JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

User Access and Authentication Administration Guide for Junos OS

Published
2025-12-08

JUNOS

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos® OS User Access and Authentication Administration Guide for Junos OS
Copyright © 2025 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide

Junos OS enables you to configure user access and authentication features at the `[edit system]` hierarchy level of the CLI. Essential user access features include login classes, user accounts, access privilege levels, and user authentication methods. Use the topics on this page to configure essential user access features for your system.

1

CHAPTER

Login Classes and Login Settings

IN THIS CHAPTER

Login Classes Overview

IN THIS SECTION

Junos OS login classes define the access privileges, permissions for using CLI commands and statements, and session idle time for the users assigned to that class. You (the system administrator) can apply a login class to an individual user account, thereby assigning certain privileges and permissions to the user.

Login Classes Overview

IN THIS SECTION

All users who can log in to a device running Junos OS must be in a login class. Each login class defines the following:

- Access privileges that users have when they log in to the network device
- Commands that users can and cannot execute
- Configuration statements that users can and cannot view or modify
- Amount of time a login session can be idle before the system disconnects the user

You can define any number of login classes. However, you only assign one login class to an individual user account.

Junos OS includes predefined login classes, which are listed in Table 1 on page 3. You cannot modify the predefined login classes.

Table 1: 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

SFTP and SCP server functionality is disabled when using the `operator` or `read-only` predefined login classes.

Starting in Junos OS Evolved Release 23.4R2, the `superuser` login class cannot write to the **/var/log/** directory. Only the `root` user can write into **/var/log/**.

Permission Bits

Each top-level CLI command and each *configuration statement* has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. Each login class defines one or more permission bits that determine the access privileges.

Two forms for the permissions control whether a user can view or modify the individual parts of the configuration:

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

Table 2 on page 4 outlines the permission flags and associated access privileges.

Table 2: Login Class Permission Flags

Permission Flag	Description
access	Can view the access configuration in operational mode or configuration mode.
access-control	Can view and configure access information at the [edit access] hierarchy level.
admin	Can view user account information in operational mode or configuration mode.
admin-control	Can view user account information and configure it at the [edit system] hierarchy level.
all	Can access all operational mode commands and configuration mode commands. Can modify the configuration in all the configuration hierarchy levels.
clear	Can clear (delete) information that the device learns from the network and stores in various network databases (using the clear commands).
configure	Can enter configuration mode (using the configure command) and commit configurations (using the commit command).
control	Can perform all control-level operations—all operations configured with the -control permission flags.
field	Can view field debug commands. Reserved for debugging support.
firewall	Can view the *firewall filter* configuration in operational mode or 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.

Table 2: Login Class Permission Flags *(Continued)*

Permission Flag	Description
`flow-tap`	Can view the flow-tap configuration in operational mode or configuration mode.
`flow-tap-control`	Can view and configure flow-tap information at the `[edit services flow-tap]` hierarchy level.
`flow-tap-operation`	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 Junos OS as an administrative user. **NOTE**: The `flow-tap-operation` option is not included in the `all-control` permissions flag.
`idp-profiler-operation`	Can view profiler data.
`interface`	Can view the interface configuration in operational mode and configuration mode.
`interface-control`	Can view chassis, *class of service* (CoS), groups, forwarding options, and interfaces configuration information. Can modify the configuration at the following hierarchy levels: • `[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 device and becoming the superuser in the shell (using the `su root` command) and halting and rebooting the device (using the `request system` commands).
`network`	Can access the network by using the `ping`, `ssh`, `telnet`, and `traceroute` commands.

Table 2: Login Class Permission Flags *(Continued)*

Permission Flag	Description
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.
rollback	Can use the rollback command to return to a previously committed configuration.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration mode and operational mode.
routing-control	Can view and configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy information at the [edit policy-options] hierarchy level.
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view and modify passwords and other authentication keys in the configuration.
security	Can view security configuration information in operational mode and configuration mode.
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 operational mode or configuration mode.

Table 2: Login Class Permission Flags *(Continued)*

Permission Flag	Description
snmp-control	Can view and modify SNMP configuration information at the [edit snmp] hierarchy level.
storage	Can view Fiber Channel storage configuration information at the [edit fc-fabrics] hierarchy level.
storage-control	Can modify Fiber Channel storage configuration information at the [edit fc-fabrics] hierarchy level.
system	Can view system-level information in operational mode or configuration mode.
system-control	Can view and modify system-level configuration information at the [edit system] hierarchy level.
trace	Can view trace file settings.
trace-control	Can modify trace file settings and configure trace file properties.
unified-edge	Can view unified edge configuration at the [edit unified-edge] hierarchy.
unified-edge-control	Can modify unified edge related configuration at the [edit unified-edge] hierarchy.
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.

Deny or Allow Individual Commands and Statement Hierarchies

By default, all top-level CLI commands and statements have associated access privilege levels. Users can execute only those commands and view and configure only those statements for which they have access privileges. For each login class, you can explicitly deny or allow users the use of operational mode commands and configuration mode commands and configuration statement hierarchies that are otherwise allowed or denied by a permission bit.

Example: Create Login Classes with Specific Privileges

You define login classes to assign certain permissions or restrictions to groups of users, ensuring that sensitive commands are only accessible to the appropriate users. By default, Juniper Networks devices have four types of login classes with preset permissions: operator, read-only, superuser or super-user, and unauthorized.

You can create custom login classes to define different combinations of permissions that are not found in the default login classes. The following example shows three custom login classes, each with specific privileges and inactivity timers. Inactivity timers help protect network security by disconnecting a user from the network if the user is inactive for too long. Disconnecting the user prevents potential security risks that result when a user leaves an unattended account logged in to a switch or router. The permissions and inactivity timers shown here are only examples; you should customize the values to your organization.

The three login classes and their privileges are as follows. All three login classes use the same inactivity timer of 5 minutes.

- `observation`—Can only view statistics and the configuration
- `operation`—Can view and modify the configuration
- `engineering`—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;
        }
    }
}
```

Understanding Exact Match Access Privileges for Login Classes

IN THIS SECTION

Exact match access privileges let you explicitly allow or deny exact configuration strings to define access control rules for login classes. Starting in Junos OS and Junos OS Evolved Release 23.4R1, you can use the `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration statements to control exact match access privileges.

Benefits

- Restrict deletion of upper level configuration hierarchies while permitting deletion of specific sub-hierarchies. This supports more targeted command authorization.
- Ensure `set` commands remain permitted on a hierarchy even if deletion is denied. This separation of authorization for `set` and `delete` enables more flexible access controls.
- Allow or deny precise configuration command strings, in addition to regular expressions. This supports configuring highly specific access rules when needed.
- Leverage advanced authorization rules from external TACACS+ servers, in addition to local rules. This facilitates centralized policy management.

You can configure exact match access privileges with the `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration statements at the `[edit system login class name]` hierarchy level. Use hierarchy strings starting with one of the following operators:

- `set`
- `delete`
- `active`
- `deactivate`

Wildcard characters are also supported. For example, the `deny-configuration-exact-match delete interfaces*` statement uses the * wildcard character to specify all interfaces.

If `delete` or `deactivate` is denied for a given configuration hierarchy, then `set` or `activate` commands can still be allowed by using `allow-configuration-exact-match`. If you configure both `allow-configuration-exact-match` and `deny-configuration-exact-match` with the same operator and configuration, then configuration access will be denied.

The new exact match rules can be configured locally or on external TACACS+ servers.

Login Settings

IN THIS SECTION

Junos OS enables you to define various settings for users when they log in to a device. You (the system administrator) can configure:

- Messages or announcements to display before or after login
- Whether to display system alarms upon login
- Login tips
- Time-based user access
- Timeout values for idle sessions
- Limits on the number of login attempts
- Whether to lock a user account after a number of failed authentication attempts

Display a System Login Announcement or Message

Sometimes you want to make announcements only to authorized users after they log in to a device. For example, you might want to announce an upcoming maintenance event. At other times, it might be appropriate to display a message, such as a security warning, to any user that connects to the device.

By default, Junos OS does not display any login message or announcement. You can configure the device to display a login message or announcement by including the `message` statement or the `announcement` statement at the `[edit system login]` hierarchy level. Whereas the device displays a login *message* after a user connects to the device but before the user logs in, it displays an *announcement* only after the user successfully logs in to the device.

You can format the message or announcement text using the following special characters. If the text contains spaces, enclose it in quotation marks:

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

To configure an announcement that only authorized users can see and a message that any user can see:

1. Include the `announcement` statement and the `message` statement at the `[edit system login]` hierarchy level.

```
[edit system login]
user@host# set announcement text
user@host# set message 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\tAcme Router Lab\n\n\tUNAUTHORIZED USE OF THIS ROUTER\n\tIS STRICTLY
PROHIBITED!\n\n\tPlease contact \'jsmith@example.com\' to gain\n\taccess to this equipment if
you need authorization.\n\n"
    }
}
```

2. Commit the configuration.

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

3. Connect to the device to verify the presence of the new message.

The preceding configuration example displays the following login message after the user connects to the device. The example displays the announcement after the user logs in:

```
server% ssh host

        Acme Router Lab

        UNAUTHORIZED USE OF THIS ROUTER
        IS STRICTLY PROHIBITED!

        Please contact 'jsmith@example.com' to gain
        access to this equipment if you need authorization.
```

```
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.
```

Display System Alarms Upon Login

You can configure Juniper Networks devices to execute the `show system alarms` command whenever a user in a given login class logs in to the device.

To display alarms whenever a user in a specific login class logs in to the device:

1. Configure the `login-alarms` statement for the appropriate login class.

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

For example, to display alarms whenever a user in the `admin` login class logs in to the device:

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

2. Commit the configuration.

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

When a user in the given login class logs in to the device, the device displays the current alarms.

```
$ ssh user@host.example.com
Password:
--- JUNOS 21.1R2.6-EVO Linux (none) 4.8.28-WR2.2.1_standard-g3999f55 #1 SMP PREEMPT Fri Jun 4
00:19:58 PDT 2021 x86_64 x86_64 x86_64 GNU/Linux

2 alarms currently active
Alarm time               Class  Description
2021-07-22 15:00:14 PDT  Minor  port-1/0/0: Optics does not support configured speed
2021-07-22 15:00:14 PDT  Minor  port-1/0/1: Optics does not support configured speed
```

Configure Login Tips

You can configure the Junos OS CLI to display a tip whenever a user in the given login class logs in to the device. The device does not display tips by default.

To enable tips:

1. Configure the `login-tip` statement at the `[edit system login class class-name]` hierarchy level.

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

2. Commit the configuration.

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

When you configure the `login-tip` statement, the device displays a tip to any user in the specified class who logs in to the device.

```
$ ssh user@host.example.com
Password:

JUNOS tip:
In configuration mode, the [edit] banner displays the current location
in the configuration hierarchy.

user@host>
```

Configure Time-Based User Access

You can configure supported Juniper Networks devices to enforce time-based user access for users in a given class. Time-based user access restricts the time and duration of user logins for all users belonging to the class. You can restrict user access based on the time of day or day of the week.

To restrict user access to certain days or times, include the following statements at the `[edit system login class` *`class-name`*`]` hierarchy level:

- `allowed-days`—Configure user access on specific days of the week.
- `access-start` and `access-end`—Configure user access between the specified start time and end time (*hh:mm*).

To configure time-based user access:

1. Enable access on specific days of the week.

   ```
   [edit system login class class-name]
   user@host# set allowed-days [ day1 day2 ]
   ```

   For example, to configure user access for the `operator-round-the-clock-access` login class from Monday through Friday without any restriction on access time:

   ```
   [edit system login class operator-round-the-clock-access]
   user@host# set allowed-days [ monday tuesday wednesday thursday friday ]
   ```

2. Enable access at specific times of the day.

```
[edit system login class class-name]
user@host# set access-start hh:mm
user#host# set access-end hh:mm
```

For example, to configure user access for the `operator-day-shift-all-days-of-the-week` login class from 8:30 AM through 4:30 PM on all days of the week:

```
[edit system login class operator-day-shift-all-days-of-the-week]
user@host# set access-start 08:30
user#host# set access-end 16:30
```

You can also configure access to include both days and times. The following example configures user access for the `operator-day-shift` login class on Monday, Wednesday, and Friday from 8:30 AM through 4:30 PM:

```
[edit system login class operator-day-shift]
user@host# set allowed-days [ monday wednesday friday ]
user@host# set access-start 08:30
user@host# set access-end 16:30
```

Alternatively, you can specify the login start time and end time for the `operator-day-shift` login class by using the following format:

```
[edit system login class operator-day-shift]
user@host# set allowed-days [ monday wednesday friday ]
user@host# set access-start 08:30am
user@host# set access-end 04:30pm
```

NOTE: The access start and end times might span across 12:00 AM on a given day. In that case, the user still has access until the next day, even if you do not explicitly configure that day in the `allowed-days` statement.

Configure the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI displays the operational mode or configuration mode prompt but there is no input from the keyboard. By default, a login session remains established until a user logs out of the device, 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. Automatically closing idle login sessions helps to prevent malicious users from gaining access to the device and performing operations with an authorized user account.

You can configure an idle timeout only for user-defined classes. You cannot configure this option for the system predefined classes: `operator`, `read-only`, `super-user` or `superuser`, and `unauthorized`.

To define the timeout value for idle login sessions:

1. Specify the number of minutes that a session can be idle before the system automatically closes the session.

   ```
   [edit system login class class-name]
   user@host# set idle-timeout minutes
   ```

   For example, to automatically disconnect idle sessions of users in the `admin` class after fifteen minutes:

   ```
   [edit system login class admin]
   user@host# set idle-timeout 15
   ```

2. Commit the configuration.

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

If you configure a timeout value, the CLI displays messages similar to the following when timing out an idle user. The CLI starts displaying these messages 5 minutes before disconnecting 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 elapses, except in the following cases:

- The user is running the `ssh` or `telnet` command.
- The user is logged into the local UNIX shell.
- The user is monitoring interfaces using the `monitor interface` or the `monitor traffic` command.

Login Retry Options

You can configure login retry options on Juniper Network devices to protect the devices from malicious users. You can configure the following options:

- The number of times a user can enter invalid login credentials before the system closes the connection.
- Whether and for how long to lock a user account after the user reaches the threshold of failed authentication attempts.

Limiting the login attempts and locking the user account help to protect the device from malicious users attempting to access the system by guessing the password of an authorized user account. You can unlock the user account or define a time period for the user account to remain locked.

You configure login retry options at the `[edit system login retry-options]` hierarchy level. The `tries-before-disconnect` statement defines the threshold of failed login attempts before the device disconnects the user. The device allows three unsuccessful login attempts by default.

The `lockout-period` statement instructs the device to lock the user account for the specified amount of time if the user reaches the threshold of unsuccessful login attempts. The lock prevents the user from performing activities that require authentication, until the lockout time period has elapsed or a system administrator manually clears the lock. Any existing locks are ignored when the user attempts to log in from the local console.

To configure login retry options:

1. Configure the number of times a user can attempt to enter a password.

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

For example, to enable a user to enter a password four times before the device closes the connection:

```
[edit system login retry-options]
user@host# set tries-before-disconnect 4
```

2. Configure the number of minutes that the user account remains locked after a user reaches the threshold of failed login attempts.

```
[edit system login retry-options]
user@host# set lockout-period minutes
```

For example, to lock a user account for 120 minutes after a user reaches the threshold of failed login attempts:

```
[edit system login retry-options]
user@host# set lockout-period 120
```

3. Commit the configuration.

```
[edit system login retry-options]
user@host# commit
```

NOTE: To clear the console during an administrator-initiated logout, include newline (\n) characters when you configure the `message` statement at the `[edit system login]` hierarchy level. To completely clear the console, the administrator can enter 50 or more \n characters in the message string. For example:

```
user@host# set system login message "\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n
\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n Welcome to Junos!!!"
```

Limit 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 to a device through SSH or Telnet. The device terminates the connection if a user fails to log in after the number of

specified attempts. 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;
    lockout-period minutes;
    maximum-time seconds
    minimum-time seconds;
}
```

You can configure the following options:

- `tries-before-disconnect`—Maximum number of times a user can enter a password when logging in to the device through SSH or Telnet. 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 3.
- `backoff-threshold`—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. The range is from 1 through 3, and the default is 2. Use the `backoff-factor` option to specify the length of the delay.
- `backoff-factor`—Length of time, in seconds, that the user must wait after a failed login attempt above the `backoff-threshold`. The delay increases by the specified value for each subsequent attempt after the `backoff-threshold` value. The range is from 5 through 10, and the default is 5 seconds.
- `lockout-period`—Length of time, in minutes, that a user account is locked after reaching the `tries-before-disconnect` threshold. The range is 1 through 43,200 minutes.
- `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 closes. 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 20 seconds.

Limiting the number of SSH and Telnet login attempts per user is one of the most effective methods of stopping brute force attacks from compromising your network security. Brute force attackers execute a

large number of login attempts in a short period of time to illegitimately gain access to a private network. By configuring the `retry-options` statements, you can create an increasing delay after each failed login attempt, eventually disconnecting any user who passes your set threshold of login attempts.

To limit the login attempts when a user logs in through SSH or Telnet:

1. Configure the limit on the number of login attempts.

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

2. Configure the number of login attempts before the user experiences a delay.

```
[edit system login retry-options]
user@host# set backoff-threshold number
```

3. Configure the number of seconds the user must wait for the login prompt after reaching the `backoff-threshold` value.

```
[edit system login retry-options]
user@host# set backoff-factor seconds
```

4. Configure the number of seconds that the connection remains open while a user attempts to log in.

```
[edit system login retry-options]
user@host# set minimum-time seconds
```

For the following configuration, 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. The connection closes after a total of 40 seconds.

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

```
        }
    }
}
```

Example: Configure Login Retry Options

IN THIS SECTION

This example shows how to configure login retry options to protect a device from malicious users.

Requirements

Before you begin, you should understand "Limit the Number of User Login Attempts for SSH and Telnet Sessions" on page 19.

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 the password of an authorized user account. You can lock a user account after a certain number of failed authentication attempts. This precaution helps protect devices from malicious users.

You can configure the number of failed login attempts before the device locks the user account, and you can configure the amount of time that the account remains locked. You can also configure the amount of time the user must wait between failed login attempts.

NOTE: This example includes the following settings:

- backoff-factor—Length of delay in seconds that the user must wait after each failed login attempt above the backoff-threshold. The delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold statement.
- backoff-threshold—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 reaches the threshold of failed login attempts, the user experiences the delay set in the backoff-factor statement. After the delay, the user can make another login attempt.
- lockout-period—Number of minutes that the user account is locked after the user reaches the tries-before-disconnect threshold. The user must wait the configured number of minutes before they can log in to the device again.
- tries-before-disconnect—Maximum number of times the user can enter a password to attempt to log in to the device through SSH or Telnet.

NOTE: If you are locked out of the device, you can log in to the device's console port, which ignores any user locks. This provides a way for administrators to remove the user lock on their own user account.

This example sets the tries-before-disconnect option to 3. As a result, the user has three attempts to log in to the device. If the number of failed login attempts is equal to the value specified in the backoff-threshold statement, the user must wait 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 device disconnects the user after the third failed attempt.

If the user does not successfully log in after three attempts, the user account is locked. The user cannot log in until 120 minutes have elapsed, unless a system administrator manually clears the lock during that time.

A system administrator can manually unlock an account by issuing the clear system login lockout user *<username>* command. The show system login lockout command displays which user accounts are locked and when the lockout period begins and ends for each user.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure system retry-options:

1. Configure the backoff factor.

```
[edit]
user@host# set system login retry-options backoff-factor 5
```

2. Configure the backoff threshold.

```
[edit]
user@host# set system login retry-options backoff-threshold 1
```

3. Configure the number of minutes that the user account remains locked after a user reaches the threshold of failed login attempts.

```
[edit]
user@host# set system login retry-options lockout-period 120
```

4. Configure the number of times a user can attempt to enter a password.

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

Results

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

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

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

Verification

IN THIS SECTION

Display the Locked User Logins

Purpose

Verify that the login lockout configuration is enabled.

Action

Attempt three unsuccessful logins for a particular username. The device will be locked for that username. Then log in to the device with a different username. From operational mode, issue the `show system login lockout` command to view the locked accounts.

```
user@host> show system login lockout
User                 Lockout start           Lockout end
jsmith     2021-08-17 16:27:28 PDT 2021-08-17 18:27:28 PDT
```

Meaning

After 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 device is locked for that user by logging in to the device with a different username and entering the `show system login lockout` command.

2
CHAPTER

User Accounts

IN THIS CHAPTER

User Accounts

IN THIS SECTION

Junos OS enables you (the system administrator) to create accounts for router, switch, and security users. All users belong to one of the system login classes.

You create user accounts so that users can access a router, switch, or security device. All users must have a predefined user account before they can log in to the device. You create user accounts and then define the login name and identifying information for each user account.

User Accounts Overview

User accounts provide one way for users to access a device. For each account, you define the user's login name, password, and any additional user information. After you have created an account, the software creates a home directory for the user.

An account for the user `root` is always present in the configuration. You can configure the password for `root` using the `root-authentication` statement.

While it is common to use remote authentication servers to centrally store information about users, it is also good practice to configure at least one non-root user on each device. This way, you can still access the device if its connection to the remote authentication server is disrupted. This non-root user usually has a generic name such as `admin`.

For each user account, you can define the following:

- Username (Required): Name that identifies the user. It must be unique. Avoid using spaces, colons, or commas in the username. The username can include up to 64 characters.
- User's full name: (Optional) If the full name contains spaces, enclose it in quotation marks. Avoid the use of colons or commas.

- User identifier (UID): (Optional) Numeric identifier that is associated with the user account name. The UID is assigned automatically when you commit the configuration, so you do not need to set it manually. However, if you choose to configure the UID manually, use a unique value in the range from 100 through 64,000.
- User's access privilege: (Required) One of the login classes you defined in the `class` statement at the `[edit system login]` hierarchy or one of the default login classes.
- Authentication method or methods and passwords for device access (Required): You can use a SSH key, an encrypted password, or a plain-text password that Junos OS encrypts 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 receive a prompt 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
  ```

  To create valid plain-text passwords, make sure that they:

  - Contain between 6 and 128 characters.
  - Include most character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters) but do not include control characters.
  - Contain at least one change of case or character class.

  Junos-FIPS and Common Criteria have the following special password requirements. They must:

  - Be between 10 and 20 characters long.
  - 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 device, you must adhere to the special password requirements, or the passwords are not configured.

For SSH authentication, you can copy the contents of an SSH key file into the configuration. You can also configure SSH key information directly. Use the `load-key-file` statement to load an SSH key file that was generated previously, (for example, by using `ssh-keygen`). The `load-key-file` argument is the path to the file location and name. The `load-key-file` statement loads RSA (SSH version 1 and SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you configure the `load-key-file` statement.

Avoid using the following Transport Layer Security (TLS) version and cipher suite (RSA host key) combinations, which will fail:

With RSA host keys:

- TLS_1.0@DHE-RSA-AES128-SHA
- TLS_1.0@DHE-RSA-AES256-SHA

For each user account and for root logins, you can configure more than one public RSA 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 the user accounts.

To view the SSH key 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_rsa.pub
.file.19692               |          0 KB |   0.3 kB/s | ETA: 00:00:00 | 100%
[edit system login user boojum]
user@host# show
authentication {
    ssh-rsa "$ABC123"; # SECRET-DATA
}
```

Junos-FIPS Crypto Officer and User Accounts Overview

IN THIS SECTION

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, only a Crypto Officer can perform FIPS-related tasks.

Crypto Officer User Configuration

Junos-FIPS offers you 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, you should reserve the `super-user` class 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 certain permissions normally reserved for a Crypto Officer; for example, you can grant a FIPS User permission to zeroize the system and individual AS-II FIPS PICs.

Example: Configure New User Accounts

IN THIS SECTION

This example shows how to configure new user accounts.

Requirements

You do not need any special configurations before using this feature.

Overview

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

- The password must be at least six characters long.
- You can include most character classes in the password (alphabetic, numeric, and special characters), but not control characters.

- The password must contain at least one change of case or character class.

In this example, you create a login class named operator-and-boot and allow it to reboot the device. You can define any number of login classes. Then, allow the operator-and-boot login class to use commands defined in the following bits:

- clear
- network
- reset
- trace
- view permission

Next, create user accounts to enable access to the device. Set the username as randomuser and the login class as superuser. Finally, define the encrypted password for the user.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

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

Step-by-Step Procedure

To configure new users:

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

```
[edit system login]
user@host# set class operator-and-boot allow-commands “request system reboot”
```

2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace view]
```

3. Set the username, login class, and encrypted password for the user.

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

GUI Quick Configuration

Step-by-Step Procedure

To configure new users:

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

   Avoid spaces, colons, and commas in the username.
6. In the User ID box, type a unique ID for the user.
7. In the Full Name box, type the user’s full name.

   If the full name contains spaces, enclose it in quotation marks. Avoid colons and commas.
8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.
9. From the Login Class list, select the user’s access privilege:

- operator
- read-only
- unauthorized

This list also includes any user-defined login classes.

10. Click OK in the Add User dialog box and Edit User Management dialog box.
11. Click OK to check your configuration and save it as a candidate configuration.
12. After you configure the device, click Commit Options>Commit.

Results

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

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

The following example shows how to create accounts for four users. It also shows how to create an account for the template user remote. All users use one of the default system login classes.

```
[edit]
system {
    login {
        user philip {
            full-name “Philip of Macedonia”;
            uid 1001;
            class super-user;
```

```
            authentication {
                encrypted-password “$ABC123”;
            }
        }
        user alexander {
            full-name “Alexander the Great”;
            uid 1002;
            class operator;
            authentication {
                encrypted-password “$ABC123”;
            }
        }
        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;
        }
    }
}
```

After you configure the device, enter `commit` in configuration mode.

Verification

IN THIS SECTION

- Verify the New Users Configuration | 36

Confirm that the configuration is working properly.

Verify the New Users Configuration

Purpose

Verify that the new users are configured.

Action

Log in to the device with the new user account or accounts and password to confirm that you have access.

Configure User Accounts in a Configuration Group

To make it easier to configure the same user accounts on multiple devices, configure the accounts inside of a configuration group. 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 username
```

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

   If the 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, the software assigns one for you. The format of the UID is a number between 100 and 64,000.

```
[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 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
     New Password: type password here
     Retype new password: retype password here
     ```

     As you enter the password in plain text, the software encrypts it. You do not need to configure the software to encrypt the password. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

   - To enter a password that is 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"
     ```

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

```
[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:

```
[edit groups global system login user user-name]
user@host# set authentication (ssh-ecdsa | ssh-ed25519 | 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.

Administrative Roles

IN THIS SECTION

Junos OS enables you to define a system user to act as a specific kind of administrator for the system. You can assign an administrative role to a user by configuring a login class to have the administrative

role attributes. You can assign one of the role attributes such as audit-officer crypto-officer, security-officer, ids-officer to an administrative user.

How to Design Administrative Roles

A system user can be a member of a class that allows the user to act as a specific kind of administrator for the system. Requiring a specific role to view or modify an item restricts the extent of information a user can obtain from the system. It also limits how much of the system is open to modification or observation by a user. You (the system administrator) should use the following guidelines when you are designing administrative roles:

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

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

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

Each role can perform the following specific management functions:

- **Cryptographic Administrator**
  - Configures the cryptographic self-test.
  - Modifies the cryptographic security data parameters.
- **Audit Administrator**
  - Configures and deletes the audit review search-and-sort feature.

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

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

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

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

Example: How to Configure Administrative Roles

IN THIS SECTION

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

Requirements

No action beyond device initialization is required before configuring this feature.

Overview

This example illustrates how to configure four admin user roles:

- `audit-officer` of the class `audit-admin`
- `crypto-officer` of the class `crypto-admin`
- `security-officer` of the class `security-admin`

- ids-officer of the class ids-admin

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

In this example, you create the four administrative user roles shown in the preceding list (audit admin, crypto admin, security admin, and ids admin). For each role, you assign relevant permission flags for the role. You then allow or deny access to configuration statements and commands by name for each administrative role. These specific restrictions take precedence over the permission flags configured in the class. For example, only the crypto-admin can run the request system set-encryption-key command, which requires having the security permission flag to access it. Only the security-admin can include the system time-zone statement in the configuration, which requires having the system-control permission flag.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set system login class audit-admin permissions security
set system login class audit-admin permissions trace
set system login class audit-admin permissions maintenance
set system login class audit-admin allow-commands "^clear (log|security log)"
set system login class audit-admin deny-commands "^clear (security alarms|system login lockout)|
^file (copy|delete|rename)|^request (security|system set-encryption-key)|^rollback|^set date|
^show security (alarms|dynamic-policies|match-policies|policies)|^start shell";
set system login class audit-admin security-role audit-administrator
set system login class crypto-admin permissions admin-control
set system login class crypto-admin permissions configure
```

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

```
set system login user crypto-officer authentication plain-text-password
set system login user security-officer authentication plain-text-password
set system login user ids-officer authentication plain-text-password
```

Step-by-Step Procedure

To configure administrative roles:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the ids-admin login class restrictions.

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

9. Assign users to the roles.

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

10. Configure passwords for the users.

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

Results

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

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

```
            deny-commands "^clear log|^(clear|show) security alarms (alarm-id|all|newer-than|
older-than|process|severity)|^(clear|show) security alarms alarm-type
            (authentication | cryptographic-self-test | decryption-failures | encryption-failures
             | ike-phase1-failures | ike-phase2-failures|key-generation-self-test |
             non-cryptographic-self-test |policy | replay-attacks) | ^file (copy|delete|rename)
            |^request (security|system set-encryption-key) | ^rollback |
            ^set date | ^show security (dynamic-policies|match-policies|policies) |^start shell";
            allow-configuration-regexps [ "security alarms potential-violation idp" "security
log exclude .* event-id IDP_.*" ];
            deny-configuration-regexps "security alarms potential-violation (authentication|
cryptographic-self-test|decryption-
            failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
            key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
            security-role ids-administrator;
        }
        user audit-officer {
            class audit-admin;
            authentication {
                 encrypted-password "$1$ABC123"; ## SECRET-DATA
            }
        }
        user crypto-officer {
            class crypto-admin;
            authentication {
                 encrypted-password "$1$ABC123."; ## SECRET-DATA
            }
        }
        user security-officer {
            class security-admin;
            authentication {
                 encrypted-password "$1$ABC123."; ##SECRET-DATA
            }
        }
        user ids-officer {
            class ids-admin;
            authentication {
                encrypted-password "$1$ABC123/"; ## SECRET-DATA
            }
        }
    }
}
```

After you configure the device, enter **commit** in configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify the Login Permissions

Purpose

Verify the login permissions for the current user.

Action

In operational mode, enter the `show cli authorization` command to verify the user's login permissions.

```
user@host> show cli authorization
Current user: 'example' class 'super-user'
Permissions:
    admin       -- Can view user accounts
    admin-control-- Can modify user accounts
    clear       -- Can clear learned network info
    configure   -- Can enter configuration mode
    control     -- Can modify any config
    edit        -- Can edit full files
    field       -- Can use field debug commands
    floppy      -- Can read and write the floppy
    interface   -- Can view interface configuration
    interface-control-- Can modify interface configuration
    network     -- Can access the network
    reset       -- Can reset/restart interfaces and daemons
    routing     -- Can view routing configuration
    routing-control-- Can modify routing configuration
    shell       -- Can start a local shell
    snmp        -- Can view SNMP configuration
    snmp-control-- Can modify SNMP configuration
```

```
    system      -- Can view system configuration
    system-control-- Can modify system configuration
    trace       -- Can view trace file settings
    trace-control-- Can modify trace file settings
    view        -- Can view current values and statistics
    maintenance -- Can become the super-user
    firewall    -- Can view firewall configuration
    firewall-control-- Can modify firewall configuration
    secret      -- Can view secret statements
    secret-control-- Can modify secret statements
    rollback    -- Can rollback to previous configurations
    security    -- Can view security configuration
    security-control-- Can modify security configuration
    access      -- Can view access configuration
    access-control-- Can modify access configuration
    view-configuration-- Can view all configuration (not including secrets)
    flow-tap    -- Can view flow-tap configuration
    flow-tap-control-- Can modify flow-tap configuration
    idp-profiler-operation-- Can Profiler data
    pgcp-session-mirroring-- Can view pgcp session mirroring configuration
    pgcp-session-mirroring-control-- Can modify pgcp session mirroring configura
tion
    storage     -- Can view fibre channel storage protocol configuration
    storage-control-- Can modify fibre channel storage protocol configuration
    all-control -- Can modify any configuration
Individual command authorization:
    Allow regular expression: none
    Deny regular expression: none
    Allow configuration regular expression: none
    Deny configuration regular expression: none
```

This output summarizes the login permissions.

How to Configure a Local Administrator Account

Superuser privileges give a user permission to use any command on the router and are generally reserved for a select few users such as system administrators. You (the system administrator) need to protect the local administrator account with a password to prevent unauthorized users from gaining access to superuser commands. These superuser commands can be used to alter the system configuration. Users with RADIUS authentication should also configure a local password. If the RADIUS

server does not respond, the login process reverts to local password authentication on the local administrator account.

The following example shows how to configure a password-protected local administration account called `admin` with superuser privileges:

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

User Access Privileges

IN THIS SECTION

You (the system administrator) grant users access or permissions to commands and configuration hierarchy levels and statements. Users can execute only those commands and view and configure only those statements for which they have access privileges. You can also use extended regular expressions to specify which operational mode commands, configuration statements, and hierarchies are allowed or denied for users. This practice prevents unauthorized users from executing sensitive commands or configuring statements that could cause damage to the network.

Access Privilege Levels Overview

IN THIS SECTION

Each top-level CLI command and *configuration statement* has an associated access privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. One or more permission flags define the access privileges for each login class.

For each login class, you can also explicitly allow or deny the use of operational mode and configuration mode commands and statement hierarchies that would otherwise be allowed or denied by a privilege level specified in the `permissions` statement.

Login Class Permission Flags

You use permission flags to grant a user access to operational mode commands and configuration hierarchy levels and statements. You configure permission flags for the user's login class at the `[edit system login class]` hierarchy level. When you specify a certain permission flag, the user gains access to the commands and to the configuration hierarchy levels and statements that correspond to that flag. To grant access to all commands and configuration statements, use the `all` permissions flag.

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.

The `permissions` statement specifies one or more of the permission flags listed in Table 3 on page 54. Permission flags are not cumulative. 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 a user's access to the individual parts of the configuration:

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

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

Table 3 on page 54 lists the login class permission flags that you can configure by including the `permissions` statement at the `[edit system login class` *`class-name`*`]` hierarchy level.

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

Table 3: Login Class Permission Flags

Permission Flag	Description
`access`	Can view the access configuration in operational mode or configuration mode.
`access-control`	Can view and configure access information at the `[edit access]` hierarchy level.
`admin`	Can view user account information in operational mode or configuration mode.
`admin-control`	Can view user account information and configure it at the `[edit system]` hierarchy level.
`all`	Can access all operational mode commands and configuration mode commands. Can modify the configuration in all the configuration hierarchy levels.
`clear`	Can clear (delete) information that the device learns from the network and stores in various network databases (using the `clear` commands).

Table 3: Login Class Permission Flags *(Continued)*

Permission Flag	Description
`configure`	Can enter configuration mode (using the `configure` command) and commit configurations (using the `commit` command).
`control`	Can perform all control-level operations—all operations configured with the `-control` permission flags.
`field`	Can view field debug commands. Reserved for debugging support.
`firewall`	Can view the *firewall filter* configuration in operational mode or 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 operational mode or configuration mode.
`flow-tap-control`	Can view and configure flow-tap information at the `[edit services flow-tap]` hierarchy level.
`flow-tap-operation`	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 Junos OS as an administrative user. **NOTE**: The `flow-tap-operation` option is not included in the `all-control` permissions flag.
`idp-profiler-operation`	Can view profiler data.
`interface`	Can view the interface configuration in operational mode and configuration mode.

Table 3: Login Class Permission Flags *(Continued)*

Permission Flag	Description
interface-control	Can view chassis, *class of service* (CoS), groups, forwarding options, and interfaces configuration information. Can modify the configuration at the following hierarchy levels: • [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 device and becoming the superuser in the shell (using the su root command) and halting and rebooting the device (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.
rollback	Can use the rollback command to return to a previously committed configuration.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration mode and operational mode.
routing-control	Can view and configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy information at the [edit policy-options] hierarchy level.

Table 3: Login Class Permission Flags *(Continued)*

Permission Flag	Description
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view and modify passwords and other authentication keys in the configuration.
security	Can view security configuration information in operational mode and configuration mode.
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 operational mode or configuration mode.
snmp-control	Can view and modify SNMP configuration information at the [edit snmp] hierarchy level.
storage	Can view Fiber Channel storage configuration information at the [edit fc-fabrics] hierarchy level.
storage-control	Can modify Fiber Channel storage configuration information at the [edit fc-fabrics] hierarchy level.
system	Can view system-level information in operational mode or configuration mode.
system-control	Can view and modify system-level configuration information at the [edit system] hierarchy level.
trace	Can view trace file settings.
trace-control	Can modify trace file settings and configure trace file properties.

Table 3: Login Class Permission Flags *(Continued)*

Permission Flag	Description
`unified-edge`	Can view unified edge configuration at the `[edit unified-edge]` hierarchy.
`unified-edge-control`	Can modify unified edge related configuration at the `[edit unified-edge]` hierarchy.
`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.

Allow and Deny Individual Commands and Statement Hierarchies for Login Classes

By default, all top-level CLI commands and configuration hierarchy levels have associated access privilege levels. Users can execute only those commands and view and configure only those statements for which they have access privileges. For each login class, you can explicitly allow and deny the use of operational mode and configuration mode commands and statement hierarchies that would otherwise be allowed or denied by a privilege level specified in the `permissions` statement.

Permission flags grant a user access to operational mode and configuration mode commands and to 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.

You can explicitly allow or deny the use of commands and statements by configuring the `allow-commands`, `deny-commands`, `allow-configuration`, and `deny-configuration` statements for a login class. In the statements, you use extended regular expressions to define which commands and statements to allow or deny for users assigned to the class.

Example: Configure User Permissions with Access Privilege Levels

IN THIS SECTION

This example configures the user permissions for a login class. You configure user permissions for a login class to prevent users from performing unauthorized network actions. Users can execute only those commands and view and modify only those statements for which they have access privileges. This constraint prevents unauthorized users from executing sensitive commands or configuring statements that could cause damage to the network.

Requirements

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

Overview

Each top-level CLI command and each configuration statement has an access privilege level associated with it. When you configure a login class, you can explicitly allow or deny the use of operational mode and configuration mode commands and configuration statements. Users can execute only those commands and view and configure only those statements for which they have access privileges.

You define the access privileges for each login class by specifying one or more permission flags in the `permissions` statement. Permission flags grant a user access to commands, statements, and hierarchies. Permission flags are not cumulative. For each login class you must list all the permission flags needed, including `view` to display information and `configure` to enter configuration mode. By specifying a specific permission flag on the user's login class, you grant the user access to the corresponding commands, statements, and hierarchies. To grant access to all commands and configuration statements, use the `all` permissions flag. The permission flags provide read-only (“plain” form) and read and write (form that ends in -control) capability for a permission type.

NOTE: The `all` login class permission bits take precedence over extended regular expressions when a user issues a `rollback` command with the `rollback` permission flag enabled.

To configure user access privilege levels for a login class, include the `permissions` statement at the `[edit system login class class-name]` hierarchy level, followed by the permission flags. Configure multiple permissions as a space-separated list enclosed in square brackets:

```
[edit system login]
user@host# set class class-name permissions permission-flag
user@host# set class class-name permissions [flag1 flag2 flag3]
```

TIP: To view the available permissions, use the CLI's context-sensitive help and type a question mark (?) after the `permissions` statement:

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

Configuration

IN THIS SECTION

This example configures the `snmp-admin` login class. Users in this login class can configure and view SNMP parameters only.

Configure User Permissions with Access Privilege Levels

Step-by-Step Procedure

To configure access privileges for the login class:

1. Configure the `snmp-admin` login class with the `configure`, `snmp`, and `snmp-control` permission flags.

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

   The configured permission flags provide both read (snmp) and read-and-write (snmp-control) capability for SNMP, and this is the only allowed access privilege for this login class. All other access privileges are denied.

2. Create the user accounts that are assigned to the `snmp-admin` login class.

```
[edit system login]
user@host# set user snmpuser class snmp-admin authentication plain-text-password
New password:
Retype new password:
```

Results

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

```
user@host# show system login
class snmp-admin {
    permissions [ configure snmp snmp-control ];
}
user snmpuser {
    class snmp-admin;
    authentication {
        encrypted-password "$ABC123"; ## SECRET-DATA
    }
}
```

After configuring the device, enter `commit` in configuration mode.

Verification

IN THIS SECTION

Log in using a username assigned to the new login class, and confirm that the configuration is working properly.

Verify SNMP Configuration

Purpose

Verify that a user in the `snmp-admin` login class can configure SNMP.

Action

In configuration mode, configure SNMP statements at the `[edit snmp]` hierarchy level.

```
[edit snmp]
user@host# set name device1
user@host# set description switch1
user@host# set location Lab1
user@host# set contact example.com
user@host# commit
```

Meaning

The user in the `snmp-admin` login class is able to configure SNMP parameters. The user can configure these parameters because the permission flags specified for this class include both snmp (read capabilities) and snmp-control (read and write capabilities) permission bits.

Verify non-SNMP Configuration

Purpose

Verify that a user in the `snmp-admin` login class cannot modify non-SNMP configuration statements.

Action

In configuration mode, attempt to configure any non-SNMP statement, such as a statement in the `interfaces` hierarchy.

```
[edit]
user@host# edit interfaces
Syntax error, expecting <statement> or <identifier>.
```

Meaning

The user in the `snmp-admin` login class is not able to configure the `[edit interfaces]` hierarchy because the permission flags specified for this class do not allow it. In this case, the CLI issues an error message.

Regular Expressions to Allow and Deny Operational Mode Commands, Configuration Statements, and Hierarchies

IN THIS SECTION

This topic contains the following sections:

Understanding the Allow and Deny Statements

Each top-level CLI command and configuration statement hierarchy has an access privilege level associated with it. Each login class can explicitly allow or deny the use of operational mode and configuration mode commands and configuration hierarchies and statements that would otherwise be allowed or denied by a privilege level. Users can execute only those commands and view and configure only those statements for which they have access privileges.

The access privileges for each login class are defined by one or more permission flags specified in the `permissions` statement at the `[edit system login class` *`class-name`*`]` hierarchy level. In addition, you can allow or deny the use of specific commands and configuration hierarchies by defining extended regular expressions. You can specify the regular expressions by configuring the following statements for a login class:

- `allow-commands` and `deny-commands`—Allow or deny access to operational mode and configuration mode commands.
- `allow-configuration` and `deny-configuration`—Allow or deny access to specific configuration hierarchies.

  NOTE: These 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 negatively affecting performance.

- `allow-commands-regexps` and `deny-commands-regexps`—Allow or deny access to particular commands using strings of regular expressions.
- `allow-configuration-regexps` and `deny-configuration-regexps`—Allow or deny access to specific configuration hierarchies using strings of regular expressions.

NOTE: If your existing configurations use the `allow/deny-commands` or `allow/deny-configuration` statements, using the same configuration options with the `allow/deny-commands-regexps` or `allow/deny-configuration-regexps` statements might not produce the same results. The search and match methods differ in the two forms of these statements.

Explicitly allowing commands and configuration statement hierarchies using the `allow/deny-*` statements adds to the permissions that the `permissions` statement already defines. Likewise, explicitly denying commands and configuration statement hierarchies using the `allow/deny-*` statements removes permissions that the `permissions` statement already defines.

For example, in the following configuration, the `configure` permission enables users in the login class to enter configuration mode. Additionally, the `allow-configuration` expression allows users to modify the configuration at the `[edit system services]` hierarchy level and commit it.

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

Similarly, in the following configuration, the login class user can perform all operations that the `all` permissions flag allows, except that the user cannot view or modify the configuration at the `[edit system services]` hierarchy level:

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

Understanding the Allow and Deny Statement Syntax

You can configure an `allow/deny-*` statement only once in each login class. When you configure a statement:

- You can configure as many regular expressions as needed.
- Regular expressions are not case-sensitive

The `allow/deny-commands` statements are mutually exclusive with the `allow/deny-commands-regexps` statements, and the `allow/deny-configuration` statements are mutually exclusive with the `allow/deny-configuration-regexps` statements. For example, you cannot configure both `allow-configuration` and `allow-configuration-regexps` in the same login class.

To define access privileges to commands, specify extended regular expressions using the `allow-commands` and `deny-commands` statements. Enclose each complete standalone expression in parentheses ( ), and use the pipe (|) symbol to separate the expressions. Do not use spaces between regular expressions that are connected with the pipe symbol. The complete expression is enclosed in double quotation marks.

```
allow-commands "(cmd1)|(cmd2)|(cmdn)"
allow-configuration "(config1)|(config2)|(confign)"
```

For example:

```
[edit system login class test]
user@host# set allow-commands "(ping .*)|(traceroute .*)|(show .*)|(configure .*)|(edit)|(exit)|
(commit)|(rollback .*)"
```

You must use anchors when specifying complex regular expressions with the `allow-commands` statement. For example:

```
[edit system login]
user@host# set class test allow-commands "(^monitor)|(^ping)|(^show)|(^exit)"
```

To define access privileges to parts of the configuration hierarchy, specify extended regular expressions in the `allow-configuration` and `deny-configuration` statements. Enclose the full paths in parentheses ( ), and use the pipe (|) symbol to separate the expressions. Do not use spaces between regular expressions that are connected with the pipe symbol. The complete expression is enclosed in double quotation marks.

```
allow-configuration "(config1)|(config2)|(confign)"
```

For example:

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

When specifying extended regular expressions using the `allow/deny-commands-regexps` or `allow/deny-configuration-regexps` statements, enclose each expression within quotation marks (" "), and separate the expressions using a space. Enclose multiple expressions in square brackets [ ]. For example:

```
[edit system login class test]
user@host# set allow-configuration-regexps ["interfaces .* description .*" "interfaces .*
unit .* description .*" “interfaces .* unit .* family inet address .*" "interfaces.* disable"]
```

Modifiers such as `set`, `log`, and `count` are not supported within the regular expression string to be matched. If you use a modifier, then nothing is matched.

Correct configuration:

```
[edit system login class test]
user@host# set deny-commands protocols
```

Incorrect configuration:

```
[edit system login class test]
user@host# set deny-commands "set protocols"
```

Understanding the Allow and Deny Statement Precedence and Matching

By default, the `allow-commands` and `allow-configuration` regular expressions take precedence over `deny-commands` and `deny-configuration` expresssions. Thus, if you configure the same command for both the `allow-commands` and `deny-commands` statements, then the allow operation takes precedence over the deny operation. Similarly, if you configure the same statement for both the `allow-configuration` and `deny-configuration` statements, then the allow operation takes precedence over the deny operation.

For instance, the following configuration allows a user in the `test` login class to install software using the `request system software add` command, even though the `deny-commands` statement includes the same command:

```
[edit system login class test]
user@host# set allow-commands "request system software add"
user@host# set deny-commands "request system software add"
```

Similarly, the following configuration allows a user in the `test` login class test to view and modify the `[edit system services]` configuration hierarchy, even though the `deny-configuration` statement includes the same hierarchy:

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

If the `allow-commands` and `deny-commands` statements have two different variants of a command, the longest match is always executed. The following configuration allows a user in the `test` login class to execute 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.

```
[edit system login class test]
user@host# set allow-commands "commit synchronize"
user@host# set deny-commands commit
```

The following configuration allows a user in the test login class to execute 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.

```
[edit system login class test]
user@host# set allow-commands commit
user@host# set deny-commands "commit synchronize"
```

In contrast to the other statements, the default behavior for the *-regexps statements is that the deny-commands-regexps and deny-configuration-regexps regular expressions take precedence over allow-commands-regexps and allow-configuration-regexps expressions. You can configure the regex-additive-logic statement at the [edit system] hierarchy level to force the allow-configuration-regexps regular expressions to take precedence over the the deny-configuration-regexps statements. Configuring the statement enables you to deny configuration hierarchies at a higher level and then only allow the user access to specific sub-hierarchies.

Understanding the Allow and Deny Statement Rules

The allow/deny-commands, allow/deny-configuration, allow/deny-commands-regexps, and allow/deny-configuration-regexps statements take precedence over the login class permissions. When you configure these statements, the following rules apply:

- Regular expressions for allow-commands and deny-commands statements can also include the commit, load, rollback, save, status, and update commands.
- The all login class permission bits take precedence over extended regular expressions when a user issues the rollback command with the rollback permission flag enabled.
- Users cannot issue the load override command when specifying an extended regular expression. Users can only issue the merge, replace, and patch configuration commands.
- You can use the * wildcard character when denoting regular expressions. However, you must use it as part of a regular expression. You cannot use [*] or [.*] as the only expression. Additionally, you cannot configure the allow-configuration statement with an expression such as (interfaces (description (|.*)), because this evaluates to allow-configuration .*.

Understanding Differences for the *-regexps Statements

This section outlines the differences between the `allow/deny-configuration` statements and the `allow/deny-configuration-regexps` statements.

The `allow/deny-configuration-regexps` statements split up the regular expression into tokens and match each piece against each part of the specified configuration's full path, whereas the `allow/deny-configuration` statements match against the full string. For `allow/deny-configuration-regexps` statements, you configure a set of strings in which each string is a regular expression, with spaces between the terms of the string. This syntax provides very fast matching but offers less flexibility. For specifying wildcard expressions, you must set up wildcards for each token of the space-delimited string you want to match, which makes it more difficult to use wildcard expressions for these statements.

For example:

- **Regular expression matching one token using allow-configuration-regexps**

  This example shows that `options` is the only matched expression against the first token of the statement.

  ```
  [edit system]
  login {
      class test {
          permissions configure;
          allow-configuration-regexps .*options;
      }
  }
  ```

  The preceding configuration matches the following statements:

  - set policy-**options** condition *condition* dynamic-db
  - set routing-**options** static route *static-route* next-hop *next-hop*
  - set event-**options** generate-event *event* time-interval *seconds*

  The preceding configuration does not match the following statements:

  - system host-name host-**options**
  - interfaces *interface-name* description **options**

- **Regular expression matching three tokens using allow-configuration-regexps**

This example shows that ssh is the only matched expression against the third token of the statement.

```
[edit system]
login {
    class test {
        permissions configure;
        allow-configuration-regexps ".* .* .*ssh";
    }
}
```

In the preceding example, the three tokens include .*, .*, and .*ssh, respectively.

The preceding configuration matches the following statements:

- system host-name hostname-**ssh**
- system services **ssh**
- system services outbound-**ssh**

The preceding configuration does not match the following statement:

- interfaces *interface-name* description **ssh**

It is easier to use the deny-configuration statement to restrict configuration access than to use the deny-configuration-regexps statement. Table 4 on page 70 illustrates the use of both the deny-configuration and deny-configuration-regexps statements in different configurations to achieve the same result of restricting access to a particular configuration.

Table 4: Restricting Configuration Access Using deny-configuration and deny-configuration-regexps Statements

Configuration Denied	Using: deny-configuration	Using: deny-configuration-regexps	Result

xnm-ssl	[edit system]
	login {
	class test {
	permissions configure;
	allow-configuration .*;
	deny-configuration .*xnm-ssl;
	}
	}
		[edit system]
		login {
		class test {
		permissions configure;
		allow-configuration .*;
		deny-configuration-regexps ".* .* .*-ssl"";
		}
		}
			The following configuration statement is denied:
			• system services xnm-ssl

ssh	[edit system]
	login {
	class test {
	permissions configure;
	allow-configuration .*;
	deny-configuration ".*ssh";
	}
	}
		[edit system]
		login {
		class test {
		permissions configure;
		allow-configuration .*;
		deny-configuration-regexps ".*ssh";
		deny-configuration-regexps ".* .*ssh";
		deny-configuration-regexps ".* .* .*ssh";
		}
		}
			The following configuration statements are denied:
			• system host-name hostname-ssh
			• system services ssh
			• system services outbound-ssh
			• security ssh-known-host

Although the `allow/deny-configuration` statements are also useful when you want a simple configuration, the `allow/deny-configuration-regexps` statements provide better performance and overcome the ambiguity that existed when combining expressions in the `allow/deny-configuration` statements.

Using Regular Expressions on Remote Authorization Servers

You can use extended regular expressions to specify which operational mode and configuration mode commands and configuration statements and hierarchies are allowed or denied for certain users. You specify these regular expressions locally in the `allow/deny-commands`, `allow/deny-configuration`, `allow/deny-commands-regexps` and `allow/deny-configuration-regexps` statements at the `[edit system login class` *`class-name`*`]` hierarchy level. You specify these regular expressions remotely by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authorization server's configuration. When you

configure authorization parameters both locally and remotely, the device merges the regular expressions received during TACACS+ or RADIUS authorization with any regular expressions defined on the local device.

NOTE: Starting in Junos OS Release 18.1, the `allow-commands-regexps` and `deny-commands-regexps` statements are supported for TACACS+ authorization.

When specifying multiple regular expressions in a local configuration using the `allow-commands`, `deny-commands`, `allow-configuration`, or `deny-configuration` statements, you configure regular expressions within parentheses and separate them using the pipe symbol. You enclose the complete expression in double quotation marks. For example, you can specify multiple `allow-commands` parameters with the following syntax:

```
allow-commands "(cmd1)|(cmd2)|(cmdn)"
```

The RADIUS authorization server uses the following attributes and syntax:

```
Juniper-Allow-Commands += "(cmd1)|(cmd2)|(cmd3)",
Juniper-Deny-Commands += "(cmd1)|(cmd2)",
Juniper-Allow-Configuration += "(config1)|(config2)",
Juniper-Deny-Configuration += "(config1)|(config2)",
```

The TACACS+ authorization server uses the following attributes and syntax:

```
allow-commands = "(cmd1)|(cmd2)|(cmdn)"
deny-commands = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration = "(config1)|(config2)|(confign)"
deny-configuration = "(config1)|(config2)|(confign)"
```

When specifying multiple regular expressions in a local configuration using the `allow-commands-regexps`, `deny-commands-regexps`, `allow-configuration-regexps`, or `deny-configuration-regexps` statements, you configure regular expressions within double quotation marks and separate them using the space operator. You enclose the complete expression in square brackets. For example, you can specify multiple allow-commands parameters with the following syntax:

```
allow-commands-regexps [ "cmd1" "cmd2" "cmdn" ]
```

The RADIUS authorization server uses the following attributes and syntax:

```
Juniper-Allow-Configuration-Regexps += "(config1)|(config2)|(confign)",
Juniper-Deny-Configuration-Regexps += "(config1)|(config2)|(confign)",
```

The TACACS+ authorization server uses the following attributes and syntax:

```
allow-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
deny-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration-regexps = "(config1)|(config2)|(confign)"
deny-configuration-regexps = "(config1)|(config2)|(confign)"
```

RADIUS and TACACS+ servers also support a simplified syntax where you specify each individual expression on a separate line. For example, the RADIUS server simplified syntax is:

```
Juniper-Allow-Commands += "cmd1",
Juniper-Allow-Commands += "cmd2",
Juniper-Allow-Commands += "cmdn",
```

Similarly, the TACACS+ server simplified syntax is:

```
allow-commands-regexps1 = "cmd1"
allow-commands-regexps2 = "cmd2"
allow-commands-regexpsn = "cmdn"
```

Table 5 on page 74 differentiates the local authorization configuration and the TACACS+ server authorization configuration using regular expressions.

Table 5: Sample Local and Remote Authorization Configuration Using Regular Expressions

Local Configuration	Remote TACACS+ Configuration

login {
class local {
permissions configure;
allow-commands "(ping .*)|
(traceroute .*)|(show .*)|
(configure .*)|(edit)|(exit)|(commit)|
(rollback .*)";
deny-commands .*;
allow-configuration
"(interfaces .* unit 0 family
ethernet-switching vlan mem.* .*)|
(interfaces .* native.* .*)|
(interfaces .* unit 0 family ethernet-
switching interface-mo.* .*)|
(interfaces .* unit .*)|
(interfaces .* disable)|
(interfaces .* description .*)|
(vlans .* vlan-.* .*)"
deny-configuration .*;
}
}
	user = remote {
	login = username
	service = junos-exec {
	allow-commands1 = "ping .*"
	allow-commands2 = "traceroute .*"
	allow-commands3 = "show .*"
	allow-commands4 = "configure"
	allow-commands5 = "edit"
	allow-commands6 = "exit"
	allow-commands7 = "commit"
	allow-commands8 = ".*xml-mode"
	allow-commands9 = ".*netconf.*"
	allow-commands10 = ".*need-trailer"
	allow-commands11 = "rollback.*"
	allow-commands12 = "junoscript"
	deny-commands1 = ".*"
	allow-configuration1 = "interfaces .* unit 0 family ethernet-
	switching vlan mem.* .*"
	allow-configuration2 = "interfaces .* native.* .*"
	allow-configuration3 = "interfaces .* unit 0 family ethernet-
	switching interface-mo.* .*"
	allow-configuration4 = "interfaces .* unit .*"
	allow-configuration5 = "interfaces .* disable"
	allow-configuration6 = "interfaces .* description .*"
	allow-configuration7 = "interfaces .*"
	allow-configuration8 = "vlans .* vlan-.* .*"
	deny-configuration1 = ".*"
	local-user-name = *local-username*
	user-permissions = "configure"
	}
	}

NOTE:

- You need to explicitly allow access to the NETCONF mode, either locally or remotely, by issuing the following three commands: `xml-mode`, `netconf`, and `need-trailer`.

- When you use the `deny-configuration = ".*"` statement, you must allow all the desired configurations using the `allow-configuration` statement. However, this configuration can affect the allowed regular expressions buffer limit for the `allow-configuration` statement. If this limit is exceeded, the allowed configuration might not work.

Specify Regular Expressions

WARNING: When you specify regular expressions for commands and configuration statements, pay close attention to the following examples. A regular expression with invalid syntax might not produce the desired results, even if the configuration is committed without any error.

You should specify regular expressions for commands and configuration statements in the same manner as executing the complete command or statement. Table 6 on page 76 lists the regular expressions for configuring access privileges for the `[edit interfaces]` and `[edit vlans]` statement hierarchies.

Table 6: Specify Regular Expressions

Statement	Regular Expression	Configuration Notes
[edit interfaces] The set command for interfaces is executed as follows: [edit] user@host# **set interfaces *interface-name* unit *interface-unit-number***	The set interfaces statement is incomplete by itself and requires the unit option to execute the statement. As a result, the regular expression required for denying the set interfaces configuration must specify the entire executable string with the .* operator in place of statement variables: [edit system login class *class-name*] user@host# **set permissions configure** user@host# **set deny-configuration "interfaces .* unit .*"**	• The .* operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any interface name with any unit value. • Specifying only the deny-configuration "interfaces .*" statement is incorrect and does not deny access to the interfaces configuration for the specified login class. • Other valid options can be included in the regular expression. For example: [edit system login class *class-name*] user@host# **set permissions configure** user@host# **set deny-configuration "interfaces .* description .*"** [edit system login class *class-name*] user@host# **set permissions configure** user@host# **set allow-configuration-regexps ["interfaces .* description .*" "interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*" "interfaces.* disable"]** [edit system login class *class-name*] user@host# **set permissions configure** user@host# **set allow-configuration "interfaces .* unit 0 family ethernet-switching vlan mem.* .*"** Note: The mem.* regular expression in this example is used when multiple

Table 6: Specify Regular Expressions *(Continued)*

Statement	Regular Expression	Configuration Notes
		strings starting with the *mem* keyword are expected to be included in the specified regular expression. When only one `member` string is expected to be included, the `member .*` regular expression is used.

[edit vlans]
 	
The `set` command for VLANs is executed as follows:
 	
`[edit`
`user@host# set vlans vlan-name vlan-id vlan-id`
	Here, the `set vlans` statement is incomplete by itself, and requires the `vlan-id` option to execute the statement.
	
	As a result, the regular expression required for allowing the `set vlans` configuration must specify the entire executable string with the `.*` operator in place of statement variables:
	
	`[edit system login class class-name]`
	`user@host# set permissions configure`
	`user@host# set allow-configuration "vlans .* vlan-id .*"`
		• The `.*` operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any VLAN name with any VLAN ID.
		
		• Other valid options under the `[edit vlans]` statement hierarchy can be included in the regular expression. For example:
		
		`[edit system login class class-name]`
		`user@host# set permissions configure`
		`user@host# set allow-configuration-regexps [ "vlans .* vlan-id .*" "vlans .* vlan-id .* description .*" "vlans .* vlan-id .* filter .*" ]`

Regular Expressions Operators

Table 7 on page 78 lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

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

Table 7: Common Regular Expression Operators

Operator	Match	Example

|	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.	`[edit system login class test]`
		`user@host# set permissions configure`
		`user@host# set allow-commands "(ping)|(traceroute)|(show system alarms)|(show system software)"`
		`user@host# set deny-configuration "(access)|(access-profile)|(accounting-options)|(applications)|(apply-groups)|(bridge-domains)|(chassis)|(class-of-service)"`
		
		With the preceding configuration, the users assigned to the test login class have operational mode access restricted to only the commands specified in the `allow-commands` statement. They also have access to configuration mode, excluding the hierarchy levels specified in the `deny-configuration` statement.

