multiplay Solutions Guide</i> • System Management Configuration Statements on page 358 |
|------------------------------|--|

tries-before-disconnect

| | |
|---------------------------------|---|
| Syntax | <code>tries-before-disconnect <i>number</i>;</code> |
| Hierarchy Level | <code>[edit system login retry-options]</code> |
| Release Information | Statement introduced in Junos OS Release 8.0. |
| Description | Configure the maximum number of times the user is allowed to enter a password to attempt to log in to the router through SSH or Telnet. |
| Options | <p><i>number</i>—Maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet.</p> <p>Range: 1 through 10</p> <p>Default: 10</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Limiting the Number of User Login Attempts for SSH and Telnet Sessions on page 57• retry-options on page 458 |

uid

| | |
|---------------------------------|--|
| Syntax | <code>uid <i>uid-value</i>;</code> |
| Hierarchy Level | <code>[edit system login user]</code> |
| 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> |
| Description | Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring. |
| Options | <p><i>uid-value</i>—Number associated with the login account. This value must be unique on the router or switch.</p> <p>Range: 100 through 64000</p> |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Configuring Junos OS User Accounts on page 53 |

user (Access)

| | |
|---------------------------------|--|
| Syntax | <pre> user username { authentication { class class-name; (encrypted-password "password" plain-text-password); full-name complete-name; load-key-file URL filename; ssh-dsa "public-key" <from hostname>; ssh-rsa "public-key" <from hostname>; uid uid-value; } } </pre> |
| Hierarchy Level | [edit system login] |
| 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> |
| Description | Configure access permission for individual users. |
| Options | The remaining statements are explained separately. |
| Required Privilege Level | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring Junos OS User Accounts on page 53 • class on page 380 |

username-include (DHCP Local Server)

| | |
|---------------------------------|---|
| Syntax | <pre>username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name ; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; }</pre> |
| Hierarchy Level | <p>[edit system services dhcp-local-server authentication], [edit system services dhcp-local-server dhcpv6 authentication], [edit system services dhcp-local-server dhcpv6 group group-name authentication], [edit system services dhcp-local-server group group-name authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | <p>Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.</p> <p>The statements are explained separately. The option-60 and option-82 statements are not supported in the DHCPv6 hierarchy levels. The <i>client-id</i>, <i>relay-agent-interface-id</i>, <i>relay-agent-remote-id</i> and <i>relay-agent-subscriber-id</i> statements are supported in the DHCPv6 hierarchy levels only.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP• Creating Unique Usernames for DHCP Clients |

user-prefix (DHCP Local Server)

| | |
|---------------------------------|--|
| Syntax | <code>user-prefix <i>user-prefix-string</i>;</code> |
| Hierarchy Level | <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> |
| Description | Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process. |
| Options | <i>user-prefix-string</i> —User prefix string. |
| 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 • *Using External AAA Authentication Services with DHCP*

versioning

| | |
|---------------------------------|---|
| Syntax | versioning; |
| Hierarchy Level | [edit system dynamic-profile-options] |
| Release Information | Statement introduced in Junos OS Release 11.4. |
| Description | Enable version support for dynamic profiles on the system. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | • <i>Enabling Dynamic Profiles to Use Multiple Versions</i> |

web-management

| | |
|---------------------------------|--|
| Syntax | <pre>web-management { http { interfaces [<i>interface-names</i>]; port <i>port</i>; } https { interfaces [<i>interface-names</i>]; local-certificate <i>name</i>; port <i>port</i>; } }</pre> |
| Hierarchy Level | [edit system services] |
| Release Information | <p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> |
| Description | <p>Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 410 • https on page 411 • port on page 449 |

wins-server (System)

| | |
|---------------------------------|--|
| Syntax | <code>wins-server { address; }</code> |
| Hierarchy Level | [edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as 192.168.1.3) to Windows NetBIOS names (such as \\Marketing). List servers in order of preference. |
| Options | address —IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple address options. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers on page 317• Configuring a DHCP Server on Switches (CLI Procedure) |

xnm-clear-text

| | |
|---------------------------------|--|
| Syntax | xnm-clear-text { <code>connection-limit</code> <i>limit</i> ; <code>rate-limit</code> <i>limit</i> ; } |
| Hierarchy Level | [edit system <code>services</code>] |
| Release Information | Statement introduced before Junos OS Release 7.4. |
| Description | Allow Junos XML protocol clear-text requests from remote systems to the local router. 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 | <ul style="list-style-type: none"> • Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348 |

xnm-ssl

| | |
|---------------------------------|--|
| Syntax | xnm-ssl { <code>connection-limit</code> <i>limit</i> ; <code>rate-limit</code> <i>limit</i> ; <code>ssl-renegotiation</code> ; } |
| Hierarchy Level | [edit system <code>services</code>] |
| Release Information | Statement introduced before Junos OS Release 7.4. Support for the <code>ssl-renegotiation</code> statement added in Junos OS Release 13.3. |
| Description | Allow Junos XML protocol SSL requests from remote systems to the local router. 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 | <ul style="list-style-type: none"> • Configuring clear-text or SSL Service for Junos XML Protocol Client Applications on page 348 |

CHAPTER 14

Operational Commands

- `show cli authorization`
- `clear system services dhcp binding`
- `clear system services dhcp conflict`
- `clear system services dhcp statistics`
- `show system services dhcp binding`
- `show system services dhcp conflict`
- `show system services dhcp global`
- `show system services dhcp pool`
- `show system services dhcp statistics`
- `show system services service-deployment`
- `show system users`
- `ssh`
- `telnet`
- `test access profile`
- `test access radius-server`

show cli authorization

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

- Related** • *show cli*
Documentation • *show cli directory*

clear system services dhcp binding

| | |
|---------------------------------|---|
| Syntax | clear system services dhcp binding <address> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool. |
| Options | address —(Optional) Remove a specific IP address binding and return it to the address pool. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none">• show system services dhcp binding on page 505 |
| List of Sample Output | clear system services dhcp binding on page 502 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

clear system services dhcp binding

```
user@host> clear system services dhcp binding
```

clear system services dhcp conflict

| | |
|---------------------------------|---|
| Syntax | clear system services dhcp conflict <address> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool. |
| Options | address —(Optional) Remove a specific IP address from the conflict list and return it to the address pool. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none">• show system services dhcp conflict on page 508 |
| List of Sample Output | clear system services dhcp conflict on page 503 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

clear system services dhcp conflict

```
user@host> clear system services dhcp conflict
```

clear system services dhcp statistics

| | |
|---------------------------------|---|
| Syntax | clear system services dhcp statistics |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics. |
| Options | This command has no options. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none">• show system services dhcp statistics on page 513 |
| List of Sample Output | clear system services dhcp statistics on page 504 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

clear system services dhcp statistics

```
user@host> clear system services dhcp statistics
```

show system services dhcp binding

| | |
|---------------------------------|---|
| Syntax | show system services dhcp binding <detail> <address> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information. |
| Options | <p>none—Display brief information about all active client bindings.</p> <p>detail—(Optional) Display detailed information about all active client bindings.</p> <p>address—(Optional) Display detailed client binding information for the specified IP address only.</p> |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none"> • clear system services dhcp binding on page 502 |
| List of Sample Output | show system services dhcp binding on page 506 show system services dhcp binding address on page 506 show system services dhcp binding address detail on page 506 |
| Output Fields | Table 15 on page 505 describes the output fields for the show system services dhcp binding command. Output fields are listed in the approximate order in which they appear. |