^	At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.	`[edit system login class test]`
		`user@host# set permissions interface`
		`user@host# set permissions interface-control`
		`user@host# set allow-commands "(^show) (log|interfaces|policer))|(^monitor)"`
		
		With the preceding configuration, the users assigned to the test login class have access to viewing and configuring the interface configuration. The `allow-commands` statement grants access to commands that begin with the `show` and `monitor` keywords.
		
		For the first filter, the commands specified include the `show log`, `show interfaces`, and `show policer` commands. The second filter specifies all commands starting with the `monitor` keyword, such as the `monitor interfaces` or the `monitor traffic` commands.

Table 7: Common Regular Expression Operators *(Continued)*

Operator	Match	Example

$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point.	`[edit system login class test]`
		`user@host# set permissions interface`
		`user@host# set allow-commands "(show interfaces$)"`
		
		With the preceding configuration, the users assigned to the test login class can view the interfaces configuration in configuration mode. The users can also view the interface configuration with the `show configuration` operational mode command. However, the regular expression specified in the `allow-commands` statement restricts the users to execute only the `show interfaces` command and denies access to the command extensions such as `show interfaces detail` or `show interfaces extensive`.

[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).	`[edit system login class test]`
		`user@host# set permissions clear`
		`user@host# set permissions configure`
		`user@host# set permissions network`
		`user@host# set permissions trace`
		`user@host# set permissions view`
		`user@host# set allow-configuration-regexps [ "interfaces [gx]e-.* unit [0-9]* description .*" ]`
		
		With the preceding configuration, the users assigned to the test login class have operator-level user permissions. These users also have access to configure interfaces within the specified range of interface name and unit number (0 through 9).

Table 7: Common Regular Expression Operators *(Continued)*

Operator	Match	Example

( )	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.	`[edit system login class test]`
		`user@host# set permissions all`
		`user@host# set allow-commands "(clear)|(configure)"`
		`user@host# deny-commands "(mtrace)|(start)|(delete)"`
		
		With the above configuration, users assigned to the test login class have superuser-level permissions and have access to the commands specified in the `allow-commands` statement.

*	Zero or more terms.	`[edit system login class test]`
		`user@host# set permissions configure`
		`user@host# set deny-configuration "(system login class m*)"`
		
		With the above configuration, users assigned to the test login class whose login username begins with `m` are denied configuration access.

+	One or more terms.	`[edit system login class test]`
		`user@host# set permissions configure`
		`user@host# set deny-configuration "(system login class m+)"`
		
		With the above configuration, users assigned to the test login class whose login username begins with `m` are denied configuration access.

Table 7: Common Regular Expression Operators *(Continued)*

Operator	Match	Example

.	Any character except for a space " ".	`[edit system login class test]`
		`user@host# set permissions configure`
		`user@host# set deny-configuration "(system login class m.)"`
		
		With the above configuration, users assigned to the test login class whose login username begins with `m` are denied configuration access.

.*	Everything from the specified point onward.	`[edit system login class test]`
		`user@host# set permissions configure`
		`user@host# set deny-configuration "(system login class m .*)"`
		
		With the above configuration, users assigned to the test login class whose login username begins with `m` are denied configuration access.
		
		Similarly, the `deny-configuration "protocols .*"` statement denies all configuration access under the `[edit protocols]` hierarchy level.
		
		NOTE:
		• The `*`, `+`, and `.` operations can be achieved by using `.*`.
		• The `deny-commands .*` and `deny-configuration .*` statements deny access to all operational mode commands and configuration hierarchies, respectively.

NOTE: The `!` regular expression operator is not supported.

Regular Expression Examples

Table 8 on page 82 lists the regular expressions used to allow configuration options under two configuration hierarchies—`[edit system ntp server]` and `[edit protocols rip]`—as an example for specifying regular expressions.

NOTE: Table 8 on page 82 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular

expressions listed in the table are validated only for the [edit system ntp server] and [edit protocols rip] statement hierarchies.

Table 8: Regular Expressions Examples

Statement Hierarchy	Regular Expressions	Allowed Configuration	Denied Configuration
[edit system ntp server]			
key *key-number*	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* key .*"] set deny-configuration-regexps ["system ntp server .* version .*" "system ntp server .* prefer"]	• server IP • server IP and key	• version • prefer
version *version-number*	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* version .*"] set deny-configuration-regexps ["system ntp server .* key .*" "system ntp server .* prefer"]	• server IP • server IP and version	• key • prefer
prefer	[edit system login class test] set permissions configure set allow-configuration-regexps ["system ntp server .*" "system ntp server .* prefer"]; set deny-configuration-regexps ["system ntp server .* key .*" "system ntp server .* version .*"]	• server IP • server IP and prefer	• key • version

Table 8: Regular Expressions Examples *(Continued)*

Statement Hierarchy	Regular Expressions	Allowed Configuration	Denied Configuration
`[edit protocols rip]`			

message-size *message-size*	`[edit system login class test]`
	`set permissions configure`
	`set allow-configuration-regexps`
	`"protocols rip message-size .*"`
	`set deny-configuration-regexps`
	`[ "protocols rip metric-in .*"`
	`"protocols rip route-timeout .*"`
	`"protocols rip update-interval .*" ]`
		• message-size	• metric-in
			• route-timeout
			• update-interval

metric-in *metric-in*	`[edit system login class test]`
	`set permissions configure`
	`set  allow-configuration-regexps`
	`"protocols rip metric-in .*"`
	`set  deny-configuration-regexps`
	`[ "protocols rip message-size .*"`
	`"protocols rip route-timeout .*"`
	`"protocols rip update-interval .*" ]`
		• metric-in	• message-size
			• route-timeout
			• update-interval

route-timeout *route-timeout*	`[edit system login class test]`
	`set permissions configure`
	`set allow-configuration-regexps`
	`"protocols rip route-timeout .*"`
	`set deny-configuration-regexps`
	`[ "protocols rip metric-in .*"`
	`"protocols rip message-size .*"`
	`"protocols rip update-interval .*" ]`
		• route-timeout	• message-size
			• metric-in
			• update-interval

Table 8: Regular Expressions Examples *(Continued)*

Statement Hierarchy	Regular Expressions	Allowed Configuration	Denied Configuration

update-interval *update-interval*	`[edit system login class test]`
	`set permissions configure`
	`set allow-configuration-regexps`
	`"protocols rip update-interval .*"`
	`set deny-configuration-regexps`
	`[ "protocols rip metric-in .*"`
	`"protocols rip route-timeout .*"`
	`"protocols rip message-size .*" ]`
		• update-interval	• message-size
			• metric-in
			• route-timeout

How to Define Access Privileges with allow-configuration and deny-configuration Statements

You can define access privileges for configuration statement hierarchies by using a combination of the following types of statements:

- permission flags
- `allow-configuration` and `deny-configuration` statements

The permission flags define the larger boundaries of what a person or login class can access and control. The `allow-configuration` and `deny-configuration` statements contain one or more regular expressions that allow or deny specific configuration hierarchies and statements. The `allow-configuration` and `deny-configuration` statements take precedence over permission flags and give the administrator finer control over exactly what hierarchies and statements the user can view and configure.

This topic explains how to define access privileges using `allow-configuration` and `deny-configuration` statements by showing examples of login class configurations that use these statements. Examples 1 through 3 create login classes that allow users access to all commands and statements except those defined in the `deny-configuration` statement.

Notice that *permission bit* and *permission flag* are used interchangeably.

Example 1

To create a login class that allows the user to execute all commands and configure everything except telnet parameters:

1. Set the user's login class permissions to `all`.

```
[edit system login]
user@host# set class all-except-telnet permissions all
```

2. Include the following `deny-configuration` statement.

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

Example 2

To create a login class that allows the user to execute all commands and configure everything except statements within any login class whose name begins with "m":

1. Set the user's login class permissions to `all`.

```
[edit system login]
user@host# set class all-except-login-class-m permissions all
```

2. Include the following `deny-configuration` statement.

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

Example 3

To create a login class that allows the user to execute all commands and configure everything except the `[edit system login class]` or `[edit system services]` hierarchy levels:

1. Set the user's login class permissions to `all`.

```
[edit system login]
user@host# set class all-except-login-class-or-system-services permissions all
```

2. Include the following `deny-configuration` statement:

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

The following examples show how to use the `allow-configuration` and `deny-configuration` statements to determine permissions inverse to each other for the `[edit system services]` hierarchy level.

Example 4

To create a login class that allows the user to have full configuration privileges only at the `[edit system services]` hierarchy level:

1. Set the user's login class permissions to `configure`.

```
[edit system login]
user@host# set class configure-only-system-services permissions configure
```

2. Include the following `allow-configuration` statement:

```
[edit system login class configure-only-system-services]
user@host# set allow-configuration "system services"
```

Example 5

To create a login class that allows the user full permissions for all commands and all configuration hierarchies except the `[edit system services]` hierarchy level:

1. Set the user's login class permissions to `all`.

```
[edit system login]
user@host# set class all-except-system-services permissions all
```

2. Include the following `deny-configuration` statement.

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

Example: Use Additive Logic with Regular Expressions to Specify Access Privileges

IN THIS SECTION

This example shows how to use additive logic when using regular expressions to set up configuration access privileges.

Requirements

This example uses a device running Junos OS Release 16.1 or later.

Overview

You can define regular expressions to control who can make changes to the configuration and what they can change. These regular expressions indicate specific configuration hierarchies that users in a login class are permitted to access. For example, you can define regular expressions that allow users to modify a group of routing instances and define regular expressions that prevent the users from making changes to any other routing instances or to other configuration levels. You define the regular expressions by configuring the `allow-configuration-regexps` and `deny-configuration-regexps` statements for a login class.

By default, the `deny-configuration-regexps` statement takes precedence over the `allow-configuration-regexps` statement. If a configuration hierarchy appears in a `deny-configuration-regexps` statement for a login class, it is not visible to the users in that class, regardless of the contents of the `allow-configuration-regexps` statement. If a configuration hierarchy does not appear in a `deny-configuration-regexps` statement, it is visible to the users in that class if it appears in an `allow-configuration-regexps` statement.

You can change this default behavior by enabling additive logic for the `*-configuration-regexps` statements. When you enable additive logic, the `allow-configuration-regexps` statement takes precedence over the `deny-configuration-regexps` statement.

Thus, if the `deny-configuration-regexps` statement denies access to all configuration hierarchies at a given level (protocols .*) but the `allow-configuration-regexps` statement allows access to one sub-hierarchy (protocols bgp .*), then by default the device denies access to the hierarchies for users in that login class

because the deny-configuration-regexps statement takes precedence. However, if you enable additive logic, the device allows access to the specified sub-hierarchy for users in that login class because the allow-configuration-regexps takes precedence in this case.

Configuration

IN THIS SECTION

Step-by-Step Procedure

To enable additive logic to explicitly allow users in a given login class access to one or more individual configuration hierarchies:

1. Include the deny-configuration-regexps statement, and explicitly deny access to configuration hierarchies.

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

For example:

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

2. Include the allow-configuration-regexps statement, and define regular expressions for the specific hierarchies to allow.

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

For example:

```
[edit system login class class-name]
user@host# set allow-configuration-regexps ["protocols bgp .*" "protocols ospf .*"]
```

3. Enable additive logic for the `allow-configuration-regexps` and `deny-configuration-regexps` regular expressions.

```
[edit system]
user@host# set regex-additive-logic
```

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

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

5. Commit your changes.

Users assigned to this login class have access to the configuration hierarchies included in the `allow-configuration-regexps` statement but do not have access to the other hierarchies specified in the `deny-configuration-regexps` statement.

NOTE: When you configure the `regex-additive-logic` statement, the behavior change applies to all `allow-configuration-regexps` and `deny-configuration-regexps` statements present in all login classes. If you enable additive logic, you should evaluate existing statements for any impact, and update the regular expressions in those statements as appropriate.

Examples

IN THIS SECTION

Use Regular Expressions with Additive Logic

Purpose

This section provides examples of regular expressions that use additive logic to give you ideas for creating configurations appropriate for your system.

Allow Specific Routing Instances

The following example login class includes a regular expression that allows configuration of routing instances whose names start with `CUST-VRF-`; for example, `CUST-VRF-1`, `CUST-VRF-25`, `CUST-VRF-100`, and so on. The example also includes a regular expression that prevents the configuration of any routing instances.

```
[edit system login class class-name]
user@host# set permissions [configure routing-control view view-configuration]
user@host# set deny-configuration-regexps "routing-instances .*"
user@host# set allow-configuration-regexps "routing-instances CUST-VRF-.* .*"
```

By default, the `deny-configuration-regexps` statement takes precedence, and the previous configuration prevents the users in the login class from configuring any routing instances, regardless of the name.

However if you configure the following statement, the `allow-configuration-regexps` statement takes precedence. Thus, the users can configure routing instances whose names start with `CUST-VRF-`, but the users cannot configure any other routing instances.

```
[edit system]
user@host# set regex-additive-logic
```

Allow BGP Peer Configuration Only

The following example login class includes regular expressions that prevent configuration at the `[edit protocols]` hierarchy level but allow configuration of BGP peers:

```
[edit system login class class-name]
user@host# set permissions [configure routing-control view view-configuration]
user@host# set deny-configuration-regexps "protocols .*"
user@host# set allow-configuration-regexps "protocols bgp group .*"
```

By default, the previous configuration prevents the users in the login class from making changes to any hierarchies under `[edit protocols]`.

However, if you configure the following statement, the users in the login class can make changes to BGP peers, but the users cannot configure other protocols or other BGP statements outside of the allowed hierarchy level.

```
[edit system]
user@host# set regex-additive-logic
```

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 configure the hierarchy levels that are allowed.
   - You should be able to configure statements in hierarchy levels that have been allowed.
   - Hierarchy levels that are denied should not be visible.
   - Any allowed or denied expressions should take precedence over any permissions granted with the `permissions` statement.

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

IN THIS SECTION

This example shows how to configure custom login classes and assign access privileges for operational mode commands. Users in the login class can execute only the commands for which they have access.

This prevents unauthorized users from executing sensitive commands that could cause damage to the network.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server

Before you begin, establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

Overview and Topology

Figure 1 on page 92 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

Figure 1: Topology

This example configures R1 with three customized login classes: Class1, Class2, and Class3. Each class defines access privileges for the user by configuring the `permissions` statement and by defining extended regular expressions using the `allow-commands` and `deny-commands` statements.

The purpose of each login class is as follows:

- **Class1**—Defines access privileges for the user with the `allow-commands` statement only. This login class provides operator-level user permissions and authorization for rebooting the device.
- **Class2**—Defines access privileges for the user with the `deny-commands` statement only. This login class provides operator-level user permissions and denies access to `set` commands.
- **Class3**—Defines access privileges for the user with both the `allow-commands` and `deny-commands` statements. This login class provides superuser-level user permissions and authorization for accessing interfaces and viewing device information. It also denies access to the `edit` and `configure` commands.

Router R1 has three different users, User1, User2, and User3 assigned to the Class1, Class2, and Class3 login classes, respectively .

Configuration

IN THIS SECTION

CLI Quick Configuration

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

R1

```
set system authentication-order tacplus
set system authentication-order radius
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66 secret "$ABC123"
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66 secret "$ABC123"
set system login class Class1 permissions clear
set system login class Class1 permissions network
set system login class Class1 permissions reset
set system login class Class1 permissions trace
set system login class Class1 permissions view
```

```
set system login class Class1 allow-commands "request system reboot"
set system login class Class2 permissions clear
set system login class Class2 permissions network
set system login class Class2 permissions reset
set system login class Class2 permissions trace
set system login class Class2 permissions view
set system login class Class2 deny-commands set
set system login class Class3 permissions all
set system login class Class3 allow-commands configure
set system login class Class3 deny-commands .*
set system login user User1 uid 2001
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2002
set system login user User2 class Class2
set system login user User2 authentication encrypted-password "$ABC123"
set system login user User3 uid 2003
set system login user User3 class Class3
set system login user User3 authentication encrypted-password "$ABC123"
set system syslog file messages any any
```

Configure Authentication Parameters for Router R1

Step-by-Step Procedure

To configure Router R1 authentication:

1. Configure the order in which R1 attempts to authenticate the user. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, and then the local password.

```
[edit system]
user@R1# set authentication-order tacplus
user@R1# set authentication-order radius
user@R1# set authentication-order password
```

2. Configure the TACACS+ server.

```
[edit system]
user@R1# set tacplus-server 10.209.1.66 secret "$ABC123"
```

```
user@R1# set tacplus-options enhanced-accounting
user@R1# set accounting destination tacplus server 10.209.1.66 secret "$ABC123"
```

3. Configure the RADIUS server.

```
[edit system]
user@R1# set radius-server 10.209.1.66 secret "$ABC123"
user@R1# set radius-options enhanced-accounting
```

4. Configure R1 accounting parameters.

```
[edit system]
user@R1# set accounting events login
user@R1# set accounting events change-log
user@R1# set accounting events interactive-commands
user@R1# set accounting traceoptions file auditlog
user@R1# set accounting traceoptions flag all
```

Configure Access Privileges with the allow-commands Statement (Class1)

Step-by-Step Procedure

To specify regular expressions using the `allow-commands` statement:

1. Configure the Class1 login class and assign operator-level user permissions.

```
[edit system login]
user@R1# set class Class1 permissions [clear network reset trace view]
```

2. Configure the `allow-commands` regular expression to enable users in the class to reboot the device.

```
[edit system login]
user@R1# set class Class1 allow-commands "request system reboot"
```

3. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set user User1 uid 2001
user@R1# set user User1 class Class1
user@R1# set user User1 authentication encrypted-password "$ABC123"
```

Configure Access Privileges with the deny-commands Statement (Class2)

Step-by-Step Procedure

To specify regular expressions using the `deny-commands` statement:

1. Configure the Class2 login class and assign operator-level user permissions.

```
[edit system login]
user@R1# set class Class1 permissions [clear network reset trace view]
```

2. Configure the `deny-commands` regular expression to prevent users in the class from executing `set` commands.

```
[edit system login]
user@R1# set class Class1 deny-commands "set"
```

3. Configure the user account for the Class2 login class.

```
[edit system login]
user@R1# set user User2 uid 2002
user@R1# set user User2 class Class2
user@R1# set user User2 authentication encrypted-password "$ABC123"
```

Configure Access Privileges with Both the allow-commands and deny-commands Statements (Class3)

Step-by-Step Procedure

To specify regular expressions using both the `allow-commands` and `deny-commands` statements:

1. Configure the Class3 login class and assign superuser-level permissions.

```
[edit system login]
user@R1# set class Class3 permissions all
```

2. Configure the `deny-commands` regular expression to prevent users in the class from executing any commands.

```
[edit system login]
user@R1# set class Class3 deny-commands ".*"
```

3. Configure the `allow-commands` regular expression to allow users to enter configuration mode.

```
[edit system login]
user@R1# set class Class3 allow-commands configure
```

4. Configure the user account for the Class3 login class.

```
[edit system login]
user@R1# set user User3 uid 2003
user@R1# set user User3 class Class3
user@R1# set user User3 authentication encrypted-password "$ABC123"
```

Results

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

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
    10.209.1.66 secret "$ABC123";
}
tacplus-server {
    10.209.1.66 secret "$ABC123";
}
radius-options {
```

```
    enhanced-accounting;
}
tacplus-options {
    enhanced-accounting;
}
accounting {
    events [ login change-log interactive-commands ];
    traceoptions {
        file auditlog;
        flag all;
    }
    destination {
        tacplus {
            server {
                10.209.1.66 secret "$ABC123";
            }
        }
    }
}
login {
    class Class1 {
        permissions [ clear network reset trace view ];
        allow-commands "request system reboot";
    }
    class Class2 {
        permissions [ clear network reset trace view ];
        deny-commands set;
    }
    class Class3 {
        permissions all;
        allow-commands configure;
        deny-commands .*;
    }
    user User1 {
        uid 2001;
        class Class1;
        authentication {
            encrypted-password "$ABC123";
        }
    }
    user User2 {
        uid 2002;
        class Class2;
```

```
        authentication {
            encrypted-password "$ABC123";
        }
    }
    user User3 {
        uid 2003;
        class Class3;
        authentication {
            encrypted-password “$ABC123”;
        }
    }
}
syslog {
    file messages {
        any any;
    }
}
```

Verification

IN THIS SECTION

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

Verifying the Class1 Configuration

Purpose

Verify that the permissions and commands allowed in the Class1 login class are working.

Action

In operational mode, run the `show system users` command.

```
User1@R1> show system users
12:39PM  up 6 days, 23 mins, 6 users, load averages: 0.00, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
User1  p0       abc.example.net 12:34AM 12:04 cli
User2  p1       abc.example.net 12:36AM 12:02 -cli (cli)
User3  p2       abc.example.net 10:41AM    11 -cli (cli)
```

In operational mode, run the `request system reboot` command.

```
User1@R1> request system ?
Possible completions:
  reboot               Reboot the system
```

Meaning

The Class1 login class to which User1 is assigned has operator-level user permissions and allows users in the class to execute the `request system reboot` command.

The predefined operator login class has the following permission flags specified:

- **clear**—Can use `clear` commands to clear (delete) information that the device learns from the network and stores in various network databases.
- **network**—Can access the network by using the `ping`, `ssh`, `telnet`, and `traceroute` commands.
- **reset**—Can restart software processes by using the `restart` command.
- **trace**—Can view trace file settings and configure trace file properties.
- **view**—Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.

For the Class1 login class, in addition to the above-mentioned user permissions, User1 can execute the `request system reboot` command. The first output displays the view permissions as an operator, and the second output shows that the only `request system` command that User1 can execute as an operator is the `request system reboot` command.

Verifying the Class2 Configuration

Purpose

Verify that the permissions and commands allowed for the Class2 login class are working.

Action

In operational mode, run the `ping` command.

```
User2@R1> ping 10.209.1.66
ping 10.209.1.66
PING 10.209.1.66 (10.209.1.66): 56 data bytes
64 bytes from 10.209.1.66: icmp_seq=0 ttl=52 time=212.521 ms
64 bytes from 10.209.1.66: icmp_seq=1 ttl=52 time=212.844 ms
64 bytes from 10.209.1.66: icmp_seq=2 ttl=52 time=211.304 ms
64 bytes from 10.209.1.66: icmp_seq=3 ttl=52 time=210.963 ms
^C
--- 10.209.1.66 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 210.963/211.908/212.844/0.792 ms
```

From the CLI prompt, check the available commands.

```
User2@R1> ?
Possible completions:
  clear               Clear information in the system
  file                Perform file operations
  help                Provide help information
  load                Load information from file
  monitor             Show real-time debugging information
  mtrace              Trace multicast path from source to receiver
  op                  Invoke an operation script
  ping                Ping remote target
  quit                Exit the management session
  request             Make system-level requests
  restart             Restart software process
  save                Save information to file
  show                Show system information
  ssh                 Start secure shell on another host
  start               Start shell
```

```
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

From the CLI prompt, execute any set command.

```
User2@R1> set
             ^
unknown command.
```

Meaning

The Class2 login class to which User2 is assigned has operator-level user permissions and denies access to all `set` commands.

The permission flags specified for the predefined operator login class are the same as those specified for Class1.

Verifying Class3 Configuration

Purpose

Verify that the permissions and commands allowed for the Class3 login class are working.

Action

In operational mode, check the available commands.

```
User3@R1> ?
Possible completions:
  configure            Manipulate software configuration information
```

Enter configuration mode.

```
User3@R1> configure
Entering configuration mode

[edit]
User3@R1#
```

Meaning

The Class3 login class to which User3 is assigned has superuser (all) permissions, but this class only allows users to execute the `configure` command. The class denies access to all other operational mode commands. Because the regular expressions specified in the `allow/deny-commands` statements take precedence over the user permissions, User3 on R1 has access only to configuration mode and is denied access to all other operational mode commands.

Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies

IN THIS SECTION

This example shows how to configure custom login classes and assign access privileges to specific configuration hierarchies. Users in the login class can view and modify only those configuration statements and hierarchies to which they have access. This prevents unauthorized users from modifying device configurations that could cause damage to the network.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server

Before you begin, establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

Overview and Topology

Figure 2 on page 104 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

Figure 2: Topology

This example configures R1 with two customized login classes: Class1 and Class2. Each class defines access privileges for the user by configuring the `permissions` statement and by defining extended regular expressions using the `allow-configuration`, `deny-configuration`, `allow-configuration-regexps`, and `deny-configuration-regexps` statements.

The purpose of each login class is as follows:

- **Class1**—Defines access privileges for the user with the `allow-configuration` and `deny-configuration` statements. This login class provides access to configure the `[edit interfaces]` hierarchy only and denies all other access on the device. To do this, the user permissions include `configure` to provide configuration access. In addition, the `allow-configuration` statement allows access to the interfaces configuration, and the `deny-configuration` statement denies access to all other configuration hierarchies. Because the allow statement takes precedence over the deny statement, the users assigned to the Class1 login class can access only the `[edit interfaces]` hierarchy level.
- **Class2**—Defines access privileges for the user with the `allow-configuration-regexps` and `deny-configuration-regexps` statements. This login class provides superuser-level user permissions and explicitly allows configuration under multiple hierarchy levels for interfaces. It also denies access to the `[edit system]` and `[edit protocols]` hierarchy levels.

Router R1 has two users, User1 and User2, assigned to the Class1 and Class2 login classes, respectively.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

R1

```
set system authentication-order tacplus
set system authentication-order radius
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66 secret "$ABC123"
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66 secret "$ABC123"
set system login class Class1 permissions configure
set system login class Class1 allow-configuration "interfaces .* unit .*"
set system login class Class1 deny-configuration .*
set system login class Class2 permissions all
set system login class Class2 allow-configuration-regexps [ "interfaces .* description .*"
"interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*"
"interfaces.* disable" ]
set system login class Class2 deny-configuration-regexps [ "system" "protocols" ]
set system login user User1 uid 2004
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2006
set system login user User2 class Class2
set system login user User2 authentication encrypted-password "$ABC123"
set system syslog file messages any any
```

Configure Authentication Parameters for Router R1

Step-by-Step Procedure

To configure Router R1 authentication:

1. Configure the order in which R1 attempts to authenticate the user. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, and then the local password.

```
[edit system]
user@R1# set authentication-order tacplus
user@R1# set authentication-order radius
user@R1# set authentication-order password
```

2. Configure the TACACS+ server.

```
[edit system]
user@R1# set tacplus-server 10.209.1.66 secret "$ABC123"
user@R1# set tacplus-options enhanced-accounting
user@R1# set accounting destination tacplus server 10.209.1.66 secret "$ABC123"
```

3. Configure the RADIUS server.

```
[edit system]
user@R1# set radius-server 10.209.1.66 secret "$ABC123"
user@R1# set radius-options enhanced-accounting
```

4. Configure the R1 accounting parameters.

```
[edit system]
user@R1# set accounting events login
user@R1# set accounting events change-log
user@R1# set accounting events interactive-commands
user@R1# set accounting traceoptions file auditlog
user@R1# set accounting traceoptions flag all
```

Configure Access Privileges with the allow-configuration and deny-configuration Statements (Class1)

Step-by-Step Procedure

To specify regular expressions using the `allow-configuration` and `deny-configuration` statements:

1. Configure the Class1 login class with `configure` permissions.

```
[edit system login]
user@R1# set class Class1 permissions configure
```

2. Configure the `allow-configuration` regular expression to allow users in the class to view and modify part of the `[edit interfaces]` hierarchy level.

```
[edit system login]
user@R1# set class Class1 allow-configuration "interfaces .* unit .*"
```

3. Configure the `deny-configuration` regular expression to deny access to all configuration hierarchies.

```
[edit system login]
user@R1# set class Class1 deny-configuration .*
```

4. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set user User1 uid 2004
user@R1# set user User1 class Class1
user@R1# set user User1 authentication encrypted-password "$ABC123"
```

Configure Access Privileges with the allow-configuration-regexps and deny-configuration-regexps Statements (Class2)

Step-by-Step Procedure

To specify regular expressions using the `allow-configuration-regexps` and `deny-configuration-regexps` statements:

1. Configure the Class2 login class and assign superuser (all) permissions.

```
[edit system login]
user@R1# set class Class2 permissions all
```

2. Configure the `allow-configuration-regexps` regular expression to allow users in the class to access multiple hierarchies under the `[edit interfaces]` hierarchy level.

```
[edit system login]
user@R1# set class Class2 allow-configuration-regexps [ "interfaces .* description .*"
"interfaces .* unit .* description .*" "interfaces .* unit .* family inet address .*"
"interfaces.* disable" ]
```

3. Configure the `deny-configuration-regexps` regular expression to prevent users in the class from viewing or modifying the configuration at the `[edit system]` and `[edit protocols]` hierarchy levels.

```
[edit system login]
user@R1# set class Class2 deny-configuration-regexps [ "system" "protocols" ]
```

4. Configure the user account for the Class2 login class.

```
[edit system login]
user@R1# set user User2 uid 2006
user@R1# set user User2 class Class2
user@R1# set user User2 authentication encrypted-password "$ABC123"
```

Results

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

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
    10.209.1.66 secret "$ABC123";
}
tacplus-server {
    10.209.1.66 secret "$ABC123";
}
radius-options {
    enhanced-accounting;
}
tacplus-options {
```

```
    enhanced-accounting;
}
accounting {
    events [ login change-log interactive-commands ];
    traceoptions {
        file auditlog;
        flag all;
    }
    destination {
        tacplus {
            server {
                10.209.1.66 secret "$ABC123";
            }
        }
    }
}
login {
    class Class1 {
        permissions configure;
        allow-configuration "interfaces .* unit .*";
        deny-configuration .*;
    }
    class Class2 {
        permissions all;
        allow-configuration-regexps [ "interfaces .* description .*" "interfaces .* unit .*
description .*" "interfaces .* unit .* family inet address .*" "interfaces.* disable" ];
        deny-configuration-regexps [ "system" "protocols" ];
    }
    user User1 {
        uid 2001;
        class Class1;
        authentication {
            encrypted-password "$ABC123";
        }
    }
    user User2 {
        uid 2002;
        class Class2;
        authentication {
            encrypted-password "$ABC123";
        }
    }
}
```

```
syslog {
    file messages {
        any any;
    }
}
```

Verification

IN THIS SECTION

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

Verify the Class1 Configuration

Purpose

Verify that the permissions allowed in the Class1 login class are working.

Action

In operational mode, check the available commands.

```
User1@R1> ?
Possible completions:
  clear               Clear information in the system
  configure           Manipulate software configuration information
  file                Perform file operations
  help                Provide help information
  load                Load information from file
  op                  Invoke an operation script
  quit                Exit the management session
  request             Make system-level requests
  save                Save information to file
  set                 Set CLI properties, date/time, craft interface message
```

```
  start                Start shell
  test                 Perform diagnostic debugging
```

In configuration mode, check the available configuration permissions.

```
User1@R1# edit ?
Possible completions:
> interfaces           Interface configuration
```

Meaning

User1 has `configure` user permissions, as seen in the first output. Additionally, in configuration mode, User1 has access to the `interfaces` hierarchy level, but only that hierarchy level, as seen in the second output.

Verify the Class2 Configuration

Purpose

Verify that the Class2 configuration is working as expected.

Action

In configuration mode, access the `interfaces` configuration.

```
[edit interfaces]
User2@R1# set ?
Possible completions:
   <interface-name> Interface name
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  ge-0/0/3             Interface name
> interface-range      Interface ranges configuration
> interface-set        Logical interface set configuration
> traceoptions         Interface trace options
```

In configuration mode, access the `system` and `protocols` configuration hierarchies.

```
User2@R1# edit system
          ^
Syntax error, expecting <statement> or <identifier>.
User2@R1# edit protocols
          ^
Syntax error, expecting <statement> or <identifier>.
```

Meaning

User2 has permissions to configure interfaces on R1, but the user does not have permission to view or modify the `[edit system]` or `[edit protocols]` hierarchy levels.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.1	Starting in Junos OS Release 18.1, the `allow-commands-regexps` and `deny-commands-regexps` statements are supported for TACACS+ authorization.

3
CHAPTER

Passwords for User Access

IN THIS CHAPTER

Root Password

IN THIS SECTION

When the device is powered on for the first time, it is ready to be configured. Initially, you log in as the user `root` with no password. You must configure a plain-text password for the root-level user (whose username is *root*) the first time you modify and commit the configuration. Configuring a plain-text password is one way to protect access to the root level by unauthorized users. If you forget the root password for the device, you can use the password recovery procedure to reset the root password.

Configure the Root Password

When you power on the router or switch, it is ready to be configured. Initially, you log in as the user `root` with no password. The root directory 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 in to 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. You *cannot*, however, 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-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 uppercase letter or one lowercase letter, or one character class.

NOTE: 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.

Starting in Junos OS Release 23.1R1, we've removed the 20 characters limit for the root password. The previous requirements for complexity and minimum length were in effect prior to Junos OS Release 23.1R1.

If you use the `encrypted-password` option, then a null-password (empty) is not permitted. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

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`* option 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-ecdsa` or `ssh-rsa` statements to directly configure SSH RSA and 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 device determines whether the private key matches any of the configured public keys.

```
[edit system]
user@host# set root-authentication load-key-file my-host:.ssh/id_rsa.pub
.file.19692               |          0 KB |   0.3 kB/s | ETA: 00:00:00 | 100%
```

In configuration mode, you can confirm your SSH key entries by entering the `show` command. It should look similar to the following output:

```
[edit system]
user@host# show
root-authentication {
    ssh-rsa "$ABC123"; ## SECRET-DATA
}
```

Example: Configure a Plain-Text Password for Root Logins

IN THIS SECTION

This example shows how to configure a plain-text password for the root-level user (the username is *root*). Configuring a plain-text password is one way to prevent unauthorized users from accessing the root level. You must prevent unauthorized users from gaining access to superuser commands that can be used to alter your system configuration.

Requirements

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

The default requirements for a plain-text password are as follows:

- Must be from 6 up to 128 characters long.
- Can include most character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Must contain at least one change of case or character class.

Overview

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

Configuration

IN THIS SECTION

CLI Quick Configuration

To quickly configure this example, copy the following command and paste it into the window. When prompted, type the new password, and then when prompted, retype it.

```
set system root-authentication plain-text-password
```

Configure a Plain-Text Password for User Root

Step-by-Step Procedure

To configure a plain-text password for the root-level user:

1. Type the `set` command for the 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.

```
New password: new-password
Retype new password:
```

3. Retype the same password next to the `Retype new password` prompt and press Enter.

```
New password: new-password
Retype new password: new-password
```

Results

In configuration mode, confirm your configuration by using the `show system` command. It should look something like this:

```
[edit]
user@host# show system
root-authentication {
    encrypted-password "$ABC123"; ## 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 configuration is correct, enter `commit` in configuration mode.

Verification

IN THIS SECTION

Verify the Configuration of a Plain-Text Password for User Root

Purpose

Verify the configuration of a plain-text password for the root-level user.

Action

In operational mode, confirm your configuration by entering the `show configuration system` command.

```
user@host> show configuration system
root-authentication {
    encrypted-password "$ABC123"; ## SECRET-DATA
}
```

Meaning

If you use a plain-text password, the device automatically encrypts the password as soon as you configure it. You do not have to configure the device to encrypt the password, as in some other systems. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration. When a user views the configuration, the user sees only the encrypted string, not the unencrypted password.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.3R1	Starting in Junos OS Release 18.3R1, the ssh-dss and ssh-dsa hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Recover a Root Password

IN THIS SECTION

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

NOTE: You cannot perform root password recovery if you configure the console port as insecure.

After you configure the console port as insecure, if a user tries to perform a password recovery operation by booting in single-user mode, the device prompts for the root password. Additionally, if a user boots in CLI recovery mode, the operation is not allowed. Thus, only a user who knows the root password is able to log in. For more information, see "Configuration Guidelines for Securing Console Port Access" on page 322.

How to Recover the Root Password for Junos OS

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

Before you begin, note the following:

- You need console access to recover the root password.

Video: How to Recover the Root Password in Junos OS

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 (usually a computer) that you 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. From 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.

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

NOTE: Depending on your device hardware, the bootstrap loader might proceed quickly at this step without pausing for input. Pay close attention to the prompts that appear and press the Spacebar immediately after seeing the above prompt flash on the screen.

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

```
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.

```
[edit]
user@host# set system root-authentication plain-text-password
```

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

CAUTION: Avoid using 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.

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

```
New password: password
```

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

```
Retype new password:
```

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

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

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, type `y` to reboot the router.

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

How to Recover the Root Password on Junos OS with Upgraded FreeBSD

If you forget the root password for a device running Junos OS with Upgraded FreeBSD, you can use the password recovery procedure to reset the root password.

For the list of Junos OS devices with upgraded FreeBSD, see Junos kernel upgrade to FreeBSD 10+

Video: How to Recover the Root Password in Junos OS with Upgraded FreeBSD

NOTE: You need console access to recover 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 (usually a computer) that you will 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. Access the Junos Main Menu.

- Prior to Junos OS Release 17.3, the Junos Main Menu appears for 3 seconds on startup before automatically booting the Junos volume. Press any key within the 3 second window to stop the automatic boot sequence and display the Junos Main Menu.

  NOTE: The Junos Main Menu will appear every time you reboot the router while connected to the console.

- Press Ctrl+c at the following part in the reboot to bring up the Junos Main Menu:

```
FreeBSD/x86 bootstrap loader, Revision 1.1
(builder@feyrith.juniper.net, Sun Feb  4 13:06:24 PST 2018)
/
Autoboot in 1 seconds... (press Ctrl-C to interrupt)
```

```
1.  Boot [J]unos volume
2.  Boot Junos volume in [S]afe mode

3.  [R]eboot

4.  [B]oot menu
5.  [M]ore options
```

11. At the Junos Main Menu, press the **M** or **5** key to activate the `5. [M]ore options` menu:

```
1.  Recover [J]unos volume
2.  Recovery mode - [C]LI

3.  Check [F]ile system

4.  Enable [V]erbose boot

5.  [B]oot prompt

6.  [M]ain menu
```

12. Press the **C** or **2** key to access the `2. Recovery mode - [C]LI` option. The router will reboot into CLI recovery mode.
13. When prompted, press the **Enter** key to immediately boot the router, or press any other key to bring up the command prompt.

14. Enter configuration mode in the CLI.

```
root>#  configure
Entering configuration mode
```

15. Set the root password.

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

```
[edit]
root#  set system root-authentication plain-text-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 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 router as root, and you will need to repeat this password recovery process.

16. At the following prompt, enter the new root password. For example:

```
New password:  password
```

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

```
Retype new password:  password
```

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

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

How to Recover the Root Password on Switches

IN THIS SECTION

Problem

Description

If you forget the root password for a switch, use the password recovery procedure to reset the root password.

Before you begin, note the following:

- You need physical access to the switch to recover the root password.

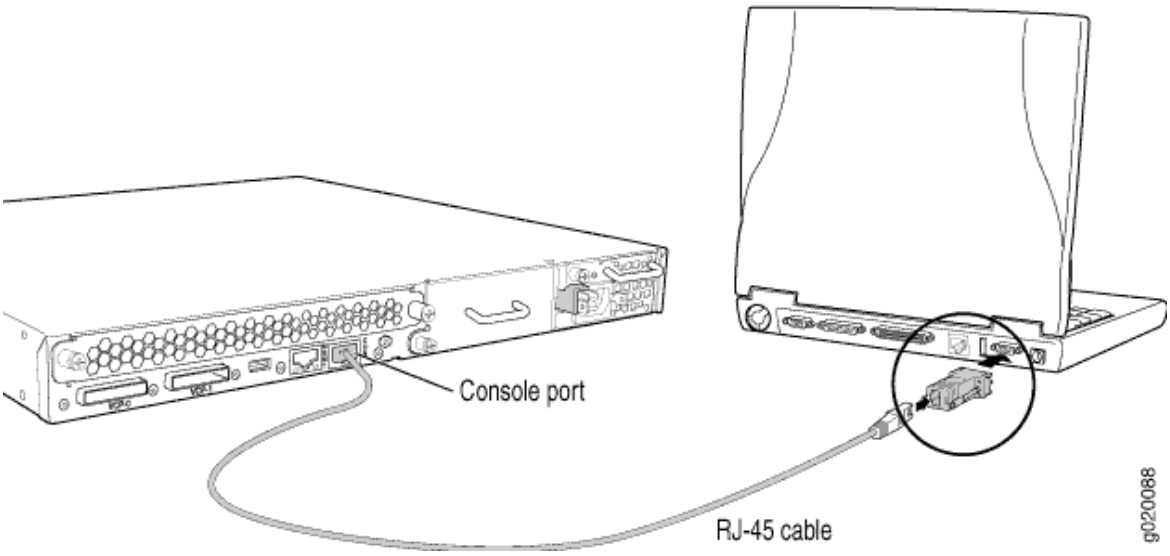
TIP: For a video on recovering the root password for routers, see "Recovering the Root Password on Routers" on page 120. The procedure is similar for switches.

Solution

To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.
2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 3 on page 127.

Figure 3: Connecting to the Console Port on the EX Series Switch



3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal). Then, select the appropriate COM port to use (for example, COM1).

4. Configure the port settings as follows:

   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt.

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 1 second...
```

NOTE: If the switch is in unattended mode for U-Boot, access to the bootstrap loader command prompt is blocked. If the root password is lost, you must reset the switch to the factory default configuration using the LCD panel.

7. At the following prompt, type `boot -s` to start up the system in single-user mode:

```
loader> boot -s
```

8. At the following prompt, type `recovery` to start the root password recovery procedure:

```
Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/
sh: recovery
```

A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:

```
user@switch> configure
```

10. Set the root password.

```
user@switch# set system root-authentication plain-text-password
```

11. At the following prompt, enter the new root password:

```
New password: password
```

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

```
Retype new password: password
```

13. After you finish configuring the device, commit the configuration.

```
root@switch# commit
commit complete
```

14. Exit configuration mode in the CLI.

```
root@switch# exit
```

15. Exit operational mode in the CLI.

```
root@switch> exit
```

16. At the prompt, enter `y` to reboot the switch.

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

Plain-Text Passwords

IN THIS SECTION

Change the Requirements for 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 (sha256 | sha512);
    maximum-length length;
    maximum-lifetime days
    minimum-changes number;
    minimum-character-changes number
    minimum-length length;
    minimum-lifetime days
    minimum-lower-cases number;
    minimum-numerics number;
    minimum-reuse number
    minimum-punctuations number;
    minimum-upper-cases number;
}
```

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

How to Change the Requirements for Plain-Text Passwords

IN THIS SECTION

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

Overview

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

Configuration

IN THIS SECTION

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

Configure the Requirements for Plain-Text Passwords

Step-by-Step Procedure

This example configures password requirements that require the user to create a password with at least 12 characters but no more than 22 characters. The password requirements also specify at least one lowercase letter and one uppercase letter, at least one punctuation character, and at least one numeric character.

1. Enter configuration mode and navigate to the `[edit system login password]` hierarchy level.

```
user@host> configure
[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 lowercase letter and at least one uppercase 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 character and at least one numeric character.

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

Results

In configuration mode, confirm your configuration by entering the `show` command at the `[edit system login password]` hierarchy level..

```
[edit system login password]
user@host# show
minimum-length 12;
```

```
maximum-length 22;
minimum-numerics 1;
minimum-upper-cases 1;
minimum-lower-cases 1;
minimum-punctuations 1;
```

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 configuration is correct, enter `commit` in configuration mode.

Master Password for Configuration Encryption

IN THIS SECTION

Use Feature Explorer to confirm platform and release support for specific features.

Junos OS and Junos OS Evolved support encryption method for configuration secrets using a master password. The master password derives an encryption key that uses AES256-GCM to protect certain secrets such as private keys, system master passwords, and other sensitive data by storing it in an AES256 encrypted format. For more information, read this topic.

NOTE: The master password is separate from the device's root password.

Hardening Shared Secrets in Junos OS

IN THIS SECTION

Understanding Hardening Shared Secrets

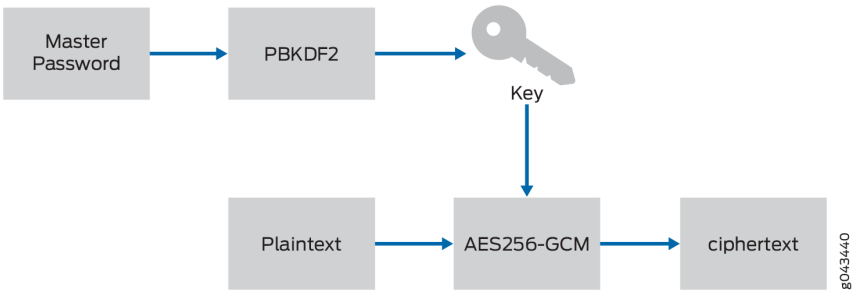
Existing shared secrets (9 format) in Junos OS currently use an obfuscation algorithm, which is not a very strong encryption for configuration secrets. If you want a strong encryption for your configuration secrets, you can configure a master password. The master password is used to derive an encryption key that is used with AES256-GCM to encrypt configuration secrets. This new encryption method uses the 8 formatted strings.

Starting with Junos OS Release 15.1X49-D50 and Junos OS Evolved Release 22.4R1, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets. The master password encrypts secrets like the RADIUS password, IKE preshared keys, and other shared secrets in the Junos OS management process (mgd) configuration. The master password itself is not saved as part of the configuration. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. the key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text). See Figure 4 on page 135

NOTE: Enabling Master Password Encryption through the Trusted Platform Module (TPM) can result in increased commit times. This is because of the encryption processing that occurs each time the configuration is committed. The increase in delay varies according to CPU capability and current loading.

Figure 4: Master Password Encryption



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

The 8-encrypted passwords have the following format:

`$8$crypt-algo$hash-algo$iterations$salt$iv$tag$encrypted`. See Table 9 on page 135 for the master password format details.

Table 9: 8-encrypted Password Format

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

The ASCII64 encoding is Base64 (RFC 4648) compatible, except no padding (character "=") is used to keep the strings short. For example: `$8$aes256-gcm$hmac-sha2-256$100$y/4YMC4YDLU$fzYDI4jjN6YCyQsYLsaf8A$Ilu4jLcZarD9YnyD /Hejww$okhBlc0cGakSqYxKww`

Chassis Cluster Considerations

When defining a chassis cluster on SRX Series Firewalls, be aware of the following restrictions:

- For SRX Series Firewalls, first configure the master password on each node, and then build the cluster. The same master password should be configured on each node.
- In chassis cluster mode, if Master Encryption Key (MEK) is set, the master password cannot be deleted but you can reset master password. You can only delete master password by zeroize the Routing Engine.

NOTE: A change in the master password would mean disruption in chassis clustering; therefore you must change the password on both nodes independently.

Using Trusted Platform Module to Bind Secrets on SRX Series Devices

IN THIS SECTION

By enabling the Trusted Platform Module (TPM) on the SRX Series Firewalls, the software layer leverages the use of the underlying TPM chip. TPM is a specialized chip that protects certain secrets at rest such as private keys, system primary passwords, and other sensitive data by storing it in an AES256 encrypted format (instead of storing sensitive data in a clear text format). The device also generates a new SHA256 hash of the configuration each time the administrator commits the configuration. This hash is verified each time the system boots up. If the configuration has been tampered with, the verification fails and the device will not continue to boot. Both the encrypted data and the hash of the configuration is protected by the TPM module using the master encryption password.

Hash validation is performed during any commit operation by performing a validation check of the configuration file against the saved hash from previous commits. In a chassis cluster system, hash is independently generated on the backup system as part of the commit process. A commit from any mode, that is, `batch-config`, `dynamic-config`, `exclusive-config`, or `private config` generates the integrity hash.

Hash is saved only for the current configuration and not for any rollback configurations. Hash is not generated during reboot or shutdown of the device.

The TPM encrypts the following secrets:

- SHA256 hash of the configuration
- device primary-password
- all key-pairs on the device

The TPM chip is enabled by default to make use of TPM functionality. You must configure master encryption password to encrypt PKI key-pairs and configuration hash.

Limitations

The following limitations and exceptions apply to the configuration file integrity feature using TPM:

- If the master encryption password is not set, data is stored unencrypted.
- The file integrity feature is not supported along with the configuration file encryption feature that uses keys saved in EEPROM. You can enable only one function at a time.
- In a chassis cluster, both nodes must have the same TPM settings. This means that both nodes in the chassis cluster must have TPM enabled, or both nodes in the chassis cluster must have TPM disabled. The chassis cluster must not have one node set to TPM enabled and the another node set to TPM disabled.

NOTE: After the Master Encryption Key (MEK) is configured and operational, downgrading to a Junos version that does not support TPM functionality is not recommended. This is because the non-TPM capable image is not able to decrypt the secrets that were encrypted by TPM after the device reboots to the non-TPM cable version.

If you must downgrade to a non-TPM capable image you must first zeroize the device. The zeroization process ensures the device does not contain any secrets and removes all the keys. After zeroization the device be downgraded to the desired non-TPM capable image.

Configuring Master Encryption Password

Before configuring master encryption password, ensure that you have configured `set system master-password plain-text-password` otherwise, certain sensitive data will not be protected by the TPM.

Set the master encryption password using the following CLI command:

```
request security tpm master-encryption-password set plain-text-password
```

You will be prompted to enter the master encryption password twice, to make sure that these passwords match. The master encryption password is validated for required password strength.

After master encryption password is set, the system proceeds to encrypt the sensitive data with the master encryption password which is encrypted by the Master Binding Key that is owned and protected by the TPM chip.

NOTE: If there is any issue with setting the master encryption password, a critical ERROR message is logged on the console and the process is terminated.

Verifying the Status of the TPM

You can use the `show security tpm status` command to verify the status of the TPM. The following information is displayed:

- TPM enabled/disabled
- TPM ownership
- TPM's Master Binding Key status (created or not created)
- master encryption password status (set or not set)

Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices. To confirm the TPM firmware version, use the `show security tpm status` command. `TPM Family` and `TPM Firmware` *`version`* output fields are introduced.

Changing the Master Encryption Password

Changing the master encryption password is done using the CLI.

To change the master encryption password, enter the following command from operational mode:

```
request security tpm master-encryption-password set plain-text-password
```

NOTE: It is recommended that no configuration changes are made while you are changing the master encryption password.

The system checks if the master encryption password is already configured. If master encryption password is configured, then you are prompted to enter the current master encryption password.

The entered master encryption password is validated against the current master encryption password to make sure these master encryption passwords match. If the validation succeeds, you will be prompted to enter the new master encryption password as plain text. You will be asked to enter the key twice to validate the password.

The system then proceeds to re-encrypt the sensitive data with the new master encryption password. You must wait for this process of re-encryption to complete before attempting to change the master encryption password again.

If for some reason, the encrypted master encryption password file is lost or corrupted, the system will not be able to decrypt the sensitive data. The system can only be recovered by re-importing the sensitive data in clear text, and re-encrypting them.

If the system is compromised, the administrator can recover the system using of the following method:

- Clear the TPM ownership in u-boot and then install the image in boot loader using TFTP or USB (if USB port is not restricted).

NOTE: If the installed software version is older than Junos OS Release 15.1X49-D110 and the master encryption password is enabled, then installation of Junos OS Release 15.1X49-D110 will fail. You must backup the configuration, certificates, key-pairs, and other secrets and use the TFTP/USB installation procedure.

Using Trusted Platform Module on MX Series Devices

IN THIS SECTION

Use Feature Explorer to confirm platform and release support for specific features.

TPM is used to protect the sensitive data such as master password of system by encryption. TPM supports to encrypt and decrypt the data using keys. To decrypt the encrypted configuration secrets, the master password must be deleted.

A master password is used to encrypt the configuration files stored in the device.

To change the master encryption password, enter the following command from operational mode:

```
request security tpm master-encryption-password set plain-text-password
```

You can prevent to delete or change the master password using `protect` option. Once the master password is protected, you need to apply `unprotect` option to delete or change the master password. Run with the following steps:

1. Configure the system master password.

```
user@host# set system master-password plain-text-password
Master password:
Repeat master password:
user@host# commit
```

2. Configure to protect the system master password from deletion.

```
user@host# protect system master-password
user@host# commit
user@host# show system
host-name device1;
kernel-replication {
    traceoptions {
        file kernel_traces.log;
        flag all;
    }
}
ports {
    console log-out-on-disconnect;
}
syslog {
    file messages {
        daemon any;
```

```
    }
}
protect: master-password {
    password-configured;
}
```

The system master password is protected. You can delete the master password by unprotecting the master password.

3. Configure to unprotect the master password by entering the right master password.

```
user@host # unprotect system master-password
Enter current master-password:
user@host # commit
host-name device1;
kernel-replication {
    traceoptions {
        file kernel_traces.log;
        flag all;
    }
}
ports {
    console log-out-on-disconnect;
}
syslog {
    file messages {
        daemon any;
    }
}
master-password {
    password-configured;
}
```

4. Once the master password is unprotected, you can delete or change the master password on the system.

```
user@host # delete system master-password
user@host # commit
user@host # show system
```

```
host-name device1;
kernel-replication {
    traceoptions {
        file kernel_traces.log;
        flag all;
    }
}
ports {
    console log-out-on-disconnect;
}
syslog {
    file messages {
        daemon any;
    }
}
```

Limitations

- If Master Encryption Key (MEK) is deleted, the data cannot be decrypted. To delete MEK, you have to zeroize the device.
- To downgrade the Routing Engine, you must zeroized the Routing Engine. Once the device is zeroized it can then be safely downgraded to the image which does not support this feature.
- In dual Routing Engine configuration, if backup Routing Engine needs to be recovered, due to MEK mismatch, GRES needs to be disabled and backup Routing Engine must be zeroized. Once backup Routine Engine comes up, configure MEK using `request security tpm master-encryption-password set plain-text-password` command on Master RE.
- In dual Routing Engine configuration, if backup Routing Engine needs to be replaced, new backup Routing Engine must be zeroized first before adding in dual Routing Engine configuration, GRES must be disabled and re-configure MEK on master RE using `request security tpm master-encryption-password set plain-text-password` command.
- When you configure OSPF, IS-IS, MACsec, BGP, and VRRP on the device and reset the master password, then there is a time (in seconds) delay for the routing/dot1x subsystem to be active.
- When you configure master password, MEK, OSPF, IS-IS, MACsec, BGP, and VRRP on the device and reboot the device, then there is a time (in seconds) delay for the routing/dot1x subsystem to be active.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.4R1	Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices. To confirm the TPM firmware version, use the `show security tpm status` command. `TPM Family` and `TPM Firmware` *`version`* output fields are introduced.
15.1X49-D50	Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets.

RELATED DOCUMENTATION

master-password

Root Password | 114

Plain-Text Passwords | 129

4

CHAPTER

Trusted Platform Module

IN THIS CHAPTER

Trusted Platform Module Overview and Functions

SUMMARY

Trusted Platform Module (TPM) is a chip, unique to your device, encrypts and securely stores data on the disk, enhancing protection against unauthorized access.

IN THIS SECTION

Understand Trusted Platform Module

SUMMARY

Trusted Platform Module (TPM) is a chip used for the identification and authentication of a device on the network and to ensure the software loaded on the system is in the correct state when it started up. Each TPM chip is unique to a particular device.

IN THIS SECTION

Use Feature Explorer to confirm platform and release support for specific features.

You can safeguard sensitive data (such as private keys, certificates, and configuration files) stored in the file systems using the TPM, thereby reinforcing the integrity and confidentiality of your device's operations.

Using TPM on the device, the hard disk drive cannot be connected and accessed outside to another device.

TPM is used to secure the device hardware through integrated cryptographic keys and to store the device identity (DevID) information. A TPM certificate securely proves a device's identity. Applications (Secure Zero Touch Provisioning (SZTP) and advanced anti-malware (AAMWD) must use it when secure device identity is required.

Table 10: Supported Features using TPM

TPM Version	Supported Features
TPM 1.2	• Using Master Password for Encryption of Files. • Remote Integrity Verification
TPM 2.0	• DevID for sZTP and AAMWD • File system Encryption

Benefits of TPM

- Enhances your device's security protections at the hardware level to prevent attacks.
- Compliance with TPM 2.0 contributing to the overall security.

Security Functions of TPM

- Data Encryption: To generate, store, and limit the use of cryptographic keys.
- Secure Boot Process: To verify that the device is booting from a trusted set of hardware and software.
- Secure Key Storage: To store private keys and sensitive data to prevent theft and modification.
- Device Identity and Authentication: To identify and authenticate the device using the cryptographic Device ID.

SEE ALSO

Master Password for Configuration Encryption | 133

No Link Title

File-System Encryption with Trusted Platform Module (TPM)

No Link Title

Download And Run the Juniper ATP Cloud Script

Enroll an SRX Series Firewall Using the CLI

File System Encryption with Trusted Platform Module

IN THIS SECTION

Encryption protects sensitive information stored in private keys, configuration files, logs, and system-generated files on disk drive file systems.

Encryption also prevents unauthorized access to data stored in files on a disk or disk volume.

File system encryption is supported on devices for bulk encryption of file names, folder names, file contents, and other meta-data that operates on an entire volume. In this method, the data is automatically encrypted when written to disk and decrypted when read from it. The encryption key is enclosed to the Trusted Platform Module (TPM) 2.0 device. The files are accessible immediately after the encryption key is provided. The data stored on the encrypted file system is read using the encryption keys.

Use Feature Explorer to confirm platform and release support for specific features.

Benefits of File System Encryption

- Prevents revealing of confidential information from offline attacks.
- Provides data destruction for secure data erasure by destroying the cryptographic keys.
- All files are automatically encrypted, by default without any user action.

SEE ALSO

request system file-system encryption enable

request system file-system encryption keys

show-system-file-system-encryption-status

Remote Integrity Verification

IN THIS SECTION

One of the features of the Trusted Platform Module (TPM) is to measure various software components during device boot. The data is stored as a cryptographic hash in the TPM's Platform Configuration Registers (PCR). You can use PCR as proof of the integrity of the devices software version. The chip includes multiple physical security mechanisms to make it tamper resistant and the malicious software cannot tamper the security functions of the TPM.

Remote Integrity Verification (RIV) defines a set of protocols and procedures to determine whether a particular device is launched with an untampered software version. The roles involved in the RIV process are Attester and Verifier.

The Attester provides evidence of identity and software state to the Verifier on demand. The Verifier verifies the evidence and makes a judgment about the integrity of the software image running on the Attester.

Benefits

- Provides the integrity of the host platform and ensures that the host platform is not hacked.
- Provides restricted access to the stored secrets (keys).
- Stores data that is not secret such as public keys used for platform identity. You cannot change the public keys without authorization.
- Creates and manages a TPM key used to sign the evidence

SEE ALSO

request-system-integrity-attestation

request-system-integrity-log-retrieval

5

CHAPTER

User Authentication

IN THIS CHAPTER

User Authentication Overview

IN THIS SECTION

Junos OS supports different authentication methods that you (the network administrator) use to control user access to the network. These methods include local password authentication, RADIUS, and TACACS+. You use one of these authentication methods to validate users and devices that attempt to access the router or switch using SSH and Telnet. Authentication prevents unauthorized devices and users from gaining access to your LAN.

User Authentication Methods

Junos OS supports three methods of user authentication: local password authentication, RADIUS and 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 any of the login methods. They are 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 a RADIUS, or TACACS+ client, or a combination. 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.

Configure Local User Template Accounts for User Authentication

You use local user template accounts to assign different login classes, and thus grant different permissions, to users who are authenticated through a remote authentication server. Each template can define a different set of permissions appropriate for the users assigned to that template. You define the templates locally on the router or switch, and the TACACS+ and RADIUS authentication servers reference the templates. When an authenticated user is assigned to a template account, the CLI username is the login name, but the user inherits privileges, file ownership, and effective user ID from the template account.

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 the user is authenticated, the server returns the local username to Junos OS (`local-user-name` for TACACS+, and `Juniper-Local-User-Name` for RADIUS). Junos OS then determines whether a local username is specified for that login name, and if so, Junos OS assigns the user to that local user template. If a local user template does not exist for the authenticated user, the router or switch defaults to the `remote` template, if configured.

To configure a local user template, define the template username at the `[edit system login]` hierarchy level. Assign a class to 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;
}
```

To assign a user to the local user template, configure the remote authentication server with the appropriate parameter (`local-user-name` for TACACS+, and `Juniper-Local-User-Name` for RADIUS), and specify the username defined for the local user template. To configure different access privileges for users who share the local user template account, you can use vendor-specific attributes in the authentication server configuration file to allow or deny specific commands and configuration hierarchies for a user.

This example configures the `sales` and `engineering` user templates on the local device. The TACACS+ server configuration file then assigns users to specific templates.

```
[edit]
system {
    login {
        user sales {
            uid 6003;
```

```
            class sales-class;
        }
        user engineering {
            uid 6004;
            class super-user;
        }
    }
}
```

When the 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.

```
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"
    }
}
```

Configure Remote User Template Accounts for User Authentication

The network device can map remotely-authenticated users to a locally defined user account or user template account, which determines authorization. The `remote` template account is a special user template. By default, Junos OS assigns remotely-authenticated users to the `remote` template account, if configured, when:

- The authenticated user does not have a user account configured on the local device.
- The remote authentication server either does not assign the user to a local user template, or the template that the server assigns is not configured on the local device.

To configure the `remote` template account, include the `user remote` statement at the `[edit system login]` hierarchy level, and specify the login class for users assigned to the `remote` template:

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

To configure different access privileges for users who share the `remote` template account, you can use vendor-specific attributes in the authentication server configuration file to allow or deny specific commands and configuration hierarchies for a user.