Table 15: show system services dhcp binding Output Fields

| Field Name | Field Description | Level of Output |
|--------------------------|--|-----------------|
| Allocated address | List of IP addresses the DHCP server has assigned to clients. | All levels |
| MAC address | Corresponding media access control (MAC) hardware address of the client. | All levels |
| Client identifier | (address option only) Client's unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings. | All levels |
| Binding Type | Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses. | All levels |
| Lease Expires at | Time the lease expires or never for leases that do not expire. | All levels |
| Lease Obtained at | (address option only) Time the client obtained the lease from the DHCP server. | detail |

Table 15: show system services dhcp binding Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|----------------------------|---|-----------------|
| State | Status of the binding. Bindings can be active or expired. | detail |
| Pool | Address pool that contains the IP address assigned to the client. | detail |
| Request received on | Interface on which the DHCP message exchange occurs. The IP address pool is configured based on the interface's IP address. If a relay agent is used, its IP address is also displayed. | detail |
| DHCP options | User-defined options created for the DHCP server. If no options have been defined, this field is blank. | detail |

Sample Output

show system services dhcp binding

```
user@host> show system services dhcp binding

Allocated address  MAC address      Binding Type  Lease expires at
192.168.1.2        00:a0:12:00:12:ab  static       never
192.168.1.3        00:a0:12:00:13:02  dynamic      2004-05-03 13:01:42 PDT
```

show system services dhcp binding address

```
user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00
3a 31 33 3a 30 32:13:02

Lease information:
  Binding Type dynamic
  Obtained at 2004-05-02 13:01:42 PDT
  Expires at 2004-05-03 13:01:42 PDT
```

show system services dhcp binding address detail

```
user@host> show system services dhcp binding 192.168.1.3 detail

DHCP binding information:
Allocated address      192.168.1.3
MAC address 00:a0:12:00:12:ab
Pool                  192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254

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: 19, Type: flag, Value: off
Code: 40, Type: string, Value: domain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33

show system services dhcp conflict

| | |
|---------------------------------|---|
| Syntax | show system services dhcp conflict |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool. |
| Options | This command has no options. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none"> clear system services dhcp conflict on page 503 |
| List of Sample Output | show system services dhcp conflict on page 508 |
| Output Fields | Table 16 on page 508 describes the output fields for the show system services dhcp conflict command. Output fields are listed in the approximate order in which they appear. |

Table 16: show system services dhcp conflict Output Fields

| Field Name | Field Description |
|------------------|--|
| Detection time | Date and time the client detected the conflict. |
| Detection method | How the conflict was detected. |
| Address | IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a clear system services dhcp conflict command to manually clear the list. |

Sample Output

show system services dhcp conflict

```
user@host> show system services dhcp conflict
```

```

Detection time      Detection method  Address
2004-08-03 19:04:00 PDT  ARP              3.3.3.5
2004-08-04 04:23:12 PDT  Ping             4.4.4.8
2004-08-05 21:06:44 PDT  Client           3.3.3.10
```

show system services dhcp global

| | |
|---------------------------------|--|
| Syntax | show system services dhcp global |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients. |
| Options | This command has no options. |
| Required Privilege Level | view and system |
| List of Sample Output | show system services dhcp global on page 510 |
| Output Fields | Table 17 on page 509 describes the output fields for the show system services dhcp global command. Output fields are listed in the approximate order in which they appear. |

Table 17: show system services dhcp global Output Fields

| Field Name | Field Description |
|---------------------------|---|
| BOOTP lease length | Length of lease time assigned to BOOTP clients. |
| Default lease time | Lease time assigned to clients that do not request a specific lease time. |
| Minimum lease time | Minimum time a client retains an IP address lease on the server. |
| Maximum lease time | Maximum time a client can retain an IP address lease on the server. |
| DHCP options | User-defined options created for the DHCP server. If no options have been defined, this field is blank. |

Sample Output

show system services dhcp global

```
user@host> show system services dhcp global

Global settings:
  BOOTP lease length      infinite

DHCP lease times:
  Default lease time      1 hour
  Minimum lease time      2 hours
  Maximum lease time      infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp pool

| | |
|---------------------------------|--|
| Syntax | show system services dhcp pool <detail> <subnet-address> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools. |
| Options | none —Display brief information about all IP address pools. detail —(Optional) Display detailed information. subnet-address —(Optional) Display information for the specified subnet address. |
| Required Privilege Level | view and system |
| List of Sample Output | show system services dhcp pool on page 512 show system services dhcp pool subnet-address on page 512 show system services dhcp pool subnet-address detail on page 512 |
| Output Fields | Table 18 on page 511 describes the output fields for the show system services dhcp pool command. Output fields are listed in the approximate order in which they appear. |

Table 18: show system services dhcp pool Output Fields

| Field Name | Field Description | Level of Output |
|--------------------|--|-----------------|
| Pool name | Subnet on which the IP address pool is defined. | None specified |
| Low address | Lowest address in the IP address pool. | None specified |
| High address | Highest address in the IP address pool. | None specified |
| Excluded addresses | Addresses excluded from the address pool. | None specified |
| Subnet | (<i>subnet-address</i> option only) Subnet to which the specified address pool belongs. | None specified |
| Address range | (<i>subnet-address</i> option only) Range of IP addresses in the address pool. | None specified |
| Addresses assigned | Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool. | detail |
| Active | Number of assigned IP addresses in the pool that are active. | detail |
| Excluded | Number of assigned IP addresses in the pool that are excluded. | detail |
| Default lease time | Lease time assigned to clients that do not request a specific lease time. | detail |

Table 18: show system services dhcp pool Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|--------------------|---|-----------------|
| Minimum lease time | Minimum time a client can retain an IP address lease on the server. | detail |
| Maximum lease time | Maximum time a client can retain an IP address lease on the server. | detail |
| DHCP options | User-defined options created for the DHCP server. If no options have been defined, this field is blank. | detail |

Sample Output

show system services dhcp pool

```
user@host> show system services dhcp pool

Pool name      Low address    High address    Excluded addresses
3.3.3.0/24     3.3.3.2       3.3.3.254     3.3.3.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 3.3.3.0/24

Pool information:
  Subnet                3.3.3.0/24
  Address range         3.3.3.2 - 3.3.3.254
  Addresses assigned    2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 3.3.3.0/24 detail

Pool information:
  Subnet                3.3.3.0/24
  Address range         3.3.3.2 - 3.3.3.254
  Addresses assigned    2/253
  Active: 1, Excluded: 1

DHCP lease times:
  Default lease time    1 hour
  Minimum lease time    2 hours
  Maximum lease time    infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Name: router, Value: { 3.3.3.1 }
  Name: server-identifier, Value: 3.3.3.1
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.333.3.3.254 3.3.3.1
```

show system services dhcp statistics

| | |
|---------------------------------|---|
| Syntax | show system services dhcp statistics |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | (J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics. |
| Options | This command has no options. |
| Required Privilege Level | view and system |
| Related Documentation | <ul style="list-style-type: none"> • clear system services dhcp statistics on page 504 |
| List of Sample Output | show system services dhcp statistics on page 514 |
| Output Fields | Table 19 on page 513 describes the output fields for the show system services dhcp statistics command. Output fields are listed in the approximate order in which they appear. |