Example: Create Template Accounts

IN THIS SECTION

This example shows how to create template accounts.

Requirements

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

Overview

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

By default, Junos OS assigns remotely-authenticated users to the `remote` template account when:

- The authenticated user does not have a user account configured on the local device.
- The remote authentication server either does not assign the user to a local user template, or the template that the server assigns is not configured on the local device.

In this example, you create the `remote` template account and set the username to `remote` and the login class for the user as `operator`. The device assigns the `remote` template to users who are authenticated by RADIUS, or TACACS+ but who do not have a local user account or belong to a different local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need to assign remotely authenticated users to different login classes. Thus, each template can grant a different set of permissions appropriate for the users assigned to that user template.

Configuration

IN THIS SECTION

Create a Remote Template Account

Step-by-Step Procedure

To create the `remote` template account:

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

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

Results

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

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

After you configure the device, enter `commit` in configuration mode.

Create a Local Template Account

Step-by-Step Procedure

To create a local template account:

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

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

Results

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

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

After you configure the device, enter `commit` in configuration mode.

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

- Configure a RADIUS server. See "Example: Configure a RADIUS Server for System Authentication" on page 183.
- Configure a TACACS+ server. See "Example: Configure a TACACS+ Server for System Authentication" on page 216.
- Configure system authentication order. See "Example: Configure Authentication Order" on page 166.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify the Template Accounts Creation

Purpose

Verify that the template accounts have been created.

Action

In operational mode, enter the `show system login` command.

What Are Remote Authentication Servers?

You probably already use a remote authentication server (or servers) in your network. Using these servers is a best practice, because they allow you to create a consistent set of user accounts centrally for all devices in your network. Managing user accounts is much easier when you use remote authentication servers to implement an authentication, authorization, and accountability (AAA) solution in your network.

Most enterprises use one of two basic remote authentication methods: RADIUS, and TACACS+. Junos OS supports both methods, and you can configure Junos OS to query any type of remote authentication server. The idea behind a RADIUS, or TACACS+ server is simple: Each acts as a central authentication server that routers, switches, security devices, and servers can use to authenticate users as they attempt to access these systems. Think of the advantages that a central user directory offers for authentication auditing and access control in a client/server model. The RADIUS and TACACS+ authentication methods offer comparable advantages for your network 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 such attacks, someone can use 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 than TACACS+. 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 anyone from trying to force their way into your network.
- Flexibility—Transmission Control Protocol (TCP) is a more flexible transport protocol than UDP. You can do more with TCP in more advanced networks. In addition, TACACS+ supports more of the enterprise protocols, such as NetBIOS.

Authentication Order for RADIUS TACACS+, and Local Password

IN THIS SECTION

Junos OS supports different authentication methods, including local password authentication, RADIUS, and TACACS+, to control access to the network.

When you configure a device to support multiple authentication methods, you can prioritize the order in which the device tries the different methods. This topic discusses how the authentication order works and how to configure it on a device.

Authentication Order Overview

IN THIS SECTION

You (the network administrator) can configure the `authentication-order` statement to prioritize the order in which Junos OS tries different authentication methods to verify user access to a router or switch. If you do not set an authentication order, by default, Junos OS verifies users based on their configured local passwords.

If the authentication order includes RADIUS or TACACS+ servers, but the servers do not respond to a request, Junos OS always defaults to trying local password authentication as a last resort.

If the authentication order includes RADIUS or TACACS+ servers, but the servers reject the request, the handling of the request is more complicated.

- If `password` (local password authentication) *is* included at the end of the authentication order and the remote authentication servers reject the authentication request, the device attempts local password authentication.
- If `password` (local password authentication) is *not* included in the authentication order and the remote authentication servers reject the authentication request, the request ends with the rejection.

Thus, the device must include `password` as a final authentication order option for the device to attempt local password authentication in the event that the remote authentication servers reject the request.

If the authentication order is set to `authentication-order password`, then the device uses only local password authentication.

Using Remote Authentication

You can configure Junos OS to be a RADIUS or TACACS+ authentication client (or a combination).

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

The RADIUS, or TACACS+ server authentication might fail for one or more 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 authentication server does not respond before the configured timeout value for that server, or before the default timeout, if no timeout is configured.
- The authentication server is not reachable because of a network problem.

The authentication server might return a reject response for one or both of the following reasons:

- The user profile of a user accessing a router or switch is not configured on the authentication server.
- The user enters incorrect logon credentials.

How to Use Local Password Authentication

You can explicitly configure the `password` authentication method in the `authentication-order` statement 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` statement.

  In this case, the device tries local password authentication if no previous authentication method accepts the logon credentials. This is true whether the previous authentication methods fail to respond or they return 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` statement.

  In this case, the operating system only tries local password authentication if all configured authentication methods fail to respond. The operating system does not use local password authentication if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

Table 11 on page 161 describes how the `authentication-order` statement at the `[edit system]` hierarchy level determines the procedure that Junos OS uses to authenticate users for access to a device.

Table 11: Order of Authentication Attempts

Syntax	Order of Authentication Attempts
`authentication-order radius;`	1. Try configured RADIUS authentication servers. 2. If a RADIUS server is available and authentication is accepted, grant access. 3. If a RADIUS server is available but authentication is rejected, deny access. 4. If no RADIUS servers are available, try local password authentication.
`authentication-order [ radius password ];`	1. Try configured RADIUS authentication servers. 2. If a RADIUS server is available and authentication is accepted, grant access. 3. If the RADIUS servers fail to respond or the servers return a reject response, try local password authentication, because it is explicitly configured in the authentication order.
`authentication-order [ radius tacplus ];`	1. Try configured RADIUS authentication servers. 2. If a RADIUS server is available and authentication is accepted, grant access. 3. If the RADIUS servers fail to respond or the servers return a reject response, try configured TACACS+ servers. 4. If a TACACS+ server is available and authentication is accepted, grant access. 5. If a TACACS+ server is available but authentication is rejected, deny access.

Table 11: Order of Authentication Attempts *(Continued)*

Syntax	Order of Authentication Attempts
`authentication-order [ radius tacplus password ];`	1. Try configured RADIUS authentication servers. 2. If a RADIUS server is available and authentication is accepted, grant access. 3. If the RADIUS servers fail to respond or the servers return a reject response, try configured TACACS+ servers. 4. If a TACACS+ server is available and authentication is accepted, grant access. 5. If the TACACS+ servers fail to respond or the servers return a reject response, try local password authentication, because it is explicitly configured in the authentication order.
`authentication-order tacplus;`	1. Try configured TACACS+ authentication servers. 2. If a TACACS+ server is available and authentication is accepted, grant access. 3. If a TACACS+ server is available but authentication is rejected, deny access. 4. If no TACACS+ servers are available, try local password authentication.
`authentication-order [ tacplus password ];`	1. Try configured TACACS+ authentication servers. 2. If a TACACS+ server is available and authentication is accepted, grant access. 3. If the TACACS+ servers fail to respond or the servers return a reject response, try local password authentication, because it is explicitly configured in the authentication order.

Table 11: Order of Authentication Attempts *(Continued)*

Syntax	Order of Authentication Attempts
`authentication-order [ tacplus radius ];`	1. Try configured TACACS+ authentication servers. 2. If a TACACS+ server is available and authentication is accepted, grant access. 3. If the TACACS+ servers fail to respond or the servers return a reject response, try configured RADIUS servers. 4. If a RADIUS server is available and authentication is accepted, grant access. 5. If a RADIUS server is available but authentication is rejected, deny access. 6. If no TACACS+ or RADIUS servers are available, try local password authentication.
`authentication-order password;`	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.

Configure the Authentication Order for RADIUS, TACACS+ and Local Password Authentication

Using the `authentication-order` statement, you can prioritize the order in which Junos OS tries the different authentication methods when verifying user access to a router or switch. If you do not set an authentication order, by default, users are verified based on their locally configured passwords.

When configuring a password using plain text and relying on Junos OS to encrypt it, you are still sending the password over the Internet in plain text. Using pre-encrypted passwords is more secure because it means that the plain text of the password never has to be sent over the internet. Also, with passwords, only one user can be assigned to a password at a time.

On the other hand, RADIUS, and TACACS+ encrypt passwords. These authentication methods let you assign a set of users at a time instead of assigning users one by one. But here are how these authentication systems differ:

- RADIUS uses UDP; TACACS+ uses TCP.
- RADIUS encrypts only the password during transmission, whereas TACACS+ encrypts the entire session.
- RADIUS combine authentication (device) and authorization (user), whereas TACACS+ separates authentication, authorization, and accountability.

In short, TACACS+ is more secure than RADIUS. However, RADIUS has better performance and is more interoperable. RADIUS is widely supported, whereas TACACS+ is a Cisco proprietary product and not widely supported outside of Cisco.

You can configure the authentication order based on your system, its restrictions, and your IT policy and operational preferences.

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

```
[edit system]
user@host# set authentication-order [authentication-methods ]
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The following are the possible authentication order entry options:

- `radius`—Verify the user using RADIUS authentication servers.
- `tacplus`—Verify the user using TACACS+ authentication servers.

- password—Verify the user using the username and password configured locally in the authentication statement at the [edit system login user] hierarchy level.

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

For example, assume that you configure three RADIUS servers so that the router or switch attempts to contact each server three times. Assume further that, with each retry, the server times out after 3 seconds. In this scenario, 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.

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 authentication fails, the authentication sequence is reinitiated by the router or switch until authentication succeeds and the link is established. However, if the RADIUS servers are unavailable and additional authentication methods such as tacplus or password are also configured, the next authentication method is tried.

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

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

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

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

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

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

Example: Configure Authentication Order

IN THIS SECTION

This example shows how to configure authentication order for user login.

Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication method order that a device uses to verify user access to the device. For each login attempt, the device tries the authentication methods in the order configured, until the password matches or all authentication methods have been tried. If you do not configure remote authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with RADIUS authentication services first, then with TACACS+ authentication services, and finally with local password 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 use remote authentication servers, you can create template accounts (for authorization purposes) that a set of users shares. When a user is assigned to a template account, the command-line interface (CLI) username is the login name; however, the user inherits the privileges, file ownership, and effective user ID from the template account.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
delete system authentication-order
set system authentication-order radius
insert system authentication-order tacplus after radius
insert system authentication-order password after tacplus
```

GUI Quick Configuration

Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select `Configure>System Properties>User Management`.
2. Click `Edit`. The Edit User Management dialog box appears.
3. Select the `Authentication Method and Order` tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users. Use the arrow button to move the item to the Selected Methods list. Available methods include:

   - RADIUS
   - TACACS+
   - Local Password

   If you want to use multiple methods to authenticate users, repeat this step to add the other methods to the Selected Methods list.
5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
6. Click `OK` to check your configuration and save it as a candidate configuration.
7. After you configure the device, click `Commit Options>Commit`.

Step-by-Step Procedure

To configure authentication order:

1. Delete any existing `authentication-order` statement.

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

2. Add RADIUS authentication to the authentication order.

```
[edit]
user@host# set system authentication-order radius
```

3. Add TACACS+ authentication to the authentication order.

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

4. Add local password authentication to the authentication order.

```
[edit]
user@host# insert system authentication-order password after tacplus
```

Results

In configuration mode, confirm your configuration by entering the `show system authentication-order` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system authentication-order
authentication-order [ radius tacplus password ];
```

After you configure the device, enter `commit` in configuration mode.

NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS, or TACACS+ server and create user accounts or user template accounts.

- Configure a RADIUS server. See "Example: Configure a RADIUS Server for System Authentication" on page 183.
- Configure a TACACS+ server. See "Example: Configure a TACACS+ Server for System Authentication" on page 216.
- Configure a user. See "Example: Configure New User Accounts" on page 31.
- Configure template accounts. See "Example: Create Template Accounts" on page 153.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify the Authentication Order Configuration

Purpose

Verify that the device uses the authentication methods in the order configured.

Action

Create a test user that has a different password for each authentication method. Log in to the device using the different passwords. Verify that the device queries subsequent authentication methods when the previous methods reject the password or fail to respond.

Alternatively, in a test environment, you can deactivate the authentication server configuration or the local user account configuration (or both) to test each authentication method. For example, to test the TACACS+ server, you can deactivate the RADIUS server configuration and the user's local account. However, if you deactivate the user's local account, you must ensure that the user still maps to a local user template account such as the `remote` user template.

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

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication on a device running Junos OS.

In this example, only the user Philip and users authenticated by a 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 "Authentication Order Overview" on page 158.

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 a set of users can share 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 "Example: Configure Authentication Order" on page 166.

When a user logs in to a device, the RADIUS or TACACS+ server uses the user's login name for authentication. If the authentication server authenticates the user successfully and the user is not configured at the `[edit system login user]` hierarchy level, this is the result: 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 lack 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 that 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 of having a unique, local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override and therefore shares access with all the other remote users, getting read-only access.

RADIUS Authentication

IN THIS SECTION

Junos OS supports RADIUS for central authentication of users on network devices. To use RADIUS authentication on the device, you (the network administrator) must configure information about one or more RADIUS servers on the network. You can also configure RADIUS accounting on the device to collect statistical data about the users logging in to or out of a LAN and send the data to a RADIUS accounting server.

Configure RADIUS Server Authentication

IN THIS SECTION

RADIUS authentication is a method of authenticating users who attempt to access a network device. The following sections describe why you would use RADIUS and how to configure it.

Why Use RADIUS

You (the network administrator) can use different protocols for the central authentication of users on network devices including 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.

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. For this reason, network engineers generally prefer RADIUS over TACACS+.

Configure RADIUS Server Details

To use RADIUS authentication on the device, configure information about one or more RADIUS servers on the network by including one `radius-server` statement at the `[edit system]` hierarchy level for each RADIUS server. The device queries the RADIUS servers in the order in which they are configured. If the primary server (the first one configured) is unavailable, the device attempts to contact each server in the list until it receives a response.

The network device can map RADIUS-authenticated users to a locally defined user account or user template account, which determines authorization. By default, Junos OS assigns RADIUS-authenticated users to the user template account `remote`, if configured, when:

- The authenticated user does not have a user account configured on the local device.
- The RADIUS server either does not assign the user to a local user template, or the template that the server assigns is not configured on the local device.

The RADIUS server can assign an authenticated user to a different user template to grant different administrative permissions to that user. The user retains the same login name in the CLI but inherits the login class, access privileges, and effective user ID from the assigned template. If the RADIUS-

authenticated user does not map to any locally defined user account or user template, and the `remote` template is not configured, then authentication fails.

NOTE: The `remote` username is a special case in Junos OS and must always be lowercase. 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. 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 in the same login class.

Because you configure remote authentication on multiple devices, it is common to configure it inside of a configuration group. The steps shown here are in a configuration group called `global`. Using a configuration group is optional.

To configure authentication by a RADIUS server:

1. Configure the IPv4 address or the IPv6 address of the RADIUS authentication server.

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

For example:

```
[edit groups global system radius-server]
user@host# set 192.168.17.28
```

```
[edit groups global system radius-server]
user@host# set 2001:db8:0:f101::8
```

2. (Optional) Configure the packet source address for requests sent to the RADIUS server.

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

For example:

```
[edit groups global system radius-server 192.168.17.28]
user@host# set source-address 192.168.17.1
```

```
[edit groups global system radius-server 2001:db8:0:f101::8]
user@host# set source-address 2001:db8:0:f101::1
```

The source address is a valid IPv4 address or IPv6 address configured on one of the router interfaces or switch interfaces. If the network device has several interfaces that can reach the RADIUS server, assign an IP address that the device can use for all its communication with the RADIUS server. Doing this sets a fixed address as the source address for locally generated IP packets.

3. Configure the shared secret password that the network device uses to authenticate with the RADIUS server.

   The configured password must match the password that is configured on the RADIUS server. If the password contains spaces, enclose it in quotation marks. The device stores the password as an encrypted value in the configuration database.

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

For example:

```
[edit groups global system radius-server 192.168.17.28]
user@host# set secret Radiussecret1
```

4. (Optional) Specify the port on which to contact the RADIUS server, if different from the default.

   The default port is 1812 (as specified in RFC 2865).

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

For example:

```
[edit groups global system radius-server 192.168.17.28]
user@host# set port 51812
```

NOTE: You can also configure the `accounting-port` statement to specify to which RADIUS server port to send accounting packets. The default is 1813 (as specified in RFC 2866).

5. (Optional) Configure the number of times that the device attempts to contact the RADIUS server and the amount of time that the device waits to receive a response from the server.

   By default, the device attempts to contact the server three times and waits three seconds. You can configure the `retry` value from 1 through 100 times and the `timeout` value from 1 through 1000 seconds.

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

   For example, to contact a RADIUS server 2 times and wait 10 seconds for a response:

   ```
   [edit groups global system radius-server 192.168.17.28]
   user@host# set retry 2
   user@host# set timeout 10
   ```

6. Specify the authentication order, and include the `radius` option.

   ```
   [edit groups global system]
   user@host# set authentication-order [ authentication-methods ]
   ```

   In the following example, whenever a user attempts to log in, Junos OS first queries the RADIUS server for authentication. If that fails, it queries the TACACS+ server. If that fails, it attempts authentication with locally configured user accounts.

   ```
   [edit groups global system]
   user@host# set authentication-order [ radius tacplus password ]
   ```

7. Assign a login class to RADIUS-authenticated users who do not have a locally defined user account.

   You configure a user template account in the same way as a local user account, except that you do not configure a local authentication password because the RADIUS server authenticates the user.

- To use the same permissions for all RADIUS-authenticated users, configure the `remote` user template.

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

For example:

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

- To use different login classes for different RADIUS-authenticated users, granting them different permissions:

a. Create multiple user templates in the Junos OS configuration. For example:

```
[edit groups global system login]
user@host# set user RO class read-only
user@host# set user OP class operator
user@host# set user SU class super-user
user@host# set user remote full-name "default remote access user template"
user@host# set user remote class read-only
```

b. Configure the RADIUS server to map the authenticated user to the appropriate user template.

Set the Juniper-Local-User-Name Juniper VSA (vendor-specific attribute) (Vendor 2636, type 1, string) to the name of a user template configured on the device, which in the previous example is RO, OP, or SU. The RADIUS server includes the attribute in the RADIUS Access-Accept message. Authentication fails if the device cannot assign a user to a local user account or user template, and the `remote` user template is not configured.

Configure RADIUS over TLS (RADSEC) for System Authentication

RADIUS over TLS (RADSEC) provides secure, encrypted communication between the Junos device and RADIUS servers for system authentication and accounting. The system uses OpenSSL APIs to establish SSL/TLS sessions and perform certificate validation.

IMPORTANT: This configuration applies to system-level authentication (administrative access) under the `system` hierarchy. For RADSEC configuration for network access control, configure RADSEC under the `access` hierarchy.

RADSEC secures administrative authentication traffic using TLS encryption on TCP port 2083 (instead of UDP ports 1812/1813). RADSEC supports two authentication modes:

- **One-way TLS:** Client verifies the server's certificate using trusted CA certificates.
- **Mutual TLS (mTLS):** Both client and server authenticate each other using certificates.

Before You Begin:

Ensure the following:

- CA certificates are available for server validation
- Client certificates are available (required only for mutual authentication)

Configure CA Certificates:

You can copy the file and rename it to subject <hash>.0 under `/var/tmp/certs/<trusted-ca-group>/`. Alternatively, you can also create a symbolic link with the subject <hash>.0 under `/var/tmp/certs/<trusted-ca-group>` and link this to the actual certificate file.

1. Generate the subject name hash:

```
openssl x509 -in <CA-file-name> -noout -subject_hash
```

2. Create a symbolic link:

```
ln -s <CA-file-name> <hash>.0
```

NOTE: If there are more than one CA files with the same subject name hash value, their extensions should be different; for example, 'e5d93f80.1' and so on. The search gets performed as to how the extension numbers are ordered accordingly.

Example:

```
cd /var/tmp/certs/grp1/
openssl x509 -in root-ca.crt -noout -subject_hash
ln -s root-ca.crt e5d93f80.0
```

Configure Client Certificates (Mutual Authentication Only):

For mutual authentication, place client certificate and private key in `/var/tmp/certs/<certificate-id>/`.

The folder must contain:

- `client.crt` - Client certificate file
- `client.key` - Client private key file

Example:

```
mkdir -p /var/tmp/certs/ca1/
cp client.crt /var/tmp/certs/ca1/
cp client.key /var/tmp/certs/ca1/
```

To configure RADSEC for system authentication:

1. Configure the RADIUS authentication server with TLS support.

   For one-way TLS (server-only authentication):

   ```
   [edit system]
   user@host# set radius-server <server-ip> port <port> tls trusted-ca-group <trusted-ca-group>
   user@host# set radius-server <server-ip> secret <password>
   ```

   For mutual TLS (two-way authentication):

   ```
   [edit system]
   user@host# set radius-server <server-ip> port <port> tls trusted-ca-group <trusted-ca-group>
   mutual-authentication certificate-id <certificate-id>
   user@host# set radius-server <server-ip> secret <password>
   ```

Example:

```
[edit system]
user@host# set radius-server 1.1.1.1 port 2083 tls trusted-ca-group grp1 mutual-
authentication certificate-id ca1
user@host# set radius-server 1.1.1.1 secret Radiussecret1
```

2. (Optional) Configure the RADIUS accounting server with TLS support.

   For one-way TLS:

```
[edit system accounting destination radius]
user@host# set server <server-ip> accounting-port <port> tls trusted-ca-group <trusted-ca-
group>
user@host# set server <server-ip> secret <password>
```

   For mutual TLS:

```
[edit system accounting destination radius]
user@host# set server <server-ip> accounting-port <port> tls trusted-ca-group <trusted-ca-
group> mutual-authentication certificate-id <certificate-id>
user@host# set server <server-ip> secret <password>
```

   Example:

```
[edit system accounting destination radius]
user@host# set server 1.1.1.1 accounting-port 2083 tls trusted-ca-group grp1 mutual-
authentication certificate-id ca1
user@host# set server 1.1.1.1 secret Radiussecret1
```

3. Configure the authentication order.

```
[edit system]
user@host# set authentication-order [ radius password ]
```

4. Configure the remote user template.

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

5. Verify the configuration.

```
[edit]
user@host# show system radius-server
user@host# show system accounting destination radius
```

6. Commit the configuration.

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

The following example shows a complete RADSEC configuration with mutual authentication:

```
[edit]
            user@host# show system
            login {
            user remote {
            class operator;
            }
            }
            authentication-order [ radius password ];
            radius-server {
            1.1.1.1 {
            port 2083;
            tls {
            trusted-ca-group grp1;
            mutual-authentication {
            certificate-id ca1;
            }
            }
            secret "$9$ABC123"; ## SECRET-DATA
            }
            }
            accounting {
            destination {
            radius {
            server {
            1.1.1.1 {
            accounting-port 2083;
            tls {
            trusted-ca-group grp1;
```

```
            mutual-authentication {
            certificate-id ca1;
            }
            }
            secret "$9$ABC123"; ## SECRET-DATA
            }
            }
            }
            }
            }
```

Verification:

Log in to the network device and verify successful authentication. To confirm RADSEC is working, attempt login with an account that does not have a local password configured.

Configuration Parameters:

- `trusted-ca-group`—Trusted CA group name corresponding to the folder containing CA certificates under `/var/tmp/certs/`. OpenSSL uses these CA certificates to validate the RADIUS server's certificate.
- `certificate-id`—Certificate identifier corresponding to the folder containing the client certificate and private key under `/var/tmp/certs/`. Required for mutual authentication.

Configure RADIUS to Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for RADIUS through the default routing instance. You can also route RADIUS packets through a management interface in a non-default VRF instance.

To route RADIUS packets through the `mgmt_junos` management instance:

1. Enable the `mgmt_junos` management instance.

```
[edit system]
user@host# set management-instance
```

2. Configure the `routing-instance mgmt_junos` statement for the RADIUS authentication server and the RADIUS accounting server, if configured.

```
[edit system]
user@host# set radius-server server-address routing-instance mgmt_junos
user@host# set accounting destination radius server server-address routing-instance mgmt_junos
```

Example: Configure a RADIUS Server for System Authentication

IN THIS SECTION

This example configures system authentication through a RADIUS server.

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Set up at least one RADIUS server on your network.

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1. You specify the shared secret password of the RADIUS server as Radiussecret1. The device stores the secret in the configuration database as an encrypted value. Finally, you specify the source address that the device uses in RADIUS server requests. In most cases, you can use the loopback address of the device, which in this example is 10.0.0.1.

You can configure support for multiple user authentication methods, such as local password authentication, RADIUS, and TACACS+, on the network device, When you configure multiple authentication methods, you can prioritize the order in which the device tries the different methods. In this example, you configure the device to use RADIUS authentication services first and then, if that fails, to attempt local password authentication.

A RADIUS-authenticated user must map to a local user account or a local user template account on the network device, which determines authorization. By default, if a RADIUS-authenticated user does not map to a local user account or a specific user template, the user is assigned to the `remote` user template, if configured. This example configures the `remote` user template.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set system radius-server 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
set system authentication-order [radius password]
set system login user remote class operator
```

Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.

```
[edit system]
user@host# set radius-server 172.16.98.1
```

2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```

3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

4. Specify the device's order of authentication, and include the `radius` option.

```
[edit system]
user@host# set authentication-order [radius password]
```

5. Configure the `remote` user template and its login class.

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

Results

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

The following output includes only those portions of the configuration hierarchy that are relevant to this example.

```
[edit]
user@host# show system
login {
    user remote {
        class operator;
    }
}
authentication-order [ radius password ];
radius-server {
    172.16.98.1 {
        secret "$9$ABC123"; ## SECRET-DATA
        source-address 10.0.0.1;
    }
}
```

After configuring the device, enter `commit` in configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify the RADIUS Server Configuration

Purpose

Verify that the RADIUS server authenticates users.

Action

Log in to the network device, and verify that the login is successful. To verify that the device uses the RADIUS server for authentication, you can attempt to log in with an account that does not define a local authentication password in the configuration.

Configure RADIUS Authentication (QFX Series or OCX Series)

IN THIS SECTION

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

NOTE: The `source-address` statement is not supported at `[edit system-radius-server name]` hierarchy level on the QFabric system.

Configure RADIUS Server Details

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:

```
[edit system]
radius-server server-address {
    accounting-port port-number;
    accounting-retry number;
    accounting-timeout seconds;
    dynamic-request-port number;
    max-outstanding-requests value;
    port number;
    preauthentication-port number;
    preauthentication-secret secret;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-addresssource-address;
    timeout seconds;
}
```

server-address is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is 1813 (as specified in RFC 2866).

You must specify a password in the `secret` *password* statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can 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 three times. You can configure this to be a value from 1 through 10 times.

You can use the source-address statement to specify a logical address for individual servers or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple radius-server statements.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in "Example: Configure Authentication Order" on page 166.

You can also configure RADIUS authentication at the [edit access] and [edit access profile] hierarchy levels. Junos OS uses the following search order to determine which set of servers is used for authentication:

1. [edit access profile *profile-name* radius-server *server-address*]
2. [edit access radius-server *server-address*]
3. [edit system radius-server *server-address*]

Configure MS-CHAPv2 for Password-Change Support

Before you configure MS-CHAPv2 for password-change support, ensure that you:

- Configure the RADIUS server authentication parameters.
- Set the **authentication-order** to use the RADIUS server for the initial password attempt.

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 the next login.

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 "$ABC123"; ## SECRET-DATA
    }
    radius-options {
        password-protocol mschap-v2;
    }
    login {
        user bob {
            class operator;
        }
    }
}
```

Specify a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the `source-address` statement at the `[edit system radius-server` *`server-address`*`]` hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

source-address is a valid IP address configured on one of the router interfaces or switch interfaces.

RELATED DOCUMENTATION

- Juniper Networks Vendor-Specific RADIUS Attributes | **189**
- Example: Configure Authentication Order | **166**
- Use Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Commands | **223**
- User Authentication Methods | **150**

Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports configuring Juniper Networks RADIUS vendor-specific attributes (VSAs) on the authentication server. These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636.

Table 12 on page 190 lists the Juniper Networks VSAs that you can configure.

Some of the attributes accept extended regular expressions, as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. For more information, see:

- "Regular Expressions to Allow and Deny Operational Mode Commands, Configuration Statements, and Hierarchies" on page 63
- "Use Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Commands" on page 223

Table 12: Juniper Networks Vendor-Specific RADIUS Attributes

Name	Description	Type	Length	String
Juniper-Local-User-Name	Indicates the name of the user template assigned to this user when the user logs 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 commands in addition to those 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.
Juniper-Deny-Commands	Contains an extended regular expression that denies the user permission to run 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.

Table 12: Juniper Networks Vendor-Specific RADIUS Attributes *(Continued)*

Name	Description	Type	Length	String
Juniper-Allow-Configuration	Contains an extended regular expression that enables the user to view and modify configuration statements in addition to those statements 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.
Juniper-Deny-Configuration	Contains an extended regular expression that denies the user permission to view or modify configuration statements 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.
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.

Table 12: Juniper Networks Vendor-Specific RADIUS Attributes *(Continued)*

Name	Description	Type	Length	String
Juniper-User-Permissions	Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. **NOTE**: When the RADIUS server defines the `Juniper-User-Permissions` attribute to grant the `maintenance` permission or `all` permission to a user, the user's list of group memberships does not automatically include the UNIX wheel group. Some operations such as running the `su root` command from a local shell require wheel group membership permissions. However, when the network device defines a local user account with the permissions `maintenance` or `all`, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a user template account with the required permissions and associate individual user accounts with the user template account.	10	≥3	One or more octets containing printable ASCII characters. 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 "Access Privilege Levels Overview" on page 53.

Table 12: 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 a RADIUS or LDAP 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
Juniper-Allow-Configuration-Regexps (RADIUS only)	Contains an extended regular expression that enables the user to view and modify configuration statements in addition to those statements authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	13	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.
Juniper-Deny-Configuration-Regexps (RADIUS only)	Contains an extended regular expression that denies the user permission to view or modify configuration statements authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	14	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression.

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

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

Junos OS can map RADIUS- and TACACS+-authenticated users to a locally defined user account or user template account, which defines the user's access privileges. You can also optionally configure a user's access privileges by defining Juniper Networks RADIUS and TACACS+ vendor-specific attributes (VSAs) on the respective authentication server.

A user's login class defines the set of permissions that determines which operational mode and configuration mode commands a user is authorized to execute and which areas of the configuration a user can view and modify. A login class can also define regular expressions that allow or deny a user the ability to execute certain commands or view and modify certain areas of the configuration, in addition to what the permission flags authorize. A login class can include the following statements to define user authorization:

- `permissions`
- `allow-commands`
- `allow-commands-regexps`
- `allow-configuration`
- `allow-configuration-regexps`
- `deny-commands`
- `deny-commands-regexps`
- `deny-configuration`
- `deny-configuration-regexps`

Similarly, a RADIUS or TACACS+ server configuration can use Juniper Networks VSAs to define specific permissions or regular expressions that determine a user's access privileges. For the list of supported RADIUS and TACACS+ VSAs, see the following:

- "Juniper Networks Vendor-Specific RADIUS Attributes" on page 189
- "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 220

You can define user permissions on the RADIUS or TACACS+ server as a list of space-separated values.

- A RADIUS server uses the following attribute and syntax:

```
Juniper-User-Permissions += "flag1 flag2 flag3",
```

  For example:

```
Juniper-User-Permissions += "interface interface-control configure",
```

- A TACACS+ server uses the following attribute and syntax:

```
user-permissions = "flag1 flag2 flag3"
```

  For example:

```
user-permissions = "interface interface-control configure"
```

A RADIUS or TACACS+ server can also define Juniper Networks VSAs that use a single extended regular expression (as defined in POSIX 1003.2) to allow or deny a user the ability to execute certain commands or view and modify areas of the configuration. You enclose multiple commands or configuration hierarchies in parentheses and separate them using a pipe symbol. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. When you configure authorization parameters both locally and remotely, the device merges the regular expressions received during TACACS+ or RADIUS authorization with any regular expressions defined on the local device.

- A RADIUS server uses the following attributes and syntax:

```
Juniper-Allow-Commands += "(cmd1)|(cmd2)|(cmdn)",
Juniper-Deny-Commands += "(cmd1)|(cmd2)|(cmdn)",
Juniper-Allow-Configuration += "(config1)|(config2)|(confign)",
Juniper-Deny-Configuration += "(config1)|(config2)|(confign)",
```

  For example:

```
Juniper-Allow-Commands += "(test)|(ping)|(quit)",
Juniper-Deny-Commands += "(request)|(restart)",
Juniper-Allow-Configuration += "(groups re0)|(system radius-server)",
Juniper-Deny-Configuration += "(system radius-options)|(system accounting)",
```

- A TACACS+ server uses the following attributes and syntax:

```
allow-commands = "(cmd1)|(cmd2)|(cmdn)"
deny-commands = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration = "(config1)|(config2)|(confign)"
deny-configuration = "(config1)|(config2)|(confign)"
```

  For example:

```
allow-commands = "(test)|(ping)|(quit)"
deny-commands = "(request)|(restart)"
allow-configuration = "(groups re0)|(system tacplus-server)"
deny-configuration = "(system tacplus-options)|(system accounting)"
```

RADIUS and TACACS+ servers also support configuring attributes that correspond to the same `*-regexps` statements that you can configure on the local device. The `*-regexps` TACACS+ attributes and the `*-Regexps` RADIUS attributes use the same regular expression syntax as the previous attributes, but they enable you to configure regular expressions with variables.

- A RADIUS server uses the following attributes and syntax:

```
Juniper-Allow-Configuration-Regexps += "(config1)|(config2)|(confign)",
Juniper-Deny-Configuration-Regexps += "(config1)|(config2)|(confign)",
```

- A TACACS+ server uses the following attributes and syntax:

```
allow-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
deny-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration-regexps = "(config1)|(config2)|(confign)"
deny-configuration-regexps = "(config1)|(config2)|(confign)"
```

  For example, the TACACS+ server configuration might define the following attributes:

```
allow-commands-regexps = "(show cli .*)|(ping 10.1.1..*)"
deny-commands-regexps = "(configure .*)|(edit)|(commit)|(rollback .*)"
```

On a RADIUS or TACACS+ server, you can also define the attributes using a simplified syntax where you specify each individual expression on a separate line.

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

```
Juniper-User-Permissions += "permission-flag1",
Juniper-User-Permissions += "permission-flag2",
Juniper-User-Permissions += "permission-flagn",
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 += "config1",
Juniper-Allow-Configuration += "config2",
Juniper-Allow-Configuration += "confign",
Juniper-Deny-Configuration += "config1",
Juniper-Deny-Configuration += "config2",
Juniper-Deny-Configuration += "confign",
```

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

```
user-permissions1 = "permission-flag1"
user-permissions2 = "permission-flag2"
user-permissionsn = "permission-flagn"
allow-commands1 = "cmd1"
allow-commands2 = "cmd2"
allow-commandsn = "cmdn"
deny-commands1 = "cmd1"
deny-commands2 = "cmd2"
deny-commandsn = "cmdn"
allow-configuration1 = "config1"
allow-configuration2 = "config2"
allow-configurationn = "confign"
deny-configuration1 = "config1"
deny-configuration2 = "config2"
deny-configurationn = "confign"
```

NOTE:

- In the TACACS+ server syntax, numeric values 1 through *n* 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 RADIUS or TACACS+ server imposes a limit on the number of individual regular expression lines.
- 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.

Users can verify their class, permissions, and command and configuration authorization by issuing the `show cli authorization` operational mode command.

```
user@host> show cli authorization
```

NOTE: When you configure the authorization parameters both locally on the network device and remotely on the RADIUS or TACACS+ server, the device merges the regular expressions received during TACACS+ or RADIUS authorization with any locally configured regular expressions. If the final expression contains a syntax error, the overall result is an invalid regular expression.

Juniper-Switching-Filter VSA Guidelines, Match Conditions and Actions

IN THIS SECTION

- Actions | 201

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS). Vendor-specific attributes extend the functionality of the RADIUS server beyond that provided by the public standard attributes, enabling the implementation of many useful features necessary for subscriber management and service support.

Juniper Networks VSAs have the vendor ID set to 2636.

Attributes are cleartext fields sent from the RADIUS server to the device as a result of authentication success or failure. Authentication prevents unauthorized user access by blocking a supplicant at the port until the device is authenticated by the RADIUS server. Implementing filtering attributes with authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

The Juniper-Switching-Filter attribute works in conjunction with 802.1X authentication to centrally control access of supplicants to the network. You can use this attribute to configure filters on the RADIUS server. These filters are sent to the switch and applied to users that have been authenticated using 802.1X authentication.

The Juniper-Switching-Filter can contain one or more filter terms. Filter terms are configured using one or more *match conditions* with a resulting *action*. Match conditions are the criteria that a packet must meet for a configured action to be applied on it. The configured action is the action that the switch takes if a packet meets the criteria specified in the match conditions. The action that the switch can take is to either accept or deny a packet.

Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and devices. One way to do this is to apply a previously configured port firewall filter directly to the RADIUS server using the Juniper-Firewall-filter-name VSA. Like port-filtering attributes, this filter is applied during the authentication process, and its actions are applied at the device port.

VSA Guidelines

Vendor-specific RADIUS attributes have a maximum of 247 characters per attribute. If more length is required, Juniper supports multiple instances of the same attribute, up to 4000 characters. To support filters that exceed 247 characters, use multiple Juniper-Switching-Filter attributes. The example below shows two attributes, each containing a new filter term that is within the 247 character limit:

```
Juniper-Switching-Filter = "Match ip-protocol 17 destination-port 67 Destination-ip
192.168.1.0/24 Action deny, match destination-ip 10.1.7.253 destination-port 53 action allow"
```

```
Juniper-Switching-Filter += "Match ip-protocol 1 destination-port 4000 Destination-ip
192.168.21.0/24 Action deny"
```

NOTE: The 4000 character limit is subject to supported MTU on both the RADIUS server and the Juniper device, and the number of other RADIUS attributes used.

The following guidelines apply to VSA match conditions and actions:

- Both the `match` statement and the `action` statement are mandatory.
- If no match condition is specified, any packet is considered a match by default.
- If no action is specified, the default action is to deny the packet.
- Any or all options can be included in each `match` and `action` statement.
- The AND operation is performed on fields that are of a different type, separated by commas. Fields of the same type cannot be repeated.
- For the `forwarding-class` option to be applied, the forwarding class must be configured on the switch. If the forwarding class is not configured on the switch, this option is ignored.

Match Conditions

Table 13 on page 200 describes the match conditions that you can specify when you configure a VSA attribute as a firewall filter by using the `match` command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 13: Match Conditions

Option	Description
`destination-mac` *mac-address*	Destination media access control (MAC) address of the packet.
`source-dot1q-tag` *tag*	Tag value in the 802.1Q header, in the range `0` through `4095`.
`destination-ip` *ip-address*	Address of the final destination node.

Table 13: Match Conditions *(Continued)*

Option	Description
ip-protocol *protocol-id*	IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: ah, egp (8), esp (50, gre (47), icmp (1), igmp (2), ipip (4), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)
source-port *port*	TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under destination-port.
destination-port *port*	TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspserver (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobilip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rkinit (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)

Actions

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 14 on page 202 shows the actions that you can specify in a term.

Table 14: Actions for VSAs

Option	Description
(allow | deny)	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
forwarding-class *class-of-service*	(Optional) Classify the packet in one of the following forwarding classes: • assured-forwarding • best-effort • expedited-forwarding • network-control
loss-priority (low | medium | high)	(Optional) Set the packet loss priority (PLP) to low, medium, or high. Specify both the forwarding class and the loss priority.

SEE ALSO

Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 384

Understanding Dynamic Filters Based on RADIUS Attributes | 395

Understanding RADIUS Accounting

Network devices support IETF RFC 2866, *RADIUS Accounting*. You can configure RADIUS accounting on a device to collect statistical data about users logging in to or out of a LAN and send the data to a RADIUS accounting server. The statistical data can be used for general network monitoring, analyzing and tracking usage patterns, or billing a user based on the duration of the session or type of services accessed.

To configure RADIUS accounting, specify:

- One or more RADIUS accounting servers to receive the statistical data from the device
- The type of accounting data to collect

You can use the same server for both RADIUS accounting and authentication, or you can use separate servers. You can specify a list of RADIUS accounting servers. The device queries the servers in the order in which they are configured. If the primary server (the first one configured) is unavailable, the device attempts to contact each server in the list until it receives a response.

The RADIUS accounting process between the device and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. The default port for RADIUS accounting is 1813.
2. The device forwards an *Accounting-Request* packet containing an event record to the accounting server. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request contains an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.
3. The RADIUS accounting server logs these events in a file as start-accounting or stop-accounting records. On FreeRADIUS, the filename is the server's address, such as 192.0.2.0.
4. The accounting server sends an *Accounting-Response* packet to the device confirming that it has received the accounting request.
5. If the device does not receive an Accounting-Response packet from the server, it continues to send accounting requests until the server returns a response.

You can view the statistics collected through this process on the RADIUS server. To see those statistics, access the log file configured to receive them.

Configure RADIUS System Accounting

IN THIS SECTION

When you enable RADIUS accounting, Juniper Networks devices, 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, *RADIUS Accounting*.

Configure Auditing of User Events on a RADIUS Server

To configure RADIUS accounting:

1. Configure the events to audit.

```
[edit system accounting]
user@host# set events [ events ]
```

For example:

```
[edit system accounting]
user@host# set events [ login change-log interactive-commands ]
```

events can include one or more of the following:

- `login`—Audit logins
- `change-log`—Audit configuration changes
- `interactive-commands`—Audit interactive commands (any command-line input)

2. Enable RADIUS accounting.

```
[edit]
user@host# set system accounting destination radius
```

3. Configure the address for one or more RADIUS accounting servers.

```
[edit system accounting destination radius]
user@host# set server server-address
```

For example:

```
[edit system accounting destination radius]
user@host# set server 192.168.17.28
```

NOTE: If you do not configure any RADIUS servers at the `[edit system accounting destination radius]` hierarchy level, the device uses the RADIUS servers configured at the `[edit system radius-server]` hierarchy level.

4. (Optional) Configure the source address for RADIUS accounting requests.

```
[edit system accounting destination radius server server-address]
user@host# set source-address source-address
```

For example:

```
[edit system accounting destination radius server 192.168.17.28]
user@host# set source-address 192.168.17.1
```

The source address is a valid IPv4 address or IPv6 address configured on one of the router interfaces or switch interfaces. If the network device has several interfaces that can reach the RADIUS server, assign an IP address that the device can use for all its communication with the RADIUS server. Doing this sets a fixed address as the source address for locally generated IP packets.

5. Configure the shared secret password that the network device uses to authenticate with the RADIUS accounting server.

The configured password must match the password that is configured on the RADIUS server. If the password contains spaces, enclose it in quotation marks. The device stores the password as an encrypted value in the configuration database.

```
[edit system accounting destination radius server server-address]
user@host# set secret password
```

For example:

```
[edit system accounting destination radius server 192.168.17.28]
user@host# set secret Radiussecret1
```

6. (Optional) If necessary, specify to which RADIUS accounting server port to send accounting packets, if different from the default (1813).

```
[edit system accounting destination radius server server-address]
user@host# set accounting-port port-number
```

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.

7. (Optional) Configure the number of times that the device attempts to contact a RADIUS accounting server and the amount of time that the device waits to receive a response from a server.

   By default, the device attempts to contact the server three times and waits three seconds. You can configure the `retry` value from 1 through 100 times and the `timeout` value from 1 through 1000 seconds.

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

   For example, to contact a server 2 times and wait 10 seconds for a response:

```
[edit system accounting destination radius server 192.168.17.28]
user@host# set retry 2
user@host# set timeout 10
```

8. (Optional) To route RADIUS accounting packets through the non-default management instance instead of the default routing instance, configure the `routing-instance mgmt_junos` statement.

```
[edit system accounting destination radius server server-address]
user@host# set routing-instance mgmt_junos
```

9. (Optional) Configure the `enhanced-accounting` statement at the `[edit system radius-options]` hierarchy level to include additional accounting attributes, including access method, remote port, and access privileges, for user login events.

```
[edit system radius-options]
user@host# set enhanced-accounting
```

NOTE: To limit the number of attribute values to audit, configure the `enhanced-avs-max <number>` statement at the `[edit system accounting]` hierarchy level.

The following example configures three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) for RADIUS accounting:

```
system {
    accounting {
        events [ login change-log interactive-commands ];
```

```
        destination {
            radius {
                server {
                    10.5.5.5 {
                        accounting-port 3333;
                        secret $ABC123;
                        source-address 10.1.1.1;
                        retry 3;
                        timeout 3;
                    }
                    10.6.6.6 secret $ABC123;
                    10.7.7.7 secret $ABC123;
                }
            }
        }
    }
}
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.1R1	Starting in Junos OS Release 18.1R1, existing RADIUS behavior is enhanced to support a management interface in a non-default VRF instance.

TACACS+ Authentication

IN THIS SECTION

Junos OS supports TACACS+ for central authentication of users on network devices. To use TACACS+ authentication on the device, you (the network administrator) must configure information about one or more TACACS+ servers on the network. You can also configure TACACS+ accounting on the device to collect statistical data about the users logging in to or out of a LAN and send the data to a TACACS+ accounting server.

Configure TACACS+ Authentication

IN THIS SECTION

TACACS+ authentication is a method of authenticating users who attempt to access a network device.

To configure TACACS+, perform the following tasks:

Configure TACACS+ Server Details

To use TACACS+ authentication on the device, 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. The device queries the TACACS+ servers in the order in which they are configured. If the primary server (the first one configured) is unavailable, the device attempts to contact each server in the list until it receives a response.

The network device can map TACACS+-authenticated users to a locally defined user account or user template account, which determines authorization. By default, Junos OS assigns TACACS+-authenticated users to the user template account `remote`, if configured, when:

- The authenticated user does not have a user account configured on the local device.

- The TACACS+ server either does not assign the user to a local user template, or the template that the server assigns is not configured on the local device.

The TACACS+ server can assign an authenticated user to a different user template to grant different administrative permissions to that user. The user retains the same login name in the CLI but inherits the login class, access privileges, and effective user ID from the assigned template. If the TACACS+-authenticated user does not map to any locally defined user account or user template, and the `remote` template is not configured, then authentication fails.

NOTE: The `remote` username is a special case in Junos OS and must always be lowercase. 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. 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 in the same login class.

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. The steps shown here are in a configuration group called `global`. Using a configuration group is optional.

To configure authentication by a TACACS+ server:

1. Configure the IPv4 address or IPv6 address of the TACACS+ authentication server.

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

For example:

```
[edit groups global system tacplus-server]
user@host# set 192.168.17.28
```

```
[edit groups global system tacplus-server]
user@host# set 2001:db8:0:f101::8
```

2. (Optional) Configure the packet source address for requests sent to the TACACS+ server.

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

For example:

```
[edit groups global system tacplus-server 192.168.17.28]
user@host# set source-address 192.168.17.1
```

```
[edit groups global system tacplus-server 2001:db8:0:f101::8]
user@host# set source-address 2001:db8:0:f101::1
```

The source address is a valid IPv4 address or IPv6 address configured on one of the router interfaces or switch interfaces. If the network device has several interfaces that can reach the TACACS+ server, assign an IP address that the device can use for all its communication with the TACACS+ server. Doing this sets a fixed address as the source address for locally generated IP packets.

3. Configure the shared secret password that the network device uses to authenticate with the TACACS+ server.

   The configured password must match the password that is configured on the TACACS+ server. If the password contains spaces, enclose it in quotation marks. The device stores the password as an encrypted value in the configuration database.

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

   For example:

   ```
   [edit groups global system tacplus-server 192.168.17.28]
   user@host# set secret Tacplussecret1
   ```

4. (Optional) Specify the port on which to contact the TACACS+ server, if different from the default port (49).

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

   For example:

   ```
   [edit groups global system tacplus-server 192.168.17.28]
   user@host# set port 50049
   ```

5. (Optional) Configure the amount of time that the device waits to receive a response from the TACACS+ server.

   By default, the device waits 3 seconds. You can configure the `timeout` value from 1 through 90 seconds.

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

   For example, to wait 15 seconds for a response from the server:

   ```
   [edit groups global system tacplus-server 192.168.17.28]
   user@host# set timeout 15
   ```

6. (Optional) Configure the device to maintain one open TCP connection to the server for multiple requests rather than opening a separate connection for each connection attempt.

   ```
   [edit groups global system tacplus-server 192.168.17.28]
   user@host# set single-connection
   ```

   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 device will be unable to communicate with that TACACS+ server.

7. (Optional) To route TACACS+ packets through a specific routing instance, configure the `routing-instance` statement and specify a valid routing instance.

   By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance.

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

8. Specify the authentication order, and include the `tacplus` option.

   ```
   [edit groups global system]
   user@host# set authentication-order [ authentication-methods ]
   ```

In the following example, whenever a user attempts to log in, Junos OS first queries the TACACS+ server for authentication. If that fails, it queries the RADIUS server. If that fails, it attempts authentication with locally configured user accounts.

```
[edit groups global system]
user@host# set authentication-order [ tacplus radius password ]
```

9. Assign a login class to TACACS+-authenticated users who do not have a locally defined user account.

   You configure a user template account in the same way as a local user account, except that you do not configure a local authentication password because the TACACS+ server authenticates the user.

   - To use the same permissions for all TACACS+-authenticated users, configure the `remote` user template.

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

     For example:

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

   - To use different login classes for different TACACS+-authenticated users, granting them different permissions:

     a. Create multiple user templates in the Junos OS configuration. For example:

     ```
     [edit groups global system login]
     user@host# set user RO class read-only
     user@host# set user OP class operator
     user@host# set user SU class super-user
     user@host# set user remote full-name "default remote access user template"
     user@host# set user remote class read-only
     ```

     b. Configure the TACACS+ server to map the authenticated user to the appropriate user template.

     For example, set the `local-user-name` Juniper vendor-specific attribute (VSA) to the name of a user template configured on the device, which in the previous example is RO, OP, or SU.

Authentication fails if the device cannot assign a user to a local user account or user template and the `remote` user template is not configured.

Configure TACACS+ to Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. You can also route TACACS+ packets through a management interface in a non-default VRF instance.

To route TACACS+ packets through the `mgmt_junos` management instance:

1. Enable the `mgmt_junos` management instance.

```
[edit system]
user@host# set management-instance
```

2. Configure the `routing-instance mgmt_junos` statement for the TACACS+ authentication server and the TACACS+ accounting server, if configured.

```
[edit system]
user@host# set tacplus-server server-address routing-instance mgmt_junos
user@host# set accounting destination tacplus server server-address routing-instance
mgmt_junos
```

Configure the Same Authentication Service for Multiple TACACS+ Servers

You can configure the same authentication service for multiple TACACS+ servers by including statements at the `[edit system tacplus-server]` and `[edit system tacplus-options]` hierarchy levels.

To assign the same authentication service to multiple TACACS+ servers:

1. Configure the TACACS+ servers as described in "Configure TACACS+ Authentication" on page 208.
2. Configure the `service-name` statement at the `[edit system tacplus-options]` hierarchy level.

   service-name is the name of the authentication service, which by default is `junos-exec`.

```
[edit system tacplus-options]
user@host set service-name service-name
```

For example:

```
[edit system tacplus-options]
service-name bob;
```

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
tacplus-server {
    10.2.2.2 secret "$ABC123"; ## SECRET-DATA
    10.3.3.3 secret "$ABC123"; ## SECRET-DATA
}
tacplus-options {
    service-name bob;
}
```

Configure Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS can map TACACS+-authenticated users to a locally defined user account or user template account, which determines authorization. You can also optionally configure a user's access privileges by defining Juniper Networks vendor-specific TACACS+ attributes on the TACACS+ server. You define the attributes in the TACACS+ server configuration file on a per-user basis. The network device retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user.

To specify these attributes, include a `service` statement of the following form in the TACACS+ server configuration file:

```
service = junos-exec {
    local-user-name = <username-local-to-router>
    allow-commands = "<allow-commands-regex>"
    allow-configuration-regexps = "<allow-configuration-regex>"
    deny-commands = "<deny-commands-regex>"
    deny-configuration-regexps = "<deny-configuration-regex>"
}
```

You can define the `service` statement in a `user` statement or a `group` statement.

Configure Periodic Refresh of the TACACS+ Authorization Profile

When you configure a device running Junos OS to use a TACACS+ server for authentication, the device prompts users for login information, which is verified by the TACACS+ server. After a user is successfully authenticated, the network device sends an authorization request to the TACACS+ server to obtain the authorization profile for the user. Authorization profiles specify the access permissions for authenticated users or devices.

The TACACS+ server sends the authorization profile as part of an authorization REPLY message. The remote user configured on the TACACS+ server is mapped to a local user or user template configured on the device running Junos OS. Junos OS combines the user's remote authorization profile and locally configured authorization profile, the latter of which is configured at the [`edit system login class`] hierarchy level.

By default, the exchange of authorization request and reply messages occurs only once, after successful authentication. You can configure the devices so that Junos OS periodically fetches the remote authorization profile from the TACACS+ server and refreshes the locally stored authorization profile. This periodic refresh ensures that the local device reflects any change in the authorization parameters without requiring that the user restart the authentication process.

To enable periodic refresh of the authorization profile, you must set the time interval at which the local device checks the authorization profile configured remotely on the TACACS+ server. If the remote authorization profile changes, the device fetches the authorization profile from the TACACS+ server and the authorization profile configured under the login class hierarchy. The device refreshes the authorization profile stored locally by combining the remote and locally configured authorization profiles.

You can configure the refresh time interval locally on the device running Junos OS or directly on the TACACS+ server. The time interval can range from 15 through 1440 minutes.

- To configure periodic refresh of the authorization profile on the local device, include the `authorization-time-interval` statement at the [`edit system tacplus-options`] hierarchy level, as follows:

```
[edit system tacplus-options]
user@host# set authorization-time-interval minutes
```

- To configure periodic refresh on the TACACS+ server, add the `refresh-time-interval` parameter in the authorization profile using the following syntax:

```
refresh-time-interval=minutes
```

Use the following guidelines to determine which time interval configuration takes precedence:

- If the refresh time interval is configured only on the TACACS+ server or only on the device running Junos OS, then the configured value takes effect.
- If the refresh time interval is configured on both the TACACS+ server and the device running Junos OS, the value configured on the TACACS+ server takes precedence.
- If no refresh time interval is configured on either the TACACS+ server or the device running Junos OS, then no periodic refresh occurs.
- If the refresh time interval configured on the TACACS+ server is out of range or invalid, the locally configured refresh time interval takes effect. If no refresh time interval is configured locally, then no periodic refresh occurs.

After the periodic refresh time interval is set, if the user changes the refresh interval before the authorization request is sent from the local device, the updated refresh interval takes effect after the next immediate periodic refresh.

Example: Configure a TACACS+ Server for System Authentication

IN THIS SECTION

This example configures system authentication through a TACACS+ server.

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Set up at least one TACACS+ server on your network.

Overview

In this example, you add a new TACACS+ server with an IP address of 172.16.98.1. You specify the shared secret password of the TACACS+ server as Tacacssecret1. The device stores the secret in the configuration database as an encrypted value. Finally, you specify the source address that the device uses in TACACS+ server requests. In most cases, you can use the loopback address of the device, which in this example is 10.0.0.1.

You can configure support for multiple user authentication methods, such as local password authentication, TACACS+, and RADIUS, on the network device, When you configure multiple authentication methods, you can prioritize the order in which the device tries the different methods. In this example, you configure the device to use TACACS+ authentication services first and, if that fails, to then attempt local password authentication.

A TACACS+-authenticated user must map to a local user account or a local user template account on the network device, which determines authorization. By default, if a TACACS+-authenticated user does not map to a local user account or a specific user template, the user is assigned to the `remote` user template, if configured. This example configures the `remote` user template.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set system tacplus-server 172.16.98.1
set system tacplus-server 172.16.98.1 secret Tacacssecret1
set system tacplus-server 172.16.98.1 source-address 10.0.0.1
set system authentication-order [tacplus password]
set system login user remote class operator
```

Step-by-Step Procedure

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server 172.16.98.1
```

2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.1 secret Tacacssecret1
```

3. Specify the device's loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.1 source-address 10.0.0.1
```

4. Specify the device's order of authentication, and include the `tacplus` option.

```
[edit system]
user@host# set authentication-order [tacplus password]
```

5. Configure the `remote` user template and its login class.

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

Results

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

The following output includes only those portions of the configuration hierarchy that are relevant to this example:

```
[edit]
user@host# show system
login {
    user remote {
        class operator;
    }
}
authentication-order [ tacplus password ];
tacplus-server {
    172.16.98.1 {
        secret "$9$ABC123"; ## SECRET-DATA
        source-address 10.0.0.1;
    }
}
```

After you configure the device, enter `commit` in configuration mode.

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verify the TACACS+ Server Configuration

Purpose

Verify that the TACACS+ server authenticates users.

Action

Log in to the network device, and verify that the login is successful. To verify that the device uses the TACACS+ server for authentication, you can attempt to log in with an account that does not define a local authentication password in the configuration.

Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports configuring Juniper Networks TACACS+ vendor-specific attributes (VSAs) on the TACACS+ server. Table 15 on page 220 lists the supported Juniper Networks VSAs.

Some of the attributes accept extended regular expressions, as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. For more information, see:

- "Regular Expressions to Allow and Deny Operational Mode Commands, Configuration Statements, and Hierarchies" on page 63
- "Use Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Commands" on page 223

Table 15: Juniper Networks Vendor-Specific TACACS+ Attributes

Name	Description	Length	String
`local-user-name`	Indicates the name of the user template assigned to this user when the user logs in to a device.	≥3	One or more octets containing printable ASCII characters.
`allow-commands`	Contains an extended regular expression that enables the user to run 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.
`allow-commands-regexps`	Contains an extended regular expression that enables the user to run 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.
`allow-configuration`	Contains an extended regular expression that enables the user to view and modify configuration statements in addition to those statements 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.

Table 15: Juniper Networks Vendor-Specific TACACS+ Attributes *(Continued)*

Name	Description	Length	String
allow-configuration-regexps	Contains an extended regular expression that enables the user to view and modify configuration statements in addition to those statements 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.
deny-commands	Contains an extended regular expression that denies the user permission to run 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.
deny-commands-regexps	Contains an extended regular expression that denies the user permission to run 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.
deny-configuration	Contains an extended regular expression that denies the user permission to view or modify configuration statements 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.
deny-configuration-regexps	Contains an extended regular expression that denies the user permission to view or modify configuration statements 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.

Table 15: Juniper Networks Vendor-Specific TACACS+ Attributes *(Continued)*

Name	Description	Length	String
`user-permissions`	Contains information the server uses to specify user permissions. **NOTE**: When the TACACS+ server defines the `user-permissions` attribute to grant the `maintenance` permission or `all` permission to a user, the user's list of group memberships does not automatically include the UNIX wheel group. Some operations such as running the `su root` command from a local shell require wheel group membership permissions. However, when the network device defines a local user account with the permissions `maintenance` or `all`, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a user template account with the required permissions and associate individual user accounts with the user template account.	≥3	One or more octets containing printable ASCII characters. See "Access Privilege Levels Overview" on page 53.
`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 a 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

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

Junos OS can map RADIUS- and TACACS+-authenticated users to a locally defined user account or user template account, which defines the user's access privileges. You can also optionally configure a user's access privileges by defining Juniper Networks RADIUS and TACACS+ vendor-specific attributes (VSAs) on the respective authentication server.

A user's login class defines the set of permissions that determines which operational mode and configuration mode commands a user is authorized to execute and which areas of the configuration a user can view and modify. A login class can also define regular expressions that allow or deny a user the ability to execute certain commands or view and modify certain areas of the configuration, in addition to what the permission flags authorize. A login class can include the following statements to define user authorization:

- `permissions`
- `allow-commands`
- `allow-commands-regexps`
- `allow-configuration`
- `allow-configuration-regexps`
- `deny-commands`
- `deny-commands-regexps`
- `deny-configuration`
- `deny-configuration-regexps`

Similarly, a RADIUS or TACACS+ server configuration can use Juniper Networks VSAs to define specific permissions or regular expressions that determine a user's access privileges. For the list of supported RADIUS and TACACS+ VSAs, see the following:

- "Juniper Networks Vendor-Specific RADIUS Attributes" on page 189
- "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 220

You can define user permissions on the RADIUS or TACACS+ server as a list of space-separated values.

- A RADIUS server uses the following attribute and syntax:

```
Juniper-User-Permissions += "flag1 flag2 flag3",
```

For example:

```
Juniper-User-Permissions += "interface interface-control configure",
```

- A TACACS+ server uses the following attribute and syntax:

```
user-permissions = "flag1 flag2 flag3"
```

For example:

```
user-permissions = "interface interface-control configure"
```

A RADIUS or TACACS+ server can also define Juniper Networks VSAs that use a single extended regular expression (as defined in POSIX 1003.2) to allow or deny a user the ability to execute certain commands or view and modify areas of the configuration. You enclose multiple commands or configuration hierarchies in parentheses and separate them using a pipe symbol. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. When you configure authorization parameters both locally and remotely, the device merges the regular expressions received during TACACS+ or RADIUS authorization with any regular expressions defined on the local device.

- A RADIUS server uses the following attributes and syntax:

```
Juniper-Allow-Commands += "(cmd1)|(cmd2)|(cmdn)",
Juniper-Deny-Commands += "(cmd1)|(cmd2)|(cmdn)",
Juniper-Allow-Configuration += "(config1)|(config2)|(confign)",
Juniper-Deny-Configuration += "(config1)|(config2)|(confign)",
```

For example:

```
Juniper-Allow-Commands += "(test)|(ping)|(quit)",
Juniper-Deny-Commands += "(request)|(restart)",
Juniper-Allow-Configuration += "(groups re0)|(system radius-server)",
Juniper-Deny-Configuration += "(system radius-options)|(system accounting)",
```

- A TACACS+ server uses the following attributes and syntax:

```
allow-commands = "(cmd1)|(cmd2)|(cmdn)"
deny-commands = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration = "(config1)|(config2)|(confign)"
deny-configuration = "(config1)|(config2)|(confign)"
```

  For example:

```
allow-commands = "(test)|(ping)|(quit)"
deny-commands = "(request)|(restart)"
allow-configuration = "(groups re0)|(system tacplus-server)"
deny-configuration = "(system tacplus-options)|(system accounting)"
```

RADIUS and TACACS+ servers also support configuring attributes that correspond to the same `*-regexps` statements that you can configure on the local device. The `*-regexps` TACACS+ attributes and the `*-Regexps` RADIUS attributes use the same regular expression syntax as the previous attributes, but they enable you to configure regular expressions with variables.

- A RADIUS server uses the following attributes and syntax:

```
Juniper-Allow-Configuration-Regexps += "(config1)|(config2)|(confign)",
Juniper-Deny-Configuration-Regexps += "(config1)|(config2)|(confign)",
```

- A TACACS+ server uses the following attributes and syntax:

```
allow-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
deny-commands-regexps = "(cmd1)|(cmd2)|(cmdn)"
allow-configuration-regexps = "(config1)|(config2)|(confign)"
deny-configuration-regexps = "(config1)|(config2)|(confign)"
```

  For example, the TACACS+ server configuration might define the following attributes:

```
allow-commands-regexps = "(show cli .*)|(ping 10.1.1..*)"
deny-commands-regexps = "(configure .*)|(edit)|(commit)|(rollback .*)"
```

On a RADIUS or TACACS+ server, you can also define the attributes using a simplified syntax where you specify each individual expression on a separate line.

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

```
Juniper-User-Permissions += "permission-flag1",
Juniper-User-Permissions += "permission-flag2",
Juniper-User-Permissions += "permission-flagn",
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 += "config1",
Juniper-Allow-Configuration += "config2",
Juniper-Allow-Configuration += "confign",
Juniper-Deny-Configuration += "config1",
Juniper-Deny-Configuration += "config2",
Juniper-Deny-Configuration += "confign",
```

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

```
user-permissions1 = "permission-flag1"
user-permissions2 = "permission-flag2"
user-permissionsn = "permission-flagn"
allow-commands1 = "cmd1"
allow-commands2 = "cmd2"
allow-commandsn = "cmdn"
deny-commands1 = "cmd1"
deny-commands2 = "cmd2"
deny-commandsn = "cmdn"
allow-configuration1 = "config1"
allow-configuration2 = "config2"
allow-configurationn = "confign"
deny-configuration1 = "config1"
deny-configuration2 = "config2"
deny-configurationn = "confign"
```

NOTE:

- In the TACACS+ server syntax, numeric values 1 through *n* 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 RADIUS or TACACS+ server imposes a limit on the number of individual regular expression lines.
- 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.

Users can verify their class, permissions, and command and configuration authorization by issuing the `show cli authorization` operational mode command.