Table 19: show system services dhcp statistics Output Fields

| Field Name | Field Description |
|---------------------------|---|
| Default lease time | Lease time assigned to clients that do not request a specific lease time. |
| Minimum lease time | Minimum time a client can retain an IP address lease on the server. |
| Maximum lease time | Maximum time a client can retain an IP address lease on the server. |
| Packets dropped | Total number of packets dropped and number of packets dropped because of: <ul style="list-style-type: none"> • Invalid hardware address • Invalid opcode • Invalid server address • No available address • No interface match • No routing instance match • No valid local addresses • Packet too short • Read error • Send error |

Table 19: show system services dhcp statistics Output Fields (*continued*)

| Field Name | Field Description |
|--------------------------|---|
| Messages received | <p>Number of the following message types sent from DHCP clients and received by the DHCP server:</p> <ul style="list-style-type: none"> • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST |
| Messages sent | <p>Number of the following message types sent from the DHCP server to DHCP clients:</p> <ul style="list-style-type: none"> • BOOTREPLY • DHCPACK • DHCPOFFER • DHCPNAK |

Sample Output

show system services dhcp statistics

```
user@host> show system services dhcp statistics
```

```
DHCP lease times:
  Default lease time      1 hour
  Minimum lease time      2 hours
  Maximum lease time      infinite
```

```
Packets dropped:
  Total                    0
  Bad hardware address     0
  Bad opcode               0
  Invalid server address   0
  No available addresses   0
  No interface match       0
  No routing instance match 0
  No valid local address   0
  Packet too short         0
  Read error               0
  Send error               0
```

```
Messages received:
  BOOTREQUEST              0
  DHCPDECLINE              0
  DHCPDISCOVER             0
  DHCPINFORM               0
  DHCPRELEASE              0
  DHCPREQUEST              0
```

```
Messages sent:
  BOOTREPLY                0
  DHCPACK                  0
  DHCPOFFER                0
  DHCPNAK                  0
```


show system services service-deployment

| | |
|---------------------------------|---|
| Syntax | show system services service-deployment |
| Release Information | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| Description | Display information about a Session and Resource Control (SRC) client. |
| Options | This command has no options. |
| Required Privilege Level | <p>system</p> <p>view</p> |
| List of Sample Output | show system services service-deployment on page 516 |
| Output Fields | Table 20 on page 516 lists the output fields for the show system services service-deployment command. Output fields are listed in the approximate order in which they appear. |

Table 20: show system services service-deployment Output Fields

| Field Name | Field Description |
|------------------------|---|
| PDT Keepalive settings | Configured PDT keepalive interval, in seconds. |
| Keepalives sent | Number of keepalives sent. |
| Notifications sent | Number of notifications sent. |
| Last update from peer | Time at which the last update from a peer was received. |

Sample Output

show system services service-deployment

```

user@host> show system services service-deployment
Connected to 192.4.4.4 port 10288 since 2004-05-03 11:04:34 PDT Keepalive settings:
Interval 15 seconds Keepalives sent: 750 Notifications sent: 0 Last update from
peer: 00:00:06 ago

```

show system users

| | |
|---------------------------------------|--|
| List of Syntax | Syntax on page 517 Syntax (TX Matrix Router) on page 517 Syntax (TX Matrix Plus Router) on page 517 Syntax (MX Series Router) on page 517 |
| Syntax | show system users <no-resolve> |
| Syntax (TX Matrix Router) | show system users <all-chassis all-lcc lccnumber scc> <no-resolve> |
| Syntax (TX Matrix Plus Router) | show system users <detail> <all-chassis all-lcc lcc number sfc number> <no-resolve> |
| Syntax (MX Series Router) | show system users <all-members> <local> <member member-id> <no-resolve> |
| Release Information | <p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>sfc option introduced for the TX Matrix Plus router in JUNOS OS Release 9.6.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| Description | List information about the users who are currently logged in to the router or switch. |



NOTE: The **show system users** command lists the information about administrative users that are logged in to a router or switch using the CLI, J-Web, or an SSH client. The output does not list information about web users or automated users that are logged in from a remote client application using Junos XML APIs, such as NETCONF.

- Options** **none**—List information about the users who are currently logged in to the router or switch.
- all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show users currently logged in to all the routers in the chassis.
- all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to all connected T1600 or T4000 LCCs.

all-members—(MX Series routers only) (Optional) Display users currently logged in to all members of the Virtual Chassis configuration.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to a specific router that is connected to the TX Matrix Plus router. Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display users currently logged in to the local Virtual Chassis member.

member *member-id*—(MX Series routers only) (Optional) Display users currently logged in to the specified member of the Virtual Chassis configuration. Replace *member-id* with a value of 0 or 1.

no-resolve—(Optional) Do not attempt to resolve IP addresses to hostnames.

scc—(TX Matrix routers only) (Optional) Show users currently logged in to the TX Matrix router (or switch-card chassis).

sfc *number*—(TX Matrix Plus routers only) (Optional) Show users currently logged in to the TX Matrix Plus router. Replace *number* with 0.

Additional Information By default, when you issue the **show system users** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level view

Related Documentation

- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output [show system users on page 519](#)
[show system users lcc no-resolve \(TX Matrix, TX Matrix Plus Router\) on page 519](#)
[show system users \(TX Matrix Plus Router\) on page 519](#)

[show system users \(QFX Series\) on page 520](#)

[show system users no-resolve \(QFX Series\) on page 520](#)

Output Fields [Table 21 on page 519](#) describes the output fields for the **show system users** command. Output fields are listed in the approximate order in which they appear.

Table 21: show system users Output Fields

| Field Name | Field Description |
|----------------------|--|
| <i>time and up</i> | Current time, in the local time zone, and how long the router or switch has been operational. |
| <i>users</i> | Number of users logged in to the router or switch. |
| <i>load averages</i> | Load averages for the last 1 minute, 5 minutes, and 15 minutes. |
| <i>USER</i> | Username. |
| <i>TTY</i> | Terminal through which the user is logged in. |
| <i>FROM</i> | System from which the user has logged in. A hyphen indicates that the user is logged in through the console. |
| <i>LOGIN@</i> | Time when the user logged in. |
| <i>IDLE</i> | How long the user has been idle. |
| <i>WHAT</i> | Processes that the user is running. |