```
user@host> show cli authorization
```

NOTE: When you configure the authorization parameters both locally on the network device and remotely on the RADIUS or TACACS+ server, the device merges the regular expressions received during TACACS+ or RADIUS authorization with any locally configured regular expressions. If the final expression contains a syntax error, the overall result is an invalid regular expression.

Configuring TACACS+ System Accounting

IN THIS SECTION

You can configure TACACS+ accounting on a device to collect statistical data about users logging in to or out of a LAN and send the data to a TACACS+ accounting server. The statistical data can be used for general network monitoring, analyzing and tracking usage patterns, or billing a user based on the duration of the session or type of services accessed.

To configure TACACS+ accounting, specify:

- One or more TACACS+ accounting servers to receive the statistical data from the device
- The type of accounting data to collect

You can use the same server for both TACACS+ accounting and authentication, or you can use separate servers. You can specify a list of TACACS+ accounting servers. The device queries the servers in the order in which they are configured. If the primary server (the first one configured) is unavailable, the device attempts to contact each server in the list until it receives a response.

When you enable TACACS+ accounting, Juniper Networks devices, acting as TACACS+ clients, can notify the TACACS+ server about user activities such as software logins, configuration changes, and interactive commands.

Configure TACACS+ Server Accounting

To configure TACACS+ server accounting:

1. Configure the events to audit.

```
[edit system accounting]
user@host# set events [ events ]
```

For example:

```
[edit system accounting]
user@host# set events [ login change-log interactive-commands ]
```

events can include one or more of the following:

- `login`—Audit logins
- `change-log`—Audit configuration changes
- `interactive-commands`—Audit interactive commands (any command-line input)

2. Enable TACACS+ accounting.

```
[edit]
user@host# set system accounting destination tacplus
```

3. Configure the address for one or more TACACS+ accounting servers.

```
[edit system accounting destination tacplus]
user@host# set server server-address
```

For example:

```
[edit system accounting destination tacplus]
user@host# set server 192.168.17.28
```

NOTE: If you do not configure any TACACS+ servers at the `[edit system accounting destination tacplus]` hierarchy level, the device uses the TACACS+ servers configured at the `[edit system tacplus-server]` hierarchy level.

4. (Optional) Configure the source address for TACACS+ accounting requests.

```
[edit system accounting destination tacplus server server-address]
user@host# set source-address source-address
```

For example:

```
[edit system accounting destination tacplus server 192.168.17.28]
user@host# set source-address 192.168.17.1
```

The source address is a valid IPv4 address or IPv6 address configured on one of the router interfaces or switch interfaces. If the network device has several interfaces that can reach the TACACS+ server, assign an IP address that the device can use for all its communication with the TACACS+ server. Doing this sets a fixed address as the source address for locally generated IP packets.

5. Configure the shared secret password that the network device uses to authenticate with the TACACS+ accounting server.

The configured password must match the password that is configured on the TACACS+ server. If the password contains spaces, enclose it in quotation marks. The device stores the password as an encrypted value in the configuration database.

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

For example:

```
[edit system accounting destination tacplus server 192.168.17.28]
user@host# set secret Tacplussecret1
```

6. (Optional) If necessary, specify to which TACACS+ accounting server port to send accounting packets, if different from the default (49).

```
[edit system accounting destination tacplus server server-address]
user@host# set port port-number
```

7. (Optional) Configure the amount of time that the device waits to receive a response from the TACACS+ accounting server.

   By default, the device waits three seconds. You can configure the `timeout` value from 1 through 90 seconds.

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

For example, to wait 15 seconds for a response from the server:

```
[edit system accounting destination tacplus server 192.168.17.28]
user@host# set timeout 15
```

8. (Optional) Configure the device to maintain one open TCP connection to the server for multiple requests rather than opening a separate connection for each connection attempt.

```
[edit system accounting destination tacplus server server-address]
user@host# set single-connection
```

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 device will be unable to communicate with that TACACS+ server.

9. (Optional) To route TACACS+ accounting packets through the non-default management instance or another routing instance instead of the default routing instance, configure the `routing-instance` statement and specify the routing instance.

```
[edit system accounting destination tacplus server server-address]
user@host# set routing-instance routing-instance
```

For example:

```
[edit system accounting destination tacplus server 192.168.17.28]
user@host# set routing-instance mgmt_junos
```

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

```
[edit system tacplus-options]
user@host# set (no-cmd-attribute-value | exclude-cmd-attribute)
```

NOTE: Both statements support the correct logging of accounting requests in the Accounting file instead of the Administration file. If you configure 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 configure the `exclude-cmd-attribute` statement, the `cmd` attribute is totally excluded from the start and stop requests.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in authentication.

17.4R1	Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos.

Authentication for Routing Protocols

IN THIS SECTION

You can configure an authentication method and password for routing protocol messages for many routing protocols including BGP, IS-IS, OSPF, RIP, and RSVP. To prevent the exchange of unauthenticated or forged packets, 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. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface.

This topic provides a high-level overview and some basic examples for authenticating routing protocols. For detailed information about configuring authentication for a specific routing protocol, see the user guide for that protocol.

Authentication Methods for Routing Protocols

Some routing protocols—BGP, IS-IS, OSPF, RIP, and RSVP—enable you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets that the protocol sends 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 *avoid* using this authentication method.

- MD5 and HMAC-MD5 (BGP, IS-IS, OSPF, RIP, and RSVP)—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 some maximum number of letters and digits. Passwords can include any ASCII characters. 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.

Example: Configure the Authentication Key for BGP and IS-IS Routing Protocols

IN THIS SECTION

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.

Junos OS supports HMAC-MD5 authentication for BGP, IS-IS, OSPF, RIP, and RSVP. HMAC-MD5 uses a secret key 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 is 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.

Configure BGP

The following example shows the configuration of a single authentication key for the different BGP peer groups. 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. The attacker may be 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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
        }
        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 "$9$aH1j8gqQ1gjyjgjhgjgiiiii";
        }
    }
}
```

Configure IS-IS

Although Junos OS supports authentication for all IGPs, some IGPs 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 MPLS. Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF. OSPF is encapsulated in IP and is therefore subject to remote spoofing and denial of service (DoS) attacks.

The following example configures authentication for IS-IS. It 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. The attacker may be sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```
[edit]
protocols {
    isis {
        level 1 {
            authentication-key "$9$aH1j8gqQ1gjyjgjhgjgiiiii"; # SECRET-DATA
            authentication-type md5;
        }
        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;
        }
        traceoptions {
            file isis-trace size 10m files 10;
            flag normal;
            flag error;
```

```
        }
    }
}
```

Configure the Authentication Key Update Mechanism for Routing Protocols

IN THIS SECTION

You can configure an authentication key update mechanism for the BGP, LDP, and IS-IS routing protocols. This mechanism enables you to update authentication keys without interrupting associated routing and signaling protocols such as OSPF and RSVP.

To configure this feature, include the `authentication-key-chains` statement at the `[edit security]` hierarchy level. To apply the key chain, you must configure the key chain identifier and the key chain algorithm at the appropriate hierarchy level for the protocol.

The following sections provide more information about configuring authentication key updates for routing protocols. For detailed information about configuring authentication key updates for a specific routing protocol, see the user guide for that protocol.

Configure 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 {
        algorithm (hmac-sha-1 | md5)
        options (basic | isis-enhanced)
        secret secret-data;
```

```
        start-time yyyy-mm-dd.hh:mm:ss;
    }
}
```

key-chain—Assign a name to the keychain mechanism. You reference this name at the appropriate hierarchy levels for the protocol to associate unique authentication key-chain attributes, as specified using the following options:

- algorithm—Authentication algorithm for IS-IS.
- key—Integer value that uniquely identifies each key within a keychain. The range is from 0 through 63.
- options—(IS-IS only) Protocol transmission encoding format for encoding the message authentication code in routing protocol packets.
- secret—Password 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 time for authentication key transmission, specified in *UTC*. The start time must be unique within the keychain.

Configure 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 within the [edit protocols (bgp | ldp)] hierarchy level. Including the authentication-key-chain statement associates each routing protocol with the [edit security authentication-key-chains] authentication keys. You must also configure the authentication-algorithm statement and specify the algorithm. For example:

```
[edit protocols]
bgp {
    group group-name {
        neighbor address {
            authentication-algorithm algorithm;
            authentication-key-chain key-chain-name;
        }
    }
}
ldp {
    session session-addr {
        authentication-algorithm algorithm;
        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 keychains. If you try this action, the CLI issues a warning, and the commit fails.

CHAPTER 6

Remote Access Management

IN THIS CHAPTER

Remote Access Overview

IN THIS SECTION

You (the network administrator) can access a router, switch, or security device remotely using services such as DHCP, Finger, FTP, rlogin, SSH, and Telnet services. This topic shows you how to configure remote access using Telnet, SSH, FTP, and Finger services.

System Services 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. Users can access the router 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.

Configure 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.

Configure FTP Service for Remote Access to the Router or Switch

To configure the device 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 not use the FTP service in a Common Criteria environment.

Configure 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 not use the finger service in a Common Criteria environment.

Configure SSH Service for Remote Access to the Router or Switch

IN THIS SECTION

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 {
    authentication-order  [method 1 method2...];
    authorized-keys-command authorized-keys-command;
    authorized-keys-command-user authorized-keys-command-user;
    authorized-principals-file filename
    authorized-principals-command program-path
    ciphers [ cipher-1 cipher-2 cipher-3 ...];
    client-alive-count-max number;
    client-alive-interval seconds;
    connection-limit limit;
    fingerprint-hash (md5 | sha2-256);
    host-certificate-file filename
    hostkey-algorithm (algorithm | no-algorithm);
    key-exchange [algorithm1 algorithm2...];
    log-key-changes log-key-changes;
    macs [algorithm1 algorithm2...];
    max-pre-authentication-packets number;
    max-sessions-per-connection number;
    no-challenge-response;
    no-password-authentication;
    no-passwords;
    no-public-keys;
    no-tcp-forwarding;
    port port-number;
    protocol-version [v2];
    rate-limit number;
    rekey {
        data-limit bytes;
        time-limit minutes;
    }
    root-login (allow | deny | deny-password);
```

```
    sftp-server;
    tcp-forwarding;
    trusted-user-ca-key-file filename
    }
```

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.

- `data-limit`—Data limit before renegotiating session keys (bytes)

- `time-limit`—Time limit before renegotiating session keys (minutes)

Starting in Junos OS Release 19.4R1 and Junos OS Release 17.4R3, you can disable either the SSH login password or the challenge-response authentication using the `no-password-authentication` and `no-challenge-response` options at the [`edit system services ssh`] hierarchy level.

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 can be used to forward TCP traffic, bypassing any firewall filters or access control lists. By bypassing firewall filters or access control lists, this type of tunnel allows 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:

Configure the Root Login Through SSH

By default, users are allowed to log in to the router or switch as `root` through SSH when the authentication method does not require a password. To control user access through SSH, include the `root-login` statement at the `[edit systems 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.

`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.

The default is `deny-password`.

Configure Incoming SFTP Connections

SSH File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. Starting in Junos OS Release 19.1R1, we have globally disabled the incoming SFTP connections by default. If desired, you can globally enable incoming SFTP connections by configuring the statement `sftp-server` at the `[edit system services ssh]` hierarchy level. Prior to Junos OS Release 19.1R1, incoming SFTP connections were globally enabled by default.

NOTE: Only the incoming SFTP connections are disabled by default. For example, given devices A and B (where device A is running 19.1R1), you cannot connect through SFTP from B to A by default. However, you can connect through SFTP from device B to device A if you configure `sftp-server` on device A.

The incoming SFTP connections are disabled by default. To enable incoming SFTP connections:

1. Configure the `sftp-server` statement at the `[edit system services ssh]` hierarchy level:

```
[edit system services ssh]
user@host# set sftp-server
```

2. Commit the configuration.

```
[edit system services ssh]
user@host# commit
```

The sftp-server statement is now active. Therefore, the incoming SFTP connections are enabled.

Configure the SSH Protocol Version

By default, only version 2 of the SSH protocol is enabled.

To configure the router or switch to use 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 ];
```

Systems in FIPS mode always use SSH protocol version v2.

Configure 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 by default. To enable it, configure the client-alive-count-max and client-alive-interval statements. 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  ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

Configure the SSH Fingerprint Hash Algorithm

To configure the hash algorithm used by the SSH server when it displays key fingerprints, include the fingerprint-hash statement and specify md5 or sha2-256 at the [edit system services ssh] hierarchy level:

```
[edit system services ssh]
fingerprint-hash (md5 | sha2-256);
```

The md5 hash algorithm is unavailable on systems in FIPS mode.

SSH Certificate-Based Authentication Overview

IN THIS SECTION

Starting in Junos OS and Junos OS Evolved Release 22.4R1, you can configure SSH certificate-based authentication for users and hosts. This feature lets you establish password-less SSH access for users and trust hosts without verifying key fingerprints.

Benefits of SSH Certificate-Based Authentication

- SSH certificate-based authentication eliminates the need for users to remember and enter passwords, streamlining the login process.
- Compared to traditional password-based approaches, SSH certificates offer stronger security. They are harder to breach with no password to guess or crack.
- SSH certificates simplify the management of authentication keys. Instead of managing individual keys for each user and host, administrators can issue and revoke certificates from a centralized certificate authority.

Generating Signing Keys

Signing keys are specialized cryptographic keys used in SSH certificate-based authentication. The first step for configuring SSH certificate-based authentication is to generate signing keys. You can generate signing keys on any Linux/FreeBSD system. Follow these steps to generate signing keys for SSH certificate-based authentication:

1. Run the command: `ssh-keygen -f <filename_ca>`. This will create a private key named <*filename*_ca> and a corresponding public key named <*filename*_ca.pub>.
2. Log in to your Juniper device and configure the SSH trusted user certificate authority (CA) key file by executing the command: `set system services ssh trusted-user-ca-key-file <path-to-public-key>` and then commit the configuration.

3. Each user can generate their own user keys using the following CLI command: `ssh-keygen -t <rsa|ecdsa|ed25519>`.
4. Copy the user-created public key onto the machine that has the user certificates <*filename*_ca> and <*filename*_ca.pub>.
5. Sign the user public key in the <*filename*_ca.pub> file.

Configuration

To configure SSH certificate-based authentication, use the following CLI configuration statements:

- `[system services ssh trusted-user-ca-key-file filename]`—Configure the `TrustedUserCAKey` file, which contains the public keys of an SSH certificate.
- `[system services ssh host-certificate-file filename]`—Configure the `HostCertificate` file, which contains the signed host certificate.
- `[system services ssh authorized-principals-file filename]`—Configure the `AuthorizedPrincipals` file, which contains a list of names, one of which must appear in the certificate for it to be accepted for authentication.
- `[system services ssh authorized-principals-command program-path]`—Specify a program to be used for generating the list of allowed certificate principals found in the `AuthorizedPrincipals` file.

Disabling SSH

If you enabled SSH and want to disable it, simply remove the `ssh` statement from the `[edit system services]` hierarchy level.

If you only want to disable external SSH, use the `access-disable-external` statement at the `[edit system services ssh]` hierarchy level.

Starting in Junos OS Release 21.4R1, Junos platforms with VM host installed have SSH enabled by default.

When SSH is enabled by default, you can't disable it through the `[edit system services]` hierarchy like normal. Instead, you can configure a firewall filter to deny SSH access:

```
set firewall family inet filter SSH-FILTER term 1 from protocol tcp
set firewall family inet filter SSH-FILTER term 1 from port ssh
set firewall family inet filter SSH-FILTER term 1 from interface fxp0
```

```
set firewall family inet filter SSH-FILTER term 1 then discard
set firewall family inet filter SSH-FILTER term 2 then accept
```

Step-by-Step Procedure

Follow these steps to configure a firewall filter to deny SSH access:

1. Define the filter term *1*. This term denies TCP traffic from SSH:

```
[edit]
user@R1# set firewall family inet filter SSH-FILTER term 1 from protocol tcp
user@R1# set firewall family inet filter SSH-FILTER term 1 from port ssh
user@R1# set firewall family inet filter SSH-FILTER term 1 from interface fxp0
user@R1# set firewall family inet filter SSH-FILTER term 1 then discard
```

2. Define the filter term *2*. This term allows any traffic that isn't denied by filter term *1*:

```
[edit]
user@R1# set firewall family inet filter SSH-FILTER term 2 then accept
```

For more information about using firewall filters to disable SSH, see "Example: Configure a Filter to Block Telnet and SSH Access" on page 243.

The telnet Command

You can use the CLI `telnet` command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name> <no-resolve>
<port port> <routing-instance routing-instance-name> <source address>
```

NOTE: On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent Telnet sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

SRX100	SRX210 SRX220	SRX240	SRX300 SRX320 SRX340	SRX345	SRX150 0
3	*3*	*5*	*3*	*5*	*5*

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter `quit`.

Table 16: CLI telnet Command Options

Option	Description
`8bit`	Use an 8-bit data path.
`bypass-routing`	Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open a Telnet session to the specified hostname or IP address.
`inet`	Force the Telnet session to an IPv4 destination.
`interface` *source-interface*	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
`no-resolve`	Suppress the display of symbolic names.
`port` *port*	Specify the port number or service name on the host.
`routing-instance` *routing-instance-name*	Use the specified routing instance for the Telnet session.
`source` *address*	Use the specified source address for the Telnet session.

The ssh Command

You can use the CLI ssh command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name> <routing-instance routing-instance-name> <source address> <v1> <v2>
```

NOTE: On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent SSH sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

SRX100	SRX210 SRX220	SRX240	SRX300 SRX320 SRX340	SRX345	SRX150 0
3	*3*	*5*	*3*	*5*	*5*

Table 17 on page 252 describes the ssh command options.

Table 17: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.
interface *source-interface*	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.

Table 17: CLI ssh Command Options *(Continued)*

Option	Description
`routing-instance` *routing-instance-name*	Use the specified routing instance for the SSH connection.
`source` *address*	Use the specified source address for the SSH connection.
`v1`	Force SSH to use version 1 for the connection.
`v2`	Force SSH to use version 2 for the connection.

Configure SSH Known Host Keys for Secure Copying of Data

IN THIS SECTION

Secure Shell (*SSH*) uses *encryption* algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (*SCP*) as an alternative to *FTP* for the background transfer of data such as configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
- Verify that the host key is authentic.

- Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

Tasks to configure SSH host keys for secure copying of data are:

Configure SSH Known Hosts

To configure SSH known hosts, include the `host` statement, and specify hostname and host key options for trusted servers at the `[edit security ssh-known-hosts]` hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server  {
    dsa-key key;
}
host archive-server-url {
    rsa-key key;
}
host server-with-ssh-version-1 {
    rsa1-key key;
}
```

Host keys are one of the following:

- `dsa-key` *key*—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- `ecdsa-sha2-nistp256-key` *key*—Base64 encoded ECDSA-SHA2-NIST256 key.
- `ecdsa-sha2-nistp384-key` *key*—Base64 encoded ECDSA-SHA2-NIST384 key.
- `ecdsa-sha2-nistp521-key` *key*—Base64 encoded ECDSA-SHA2-NIST521 key.
- `ed25519-key` *key*—Base64 encoded ED25519 key.
- `rsa-key` *key*—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- `rsa1-key` *key*—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

Configure Support for SCP File Transfer

To configure a known host to support background SCP file transfers, include the `archive-sites` statement at the `[edit system archival configuration]` hierarchy level.

```
[edit system archival configuration]
archive-sites {
    scp://username<:password>@host<:port>/url-path;
}
```

NOTE: When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, **"scp://*username*<:*password*>@[*host*]<:*port*>/*url-path*";**

Setting the `archive-sites` statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites "<scp-url-path>"
The authenticity of host <my-archive-server (<server-ip-address>)> can't be established. RSA key
fingerprint is <ascii-text key>. Are you sure you want to continue connecting (yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering **yes** at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

Update SSH Host Key Information

IN THIS SECTION

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the `archival configuration archive-sites` statement at the `[edit system]` hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

Retrieve Host Key Information Manually

To manually retrieve SSH public host key information, configure the `fetch-from-server` option at the `[edit security ssh-known-hosts]` hierarchy level. You must to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

Import Host Key Information from a File

To manually import SSH host key information from a **known_hosts** file, include the `load-key-file` option at the `[edit security ssh-known-hosts]` hierarchy level. You must specify the path to the file from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

Configure the SSH Service to Support Legacy Cryptography

You can configure Junos OS to support legacy cryptography ciphers and key exchange methods.

NOTE: Lack of support for legacy cryptography in devices causes Junos Space device discovery to fail. To work around this issue, configure the device to support the `3des-cbc` or `blowfish-cbc` cipher, or both, and the `dh-group1-sha1` key-exchange method. This issue does not affect devices running Junos OS with upgraded FreeBSD.

Junos OS supports the following set of ciphers by default:

- `chacha20-poly1305@openssh.com`
- `aes128-ctr`
- `aes192-ctr`
- `aes256-ctr`
- `aes128-gcm@openssh.com`
- `aes256-gcm@openssh.com`

In Junos OS, the following ciphers are not supported by default, but you can configure your device to support them. They are listed from the most secure to the least secure:

- aes256-cbc
- aes192-cbc
- aes128-cbc
- 3des-cbc

Junos OS supports the following set of key-exchange methods by default:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- group-exchange-sha2
- dh-group14-sha1

In Junos OS, the following key-exchange methods are not supported by default, but you can configure your device to support them:

- group-exchange-sha1
- dh-group1-sha1

To configure the SSH service to support legacy cryptography:

NOTE: By configuring an ordered set of ciphers, key-exchange methods, or message authentication codes (MACs), the newly defined set is applied to both server and client commands. Changes to the defaults affect the `file copy` command when you use Secure Copy Protocol (SCP).

1. Add support for ciphers by using the `set system services ssh ciphers [ cipher 1 cipher 2 ... ]` command. We recommend that you add the ciphers to the end of the configuration list so that they are among

the last options used. In the following example, the `arcfour` and `blowfish-cbc` ciphers are added to the default set:

```
[edit system services ssh]
user@device# set ciphers [ chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr
aes128-gcm@openssh.com aes256-gcm@openssh.com arcfour blowfish-cbc ]
```

2. Add support for key-exchange methods by using the `set system services ssh key-exchange [ method 1 method 2 ... ]` command. We recommend that you add the key-exchange methods to the end of the configuration list so that they are among the last options used. In the following example, the `dh-group1-sha1` key-exchange method is added to the default set:

```
[edit system services ssh]
user@device# set key-exchange [ curve25519-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-
sha2-nistp521 group-exchange-sha2 dh-group14-sha1 dh-group1-sha1 ]
```

3. Commit the configuration:

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

SEE ALSO

key-exchange

Configure Outbound SSH Service

IN THIS SECTION

You can configure a device running Junos OS to initiate a TCP/IP connection with a client management application. If the management application does not reach a Juniper Networks device, for example, the device being a firewall. In such cases, `outbound-ssh` can be configured on the Juniper Networks device. An `outbound-ssh` configuration initiates a reverse SSH connection from server to client to the management application. This outbound SSH connection is closed only after the configuration are removed from the device.

NOTE: There is no initiation command with outbound SSH. After you configure and commit outbound SSH, the device begins to initiate an outbound SSH connection based on the committed configuration. The device repeatedly attempts to create this connection until successful. If the connection between the device and the client management application is dropped, the device again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the device for outbound SSH connections, include the `outbound-ssh` statement at the `[edit system services]` hierarchy level:

```
[edit system services outbound-ssh]
```

The following topics describe the tasks for configuring the outbound SSH service.

Send the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of *device-id*.

To configure the device identifier of the router or switch, include the `device-id` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when secret is not configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
```

During the initialization of an SSH connection, the client authenticates the identity of the device using the public SSH host key of the device. Therefore, before the client can initiate the SSH sequence, the client needs the public SSH key of the device. When you configure the secret statement, the device passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the secret statement is set and the device establishes an outbound SSH connection, the device communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the secret statement. The value of the secret statement is shared between the device and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the device identified by the device-id statement.

Using the secret statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.

NOTE: Including the secret statement means that the device sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if the client already has an SSH key for that device. We recommend that you replace the client's copy of the SSH host key with the new key. Host keys can change for various reasons. By replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router's or switch's public SSH host key when the device connects to the client, include the secret statement at the [edit system services outbound-ssh client *client-id*] hierarchy level:

```
[edit system services outbound-ssh client client-id]
secret password;
```

The following message is sent by the device when the secret attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO\r\n
MSG-VER: V1\r\n
DEVICE-ID: <device-id>\r\n
HOST-KEY: <public-host-key>\r\n
HMAC:<HMAC(pub-SSH-host-key, <secret>>)>\r\n
```

Configure Keepalive Messages for Outbound SSH Connections

After the client application has the router's or switch's public SSH host key, it can initiate the SSH sequence as if it had created the TCP/IP connection. The client can then authenticate the device using its copy of the router's or switch's public host SSH key as part of that sequence. The device authenticates the client user through the mechanisms supported in Junos OS (RSA/DSA public string or password authentication).

To enable the device to send SSH protocol keepalive messages to the client application, configure the `keep-alive` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
    retry number;
    timeout seconds;
}
```

Configure a New Outbound SSH Connection

When disconnected, the device begins to initiate a new outbound SSH connection. To specify how the device reconnects to the server after a connection is dropped, include the `reconnect-strategy` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client-id]
reconnect-strategy (sticky | in-order);
```

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See "Configure Keepalive Messages for Outbound SSH Connections" on page 261.

Configure 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;
}
```

Configure Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
    address address {
        retry number;
        timeout seconds;
        port port-number;
    }
```

NOTE: Outbound SSH connections support IPv4 and IPv6 address formats.

Configure Routing Instances for Outbound SSH Clients

To use the management routing instance, first enable the `mgmt_junos` routing instance using the `set system management-instance` command.

To use any other routing instance, first configure the routing instance at the `[edit routing-instances]` hierarchy.

If you do not specify a routing instance, your device will establish the outbound SSH connection using the default routing table.

Configure NETCONF-Over-SSH Connections on a Specified TCP Port

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.

Configure Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, a device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.

  For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.
- Enforces a minimum session time of 20 seconds, during which a session cannot be disconnected. Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect. Configuring the minimum session time also prevents them from attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
- Enforce a minimum session time of 40 seconds, during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is `10`, but you can set a number from `1` through `10`.

```
[edit system login retry-options]
user@host# set tries-before-disconnect 4
```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is 2, but you can specify a value from 1 through 3.

```
[edit system login retry-options]
user@host# set backoff-threshold 2
```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of 5 seconds, but you can specify a value from 5 through 10 seconds.

```
[edit system login retry-options]
user@host# set backoff-factor 5
```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is 20 seconds, but you can specify an interval from 20 through 60 seconds.

```
[edit system login retry-options]
user@host# set minimum-time 40
```

5. After you configure the device, enter commit in configuration mode.

Example: Configure a Filter to Block Telnet and SSH Access

IN THIS SECTION

Requirements

You need two devices running Junos OS with a shared network link. No special configuration beyond basic device initialization (management interface, remote access, user login accounts, etc.) is required

before configuring this example. While not a strict requirement, console access to the R2 device is recommended.

NOTE: Our content testing team has validated and updated this example.

Overview and Topology

IN THIS SECTION

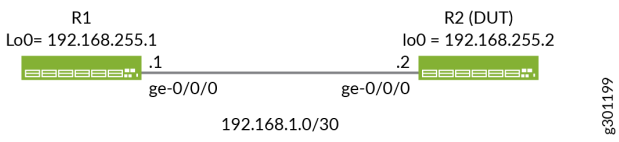
In this example, you create an IPv4 stateless firewall filter that logs and rejects Telnet or SSH packets sent to the local Routing Engine, unless the packet originates from the 192.168.1.0/30 subnet. The filter is applied to the loopback interface to ensure that only traffic destined to the local device is affected. You apply the filter in the input direction. An output filter is not used. As a result all locally generated traffic is allowed.

- To match packets originating from a specific subnet or IP prefix, you use the `source-address` IPv4 match condition applied in the input direction.
- To match packets destined for the Telnet port and SSH ports, you use the `protocol tcp` match condition combined with a `port telnet` and `port ssh` IPv4 match conditions applied in the input direction.

Example Topology

Figure 5 on page 265 shows the test topology for this example. The firewall filter is applied to the R2 device, making it the device under test (DUT). The R1 and the R2 devices share a link that is assigned a subnet of 192.168.1.0/30. Both devices have loopback addresses assigned from the 192.168.255.0/30 prefix using a /32 subnet mask. Static routes provide reachability between loopback addresses because an interior gateway protocol is not configured in this basic example.

Figure 5: Example Topology



Configuration

IN THIS SECTION

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

CAUTION: By design the sample filter restricts Telnet and SSH access to R2 unless it originates from the shared subnet at R1. If you use SSH or Telnet to access the R2 device directly, you will lose connectivity when the filter is applied. We recommend that you have console access when configuring this example. If needed you can use the R1 device as a jump host to launch an SSH session to R2 after the filter is applied. Alternatively, consider modifying the sample filter to also permit the IP subnet assigned to the machine you use to access the R2 device.

Perform the following tasks to configure this example:

CLI Quick Configuration

Quick Configuration for the R1 Device

To quickly configure the R1 device, edit the following commands as needed and paste them into the CLI at the `[edit]` hierarchy level. Be sure to issue a `commit`in configuration mode to activate the changes.

```
set system host-name R1
set system services ssh root-login allow
set interfaces ge-0/0/0 description "Link from R1 to R2"
set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.1/30
set interfaces lo0 unit 0 family inet address 192.168.255.1/32
set routing-options static route 192.168.255.2/32 next-hop 192.168.1.2
```

Quick Configuration for the R2 Device

To quickly configure the R2 device, edit the following commands as needed and paste them into the CLI at the `[edit]` hierarchy level. Be sure to issue a `commit` in configuration mode to activate the changes.

TIP: Consider using `commit-confirmed` when making changes that might affect remote access to your device. *Activating a Junos OS Configuration but Requiring Confirmation*

```
set system host-name R2
set system services ssh root-login allow
set system services telnet
set interfaces ge-0/0/0 description "Link from R2 to R1"
set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.2/30
set interfaces lo0 unit 0 family inet filter input local_acl
set interfaces lo0 unit 0 family inet address 192.168.255.2/32
set firewall family inet filter local_acl term terminal_access from source-address 192.168.1.0/30
set firewall family inet filter local_acl term terminal_access from protocol tcp
set firewall family inet filter local_acl term terminal_access from port ssh
set firewall family inet filter local_acl term terminal_access from port telnet
set firewall family inet filter local_acl term terminal_access then accept
set firewall family inet filter local_acl term terminal_access_denied from protocol tcp
set firewall family inet filter local_acl term terminal_access_denied from port ssh
set firewall family inet filter local_acl term terminal_access_denied from port telnet
set firewall family inet filter local_acl term terminal_access_denied then log
set firewall family inet filter local_acl term terminal_access_denied then reject
set firewall family inet filter local_acl term tcp-estab from protocol tcp
set firewall family inet filter local_acl term tcp-estab from tcp-established
set firewall family inet filter local_acl term tcp-estab then accept
set firewall family inet filter local_acl term default-term then accept
set routing-options static route 192.168.255.1/32 next-hop 192.168.1.1
```

Configure the R1 Device

Step-by-Step Procedure

Follow these steps to configure the R1 device:

1. Configure the interfaces:

```
[edit]
user@R1# set interfaces ge-0/0/0 description "Link from R1 to R2"
user@R1# set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.1/30
user@R1# set interfaces lo0 unit 0 family inet address 192.168.255.1/32
```

2. Configure the host name and static route to the R2 device's loopback address. You also configure Telnet and SSH access:

```
[edit]
user@R1# set system host-name R1
user@R1# set system services ssh root-login allow
user@R1# set system services telnet
user@R1# set routing-options static route 192.168.255.2/32 next-hop 192.168.1.2
```

Verify and Commit the Configuration at the R1 Device

Step-by-Step Procedure

Complete the following steps to verify and commit your candidate configuration at the R1 device:

1. Confirm interface configuration with the `show interfaces` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@R1# show interfaces
ge-0/0/0 {
    description "Link from R1 to R2";
    unit 0 {
        family inet {
            address 192.168.1.1/30;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 192.168.255.1/32;
```

```
        }
    }
}
```

2. Verify the static route used to reach the R2 device's loopback address and that SSH and Telnet access are enabled. Use the `show routing-options` and `show system services` configuration mode commands. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@R1# show routing-options
static {
    route 192.168.255.2/32 next-hop 192.168.1.2;
}
user@R1# show system services
ssh {
    root-login allow;
    }
telnet;
```

3. When satisfied with the configuration on the R1 device, commit your candidate configuration.

```
[edit]
user@R1# commit
```

Configure the R2 Device

Step-by-Step Procedure

Complete the following steps to configure the R2 device. You begin by defining the stateless firewall filter that selectively blocks Telnet and SSH access:

1. Position yourself at the `edit firewall family inet filter` *local_acl* hierarchy:

```
[edit]
user@R2# edit firewall family inet filter local_acl
```

2. Define the filter term *terminal_access*. This term permits Telnet and SSH from the specified source prefix(s):

```
[edit firewall family inet filter local_acl]
user@R2# set term terminal_access from source-address 192.168.1.0/30
user@R2# set term terminal_access from protocol tcp
user@R2# set term terminal_access from port ssh
user@R2# set term terminal_access from port telnet
user@R2# set term terminal_access then accept
```

3. Define the filter term *terminal_access_denied*. This term rejects SSH and Telnet from *all other* source addresses. This term is configured to log matches to the term and to generate an explicit Internet Control Message Protocol (ICMP) destination unreachable response back to the packet's source. See *Firewall Filter Logging Actions* for details on filter logging options.

TIP: You can use the `discard` action to suppress generation of ICMP error messages back to the source. See *Firewall Filter Terminating Actions* for details.

```
[edit firewall family inet filter local_acl]
user@R2# set term terminal_access_denied from protocol tcp
user@R2# set term terminal_access_denied from port ssh
user@R2# set term terminal_access_denied from port telnet
user@R2# set term terminal_access_denied then log
user@R2# set term terminal_access_denied then reject
user@R2# set term default-term then accept
```

4. Optional.

   Define the filter term *tcp-estab*. This term permits outbound access to the Internet to support connections to the Juniper Mist cloud (*tcp-established* is a bit-field match condition, **tcp-flags "(ack | rst)"**, which indicates an established TCP session, but not the first packet of a TCP connection):

```
[edit firewall family inet filter local_acl]
user@R2# set term tcp-estab from protocol tcp
user@R2# set term tcp-estab from tcp-established
user@R2# set term tcp-estab then accept
```

5. Define the filter term *default-term*. This term accepts all other traffic. Recall that Junos OS stateless filters have an implicit *deny* term at their end. The *default-term* overrides this behavior by

terminating the filter with an explicit *accept* action. The termination of the filter results in all other traffic being accepted by the filer.

> **NOTE**: For this example we are allowing all other traffic, but for your network you might want to secure the routing engine. See protecting the routing engine for more information.

```
[edit firewall family inet filter local_acl]
user@R2# set term default-term then accept
```

6. Configure the loopback interface, and apply the filter in the input direction:

```
[edit]
user@R2# set interfaces lo0 unit 0 family inet filter input local_acl
user@R2# set interfaces lo0 unit 0 family inet address 192.168.255.2/32
```

7. Configure the host name, the ge-0/0/0 interface, the static route to the R1 device's loopback address, and enable remote access through SSH and Telnet:

```
[edit]
user@R2# set system host-name R2
user@R2# set system services ssh root-login allow
user@R2# set system services telnet
user@R2# set interfaces ge-0/0/0 description "Link from R2 to R1"
user@R2# set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.2/30
user@R2# set routing-options static route 192.168.255.1/32 next-hop 192.168.1.1
```

Verify and Commit the Configuration at Device R2

Step-by-Step Procedure

Complete the following steps to verify and commit your candidate configuration at the R2 device:

1. Confirm the configuration of the stateless firewall filter with the `show firewall` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@R2# show firewall
family inet {
    filter local_acl {
        term terminal_access {
            from {
                source-address {
                    192.168.1.0/30;
                }
                protocol tcp;
                port [ssh telnet];
            }
            then accept;
        }
        term terminal_access_denied {
            from {
                protocol tcp;
                port [ssh telnet];
            }
            then {
                log;
                reject;
            }
        }
        term default-term {
            then accept;
        }
    }
}
```

2. Confirm interface configuration and filter application with the `show interfaces` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@R2# show interfaces
ge-0/0/0 {
```

```
    description "Link from R2 to R1";
    unit 0 {
        family inet {
            address 192.168.1.2/30;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            filter {
                input local_acl;
            }
            address 192.168.255.2/32;
        }
    }
}
```

3. Verify the static route used to reach the loopback address of the R1 device, and verify that Telnet and SSH access are enabled. Use the `show routing-options` and `show system services` configuration mode commands. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@R2# show routing-options
static {
    route 192.168.255.1/32 next-hop 192.168.1.1;
}
user@R2# show system services
ssh {
    root-login allow;
    }
telnet;
```

4. When satisfied with the configuration on the R2 device, commit your candidate configuration.

TIP: Consider using `commit-confirmed` when making changes that might affect remote access to your device.

```
[edit]
user@R2# commit
```

Verify the Stateless Firewall Filter

IN THIS SECTION

Confirm that the firewall filter to limit Telnet and SSH access is working properly.

Verify Accepted Packets

Purpose

Verify that the firewall filter correctly allows SSH and Telnet when the traffic is sourced from the 192.168.1.0/30 subnet.

Action

1. Clear the firewall log on your router or switch.

```
user@R2> clear firewall log
```

2. From a host at an IP address *within* the 192.168.1.0/30 subnet, use a `ssh` *192.168.255.2* command to verify that you can log in to the device using SSH from an allowed source address. This packet should be accepted, but the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine. You will be prompted to save the SSH host key if this is the first SSH login as *user* between these devices.

NOTE: By default the R1 device will source the SSH traffic from the egress interface used to reach the destination. As a result this traffic is sourced from the 192.168.1.1 address assigned to the R1 device's ge-0/0/0 interface.

```
user@R1>ssh 192.168.255.2
Password:
Last login: Wed Aug 19 09:23:58 2020 from 192.168.1.1
--- JUNOS 20.2R1.10 Kernel 64-bit  JNPR-11.0-20200608.0016468_buil
user@R2>
```

3. Log out of the CLI at the R2 device to close the SSH session.

```
user@R2> exit
logout
Connection to 192.168.255.2 closed.
user@R1>
```

4. From a host at an IP address *within* the 192.168.1.0/30 subnet, use the `telnet` *192.168.255.2* command to verify that you can log in to your router or switch using Telnet from an allowed source address. This packet should be accepted, but the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

```
user@host-A> telnet 192.168.255.2
Trying 192.168.255.2...
Connected to 192.168.255.2.
Escape character is '^]'.
login: user
Password:

--- JUNOS 20.2R1.10 Kernel 64-bit  JNPR-11.0-20200608.0016468_buil
user@R2>
```

5. Log out of the CLI to close the Telnet session to the R2 device.

```
user@R2:~ # exit
Connection closed by foreign host.
```

```
root@R1>
```

6. Use the `show firewall log` command to verify that the firewall log buffer on the R2 device's Packet Forwarding Engine (PFE) *does not* contain any entries with a source address in the 192.168.1.0/30 subnet.

```
user@R2> show firewall log
```

Verify Logged and Rejected Packets

Purpose

Verify that the firewall filter correctly rejects SSH and Telnet traffic that does *not* originate from the 192.168.1.0/30 subnet.

Action

1. Clear the firewall log on your router or switch.

```
user@R2> clear firewall log
```

2. Generate SSH traffic sourced from the loopback address of the R1 device. The source address of this traffic is *outside of* the allowed 192.168.1.0/30 subnet. Use the `ssh` *192.168.255.2* `source` *192.168.255.1* command to verify that you *cannot* log in to the device using SSH from this source address. This packet should be rejected, and the packet header information should be logged in the firewall filter log buffer.

```
user@R1 ssh 192.168.255.2 source 192.168.255.1
ssh: connect to host 192.168.255.2 port 22: Connection refused

root@R1>
```

   The output shows that the SSH connection is rejected. This output confirms that the filter is generating an ICMP error message and that it correctly blocks SSH traffic when sent from a disallowed source address.

3. Generate Telnet traffic sourced from the loopback address of the R1 device. The source address of this traffic is *outside of* the allowed 192.168.1.0/30 subnet. Use the `telnet` *192.168.255.2* `source`

192.168.255.1 command to verify that you *cannot* log in to the device using Telnet from this source address. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the PFE.

```
user@R1> telnet 192.168.255.2 source 192.168.255.1
Trying 192.168.255.2...
telnet: connect to address 192.168.255.2: Connection refused
telnet: Unable to connect to remote host
```

The output shows that the Telnet connection is rejected. This output confirms that the filter is generating an ICMP error message and that it correctly blocks Telnet traffic when sent from a disallowed source address.

4. Use the `show firewall log` command to verify that the firewall log buffer on the R2 device contains entries showing that packets with a source address of 192.168.255.1 were rejected.

```
user@R2> show firewall log
Log :
Time      Filter  Action  Interface     Protocol   Src Addr        Dest Addr
15:17:11  pfe     R       ge-0/0/0.0    TCP        192.168.255.1   192.168.255.2
15:12:04  pfe     R       ge-0/0/0.0    TCP        192.168.255.1   192.168.255.2
```

The output confirms that traffic from the 192.168.255.1 source address matched the filter's *terminal_access_denied* term. The `Action` column displays an `R` to indicate that these packets were rejected. The interface, transport protocol, and source and destination addresses are also listed. These results confirm that the firewall filter is working properly for this example.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.4R1	Starting in Junos OS Release 19.4R1 and Junos OS Release 17.4R3, you can disable either the SSH login password or the challenge-response authentication using the `no-password-authentication` and `no-challenge-response` options at the `[edit system services ssh]` hierarchy level.
19.1R1	Starting in Junos OS Release 19.1R1, we have globally disabled the incoming SFTP connections by default. If desired, you can globally enable incoming SFTP connections by configuring the statement `sftp-server` at the `[edit system services ssh]` hierarchy level

18.3R1	Starting in Junos OS Release 18.3R1, the ssh-dss and ssh-dsa hostkey algorithms are deprecated— rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.
18.3R1	(SRX Series and MX Series only) Starting in Junos OS Release 19.3R1, you can specify the name of the routing instance on which the outbound SSH connectivity needs to be established by including the routing-instance statement at the [edit system services outbound-ssh] hierarchy level:

RELATED DOCUMENTATION

- USB Modems for Remote Management of Security Devices | 278
- Secure Web Access for Remote Management | 300

USB Modems for Remote Management of Security Devices

IN THIS SECTION

Junos OS allows the use of USB modems for remote management on SRX Series Firewall. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. For more information, read this topic.

USB Modem Interface Overview

IN THIS SECTION

Juniper Networks SRX Series Firewalls support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

NOTE: USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550HM devices.

You can configure your device to fail over to a USB modem connection when the primary Internet connection experiences interruption.

A USB modem connects to a device through modem interfaces that you configure. The device applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the device and the modem at the user end of the network.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.

NOTE: Low-latency traffic such as VoIP traffic is not supported over USB modem connections.

NOTE: We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity:

- A physical interface which uses the naming convention `umd0`. The device creates this interface when a USB modem is connected to the USB port.
- A *logical interface* called the dialer interface. You use the dialer interface, `dln`, to configure dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP). You can configure multiple dialer interfaces for different functions on the device. After configuring the dialer interface, you must configure a backup method such as a dialer backup, a dialer filter, or a dialer watch.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface. Dialer pool priority has a range from 1 to 255, with 1 designating the lowest priority interfaces and 255 designating the highest priority interfaces.

Dialer Interface Rules

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- The dialer interface cannot be configured as a constituent link in a multilink bundle.
- The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
  - As a backup interface—for one primary interface
  - As a dialer filter
  - As a dialer watch interface

The backup dialer interfaces are activated only when the primary interface fails. USB modem backup connectivity is supported on all interfaces except lsq-0/0/0.

The dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed. You define an interesting packet using the dialer filter feature of the device. To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route. If the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

How the Device Initializes USB Modems

When you connect the USB modem to the USB port on the device, the device applies the modem AT commands configured in the `init-command-string` command to the initialization commands on the modem.

If you do not configure modem AT commands for the `init-command-string` command, the device applies the following default sequence of initialization commands to the modem: `AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0`. Table 18 on page 281 describes the commands. For more information about these commands, see the documentation for your modem.

Table 18: Default Modem Initialization Commands

Modem Command	Description
`AT`	Attention. Informs the modem that a command follows.
`S7=45`	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
`S0=0`	Disables the auto answer feature, whereby the modem automatically answers calls.
`V1`	Displays result codes as words.
`&C1`	Disables reset of the modem when it loses the carrier signal.
`E0`	Disables the display on the local terminal of commands issued to the modem from the local terminal.
`Q0`	Enables the display of result codes.
`&Q8`	Enables Microcom Networking Protocol (MNP) error control mode.

Table 18: Default Modem Initialization Commands *(Continued)*

Modem Command	Description
%C0	Disables data compression.

When the device applies the modem AT commands in the `init-command-string` command or the default sequence of initialization commands to the modem, it compares them to the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include `S0=0` and the device's `init-command-string` command includes `S0=2`, the device applies `S0=2`.
- If the initialization commands on the modem do not include a command in the device's `init-command-string` command, the device adds it. For example, if the `init-command-string` command includes the command `L2`, but the modem commands do not include it, the device adds `L2` to the initialization commands configured on the modem.

NOTE: On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), keepalives do not get exchanged, and the interface goes down. (Platform support depends on the Junos OS release in your installation.)

USB Modem Configuration Overview

NOTE: USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, and SRX345 devices.

Before you begin:

1. Install device hardware. For more information, see the Getting Started Guide for your device.
2. Establish basic connectivity. For more information, see the Getting Started Guide for your device.
3. Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637 (http://www.usr.com/).
4. Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
5. Connect the USB modem to the device's USB port.

NOTE: When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

a. Plug the modem into the USB port.

b. Connect the modem to your telephone network.

i.

Suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. This example shows you how to establish a backup connection between the branch office and head office routers. See Table 19 on page 283 for a summarized description of the procedure.

Table 19: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity

Router Location	Configuration Requirement	Procedure
Branch Office	Configure the logical dialer interface on the branch office router for USB modem dial backup.	To configure the logical dialer interface, see "Example: Configuring a USB Modem Interface" on page 285.

Table 19: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity *(Continued)*

Router Location	Configuration Requirement	Procedure
	Configure the dialer interface `dl0` on the branch office router using one of the following backup methods: • Configure the dialer interface `dl0` as the backup interface on the branch office router's primary T1 interface `t1-1/0/0`. • Configure a dialer filter on the branch office router's dialer interface. • Configure a dialer watch on the branch office router's dialer interface.	Configure the dialer interface using one of the following backup methods: • To configure `dl0` as a backup for `t1-1/0/0` see *Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup*. • To configure a dialer filter on `dl0`, see *Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup*. • To configure a dialer watch on `dl0`, see *Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup*.
Head Office	Configure dial-in on the dialer interface `dl0` on the head office router.	To configure dial-in on the head office router, see "Example: Configuring a Dialer Interface for USB Modem Dial-In" on page 294.

If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085321091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

See Table 20 on page 285 for a list of available incoming map options.

Table 20: Incoming Map Options

Option	Description
accept-all	Dialer interface accepts all incoming calls. You can configure the `accept-all` option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the `accept-all` option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.
caller	Dialer interface accepts calls from a specific caller ID. You can configure a maximum of 15 caller IDs per dialer interface. The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.

You configure dialer interfaces to support PAP. PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair are repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

Example: Configuring a USB Modem Interface

IN THIS SECTION

This example shows how to configure a USB modem interface for dial backup.

NOTE: USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, and SRX345 devices.

Requirements

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

Overview

In this example, you create an interface called as umd0 for USB modem connectivity and set the dialer pool priority to 25. You also configure a modem initialization string to autoanswer after a specified number of rings. The default modem initialization string is `AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0`. The modem command `S0=0` disables the modem from autoanswering the calls. Finally, you set the modem to act as a dial-in WAN backup interface.

Configuration

IN THIS SECTION

- Procedure | 286

Procedure

CLI Quick Configuration

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

```
set interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
set modem-options init-command-string "ATS0=2 \n" dialin routable
```

Step-by-Step Procedure

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

To configure a USB modem interface for dial backup:

1. Create an interface.

```
[edit]
user@host# edit interfaces umd0
```

2. Set the dialer options and priority.

```
[edit interfaces umd0]
user@host# set dialer-options pool usb-modem-dialer-pool priority 25
```

3. Specify the modem options.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "ATS0=2 \n"
```

4. Set the modem to act as a dial-in WAN backup interface.

```
[edit interfaces umd0]
user@host# set modem-options dialin routable
```

Results

From configuration mode, confirm your configuration by entering the `show interface umd0` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
    user@host# show interface umd0
modem-options {
init-command-string "ATS0=2 \n";
    dialin routable;
}
dialer-options {
    pool usb-modem-dialer-pool priority 25;
}
```

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

Verification

IN THIS SECTION

- Verifying the Configuration | **288**

Confirm that the configuration is working properly.

Verifying the Configuration

Purpose

Verify a USB modem interface for dial backup.

Action

From configuration mode, enter the `show interfaces umd0 extensive` command. The output shows a summary of interface information and displays the modem status.

```
Physical interface:   umd0, Enabled, Physical link is Up
Interface index:      64, SNMP ifIndex: 33, Generation: 1
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
Clocking: Unspecified, Speed: MODEM
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : None
  Hold-times     : Up 0 ms, Down 0 ms
  Last flapped   : Never
  Statistics last cleared: Never
 Traffic statistics:
   Input  bytes  :               21672
   Output bytes  :               22558
   Input  packets:                1782
   Output packets:                1832
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
```

```
Resource errors: 0
  Output errors:
    Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
  MODEM status:
    Modem type                   : LT V.92 1.0 MT5634ZBA-USB-V92 Data/Fax Modem
(Dual Config) Version 2.27m
    Initialization command string : ATS0=2
    Initialization status        : Ok
    Call status                  : Connected to 4085551515
    Call duration                : 13429 seconds
    Call direction               : Dialin
    Baud rate                    : 33600 bps
    Most recent error code       : NO CARRIER

  Logical interface umd0.0 (Index 2) (SNMP ifIndex 34) (Generation 1)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PPP-Subordinate
```

Example: Configuring a Dialer Interface

IN THIS SECTION

This example shows how to configure a logical dialer interface for an SRX300, SRX320, SRX340, or SRX345 device.

Requirements

Before you begin:

- Install device hardware and establish basic connectivity. See the Getting Started Guide for your device.

- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637, from US Robotics (http://www.usr.com/).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the device.
- Order a PSTN line from your telecommunications service provider. Contact your service provider.

Overview

In this example, you configure a logical dialer interface called dl0 to establish USB connectivity. You can configure multiple dialer interfaces for different functions on the device. You add a description to differentiate among different dialer interfaces. For example, this modem is called USB-modem-remote-management. Configure PPP encapsulation and set the logical unit as 0. You then specify the name of the dialer pool as usb-modem-dialer-pool and set the source and destination IP addresses as 172.20.10.2, and 172.20.10.1, respectively.

NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.

NOTE: If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set interfaces dl0 description USB-modem-remote-management  encapsulation ppp
set interfaces dl0 unit 0 dialer-options pool usb-modem-dialer-pool
set interfaces dl0 unit 0 family inet address 172.20.10.2 destination 172.20.10.1
```

Step-by-Step Procedure

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

To configure a logical dialer interface for the device:

1. Create an interface.

```
[edit]
user@host# set interfaces dl0
```

2. Add a description and configure PPP encapsulation.

```
[edit interfaces dl0]
user@host# set description USB-modem-remote-management
user@host# set encapsulation ppp
```

3. Create the logical unit.

NOTE: The logical unit number must be `0`.

```
[edit interfaces dl0]
user@host# set unit 0
```

4. Configure the name of the dialer pool to use for USB modem connectivity.

```
[edit interfaces dl0 unit 0]
user@host# set dialer-options pool usb-modem-dialer-pool
```

5. Configure source and destination IP addresses for the dialer interface.

```
[edit interfaces dl0 unit 0]
user@host# set family inet address 172.20.10.2 destination 172.20.10.1
```

Results

From configuration mode, confirm your configuration by entering the `show interfaces dl0` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces dl0
description USB-modem-remote-management;
    encapsulation ppp;
    unit 0 {
    family inet {
        address 172.20.10.2/32 {
        destination 172.20.10.1;
    }
    }
    dialer-options {
        pool usb-modem-dialer-pool;
    }
}
```

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying a Dialer Interface

Purpose

Verify that the dialer interface has been configured.

Action

From configuration mode, enter the `show interfaces dl0 extensive` command. The output shows a summary of dialer interface information.

```
Physical interface: dl0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed: Unspecified
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : Keepalives
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                13859                    0 bps
   Output bytes  :                    0                    0 bps
   Input  packets:                  317                    0 pps
   Output packets:                    0                    0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

  Logical interface dl0.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
    Description: USB-modem-remote-management
    Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
    Dialer:
      State: Active, Dial pool: usb-modem-dialer-pool
```

```
      Dial strings: 220
      Subordinate interfaces: umd0 (Index 64)
      Activation delay: 0, Deactivation delay: 0
      Initial route check delay: 120
      Redial delay: 3
      Callback wait period: 5
      Load threshold: 0, Load interval: 60
    Bandwidth: 115200
    Traffic statistics:
     Input  bytes  :                24839
     Output bytes  :                17792
     Input  packets:                  489
     Output packets:                  340
    Local statistics:
     Input  bytes  :                10980
     Output bytes  :                17792
     Input  packets:                  172
     Output packets:                  340
    Transit statistics:
     Input  bytes  :                13859                    0 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                  317                    0 pps
     Output packets:                    0                    0 pps
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
  CHAP state: Success
    Protocol inet, MTU: 1500, Generation: 136, Route table: 0
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 172.20.10.1, Local: 172.20.10.2, Broadcast: Unspecified,
Generation: 134
```

Example: Configuring a Dialer Interface for USB Modem Dial-In

IN THIS SECTION

This example shows how to configure a dialer interface for USB modem dial-in.

NOTE: USB modems are no longer supported for dial-in to a dialer interface on SRX300, SRX320, SRX340, and SRX345 devices.

Requirements

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

Overview

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the system matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the system performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

You can configure the following incoming map options for the dialer interface:

- `accept-all`—Dialer interface accepts all incoming calls.

  You can configure the `accept-all` option for only one of the dialer interfaces associated with a USB modem physical interface. The device uses the dialer interface with the `accept-all` option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

- `caller`—Dialer interface accepts calls from a specific caller ID— for example, `4085550115`. You can configure a maximum of 15 caller IDs per dialer interface.

The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.

In this example, you configure the incoming map option as caller 4085550115 for dialer interface dl0.

Configuration

IN THIS SECTION

CLI Quick Configuration

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

```
set interfaces dl0 unit 0 dialer-options incoming-map caller 4085550115
```

Procedure

Step-by-Step Procedure

To configure a dialer interface for USB modem dial-in:

1. Select a dialer interface.

```
[edit]
user@host# edit interfaces dl0
```

2. Configure the incoming map options.

```
[edit]
user@host# edit unit 0 dialer-options incoming-map caller 4085551515
```

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

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

Verification

To verify the configuration is working properly, enter the `show interface dl0` command.

Configuring a Dial-Up Modem Connection Remotely

To remotely connect to the USB modem connected to the USB port on the device, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection remotely:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. Connect the modem to your telephone network.
3. On the PC or laptop computer, select `Start>Settings>Control Panel>Network Connections`. The Network Connections page appearts.
4. Click `Create a new connection`. The New Connection Wizard appears.
5. Click `Next`. The New Connection Wizard: Network Connection Type page appears.
6. Select `Connect to the network at my workplace`, and then click `Next`.

   The New Connection Wizard: Network Connection page appears.
7. Select `Dial-up connection`, and then click `Next`. The New Connection Wizard: Connection Name page appears.
8. In the Company Name box, type the dial-up connection name, for example `USB-modem-connect`. Then, click `Next`. The New Connection Wizard: Phone Number to Dial page appears.
9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the device end.
10. Click `Next` twice, and then click `Finish`. The Connect USB-modem-connect page appears.
11. If CHAP is configured on the dialer interface used for the USB modem interface at the device end, type the username and password configured in the CHAP configuration in the User name and Password boxes.
12. Click `Properties`. The USB-modem-connect Properties page appears.

13. In the Networking tab, select `Internet Protocol (TCP/IP)`, and then click `Properties`. The Internet Protocol (TCP/IP) Properties page appears.
14. Click `Advanced`. The Advanced TCP/IP Settings page appears.
15. Clear the `Use IP header compression` check box.

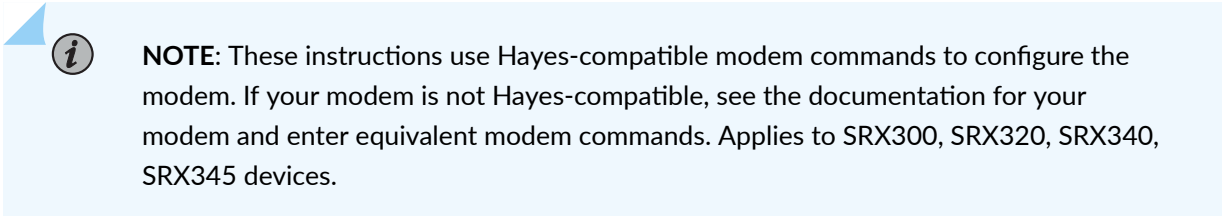
Connecting to the Device Remotely

To remotely connect to the device through a USB modem connected to the USB port on the device:

1. On the PC or laptop computer at your remote location, select `Start>Settings>Control Panel>Network Connections`. The Network Connections page appears.
2. Double-click the `USB-modem-connect` dial-up connection. The Connect USB-modem-connect page appears.
3. Click `Dial` to connect to the Juniper Networks device.

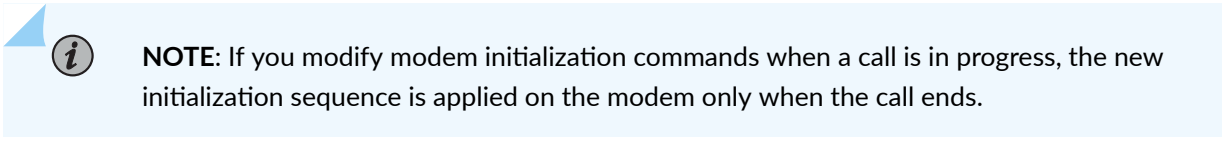
   When the connection is complete, you can use Telnet or SSH to connect to the device.

Modifying USB Modem Initialization Commands



NOTE: These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands. Applies to SRX300, SRX320, SRX340, SRX345 devices.

You can use the CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.



NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.

You can configure the following modem AT commands to initialize the USB modem:

- The command `S0=2` configures the modem to automatically answer calls on the second ring.
- The command `L2` configures medium speaker volume on the modem.

You can insert spaces between commands.

When you configure modem commands in the CLI configuration editor, you must follow these conventions:

- Use the newline character `\n` to indicate the end of a command sequence.
- Enclose the command string in double quotation marks.

You can override the value of the `S0=0` command in the initialization sequence configured on the modem and add the `L2` command.

To modify the initialization commands on a USB modem:

1. Configure the modem AT commands to initialize the USB modem.