Sample Output

show system users

```
user@host> show system users
 7:30PM up 4 days, 2:26, 2 users, load averages: 0.07, 0.02, 0.01
USER   TTY FROM                LOGIN@  IDLE WHAT
root   d0  -                    Fri05PM 4days -csh (csh)
blue   p0  leve15.company.net 7:30PM  - cli
```

show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router)

```
user@host> show system users lcc 2 no-resolve
```

```
lcc2-re0:
-----
10:34AM PDT up 1 day, 7:11, 5 users, load averages: 0.03, 0.01, 0.00
USER   TTY FROM                LOGIN@  IDLE WHAT
root   d0  -                    3:21AM  7:12 /bin/csh
user1  p0  scc-re0              10:15AM  - telnet hostA
user1  p1  scc-re0              10:16AM  - telnet hostA
user1  p2  scc-re0              10:19AM  - telnet hostA
user1  p3  scc-re0              10:24AM  - telnet hostA
```

show system users (TX Matrix Plus Router)

```
user@host> show system users
```

sfc0-re0:

```

-----
1:41AM up 26 mins, 3 users, load averages: 0.08, 0.04, 0.03
USER   TTY   FROM                               LOGIN@  IDLE WHAT
user2  p0    10.209.208.123                   1:18AM  21 cli
user2  p1    172.17.29.207                   1:37AM   2 cli
user2  p2    172.17.28.19                    1:40AM   - cli

```

lcc0-re0:

```

-----
1:41AM up 26 mins, 0 users, load averages: 0.00, 0.00, 0.03

```

lcc1-re0:

```

-----
1:41AM up 26 mins, 0 users, load averages: 0.00, 0.02, 0.03

```

lcc2-re0:

```

-----
1:41AM up 26 mins, 0 users, load averages: 0.16, 0.06, 0.02

```

lcc3-re0:

```

-----
1:41AM up 26 mins, 0 users, load averages: 0.12, 0.04, 0.04

```

user3@aj> show system users

sfc0-re0:

```

-----
1:42AM up 28 mins, 4 users, load averages: 0.02, 0.03, 0.02
USER   TTY   FROM                               LOGIN@  IDLE WHAT
user   p0    device1.example.com             1:18AM  22 cli
user   p1    device2.example.com             1:37AM   - cli
user   p2    device3.example.com             1:40AM   - cli
user   p3    device4.example.com             1:42AM   - -csh (csh)

```

lcc0-re0:

```

-----
1:42AM up 28 mins, 0 users, load averages: 0.02, 0.01, 0.03

```

lcc1-re0:

```

-----
1:42AM up 28 mins, 0 users, load averages: 0.07, 0.04, 0.03

```

lcc2-re0:

```

-----
1:42AM up 27 mins, 0 users, load averages: 0.07, 0.06, 0.02

```

lcc3-re0:

```

-----
1:42AM up 28 mins, 0 users, load averages: 0.05, 0.04, 0.04

```

show system users (QFX Series)

user@switch> show system users

```

USER   TTY   FROM                               LOGIN@  IDLE WHAT
tlewis p0    172.22.18.117                   2:54AM  39 -cli (cli)
tlewis p1    172.22.18.117                   3:01AM   - -cli (cli)
tcheng p2    172.22.17.197                   3:08AM  11 -cli (cli)

```

show system users no-resolve (QFX Series)

user@switch> show system users no-resolve

| USER | TTY | FROM | LOGIN@ | IDLE | WHAT |
|--------|-----|---------------|--------|------|------------|
| tlewis | p0 | 172.22.18.117 | 2:54AM | 39 | -cli (cli) |
| tlewis | p1 | 172.22.18.117 | 3:01AM | - | -cli (cli) |
| tcheng | p2 | 172.22.17.197 | 3:08AM | 11 | -cli (cli) |

ssh

List of Syntax [Syntax on page 522](#)
 [Syntax \(EX Series Switch and the QFX Series\) on page 522](#)

Syntax `ssh host`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<logical-system logical-system-name>`
 `<routing-instance routing-instance-name>`
 `<source address>`
 `<v1 | v2>`

Syntax (EX Series Switch and the QFX Series) `ssh host`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<routing-instance routing-instance-name>`
 `<source address>`
 `<v1 | v2>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the **ssh** command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

```
ssh address 'cli-command1 ; cli-command2 '
```

Options **host**—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface interface-name—(Optional) Interface name for the SSH session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system logical-system-name—(Optional) Name of a particular logical system for the SSH attempt.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the SSH attempt.

source address—(Optional) Source address of the SSH connection.

v1 | v2—(Optional) Use SSH version 1 or 2, respectively, when connecting to a remote host.

Additional Information To configure an SSH (version 1) key for your user account, include the **authentication ssh-rsa** statement at the **[edit system login user *user-name*]** hierarchy level. To configure an SSH (version 2) key for your user account, include the **authentication dsa-rsa** statement at the **[edit system login user *user-name*]** hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the **retry-options** statement at the **[edit system login]** hierarchy level. For details, see the .

Required Privilege Level network

Related Documentation • *Configuring SSH Host Keys for Secure Copying of Data*

List of Sample Output [ssh on page 523](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

ssh

```
user@switch> ssh cree
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?cree' added to the list of known hosts.
boojun@cree's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```

telnet

List of Syntax [Syntax on page 524](#)
 [Syntax \(EX Series Switches\) on page 524](#)

Syntax `telnet host`
 `<8bit>`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<logical-system logical-system-name>`
 `<no-resolve>`
 `<port port-number>`
 `<routing-instance routing-instance-name>`
 `<source source-address>`

Syntax (EX Series Switches) `telnet host`
 `<8bit>`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<no-resolve>`
 `<port port-number>`
 `<routing-instance routing-instance-name>`
 `<source source-address>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type **quit** to exit from telnet.

Options **host**—Name or address of the remote system.

8bit—(Optional) Use an 8-bit data path.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Open an IPv4 or IPv6 session, respectively.

interface *interface-name*—(Optional) Interface name for the telnet session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system *logical-system-name*—(Optional) Name of a particular logical system for the telnet attempt.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

port *port-number*—(Optional) Port number or service name on the remote system.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the telnet attempt.

source *source-address*—(Optional) Source address of the telnet connection.

Additional Information You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the **retry-options** statement at the **[edit system login]** hierarchy level. For details, see the *Junos OS Administration Library for Routing Devices*.

Required Privilege Level network

List of Sample Output [telnet on page 525](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

telnet