```
[edit interfaces umd0]
user@host# set modem-options init-command-string "AT S0=2 L2 \n"
```

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

Resetting USB Modems

For SRX300, SRX320, SRX340, and SRX345 devices, if the USB modem does not respond, you can reset the modem.

CAUTION: If you reset the modem when a call is in progress, the call is terminated.

To reset the USB modem, in operational mode, enter the following command:

```
user@host> request interface modem reset umd0
```

RELATED DOCUMENTATION

User Authentication Overview | 150

USB Modems for Remote Management of Security Devices | 278

Secure Web Access for Remote Management | 300

Secure Web Access for Remote Management

IN THIS SECTION

You can manage a Juniper Networks device remotely through the J-Web interface. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports on the device as needed. Read this topic for information.

Secure Web Access Overview

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

SEE ALSO

Configuring Device Addresses (IPv4 and Loopback Addresses)

Generating SSL Certificates for Secure Web Access (SRX Series Firewalls)

To generate an SSL certificate using the `openssl` command:

1. Enter `openssl` in the CLI. The `openssl` command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the `openssl` command.

   ```
   % openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
   ```

   Replace *filename* with the name of a file in which you want the SSL certificate to be written—for example, `new.pem`.
2. When prompted, type the appropriate information in the identification form. For example, type `US` for the country name.
3. Display the contents of the file `new.pem`.

   ```
   cat new.pem
   ```

   Copy the contents of this file for installing the SSL certificate.

Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following `openssl` command in your SSH command-line interface on a BSD or Linux system on which **openssl** is installed. The `openssl` command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   % openssl req –x509 –nodes –newkey rsa:1024 –keyout *filename*.pem -out *filename*.pem

   where ***filename*** is the name of a file in which you want the SSL certificate to be written—for example, `my-certificate`.
2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file that you created.

   cat my-certificate.pem

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.

You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```

For more information on installing certificates, see "Example: Configuring Secure Web Access" on page 308.

SEE ALSO

Configuring Management Access for the EX Series Switch (J-Web Procedure)

Overview of Port Security

Generating a Self-Signed SSL Certificate Automatically

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

```
user@host> request system reboot
Reboot the system ? [yes,no] yes
```

3. Specify `system-generated-certificate` under HTTPS Web management.

```
[edit]
user@host# show system services web-management https system-generated-certificate
```

Manually Generate Self-Signed SSL Certificates

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.
2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:

```
root@host> request security pki generate-key-pair size 512 certificate-id certname
```

```
Generated key pair sslcert, key size 512 bits
```

```
root@host> request security pki local-certificate generate-self-signed certificate-id cert-name email
email domain-name domain name ip-address IP address subject “DC= Domain name, CN= Common-Name, OU=
Organizational-Unit-name, O= Organization-Name, ST= state, C= Country”
```

```
Self-signed certificate generated and loaded successfully
```

When you generate the certificate, you must specify the subject, e-mail address, and either the domain-name or the IP address.

3. To verify that the certificate was generated and loaded properly, enter the `show security pki local-certificate` operational command and specify `local-certificate` under HTTPS Web management.

```
[edit]
root@host# show system services web-management https local-certificate certname
```

Delete a Certificate

IN THIS SECTION

You can delete a local or trusted CA certificate that is automatically or manually generated.

Use the following command to delete a local certificate.

```
user@host> clear security pki local certificate certificate-id (certificate-id| all | system-
generated )
```

Specify a certificate ID to delete a local certificate with a specific ID. Use `all` to delete all local certificates, or specify `system-generated` to delete the automatically generated self-signed certificate.

When you delete an automatically generated self-signed certificate, the device generates a new one.

To delete a CA certificate, use the following command.

```
user@host> clear security pki ca-certificate ca-profile (ca-profile-name | all)
```

Specify a CA profile to delete a specific CA certificate, or use `all` to delete all CA certificates present in the persistent store.

You are asked for confirmation before a CA certificate can be deleted.

Delete a Loaded CRL

You can choose to delete a loaded CRL if you no longer need to use it to manage certificate revocations and validation.

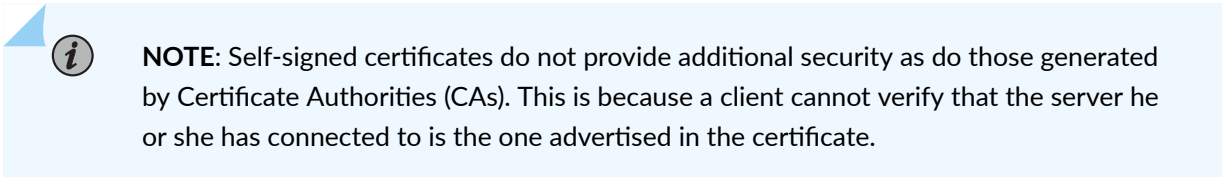
Use the following command to delete a loaded CRL.

```
user@host> clear security pki crl ca-profile (ca-profile all)
```

Specify a CA profile to delete a CRL associated with the CA identified by the profile, or use `all` to delete all CRLs.

Understanding Self-Signed Certificates on EX Series Switches

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.



NOTE: Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.

The switches provide two methods for generating a self-signed certificate:

- Automatic generation

  In this case, the creator of the certificate is the switch. An automatically generated (also called “system-generated”) self-signed certificate is configured on the switch by default.

  After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

  A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a `request system snapshot` command is issued.

  The switch uses the following distinguished name for the automatically generated certificate:

  “ CN=<device serial number>, CN=system generated, CN=self-signed”

  If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- Manual generation

  In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.

Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

Manually Generated Self-Signed Certificates on Switches (CLI Procedure)

IN THIS SECTION

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

Generating a Public-Private Key Pair on Switches

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```

Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.

After the public-private key pair is generated, the switch displays the following:

```
generated key pair certificate-id-name, key size 1024 bits
```

Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id
certificate-id-name domain-name domain-name email email-address ip-address switch-ip-address
subject subject-of-distinguished-name
```

The certificate you have generated is stored in the switch's file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the `show security pki local-certificate` operational command.

Example: Configuring Secure Web Access

IN THIS SECTION

This example shows how to configure secure Web access on your device.

Requirements

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

NOTE: You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.

Overview

IN THIS SECTION

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

Step-by-Step Procedure

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

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

```
[edit security]
user@host# set certificates local new load-key-file /var/tmp/new.pem
```

2. Enable HTTPS access and specify the SSL certificate and port.

```
[edit system]
user@host# set services web-management https local-certificate new port 8443
```

Results

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

```
[edit]
user@host# show security
certificates {
    local {
        new {
            "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQC/C5UI4frNqbi
qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY Y5rCXLf4+2s8k9EypLtYRw/
Ts66DZoXI4viqE7HSsK\n5sQw/UDBIw7/MJ+OpA ... KYiFf4CbBBbjlMQJ0HFudW6ISVBslONkzX+FT
\ni95ddka6iIRnArEb4VFCRh+ e1QBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
CERTIFICATE----- \nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ... FADCBkTELMAkGA1UEBhMCdXMx
\nCzAJBgNVBAgTAmNhMRIwEAYDVQQHEwlzdW5ue HB1YnMxDTALBgNVBAMTBGpucHIxJDAiBgkqhkiG
\n9w0BCQEWFW5iaGFyZ2F2YUB fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
        }
    }
}
```

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

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying an SSL Certificate Configuration

Purpose

Verify the SSL certificate configuration.

Action

From operational mode, enter the `show security` command.

Verifying a Secure Access Configuration

Purpose

Verify the secure access configuration.

Action

From operational mode, enter the `show system services` command. The following sample output displays the sample values for secure Web access:

```
[edit]
user@host# show system services
web-management {
    http;
    https {
        port 8443;
        local-certificate new;
```

```
    }
}
```

RELATED DOCUMENTATION

- Remote Access Overview | 240
- User Authentication Overview | 150

Example: Control Management Access on Juniper Networking Devices

IN THIS SECTION

NOTE: Our content testing team has validated and updated this example.

This example shows how to limit management access to Juniper Networking devices based on a specific set of allowed IP addresses. This type of functionality is often referred to as an access control list (ACL), and is implemented as a stateless firewall filter in the Junos OS.

Requirements

A Juniper networking device connected to a management network. To help validate the configuration there should be at least one other device with access to the management network that can initiate SSH or Telnet connections to the device under test (DUT). No special configuration beyond basic device

initialization (management interface and related static route, system services, user login accounts, and so on), is required before you configure this example.

Overview

IN THIS SECTION

You can configure a firewall filter to limit the IP addresses that can manage a device. This firewall filter must include a term to deny all traffic except the IP addresses that are allowed to manage the device. You must apply the firewall filter to the loopback interface (lo0) to ensure that only management traffic, that is, traffic sent to the device itself, is filtered.

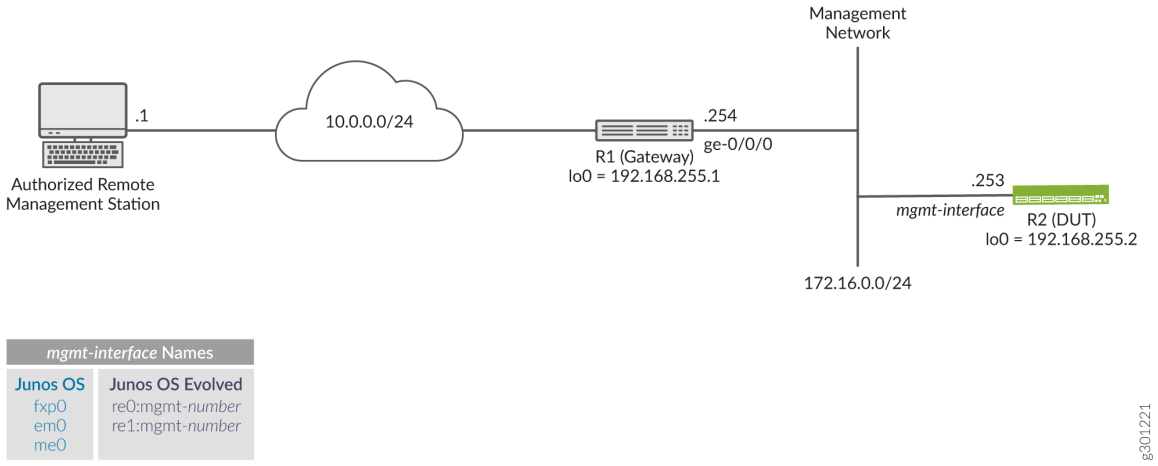
Example Topology

Figure 6 on page 314 shows the topology for this example. The R1 device serves as the default gateway for the management network that is assigned the 172.16.0.0/24 subnet. You apply the filter that limits management access to the R2 device, making it the DUT in this example. The remote workstation is authorized to manage the DUT and has been assigned the 10.0.0.1/32 address.

In this example you:

- Configure a prefix-list called *manager-ip*. This list defines the set of IP addresses that are allowed to manage the device. In this example the list includes the management subnet itself (172.16.0.0/24), and the IP address of an authorized remote user (10.0.0.1/32).
- Configure a firewall filter *limit-mgmt-access* that rejects all source addresses *except* the specific set of addresses defined in the *manager-ip* prefix list. This ensures that only IP addresses listed in the prefix list can manage the device.
- Apply the *limit-mgmt-access* filter to the loopback interface. Any time a packet addressed to the local device arrives on any interface, the loopback interface applies the filter *limit-mgmt-access* to limit management access to only allowed addresses.

Figure 6: Example Network Topology



Configure an IP Address List to Restrict Management Access to a Device

IN THIS SECTION

- Procedure | 314

Procedure

CLI Quick Configuration

To quickly configure this example, edit the following commands as needed and paste them into the CLI of the R2 device at the `[edit]` hierarchy level. For completeness the configuration includes commands to configure SSH (for non- users) and the Telnet system services. It also provides the configuration of the management interface and related static route. These commands are not needed if your device already has this functionality configured.

NOTE: Telnet does not support root login on Juniper Networks devices. SSH login for the root user is not configured in this example. Your device should have a non-root user

configured to permit remote login. Alternatively, you can add the `root-login allow` argument to the `system services ssh` statement to permit root user login using SSH.

Be sure to issue a `commit` from configuration mode to activate the changes.

TIP: When applying a filter that restricts access to the device, consider using `commit confirmed`. This option automatically rolls back the configuration if you are unable to issue another commit in the specified time.

```
set system services ssh
set system services telnet
set interfaces fxp0 unit 0 family inet address 172.16.0.253/24
set interfaces lo0 unit 0 family inet address 192.168.255.2/32
set routing-options static route 0.0.0.0/0 next-hop 172.16.0.254 no-readvertise
set policy-options prefix-list manager-ip 172.16.0.0/24
set policy-options prefix-list manager-ip 10.0.0.1/32
set firewall filter limit-mgmt-access term block_non_manager from source-address 0.0.0.0/0
set firewall filter limit-mgmt-access term block_non_manager from source-prefix-list manager-ip
except
set firewall filter limit-mgmt-access term block_non_manager from protocol tcp
set firewall filter limit-mgmt-access term block_non_manager from destination-port ssh
set firewall filter limit-mgmt-access term block_non_manager from destination-port telnet
set firewall filter limit-mgmt-access term block_non_manager then log
set firewall filter limit-mgmt-access term block_non_manager then discard
set firewall filter limit-mgmt-access term accept_everything_else then accept
set interfaces lo0 unit 0 family inet filter input limit-mgmt-access
```

Step-by-Step Procedure

The following steps require you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Configure the management and loopback interfaces and ensure that the Telnet and SSH system services are enabled.

```
[edit]
user@R2# set interfaces fxp0 unit 0 family inet address 172.16.0.253/24
user@R2# set interfaces lo0 unit 0 family inet address 192.168.255.2/32
user@R2# set routing-options static route 0.0.0.0/0 next-hop 172.16.0.254 no-readvertise
```

```
user@R2# set system services ssh
user@R2# set system services telnet
```

2. Define the set of allowed host addresses in the prefix list. This list includes prefixes for the management subnet and for a single authorized remote management station.

```
[edit policy-options]
user@R2# set prefix-list manager-ip 172.16.0.0/24
user@R2# set prefix-list manager-ip 10.0.0.1/32
```

The prefix list is referenced in the firewall filter. Using a prefix list makes it easy to update the addresses that are permitted to access the device. This is because only the prefix list needs to be updated. No edits are required to the firewall filter itself when adding or removing allowed prefixes.

3. Configure a firewall filter to deny Telnet and SSH traffic from all IP addresses *except* those defined in the prefix list.

```
[edit firewall filter limit-mgmt-access]
user@R2# set term block_non_manager from source-address 0.0.0.0/0
user@R2# set term block_non_manager from source-prefix-list manager-ip except
user@R2# set term block_non_manager from protocol tcp
user@R2# set term block_non_manager from destination-port ssh
user@R2# set term block_non_manager from destination-port telnet
user@R2# set term block_non_manager then discard
```

Note the use of the `except` action modifier. The first term matches on all possible source addresses. The next term inverts the match for those source addresses in the specified prefix list. The result is that management traffic destined to the specified protocol and ports is only accepted when the traffic comes from an address in the list. Traffic from all other source prefixes to the same combination of protocol and ports is discarded. In this example a logging action is added to assist in filter debugging and verification.

4. Configure a default term to accept all other traffic. This ensures that other services and protocols, for example pings, BGP, or OSPF, are not affected by the filter.

TIP: The example filter is permissive by design. It can represent a security threat given it explicitly accepts all traffic that has not been rejected or discarded by previous filter terms. You can configure a stronger security filter by explicitly listing all protocols and services that should be accepted ending the filter with a deny all term, either implicitly

or explicitly, to filter all other traffic. The drawback to a restrictive filter is it must be edited each time a supported service is added or removed.

```
[edit firewall filter imit-mgmt-access]
user@R2# set term accept_everything_else then accept
```

5. Apply the stateless firewall filter to the loopback interface as an input filter. Traffic sent from the local device is not filtered in this example.

```
[edit interfaces lo0 unit 0 ]
user@R2# set family inet filter input limit-mgmt-access
```

Results

Confirm your work by entering the following `show configuration` commands from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@R2# show policy-options
prefix-list manager-ip {
    172.16.0.0/24;
    10.0.0.1/32;
}
```

```
user@R2# show firewall
filter limit-mgmt-access {
    term block_non_manager {
        from {
            source-address {
                0.0.0.0/0;
            }
            source-prefix-list {
                manager-ip except;
            }
            protocol tcp;
            destination-port [ ssh telnet ];
        }
        then {
```

```
            log;
            discard;
        }
    }
    term accept_everything_else {
        then accept;
    }
}
```

```
user@R2# show interfaces
fxp0 {
    unit 0 {
        family inet {
            address 172.16.0.253/24;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            filter {
                input limit-mgmt-access;
            }
            address 192.168.255.2/32;
        }
    }
}
```

```
user@R2# show routing-options
static {
    route 0.0.0.0/0 {
        next-hop 172.16.0.254;
        no-readvertise;
```

```
    }
}
```

```
user@R2# show system services
ssh;
telnet;
```

When satisfied with your work enter `commit` from configuration mode.

TIP: When applying a filter that restricts access to the device, consider using `commit confirmed`. This option automatically rolls back the configuration if you are unable to issue another commit in the specified time.

Verify the Stateless Firewall Filter

IN THIS SECTION

Confirm that the firewall filter to limit management access is working properly.

Verify Accepted Packets

Purpose

Verify that the firewall filter correctly allows SSH and Telnet when the traffic is sourced from the 172.16.0.0/24 subnet or from the 10.0.0.1 host prefix associated with the remote management station.

Action

1. Clear the firewall log on your router or switch.

```
user@R2> clear firewall log
```

2. From a host attached *to* the 172.16.0.0/24 subnet, such as the R1 device, use the `ssh` *`172.16.0.253`* command to initiate a connection to the DUT. By default the R1 device sources it's traffic from the egress interface used to reach the destination. As a result the test traffic is sourced from R1's 172.16.0.254 address. This traffic does not match the *block_non_manager* filter term because of the `except` action modifier for addresses that match the referenced prefix list. This traffic matches the *accept_everything_else* filter term causing it to be accepted

NOTE: You will be prompted to save the SSH host key if this is the first SSH login as *user* between these devices.

```
user@R1>ssh user@172.16.0.253
Password:
Last login: Tue Sep  8 09:46:58 2020 from 10.107.199.39
--- JUNOS 20.2R1.10 Kernel 64-bit XEN JNPR-11.0-20200608.0016468_buil
user@R2>
```

3. Logout out of the CLI at the R2 device to close the SSH session.

```
user@R2> exit
logout
Connection to 172.16.0.253 closed.
user@R1>
```

NOTE: Repeat this step using the `telnet` command. The Telnet connection should succeed.

4. Use the `show firewall log` command at the R2 device to verify that the firewall log buffer on the R2 device *does not* contain entries with a source address in the 172.16.0.0/24 subnet. This means the

packet header information for this traffic is *not* logged in the firewall filter log. Only traffic that matches the *block_non_manager* term is logged in this example.

```
user@R2> show firewall log
user@R2>
```

Meaning

The output confirms that SSH (and Telnet) connections are accepted when sourced from the management network. It also shows that packets which don't match the *block_non_manager* term are not logged. The same results are expected if the SSH or Telnet traffic is generated by the remote management station that is assigned the 10.0.0.1 address.

Verify Logged and Rejected Packets

Purpose

Verify that the firewall filter correctly discards SSH and Telnet traffic that does *not* originate from one of the prefixes in the *manager-ip* prefix list.

Action

1. Generate SSH traffic sourced from an address that is not specified in the *manager-ip* prefix list. You can source the session from the R1 device's loopback address to simulate a non-authorized IP. Alternatively, initiate the connection from any remote device that is not connected to the management subnet, and which has not been assigned an IP address of 10.0.0.1. The packets for this SSH session should be discarded, and the packet header information should be logged in the firewall filter log buffer.

   NOTE: You should not expect any error message or reply. The connection attempt will time-out. This is because the sample filter uses a `discard` rather than a `reject` action.

   ```
   user@unauthorized-remote-host ssh user@172.16.0.253
   ssh: connect to host 172.16.0.253 port 22: Connection timed out
   ```

   The output shows the SSH connection does not succeed. This confirms the filter correctly blocks SSH traffic when sent from a disallowed source address. The same result is expected for Telnet sessions initiated by any non-authorized IP source address.

2. Use the `show firewall log` command to verify that the firewall log buffer on the R2 device now contains entries for packets with a non-authorized source address.

```
user@R2> show firewall log
Log :
Time      Filter    Action Interface       Protocol     Src Addr         Dest Addr
11:35:46  limit-mgmt-access D fxp0.0       TCP          10.0.0.119       172.16.0.253
11:35:14  limit-mgmt-access D fxp0.0       TCP          10.0.0.119       172.16.0.253
11:34:58  limit-mgmt-access D fxp0.0       TCP          10.0.0.119       172.16.0.253
```

Meaning

The output confirms that traffic from the 10.0.0.119 source address has matched a logging term in the *limit-mgmt-access* filter. Recall that only the *block_non_manager* term has a log action in this example. The `Action` column displays a `D` to indicate the packets were discarded. The ingress interface for the filtered traffic is confirmed to be the management port `fxp0.0` on the device. The transport protocol `TCP` and IP addresses of the filtered packets are also shown. Note that the source address `10.0.0.119` for this traffic is not listed in the *manager-ip* prefix list.

These results confirm the firewall filter is working properly for this example.

Configuration Guidelines for Securing Console Port Access

IN THIS SECTION

We recommend that you (the network administrator) disable the console port to prevent unauthorized access to the device.

Secure the Console Port

You can use the console port on a device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:

- Log out of the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to the console. This action prevents a non-root user from performing password recovery operation using the console.
- Disable the console port. We recommend that you disable the console port to prevent unauthorized access to the device. Preventing unauthorized access is especially important when the device is used as customer premises equipment (CPE) and is forwarding sensitive traffic.

> **NOTE**: It is not always possible to disable the console port, because console access is important during operations such as software upgrades.

> **WARNING**: On SRX300, SRX320, SRX340, and SRX345 devices, if you configure both the `set system ports console insecure` and `set chassis routing-engine bios uninterrupt` options, there is no alternative recovery method available if Junos OS fails to boot.

To secure the console port:

1. Do one of the following:
   - Disable the console port.

```
[edit system ports console]
user@host# set disable
```

   - Disable root login connections to the console.

```
[edit system ports console]
user@host# set insecure
```

> **NOTE**: After you configure the console port as insecure, if a user tries to perform the password recovery operation by booting in recovery mode, the device will

prompt for the root password. This way, only a user who knows the root password will be able to log in to recovery mode for password recovery.

- Log out of the console session when the serial cable connected to the console port is unplugged. Enter

```
[edit system ports console]
user@host# set log-out-on-disconnect
```

NOTE: The `log-out-on-disconnect` statement is not operational on SRX1500, SRX4100, SRX4200, or SRX4600 devices; on these devices, you must manually log out of the console with the `request system logout` command.

2. After you configure the device, enter `commit` in configuration mode.

Secure Mini-USB Ports

SRX320, SRX320, SRX340, and SRX345 devices have a mini-USB Type-B port. You can connect your management device to the Mini-USB Type-B console port for CLI management.

You can disable mini-USB ports on the SRX Series Firewalls to block users from connecting a USB mass storage device to the services gateway. When you disable the mini-USB port on the device, any transactions in progress on the USB device are terminated.

Use the following command to disable mini-USB ports:

```
[edit]
user@host#  set chassis usb storage disable
```

Use the following command to enable mini-USB ports:

```
[edit]
user@host# delete chassis usb storage disable
```

This action re-enables the disabled mini-USB ports.

Use the `show` command to verify the status of the mini-USB:

```
user@host> show chassis usb storage
```

The output displays the current status of the USB mass storage device and indicates whether the USB ports are enabled or disabled.

Configuring the Console Port Type (CLI Procedure)

Some devices have two console ports: an RJ-45 console port and a Mini-USB Type-B console port. You can configure and manage the device using either port. To connect to the device using a passive port, you must first configure the port as active and then reboot the device.

When a console port is active, it can display all the early boot and low-level message output. You can access the device through this port in the debugger prompt. On some devices, only one console port is active at a time and the console input is active only on that port. Check the hardware guide for your particular device for whether both ports can be active at the same time.

The RJ-45 console port is the active port by default. To activate the Mini-USB Type-B console port:

1. Connect the host machine to the device directly using the active console port or remotely using the management interface. To connect using the active console port, which is the RJ-45 console port by default, see *Connect a Device to a Management Console Using an RJ-45 Connector*.
2. Connect to your device using the Mini-USB Type-B console port. See the hardware guide for your particular device for how to connect to the port.
3. Configure the port type as `mini-usb`:

   ```
   [edit]
   user@switch# set system ports auxiliary port-type mini-usb
   ```

4. Commit the configuration and `Exit`. The initial logs will show the Mini-USB Type-B console port as active.
5. Reboot the switch. The boot log appears on the activated console. If your device supports both ports being active at the same time, both ports are now active and can be used as console ports.

NOTE: Do not use the `delete system ports auxiliary port-type` command to delete the port-type configuration. Always use the `set system ports auxiliary port-type` *type* command to change the active management console port type.

To configure the RJ-45 console port as the active port, use the same procedure with the `set system ports auxiliary port-type rj45` command.

RELATED DOCUMENTATION

- *Connect a Device to a Management Console Using an RJ-45 Connector*
- *Connect an EX Series Switch to a Management Console Using the Mini-USB Type-B Console Port*
- Connecting an MX150 to a Management Console Using Mini-USB Type-B Console Port
- Connecting an NFX250 Device to a Management Console Using Mini-USB Type-B Console Port
- Connecting an OCX1100 Switch to a Management Console by Using the Mini-USB Type-B Console Port

CHAPTER 7

Access Control

IN THIS CHAPTER

Access Control Authentication Methods

IN THIS SECTION

You can control access to your network through a device by using several different authentication. Junos OS devices support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. Read this topic for more information.

Authentication Overview

IN THIS SECTION

You can control access to your network through a Juniper Networks device by using authentication methods such as 802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. For captive portal authentication, the device allows the end devices to acquire an IP address in order to redirect them to a login page for authentication.

802.1X Authentication

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN. The 802.1X authentication feature is based upon the IEEE 802.1X standard *Port-Based Network Access Control*.

The communication protocol between the end device and the device is Extensible Authentication Protocol over LAN (EAPoL). EAPoL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the device is RADIUS.

During the authentication process, the device completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic and control traffic can transit the network. Other traffic, such as DHCP traffic and HTTP traffic, is blocked at the data link layer.

NOTE: You can configure both the maximum number of times an EAPoL request packet is retransmitted and the timeout period between attempts. For information, see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378.

An 802.1X authentication configuration for a LAN contains three basic components:

Supplicant **(also called end device)**

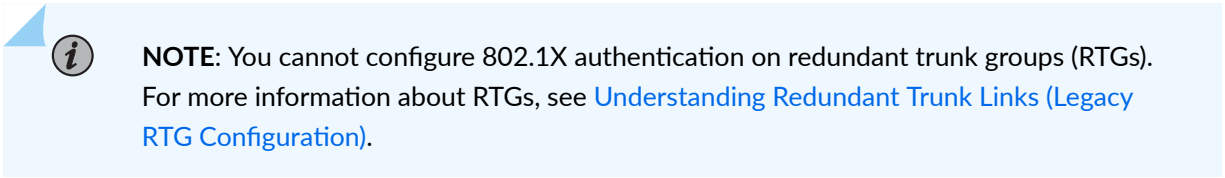
Supplicant is the IEEE term for an end device that requests to join the network. The end device can be responsive or nonresponsive. A responsive end device is 802.1X-enabled and provides authentication credentials using EAP. The credentials required depend on the version of EAP being used—specifically, a username and password for EAP MD5 or a username and client certificates for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected EAP (PEAP).

You can configure a server-reject VLAN to provide limited LAN access for responsive 802.1X-enabled end devices that sent incorrect credentials. A server-reject VLAN can provide a remedial connection, typically only to the Internet, for these devices. See Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients for additional information.

NOTE: If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is dropped.

A nonresponsive end device is one that is not 802.1X-enabled. It can be authenticated through MAC RADIUS authentication.

Authenticator port access entity	The IEEE term for the authenticator. The device is the authenticator, and it controls access by blocking all traffic to and from end devices until they are authenticated.
Authentication server	The authentication server contains the backend database that makes authentication decisions. It contains credential information for each end device that is authenticated to connect to the network. The authenticator forwards credentials supplied by the end device to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied.



NOTE: You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information about RTGs, see Understanding Redundant Trunk Links (Legacy RTG Configuration).

MAC RADIUS Authentication

The 802.1X authentication method only works if the end device is 802.1X-enabled, but many single-purpose network devices such as printers and IP phones do not support the 802.1X protocol. You can configure MAC RADIUS authentication on interfaces that are connected to network devices that do not support 802.1X and for which you want to allow to access the LAN. When an end device that is not 802.1X-enabled is detected on the interface, the device transmits the MAC address of the device to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the end device is authenticated.

You can configure both 802.1X and MAC RADIUS authentication methods on the interface. In this case, the device first attempts to authenticate the end device by using 802.1X, and if that method fails, it attempts to authenticate the end device by using MAC RADIUS authentication. If you know that only non-responsive supplicants connect on that interface, you can eliminate the delay that occurs for the device to determine that the end device is not 802.1X-enabled by configuring the `mac-radius restrict` option. When this option is configured, the device does not attempt to authenticate the end device through 802.1X authentication but instead immediately sends a request to the RADIUS server for authentication of the MAC address of the end device. If the MAC address of that end device is configured as a valid MAC address on the RADIUS server, the device opens LAN access to the end device on the interface to which it is connected.

The `mac-radius-restrict` option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. If you configure `mac-radius-restrict` on an interface, the device drops all 802.1X packets.

The authentication protocols supported for MAC RADIUS authentication are EAP-MD5, which is the default, Protected EAP (EAP-PEAP), and Password Authentication Protocol (PAP). You can specify the

authentication protocol to be used for MAC RADIUS authentication using the `authentication-protocol` statement.

Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) enables you to authenticate users by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database by using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Junos OS provides a template that enables you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time an end device connected to a captive portal interface attempts to access a webpage, the device presents the captive portal login page. After the device is successfully authenticated, it is allowed access to the network and to continue to the original page requested.

NOTE: If HTTPS is enabled, HTTP requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the end device is returned to the HTTP connection.

If there are end devices that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC addresses to an authentication whitelist.

When a user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the device.

Captive portal has the following limitations:

-
  - Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
  - If the user remains idle for more than about 5 minutes and there is no traffic passed, the user must log back in to the captive portal.

Static MAC Bypass of Authentication

You can allow end devices to access the LAN without authentication on a RADIUS server by including their MAC addresses in the static MAC bypass list (also known as the exclusion list).

You might choose to include a device in the bypass list to:

- Allow non-802.1X-enabled devices access to the LAN.

- Eliminate the delay that occurs for the device to determine that a connected device is a non-802.1X-enabled host.

When you configure static MAC, the MAC address of the end device is first checked in a local database (a user-configured list of MAC addresses). If a match is found, the end device is successfully authenticated and the interface is opened up for it. No further authentication is done for that end device. If a match is not found and 802.1X authentication is enabled on the device, the device attempts to authenticate the end device through the RADIUS server.

For each MAC address, you can also configure the VLAN to which the end device is moved or the interfaces on which the host connects.

NOTE: When you clear the learned MAC addresses from an interface, using the `clear dot1x interface` command, all MAC addresses are cleared, including those in the static MAC bypass list.

Fallback of Authentication Methods

You can configure 802.1X, MAC RADIUS, and captive portal authentication on a single interface to enable fallback to another method if authentication by one method fails. The authentication methods can be configured in any combination, except that you cannot configure both MAC RADIUS and captive portal on an interface without also configuring 802.1X. By default, most devices use the following order of authentication methods:

1. 802.1X authentication—If 802.1X is configured on the interface, the device sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the device checks whether MAC RADIUS authentication is configured on the interface.

2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the device sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the device checks whether captive portal is configured on the interface.

3. Captive portal authentication—If captive portal is configured on the interface, the device attempts to authenticate the end device by using this method after the other authentication methods configured on the interface have failed.

For an illustration of the default process flow when multiple authentication methods are configured on an interface, see Understanding Access Control on Switches.

You can override the default order for fallback of authentication methods by configuring the authentication-order statement to specify that the device use either 802.1X authentication or MAC

RADIUS authentication first. Captive portal must always be last in the order of authentication methods. For more information, see Configuring Flexible Authentication Order.

NOTE: If an interface is configured in multiple-supplicant mode, end devices connecting through the interface can be authenticated using different methods in parallel. Therefore, if an end device on the interface was authenticated after fall back to captive portal, then additional end devices can still be authenticated using 802.1X or MAC RADIUS authentication.

RELATED DOCUMENTATION

802.1X Authentication | 369

802.1X and RADIUS Accounting | 444

MAC RADIUS Authentication | 432

Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot

IN THIS SECTION

Junos OS allows you to configure anattended mode for U-Boot to prevent unauthorized access to the switch during the boot process. When you configure unattended mode, an user can access the CLI during the boot process by supplying the boot-loader password. This prevents unauthorized access during boot process. Read this topic for more information.

Understanding Unattended Mode for U-Boot on EX Series Switches

Unattended mode for U-Boot can be configured to prevent unauthorized access to the switch that can occur during the boot process. After the CPU has been reset, there are several known methods of accessing the system before the JUNOS OS login prompt appears that do not require the user to enter authorization credentials. By gaining unauthorized access, the user can view, modify, or corrupt the switch configuration, or make the switch unavailable on the network.

When unattended mode is configured, the user can access the CLI during the boot process only by pressing <Ctrl+c> and entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch. Entering the correct boot-loader password will place the user in the U-Boot CLI. If the password is incorrect, or if no password is entered within one minute, access to the U-Boot CLI is blocked and the boot process continues automatically.

Access to the bootstrap loader command prompt (`loader>`) is blocked in unattended mode, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see *Reverting to the Default Factory Configuration for the EX Series Switch*.

If unattended mode is not configured, but a boot-loader password has been configured, the user must enter the correct password to access the U-Boot CLI. If a boot-loader password has not been configured, the user can access the U-Boot CLI without entering a password. In either case, the user can access the bootstrap loader command prompt, which enables root password recovery by using single-user mode as well as booting from a USB flash drive.

Unattended mode is not enabled by default. When configured, unattended mode is turned on and will block unauthorized access to the switch. Table 21 on page 336 summarizes the behaviors for U-Boot mode.

Table 21: Unattended Mode Behavior

Unattended Mode	Boot-loader password	Behavior
On	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.
On	Not Set	• Access to U-Boot CLI is blocked. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.
Off	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.
Off	Not Set	• Access to U-Boot CLI is allowed. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.

SEE ALSO

Root Password | 114

Using Unattended Mode for U-Boot to Prevent Unauthorized Access

IN THIS SECTION

Unattended mode for U-Boot can be used to prevent unauthorized access to the switch that can occur during the boot process. When unattended mode is configured, the user can access the CLI during the boot process only by entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch.

When unattended mode is configured, access to the bootstrap loader command prompt (`loader>`) is blocked, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

WARNING: On EX2200 switches, if both the root and unattended mode password are lost while the switch is in unattended mode, there is no alternative recovery method available. The switch must be returned to Juniper Networks. For more information, see Returning an EX2200 Switch or Component for Repair or Replacement.

To use unattended mode, follow the following procedures:

Configuring the Boot Loader Password

To configure the boot loader password, you can use either a plain-text password that the system encrypts for you, or a password that has already been encrypted. If you use a plain-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. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

To configure the boot-loader password:

1. Enter either a plain-text password or an encrypted password by using the `set system boot-loader authentication` command.

- To enter a plain-text password, use the `plain-text-password` option, and re-enter the password when prompted:

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

- To enter a password that is already encrypted, use the `encrypted-password` option:

```
[edit]
root@# set system boot-loader-authentication encrypted-password password
```

2. Commit the changes.

```
[edit]
root@# commit
```

3. To view the encrypted password entries, use the configuration mode `show` command. For example:

```
[edit]
root@# show system boot-loader-authentication
encrypted-password “$ABC123”; ## SECRET-DATA
```

Configuring Unattended Mode for U-Boot

Before enabling unattended mode for U-Boot, you must download and install the jloader firmware package **/volume/build/junos/13.2/service/13.2X51-D20.2/ship/jloader-ex-2200-13.2X51-D20.2-signed.tgz**, as described in TSB16425.

Unattended mode for U-Boot is not enabled by default. Use the following procedure to configure unattended mode:

1. Configure unattended mode.

```
[edit]
root@# set system unattended-boot
```

2. Commit the changes.

```
[edit]
root@# commit
```

Accessing the U-Boot CLI

When unattended mode for U-Boot is configured and the boot-loader password has been set, you can access the U-Boot CLI during the boot process by pressing <Ctrl+c> and entering the password at the prompt:

```
Press Ctrl-C in next 1 seconds to enter u-boot prompt...
Enter password:
password correct...
=>
```

The correct password must be entered within one minute after the prompt appears. If the password is not entered within one minute, or if the password is incorrect or has not been configured, access to the U-Boot CLI will be blocked, and the boot process will continue. For more information about unattended mode behavior, see "Understanding Unattended Mode for U-Boot on EX Series Switches" on page 335.

RELATED DOCUMENTATION

unattended-boot

boot-loader-authentication

RELATED DOCUMENTATION

Access Control and Authentication on Switching Devices

Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot

IN THIS SECTION

Junos OS allows you to configure anattended mode for U-Boot to prevent unauthorized access to the switch during the boot process. When you configure unattended mode, an user can access the CLI during the boot process by supplying the boot-loader password. This prevents unauthorized access during boot process. Read this topic for more information.

Understanding Unattended Mode for U-Boot on EX Series Switches

Unattended mode for U-Boot can be configured to prevent unauthorized access to the switch that can occur during the boot process. After the CPU has been reset, there are several known methods of accessing the system before the JUNOS OS login prompt appears that do not require the user to enter authorization credentials. By gaining unauthorized access, the user can view, modify, or corrupt the switch configuration, or make the switch unavailable on the network.

When unattended mode is configured, the user can access the CLI during the boot process only by pressing <Ctrl+c> and entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch. Entering the correct boot-loader password will place the user in the U-Boot CLI. If the password is incorrect, or if no password is entered within one minute, access to the U-Boot CLI is blocked and the boot process continues automatically.

Access to the bootstrap loader command prompt (`loader>`) is blocked in unattended mode, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see *Reverting to the Default Factory Configuration for the EX Series Switch*.

If unattended mode is not configured, but a boot-loader password has been configured, the user must enter the correct password to access the U-Boot CLI. If a boot-loader password has not been configured, the user can access the U-Boot CLI without entering a password. In either case, the user can access the bootstrap loader command prompt, which enables root password recovery by using single-user mode as well as booting from a USB flash drive.

Unattended mode is not enabled by default. When configured, unattended mode is turned on and will block unauthorized access to the switch. Table 21 on page 336 summarizes the behaviors for U-Boot mode.

Table 22: Unattended Mode Behavior

Unattended Mode	Boot-loader password	Behavior
On	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.
On	Not Set	• Access to U-Boot CLI is blocked. • Access to loader command prompt is blocked. • Booting from USB is blocked. • Root password recovery by using single-user mode is blocked.

Table 22: Unattended Mode Behavior *(Continued)*

Unattended Mode	Boot-loader password	Behavior
Off	Set	• Access to U-Boot CLI is allowed only after entering correct password. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.
Off	Not Set	• Access to U-Boot CLI is allowed. • Access to loader command prompt is allowed. • Booting from USB is allowed. • Root password recovery by using single-user mode is allowed.

SEE ALSO

Root Password | 114

Using Unattended Mode for U-Boot to Prevent Unauthorized Access

IN THIS SECTION

Unattended mode for U-Boot can be used to prevent unauthorized access to the switch that can occur during the boot process. When unattended mode is configured, the user can access the CLI during the boot process only by entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch.

When unattended mode is configured, access to the bootstrap loader command prompt (`loader>`) is blocked, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

WARNING: On EX2200 switches, if both the root and unattended mode password are lost while the switch is in unattended mode, there is no alternative recovery method available. The switch must be returned to Juniper Networks. For more information, see Returning an EX2200 Switch or Component for Repair or Replacement.

To use unattended mode, follow the following procedures:

Configuring the Boot Loader Password

To configure the boot loader password, you can use either a plain-text password that the system encrypts for you, or a password that has already been encrypted. If you use a plain-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. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

To configure the boot-loader password:

1. Enter either a plain-text password or an encrypted password by using the `set system boot-loader authentication` command.
   - To enter a plain-text password, use the `plain-text-password` option, and re-enter the password when prompted:

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

   - To enter a password that is already encrypted, use the `encrypted-password` option:

     ```
     [edit]
     root@# set system boot-loader-authentication encrypted-password password
     ```

2. Commit the changes.

```
[edit]
root@# commit
```

3. To view the encrypted password entries, use the configuration mode `show` command. For example:

```
[edit]
root@# show system boot-loader-authentication
encrypted-password “$ABC123”; ## SECRET-DATA
```

Configuring Unattended Mode for U-Boot

Before enabling unattended mode for U-Boot, you must download and install the jloader firmware package **/volume/build/junos/13.2/service/13.2X51-D20.2/ship/jloader-ex-2200-13.2X51-D20.2-signed.tgz**, as described in TSB16425.

Unattended mode for U-Boot is not enabled by default. Use the following procedure to configure unattended mode:

1. Configure unattended mode.

```
[edit]
root@# set system unattended-boot
```

2. Commit the changes.

```
[edit]
root@# commit
```

Accessing the U-Boot CLI

When unattended mode for U-Boot is configured and the boot-loader password has been set, you can access the U-Boot CLI during the boot process by pressing <Ctrl+c> and entering the password at the prompt:

```
Press Ctrl-C in next 1 seconds to enter u-boot prompt...
Enter password:
```

```
password correct...
=>
```

The correct password must be entered within one minute after the prompt appears. If the password is not entered within one minute, or if the password is incorrect or has not been configured, access to the U-Boot CLI will be blocked, and the boot process will continue. For more information about unattended mode behavior, see "Understanding Unattended Mode for U-Boot on EX Series Switches" on page 335.

RELATED DOCUMENTATION

unattended-boot

boot-loader-authentication

RELATED DOCUMENTATION

Access Control and Authentication on Switching Devices

RADIUS Server Configuration for Authentication

IN THIS SECTION

Juniper Networks Ethernet Switches use 802.1X, MAC RADIUS, or captive portal authentication to provide access control to the devices or users. When 802.1X, MAC RADIUS, or captive portal authentications are configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. To use 802.1X or MAC RADIUS authentication, you must specify the

connections on the switch for each RADIUS server to which you want to connect. Read this topic for more information.

Specifying RADIUS Server Connections on Switches (CLI Procedure)

IN THIS SECTION

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure multiple RADIUS servers, include multiple `radius-server` statements. When multiple servers are configured, servers are accessed in order of configuration, by default. The first server configured is the primary server. If the primary server is unreachable, the router attempts to reach the second configured server, and so on. You can load balance the requests by configuring the round-robin method. 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.

NOTE: The round-robin access method is not recommended for use with EX Series switches.

You can also configure a fully qualified domain name (FQDN) that resolves to one or more IP addresses. See "Specifying RADIUS Server Connections on Switches (CLI Procedure)" on page 346.

To configure a RADIUS server on the switch:

1. Configure the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. The secret password on the switch must match the secret password on the server.

```
[edit access]
user@switch# set radius-server server-address port 1812 secret password
```

> **NOTE**: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify the IP address, the RADIUS server uses the address of the interface that sends the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch.

```
[edit access]
user@switch# set radius-server source-address source-address
```

3. Configure the authentication order, making `radius` the first method of authentication:

```
[edit access]
user@switch# set profile profile-name authentication-order radius
```

4. (Optional) Configure the method the router uses to access RADIUS authentication and accounting servers when multiple servers are configured:

   - `direct`—The default method, in which there is no load balancing. The first server configured is the primary server; servers are accessed in order of configuration. If the primary server is unreachable, the router attempts to reach the second configured server, and so on.

   - `round-robin`—The method that provides load balancing by rotating router requests among the list of configured RADIUS servers. The server chosen for access is rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.

> **NOTE**: When a RADIUS server in the round-robin list becomes unreachable, the next reachable server in the round-robin list is used for the current request. That same server is also used for the next request because it is at the top of the list of available servers. As a result, after a server failure, the server that is used takes up the load of two servers.

- To configure the method the router uses to access RADIUS accounting servers:

```
[edit access profile profile-name radius options]
user@host# set client-accounting-algorithm (direct | round-robin)
```

- To configure the method the router uses to access RADIUS authentication servers:

```
[edit access profile profile-name radius options]
user@host# set client-authentication-algorithm (direct | round-robin)
```

5. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different sent of authentication servers.

```
[edit access profile profile-name]
user@switch# set radius authentication-server server-address server-address
```

6. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit]
user@switch# set protocols dot1x authenticator authentication-profile-name access-profile-name
```

7. Configure the IP address of the switch in the list of clients on the RADIUS server. For information about configuring the RADIUS server, consult the documentation for your server.

Configuring a RADIUS Server Using an FQDN

You can configure a fully qualified domain name (FQDN) that resolves to one or more IP addresses. Configure a RADIUS server using an FQDN at the [`edit access radius-server-name` *hostname*] hierarchy level. When an FQDN resolves to multiple addresses, the servers are accessed in order of configuration, by default. The first resolved address is the primary server. If the primary server is unreachable, the router attempts to reach the second server, and so on. You can load balance the requests by configuring the

round-robin method. 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.

1. Configure the FQDN of the RADIUS server, the RADIUS server authentication port number, and the secret password. The secret password on the switch must match the secret password on the server.

```
[edit access]
user@switch# set radius-server-name hostname port 1812 secret password
```

NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Configure the interval for resolving an FQDN as the server address. The FQDN is resolved dynamically at fixed intervals based on the configured value.

```
[edit access]
user@switch# set radius-server-name hostname dns-query-interval minutes
```

3. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify the IP address, the RADIUS server uses the address of the interface that sends the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch.

```
[edit access]
user@switch# set radius-server-name hostname source-address source-address
```

4. Configure the authentication order, making `radius` the first method of authentication:

```
[edit access]
user@switch# set profile profile-name authentication-order radius
```

5. (Optional) Configure the method the switch uses to access RADIUS authentication and accounting servers when multiple servers are configured:

   - `direct`—The default method, in which there is no load balancing. The first server configured is the primary server; servers are accessed in order of configuration. If the primary server is unreachable, the router attempts to reach the second configured server, and so on.

- round-robin—The method that provides load balancing by rotating requests among the list of configured RADIUS servers. The server chosen for access is rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.

  NOTE: When a RADIUS server in the round-robin list becomes unreachable, the next reachable server in the round-robin list is used for the current request. That same server is also used for the next request because it is at the top of the list of available servers. As a result, after a server failure, the server that is used takes up the load of two servers.

- To configure the method the switch uses to access RADIUS accounting servers:

```
[edit access profile profile-name radius options]
user@host# set client-accounting-algorithm (direct | round-robin)
```

- To configure the method the switch uses to access RADIUS authentication servers:

```
[edit access profile profile-name radius options]
user@host# set client-authentication-algorithm (direct | round-robin)
```

6. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers.

```
[edit access profile profile-name]
user@switch# set radius authentication-server-name hostname
```

7. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit]
user@switch# set protocols dot1x authenticator authentication-profile-name access-profile-name
```

8. Configure the IP address of the switch in the list of clients on the RADIUS server. For information about configuring the RADIUS server, consult the documentation for your server.

SEE ALSO

Configuring 802.1X Interface Settings (CLI Procedure) | 378

Configuring 802.1X Authentication (J-Web Procedure)

Configuring MAC RADIUS Authentication (CLI Procedure) | 433

Configuring 802.1X RADIUS Accounting (CLI Procedure) | 448

Understanding Session-Aware Round-Robin RADIUS Requests

Starting in Junos OS Release 22.4R1, authentication(authd) services are session aware when round-robin algorithm is configured so that the corresponding access request is sent to the same RADIUS server in response to access challenge from the RADIUS server, which results in successful authentication.

As per existing behaviour, on receipt of access challenge and state attribute from one of the RADIUS servers, the corresponding access request is sent to the next RADIUS Server using Round-robin algorithm. Since the next RADIUS server does not have a record of this session, it rejects the access request which results in authentication failure. With the new feature, the corresponding algorithm is configured so that the respective access request gets sent to the same RADIUS server in response to the access challenge from RADIUS server, and this results in successful authentication. If the RADIUS server does not respond with an access challenge, it either accepts or rejects the request. For the next authentication request, requests get sent to the next RADIUS server as per the Round-robin method. Any number of access challenges can be sent from the RADIUS server in response to each access request and authd responds to the same RADIUS server until the request is accepted or rejected by the RADIUS server.

Note that this feature is supported only for authd-lite clients (dot1x etc) and not for broadband clients that use Point-to-Point Protocol (PPP), as this is not supported on broadband clients. Also, access challenge messages are exchanged between RADIUS client and RADIUS server only in case of authentication, and not for accounting.

Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

Junos OS for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433, *Microsoft PPP CHAP Extensions*, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:

- Configured RADIUS server authentication. Configure users on the authentication server and set the first-tried option in the authentication order to radius. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

SEE ALSO

> Managing Users (J-Web Procedure)
>
> Junos OS Access Privilege Configuration Guide

Configuring MS-CHAPv2 for Password-Change Support

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.

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.

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.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
    }
    radius-options {
        password-protocol mschap-v2;
    }
    login {
        user bob {
            class operator;
        }
    }
}
```

Understanding Server Fail Fallback and Authentication on Switches

Juniper Networks Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication is configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

Server fail fallback enables you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback enables you to specify one of four actions to be taken for end devices awaiting authentication when the server is timed out. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch. The configured VLAN name overrides any attributes sent by the server.

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- *Move* the end device to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server. (The VLAN must already exist on the switch.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

When a VLAN is configured with Server Fail VoIP, and the server fails, an Interface Bridge Domain (IFBD) is created for this VLAN during client authentication. This allows the switch to move VoIP clients to a fallback VLAN if the authentication server is unreachable or times out, ensuring voice traffic continuity. The `server-fail-voip` statement specifically handles voice VLAN tagged traffic fallback actions, such as permitting access, denying access, or moving clients to a designated VLAN already configured on the switch. If the `server-fail-voip` statement is configured, the switch uses it to isolate and manage VoIP client traffic during server fail conditions, maintaining voice service availability even when authentication cannot be completed.

SEE ALSO

802.1X for Switches Overview | **370**

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | **399**

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Configuring 802.1X Interface Settings (CLI Procedure) | **378**

Configuring RADIUS Server Fail Fallback (CLI Procedure)

You can configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or

denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the `server-fail-voip` statement. For all data traffic, use the `server-fail` statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with `server-fail`, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with `server-fail-voip`. If `server-fail-voip` is not configured, the voice traffic is dropped.

NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the `server-fail-voip` statement in place of the `server-fail` statement.

To configure server fail fallback actions:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name  server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been denied access by the RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name  server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail vlan-name
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new end devices are denied access):

```
[edit protocols dot1x authenticator]
user@switch# set  interface interface-name server-fail use-cache
```

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

-
```
[edit protocols dot1x authenticator]
user@switch# set  interface interface-name server-reject-vlan vlan-sf
```

SEE ALSO

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 399

Configuring 802.1X Interface Settings (CLI Procedure) | 378

Monitoring 802.1X Authentication | 414

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1X53-D40	Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.

RELATED DOCUMENTATION

- Access Control and Authentication on Switching Devices
- 802.1X Authentication | **369**
- 802.1X and RADIUS Accounting | **444**
- MAC RADIUS Authentication | **432**

RADIUS over TLS (RADSEC)

IN THIS SECTION

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect. RADIUS over TLS is designed to provide secure communication of RADIUS requests using the Transport Secure Layer (TLS) protocol. RADIUS over TLS, also known as RADSEC, redirects regular RADIUS traffic to remote RADIUS servers connected over TLS. RADSec allows RADIUS authentication, authorization and accounting data to be passed safely across untrusted networks.

RADSEC uses TLS in combination with the Transmission Control Protocol (TCP). This transport profile provides stronger security than the User Datagram Protocol (UDP) which was originally used for

RADIUS transmission. RADIUS over UDP encrypts the shared secret password using the MD5 algorithm, which is vulnerable to attacks. RADSEC mitigates the risk of attacks on MD5 by exchanging RADIUS packet payloads over an encrypted TLS tunnel.

NOTE: Due to limitations of the TCP protocol, RADSEC can have no more than 255 RADIUS messages in flight.

Configure the RADSEC Destination

RADSEC servers are represented by RADSEC destination objects. To configure RADSEC, you must define the RADSEC server as a destination, and direct RADIUS traffic to that destination.

You define the RADSEC server as a destination using the `radsec` statement at the `[edit access]` hierarchy level. RADSEC destinations are identified by a unique numeric ID. You can configure multiple RADSEC destinations with different parameters pointing to the same RADSEC server.

To redirect traffic from a standard RADIUS server to a RADSEC server, associate the RADIUS server with a RADSEC destination. For example, the RADIUS server `10.1.1.1` is associated with RADSEC destination `10`:

```
access {
    radius-server 10.1.1.1 {
        secret zzz;
        radsec-destination 10;
    }
}
```

You can also associate the RADIUS server with a RADSEC destination inside an access profile. For example, RADIUS server `10.2.2.2` in profile `acc_profile` is associated with RADSEC destination `10`:

```
access {
    profile acc_profile {
       radius-server 10.2.2.2 {
          secret zzz;
          radsec-destination 10;
       }
```

```
    }
}
```

NOTE: You can redirect more than one RADIUS server to the same RADSEC destination.

To configure RADSEC:

1. Configure the RADSEC destination with a unique ID and an IP address.

```
[edit access]
user@host# radsec destination id-number address server-address
```

2. Configure the port of the RADSEC server. If no port is configured, the default RADSEC port 2083 is used.

```
[edit access radsec destination id-number]
user@host# port port-number
```

3. Redirect traffic from a RADIUS server to the RADSEC destination:

```
[edit access]
user@host# radius-server server-address radsec-destination id-number
```

Configure TLS Connection Parameters

The TLS connection provides encryption, authentication, and data integrity for the exchange of RADIUS messages. TLS relies on certificates and private-public key exchange pairs to secure the transmission of data between the RADSEC client and server. The RADSEC destination uses local certificates that are dynamically acquired from the Junos PKI infrastructure.

To enable RADSEC, you must specify the name of the local certificate. For information on configuring the local certificate and certificate authority (CA), see *Configuring Digital Certificates*.

1. Specify the name of the local certificate to be used for TLS communications.

```
[edit access]
user@host# radsec destination id-number tls-certificate certificate-name
```

2. Configure the certified name of the RADSEC server.

```
[edit access]
user@host# radsec destination id-number tls-peer-name cert-server-name
```

3. (Optional) Configure the TLS connection timeout (default is 5 seconds).

```
[edit access]
user@host# radsec destination id-number tls-timeout seconds
```

Example: Simple RADSEC Configuration

The following example is a simple RADSEC configuration with one RADIUS server and one RADSEC destination. RADIUS traffic is redirected from RADIUS server 10.1.1.1 to RADSEC destination 10.

```
access {
    radius-server 10.1.1.1 {
        secret zzz;
        radsec-destination 10;
    }
    radsec {
        destination 10 {
            address 10.10.1.1;
            max-tx-buffers 1000;
            id-reuse-timeout 60;
            port 1777;
            source-address 10.1.1.2;
            tls-certificate my_cert;
            tls-min-version { v1.1 | v1.2 };
            tls-peer-name x0.radsec.com
            tls-timeout 10;
        }
    }
}
```

Monitoring Certificates

To view information about the state and statistics of local certificate acquisition: **show network-access radsec local-certificate**.

Monitoring RADSEC Destinations

To view statistics for the RADSEC destinations: **show network-access radsec statistics**.

To view the state of the RADSEC destinations: **show network-access radsec state**.

RELATED DOCUMENTATION

Example: Configure System Authentication for RADIUS, TACACS+, and Password Authentication | 170

Example: Configure Authentication Order | 166

Understanding Per Service Radius Accounting Override Default Service Activation

SUMMARY

Learn how to understand per-service radius accounting override default service activation

IN THIS SECTION

Enhancing network service management with Per-Service Accounting over RADIUS allows you to customize accounting configurations on a per-service basis. This provides tailored accounting for individual services within a subscriber session. Additionally, Default Service Activation ensures continuous service availability by assigning a local service profile when external RADIUS servers are unreachable. Acting as a fallback for PPPoE sessions, this feature maintains service resilience. Configure these functionalities using options like `service-profile <service-name>;` for default service activation and

accounting-server [<list-of-server-addresses>]; for RADIUS override, ensuring integration into existing systems without impacting high availability or security. These enhancements offer granular control and flexibility, optimizing service session management and adapting accounting to meet operational needs effectively.

Benefits

- Enhanced flexibility through unique accounting configurations for individual services, enabling tailored service management for different operational requirements.
- Continuous service availability via Default Service Activation maintains subscriber sessions even when external authentication servers are down.
- Resilience in service management by automatically assigning a fallback local service profile, preventing service disruptions during server outages.
- Simplified network configuration by integrating updates into existing systems, reducing complexity in implementation without compromising system stability.
- Operational efficiency without introducing new Application Programming Interfaces, SNMP changes, or system log messages, facilitating easy adoption and minimizing integration challenges.

Overview

Implementing Per-Service RADIUS Accounting Override enables customization of accounting configurations on a per-service basis within a subscriber session. Specify distinct RADIUS accounting servers and intervals for individual services, enhancing granularity in service management. Use the configuration option accounting-server [<list-of-server-addresses>]; to define unique server lists for each service, aligning accounting with specific operational needs. Additionally, update-interval <n>; allows adjustment of accounting update intervals, ensuring data collection at optimal frequencies suited to service demands.

Default Service Activation ensures uninterrupted service availability by assigning a fallback local service profile when external RADIUS servers are unreachable. Acting as a fallback for PPPoE sessions, similar to DHCP sessions, it uses service-profile <service-name>; to activate a predefined local service profile, maintaining access to essential services during external server outages. default-service-local-only; refines functionality by restricting default service activation to local authentication scenarios, engaging fallback services only when necessary.

These enhancements integrate seamlessly into existing systems without altering high availability or security protocols. They leverage existing configuration structures to implement advanced service management capabilities, simplifying adoption and minimizing integration complexities, maintaining operational efficiency while expanding flexibility and reliability in service management.

Configuration Details

To utilize these features effectively, modify access profile configurations to include necessary RADIUS accounting override settings. Navigate to the service configuration within your desired access profile using the command-line interface, and integrate specific accounting server and interval overrides. Set a unique accounting server for a service with the following configuration block:

```
[edit access profile <profile-name> service]

name <service-name> {

radius {

accounting-server [<list-of-server-addresses>];

}

}
```

Adjust the accounting update interval as needed:

```
[edit access profile <profile-name> service]

name <service-name> {

accounting {

update-interval <n>;

}

}
```

For Default Service Activation, specify the local service profile and restrict activation to local-only scenarios with:

```
[edit access profile <profile-name>]

service-profile <service-name>;

default-service-local-only;
```

These steps are crucial for realizing the full potential of the enhancements, ensuring your network service remains adaptable and resilient in the face of external server challenges.

Understanding Server-Fail Persistent Cache

SUMMARY

Understand Server-Fail Persistent Cache

IN THIS SECTION

The Server-Fail Persistent Cache enhances the resilience of 802.1X authenticated sessions during authentication server outages. By retaining cached authentication information across device reboots, it ensures continuous network access during power disruptions or server connectivity issues. This mechanism is particularly beneficial for MAC authenticated sessions, where persistent storage of session attributes mitigates potential service interruptions. You can enable this functionality through specific CLI commands, maintaining session data integrity with periodic file updates and checksum validation. Designed to operate seamlessly across various platforms, this feature integrates without impacting performance or scalability while upholding stringent security protocols.

Benefits of Server-Fail Persistent Cache

- The cache ensures continuous network access by retaining authentication information during server outages, allowing devices to maintain connectivity even when the authentication server is unreachable.
- It preserves session attributes across device reboots, preventing service interruptions caused by power disruptions and ensuring seamless network operation.
- The feature enhances data integrity by using checksum validation, guarding against corrupted session data and maintaining reliable network sessions.
- It operates effectively on various platforms without impacting performance or scalability, providing a robust solution across different hardware environments.

Overview

The Server-Fail Persistent Cache is engineered to bolster the resilience of 802.1X authenticated sessions, particularly when authentication servers are unreachable. You can activate this feature to ensure that devices retain their session attributes even if they undergo a reboot due to power interruptions. This capability is crucial for maintaining uninterrupted network connectivity, as the cache preserves the authentication data required for MAC authenticated sessions, circumventing the need for immediate server interaction. The persistent storage mechanism writes authenticated session information to a file periodically, safeguarding it with checksum validation to prevent the use of corrupted data.

To enable the Server-Fail Persistent Cache feature, input the following command within the CLI: `set protocol dot1x authenticator cache persistent`. This command activates the persistent cache, allowing session attributes to be retained across device reboots. If you decide to revert to the default behavior, use `set protocol dot1x authenticator cache non-persistent` to disable caching. Additionally, configure the server reachability query period by using `set protocols dot1x authenticator radius-reachability query-period` *seconds*, where *seconds* specifies the interval between reachability checks. These configurations ensure that your network remains robust and responsive to server outages, providing seamless connectivity for authenticated clients.

Understanding Graceful Routing Engine Switchover Support for 802.1X

SUMMARY

Understand how graceful routing engine switchover works on 802.1X.

IN THIS SECTION

Integrating Graceful Routing Engine Switchover (GRES) support with the 802.1X protocol enhances network resilience by ensuring uninterrupted client connectivity during a switchover event. This integration preserves the authentication state of each 802.1X client, allowing seamless session management without requiring reauthentication, which significantly reduces traffic disruptions. The feature encompasses session rebuilding through the 802.1X process (daemon), managing captive portal and client-to-server traffic sessions, and handling MAC filters and VLANs to maintain network integrity.

Additionally, the `show dot1x sync-pending-sessions` command facilitates verification of session statuses, aiding network administrators in troubleshooting and ensuring smooth operation. This integration optimizes client connectivity and performance by adhering to security policies without manual intervention, leveraging existing infrastructure components for efficient deployment.

Benefits of GRES Support for 802.1X

- Ensures continuous client connectivity during a GRES event by preserving authentication states, minimizing traffic disruptions.
- Prevents the need for 802.1X clients to reinitiate authentication, enhancing reliability and providing a seamless network experience.
- Supports efficient management of MAC filters and VLANs, reducing the risk of incorrect deletions and maintaining network integrity.
- Facilitates session rebuilding by accessing stored session data, ensuring that authorization changes are updated without manual intervention.
- Optimizes network performance while adhering to security policies, utilizing existing infrastructure components for streamlined deployment.

Overview

The integration of Graceful Routing Engine Switchover (GRES) support with the 802.1X protocol focuses on maintaining seamless client connectivity during switchover events by preserving the authentication states of connected devices. This capability is achieved through the 802.1X process (daemon), responsible for session rebuilding post-switchover. It accesses stored session data and triggers reauthentication processes to ensure any changes in authorization are updated automatically. This prevents traffic disruptions and eliminates the need for clients to reinitiate authentication, thus providing a stable network experience.

In addition to session management, GRES support carefully handles MAC filters and VLAN configurations to maintain network integrity. During switchover events, the feature ensures these configurations are preserved, reducing the risk of incorrect deletions that could compromise network security and performance. By leveraging existing infrastructure components, you can streamline the deployment of this feature without requiring additional software licenses or changes. This interaction is crucial for maintaining the reliability and effectiveness of the network, as it ensures all components work together to support uninterrupted client connectivity.

To verify session statuses and troubleshoot potential issues post-GRES switchover, utilize the command `show dot1x sync-pending-sessions`. This command provides detailed information on interfaces, session states, MAC addresses, and authentication modes. By displaying all previously authenticated sessions awaiting synchronization, it aids in monitoring and managing the network environment efficiently. This tool is essential for network administrators, as it helps ensure that the implementation of GRES support functions optimally and that all clients maintain their required network access and security policies.

Implementation Considerations

Effective implementation of GRES support for 802.1X requires attention to several key technical considerations. Ensure existing infrastructure components, such as the kernel and associated modules, are compatible with this update, as they play a significant role in maintaining authentication states and session data. While deploying this feature does not necessitate new licensing or packaging changes, verifying the compatibility of all components is vital to prevent disruptions. Thorough testing and validation of the `show dot1x sync-pending-sessions` command should be conducted to guarantee its effectiveness in real-world network scenarios, ensuring administrators have the necessary insights to manage and optimize network resilience during GRES events.

Understanding 802.1X Selective Server-Reject VLAN

SUMMARY

Understand how the 802.1X selective server-reject VLAN feature works.

IN THIS SECTION

The 802.1X Selective Server-Reject VLAN feature enhances the flexibility of 802.1x authentication processes by altering the handling of client authentication rejections from RADIUS servers. Instead of directly assigning clients to a server-reject VLAN upon failed authentication, you can configure the system to attempt alternative methods such as MAC-RADIUS. This approach provides more granular management of client authentication, optimizing network access and minimizing authentication-related

issues. Implementing this feature requires a specific configuration command that defines the sequence of authentication methods and specifies VLAN parameters. Compatible across all software platforms, this feature integrates seamlessly, provided no captive portal is present on the interface to maintain operational compatibility.

Benefits of Dot1x Selective Server-Reject VLAN

- Enhance authentication flexibility by allowing alternative methods before assigning clients to a server-reject VLAN, improving client access management.
- Minimize network disruptions by reducing the number of clients immediately placed in a restricted VLAN, maintaining consistent network service.
- Provide network administrators with granular control over authentication processes, helping tailor network access policies effectively.
- Optimize network access by attempting multiple authentication methods, increasing successful client connections and reducing failed authentication incidents.
- Ensure broad compatibility across software platforms, broadening the feature's applicability without requiring additional platform-specific customization.

Overview

The Dot1x Selective Server-Reject VLAN feature introduces a refined approach to handling authentication rejections by a RADIUS server. If a RADIUS server rejects a client attempting 802.1x authentication, this feature allows your network system to sequentially attempt alternative methods, such as MAC-RADIUS, before defaulting to a server-reject VLAN assignment. This configuration uses the command `set protocols dot1x authenticator interface INTF_NAME server-reject-vlan post-auth-order`, where you specify the sequence of authentication methods and VLAN parameters, ensuring the system tries multiple approaches before isolating the client.

To effectively deploy this feature, ensure that the interface does not have a captive portal configuration, as its presence can lead to incompatibility issues. The feature is designed to be universally compatible across software platforms, allowing broad applicability without necessitating platform-specific adjustments. It is important to configure the feature with the necessary MAC-RADIUS settings to fully leverage its capabilities. Although the feature may introduce a slight delay in the authentication process due to the sequential nature of attempting multiple authentication methods, this trade-off results in increased flexibility and potentially higher rates of successful client authentications.

Configuration Considerations

When implementing the Dot1x Selective Server-Reject VLAN feature, consider the network design and existing configurations to avoid potential conflicts. Ensure that MAC-RADIUS is correctly configured on the interface, as this serves as a fundamental alternative method in the authentication sequence. Additionally, verify that no captive portal settings are active, as these can interfere with the feature's operation. Adjust VLAN settings appropriately to reflect the desired network access policies, specifying VLAN names or tags in the configuration command to guide the post-authentication process. By meticulously configuring these aspects, you can maximize the feature's benefits, resulting in improved authentication flexibility and network access optimization.

802.1X Authentication

IN THIS SECTION

IEEE 802.1X standard for port-based network access control and protects Ethernet LANs from unauthorized user access. It blocks all traffic from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant. Read this topic for more information.

802.1X for Switches Overview

IN THIS SECTION

How 802.1X Authentication Works

802.1X authentication works by using an authenticator port access entity (the switch) to block ingress traffic from a supplicant (end device) at the port until the supplicant's credentials are presented and match on the authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in *single supplicant* mode, *single-secure supplicant* mode, or *multiple supplicant* mode:

- single supplicant—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively *piggyback* on the first end device's authentication.
- single-secure supplicant—Allows only one end device to connect to the port. No other end device is allowed to connect until the first device logs out.
- multiple supplicant—Allows multiple end devices to connect to the port. Each end device is authenticated individually.

Network access can be further defined by using VLANs and firewall filters, both of which act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication is configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 354.

802.1X Features Overview

The following 802.1X features are supported on Juniper Networks Ethernet Switches:

- Guest VLAN—Provides limited access to a LAN, typically only to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication is not configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access only to the Internet and to other guests' end devices.
- Server-reject VLAN—Provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.
- Server-fail VLAN—Provides limited access to a LAN, typically only to the Internet, for 802.1X end devices during a RADIUS server timeout.
- Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).
- Dynamic changes to a user session—Enables the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.

- VoIP VLAN—Supports IP telephones. The implementation of a voice VLAN on an IP telephone is vendor-specific. If the phone is 802.1X-enabled, it is authenticated as any other supplicant is. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (provided that the interface is configured in single supplicant mode and not in single-secure supplicant mode).

  NOTE: Configuring a VoIP VLAN on private VLAN (PVLAN) interfaces is not supported.

- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

- RADIUS server attributes for 802.1X—The `Juniper-Switching-Filter` is a vendor-specific attribute (VSA) that can be configured on the RADIUS server to further define a supplicant's access during the 802.1X authentication process. Centrally configuring attributes on the authentication server obviates the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant might connect to the LAN. The `Juniper-Switching-Filter` is equivalent to the NAS-Filter-Rule referenced in Attribute 92 of RFC4849.

- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)—Enables MS-CHAPv2 authentication for 802.1X EAP capable clients.

- Micro and Macro Segmentation with GBP using Mist Access Assurance—You can apply microsegmentation and macrosegmentation in a Virtual Extensible LAN (VXLAN) architecture by using group-based policy (GBP). GBP leverages the underlying VXLAN technology to provide location-agnostic endpoint access control. With GBP, you can implement consistent security policies across the enterprise network domains. Thereby you can avoid configuring a large number of firewall filters on all your switches and simplify your network configuration. The network access control (NAC) of the Juniper Mist cloud dynamically assigns GBP tags during a RADIUS transaction. With RADIUS 802.1X authentication, network operators can automatically authenticate and authorize a user or device and let them into the network. Juniper Mist Access Assurance uses user and device identity to determine the role and the network segment that the network assigns to each user. The network uses VLAN or GBP to group the users into network segments. Juniper Mist Access Assurance then applies network policies associated with each segment

  We currently support this on EX4100, EX4400, and on EX4650 virtual chassis.

  For more information see, *Micro and Macro Segmentation using Group Based Policy in a VXLAN*.

The following features are supported to authenticate devices that are not 802.1X-enabled:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.

- MAC RADIUS authentication—Provides a means to permit hosts that are not 802.1X-enabled to access the LAN. MAC-RADIUS simulates the supplicant functionality of the client device, using the MAC address of the client as username and password.

802.1X Authentication on Trunk Ports

Starting in Junos OS Release 18.3R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device. An AP or switch connected to the NAS will support multiple VLANs, so must connect to a trunk port. Enabling 802.1X authentication on the trunk interface protects the NAS from a security breach in which an attacker might disconnect the AP and connect a laptop to get free access to network for all the configured VLANs.

Please note the following caveats when configuring 802.1X authentication on trunk interfaces.

- Only single and single-secure supplicant modes are supported on trunk interfaces.
- You must configure 802.1X authentication locally on the trunk interface. If you configure 802.1X authentication globally using the `set protocol dot1x interface all` command, the configuration is not applied to the trunk interface.
- Dynamic VLANS are not supported on trunk interfaces.
- Guest VLAN and server-reject VLAN are not supported on trunk interfaces.
- Server fail fallback for VoIP clients is not supported on trunk interfaces (`server-fail-voip`).
- `Server-fail (permit, use-cache, vlan-name), Server-reject (vlan vlan-name)`are not supported for EAP-TLS clients.
- Authentication on trunk port is not supported using captive portal.
- Authentication on trunk port is not supported on aggregated interfaces.
- Configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs) is not supported on trunk ports.

802.1X Authentication on Layer 3 Interfaces

Starting in Junos OS Release 20.2R1, you can configure 802.1X authentication on layer 3 interfaces. Please note the following caveats when configuring 802.1X authentication on layer 3 interfaces:

- Only EAP-capable clients are supported.
- Only single supplicant mode is supported.

- You must configure 802.1X authentication locally on layer 3 interfaces. If you configure 802.1X authentication globally using the `set protocol dot1x interface all` command, the configuration is not applied to layer 3 interfaces.
- Support for layer 3 interfaces does not include IRB or sub-interfaces.
- Guest VLAN, server-reject VLAN, and server-fail VLAN are not supported.
- Server fail fallback for VoIP clients is not supported (`server-fail-voip`).
- Only the following attributes are accepted from the authentication server as part of RADIUS access-accept or COA messages for clients authenticated on layer 3 interfaces:
  - User-Name
  - Session-Timeout
  - Calling-Station-ID
  - Acct-Session-ID
  - NAS-Port-Id
  - Port-Bounce

802.1X Support on Junos OS Evolved Software

Starting in Junos OS Evolved Release 22.3R1, you can configure 802.1X authentication on layer 2 interfaces. Follow caveats apply for 802.1X authentication on layer 2 interfaces.

- Unsupported features include:
  - Guest VLAN, server-reject VLAN, and server-fail VLAN
  - Server fail fallback for VoIP clients (server-fail-voip)
  - Dynamic VLAN
  - Authentication on layer 2 interfaces using captive portal and central Web authentication (CWA).
- Unsupported attributes from the authentication server of RADIUS access-accept or COA messages for clients authenticated on layer 2 interfaces include:
  - Ip-Mac-Session-Binding
  - Juniper-CWA-Redirect
  - Juniper-Switching-Filter

- Filter-Id
- Tunnel-Medium-Type
- Juniper-VoIP-VLAN
- Egress-VLAN-Name
- Egress-VLAN-ID
- Tunnel-Type
- Tunnel-Private-Group-Id

- If IRB is in the bridge domain, 802.1x enabled ports do not drop routed traffic for single-secure and multiple supplicant modes, even if the user is not authenticated. 802.1x enabled ports on layer 2 interface drop routed traffic only for single supplicant mode configuration.

SEE ALSO

Understanding Authentication on Switches

Understanding 802.1X and VoIP on EX Series Switches | **554**

Understanding LLDP and LLDP-MED on EX Series Switches | **711**

Understanding 802.1X and RADIUS Accounting on Switches | **445**

Understanding Server Fail Fallback and Authentication on Switches | **353**

802.1X Authentication on Layer 2 Interfaces

IN THIS SECTION

Overview

IN THIS SECTION

The IEEE 802.1X standard for port-based network access control (PNAC) provides a mechanism to authenticate users of devices attached to a LAN port. The 802.1X standard verifies the user's credentials in a local or remote user database. The authentication mechanism allows only users with the correct credentials to access the network. It denies access for all other users, thereby controlling network access.

The three basic components of a network with 802.1X authentication are:

- Authenticator port access entity (PAE): A switch or router port to which a client connects. Authenticator PAEs form the control gate that blocks all traffic to and from the clients until 802.1X authenticates the clients.
- Supplicants: Clients that are trying to access the network and need to be authenticated. Supplicants connect to authenticator PAEs.
- Authentication server: The back-end database containing information about the users that are allowed to connect to the network. When a supplicant attempts to log in, 802.1X sends the supplicant's credentials to this server for authentication.

After the authentication server authenticates the supplicant's credentials, the device stops blocking access on the PAE. The device opens the interface to the supplicant and allows it to access the network. You (the network administrator) can configure 802.1X on Layer 2 (L2) interfaces.

The 802.1X IEEE standard allows you to use any authentication server for client authentication. RADIUS servers are most commonly used because those servers are easy to configure. RADIUS servers also provide the option to define proprietary, or vendor-specific, attributes. The device and the server can exchange these attributes.

Benefits

- Authenticate users.
- Prevent bad actors from accessing your network.
- Control network access.

Configuration

1. Configure the L2 interface.

   For example:

```
set interfaces et-0/0/0 unit 0 family ethernet-switching interface-mode access
set interfaces et-0/0/0 unit 0 family ethernet-switching vlan members v10
set vlans v10 vlan-id 10
```

2. Enable 802.1X authentication using the `authenticator` statement.

   a. Single-supplicant mode:

```
set protocols dot1x authenticator interface et-0/0/0.0 supplicant single
```

   b. Single-secure-supplicant mode:

```
set protocols dot1x authenticator interface et-0/0/0.0 supplicant single-secure
```

   c. Multiple-supplicant mode:

```
set protocols dot1x authenticator interface et-0/0/0.0 supplicant multiple
```

3. Create the 802.1X profiles and associate the profiles to 802.1X, the RADIUS authentication server, and the RADIUS accounting server.

   For example:

```
set access profile dot1x-auth-profile authentication-order radius
set access profile dot1x-auth-profile radius authentication-server address
set access profile dot1x-auth-profile radius accounting-server address
set protocols dot1x authenticator authentication-profile-name dot1x-auth-profile
set access profile dot1x-accounting authentication-order radius
set access profile dot1x-accounting accounting order radius
```

4. Configure the RADIUS authentication server.

   For example:

```
set access radius-server address port 1812
set access radius-server address secret secret
```

```
set access radius-server address timeout 3
set access radius-server address retry 3
set access radius-server address source-address source-address
```

5. Verify the configuration using the following commands.
   - **show vlans**
   - **show ethernet-switching table**
   - **show mac-vrf forwarding mac-table**
   - **show dot1x interface detail**

Configuring 802.1X Interface Settings (CLI Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See "Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)" on page 494.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See "Specifying RADIUS Server Connections on Switches (CLI Procedure)" on page 346.

To configure 802.1X on an interface:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name supplicant multiple
```

NOTE: Multiple supplicant mode is not supported on trunk interfaces.

2. Enable reauthentication and specify the reauthentication interval:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  reauthentication interval seconds
```

3. Configure the interface timeout value for the response from the supplicant:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  supplicant-timeout seconds
```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  server-timeout seconds
```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  transmit-period seconds
```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  maximum-requests number
```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name  retries number
```

NOTE: If the RADIUS authentication servers become unavailable or inaccessible the server fail fallback is triggered. By default, the `deny` option is configured under `server-fail`, which force fails the supplicant authentication. However, there are other options that you can configure as actions to be taken for end devices awaiting authentication when the server times out.

For more information, see **interface (802.1X)**

NOTE: This setting specifies the number of attempts before the switch puts the interface in a *HELD* state.

SEE ALSO

- Configuring 802.1X Authentication (J-Web Procedure)
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | **557**
- Configuring LLDP (CLI Procedure) | **703**
- Understanding Authentication on Switches

Understanding RADIUS-Initiated Changes to an Authorized User Session

IN THIS SECTION

When using an authentication service that is based on a client/server RADIUS model, requests are typically initiated by the client and sent to the RADIUS server. There are instances in which a request might be initiated by the server and sent to the client in order to dynamically modify an authenticated user session already in progress. The client that receives and processes the messages is the switch, which acts as the network access server, or NAS. The server can send the switch a Disconnect message

requesting to terminate a session, or a Change of Authorization (CoA) message requesting to modify the session authorization attributes.

The switch listens for unsolicited RADIUS requests on UPD port 3799, and accepts requests only from a trusted source. Authorization to send a Disconnect or CoA request is determined based on the source address and the corresponding shared secret, which must be configured on the switch as well as on the RADIUS server. For more information about configuring the source address and shared secret on the switch, see "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.

Disconnect Messages

The RADIUS server sends a Disconnect-Request message to the switch in order to terminate a user session and discard all associated session context. The switch responds to a Disconnect-Request packet with a Disconnect-ACK message if the request is successful, that is, all associated session context is discarded and the user session is no longer connected, or with a Disconnect-NAK packet if the request fails, that is, the authenticator is unable to disconnect the session and discard all associated session context.

In Disconnect-Request messages, RADIUS attributes are used to uniquely identify the switch (NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match at least one session for the request to be successful; otherwise, the switch responds with a Disconnect-NAK message. A Disconnect-Request message can contain only NAS and session identification attributes; if any other attributes are included, the switch responds with a Disconnect-NAK message.

Change of Authorization Messages

Change of Authorization (CoA) messages contain information for dynamically modifying the authorization attributes for a user session to change the authorization level. This occurs as part of a two-step authentication process, in which the endpoint is first authenticated using MAC RADIUS authentication, and is then profiled based on the type of device. The CoA message is used to apply an enforcement policy that is appropriate for the device, typically by changing the data filters or the VLAN.

The switch responds to a CoA message with a CoA-ACK message if the authorization change is successful, or a with CoA-NAK message if the change is unsuccessful. If one or more authorization changes specified in a CoA-Request message cannot be carried out, the switch responds with a CoA-NAK message.

In CoA-Request messages, RADIUS attributes are used to uniquely identify the switch (acting as the NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match the identification attributes of at least one session for the request to be successful; otherwise, the switch responds with a CoA-NAK message.

CoA-Request packets also include the session authorization attributes that will be modified if the request is accepted. The supported session authorization attributes are listed below. The CoA message can contain any or all of these attributes. If any attribute is not included as part of the CoA-Request message, the NAS assumes that the value for that attribute is to remain unchanged.

- Filter-ID
- Tunnel-Private-Group-ID
- Juniper-Switching-Filter
- Juniper-VoIP-VLAN
- Session-Timeout

CoA Request Port Bounce

When a CoA message is used to change the VLAN for an authenticated host, end devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.

The command to bounce the port is sent from the RADIUS server using a Juniper Networks vendor-specific attribute (VSA). The port is bounced if the following VSA attribute-value pair is received in the CoA message from the RADIUS server:

- Juniper-AV-Pair = “Port-Bounce”

To enable the port bounce feature, you must update the Junos dictionary file (**juniper.dct**) on the RADIUS server with the Juniper-AV-Pair VSA. Locate the dictionary file and add the following text to the file:

```
ATTRIBUTE Juniper-AV-Pair        Juniper-VSA(52, string) r
```

For more information about adding the VSA, consult the FreeRADIUS documentation.

You can disable the feature by configuring the `ignore-port-bounce` statement at the [`edit protocols dot1x authenticator interface interface-name`] hierachy level.

Error-Cause Codes

When a disconnect or CoA operation is unsuccessful, an Error-Cause attribute (RADIUS attribute 101) can be included in the response message sent by the NAS to the server to provide detail about the cause of the problem. If the detected error does not map to one of the supported Error-Cause attribute

values, the router sends the message without an error-cause attribute. See Table 23 on page 383 for descriptions of error-cause codes that can be included in response messages sent from the NAS.

Table 23: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
201	Residual session context removed	Sent in response to a Disconnect-Request message if one or more user sessions are no longer active, but residual session context was found and successfully removed. This code is sent only within a Disconnect-ACK message.
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
403	NAS identification mismatch	Request contains one or more NAS identification attributes that do not match the identity of the NAS receiving the request.
404	Invalid request	Some other aspect of the request is invalid—for example, if one or more attributes are not formatted properly.
405	Unsupported service	The Service-Type attribute included with the request contains an invalid or unsupported value.
406	Unsupported extension	The entity receiving the request (either an NAS or a RADIUS proxy) does not support RADIUS-initiated requests.
407	Invalid attribute value	The request contains an attribute with an unsupported value.
501	Administratively prohibited	The NAS is configured to prohibit honoring of Disconnect-Request or CoA-Request messages for the specified session.
503	Session context not found	The session context identified in the request does not exist on the NAS.

Table 23: Error-Cause Codes (RADIUS Attribute 101) ***(Continued)***

Code	Value	Description
504	Session context not removable	The subscriber identified by attributes in the request is owned by a component that is not supported. This code is sent only within a Disconnect-NAK message.
506	Resources unavailable	A request could not be honored because of lack of available NAS resources (such as memory).
507	Request initiated	The CoA-Request message includes a Service-Type attribute with a value of Authorize Only.
508	Multiple session selection unsupported	The session identification attributes included in the request match multiple sessions, but the NAS does not support requests that apply to multiple sessions.

Filtering 802.1X Supplicants by Using RADIUS Server Attributes

IN THIS SECTION

There are two ways to configure the a RADIUS server with port firewall filters (Layer 2 firewall filters):

- Include one or more filter terms in the Juniper-Switching-Filter attribute. The Juniper-Switching-Filter attribute is a vendor-specific attribute (VSA) listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server. Use this VSA to configure simple filter conditions for 802.1X authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.

- Configure a local firewall filter on each switch and apply that firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. The firewall filter must be configured on each switch.

  NOTE: If the firewall filter configuration is modified after users are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter configuration changes to take effect.

This topic includes the following tasks:

Configuring Firewall Filters on the RADIUS Server

Starting in Junos OS Evolved Release 22.4R1, you can configure multiple source and destination ports (or port ranges) within a single line without having to repeat the match condition again. This feature enables shorter VSA lengths and also helps reduce the size of radius response packets.

The switching-filter allows provisioning a list of values for ether type, IP, source tag, source port, and destination port.

```
Juniper-Switching-Filter = match dst-port [ 80 25 443 ] src-port [5060 1025-2000] action allow

Juniper-Switching-Filter = match dst-port 500 source-tag [ 100, 200 ] action allow

Juniper-Switching-Filter = match src-port 9090 ip-proto [ 25 17] action allow

Juniper-Switching-Filter = match ether-type [ 3000-4000 8000 ] action allow
```

You can configure simple filter conditions by using the Juniper-Switching-Filter attribute in the Juniper dictionary on the RADIUS server. These filters are sent to a switch whenever a new user is authenticated successfully. The filters are created and applied on all EX Series switches that authenticate users through that RADIUS server without the need for you to configure anything on each individual switch.

NOTE: This procedure describes using FreeRADIUS software to configure the Juniper-Switching-Filter VSA. For specific information about configuring your server, consult the AAA documentation included with your server.

To configure the Juniper-Switching-Filter attribute, enter one or more filter terms by using the CLI for the RADIUS server. Each filter term consists of match conditions with a corresponding action. Enter the filter terms enclosed within quotation marks (" ") by using the following syntax:

```
Juniper-Switching-Filter = “match <destination-mac mac-address> <source-vlan vlan-name> <source-dot1q-tag
tag> <destination-ip ip-address> <ip-protocol protocol-id> <source-port port> <destination-port port> action
(allow | deny) <loss-priority (low | medium | high)>”
```

More than one match condition can be included in a filter term. When multiple conditions are specified in a filter term, they must all be fulfilled for the packet to match the filter term. For example, the following filter term requires a packet to match *both* the destination IP address and the destination MAC address to meet the term criteria:

```
Juniper-Switching-Filter = “match destination-ip 10.10.10.8 destination-mac 00:00:00:01:02:03 action allow”
```

Multiple filter terms should be separated with commas—for example:

```
Juniper-Switching-Filter = “match destination-mac 00:00:00:01:02:03 action allow, match destination-port 80
destination-mac 00:aa:bb:cc:dd:ee action allow”
```

See "Juniper-Switching-Filter VSA Match Conditions and Actions" on page 198 for definitions of match conditions and actions.

NOTE: On EX9200 switches, and in a Junos Fusion Enterprise with EX9200 as the aggregate device, the dynamic firewall filter is strictly applied for all IP packets. If the filter is configured to allow only a specific destination IP address, packets with other IP addresses as the destination IP will be dropped per the filter rules. This includes any IP protocol packets, such as DHCP, IGMP and ARP packets.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute **Juniper-Switching-Filter** (attribute ID 48):

```
[root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper

#  dictionary.juniper
#
# Version:      $Id: dictionary.juniper,v 1.2.6.1 2005/11/30 22:17:25 aland Exp
$
```

```
#  VENDOR          Juniper                         2636
BEGIN-VENDOR    Juniper
ATTRIBUTE       Juniper-Local-User-Name              1       string
ATTRIBUTE       Juniper-Allow-Commands               2       string
ATTRIBUTE       Juniper-Deny-Commands                3       string
ATTRIBUTE       Juniper-Allow-Configuration          4       string
ATTRIBUTE       Juniper-Deny-Configuration           5       string
ATTRIBUTE       Juniper-Switching-Filter             48      string
ATTRIBUTE       Juniper-VoIP-Vlan                    49      string
ATTRIBUTE       Juniper-CWA-Redirect                 50      string
ATTRIBUTE       Juniper-AV-Pair                      52      string
<-
```

2. Enter the match conditions and actions. For example:

   - To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is **10**):

     ```
     [root@freeradius]#
     cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the **Juniper-Switching-Filter** attribute:

     ```
     Juniper-Switching-Filter = "Match Source-dot1q-tag 10 Action deny"
     ```

   - To deny access based on a destination IP address:

     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```

     For each relevant user, add the **Juniper-Switching-Filter** attribute:

     ```
     Juniper-Switching-Filter = “Match Destination-ip 192.168.1.0/31 Action deny”
     ```

   - To set the packet loss priority (PLP) to **high** based on a destination MAC address and the IP protocol:

     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```

For each relevant user, add the **Juniper-Switching-Filter** attribute:

```
Juniper-Switching-Filter = "Match Destination-mac 00:04:0f:fd:ac:fe, Ip-protocol 2, Action
loss-priority high"
```

3. Stop and restart the RADIUS process to activate the configuration.

Applying a Locally Configured Firewall Filter from the RADIUS Server

You can apply a port firewall filter (Layer 2 firewall filter) to user policies centrally from the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests authentication, reducing the need to configure the same firewall filter on multiple switches. Use this method when the firewall filter contains a large number of conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview*.

To apply a port firewall filter centrally from the RADIUS server:

NOTE: If port firewall filters are also configured locally for the interface, then the firewall filters configured by using VSAs take precedence if they conflict with the locally configured port firewall filters. If there is no conflict, they are merged.

1. Create the firewall filter on the local switch. See *Configuring Firewall Filters (CLI Procedure)* for more information on configuring a port firewall filter.
2. On the RADIUS server, open the **users** file to display the local user profiles of the end devices to which you want to apply the filter:

```
[root@freeradius]#
cat /usr/local/etc/raddb/usersvi users
```

3. Apply the filter to each user profile by adding the Filter-ID attribute with the filter name as the attribute value:

```
Filter-Id =filter-name
```

For example, the user profile below for `supplicant1` includes the Filter-ID attribute with the filter name `filter1`:

```
[root@freeradius]# cat /usr/local/etc/raddb/users

supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005",
        Filter-Id = "filter1"
```

NOTE: Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to the switch on the same interface by configuring a single filter with policies for each of those users.

4. Stop and restart the RADIUS process to activate the configuration.

RELATED DOCUMENTATION

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch | **467**

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch

IN THIS SECTION

802.1X is the IEEE standard for port-based network access control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an EX Series switch, and configure it for 802.1X:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* . For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Configured users on the RADIUS authentication server.

Overview and Topology

The EX Series switch acts as an authenticator PAE. It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 7 on page 391 shows one EX4200 switch that is connected to the devices listed in Table 24 on page 392.

Figure 7: Topology for Configuration

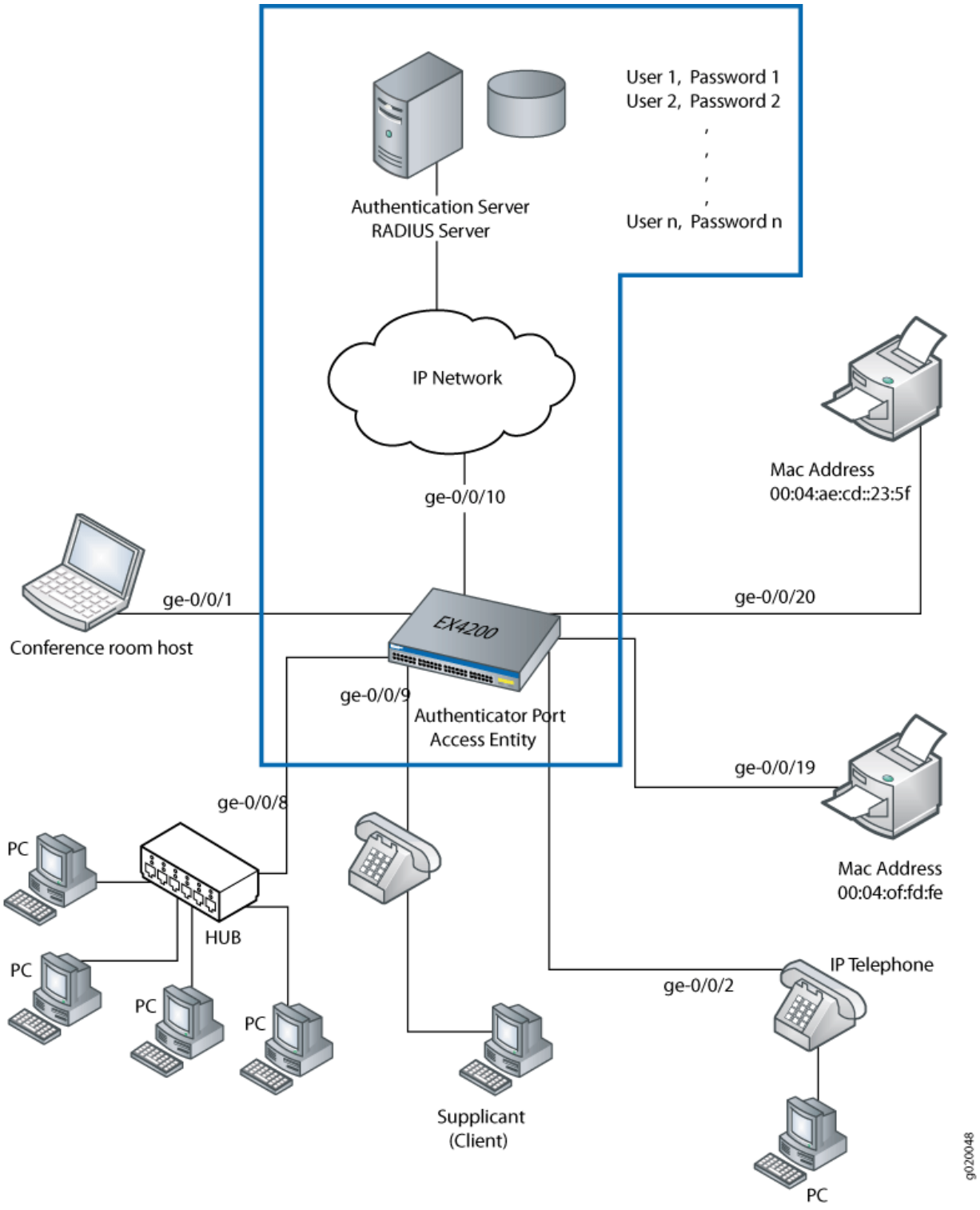


Table 24: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
VLAN name	default
One RADIUS server	Backend database with an address **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, connect the RADIUS server to access port ge-0/0/10 on the EX4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the *Junos OS System Basics Configuration Guide*.

Configuration

IN THIS SECTION

- Procedure | 392

Procedure

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
```

```
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:

```
[edit]
user@switch# set access radius-server 10.0.0.100 secret juniper
user@switch# set access radius-server 10.0.0.200 secret juniper
```

2. Configure the authentication order, making **radius** the first method of authentication:

```
[edit]
user@switch# set access profile profile1 authentication-order radius
```

3. Configure a list of server IP addresses to be tried in sequential order to authenticate the supplicant:

```
[edit]
user@switch# set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Results

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
    10.0.0.100
        port 1812;
        secret "$ABC123"; ## SECRET-DATA
        }
    }
    profile profile1{
        authentication-order radius;
        radius {
```

```
            authentication-server 10.0.0.100 10.0.0.200;
        }
    }
}
```

Verification

IN THIS SECTION

- Verify That the Switch and RADIUS Server Are Properly Connected | **394**

To confirm that the configuration is working properly, perform these tasks:

Verify That the Switch and RADIUS Server Are Properly Connected

Purpose

Verify that the RADIUS server is connected to the switch on the specified port.

Action

Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning

ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether the server is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

SEE ALSO

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | **460**

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | **557**

Configuring 802.1X RADIUS Accounting (CLI Procedure) | **448**

Understanding Dynamic Filters Based on RADIUS Attributes

You can use RADIUS server attributes to implement port firewall filters on a RADIUS authentication server. These filters can be dynamically applied to supplicants that request authentication through that server. RADIUS server attributes are clear-text fields encapsulated in Access-Accept messages sent from the authentication server to the switch when a supplicant connected to the switch is successfully authenticated. The switch, acting as the authenticator, uses the information in the RADIUS attributes to apply the related filters to the supplicant. Dynamic filters can be applied to multiple ports on the same switch, or to multiple switches that the use same authentication server, providing centralized access control for the network.

You can define firewall filters directly on the RADIUS server by using the Juniper-Switching-Filter attribute, which is a RADIUS attribute specific to Juniper Networks, also known as a vendor-specific attribute (VSA). VSAs are described in RFC 2138, *Remote Authentication Dial In User Service* (RADIUS). The Juniper-Switching-Filter VSA is listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server, with the vendor ID set to the Juniper Networks ID number 2636. Using this attribute, you define filters on the authentication server, which are applied on all switches that authenticate supplicants through that server. This method eliminates the need to configure the same filters on multiple switches.

Alternatively, you can apply a port firewall filter to multiple ports on the same switch by using the Filter-ID attribute, which is RADIUS attribute ID number 11. To use the Filter-ID attribute, you must first configure a filter on the switch, and then add the filter name to user policies on the RADIUS server as the value of the Filter-ID attribute. When a supplicant defined in one of those policies is authenticated by the RADIUS server, the filter is applied to the switch port that has been authenticated for the supplicant. Use this method when the firewall filter has complex conditions, or if you want to use different conditions for the same filter on different switches. The filter named in the Filter-ID attribute must be configured locally on the switch at the [`edit firewall family ethernet-switching filter`] hierarchy level.

VSAs are supported only for 802.1X single supplicant configurations and multiple supplicant configurations.

SEE ALSO

Understanding Authentication on Switches

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch | 467

Configuring Firewall Filters (CLI Procedure)

Juniper-Switching-Filter VSA Guidelines, Match Conditions and Actions | 198

Understanding Dynamic VLAN Assignment Using RADIUS Attributes

VLANs can be dynamically assigned by a RADIUS server to supplicants requesting 802.1X authentication through that server. You configure the VLAN on the RADIUS server using RADIUS server attributes, which are clear-text fields encapsulated in messages sent from the authentication server to the switch when a supplicant connected to the switch requests authentication. The switch, acting as the authenticator, uses the information in the RADIUS attributes to assign the VLAN to the supplicant. Based on the results of the authentication, a supplicant that began authentication in one VLAN might be assigned to another VLAN.

Successful authentication requires that the VLAN ID or VLAN name is configured on the switch acting as 802.1X authenticator, and that it matches the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is not authenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

The RADIUS server attributes used for dynamic VLAN assignment described in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*.

- Tunnel-Type—Defined as RADIUS attribute type 64. The value should be set to `VLAN`.
- Tunnel-Medium-Type—Defined as RADIUS attribute type 65. The value should be set to `IEEE-802`.
- Tunnel-Private-Group-ID—Defined as RADIUS attribute type 81. The value should be set to the VLAN ID or the VLAN name.

For more information about configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

SEE ALSO

Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 434

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 460

Configuring VLAN Groups on EX Series Switches

With the VLAN group feature, you can distribute clients across the VLANs. When you enable this feature, you can align a single wireless LAN (WLAN) to a single VLAN or to multiple VLANs. When you configure VLAN group, a client gets assigned to one of the configured VLANs. This feature supports dynamic load balancing of users across VLANs in a VLAN group. This feature follows the round-robin algorithm to assign users to the next available VLAN in a VLAN group.

For dynamic VLAN load balancing, you add the VLAN group name instead of a regular VLAN ID or a VLAN name in the `Tunnel-Private-Group-ID` attribute (defined in RFC 2868 as RADIUS attribute type 81). Subsequently, you send this information in the RADIUS response when a supplicant requests 802.1X authentication through the RADIUS server. When the switch receives the VLAN group name, the switch assigns the endpoint to one of the VLANs in that group using the round-robin algorithm. The VLAN group enables allocating a VLAN from a preconfigured list, thus reducing the need for administrators to load balance the network.

When you configure a VLAN group, note that:

- You can configure a maximum of 4096 VLAN groups.
- You must create a VLAN before allocating it to clients. Any VLAN that does not exist on the switch is ignored during allocation.
- A VLAN name cannot be the same as the VLAN group name.
- A VoIP VLAN should not be part of vlan-group. A VoIP VLAN, if present, will be ignored.
- When you delete a VLAN, all the 802.1X authenticated sessions associated with that VLAN are terminated.
- You can delete a VLAN group without causing any disruption for the clients that have already been allocated to VLANs in that VLAN group.
- You can remove a VLAN from a VLAN group without causing any disruption to the clients that have already been allocated to that VLAN. However, a client may face disruption if:
  - The client session expires.
  - A reauthentication or a change of role is performed using change of authorization (CoA) request.

To configure VLAN groups on EX Series switches:

1. Configure `vlans vlan-groups` *vlan_group_name*. Use the following command:

```
[edit]
user@switch# set vlans vlan-groups vlan_group_name vlan-id-list vlan-id-list
```

```
[edit]
user@switch# set vlans vlan-groups group1 vlan-id-list [500 600 700-750]
```

2. Commit the configuration and exit configuration mode.

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

3. To verify results of the configuration on a switch:

```
[edit]
user@switch> show vlans vlan-groups
```

```
user@switch> show vlans vlan-groups

Vlan Group Name:          Last vlan used:    Associated Vlan Ids:
group1                    0
                                             500, 600, 700-750
```

SEE ALSO

vlan-groups

show vlans vlan-groups

Understanding Guest VLANs for 802.1X on Switches

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for corporate guests. Guest VLAN is used as a fallback when:

- The supplicant is not 802.1X-enabled and does not respond to EAP messages.

- MAC RADIUS authentication has not been configured on the switch interfaces to which the supplicant is connected.
- Captive portal has not been configured on the switch interfaces to which the supplicant is connected.

A guest VLAN is not used for supplicants that send incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

SEE ALSO

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | **460**

Understanding Authentication on Switches

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch

IN THIS SECTION

Server fail fallback enables you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable.

You use 802.1X to control network access. Only users and devices (supplicants) providing credentials that have been verified against a user database are allowed access to the network. You use a RADIUS server as the user database.

This example describes how to configure an interface to move a supplicant to a VLAN in the event of a RADIUS server timeout:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Configured users on the authentication server.

Overview and Topology

IN THIS SECTION

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, you configure alternative options for supplicants attempting LAN access. You can configure the switch to accept or deny access to supplicants or to maintain the access already granted to supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs.

Figure 8 on page 402 shows the topology used for this example. The RADIUS server is connected to the EX4200 switch on access port **ge-0/0/10**. The switch acts as the authenticator port access entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface ge-0/0/1.

NOTE: This figure also applies to QFX5100 switches.

Figure 8: Topology for Configuring 802.1X Options

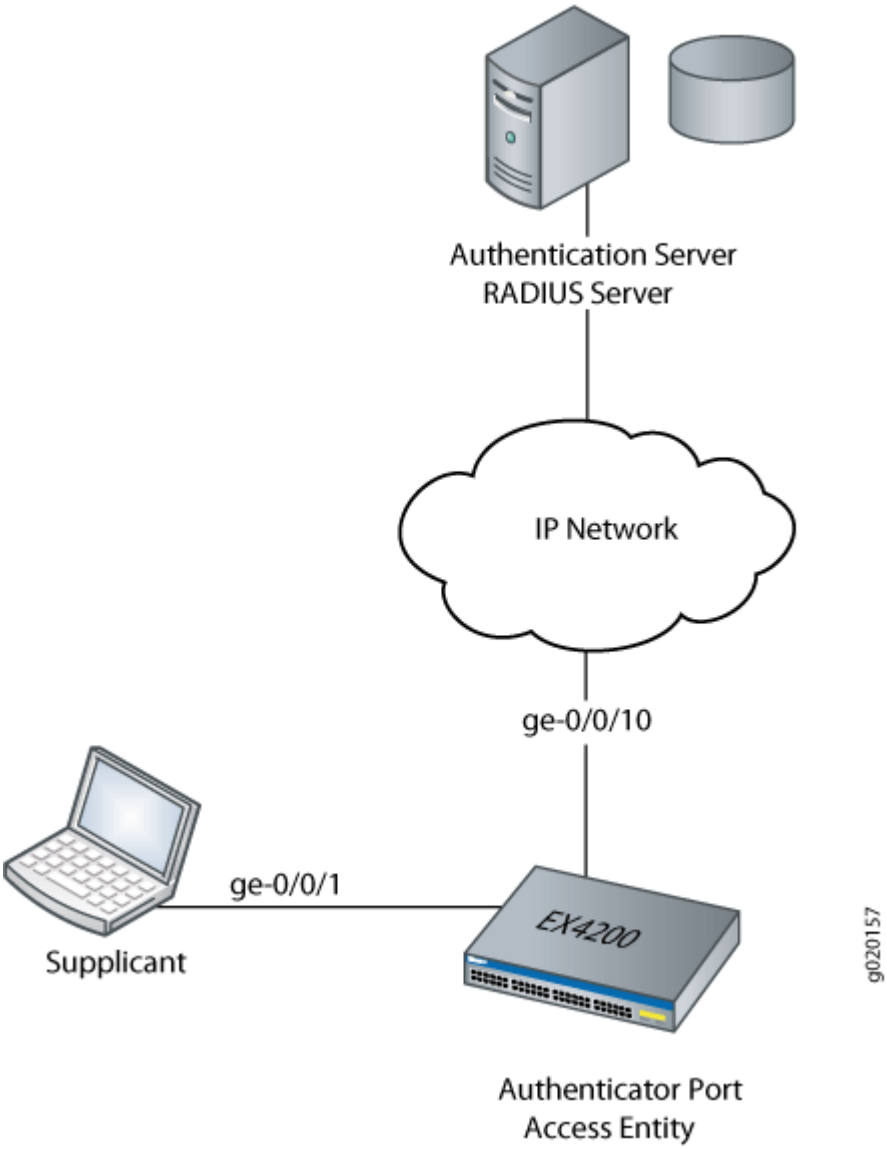


Table 25 on page 402 describes the components in this topology.

Table 25: Components of the Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.

Table 25: Components of the Topology *(Continued)*

Property	Settings
VLAN names	**default** VLAN **vlan-sf** VLAN
Supplicant	Supplicant attempting access on interface **ge-0/0/1**
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, configure interface ge-0/0/1 to move a supplicant attempting access to the LAN during a RADIUS timeout to another VLAN. A RADIUS timeout prevents the normal exchange of EAP messages that carry information from the RADIUS server to the switch and permit the authentication of a supplicant. The default VLAN is configured on interface ge-0/0/1. When a RADIUS timeout occurs, supplicants on the interface will be moved from the default VLAN to the VLAN named vlan-sf.

Topology

Configuration

IN THIS SECTION

- Procedure | 403

Procedure

CLI Quick Configuration

To quickly configure server fail fallback on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit protocols dot1x authenticator]
set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Step-by-Step Procedure

To configure an interface to divert supplicants to a specific VLAN when a RADIUS timeout occurs (here, the VLAN is **vlan-sf**):

1. Define the VLAN to which supplicants are diverted:

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Results

Display the results of the configuration:

```
user@switch> show configuration
    interfaces {
        ge-0/0/1 {
            unit 0 {
                family ethernet-switching {
                    vlan {
                        members default;
                    }
                }
            }
        }
    protocols {
        dot1x {
            authenticator {
                interface {
                    ge-0/0/1.0 {
                        server-fail vlan-name vlan-sf;
                    }
                }
            }
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout

Purpose

Verify that the interface moves supplicants to an alternative VLAN during a RADIUS timeout.

NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see *show vlans*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*

Action

Display the VLANs configured on the switch; the interface **ge-0/0/1.0** is a member of the **default** VLAN:

```
user@switch>   show vlans
Name           Tag     Interfaces
default
                       ge-0/0/0.0, ge-0/0/1.0*, ge-0/0/5.0*, ge-0/0/10.0,
                       ge-0/0/12.0*, ge-0/0/14.0*, ge-0/0/15.0, ge-0/0/20.0
v2             77
                       None
vlan-sf        50
                       None
mgmt
                       me0.0*
```

Display 802.1X protocol information on the switch to view supplicants that are authenticated on interface `ge-0/0/1.0`:

```
user@switch>                              show dot1x interface brief
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Authenticated   00:00:00:00:00:01    abc
ge-0/0/10.0   Authenticator  Initialize
ge-0/0/14.0   Authenticator  Connecting
ge-0/0/15.0   Authenticator  Initialize
ge-0/0/20.0   Authenticator  Initialize
```

A RADIUS server timeout occurs. Display the Ethernet switching table to show that the supplicant with the MAC address **00:00:00:00:00:01** previously accessing the LAN through the **default** VLAN is now being learned on the VLAN named **vlan-sf**:

```
user@switch>                show ethernet-switching
table
Ethernet-switching table: 3 entries, 1 learned
  VLAN              MAC address       Type         Age Interfaces
  v1                *                 Flood          - All-members
  vlan-sf           00:00:00:00:00:01 Learn       1:07 ge-0/0/1.0
  default           *                 Flood          - All-members
```

Display 802.1X protocol information to show that interface **ge-0/0/1.0** is connecting and will open LAN access to supplicants:

```
user@switch>                              show dot1x interface brief

802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Connecting
ge-0/0/10.0   Authenticator  Initialize
ge-0/0/14.0   Authenticator  Connecting
ge-0/0/15.0   Authenticator  Initialize
ge-0/0/20.0   Authenticator  Initialize
```

Meaning

The `show vlans` command displays interface **ge-0/0/1.0** as a member of the **default** VLAN. The `show dot1x interface brief` command shows that a supplicant (**abc**) is authenticated on interface **ge-0/0/1.0** and has the MAC address **00:00:00:00:00:01**. A RADIUS server timeout occurs, and the authentication server cannot be reached by the switch. The **show-ethernet-switching table** command shows that MAC address **00:00:00:00:00:01** is learned on VLAN **vlan-sf**. The supplicant has been moved from the **default** VLAN to the **vlan-sf** VLAN. The supplicant is then connected to the LAN through the VLAN named **vlan-sf**.

SEE ALSO

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**
- Configuring RADIUS Server Fail Fallback (CLI Procedure) | **354**
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | **448**
- Understanding Server Fail Fallback and Authentication on Switches | **353**

Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients

IN THIS SECTION

For 802.1X user authentication, EX Series switches support RADIUS authentication servers that are using Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) to authenticate Odyssey Access Client (OAC) supplicants. OAC networking software runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices) and provides secure access to both wired and wireless networks.

This example describes how to configure an 802.1X-enabled interface on the switch to provide fallback support for OAC users who have entered incorrect login credentials:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 11.2 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.
- One OAC end device acting as a supplicant.

Before you begin configuring the fallback option, ensure that you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Configured EAP-TTLS on the server. See your RADIUS server documentation.
- Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

IN THIS SECTION

OAC is networking software that runs on endpoint computers (desktop, laptop, or notepad) and supported wireless devices. OAC provides full support for EAP, which is required for secure wireless LAN access.

In this topology, OAC is deployed with an 802.1X-enabled switch and a RADIUS server. The switch functions as an enforcement point in the network security architecture. This topology:

- Ensures that only authorized users can connect.
- Maintains privacy of login credentials.
- Maintains data privacy over the wireless link.

This example includes the configuration of a server-reject VLAN on the switch, which can be used to prevent accidental lockout for users who have entered incorrect login credentials. These users can be given limited LAN access.

However, this fallback configuration is complicated by the fact that the OAC supplicant and RADIUS server are using EAP-TTLS. EAP-TTLS creates a secure encrypted tunnel between the server and the end device to complete the authentication process. When the user enters incorrect login credentials, the RADIUS server sends EAP failure messages directly to the client through this tunnel. The EAP failure message causes the client to restart the authentication procedure, so that the switch's 802.1X authentication process tears down the session that was established with the switch using the server-reject VLAN. You can enable the remedial connection to continue by configuring:

- **eapol-block**—Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN. The block timer causes the authentication port access entity to ignore EAP start messages from the client, attempting to restart the authentication procedure.

  NOTE: The EAPoL block timer is triggered only after the configured number of allowed reattempts (using the **retries** option) on the 802.1X interface have been exhausted. You can configure **retries** to specify the number of times the switch attempts to authenticate the port after an initial failure. The default is three retries.

- **block-interval**—Configure the amount of time that you want the EAPoL block timer to continue to ignore EAP start messages. If you do not configure the block interval, the EAPoL block timer defaults to 120 seconds.

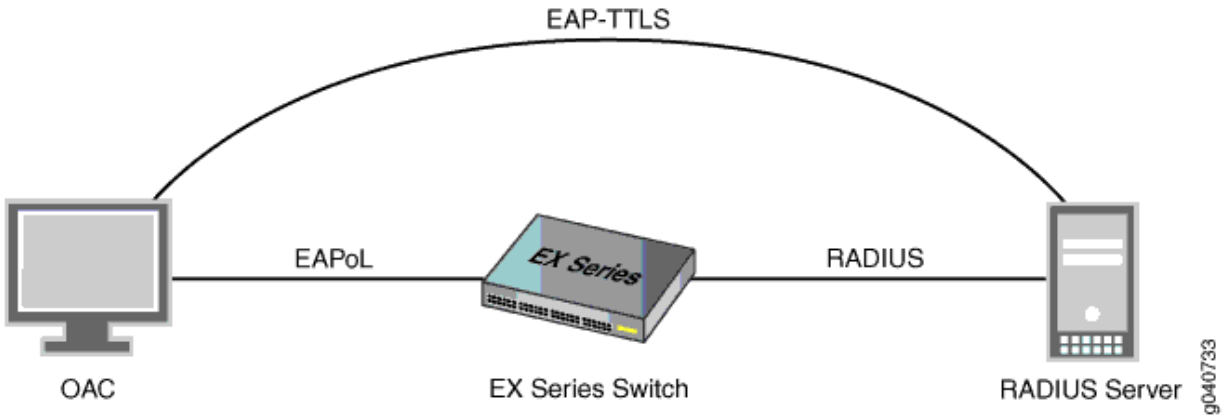
When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing remedial session that was established through the server-reject VLAN to remain open.

These configuration options apply to single, single-secure, and multiple supplicant authentication modes. In this example, the 802.1X interface is configured in single supplicant mode.

Figure 9 on page 410 shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.

NOTE: This figure also applies to QFX5100 switches.

Figure 9: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication



Topology

Table 26 on page 410 describes the components in this OAC deployment:.

Table 26: Components of the OAC Deployment

Property	Settings
Switch hardware	EX Series switch
VLANs	**default** **server-reject-vlan**: VLAN name is **remedial** and VLAN ID is **700**
802.1X interface	**ge-0/0/8**
OAC supplicant	EAP-TTLS
One RADIUS authentication server	EAP-TTLS

Configuration

IN THIS SECTION

- Procedure | 411

Procedure

CLI Quick Configuration

To quickly configure the fallback options for EAP-TTLS and OAC supplicants, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans remedial vlan-id 700
set protocols dot1x authenticator interface ge-0/0/8 retries 4
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan remedial
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan eapol-block
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130
```

Step-by-Step Procedure

To configure the fallback options for EAP-TTLS and OAC supplicants:

TIP: In this example, the switch has only one server-reject VLAN. Therefore, the configuration specifies **eapol-block** and **block-interval** directly after **server-reject-vlan**. However, if you have configured multiple VLANs on the switch, you must include the VLAN name or VLAN ID directly after **server-reject-vlan** to indicate which VLAN is being modified.

1. Configure a VLAN that will function as the server-reject VLAN to provide limited LAN access for users who have entered incorrect login credentials:

```
[edit]
user@switch# set vlans remedial vlan-id 700
```

2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set retries 4
```

3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan remedial
```

4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN.

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan eapol-block
```

5. Configure the amount of time for the EAPoL block to remain in effect:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan block-interval 130
```

Results

Check the results of the configuration:

```
user@switch> show configuration
    protocols {
        dot1x {
            authenticator {
                interface {
                    ge-0/0/8.0 {
                        supplicant single;
                        retries 4;
                        server-reject-vlan remedial block-interval 130 eapol-block;
                    }
```

Verification

IN THIS SECTION

- Verifying the Configuration of the 802.1X Interface | 413

To confirm that the configuration and the fallback options are working correctly, perform this task:

Verifying the Configuration of the 802.1X Interface

Purpose

Verify that the 802.1X interface is configured with the desired options.

Action

```
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 4
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 120 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPoL requests: 2
  Guest VLAN member: guest
  Number of connected supplicants: 1
    Supplicant: tem, 2A:92:E6:F2:00:00
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: remedial
```

```
        Session Reauth interval: 120 seconds
        Reauthentication due in 68 seconds
```

Meaning

The `show dot1x ge-0/0/8 detail` command output shows that the **ge-0/0/8** interface is in the **Authenticated** state and that it is using the **remedial** VLAN.

SEE ALSO

- Understanding Authentication on Switches

Monitoring 802.1X Authentication

IN THIS SECTION

Purpose

NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to display details of authenticated users and users that failed authentication.

Action

To display authentication details in the J-Web interface, select **Monitoring** > **Security** > **802.1X**.

To display authentication details in the CLI, enter the following commands:

- `show dot1x interface detail | display xml`

- `show dot1x interface detail <interface> | display xml`
- `show dot1x auth-failed-users`

Meaning

The details displayed include:

- A list of authenticated users.
- The number of connected users.
- A list of users that failed authentication.

You can also specify an interface for which the details must be displayed.

SEE ALSO

Configuring 802.1X Authentication (J-Web Procedure)

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Verifying 802.1X Authentication

IN THIS SECTION

Purpose

Verify that supplicants are being authenticated on an interface on a switch with the interface configured for 802.1X authentication, and display the method of authentication being used.

Action

Display detailed information about an interface configured for 802.1X (here, the interface is ge-0/0/16):

```
user@switch> show dot1x interface ge-0/0/16.0 detail
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
      Reauthentication due in 17 seconds
```

Meaning

The sample output from the `show dot1x interface detail` command shows that the `Number of connected supplicants` is 1. The supplicant that was authenticated and is now connected to the LAN is known as **user5** on the RADIUS server and has the MAC address **00:30:48:8C:66:BD**. The supplicant was authenticated by means of the 802.1X authentication method called RADIUS authentication, as indicated by `Radius` in the output. When RADIUS authentication is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN **v200**.

Other 802.1X authentication methods supported on EX Series switches in addition to RADIUS authentication are:

- Guest VLAN—A nonresponsive host is granted Guest-VLAN access.

- MAC Radius—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server notifies the switch that the MAC address is a permitted address, and the switch grants LAN access to the nonresponsive host on the interface to which it is connected.
- Server-fail deny—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from the supplicant from traversing through the interface. This is the default.
- Server-fail permit—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant were successfully authenticated by the RADIUS server.
- Server-fail use-cache—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted LAN access, but new supplicants are denied LAN access.
- Server-fail VLAN—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

SEE ALSO

Configuring 802.1X Authentication (J-Web Procedure)

Configuring MAC RADIUS Authentication (CLI Procedure) | **433**

Configuring RADIUS Server Fail Fallback (CLI Procedure) | **354**

Troubleshooting Authentication of End Devices on EX Series Switches

IN THIS SECTION

Problem

Description

End devices configured using static MAC addresses lose connection to the switch after the clear dot1x interface command is run to clear all learned MAC addresses.

Before clearing MAC addresses:

```
user@switch# run show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  vlan100           *                 Flood          - All-members
  default           *                 Flood          - All-members
  default           00:a0:d4:00:03:00 Learn          0 ge-3/0/16.0

user@switch> show dot1x authentication-bypassed-users
MAC address        Interface         VLAN
00:a0:d4:00:03:00  ge-3/0/16.0       configured/default
```

To clear MAC addresses:

```
user@switch> clear dot1x interface
```

After clearing MAC addresses:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 2 entries, 0 learned, 0 persistent entries
  VLAN              MAC address       Type         Age Interfaces
  vlan100           *                 Flood          - All-members
  default           *                 Flood          - All-members

user@switch> show dot1x authentication-bypassed-users
```

Note that there are no end devices on the authentication bypass list.

Cause

Static MAC addresses are treated the same as other learned MAC addresses on an interface. When the clear dot1x interface command is run, it clears all learned MAC addresses from the interface, including the static MAC bypass list (also known as the exclusion list).

Solution

If you run the clear dot1x interfaces command for an interface that has static MAC addresses configured for authentication bypass, re-add the static MAC addresses to the static MAC bypass list.

SEE ALSO

> *clear dot1x*
>
> Understanding Authentication on Switches

RADIUS Attributes and Juniper Networks Vendor-Specific Attributes (VSAs) Supported by 802.1X

Authenticator (Network Access Server), supplicant (client), and the authentication server are all involved in 802.1X authentication (RADIUS-server). The RADIUS protocol is used as a request/response mechanism for communication between the NAS and Radius-server. There are zero or more Type Length Values (TLVs/Attributes) in both requests and responses.