```
user@host> telnet 192.154.1.254
Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
ttypa
login:
```

test access profile

| | |
|---------------------------------|--|
| Syntax | <code>test access profile <i>profile-name</i> user <i>username</i> password <i>password</i> <detail></code> |
| Release Information | Command introduced in Junos OS Release 9.1. |
| Description | Specify a profile to use to get information from a RADIUS server, which includes all the information from the test access radius-server command. |
| Options | <p>detail—(Optional) Show the RADIUS attributes returned by the server.</p> <p>profile-name—Access profile name configured.</p> <p>password—Password for the username.</p> <p>username—User name to be authenticated to the RADIUS server.</p> |
| Required Privilege Level | view |
| List of Sample Output | <p>test access profile on page 527</p> <p>test access profile detail on page 527</p> |
| Output Fields | Table 22 on page 526 lists the output fields for the test access profile command. Output fields are listed in the approximate order in which they appear. |

Table 22: test access profile Output Fields

| Field Name | Field Description |
|-----------------|--|
| Profile Name | Name of the configured access profile. |
| Client Username | The user name authenticated by the RADIUS server. |
| Client Password | The user password authenticated by the RADIUS server. |
| Num Servers | Number of RADIUS servers in the configured access profile. |
| Server List | List of RADIUS servers in the configure access profile. |
| IP Address | The IP address of the RADIUS server authenticated. |
| UDP Port | The RADIUS server port utilized during the authentication test. |
| Source Address | The source IP address of the client making the RADIUS request. If no address is shown, it defaults to the address of the outgoing interface. |
| Timeout | The RADIUS server timeout period. |
| Retry Count | The number of authentication attempts allowed by the RADIUS server. |

Table 22: test access profile Output Fields (*continued*)

| Field Name | Field Description |
|---------------------------|--|
| Secret | The shared secret used for authentication with the RADIUS server. |
| Status | The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication. |
| Attempts | The number of authentication attempts on the RADIUS server. |
| Attribute List | The list of returned RADIUS attributes, sorted by the attribute name, and including parameter length and value. See your RADIUS server documentation for attribute descriptions. |
| (Attribute) Name | The name of the attribute. |
| (Attribute) Length | The attribute length in bytes. |
| (Attribute) Value | The attribute value. |

Sample Output

test access profile

The following example uses the **test access profile** command to access and display basic information about the RADIUS server(s) shown in the resulting output:

```

user@host> test access profile alpha user TEST password TEST
user@host> test access profile alpha user TEST password TEST
Test Radius Profile Access
  Profile Name      : alpha
  Client Username   : TEST
  Client Password   : TEST
  Num Servers       : 5
  Server List
    IP Address      UDP    Source      Retry
    Attempts        Port   Address      Timeout Count Secret      Status
1.1.1.1            1812  10.10.10.10  2        1    TEST      Timeout
2
1.2.3.4            1812  Default      1        2    TEST      Timeout
3
192.168.10.10      1812  Default      3        3    TEST      Accepted
1

```

test access profile detail

The following example uses the **test access profile detail** command to access and display detailed information about the RADIUS server(s) shown in the resulting output:

```

user@host> test access profile alpha user TEST password TEST detail
user@host> test access profile alpha user TEST password TEST detail
Test Radius Profile Access Detailed
  Profile Name      : alpha
  Client Username   : TEST

```

```

Client Password      : TEST
Num Servers          : 5
Radius Server List

```

```

IP Address           : 1.2.3.4
UDP Port              : 1812
Source Address        : 192.168.10.10
Timeout               : 2
Retry Count           : 1
Secret                : TEST
Status                : Timeout
Attempts              : 2

```

```

IP Address           : 1.2.3.5
UDP Port              : 1812
Source Address        : Default
Timeout               : 1
Retry Count           : 2
Secret                : TEST
Status                : Timeout
Attempts              : 3

```

```

IP Address           : 192.168.10.10
UDP Port              : 1812
Source Address        : Default
Timeout               : 3
Retry Count           : 3
Secret                : TEST
Status                : Accepted
Attempts              : 1

```

Attribute List

| Name | Length | Value |
|-----------------------|--------|-------------------|
| Class | 52 | SBR2CL1%ζδ0%ζ |
| Acct-Interim-Interval | 4 | 5 |
| Callback-Id | 12 | 123-456-789 |
| Callback-Number | 13 | 555-555-1212 |
| Class | 15 | Class information |
| Filter-Id | 4 | 999 |
| Filter-Id | 6 | 12345 |
| Framed-Compression | 4 | 0 |
| Framed-IP-Address | 4 | 1:2:3:4 |
| Framed-IP-Netmask | 4 | 255:255:255:255 |
| Framed-IPv6-Route | 15 | 1:2:3:4:5:6:7:8 |
| Framed-MTU | 4 | 1024 |
| Framed-Pool | 9 | pool sbr |
| Framed-Protocol | 4 | 1 |
| Framed-Route | 8 | iproute |
| Framed-Routing | 4 | 0 |
| Vendor-Specific | 11 | 583 |
| Idle-Timeout | 4 | 3 |
| Vendor-Specific | 10 | a4c |
| Vendor-Specific | 14 | a4c |
| Login-IP-Host | 4 | 10:1:1:1 |
| Login-LAT-Group | 10 | lat group |
| Login-LAT-Node | 9 | lat node |
| Login-LAT-Port | 9 | lat port |
| Login-LAT-Service | 12 | lat service |
| Login-Service | 4 | 0 |
| Login-TCP-Port | 4 | 1812 |

| | | |
|-------------------------------|----|------------------|
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 38 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 9 | 137 |
| Vendor-Specific | 16 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 9 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 10 | 137 |
| Vendor-Specific | 10 | 137 |
| Password-Retry | 4 | 3 |
| Port-Limit | 4 | 100 |
| Prompt | 4 | |
| Reply-Message | 18 | Radius Server SB |
| Service-Type | 4 | 2 |
| Session-Timeout | 4 | 10 |
| Termination-Action | 4 | 1 |
| Tunnel-Assignment-ID | 4 | |
| Tunnel-Client-Auth-ID | 6 | |
| Tunnel-Client-Endpoint | 4 | |
| Tunnel-Password | 19 | |
| Tunnel-Type | 4 | 12 |
| MS BAP Usage | 4 | 0 |
| MS-CHAP MPPE-Keys | 32 | -1234567890 |
| MS-CHAP2 Success | 3 | 123456789 |
| MS Filter | 10 | ms-filter |
| MS Link Drop Time Limit | 4 | 5 |
| MS Link Utilization Threshold | 4 | 6 |
| MS MPPE Encryption Policy | 4 | 1 |
| MS MPPE Encryption Types | 3 | -556677889 |
| MS Primary DNS Server | 4 | 1:1:1:1 |
| MS Primary NBNS Server | 4 | 2:2:2:2 |
| MS Secondary DNS Server | 4 | 3:3:3:3 |
| MS Secondary NBNS Server | 4 | 4:4:4:4 |

test access radius-server

| | |
|---------------------------------|--|
| Syntax | <code>test access radius-server address user username password password secret secret</code> <code><authentication-port port></code> <code><retry number></code> <code><source-address address></code> <code><timeout number></code> |
| Release Information | Command introduced in Junos OS Release 9.1. |
| Description | Verify RADIUS server authentication parameters. |
| Options | <p>address—RADIUS server under test IP address.</p> <p>password—Password for the user.</p> <p>secret—Secret shared with the RADIUS server.</p> <p>user—User name to be authenticated to the RADIUS server.</p> <p>authentication-port—(Optional) RADIUS server authentication port number (1through 65535).</p> <p>retry—(Optional) Retry attempts (1through 10).</p> <p>source-address—(Optional) Use an alternate address as the source address.</p> <p>timeout—(Optional) Request timeout period (1through 90 seconds).</p> |
| Required Privilege Level | view |
| List of Sample Output | test access radius-server user password secret on page 531 |
| Output Fields | Table 23 on page 530 lists the output fields for the test access radius-server command. Output fields are listed in the approximate order in which they appear. |

Table 23: test access radius-server Output Fields

| Field Name | Field Description |
|-------------------|--|
| Server | The IP address of the RADIUS server authenticated. |
| UDP port | The RADIUS server port utilized during the authentication test. |
| Source IP Address | "Default" is shown if the IP address is the same as that of the RADIUS server. Alternatively, an IP address specified for authentication is shown. |
| Server timeout | The RADIUS server timeout period. |
| Sever retry count | The number of authentication attempts allowed by the RADIUS server. |

Table 23: test access radius-server Output Fields (*continued*)

| Field Name | Field Description |
|------------------------|---|
| Secret | The shared secret used for authentication with the RADIUS server. |
| Client Username | The user name authenticated by the RADIUS server. |
| Client Password | The user password authenticated by the RADIUS server. |
| Status | The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication. |

Sample Output

test access radius-server user password secret

The following example command tests RADIUS authentication with a specific server (172.28.30.95), user (JOHNDOE), secret (No1Knows), and password (JohnPass); and displays the resulting output:

```
user@host> test access radius-server 172.28.30.95 user JOHNDOE password JohnPass secret
No1Knows
Test Radius Server Access
  Server           : 172.28.30.95
  UDP port         : 1812
  Source IP Address : Default
  Server timeout   : 3
  Sever retry count : 3
  Secret           : No1Knows
  Client Username   : JOHNDOE
  Client Password   : JohnPass
  Status           : Accepted, retransmits: 0
```


CHAPTER 15

Index

- [Index on page 535](#)

Index

Symbols

| | |
|--|--------|
| ! | |
| regular expression operator..... | 66, 68 |
| #, comments in configuration statements..... | xx |
| \$ | |
| regular expression operator..... | 66, 69 |
| () | |
| regular expression operator..... | 66, 69 |
| (), in syntax descriptions..... | xx |
| * | |
| regular expression operator..... | 69 |
| + | |
| regular expression operator..... | 69 |
| . | |
| regular expression operator..... | 69 |
| < >, in syntax descriptions..... | xx |
| [], in configuration statements..... | xx |
| \ | |
| regular expression operator..... | 66, 69 |
| ^ | |
| regular expression operator..... | 66, 69 |
| { }, in configuration statements..... | xx |
| (pipe), in syntax descriptions..... | xx |

A

| | |
|-------------------------------------|----------|
| access privilege levels | |
| configuration example..... | 64 |
| configuration mode hierarchies..... | 72 |
| operational mode commands..... | 67 |
| configuring..... | 63 |
| configuration mode hierarchies..... | 67 |
| operational mode commands..... | 64 |
| login classes..... | 26 |
| user accounts..... | 24 |
| access-end statement..... | 367 |
| access-start statement..... | 367 |
| accounting statement..... | 366 |
| authentication | |
| usage guidelines..... | 276, 295 |
| accounting-port statement | |
| RADIUS servers..... | 368 |

| | |
|--|-----------------------|
| allow-commands statement..... | 368 |
| usage guidelines..... | 29 |
| allow-configuration statement..... | 369 |
| usage guidelines..... | 29 |
| allow-configuration-regexps statement..... | 370 |
| allowed-days statement..... | 370 |
| allowing commands to login classes..... | 29 |
| announcement statement | |
| usage guidelines..... | 43 |
| announcements | |
| system login..... | 43 |
| authentication | |
| order..... | 32, 262, 281, 297 |
| protocol..... | 36 |
| RADIUS..... | 30, 52, 267, 280, 297 |
| root password..... | 245, 257 |
| shared user accounts..... | 52, 280, 297 |
| TACACS+ | 30, 52, 280, 285, 297 |
| users..... | 30 |
| authentication key update mechanism..... | 353 |
| authentication statement | |
| DHCP local server..... | 371 |
| login..... | 372 |
| usage guidelines..... | 24, 53 |
| authentication-order statement..... | 373 |
| usage guidelines..... | 32, 262, 281, 297 |
| authorization See permissions | |

B

| | |
|--|-----|
| backoff-factor statement..... | 374 |
| backoff-threshold statement..... | 374 |
| BGP | |
| security configuration example..... | 352 |
| boot-file statement..... | 375 |
| usage guidelines..... | 317 |
| boot-server statement | |
| DHCP..... | 376 |
| braces, in configuration statements..... | xx |
| brackets | |
| angle, in syntax descriptions..... | xx |
| square, in configuration statements..... | xx |

C

| | |
|------------------------------------|-----|
| cables | |
| console port, connecting..... | 250 |
| Ethernet rollover, connecting..... | 250 |
| change-type statement..... | 377 |
| usage guidelines..... | 257 |
| ciphers..... | 378 |

| | | | |
|---|------------|--|----------|
| circuit-type statement..... | 379 | DHCP | |
| class statement | | address bindings | |
| assigning to user..... | 380 | clearing..... | 502 |
| login..... | 381 | displaying..... | 505 |
| usage guidelines..... | 23, 24, 53 | address conflicts | |
| clear system services dhcp binding command..... | 502 | clearing..... | 503 |
| clear system services dhcp conflict | | displaying..... | 508 |
| command..... | 503 | address pools, displaying..... | 511 |
| clear system services dhcp statistics | | address statistics | |
| command..... | 504 | clearing..... | 504 |
| CLI | | displaying..... | 513 |
| permissions, displaying..... | 500 | global settings, displaying..... | 509 |
| client-alive-count-max statement..... | 382 | tracing operations..... | 318 |
| client-alive-interval statement..... | 382 | DHCP local server statements | |
| client-identifier statement..... | 383 | delimiter..... | 386 |
| usage guidelines..... | 309 | dhcp-local-server..... | 396 |
| commands | | dhcpv6..... | 393 |
| allowing or denying to login classes..... | 29 | domain-name..... | 402 |
| comments, in configuration statements..... | xx | group..... | 408 |
| conflicting IP addresses, displaying..... | 508 | interface..... | 414 |
| connection-limit statement..... | 384 | ip-address-first..... | 415 |
| usage guidelines..... | 337 | logical-system-name..... | 420 |
| connections | | mac-address..... | 423 |
| SSH, opening..... | 522 | option-60..... | 438 |
| console port | | option-82..... | 439, 440 |
| adapter..... | 250 | password..... | 444 |
| conventions | | pool-match-order..... | 448 |
| text and syntax..... | xix | routing-instance-name..... | 461 |
| Crypto Officer..... | 47 | traceoptions..... | 482 |
| user configuration..... | 47 | username-include..... | 492 |
| curly braces, in configuration statements..... | xx | DHCP relay agent statements | |
| customer support..... | xxi | traceoptions..... | 482 |
| contacting JTAC..... | xxi | user-prefix..... | 493 |
| D | | DHCP statement | |
| default-lease-time statement..... | 385 | usage guidelines..... | 317 |
| usage guidelines..... | 310 | dhcp statement..... | 391 |
| delimiter statement | | dhcp-local-server statement..... | 396 |
| DHCP local server..... | 386 | usage guidelines..... | 322 |
| deny-commands statement..... | 387 | dhcpv6 statement..... | 393 |
| usage guidelines..... | 29 | documentation | |
| deny-configuration statement..... | 388 | comments on..... | xxi |
| usage guidelines..... | 29 | domain-name statement | |
| denying commands to login classes..... | 29 | DHCP..... | 401 |
| destination statement..... | 390 | DHCP local server..... | 402 |
| usage guidelines..... | 276, 295 | Dynamic Host Configuration Protocol See DHCP | |
| | | dynamic service activation..... | 350 |
| | | dynamic-profile-options statement..... | 403 |

E

| | |
|---|----------|
| encrypted passwords..... | 245, 257 |
| encrypted-password option..... | 245, 257 |
| enhanced-accounting statement..... | 403 |
| Ethernet rollover cable, connecting the router to a management device..... | 250 |
| events statement usage guidelines..... | 277, 295 |
| exclude-cmd-attribute statement..... | 477 |

F

| | |
|-----------------------------------|--------|
| finger statement..... | 404 |
| usage guidelines..... | 339 |
| FIPS..... | 48 |
| user configuration..... | 48 |
| <i>See also</i> Junos-FIPS | |
| flags login class..... | 26, 78 |
| user permissions..... | 26 |
| flow-tap-dtcp statement..... | 405 |
| usage guidelines..... | 346 |
| font conventions..... | xix |
| format statement..... | 406 |
| FTP service, configuring..... | 339 |
| ftp statement..... | 407 |
| usage guidelines..... | 339 |
| full names, in user accounts..... | 24 |
| full-name statement..... | 407 |
| usage guidelines..... | 24, 53 |

G

| | |
|---|-----|
| group statement DHCP local server..... | 408 |
| usage guidelines..... | 322 |

H

| | |
|------------------------------|-----|
| HMAC-MD5 authentication..... | 36 |
| hostkey-algorithm..... | 412 |
| http statement..... | 410 |
| https statement..... | 411 |

I

| | |
|---|-----|
| idle timeout values login classes..... | 40 |
| idle-timeout statement..... | 413 |
| usage guidelines..... | 40 |
| interface statement DHCP local server..... | 414 |
| usage guidelines..... | 322 |

IP addresses

| | |
|--|-----|
| conflicting, displaying..... | 508 |
| removing from DHCP server conflict list..... | 503 |
| ip-address-first statement..... | 415 |
| usage guidelines..... | 322 |
| IS-IS security configuration example..... | 352 |

J

| | |
|---|-------------|
| Juniper-Allow-Commands attribute (RADIUS)..... | 274 |
| Juniper-Allow-Configuration attribute (RADIUS)..... | 274 |
| Juniper-Authentication-Type..... | 276 |
| Juniper-Configuration-Change attribute (RADIUS)..... | 275 |
| Juniper-Deny-Commands attribute (RADIUS)..... | 274 |
| Juniper-Deny-Configuration attribute (RADIUS)..... | 275 |
| Juniper-Interactive-Command attribute (RADIUS)..... | 275 |
| Juniper-Local-User-Name attribute (RADIUS)..... | 274 |
| Juniper-Session-Port | 276 |
| Juniper-User-Permissions attribute (RADIUS)..... | 275 |
| Junos OS SRC client, displaying..... | 516 |
| Junos XML protocol SSL service..... | 349 |
| Junos-FIPS password requirements..... | 25, 37, 246 |
| remote services..... | 337 |
| user accounts..... | 47 |

K

| | |
|-------------------|-----|
| key-exchange..... | 416 |
|-------------------|-----|

L

| | |
|---|------------------|
| laptop <i>See</i> management device | |
| load-key-file command usage guidelines..... | 24, 53, 246 |
| load-key-file statement..... | 417 |
| usage guidelines..... | 24, 53, 245, 257 |
| local password authentication..... | 52 |
| local user template accounts..... | 50 |
| local-certificate statement..... | 418 |
| lockout-period statement..... | 419 |
| logging in as root..... | 341 |
| logical-system-name statement DHCP local server..... | 420 |

| | |
|-------------------------------------|----------------|
| login announcements, system..... | 43 |
| login classes | |
| access privilege levels..... | 26 |
| commands, allowing or denying..... | 29 |
| defining..... | 23 |
| idle timeout values..... | 40 |
| security configuration example..... | 40 |
| login messages, system..... | 42 |
| login statement..... | 421 |
| usage guidelines..... | 23, 24, 53, 57 |
| login-alarms statement..... | 422 |
| usage guidelines..... | 46 |
| login-script statement..... | 422 |

M

| | |
|-------------------------------------|----------|
| mac-address statement | |
| DHCP local server..... | 423 |
| macs..... | 424 |
| management device | |
| recovering root password from..... | 250 |
| manuals | |
| comments on..... | xxi |
| max-sessions-per-connection..... | 426, 436 |
| maximum-lease-time statement..... | 425 |
| usage guidelines..... | 310, 317 |
| maximum-length statement..... | 426 |
| usage guidelines..... | 257 |
| maximum-time statement..... | 427 |
| MD5 authentication..... | 36 |
| message statement | |
| usage guidelines..... | 42 |
| messages | |
| system login..... | 42 |
| minimum-changes statement..... | 428 |
| usage guidelines..... | 257 |
| minimum-length statement..... | 429 |
| usage guidelines..... | 257 |
| minimum-lower-cases statement..... | 430 |
| minimum-numeric statement..... | 431 |
| minimum-punctuations statement..... | 432 |
| minimum-time statement..... | 433 |
| minimum-upper-cases statement..... | 434 |
| ms-chapv2 | |
| changing password ms-chapv2..... | 254 |

N

| | |
|----------------------------|-----|
| NETCONF-over-SSH | |
| TCP port..... | 348 |
| next-server statement..... | 435 |

| | |
|---------------------------------------|-----|
| no-cmd-attribute-value statement..... | 477 |
|---------------------------------------|-----|

O

| | |
|---------------------------------------|--------|
| operators, regular expression..... | 66, 68 |
| option-60 statement | |
| DHCP local server..... | 438 |
| option-82 statement | |
| DHCP local server authentication..... | 439 |
| DHCP local server pool matching..... | 440 |
| usage guidelines..... | 322 |
| outbound SSH | |
| router-initiated SSH..... | 441 |
| outbound SSH service | |
| configuring..... | 342 |
| outbound-ssh statement..... | 441 |
| usage guidelines..... | 342 |

P

| | |
|--|----------|
| parentheses, in syntax descriptions..... | xx |
| password | |
| ssh public string..... | 55 |
| password statement | |
| DHCP local server..... | 444 |
| login..... | 445 |
| passwords | |
| RADIUS..... | 267 |
| root..... | 245, 257 |
| root password, recovering..... | 250 |
| shared user..... | 52 |
| passwords statement | |
| usage guidelines..... | 257 |
| PC See management device | |
| permission flags | |
| login class..... | 26 |
| user..... | 26 |
| permissions statement..... | 446 |
| usage guidelines..... | 26 |
| permissions, CLI, displaying..... | 500 |
| plain-text passwords..... | 246 |
| for user accounts..... | 25 |
| root password..... | 245, 257 |
| plain-text-password option..... | 245, 257 |
| pool statement | |
| DHCP..... | 447 |
| usage guidelines..... | 317 |
| pool-match-order statement..... | 448 |
| usage guidelines..... | 322 |

-
- port statement
 - HTTP/HTTPS.....449
 - NETCONF-over-SSH.....450
 - RADIUS.....451
 - SRC.....451
 - TACACS+.....452
 - usage guidelines.....285
 - usage guidelines.....267, 350
 - ports
 - RADIUS servers.....267
 - protocol-version statement.....452
 - usage guidelines.....341, 342
 - protocols
 - authentication.....36
 - R**
 - RADIUS
 - about.....31
 - RADIUS accounting.....276
 - RADIUS authentication.....30, 267