Each applicant's access can be restricted by using a standard set of defined features and vendor-specific attributes enabled by 802.1X. (client). Certain attributes may be utilised more than once in order to support longer values because the Radius Class attribute has a maximum size of 253 bytes.

Benefits of Using RADIUS Standard Attributes and VSAs

To connect with an external RADIUS server for subscriber authentication, authorization, and accounting, RADIUS standard attributes are required.

VSAs enable the implementation of numerous valuable features that are necessary for subscriber management and service support, extending the RADIUS server's capability beyond what is provided by public standard attributes.

Radius Attributes and VSA list supported by 802.1X

Table 27 on page 420 lists the RADIUS Attributes and VSAs supported by 802.1X, and the defining RFC for each attribute.

Table 27: Radius Attributes and VSA list supported by 802.1X

Type	Attribute	Definition
1	User-Name	RFC 2865
6	Service-Type	RFC 2865
11	Filter-Id	RFC 2865
24	State	RFC 2865
25	Class	RFC 2865
26	Vendor-Specific	RFC 2865
27	Session-Timeout	RFC 2865
56	Egress-VLANID	RFC 4675
57	Egress-VLAN-Name	RFC 4675
61	NAS-Port-Type	RFC 2865
64	Tunnel-Type	RFC 2868
65	Tunnel-Medium-Type	RFC 2868
81	Tunnel-Private-Group-ID	RFC 2868
85	Acct-Interim-Interval	RFC 2869

Table 27: Radius Attributes and VSA list supported by 802.1X *(Continued)*

Type	Attribute	Definition
102	EAP-Key-Name	RFC 4072

Table 28 on page 421lists the Vendor IDs and Juniper VSAs.

Table 28: Vendor IDs and Juniper VSAs

Vendor ID	Number	Juniper VSAs	Microsoft VSAs	Cisco VSA
2636	48	Juniper-Switching-Filter		
	49	Juniper-VoIP-Vlan		
	50	Juniper-CWA-Redirect-URL		
	52	Juniper-AV-Pair = Port-Bounce		
		Juniper-AV-Pair = Juniper Ip-Mac-Session-Binding		
		Juniper-AV-Pair = No-Mac-Binding-Reauth		
		Juniper-AV-Pair = Supplicant-Mode-Single		
		Juniper-AV-Pair = Supplicant-Mode-Single-Secure		
		Juniper-AV-Pair = Retain-Mac-Aged-Session		
	53	Juniper-Event-Type		
	54	Juniper-Sub-Event-Type		

Table 28: Vendor IDs and Juniper VSAs *(Continued)*

Vendor ID	Number	Juniper VSAs	Microsoft VSAs	Cisco VSA
	55	Juniper-Generic-Message		
311	16		MS-MPPE-Send-Key	
	17		MS-MPPE-Recv-Key	
9	1			Cisco-AVPair = "subscriber:command=bounce-host-port"
				Cisco-AVPair = "subscriber:command=reauthenticate"
				Cisco-AVPair = "subscriber:reauthenticate-type=rerun"
				"subscriber:reauthenticate-type=last"
				"url-redirect"

802.1X Supported RADIUS Attributes

User-Name:

The name of the user who has to be verified is indicated by this attribute. If available, Access-Request packets must be used to send this attribute. The RADIUS type for this attribute is 1.

Filter-Id:

On the RADIUS server, user policies can be subject to a firewall filter. The RADIUS server can then be utilised to specify the firewall filters to be applied to each user who submits an authentication request. Each switch needs to be configured with firewall filters.

You must set up firewall filter on the local switch in order to apply filter centrally from the RADIUS server.

```
[root@freeradius]#
cd /usr/local/pool/raddb
vi users
```

Add the filter for each relevant user.

```
Filter-Id = Filter1
```

To activate the configuration, restart the RADIUS server now.

NOTE: VSAs take precedence over filters if port firewall filters are also locally specified for the interface. VSAs and local port firewall filters are integrated if they do not clash. Moreover, more than one filter cannot be implemented on a single interface. But, by establishing a single filter with policies for each of those users, you can support multiple filters for numerous users who are connected to the switch on the same interface.

State:

Between the device and the RADIUS server, state information can be preserved with the use of the String attribute. The RADIUS type for this attribute is 24.

Egress-VLANID:

A permitted IEEE 802 Egress VLANID for this port is represented by the Egress-VLANID attribute, which also specifies whether the VLANID is permitted for tagged or untagged frames in addition to VLANID. The Egress-VLANID attribute is defined in In RFC 4675.

Egress-VLANID attributes from the Access-Request, Access-Accept, or CoA-Request packets may include multiple values. No Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK may include this characteristic. Every attribute adds the provided VLAN to the port's list of permitted egress VLANs.

If the frames on VLAN are tagged (0x31) or untagged (0x32), the Tag Indication field, which is one octet in length states it. The VLANID is 12 bits in length and contains the VLAN VID value.

For Egress-VLAN-ID:

```
0x31 = tagged
0x32 = untagged
```

For example, the following RADIUS profile includes one tagged and one untagged VLAN:

```
001094001177 Cleartext-Password := "001094001177"
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Egress-VLANID += 0x3100033,
Egress-VLANID += 0x3200034,
```

Egress-VLAN-Name:

Egress-VLAN-Name represents a permitted VLAN for this port. Similar to the Egress-VLANID attribute, however instead of using the VLAN-ID, which is defined or known, the VLAN name is used to identify the VLAN within the system. RFC 4675 contains a definition for the Egress-VLAN-Name attribute.

The VLAN name is the second part of the two-part Egress-VLAN-Name attribute, which also specifies whether frames on the VLAN for this port should be displayed in tagged or untagged format.

For Egress-VLAN-Name: 1 = tagged and 2 = untagged

The example below shows that VLAN 1vlan-2 is tagged, while VLAN 2vlan-3 is not.

```
001094001144 Cleartext-Password := "001094001144"
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Egress-VLAN-Name += 1vlan-2,
Egress-VLAN-Name += 2vlan-3,
```

Tunnel-Type:

This attribute specifies either the tunnelling protocol currently in use or the tunnelling protocol that will be used (in the case of a tunnel initiator) (in the case of a tunnel terminator). RFC 2868 specifies the Tunnel-Type attribute. The RADIUS type for this attribute is 64

Tunnel-Private-Group-Id:

The VLAN ID or NAME for the session is displayed by the Tunnel-Medium-Type attribute. The device verifies if the string it receives is a VLAN name or an ID after getting a value supplied for the Tunnel-Private-Group-ID attribute from the radius and checks to see if the device is setup with a VLAN.

If a VLAN has been configured, the client port is added to that VLAN. Otherwise, due to a failure in the VLAN validation, the client won't be permitted and will be maintained in a held status.

The RADIUS type for this attribute is 81, as per RFC 2868.

```
[root@freeradius]# cat /usr/local/etc/raddb/users
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
Tunnel-Type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-Id = "1005",
```

Acct-Interim-Interval:

The value of the Acct-Interim-Interval attribute represents the time interval in seconds between each transmittal of an interim update for a particular session. The number of seconds that have passed since the last accounting update message is the value of this attribute.

A minimum value may also be set by an administrator locally on a RADIUS client, however this value always takes precedence over any Acct-Interim-Interval values detected in an Access-Accept packet. The RADIUS type for this attribute is 85.

Juniper Networks VSAs

Juniper-Switching-Filter:

The Juniper-Switching-Filter attribute in the Juniper dictionary on the RADIUS server allows you to specify straightforward filter criteria. After that, whenever a new user is successfully authorised, these filters are delivered to a switch.

Switches that use RADIUS server for user authentication automatically construct and apply the filters without requiring any switch-specific configuration. Enter one or more match conditions, actions, and user associations in the RADIUS server to configure the Juniper-Switching-Filter property.

For longer switching-filters, use multiple instances of the Juniper-switching-filter attribute with a maximum limit of 20 match conditions and a maximum total size of 4000 characters. The maximum length of any radius attribute is 253 characters, so each line of the "Juniper-switching-filter" attribute should also be less than 253 characters.

```
 spirent123 Auth-Type := EAP, User-Password := "spirent123"
 Juniper-Switching-Filter = "match src-tag dst-port [ 80 25 443 ] src-port [5060 1025-2000]
action allow ",
 Juniper-Switching-Filter += "match src-port 500 dst-port 600 src-tag [ 100, 200 ] action allow
```

```
",
 Juniper-Switching-Filter += "match ip-proto src-port 9090 ip-proto [ 25 17] action allow ",
 Juniper-Switching-Filter += "match src-port 100-120 200-220 300-320 src-tag ip-proto 26 18
action allow ",
 Juniper-Switching-Filter += "match ether-type [ 3000-4000 8000 ] ip-proto 240 action allow "
```

The following filter match conditions are supported:

```
· destination-mac / dst-mac
· destination-port / dst-port
· destination-ip / dst
· ip-protocol / ip-proto
· source-port / src-port
· source-dot1q-tag / src-tag
· ether-type
```

The following filter actions are supported:

```
- Allow
· Deny
· GBP
· Trap to CPU
· Loss-Priority
```

To configure match conditions on the RADIUS server:
i) Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute Juniper-Switching-Filter, attribute ID 48:

```
[root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper
# dictionary.juniper
#
$
# VENDOR Juniper 2636
BEGIN-VENDOR Juniper
ATTRIBUTE Juniper-Local-User-Name 1 string
ATTRIBUTE Juniper-Allow-Commands 2 string
ATTRIBUTE Juniper-Deny-Commands 3 string
ATTRIBUTE Juniper-Allow-Configuration 4 string
ATTRIBUTE Juniper-Deny-Configuration 5 string
ATTRIBUTE Juniper-Switching-Filter 48 string
ATTRIBUTE Juniper-VoIP-Vlan 49 string
```

```
ATTRIBUTE Juniper-CWA-Redirect 50 string
ATTRIBUTE Juniper-AV-Pair 52 string
END-VENDOR Juniper
```

ii) Enter the match conditions and actions.

```
[root@freeradius]#
cd /usr/local/etc/raddb
vi users
```

For each relevant user, add the Juniper-Switching-Filter attribute. To deny or allow access based on the destination MAC, use

```
Juniper-Switching-Filter = "Match Destination mac 00:00:00:01:02:03 Action allow",
```

or

```
Juniper-Switching-Filter = "Match Destination-mac 00:00:00:01:02:03 Action deny",
```

To deny or allow access based on the destination IP address:

```
Juniper-Switching-Filter = "match destination-ip 192.168.1.0/31 action deny"
```

or

```
Juniper-Switching-Filter = "match destination-ip 192.168.1.0/31 action allow"
```

To send multiple filters with different matches and actions:

```
spirent123 Auth-Type := EAP, User-Password := "spirent123"
 Juniper-Switching-Filter += "Match Ip-protocol 1 Destination-port 53 Action allow,",
 Juniper-Switching-Filter += "Match ip-proto [ 17, 25 ] dst-port 53 Action allow,",
 Juniper-Switching-Filter += "Match Ip-protocol 2 src-port 67 Action allow,",
 Juniper-Switching-Filter += "match ether-type [ 3000-4000 8000] action deny,",
 Juniper-Switching-Filter += "Match destination-port 23 Action allow,",
 Juniper-Switching-Filter += "Match Ip-protocol 6 Destination-port 80 Action trap,",
```

or

```
Juniper-Switching-Filter = "Match Ip-protocol 6 Destination-port 53 Action allow , Match Ip-
protocol [ 17 25] Destination-port 53 Action allow , Match Ether-type [2054-2070] Action deny,
Match Ip-protocol 6 Destination-port 443 Action trap"
```

To set the packet loss priority (PLP) to high based on a destination MAC address and the IP protocol:

```
Juniper-Switching-Filter = "match destination-mac 00:04:0f:fd:ac:fe, ip-protocol 2, action loss-
priority high"
```

iii) For the configuration to take effect, stop and restart the RADIUS process.

Juniper-VoIP-Vlan:

The VOIP vlan is retrieved from the radius server using the VSA Juniper-VoIP-Vlan in an access-accept message or COA request message. This attribute is number 49.

```
 Juniper-VoIP-Vlan = "voip_vlan"
```

VoIP allows you to connect IP phones to the switch and set up IEEE 802.1X authentication for IP phones that are 802.1X-compatible.

Ethernet LANs are secured against illegal user access thanks to the 802.1X authentication. A protocol known as VoIP is used to transmit voice over packet-switched networks. A network connection, as opposed to an analog phone line, is used by VoIP to transmit voice calls. When VoIP is used with 802.1X, the RADIUS server verifies the phone's identity while Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) gives the phone the class-of-service (CoS) parameters.

Juniper-CWA-Redirect:

With the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary, the redirect URL can be centrally configured on the AAA server. The dynamic firewall filter and URL are both delivered by the AAA server to the switch in the same RADIUS Access-Accept message. As a backup authentication mechanism, central Web authentication (CWA) redirects the host's web browser to a central Web authentication server. The user can enter a username and password on the CWA server's web interface. The user is authenticated and given access to the network if the CWA server accepts their credentials.

After a host fails MAC RADIUS authentication, central Web authentication is used. The switch, acting as the authenticator, receives a RADIUS Access-Accept message from the AAA server that contains a dynamic firewall filter and a redirect URL for central Web authentication.

For the central Web authentication procedure to be activated, both the redirect URL and the dynamic firewall filter need to be present. To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter terms directly on the AAA server. The filter must include a term to match the destination IP address of the CWA server with the action allow.

For example:

```
 001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455" Session-Timeout = "300",
 Juniper-CWA-Redirect-URL = "https://10.10.10.10",
 Juniper-Switching-Filter = "Match Destination-ip 10.10.10.10 Action allow, Match ip-protocol 17
Action allow, Match Destination-mac 00:01:02:33:44:55 Action deny"
```

NOTE: For the redirect URL, the switch does not resolve DNS queries. To enable the CWA server's destination IP address, you must configure the Juniper-Switching-Filter property.

Juniper-AV-Pair:

The Juniper-AV-Pair attribute is a Juniper Networks vendor-specific attribute (VSA). In order to provide numerous important features required for subscriber management and service support, it is used to enhance the capabilities of the RADIUS server beyond that offered by the public standard attributes.

i) Port-Bounce:

With the CoA bounce host port command, a session is ended and the port is bounced (initiates a link down event followed by a link up event). The request is sent by the radius server in a typical CoA-Request message with the VSA listed below:

```
 Juniper-AV-Pair = "Port-Bounce".
```

This command requires one or more of the session identification attributes listed in the "Session Identification" section because it is session-oriented. The device sends a CoA-NAK message with the error-code attribute "Session Context Not Found" if the session cannot be found.

The device shuts the hosting port for 4 seconds, enables it again (port bounce), and then returns a CoA-ACK if the session has been located.

ii) Ip-Mac-Session-Binding:

This is used to stop the authentication session for that device from being terminated when a device's MAC address ages out and needs to be re-learned. We receive this attribute-value from a VSA Juniper AV Pair on an access-accept or COA request message.

Configure the RADIUS server with both of the following attribute-value pairs in order to maintain the authentication session based on IP-MAC address bindings.

```
Juniper-AV-Pair = "IP-Mac-Session-Binding
Juniper-AV-Pair = "No-Mac-Binding-Reauth"
```

iii) No-Mac-Binding-reauth:

This is used to block client reauthentication and stop the authentication session from being terminated when a device's MAC address becomes outdated. This property value gets sent to us by a VSA Juniper AV Pair on an access-accept or COA request message.

```
Juniper-AV-Pair = "No-Mac-Binding-Reauth"
Detailed information is provided in the document:
Retain the Authentication Session Using IP-MAC Bindings
```

iv) Supplicant-Mode-Single:

The device switches from the current set mode to single in response to receiving this attribute-value from a VSA Juniper-AV-Pair on an access-accept or COA request message.

```
Juniper-AV-Pair = "Supplicant-Mode-Single"
```

v) Supplicant-Mode-Single-Secure:

The device switches from its current set mode to single-secure in response to receiving this attribute-value from a VSA Juniper-AV-Pair on an access-accept or COA request message.

```
Juniper-AV-Pair = "Supplicant-Mode-Single-Secure"
```

vi) Retain-Mac-Aged-Session:

If this attribute-value is received from a VSA Juniper-AV-Pair on an access-accept message for an 802.11X client, the client stays active even if the mac has aged out, and the mac is re-learned.

```
Juniper-AV-Pair = "Retain-Mac-Aged-Session"
```

MS-MPPE-Send-Key & MS-MPPE-Recv-Key:

These are the MACSEC CAK generation keys together with the EAP key name that are utilised in dynamic CAK scenarios.

Cisco-AVPair:

Cisco Systems, IANA private enterprise number 9, uses a single VSA, Cisco-AVPair (26-1). Based on the values it has, this VSA transmits various pieces of information. In some subscriber access networks with a BNG connected to a RADIUS server and a Cisco BroadHop application that serves as the Policy Control and Charging Rules Function (PCRF) server for provisioning services using RADIUS change of authorization (CoA) messages, you can use this VSA in RADIUS messages to activate and deactivate services.

When the BNG delivers RADIUS messages, you cannot change any of the properties in the accounting, CoA, or authentication answers.

i) Cisco-AVPair = "subscriber:command=bounce-host-port"

A session is ended and the port is bounced via the CoA bounce host port command (initiates a link down event followed by a link up event). The request is sent by the AAA server in a typical CoA-Request message with the VSA listed below.

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

This command requires one or more of the session identification attributes listed in the "Session Identification" section because it is session-oriented. The device sends a CoA-NAK message with the error-code attribute "Session Context Not Found" if the session cannot be found. The device shuts the hosting port for 4 seconds, enables it again (port bounce), and then returns a CoA-ACK if the session has been located.

ii) Cisco-AVPair Reauthenticate command

To initiate session authentication, the AAA server sends a standard CoA-Request message containing the following VSAs:

```
Cisco:Avpair="subscriber:command=reauthenticate"
Cisco:Avpair="subscriber:reauthenticate-type=<last | rerun>"
```

`reauthenticate-type` defines whether the CoA reauthentication request uses the authentication method that last succeeded on the session or whether the authentication process is completely rerun.

`"subscriber:command=reauthenticate"` must be present to cause a reauthentication. The default action is to repeat the previous successful authentication method used for the session if "subscriber:reauthenticate-type" is not given. If the method successfully reauthenticates, all previous authorization data is swapped out for the newly reauthenticated authorization data.

Only when "subscriber:command=reauthenticate" is also present is "subscriber:reauthenticate-type" valid. The VSA is disregarded if it is contained in another CoA command.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
20.2R1	Starting in Junos OS Release 20.2R1, you can configure 802.1X authentication on layer 3 interfaces
18.4R1	Starting in Junos OS Release 18.3R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device.
17.3R1	Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.

RELATED DOCUMENTATION

- RADIUS Server Configuration for Authentication | 345
- 802.1X and RADIUS Accounting | 444
- MAC RADIUS Authentication | 432
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 451
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 460

MAC RADIUS Authentication

IN THIS SECTION

You can control access to your network through a switch by using several different authentication methods. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network.

You can configure MAC RADIUS authentication on the switch interfaces to which the hosts are connected to provide LAN access. For more information, read this topic.

Configuring MAC RADIUS Authentication (CLI Procedure)

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the switch interfaces to which the hosts are connected.

NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPoL requests to the host. If there is no response from the host, the switch sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the **mac-radius restrict** option), the switch attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.

To configure MAC RADIUS authentication by using the CLI:

- On the switch, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the **restrict** qualifier for interface **ge-0/0/20** to have it use only MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f**):

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
 0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

- (Optional) Configure a global password for all MAC RADIUS authentication, instead of using the MAC address as the password (here the global password is **9H.fQ/CuEclFnclKMN-HqmPfQFn/AuOzF**):

```
[edit]#
user@switch# edit protocols dot1x authenticator mac-radius password $9$H.fQ/CuEclFnclKMN-
HqmPfQFn/AuOzF
```

SEE ALSO

Understanding Authentication on Switches

Example: Configuring MAC RADIUS Authentication on an EX Series Switch

IN THIS SECTION

To permit hosts that are not 802.1X-enabled to access a LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the switch will attempt to authenticate the host with the RADIUS server by using the host's MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches.
- An EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  NOTE: For more about ELS, see: *Using the Enhanced Layer 2 Software CLI*

- Performed basic 802.1X configuration. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378.

Overview and Topology

IN THIS SECTION

IEEE 802.1X port-based network access control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch by using the 802.1X protocol (that is, the devices are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is connected only to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication by using the **mac-radius restrict** option, and thus avoid the delay that occurs while the switch determines that the device is does not respond to EAP messages.

Figure 10 on page 437 shows the two printers connected to the switch.

NOTE: This figure also applies to QFX5100 switches.

Figure 10: Topology for MAC RADIUS Authentication Configuration

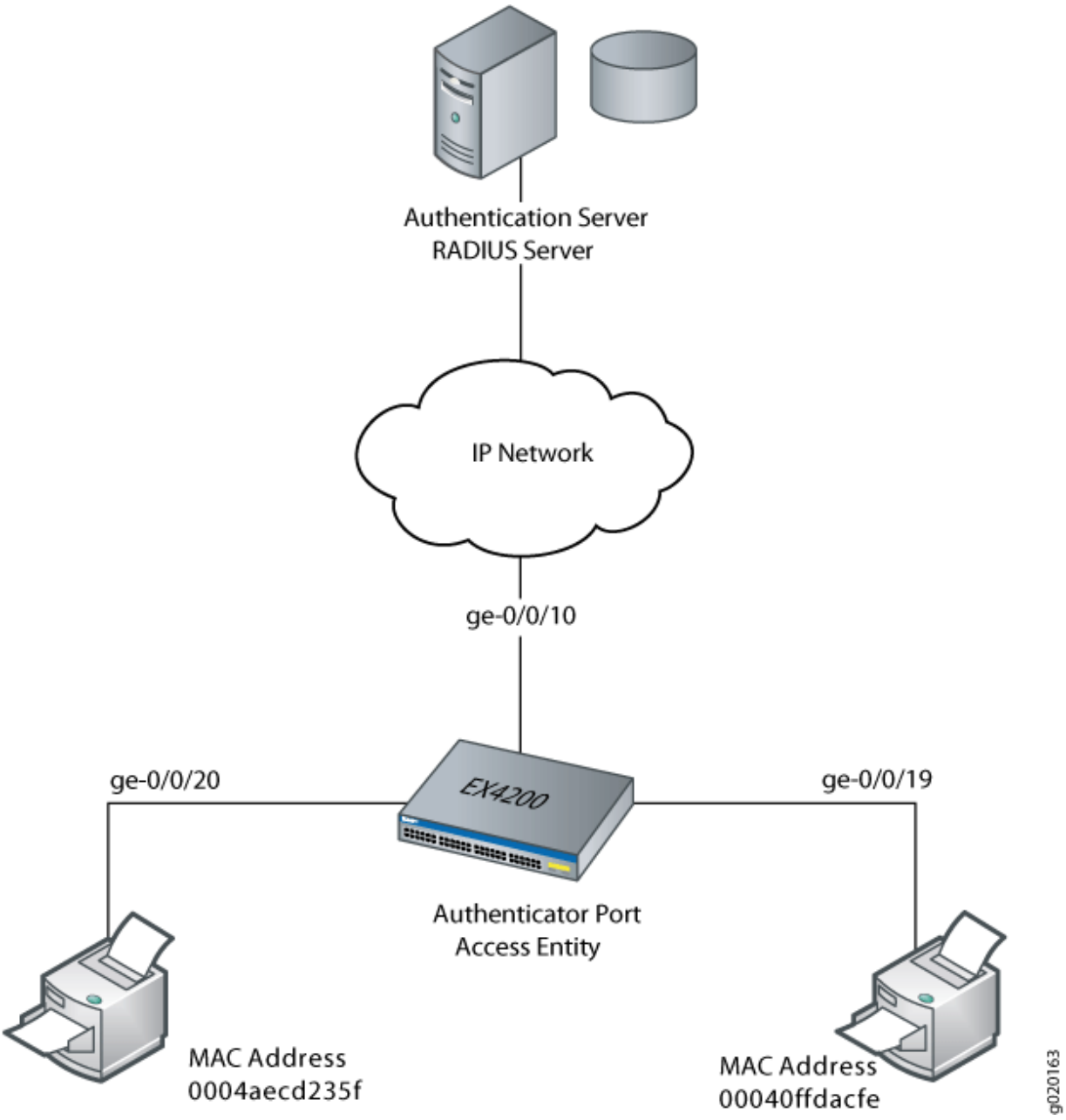


Table 29 on page 437 shows the components in the example for MAC RADIUS authentication.

Table 29: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200 ports (ge-0/0/0 through ge-0/0/23)

Table 29: Components of the MAC RADIUS Authentication Configuration Topology *(Continued)*

Property	Settings
VLAN name	sales
Connections to printers (no PoE required)	ge-0/0/19, MAC address 00040ffdacfe ge-0/0/20, MAC address 0004aecd235f
RADIUS server	Connected to the switch on interface **ge-0/0/10**

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the switch, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the switch attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the `mac radius restrict` option.

Topology

Configuration

IN THIS SECTION

- Procedure | 438

Procedure

CLI Quick Configuration

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
  set protocols dot1x authenticator interface ge-0/0/19 mac-radius
```

```
set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

NOTE: You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

Step-by-Step Procedure

Configure MAC RADIUS authentication on the switch and on the RADIUS server:

1. On the switch, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the restrict option on interface ge-0/0/20, so that only MAC RADIUS authentication is used:

```
[edit]
user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-
radius
user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

```
[root@freeradius]#
                            edit /etc/raddb
                            vi users
                            00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
                            0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
```

Results

Display the results of the configuration on the switch:

```
user@switch> show configuration
protocols {
    dot1x {
        authenticator {
            authentication-profile-name profile52;
```

```
            interface {
                ge-0/0/19.0 {
                    mac-radius;
                }
                ge-0/0/20.0 {
                    mac-radius {
                        restrict;
                    }
                }
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying That the Supplicants Are Authenticated | **440**

Verify that the supplicants are authenticated:

Verifying That the Supplicants Are Authenticated

Purpose

After supplicants are configured for MAC RADIUS authentication on the switch and on the RADIUS server, verify that they are authenticated and display the method of authentication.

Action

Display information about the 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

```
user@switch> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
```

```
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds

user@switch> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentcation method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
```

```
        Session Reauth interval: 60 seconds
        Reauthentication due in 50 seconds
```

Meaning

The sample output from the `show dot1x interface detail` command displays the MAC address of the connected end device in the **Supplicant** field. On interface ge-0/0/19, the MAC address is **00:04:0f:fd:ac:fe**, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **Radius**. On interface **ge-0/0/20**, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **Radius**.

RELATED DOCUMENTATION

Interfaces Enabled for 802.1X or MAC RADIUS Authentication | 467

Static MAC Bypass of 802.1X and MAC RADIUS Authentication | 493

Service-Type Attribute and Jumbo Frame Handling Overview

IN THIS SECTION

Service-Type Attribute support and Jumbo Frame handling are integral features that enhance network authentication and packet handling capabilities. The Service-Type Attribute enables the identification of service types requested or provided by the network access server (NAS) across different authentication modes, including MAC RADIUS, Extensible Authentication Protocol (EAP), and Captive Portal, each with specific Service-Type values such as Call Check, Framed, and Login. Jumbo Frame support extends the ability to process EAP packets with body lengths up to 4096 bytes, ensuring efficient handling of larger

authentication packets. These features improve the system's robustness, providing granular service-type information and accommodating larger packet sizes, which are essential for maintaining high network performance and reliability. Additionally, supplementary functionalities like EAP packet fragmentation and enhanced memory usage management further bolster the system's capacity to handle complex authentication scenarios.

Benefits of Service-Type Attribute Support and Jumbo Frame Handling

- Enhances network authentication reliability by supporting larger EAP packets up to 4096 bytes, ensuring that complex authentication data is transmitted without loss.
- Provides detailed service-type information for various authentication modes, improving the granularity of user management and network service allocation.
- Facilitates better network performance by allowing the system to efficiently process and fragment EAP packets that exceed the configured maximum transmission unit (MTU), ensuring seamless packet handling.
- Increases the flexibility of authentication mechanisms, supporting MAC RADIUS, EAP, and Captive Portal modes, each with specific Service-Type values tailored to the service context.
- Maintains system scalability with a minor increase in memory usage, ensuring that the network can support numerous clients without significant performance degradation.

Overview

Service-Type Attribute support and Jumbo Frame handling significantly enhance your network's authentication and packet processing capabilities. The Service-Type Attribute, which indicates the service type being requested or provided by the NAS, can be used in Access-Request and Access-Accept packets. This attribute is supported for MAC RADIUS, EAP, and Captive Portal authentication modes, each with specific Service-Type values—Call Check, Framed, and Login. This allows for more precise user management and service allocation, improving overall network efficiency.

Jumbo Frame support is another critical enhancement, enabling the processing of EAP packets with a body length exceeding the traditional 1496 bytes, up to a maximum of 4096 bytes. This support ensures that larger authentication packets, which are becoming increasingly common, are handled correctly without being dropped or fragmented unnecessarily. This capability is crucial for maintaining high performance and reliability within your network, especially in environments with complex authentication requirements.

Additionally, when the received EAP packet length exceeds the configured MTU limit on the interface, the packet will be fragmented and processed accordingly. This fragmentation mechanism ensures that even the largest EAP packets are managed efficiently without loss, optimizing the authentication process. While the implementation of these features does increase memory usage slightly—by approximately 2500 bytes per session—the trade-off is minimal compared to the substantial benefits in terms of network robustness and user experience.

CLI Commands

Understanding and configuring these features is streamlined through specific CLI commands. For instance, the command `run show dot1x accounting-attributes` provides detailed accounting attributes, including the new Service-Type field. This command aids in monitoring and troubleshooting network authentication sessions by displaying essential attributes such as NAS port, MAC address, called and calling station IDs, framed MTU, session timeout, and more.

802.1X and RADIUS Accounting

IN THIS SECTION

EX Series Switches support RADIUS accounting. You can configure RADIUS accounting on an EX Series switch to collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The data gathered is used for network monitoring purpose.

Understanding 802.1X and RADIUS Accounting on Switches

IN THIS SECTION

Juniper Networks EX Series Ethernet Switches support IETF RFC 2866, *RADIUS Accounting*. By configuring RADIUS accounting on an EX Series switch, you can collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based on the amount of time or type of services accessed.

RADIUS Accounting Process

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client forwards user accounting statistics to a designated RADIUS accounting server. The RADIUS accounting server must send a response to the client when it has successfully received and recorded the accounting statistics.

The RADIUS accounting process between a switch and a RADIUS server is based on the exchange of two types of RADIUS messages—Accounting-Request and Accounting-Response. Accounting-Request messages are sent from the switch to the server and convey information used to account for a service provided to a user. Accounting-Response messages are sent from the server to acknowledge receipt of the Accounting-Request packets. The exchange of messages between the switch and the server proceeds as follows:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. When a supplicant is authenticated through 802.1X authentication and then connected to the LAN, the switch forwards an Accounting-Request message with a record of the event to the accounting server. The Accounting-Request message sent by the switch includes the RADIUS attribute Acct-Status-Type with a value of Start, which indicates the beginning of user service for this supplicant. The accounting server records this event in the accounting log file as a start record.
3. The accounting server sends an Accounting-Response message back to the switch confirming that it received the accounting request. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

4. The switch might send an interim message to the accounting server to periodically update the server with information pertaining to a specific session. Interim messages are sent as Accounting-Request messages with the Acct-Status-Type attribute value of Interim-Update. The accounting server sends an Accounting-Response messae back to the switch to confirm receipt of an interim update.

5. When the supplicant's session ends, the switch forwards an Accounting-Request message with the Acct-Status-Type attribute value set to Stop, indicating the end of user service. The accounting server records this event in the accounting log file as a stop record that contains session information and the length of the session.

The statistics collected through this process can be displayed from the RADIUS server. To view those statistics, the user needs to access the accounting log file configured to receive them. On FreeRADIUS, the filename is the server's address—for example, 122.69.1.250.

Supported RADIUS Attributes

RADIUS accounting statistics are conveyed through the attributes included in each Accounting-Request message sent from the NAS to the server. Table 30 on page 446 list the RADIUS attributes supported for Accounting-Request messages.

Table 30: RADIUS Accounting Request Attributes

Type	Attribute	Description
1	User-Name	The name of the authenticated user.
5	NAS-Port	The physical port number of the NAS that authenticates the user. Either NAS-Port or NAS-Port-ID must be contained in the packet.
8	Framed-IP-Address	The IP address of the authenticated user. **NOTE**: The Framed-IP-Address attribute is sent only if a valid DHCP binding exists for the host in the DHCP snooping table.
11	Filter-ID	The name of the filter list for the user.
12	Framed-MTU	The maximum transmission unit that can be configured for the user.
26	Client-System-Name	Vendor-specific attribute (VSA) used to indicate the client's hostname. Supported for LLDP-capable devices only.

Table 30: RADIUS Accounting Request Attributes *(Continued)*

Type	Attribute	Description
27	Session-Timeout	Sets the maximum time (in seconds) that a session stays active before it terminates or a prompt is issued notifying its termination.
28	Idle-Timeout	The maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
30	Called-Station-ID	Enables the NAS to identify the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology.
31	Calling-Station-ID	Enables the NAS to identify the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology.
32	NAS-Identifier	Contains a string identifying the NAS originating the Accounting-Request message.
40	Acct-Status-Type	Indicates whether this Accounting-Request message marks the beginning (Start) or the end (Stop) of the user session. Can also be used for an interim update (Interim-Update).
44	Acct-Session-ID	A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file.
45	Acct-Authentic	Indicates whether the user was authenticated locally, by the RADIUS server, or by another remote authentication protocol.
55	Event-Timestamp	Records the time an event occurred.
87	NAS-Port-ID	Text string that identifies the port that authenticates the user. Either NAS-Port or NAS-Port-ID must be present in the packet.

SEE ALSO

802.1X for Switches Overview | 370

Configuring 802.1X RADIUS Accounting (CLI Procedure)

RADIUS accounting enables statistical data about users logging in to or out of a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client is responsible for forwarding user accounting statistics to a designated RADIUS accounting server. To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, then each RADIUS server in the list is tried in the order in which the servers are configured in Junos OS.

To configure RADIUS accounting by using the CLI:

1. Configure an access profile and specify the accounting servers to which the switch forwards accounting statistics:

```
[edit access]
user@switch# set profile profile-name  radius accounting-server [server-
addresses]
```

2. Define the address of RADIUS accounting servers and configure the secret password (the secret password on the switch must match the secret password on the server):

```
[edit access]
user@switch#   set radius-server server-address secret password
```

3. Enable accounting for the access profile:

```
[edit access]
user@switch# set profile profile-name accounting
```

4. Configure the accounting order, making RADIUS the first method for sending accounting messages and updates:

```
[edit access]
user@switch# set profile profile-name accounting order radius
```

5. Configure the statistics to be collected on the switch and forwarded to the accounting server:

```
[edit access]
user@switch# set profile profile-name accounting accounting-stop-on-access-deny
user@switch# set profile profile-name accounting accounting-stop-on-
failure
```

6. (Optional) Configure the switch to send periodic updates for a user session at a specified interval to the accounting server:

```
[edit access]
user@switch# set profile profile-name accounting update-interval minutes
```

7. Display accounting statistics collected on the switch using the `show network-access aaa statistics accounting` command, for example:

```
user@switch> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```

8. Open an accounting log on the RADIUS accounting server by using the server's address, and view accounting statistics, for example:

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/192.168.0.1
[root@freeradius 192.168.0.1]# ls
```

```
detail-20071214


[root@freeradius 192.168.0.1]# vi details-20071214


        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Stop
        Acct-Session-Id = "8O2.1x811912"
        Acct-Input-Octets = 17454
        Acct-Output-Octets = 4245
        Acct-Session-Time = 1221041249
        Acct-Input-Packets = 72
        Acct-Output-Packets = 53
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual

        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Start
        Acct-Session-Id = "8O2.1x811219"
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual
```

SEE ALSO

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 389

RELATED DOCUMENTATION

RADIUS Server Configuration for Authentication | 345

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch

IN THIS SECTION

802.1x port-based network access control (PNAC) authentication on EX Series switches provides three types of authentication to meet the access needs of your enterprise LAN:

- Authenticate the first end device (supplicant) on an authenticator port, and allow all other end devices also connecting to have access to the LAN.
- Authenticate only one end device on an authenticator port at one time.
- Authenticate multiple end devices on an authenticator port. Multiple supplicant mode is used in VoIP configurations.

This example configures an EX Series switch to use IEEE 802.1X to authenticate end devices that use three different administrative modes.

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from end devices until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for end devices (supplicants) that have permission to connect to the network.

Before you configure the ports for 802.1X authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Configured users on the authentication server.

Overview and Topology

IN THIS SECTION

As shown in Figure 11 on page 454, the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.

NOTE: This figure also applies to QFX5100 switches.

Topology

Figure 11: Topology for Configuring Supplicant Modes

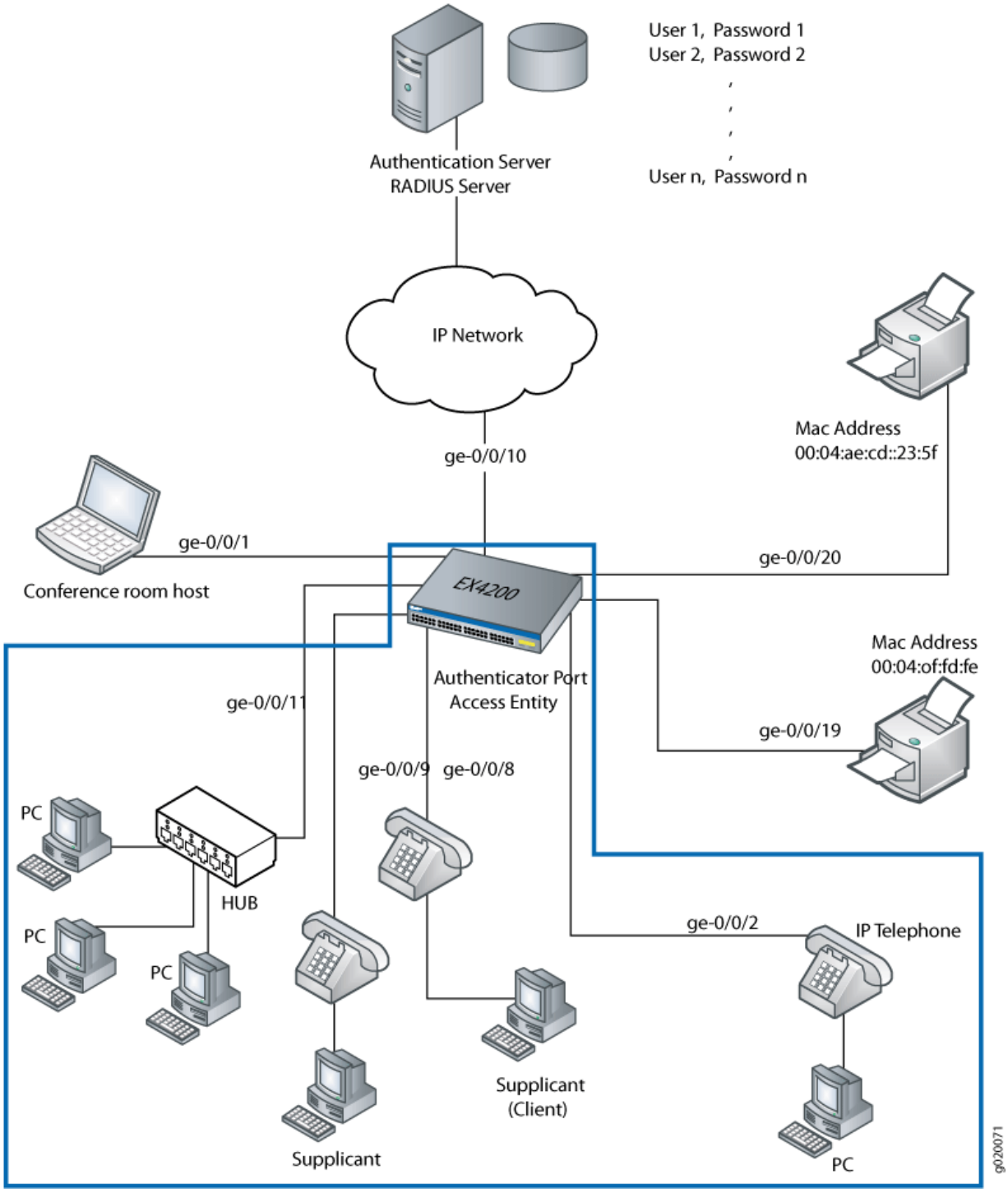


Table 31: Components of the Supplicant Mode Configuration Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)
Connections to Avaya phones—with integrated hub, to connect phone and desktop PC to a single port; (requires PoE)	ge-0/0/8, ge-0/0/9, and ge-0/0/11

To configure the administrative modes to support supplicants in different areas of the Enterprise network:

- Configure access port ge-0/0/8 for single supplicant mode authentication.
- Configure access port ge-0/0/9 for single secure supplicant mode authentication.
- Configure access port ge-0/0/11 for multiple supplicant mode authentication.

Single supplicant mode authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

Single-secure supplicant mode authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.

Multiple supplicant mode authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

Configuration of 802.1X to Support Multiple Supplicant Modes

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure the ports with different 802.1X authentication modes, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/8 supplicant single
set protocols dot1x authenticator interface ge-0/0/9 supplicant single-secure
set protocols dot1x authenticator interface ge-0/0/11 supplicant multiple
```

Step-by-Step Procedure

Configure the administrative mode on the interfaces:

1. Configure the supplicant mode as single on interface ge-0/0/8:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/8 supplicant single
```

2. Configure the supplicant mode as single secure on interface ge-0/0/9:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/9 supplicant single-secure
```

3. Configure multiple supplicant mode on interface ge-0/0/11:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/11 supplicant multiple
```

Results

Check the results of the configuration:

```
[edit]
user@access-switch> show configuration
protocols {
    dot1x {
        authenticator {
            interface {
                ge-0/0/8.0 {
                    supplicant single;
                )
                ge-0/0/9.0 {
                    supplicant single-secure;
                )
                ge-0/0/11.0 {
                    supplicant multiple;
                )
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying the 802.1X Configuration | 458

To confirm that the configuration is working properly, perform these tasks:

Verifying the 802.1X Configuration

Purpose

Verify the 802.1X configuration on interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11.

Action

Verify the 802.1X configuration by issuing the operational mode command `show dot1x interface`:

```
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
user@switch> show dot1x interface ge-0/0/9.0 detail
ge-0/0/9.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single-Secure
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
```

```
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0

user@switch> show dot1x interface ge-0/0/11.0 detail
ge-0/0/11.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```

Meaning

The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface **ge-0/0/8.0** displays **Single** supplicant mode. Interface **ge-0/0/9.0** displays **Single-Secure** supplicant mode. Interface **ge-0/0/11.0** displays **Multiple** supplicant mode.

RELATED DOCUMENTATION

- Access Control and Authentication on Switching Devices
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | **389**
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | **460**
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | **557**
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | **448**
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes | **384**
- Understanding Authentication on Switches

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch

IN THIS SECTION

802.1X on EX Series switches provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as *guests*, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as a port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure guest VLAN authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

> **NOTE**: For more about ELS, see: *Using the Enhanced Layer 2 Software CLI*

Overview and Topology

IN THIS SECTION

As part of IEEE 802.1X port-based network access control (PNAC), you can provide limited network access to supplicants who do not belong to a VLAN authentication group by configuring authentication for a guest VLAN. Typically, guest VLAN access is used to provide Internet access to visitors to a corporate site. However, you can also use the guest VLAN feature to provide access to a VLAN with limited resources to supplicants that fail 802.1X authentication on a corporate LAN.

> **NOTE**: This figure also applies to QFX5100 switches.

Topology

Figure 12 on page 462 shows the conference room connected to the switch at interface ge-0/0/1.

Figure 12: Topology for Guest VLAN Example

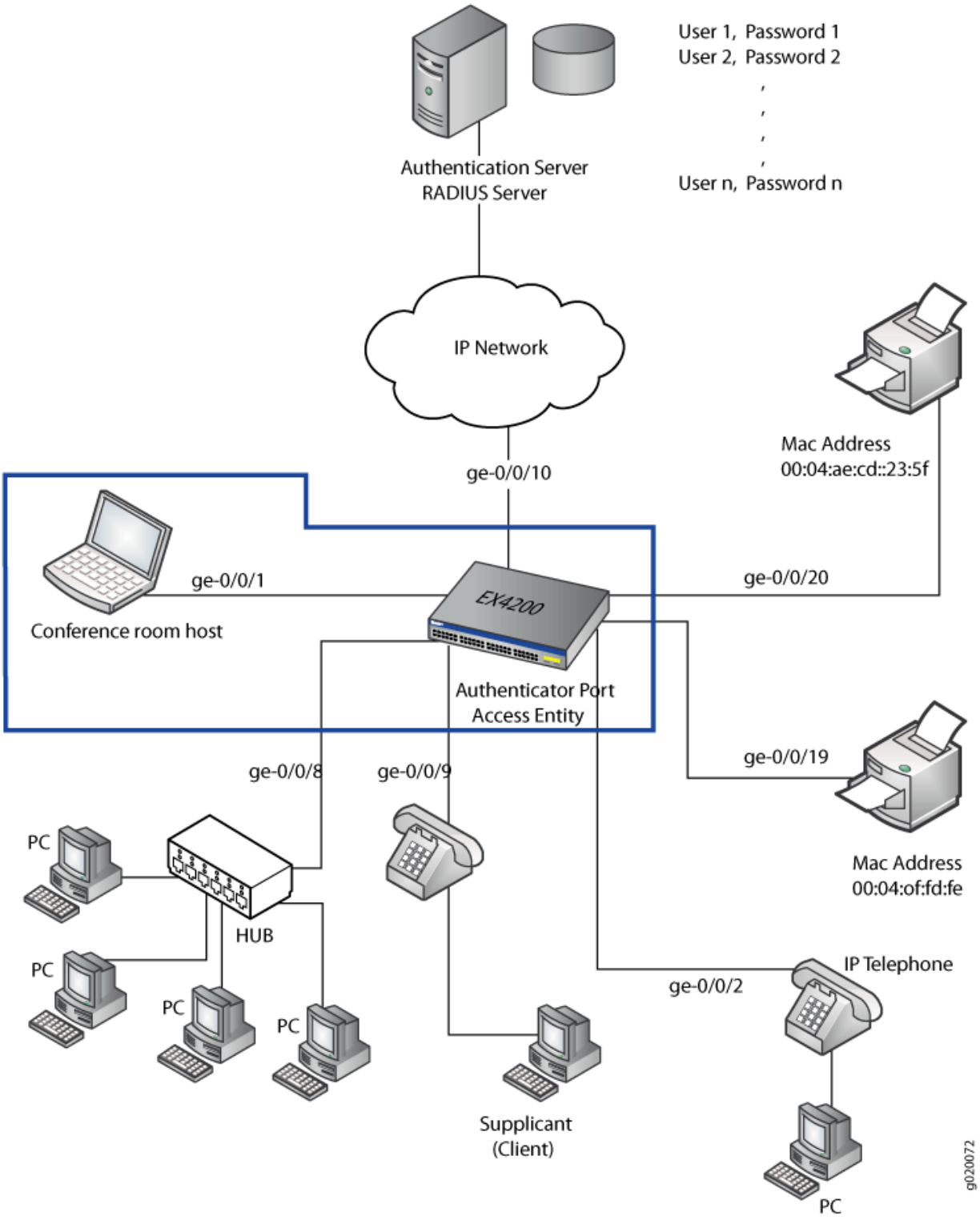


Table 32: Components of the Guest VLAN Topology

Property	Settings
Switch hardware	EX4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (**ge-0/0/0** through **ge-0/0/7**) and 16 non-PoE interfaces (**ge-0/0/8** through **ge-0/0/23**)
VLAN names and tag IDs	**sales**, tag **100** **support**, tag **200** **guest-vlan**, tag **300**
One RADIUS server	Backend database connected to the switch through interface **ge-0/0/10**

In this example, access interface **ge-0/0/1** provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans guest-vlan vlan-id 300
 set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on an EX Series switch:

1. Configure the VLAN ID for the guest VLAN:

```
[edit]
user@switch# set vlans guest-vlan vlan-id 300
```

2. Configure the guest VLAN under **dot1x** protocol:

```
[edit]
user@switch# set protocols dot1x authenticator interface all guest-vlan guest-
vlan
```

Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
    dot1x {
        authenticator {
            interface {
                all {
                    guest-vlan {
                        guest-vlan;
                    }
                }
            }
        }
    }
}
vlans {
    guest-vlan {
        vlan-id 300;
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Guest VLAN Is Configured

Purpose

Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.

NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see *show vlans*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Action

Issue the operational mode commands:

```
user@switch> show vlans

Name            Tag     Interfaces
default
                        ge-0/0/3.0*
dynamic         40
                        None
guest           30
                        None
guest-vlan      300
                        ge-0/0/1.0*
vlan_dyn
```

```
                        None


user@switch> show dot1x interface ge-0/0/1.0 detail
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Guest VLAN
      Authenticated VLAN: guest-vlan
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The output of the `show vlans` command shows **guest-vlan** as the name of the VLAN and the VLAN ID as **300**.

The output of the `show dot1x interface ge-0/0/1.0 detail` command displays the **Guest VLAN membership** field, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the **guest-vlan**.

RELATED DOCUMENTATION

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 389

Interfaces Enabled for 802.1X or MAC RADIUS Authentication

IN THIS SECTION

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes. Terms are applied after a device is successfully authenticated through 802.1X. For more information, read this topic.

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch

IN THIS SECTION

You can use RADIUS server attributes and a port firewall filter to centrally apply terms to multiple supplicants (end devices) connected to an EX Series switch in your enterprise. Terms are applied after a device is successfully authenticated through 802.1X. If the firewall filter configuration is modified after end devices are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter changes to take effect.

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For information about configuring your server, consult the documentation that was included with your RADIUS server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Configured 802.1X authentication on the switch, with the supplicant mode for interface ge-0/0/2 set to **multiple**. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 451.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

Overview and Topology

IN THIS SECTION

When the 802.1X configuration on an interface is set to **multiple** supplicant mode, you can apply a single port firewall filter configured through the Junos OS CLI on the EX Series switch to any number of end devices (supplicants) by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate end devices.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview* or *Overview of Firewall Filters (QFX Series)*.

RADIUS server attributes are applied to the port where the end device is connected after the device is successfully authenticated using 802.1X. To authenticate an end device, the switch forwards the end device's credentials to the RADIUS server. The RADIUS server matches the credentials against preconfigured information about the supplicant located in the supplicant's user profile on the RADIUS server. If a match is found, the RADIUS server instructs the switch to open an interface to the end device. Traffic then flows from and to the end device on the LAN. Further instructions configured in the port firewall filter and added to the end device's user profile using a RADIUS server attribute further define the access that the end device is granted. Filtering terms configured in the port firewall filter are applied to the port where the end device is connected after 802.1X authentication is complete.

NOTE: If you modify the port firewall filter after an end device is successfully authenticated using 802.1X, you must terminate and re-establish the 802.1X authentication session for the firewall filter configuration changes to be effective.

Topology

Figure 13 on page 471 shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port ge-0/0/10. Two end devices (supplicants) are accessing the LAN on interface ge-0/0/2. Supplicant 1 has the MAC address 00:50:8b:6f:60:3a. Supplicant 2 has the MAC address 00:50:8b:6f:60:3b.

NOTE: This figure also applies to QFX5100 switches.

Figure 13: Topology for Firewall Filter and RADIUS Server Attributes Configuration

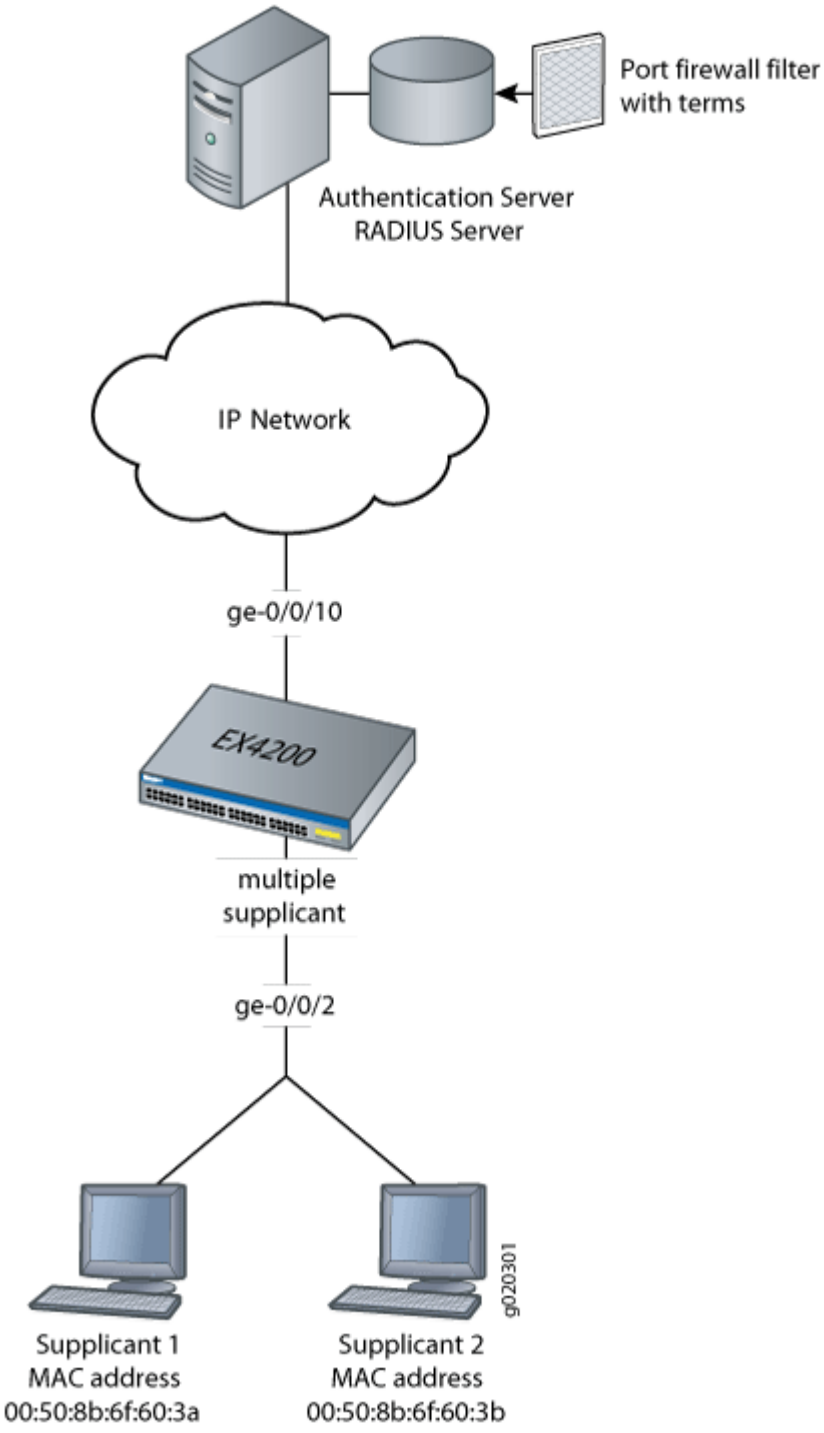


Table 33 on page 472 describes the components in this topology.

Table 33: Components of the Firewall Filter and RADIUS Server Attributes Topology

Property	Settings
Switch hardware	EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.
One RADIUS server	Backend database with the address **10.0.0.100** connected to the switch at port **ge-0/0/10**.
802.1X supplicants connected to the switch on interface **ge-0/0/2**	• **Supplicant 1** has MAC address **00:50:8b:6f:60:3a**. • **Supplicant 2** has MAC address **00:50:8b:6f:60:3b**.
Port firewall filter to be applied on the RADIUS server	**filter1**
Counters	**counter1** counts packets from Supplicant 1, and **counter2** counts packets from Supplicant 2.
Policer	**policer p1**
User profiles on the RADIUS server	• Supplicant 1 has the user profile **supplicant1**. • Supplicant 2 has the user profile **supplicant2**.

In this example, you configure a port firewall filter named **filter1**. The filter contains terms that will be applied to the end devices based on the MAC addresses of the end devices. When you configure the filter, you also configure the counters **counter1** and **counter2**. Packets from each end device are counted, which helps you verify that the configuration is working. Policer **p1** limits the traffic rate based on the values for **exceeding** and **discard** parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

Configuring the Port Firewall Filter and Counters

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-address
00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-address
00:50:8b:6f:60:3b
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term supplicant1 then count counter1
set firewall family ethernet-switching filter filter1 term supplicant1 then policer p1
set firewall family ethernet-switching filter filter1 term supplicant2 then count counter2
```

Step-by-Step Procedure

To configure a port firewall filter and counters on the switch:

1. Configure a port firewall filter (here, **filter1**) with terms for each end device based on the MAC address of each end device:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
user@switch# set filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
```

2. Set policer definition:

```
[edit]
user@switch# set firewall policer p1 if-exceeding bandwidth-limit 1m
user@switch# set firewall policer p1 if-exceeding burst-size-limit 1k
user@switch# set firewall policer p1 then discard
```

3. Create two counters that will count packets for each end device and a policer that limits the traffic rate:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 then count counter1
user@switch# set filter filter1 term supplicant1 then policer p1
user@switch# set filter filter1 term supplicant2 then count counter2
```

Results

Display the results of the configuration:

```
user@switch> show configuration
    firewall {
        family ethernet-switching {
            filter filter1 {
                term supplicant1 {
                    from {
                        source-mac-address {
                            00:50:8b:6f:60:3a;
                        }
                    }
                    then count counter1;
                    then policer p1;
                }
                term supplicant2 {
                    from {
                        source-mac-address {
                            00:50:8b:6f:60:3b;
                        }
                    }
                    then count counter2;
                }
```

```
        }
    }
}
policer p1 {
    if-exceeding {
        bandwidth-limit 1m;
            burst-size-limit 1k;
        }
        then discard;
    }
```

Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

IN THIS SECTION

- Procedure | 475

Procedure

Step-by-Step Procedure

To verify that the RADIUS server attribute **Filter-ID** is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary **dictionary.rfc2865** on the RADIUS server, and verify that the attribute **Filter-ID** is in the dictionary:

```
[root@freeradius]# cd usr/share/freeradius/dictionary.rfc2865
```

2. Close the dictionary file.

3. Display the local user profiles of the end devices to which you want to apply the filter (here, the user profiles are called **supplicant1** and **supplicant2**):

```
[root@freeradius]# cat /usr/local/etc/raddb/users
```

The output shows:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005"
```

4. Apply the filter to both user profiles by adding the line **Filter-Id = “filter1”** to each profile, and then close the file:

```
[root@freeradius]# cat /usr/local/etc/raddb/users
```

After you paste the line into the files, the files look like this:

```
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005",
        Filter-Id = "filter1"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
        Tunnel-Type = VLAN,
        Tunnel-Medium-Type = IEEE-802,
        Tunnel-Private-Group-Id = "1005",
        Filter-Id = "filter1"
```

Verification

IN THIS SECTION

Verifying That the Filter Has Been Applied to the Supplicants

Purpose

After the end devices are authenticated on interface ge-0/0/2, verify that the filter has been configured on the switch and includes the results for both supplicants:

Action

```
user@switch> show dot1x firewall

Filter: dot1x-filter-ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter2_dot1x_ge-0/0/2_user2 400
```

Meaning

The output of the `show dot1x firewall` command displays **counter1** and **counter2**. Packets from User_1 are counted using **counter1**, and packets from User 2 are counted using **counter2**. The output displays packets incrementing for both counters. The filter has been applied to both end devices.

SEE ALSO

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

Configuring 802.1X RADIUS Accounting (CLI Procedure) | **448**

Understanding Authentication on Switches

Understanding Dynamic Filters Based on RADIUS Attributes | **395**

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication

IN THIS SECTION

On supported switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following hardware and software components:

- Supported Junos OS Release for the switches
- A supported switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.
- Configured 802.1X authentication on the switch, with the authentication mode for interface **ge-0/0/2** set to **multiple**. See Configuring 802.1X Interface Settings (CLI Procedure) and Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch.

- Configured users on the RADIUS authentication server.

Overview and Topology

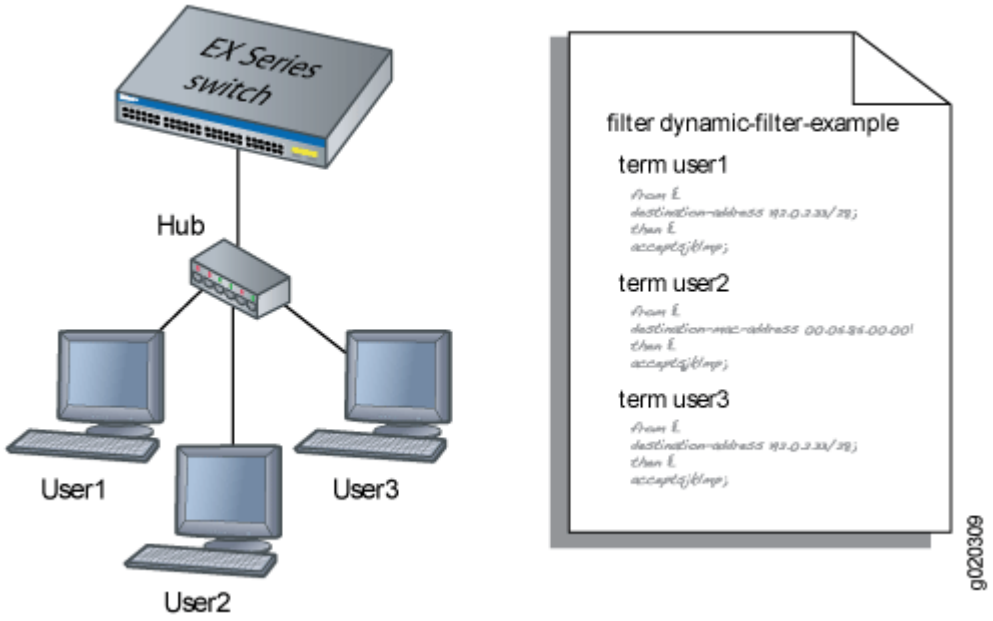
IN THIS SECTION

Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 14 on page 480, when User1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 14: Conceptual Model: Dynamic Filter Updated for Each New User

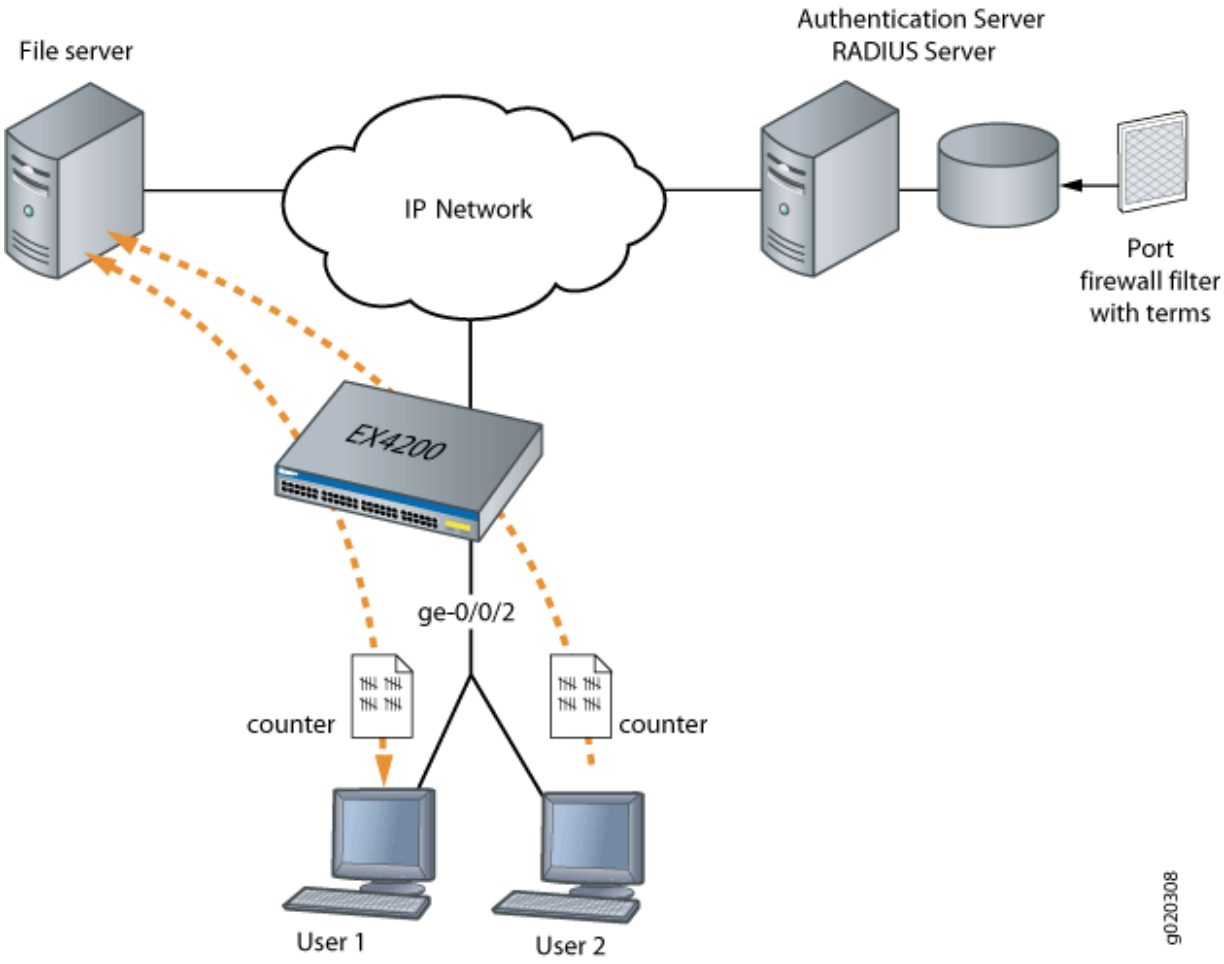


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. Figure 15 on page 481 shows the network topology for this example.

Figure 15: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

IN THIS SECTION

- Configuring Firewall Filters on Interfaces with Multiple Supplicants | **482**

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
                        set protocols dot1x authenticator interface ge-0/0/2 supplicant
multiple
                        set firewall family ethernet-switching filter filter1 term term1 from
destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
                        set firewall family ethernet-switching filter filter1 term term1 then
count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/2 supplicant multiple
```

2. Set policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results

Check the results of the configuration:

```
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
                term term2 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
                burst-size-limit 1k;
            }
            then discard;
```

```
        }
}
protocols {
    dot1x {
        authenticator
            interface ge-0/0/2 {
                supplicant multiple;
            }
        }
    }
```

Verification

IN THIS SECTION

- Verifying Firewall Filters on Interfaces with Multiple Supplicants | 484

To confirm that the configuration is working properly, perform these tasks:

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose

Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on **ge-0/0/2**:

```
user@switch> show dot1x firewall

Filter: dot1x_ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
```

2. When a second user, User2, is authenticated on the same interface, **ge-0/0/2**, you can verify that the filter includes the results for both of the users authenticated on the interface:

```
user@switch>  show dot1x firewall

Filter: dot1x-filter-ge-0/0/0
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter1_dot1x_ge-0/0/2_user2 400
```

Meaning

The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

SEE ALSO

> *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
>
> Filtering 802.1X Supplicants by Using RADIUS Server Attributes

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on EX Series Switches with ELS Support

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication*. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2 or later for EX Series switches
- One EX Series switch with support for ELS
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to `multiple`. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 451.
- Configured users on the RADIUS authentication server.