 - security configuration example.....272
 - TACACS+52
 - RADIUS authorization See RADIUS authentication
 - radius statement
 - accounting.....453
 - RADIUS templates
 - security configuration example.....273
 - radius-options statement454
 - radius-server statement.....455
 - usage guidelines.....267
 - rate-limit statement.....456
 - usage guidelines.....337
 - regular expression operators.....66, 68
 - remote
 - access, configuring.....337
 - template account.....52
 - remote authentication servers
 - about.....31
 - remote system access, operational mode
 - commands.....524
 - retry statement.....457
 - usage guidelines.....267
 - retry-options statement.....458
 - usage guidelines.....57
 - RJ-45-to-DB-9 serial port adapter.....250
 - rollover cable, connecting the console port.....250
 - root password.....245, 257
 - root password recovery.....250
 - root-authentication statement
 - usage guidelines.....245, 257
 - root-login statement.....459
 - usage guidelines.....341
 - router statement.....460
 - routers
 - login classes.....23
 - ports
 - RADIUS servers.....267
 - root login, controlling.....341
 - system services, configuring.....337
 - user accounts.....24, 53
 - routing-instance statement
 - usage guidelines.....267
 - routing-instance-name statement
 - DHCP local server.....461
 - S**
 - secret statement
 - authentication.....462
 - usage guidelines, RADIUS.....267
 - usage guidelines, TACACS+285
 - server statement
 - RADIUS accounting.....463
 - TACPLUS+.....463
 - server-identifier statement.....465
 - usage guidelines.....317
 - servers statement.....464
 - usage guidelines.....350
 - service-deployment statement.....466
 - usage guidelines.....350
 - service-name statement.....477
 - services statement
 - remote router access.....467
 - usage guidelines.....337
 - Session and Resource Control.....516
 - session statement.....469
 - show cli authorization command.....500
 - show system services dhcp binding
 - command.....505
 - show system services dhcp conflict
 - command.....508
 - show system services dhcp global command.....509
 - show system services dhcp pool command.....511
 - show system services dhcp statistics
 - command.....513
 - show system services service-deployment
 - command.....516
 - show system users command.....517

| | | | |
|--|-------------------|---|-----|
| simple authentication..... | 36 | SSH..... | 340 |
| single-connection statement..... | 470 | telnet..... | 338 |
| usage guidelines..... | 285 | system statement..... | 476 |
| source-address statement | | usage guidelines..... | 358 |
| NTP..... | 471 | | |
| RADIUS | | T | |
| usage guidelines..... | 267 | TACACS+ | |
| RADIUS and TACACS+..... | 471 | about..... | 31 |
| SDX | | TACACS+ accounting..... | 295 |
| usage guidelines..... | 350 | usage guidelines, TX Matrix router..... | 297 |
| SRC..... | 472 | TACACS+ authentication | |
| system logging..... | 471 | configuring..... | 285 |
| usage guidelines | | overview..... | 30 |
| usage guidelines, RADIUS..... | 267 | tacplus statement..... | 476 |
| source-port statement..... | 472 | tacplus-options statement..... | 477 |
| SRC client information, displaying..... | 516 | usage guidelines..... | 291 |
| SRC software..... | 350, 466 | tacplus-server statement..... | 478 |
| ssh command..... | 522 | usage guidelines..... | 285 |
| SSH key files..... | 245, 257 | technical support | |
| SSH service | | contacting JTAC..... | xxi |
| configuring..... | 340 | telnet | |
| limiting login attempts..... | 57 | service, configuring..... | 338 |
| root login..... | 341 | service, limiting login attempts..... | 57 |
| SSH protocol version..... | 341, 342 | telnet command..... | 524 |
| ssh statement..... | 473 | telnet statement..... | 478 |
| usage guidelines..... | 340 | usage guidelines..... | 338 |
| SSH, opening a connection..... | 522 | template accounts..... | 52 |
| SSL..... | 349 | test access profile command..... | 526 |
| static-binding statement..... | 475 | test access radius-server command..... | 530 |
| usage guidelines..... | 317 | timeout statement | |
| statistics | | authentication | |
| DHCP server, displaying..... | 513 | usage guidelines, RADIUS..... | 267 |
| support, technical See technical support | | usage guidelines, TACACS+ | 285 |
| syntax conventions..... | xix | RADIUS and TACACS+..... | 479 |
| system..... | 59 | timestamp-and-timezone statement..... | 477 |
| retry options..... | 59 | traceoptions statement | |
| system authentication | | address-assignment pool..... | 480 |
| authentication order..... | 32, 262, 281, 297 | DHCP..... | 485 |
| RADIUS | | usage guidelines..... | 318 |
| configuring..... | 267 | DHCP local server..... | 482 |
| remote template accounts..... | 52 | DHCP relay agent..... | 482 |
| TACACS+..... | 285 | SBC configuration process | |
| system login..... | 42, 43 | border signaling gateways..... | 488 |
| system services | | usage guidelines..... | 322 |
| DHCP..... | 317 | tracing operations | |
| DHCP local server..... | 322 | DHCP..... | 318 |
| finger | 339 | tries-before-disconnect statement..... | 490 |
| FTP | 339 | troubleshooting | |
| outbound SSH..... | 342 | root password recovery..... | 250 |

U

| | |
|---------------------------------------|------------|
| uid statement..... | 490 |
| usage guidelines..... | 24, 53 |
| UIDs..... | 24 |
| user access | |
| login classes..... | 23 |
| user accounts..... | 24, 47, 53 |
| user accounts | |
| configuring..... | 24, 53 |
| in Junos-FIPS..... | 47 |
| security configuration example..... | 52 |
| shared user accounts..... | 52 |
| user authentication | |
| methods for..... | 30 |
| user identifiers See UIDs | |
| user permission flags..... | 26 |
| user statement | |
| access..... | 491 |
| usage guidelines..... | 24, 53 |
| user-prefix statement | |
| DHCP local server..... | 493 |
| username-include statement | |
| DHCP local server..... | 492 |
| users | |
| CLI permissions, displaying..... | 500 |
| logged in, displaying..... | 517 |
| using outbound-ssh | |
| connect routers behind firewalls..... | 441 |

V

| | |
|---------------------------|-----|
| versioning statement..... | 494 |
|---------------------------|-----|

W

| | |
|-------------------------------|-----|
| web-management statement..... | 495 |
| wins-server statement..... | 496 |
| usage guidelines..... | 317 |

X

| | |
|-------------------------------|-----|
| xnm-clear-text statement..... | 497 |
| usage guidelines..... | 348 |
| xnm-ssl statement..... | 497 |
| usage guidelines..... | 349 |