Overview and Topology

IN THIS SECTION

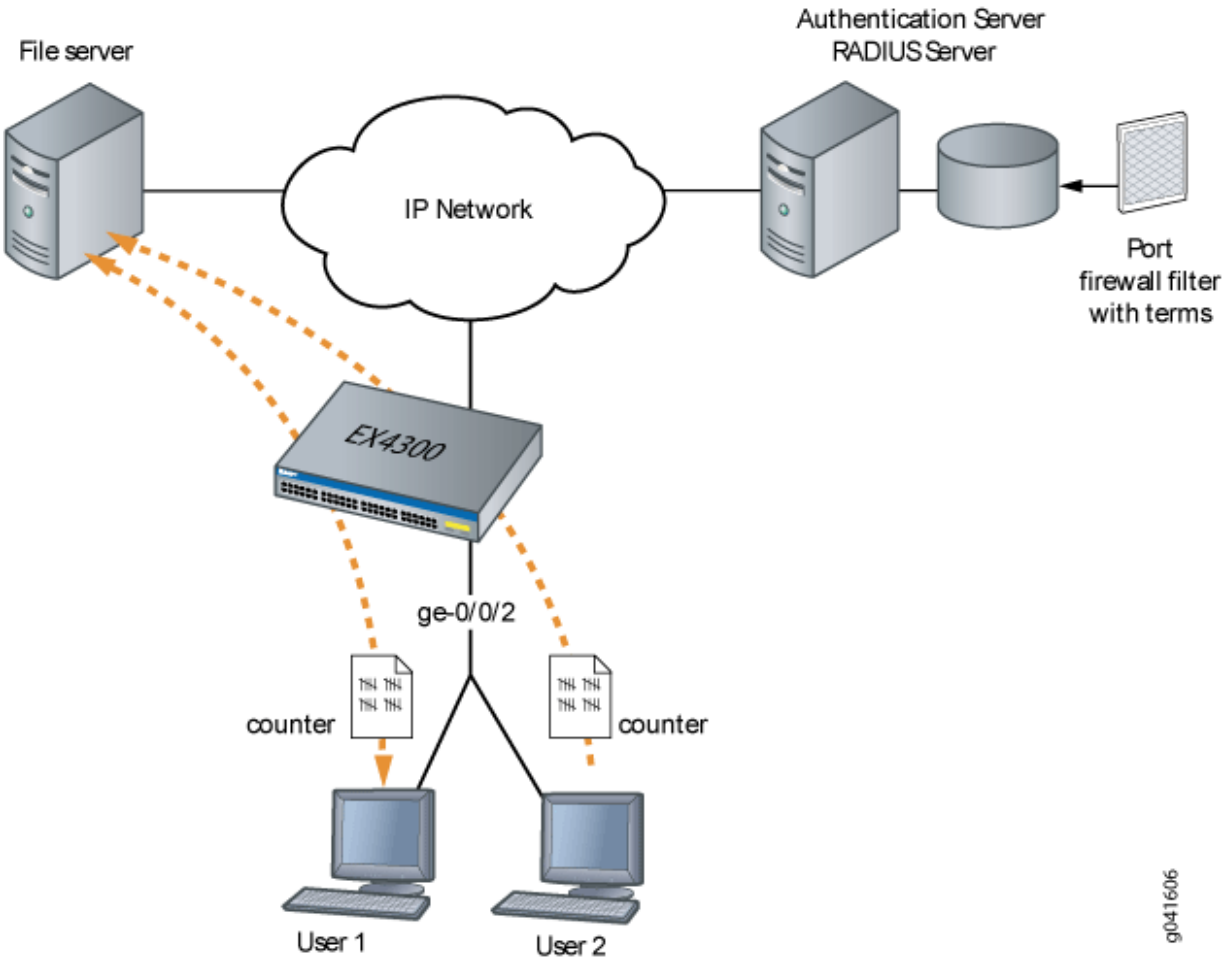
Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 16 on page 488, when User 1 is authenticated by the EX Series switch, the system adds a term to the firewall filter **dynamic-filter-example**. When User 2 is authenticated, another term is added to the firewall filter, and so on.

NOTE: This figure also applies to QFX5100 switches.

Figure 16: Conceptual Model: Dynamic Filter Updated for Each New User

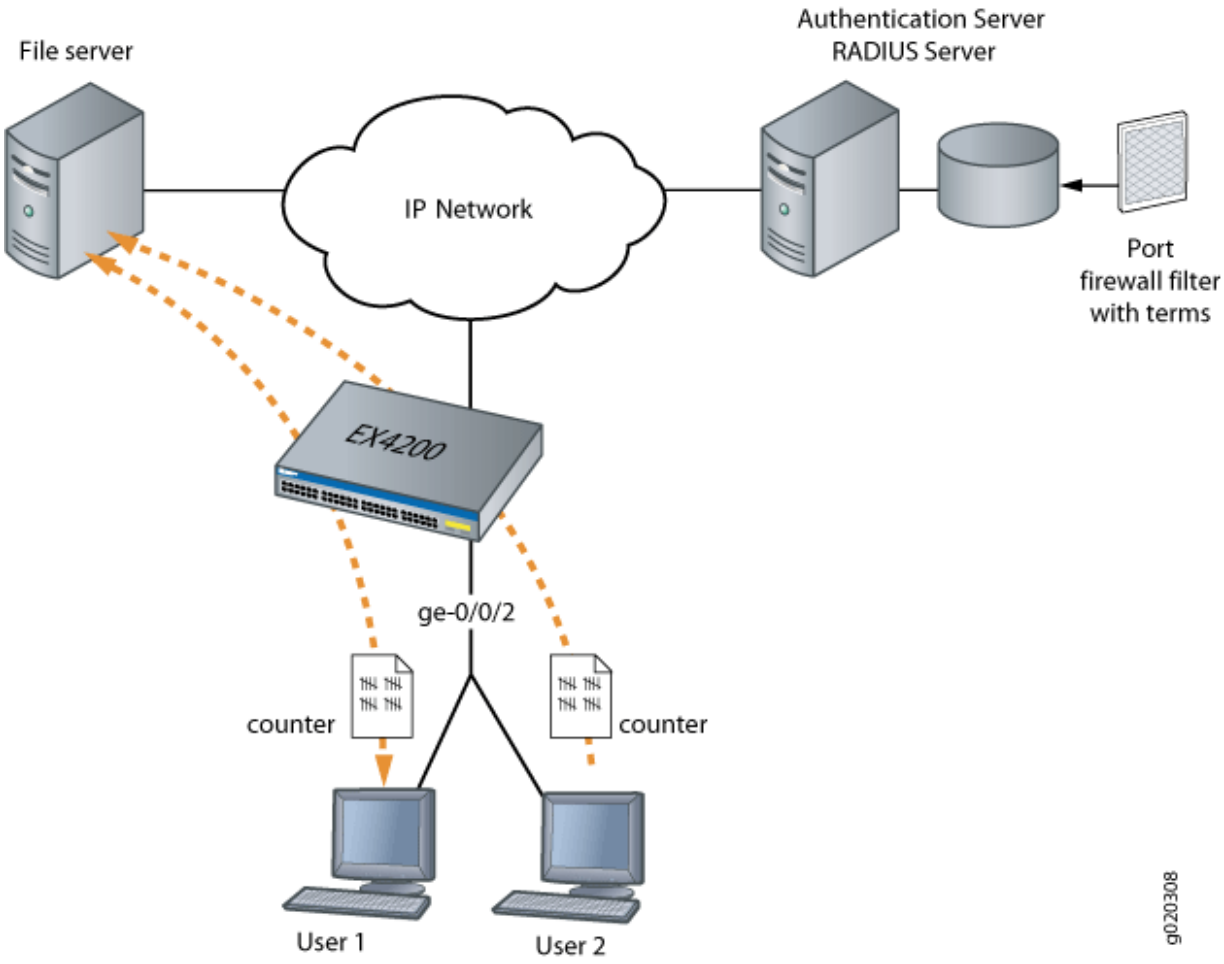


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. Figure 17 on page 489 shows the network topology for this example.

Figure 17: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

IN THIS SECTION

- Configuring Firewall Filters on Interfaces with Multiple Supplicants | **490**

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
                        set firewall family ethernet-switching filter filter1 term term1 from
ip-destination-address 192.0.2.16/28
                        set firewall family ethernet-switching filter filter1 term term2 from
ip-destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
                        set firewall family ethernet-switching filter filter1 term term1 then
count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Set the policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```

2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results

Check the results of the configuration:

```
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
                term term2 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
                burst-size-limit 1500;
            }
            then discard;
        }
}
protocols {
    dot1x {
        authenticator
            interface ge-0/0/2 {
                supplicant multiple;
            }
```

```
        }
    }
```

Verification

IN THIS SECTION

- Verifying Firewall Filters on Interfaces with Multiple Supplicants | 492

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose

Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2:

```
user@switch> show dot1x firewall

Filter: dot1x_ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
```

2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

```
user@switch>  show dot1x firewall

Filter: dot1x-filter-ge-0/0/0
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter1_dot1x_ge-0/0/2_user2 400
```

Meaning

The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address `100` times, while User 2 accessed the same file server `400` times.

SEE ALSO

> *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
>
> Filtering 802.1X Supplicants by Using RADIUS Server Attributes | **384**

RELATED DOCUMENTATION

> Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Static MAC Bypass of 802.1X and MAC RADIUS Authentication

IN THIS SECTION

Junos OS allows you to configure access to your LAN through 802.1X-configured interfaces without authentication, by configuring a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server. For more information, read this topic.

NOTE: If you add a static MAC address entry to the Ethernet switching table, this has the same effect as adding a MAC address to the static MAC bypass list. For information on configuring static MAC address entries see *MAC Addresses*.

Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe
```

- Configure a supplicant to bypass authentication if it is connected through a particular interface:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
```

- Configure a supplicant to be moved to a specific VLAN after it is authenticated:

```
[edit protocols dot1x]
user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment
default-vlan
```

SEE ALSO

Configuring 802.1X Interface Settings (CLI Procedure) | 378

Configuring 802.1X Authentication (J-Web Procedure)

Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch

IN THIS SECTION

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you configure static MAC bypass of authentication, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging*

and a VLAN on Switches. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

For more about ELS, see: *Using the Enhanced Layer 2 Software CLI*.

- Specified the RADIUS server connections and configured an access profile on the switch. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.

Overview and Topology

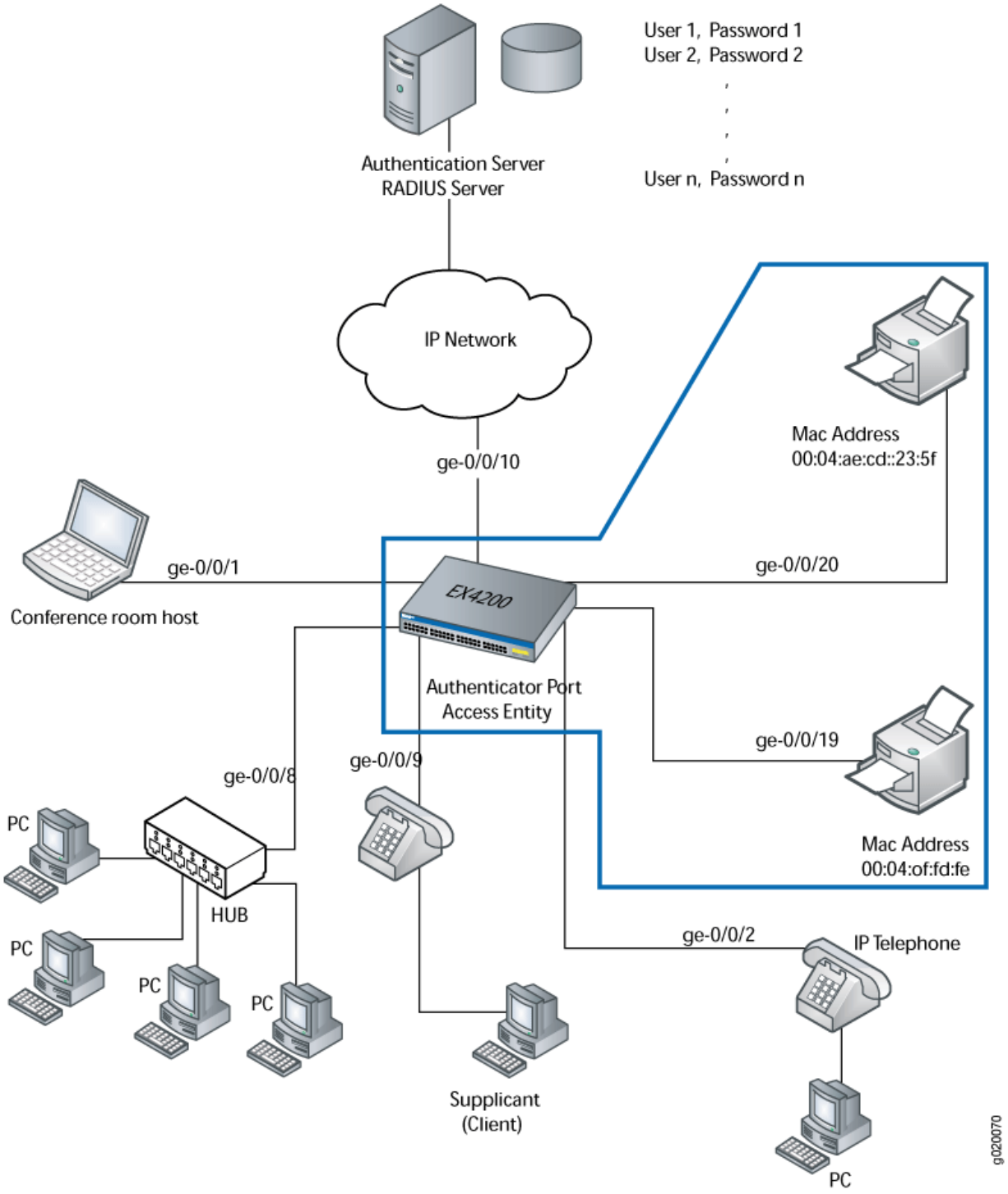
IN THIS SECTION

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Figure 18 on page 497 shows the two printers connected to the EX4200.

NOTE: This figure also applies to QFX5100 switches.

Figure 18: Topology for Static MAC Bypass of Authentication Configuration



The interfaces shown in Table 34 on page 498 will be configured for static MAC bypass of authentication.

Table 34: Components of the Static MAC Bypass of Authentication Configuration Topology

Property	Settings
Switch hardware	EX4200, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports (`ge-0/0/0` through `ge-0/0/23`)
VLAN name	`default`
Connections to integrated printer/fax/ copier machines (no PoE required)	`ge-0/0/19`, MAC address 00:04:0f:fd:ac:fe `ge-0/0/20`, MAC address 00:04:ae:cd:23:5f

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface `ge-0/0/19`. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface `ge-0/0/20`. Both printers will be added to the static list and bypass 802.1X authentication.

Topology

Configuration

IN THIS SECTION

- Procedure | 498

Procedure

CLI Quick Configuration

To quickly configure the static MAC bypass list, copy the following commands and paste them into the switch terminal window:

```
[edit]

set protocols dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
```

```
set protocols dot1x authenticator interface all supplicant multiple
set protocols dot1x authenticator authenticaton-profile-name profile1
```

Step-by-Step Procedure

Configure the static MAC bypass list:

1. Configure MAC addresses `00:04:0f:fd:ac:fe` and `00:04:ae:cd:23:5f` as static MAC addresses:

```
[edit protocols]
user@switch# set dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
```

2. Configure the 802.1X authentication method:

```
[edit protocols]
user@switch# set dot1x authenticator interface all supplicant multiple
```

3. Configure the authentication profile name (access profile name) to use for authentication:

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name profile1
```

NOTE: Access profile configuration is required only for 802.1X clients, not for static MAC clients.

Results

Display the results of the configuration:

```
user@switch> show
interfaces {
    ge-0/0/19 {
        unit 0 {
            family ethernet-switching {
                vlan members default;
            }
        }
```

```
    }
    ge-0/0/20 {
        unit 0 {
            family ethernet-switching {
                vlan members default;
            }
        }
    }
}
protocols {
    dot1x {
        authenticator {
            authentication-profile-name profile1
            static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
            interface {
                all {
                    supplicant multiple;
                }
            }
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying Static MAC Bypass of Authentication

Purpose

Verify that the MAC addresses of both printers are configured and associated with the correct interfaces.

Action

Issue the operational mode command:

```
user@switch> show dot1x static-mac-address

MAC address           VLAN-Assignment          Interface
00:04:0f:fd:ac:fe     default                  ge-0/0/19.0
00:04:ae:cd:23:5f     default                  ge-0/0/20.0
```

Meaning

The output field `MAC address` shows the MAC addresses of the two printers.

The output field `Interface` shows that the MAC address `00:04:0f:fd:ac:fe` can connect to the LAN through interface `ge-0/0/19.0` and that the MAC address `00:04:ae:cd:23:5f` can connect to the LAN through interface `ge-0/0/20.0`.

SEE ALSO

- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring 802.1X Interface Settings (CLI Procedure) | **378**
- Understanding Authentication on Switches

RELATED DOCUMENTATION

- Interfaces Enabled for 802.1X or MAC RADIUS Authentication | **467**
- 802.1X Authentication | **369**
- MAC RADIUS Authentication | **432**

Configuring PEAP for MAC RADIUS Authentication

Extensible Authentication Protocol (EAP) is an extensible protocol that provides support for multiple authentication methods, including password-based authentication methods and more secure certificate-

based authentication methods. EAP facilitates the negotiation between the authenticator, or switching device, and the authentication server, to determine which authentication method to use for a supplicant. The default authentication method used for MAC RADIUS authentication is EAP-MD5, in which the server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with MD5. Because EAP-MD5 only provides for client authentication and not for server authentication, it can be vulnerable to spoofing attacks.

You can configure the Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, to address the security vulnerabilities of EAP-MD5. PEAP is a protocol that encapsulates EAP packets within an encrypted and authenticated Transport Layer Security (TLS) tunnel. PEAP is referred to as the outer authentication protocol because it sets up the tunnel and is not directly involved with authenticating the endpoints. The inner authentication protocol, used to authenticate the client’s MAC address inside the tunnel, is Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). The encrypted exchange of information inside the tunnel ensures that user credentials are safe from eavesdropping.

One of the advantages of PEAP, when used with MS-CHAPv2, is that it requires only a server-side certificate to establish the secure tunnel, and uses server-side public key certificates to authenticate the server. This eliminates the overhead involved in deploying digital certificates for every client that requires authentication.

Once a client has been authenticated on the switch using MAC RADIUS authentication, subsequent clients can use the same outer tunnel that was established by the first client to communicate with the server. This is achieved using the session resumption functionality provided by SSL. Session resumption reduces latency that can occur as subsequent clients wait for a new TLS tunnel to be established.

Before you configure the PEAP authentication protocol for MAC RADIUS authentication, make sure that the authentication server is also configured to use PEAP with MS-CHAPv2 as the inner authentication protocol. For information about configuring the authentication server, consult the documentation for your server.

NOTE: The authentication protocol can be configured globally using the `interface all` option as well as locally using the individual interface name. If the authentication protocol is configured both for an individual interface and for all interfaces, the local configuration for that interface overrides the global configuration.

To configure the PEAP authentication protocol for MAC RADIUS authentication:

1. Configure the `eap-peap` option for the `authentication-protocol` statement:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name mac-radius
authentication-protocol eap-peap
```

2. (Optional) Enable session resumption to allow for faster authentication of subsequent clients:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name mac-radius
authentication-protocol eap-peap resume
```

3. Load the server-side SSL certificate using either the filename or path.

   a. To load the certificate using the file name:

```
[edit]
user@root# run load ssl-certificate file certificate-name
```

   b. To load the certificate using the file path:

```
[edit]
user@root# run load ssl-certificate path certificate-path
```

NOTE: If you are using an SSL certificate with a path other than the default path of `/var/tmp/`, you must first configure the SSL certificate path using the following command:

```
[edit]
set protocols dot1x ssl-certificate-path certificate-path
```

   c. To verify the certificates:

```
[edit]
user@root# run show ssl-certificates
```

Captive Portal Authentication

IN THIS SECTION

You can control access to your network through a switch by using several different authentication methods. Junos OS switches support 802.1X, MAC RADIUS, and captive portal authentication. You can set up captive portal authentication on a switch to redirect web browser requests to a login page that requires the user to input a username and password.

Example: Setting Up Captive Portal Authentication on an EX Series Switch

IN THIS SECTION

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

Requirements

This example uses the following hardware and software components:

- An EX Series switch that supports captive portal
- Junos OS Release 10.1 or later for EX Series switches

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 302.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 514.

Overview and Topology

IN THIS SECTION

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication allowlist. The MAC addresses in this list are permitted access on the interface without captive portal.

Topology

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

IN THIS SECTION

To configure captive portal on your switch:

CLI Quick Configuration

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.204.96.165 port 1812
set access radius-server 10.204.96.165 secret "ABC123"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.204.96.165
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set services captive-portal authentication-profile-name profile1
set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
set services captive-portal custom-options post-authentication-url http://www.my-home-page.com
```

Procedure

Step-by-Step Procedure

To configure captive portal on the switch:

1. Define the server IP address, the server authentication port number, and configure the secret password. The secret password on the switch must match the secret password on the server:

```
[edit]
user@switch# set access radius-server 10.204.96.165 port 1812
[edit]
user@switch# set access radius-server 10.204.96.165 secret "ABC123"
```

2. Configure the authentication order, making `radius` the first method of authentication:

```
[edit]
user@switch# set access profile profile1 authentication-order radius
```

3. Configure the server IP address to be tried in order to authenticate the supplicant:

```
[edit]
user@switch# set access profile profile1 radius authentication-server 10.204.96.165
```

4. Enable HTTP access on the switch:

```
[edit]
user@switch# set system services web-management http
```

5. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:

NOTE: You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

Step-by-Step Procedure

a. Associate the security certificate with the Web server and enable HTTPS access on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate my-signed-cert
```

b. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

6. Enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
```

7. Specify the name of the access profile to be used for captive portal authentication:

```
[edit]
user@switch# set services captive-portal authentication-profile-name profile1
```

8. (Optional) Allow specific clients to bypass captive portal:

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address` *`mac-address`* command after adding its MAC address to the allowlist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

9. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit]
user@switch# set services captive-portal custom-options post-authentication-url http://www.my-home-page.com
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show
system {
    services {
        web-management {
            http;
            https {
                local-certificate my-signed-cert;
            }
        }
    }
}
security {
    certificates {
        local {
            my-signed-cert {
                "-----BEGIN RSA PRIVATE KEY-----ABC123
 ...
ABC123-----END CERTIFICATE-----\n"; ## SECRET-DATA
            }
        }
    }
}
services {
    captive-portal {
        interface {
            ge-0/0/10.0 {
                supplicant multiple;
            }
        }
        secure-authentication https;
    }
}
ethernet-switching-options {
    authentication-whitelist {
        00:10:12:e0:28:22/48;
```

```
    }
}
```

Verification

IN THIS SECTION

To confirm that captive portal is configured and working properly, perform these tasks:

Verifying That Captive Portal Is Enabled on the Interface

Purpose

Verify that captive portal is configured on interface ge-0/0/10.

Action

Use the operational mode command `show captive-portal interface` *`interface-name`* `detail`:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning

The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose

Verify that captive portal is working on the switch.

Action

Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

IN THIS SECTION

To troubleshoot captive portal, perform these tasks:

Troubleshooting Captive Portal

Problem

The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a Web page.

Solution

You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
```

```
Counters:
Name                          Bytes              Packets
dot1x_ge-0/0/10_CP_arp         7616                  119
dot1x_ge-0/0/10_CP_dhcp           0                    0
dot1x_ge-0/0/10_CP_http           0                    0
dot1x_ge-0/0/10_CP_https          0                    0
dot1x_ge-0/0/10_CP_t_dns          0                    0
dot1x_ge-0/0/10_CP_u_dns          0                    0
```

Configuring Captive Portal Authentication (CLI Procedure)

IN THIS SECTION

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a web page, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 302.
- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 514.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Enable HTTP access on the switch:

```
[edit]
user@switch# set system services web-management http
```

2. Associate the security certificate with the Web server and enable HTTPS access on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate my-signed-cert
```

NOTE: You can enable HTTP without HTTPS, but we recommend HTTPS for security purposes.

3. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface interface-name
```

For example, to enable captive portal on the interface ge-0/0/10:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

To allow specific clients to bypass captive portal:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist mac-address
```

For example, to allow specific clients to bypass captive portal:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the allowlist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.

Designing a Captive Portal Authentication Login Page on Switches

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires users to input a username and password before they are allowed access. Upon successful authentication, users are allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the terms and conditions of use. By clicking the Agree button, the user can access the captive portal login page.

Figure 19 on page 515 shows an example of a captive portal login page:

Figure 19: Example of a Captive Portal Login Page

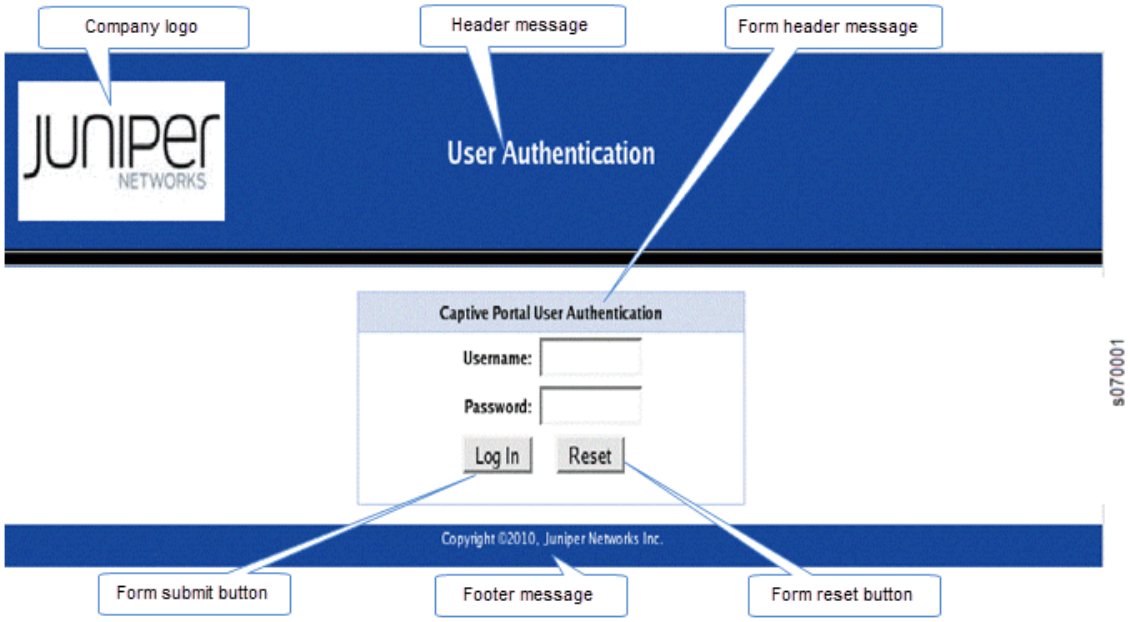


Table 35 on page 515 summarizes the configurable elements of a captive portal login page.

Table 35: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	**footer-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the captive portal login page footer.
Footer message	**footer-message** *text-string*	Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy The default text shown in the footer is **Copyright @2010, Juniper Networks Inc.**
Footer text color	**footer- text-color** *color*	Color of the text in the footer. The default color is white.
Form header background color	**form-header-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.

Table 35: Configurable Elements of a Captive Portal Login Page *(Continued)*

Element	CLI Statement	Description
Form header message	**form-header-message** *text-string*	Text displayed in the header of the captive portal login page. The default text is **Captive Portal User Authentication** .
Form header text color	**form-header- text-color** *color*	Color of the text in the form header. The default color is black.
Form reset button label	**form-reset-label** *label-name*	Using the **Reset** button, the user can clear the username and password fields on the form.
Form submit button label	**form-submit-label** *label-name*	Using the **Login** button, the user can submit the login information.
Header background color	**header-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the captive portal login page header.
Header logo	**header-logo** *filename*	Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format. You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.
Header message	**header-message** *text-string*	Text displayed in the page header. The default text is **User Authentication**.
Header text color	**header-text-color***color*	Color of the text in the header. The default color is white.
Post-authentication URL	**post-authentication-url** *url*	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

```
user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

```
[edit system services captive-portal]
user@switch# set custom-options header-bgcolor #006600
set custom-options header-message “Welcome to Our Network”
set custom-options banner-message “Please enter your username and password”.The banner
displays the message ”XXXXXXX” by default. The user can modify this message.
set custom-options footer-message “Copyright ©2010, Our Network”
```

Now you can commit the configuration.

NOTE: For the custom options that you do not specify, the default value is used.

SEE ALSO

Understanding Authentication on Switches

captive-portal

Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switche with ELS Support

IN THIS SECTION

NOTE: This task uses Junos OS for switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring Captive Portal Authentication (CLI Procedure)" on page 512. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Configure captive portal authentication (hereafter referred to as captive portal) on a switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 302.
- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 514.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate certificate-name
```

NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface interface-name
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@switch# set switch-options authentication-whitelist mac-address
```

NOTE: Optionally, you can use `set switch-options authentication-whitelist` *mac-address* `interface` *interface-name* to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address` *session-mac-addr* command after adding its MAC address to the allowlist. Otherwise, the new entry for the MAC address is not added to the Ethernet switching table and the authentication bypass is not allowed.

Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Setting Up Captive Portal Authentication on an EX Series Switch" on page 504. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50 or later for EX Series switches
- An EX Series switch with support for ELS

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 302.

- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 514.

Overview and Topology

IN THIS SECTION

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN, add its MAC address to the authentication allowlist and assign it to a VLAN, vlan1. The MAC addresses on this list are permitted access on the interface without captive portal authentication.

Topology

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

IN THIS SECTION

To configure captive portal on your switch:

CLI Quick Configuration

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
set custom-options post-authentication-url http://www.my-home-page.com
```

Procedure

Step-by-Step Procedure

1. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:

   #### Step-by-Step Procedure

   a. Associate the security certificate with the Web server and enable HTTPS on the switch:

   ```
   [edit]
   user@switch# set system services web-management https local-certificate my-signed-cert
   ```

   NOTE: You can enable HTTP instead of HTTPS, but we recommend that you enable HTTPS for security purposes.

   b. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@switch# set services captive-portal secure-authentication https
   ```

2. Enable an interface for captive portal:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
```

3. (Optional) Allow specific clients to bypass captive portal authentication:

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address` *mac-address* command after adding its MAC address to the allowlist. Otherwise, the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

```
[edit]
user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment
vlan1
```

NOTE: Optionally, you can use **set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1 interface ge-0/0/10.0** to limit the scope to the interface.

4. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@switch# set custom-options post-authentication-url http://www.my-home-page.com
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show
system {
    services {
        web-management {
```

```
            https {
                local-certificate my-signed-cert;
            }
        }
    }
}
security {
    certificates {
        local {
            my-signed-cert {
                "-----BEGIN RSA PRIVATE KEY-----\ABC123
ABC123ABC123ABC123 ... ABC123
----END CERTIFICATE-----\n"; ## SECRET-DATA
            }
        }
    }
}
services {
    captive-portal {
        interface {
            ge-0/0/10.0 {
                supplicant multiple;
            }
        }
        secure-authentication https;
        custom-options {
            post-authentication-url http://www.my-home-page.com;
        }
    }
}
switch-options {
    authentication-whitelist {
        00:10:12:e0:28:22/48 {
            vlan-assignment vlan1;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that captive portal authentication is configured and working properly, perform these tasks:

Verifying That Captive Portal Is Enabled on the Interface

Purpose

Verify that captive portal is configured on the interface ge-0/0/10.

Action

Use the operational mode command `show captive-portal interface` *`interface-name`* `detail`:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning

The output confirms that captive portal is configured on the interface `ge-0/0/10`, with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose

Verify that captive portal is working on the switch.

Action

Connect a client to the interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

IN THIS SECTION

To troubleshoot captive portal, perform this task:

Troubleshooting Captive Portal

Problem

The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.

Solution

You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                          Bytes              Packets
dot1x_ge-0/0/10_CP_arp         7616                  119
dot1x_ge-0/0/10_CP_dhcp           0                    0
dot1x_ge-0/0/10_CP_http           0                    0
dot1x_ge-0/0/10_CP_https          0                    0
```

```
dot1x_ge-0/0/10_CP_t_dns          0                    0
dot1x_ge-0/0/10_CP_u_dns          0                    0
```

RELATED DOCUMENTATION

Flexible Authentication Order on EX Series Switches | 527

Central Web Authentication | 544

Centralized Access Control to Network Resources on EX Series Switches

Flexible Authentication Order on EX Series Switches

IN THIS SECTION

Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. For more information, read this topic.

Configuring Flexible Authentication Order

You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch will attempt authentication using MAC RADIUS. If MAC RADIUS

fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

With a flexible authentication order, the sequence of authentication method used can be changed based on the type of clients connected to the interface. You can configure the `authentication-order` statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried. Captive portal is always the last authentication method tried.

If MAC RADIUS authentication is configured as the first authentication method in the order, then on receiving data from any client, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch uses 802.1X authentication to authenticate the client. If 802.1X authentication fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

NOTE: If 802.1X authentication and MAC RADIUS authentication fail, and captive portal is not configured on the interface, the client is denied access to the LAN unless a server fail fallback method is configured. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 354 for more information.

Different authentication methods can be used in parallel on an interface that is configured in multiple-supplicant mode. Therefore, if an end device is authenticated on the interface by using captive portal, another end device connected to that interface can still be authenticated using 802.1X or MAC RADIUS authentication.

Before you configure the flexible authentication order on an interface, make sure that the authentication methods are configured on that interface. The switch does not attempt authentication using a method that is not configured on the interface, even if that method is included in the authentication order; the switch ignores that method and attempts the next method in the authentication order that is enabled on that interface.

Use the following guidelines when configuring the `authentication-order` statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If `mac-radius-restrict` is configured on an interface then the authentication order cannot be configured on that interface.

To configure a flexible authentication order, use one of the following valid combinations:

NOTE: The authentication order can be configured globally using the `interface all` option as well as locally using the individual interface name. If the authentication order is configured both for an individual interface and for all interfaces, the local configuration for that interface overrides the global configuration.

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication, and then captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x mac-radius captive-portal]
```

- To configure 802.1X authentication as the first authentication method, followed by captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x captive-portal]
```

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[dot1x mac-radius]
```

- To configure MAC RADIUS authentication as the first authentication method, followed by 802.1X, followed by captive portal:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name authentication-order
[mac-radius dot1x captive-portal]
```

After you configure the authentication order, you must use the `insert` command to make any modifications to the authentication order. Using the `set` command does not change the configured order.

To change the authentication order after initial configuration:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
authentication-method before authentication-method
```

For example, to change the order from `[mac-radius dot1x captive portal]` to `[dot1x mac-radius captive portal]`:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order
dot1x before mac-radius
```

SEE ALSO

Understanding Authentication on Switches

Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 434

Configuring EAPoL Block to Maintain an Existing Authentication Session

When a switch acting as an 802.1X authenticator receives an EAP-Start message from an authenticated client, the switch tries to re-authenticate the client using the 802.1X method and typically returns an EAP-Request message, and waits for a response. If the client fails to respond, the switch attempts to re-authenticate the client using MAC RADIUS or captive portal method if these methods were configured. Clients that have been authenticated using MAC RADIUS or captive portal authentication are non-responsive, and traffic is dropped on the interface as the switch attempts re-authentication.

If you have configured flexible authentication order on the interface so that MAC RADIUS is the first method used to authenticate a client, the switch still reverts to using 802.1X for re-authentication if the client sends an EAP-Start message, even if the client was successfully authenticated using MAC RADIUS authentication. You can configure an EAPoL block with either a fixed or flexible authentication order. If you do not configure the `authentication-order` statement, the order is fixed by default. The `eapol-block` statement can be configured with or without configuring the `authentication-order` statement.

You can configure a switch to ignore EAP-Start messages sent from a client that has been authenticated using MAC RADIUS authentication or captive portal authentication using the `eapol-block` statement. With a block of EAPoL messages in effect, if the switch receives an EAP-Start message from the client, it does not return an EAP-Request message, and the existing authentication session is maintained.

NOTE: If the endpoint has not been authenticated with MAC RADIUS authentication or captive portal authentication, the EAPoL block does not take effect. The endpoint can authenticate using 802.1X authentication.

If `eapol-block` is configured with the `mac-radius` option, then once the client is authenticated with MAC RADIUS authentication or CWA (Central Web Authentication), the client remains in authenticated state even if it sends an EAP-Start message. If `eapol-block` is configured with the `captive-portal` option, then once the client is authenticated with captive portal, the client remains in authenticated state even if it sends an EAP-Start message.

NOTE: This feature is supported on EX4300 and EX9200 switches.

To configure a block of EAPoL messages to maintain an existing authentication session:

- To configure EAPoL block for a client authenticated using MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name eapol-block mac-radius
```

- To configure EAPoL block for a client authenticated using captive portal authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name eapol-block captive-
portal
```

SEE ALSO

Understanding Authentication on Switches

RELATED DOCUMENTATION

Access Control and Authentication on Switching Devices

Server Fail Fallback and Authentication

SUMMARY

The server fail fallback mechanism for 802.1X, MAC RADIUS, and captive portal authentication defines how devices states are handled if the RADIUS server becomes unavailable or rejects access.

IN THIS SECTION

Understanding Server Fail Fallback and Authentication on Switches

Juniper Networks Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication is configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

Server fail fallback enables you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback enables you to specify one of four actions to be taken for end devices awaiting authentication when the server is timed out. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch. The configured VLAN name overrides any attributes sent by the server.

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.

- *Move* the end device to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server. (The VLAN must already exist on the switch.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

When a VLAN is configured with Server Fail VoIP, and the server fails, an Interface Bridge Domain (IFBD) is created for this VLAN during client authentication. This allows the switch to move VoIP clients to a fallback VLAN if the authentication server is unreachable or times out, ensuring voice traffic continuity. The `server-fail-voip` statement specifically handles voice VLAN tagged traffic fallback actions, such as permitting access, denying access, or moving clients to a designated VLAN already configured on the switch. If the `server-fail-voip` statement is configured, the switch uses it to isolate and manage VoIP client traffic during server fail conditions, maintaining voice service availability even when authentication cannot be completed.

SEE ALSO

802.1X for Switches Overview | **370**

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | **399**

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Configuring 802.1X Interface Settings (CLI Procedure) | **378**

Configuring RADIUS Server Fail Fallback (CLI Procedure)

You can configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to

supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the `server-fail-voip` statement. For all data traffic, use the `server-fail` statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with `server-fail`, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with `server-fail-voip`. If `server-fail-voip` is not configured, the voice traffic is dropped.

NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.

You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the `server-fail-voip` statement in place of the `server-fail` statement.

To configure server fail fallback actions:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name  server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been denied access by the RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name  server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

```
[edit protocols dot1x authenticator]
user@switch# set interface interface-name server-fail vlan-name
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new end devices are denied access):

```
[edit protocols dot1x authenticator]
user@switch# set  interface interface-name server-fail use-cache
```

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

-
```
[edit protocols dot1x authenticator]
user@switch# set  interface interface-name server-reject-vlan vlan-sf
```

SEE ALSO

Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 399

Configuring 802.1X Interface Settings (CLI Procedure) | 378

Monitoring 802.1X Authentication | 414

Configuring RADIUS Reachability to Reauthenticate Server Fail Sessions

When an authentication attempt triggers server fail fallback, the end device can reattempt authentication after a period of time. The default time interval that the end device must wait for reauthentication is 60 minutes. The reauthentication time interval can be configured using the `reauthentication` CLI statement.

The server might become available before the reauthentication timer expires. When the RADIUS reachability feature is enabled, it triggers reauthentication once it detects that the server is reachable,

without waiting for the reauthentication timer to expire. Once a session moves to server fail fallback, the authenticator will periodically query the server by initiating authentication for that session. When the authenticator receives a response, indicating that the server is reachable, it will initiate authentication for all server fail sessions.

To enable RADIUS reachability, you must configure the query period, which determines how often the authenticator queries the server for reachability. Configure the query period using the following command:

```
set protocols dot1x authenticator radius-reachability query-period
```

NOTE: The quiet period must be shorter than the query period. The quiet period is the period during which the interface remains in the wait state following a failed authentication attempt before reattempting authentication.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1X53-D40	Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.

Authentication Session Timeout

IN THIS SECTION

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. Read this topic for more information.

Understanding Authentication Session Timeout

Information about authentication sessions—including the associated interfaces and VLANs for each MAC address that is authenticated—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured `mac-table-aging-time` value, the MAC address is removed from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication session table, with the result that the session ends.

When the authentication session ends due to MAC address aging, the host must re-attempt authentication. To limit the downtime resulting from re-authentication, you can control the timeout of authentication sessions in the following ways:

- For 802.1X and MAC RADIUS authentication sessions, disassociate the authentication session table from the Ethernet switching table by using the `no-mac-table-binding` statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.
- For captive portal authentication sessions, configure a keep-alive timer using the `user-keepalive` statement. With this option configured, when the associated MAC address ages out of the Ethernet switching table, the keep-alive timer is started. If traffic is received within the keep-alive timeout period, the timer is deleted. If there is no traffic within the keep-alive timeout period, the session is deleted.

You can also specify timeout values for authentication sessions to end the session before the MAC aging timer expires. After the session times out, the host must re-attempt authentication.

- For 802.1X and MAC RADIUS authentication sessions, the duration of the session before timeout depends on the value of the `reauthentication` statement. If the MAC aging timer expires before the session times out, and the `no-mac-table-binding` statement is not configured, the session is ended, and the host must re-authenticate.
- For captive portal authentication sessions, the duration of the session depends on the value configured for the `session-expiry` statement. If the MAC aging timer expires before the session times out, and the `user-keepalive` statement is not configured, the session is ended, and the host must re-authenticate.

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using either the `reauthentication` statement or the `session-expiry` statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message. For information about configuring the authentication server to send an authentication session timeout, see the documentation for your server.

SEE ALSO

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Configuring MAC Table Aging on Switches

Controlling Authentication Session Timeouts (CLI Procedure)

The expiration of an authentication session can result in downtime because the host must re-attempt authentication. You can limit this downtime by controlling the timeout period for authentication sessions.

An authentication session can end when the MAC address associated with the authenticated host ages out of the Ethernet switching table. When the MAC address is cleared from the Ethernet switching table, the authenticated session for that host ends, and the host must re-attempt authentication.

To prevent the authentication session from ending when the MAC address ages out of the Ethernet switching table:

- For sessions authenticated using 802.1X or MAC RADIUS authentication, you can prevent authentication session timeouts due to MAC address aging by disassociating the authentication session table from the Ethernet switching table using the `no-mac-table-binding` statement:

```
[edit]
user@switch# set protocols dot1x authenticator no-mac-table-binding;
```

- For sessions authenticated using captive portal authentication, you can prevent authentication session timeouts due to MAC address aging by extending the timeout period using the `user-keepalive` statement:

```
[edit]
user@switch# set services captive-portal interface interface-name user-keepalive minutes;
```

You can also configure timeout values for authentication sessions to end an authenticated session before the MAC aging timer expires.

NOTE: Configuring the session timeout for an authentication session does not extend the session after the MAC aging timer expires. You must configure either the `no-mac-table-binding` statement for 802.1X and MAC RADIUS authentication, or the `user-keepalive` statement for captive portal authentication, to prevent session timeout due to MAC aging.

For 802.1X and MAC RADIUS authentication sessions, configure the timeout value using the `reauthentication` statement.

- To configure the timeout value on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name reauthentication
seconds;
```

- To configure the timeout value on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all reauthentication seconds;
```

For captive portal authentication sessions, configure the timeout value using the `session-expiry` statement.

- To configure the timeout value on a single interface:

```
[edit]
user@switch# set services captive-portal interface interface-name session-expiry minutes;
```

- To configure the timeout value on all interfaces:

```
[edit]
user@switch# set services captive-portal interface all session-expiry minutes;
```

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured using the `reauthentication` statement or the `session-expiry` statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

SEE ALSO

Configuring MAC Table Aging on Switches

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 451

Retaining the Authentication Session Based on IP-MAC Address Bindings

IN THIS SECTION

MAC RADIUS authentication is often used to permit hosts that are not enabled for 802.1X authentication to access the LAN. End devices such as printers are not very active on the network. If the MAC address associated with an end device ages out due to inactivity, the MAC address is cleared from the Ethernet switching table, and the authentication session ends. This means that other devices will not be able to reach the end device when necessary.

If the MAC address that ages out is associated with an IP address in the DHCP, DHCPv6, or SLAAC snooping table, that MAC-IP address binding will be cleared from the table. This can result in dropped traffic when the DHCP client tries to renew its lease.

You can configure the switching device to check for an IP-MAC address binding in the DHCP, DHCPv6, or SLAAC snooping table before terminating the authentication session when the MAC address ages out. If the MAC address for the end device is bound to an IP address, then it will be retained in the Ethernet switching table, and the authentication session will remain active.

This feature can be configured globally for all authenticated sessions using the CLI, or on a per-session basis using RADIUS attributes.

Benefits

This feature provides the following benefits:

- Ensures that an end device is reachable by other devices on the network even if the MAC address ages out.
- Prevents traffic from dropping when the end device tries to renew its DHCP lease.

CLI Configuration

Before you can configure this feature:

- DHCP snooping, DHCPv6 snooping, or SLAAC snooping must be enabled on the device.
- The `no-mac-table-binding` CLI statement must be configured. This disassociates the authentication session table from the Ethernet switching table, so that when a MAC address ages out, the authentication session will be extended until the next reauthentication.

```
[edit]
user@switch# set protocols dot1x authenticator no-mac-table-binding;
```

To configure this feature globally for all authenticated sessions:

- Configure the switching device to check for an IP-MAC address binding in the DHCP, DHCPv6, or SLAAC snooping table before terminating the authentication session when the MAC address ages out using the `ip-mac-session-binding` CLI statement:

```
[edit]
user@switch# set protocols dot1x authenticator ip-mac-session-binding;
```

NOTE: You cannot commit the `ip-mac-session-binding` configuration unless the `no-mac-table-binding` is also configured.

RADIUS Server Attributes

You can configure this feature for a specific authentication session using RADIUS server attributes. RADIUS server attributes are clear-text fields encapsulated in Access-Accept messages sent from the authentication server to the switching device when a supplicant connected to the switch is successfully authenticated.

To retain the authentication session based on IP-MAC address bindings, configure both of the following attribute-value pairs on the RADIUS server:

- Juniper-AV-Pair = “Ip-Mac-Session-Binding”
- Juniper-AV-Pair = “No-Mac-Binding-Reauth”

The Juniper-AV-Pair attribute is a Juniper Networks vendor-specific attribute (VSA). Verify that the Juniper dictionary is loaded on the RADIUS server and includes the Juniper-AV-Pair VSA (ID# 52).

If you need to add the attribute to the dictionary, locate the dictionary file (**juniper.dct**) on the RADIUS server and add the following text to the file:

```
ATTRIBUTE Juniper-AV-Pair       Juniper-VSA(52, string) r
```

NOTE: For specific information about configuring your RADIUS server, consult the AAA documentation included with your server.

Verification

Verify the configuration by issuing the operational mode command `show dot1x interface` *`interface-name`* `detail` and confirm that the `Ip Mac Session Binding` and `No Mac Session Binding` output fields indicate that the feature is enabled.

```
user@switch> show dot1x interface ge-0/0/16.0 detail

 ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
```

```
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 5 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Mac Radius Authentication Protocol: EAP-MD5
Reauthentication: Disabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
No Mac Session Binding: Enabled
Ip Mac Session Binding: Enabled
Number of connected supplicants: 1
  Supplicant: abc, 00:00:5E:00:53:00
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Mac Radius
    Authenticated VLAN: v100
    Session Reauth interval: 3600 seconds
    Reauthentication due in 0 seconds
    Ip Mac Session Binding: Enabled
    No Mac Binding Reauth: Enabled
    Eapol-Block: Not In Effect
```

Clients authenticated with MAC RADIUS should remain authenticated, and MAC address entries in the Ethernet switching table should also be retained after expiration of the MAC timer.

RELATED DOCUMENTATION

- 802.1X Authentication | **369**
- 802.1X and RADIUS Accounting | **444**
- MAC RADIUS Authentication | **432**

Central Web Authentication

IN THIS SECTION

Web authentication provides access to network for users by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Understanding Central Web Authentication

IN THIS SECTION

Web authentication redirects Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed access to the network. Web authentication is useful for providing network access to temporary users, such as visitors to a corporate site, who try to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Web authentication can be done locally on the switch using captive portal, but this requires that the Web portal pages be configured on each switch used as a network access device. Central Web

authentication (CWA) provides efficiency and scaling benefits by redirecting the client's Web browser to a central Web authentication server (CWA server), which handles the complete login process.

NOTE: CWA is supported with MAC RADIUS authentication only. CWA is not supported with 802.1X authentication.

Central Web Authentication Process

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The host can attempt authentication using 802.1X authentication first, but must then attempt MAC RADIUS authentication before attempting central Web authentication. The switch, operating as the authenticator, exchanges RADIUS messages with the authentication, authorization, and accounting (AAA) server. After MAC RADIUS authentication fails, the switch receives an Access-Accept message from the AAA server. This message includes a dynamic firewall filter and a redirect URL for central Web authentication. The switch applies the filter, which allows the host to receive an IP address, and uses the URL to redirect the host to the Web authentication page.

The host is prompted for login credentials and might also be asked to agree to an acceptable use policy. If Web authentication is successful, the AAA server sends a Change of Authorization (CoA) message, which updates the terms of the authorized session in progress. This enables the authenticator to update the filter or VLAN assignment applied to the controlled port, to allow the host to access the LAN.

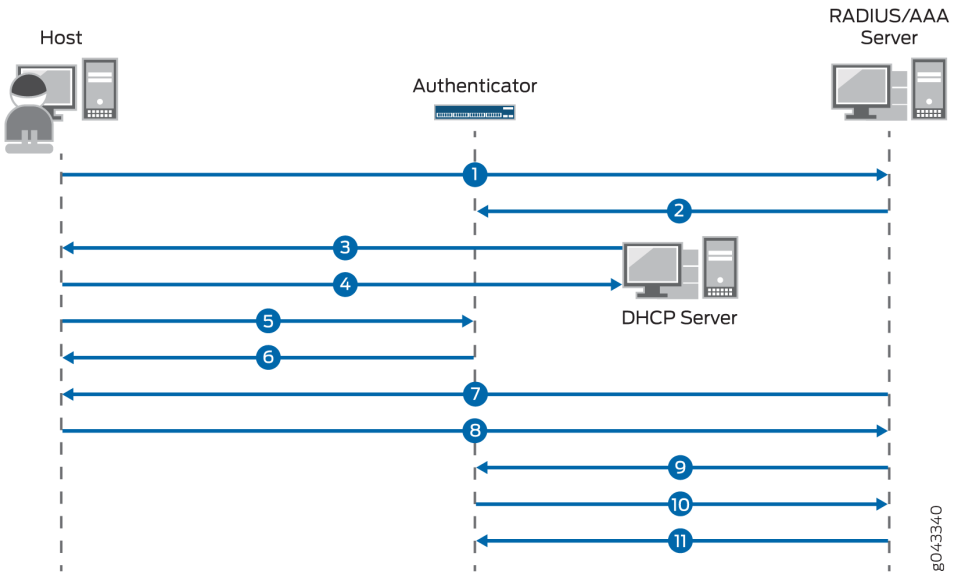
The sequence of events in central Web authentication is as follows (see Figure 20 on page 546):

1. A host connected to the switch (authenticator) initiates MAC RADIUS authentication.
2. MAC RADIUS authentication fails. Instead of sending an Access-Reject message to the switch, the AAA server sends an Access-Accept message that includes a dynamic firewall filter and a CWA redirect URL.
3. The host is allowed by the terms of the filter to send DHCP requests.
4. The host receives an IP address and DNS information from the DHCP server. The AAA server initiates a new session that has a unique session ID.
5. The host opens a Web browser.
6. The authenticator sends the CWA redirect URL to the host.
7. The host is redirected to the CWA server and is prompted for login credentials.
8. The host provides the username and password.
9. After successful Web authentication, the AAA server sends a CoA message to udpate the filter or VLAN assignment applied on the controlled port, allowing the host to access the LAN.

10. The authenticator responds with a CoA-ACK message and sends a MAC RADIUS authentication request to the AAA server.

11. The AAA server matches the session ID to the appropriate access policy and sends an Access-Accept message to authenticate the host.

Figure 20: Central Web Authentication Process



Dynamic Firewall Filters for Central Web Authentication

Central Web authentication uses dynamic firewall filters, which are centrally defined on the AAA server and dynamically applied to supplicants that request authentication through that server. The filter allows the host to get an IP address dynamically using DHCP. You define the filters by using RADIUS attributes, which are included in the Access-Accept messages sent from the server. Filters can be defined using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter with the correct terms that allow the destination IP address of the CWA server. This configuration is done directly on the AAA server. To use the Filter-ID attribute for central web authentication, enter the value as JNPR_RSVD_FILTER_CWA on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required. For more information about configuring dynamic firewall filters for central web authentication, see "Configuring Central Web Authentication" on page 547.

Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. After redirection, the CWA server completes the login process. The redirect URL for central web authentication can be configured on the AAA server or on the authenticator. The redirect URL, along with the dynamic firewall filter, must be present to trigger the central web authentication process after the failure of MAC RADIUS authentication.

The redirect URL can be centrally defined on the AAA server by using the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter. You can also configure the redirect URL locally on the host interface by using the CLI statement `redirect-url` at the [`edit protocols dot1x authenticator interface` *`interface-name`*] hierarchy level. For more information about configuring the redirect URL, see "Configuring Central Web Authentication" on page 547.

SEE ALSO

Understanding Dynamic Filters Based on RADIUS Attributes | 395

Understanding Dynamic VLAN Assignment Using RADIUS Attributes | 396

Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 384

Configuring Central Web Authentication

IN THIS SECTION

Central Web authentication is a fallback method of authentication in which the host's Web browser is redirected to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The switch, operating as the authenticator, receives a RADIUS Access-Accept message from the AAA server that includes a dynamic firewall filter and a redirect URL for central Web authentication. The dynamic firewall filter and the redirect URL must both be present for the central Web authentication process to be triggered.

Configuring Dynamic Firewall Filters for Central Web Authentication

Dynamic firewall filters are used in central Web authentication to enable the host to get an IP address from a DHCP server, which allows the host to access the network. The filters are defined on the AAA server using RADIUS attributes, which are sent to the authenticator in an Access-Accept message. You can define the filter using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

- To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter terms directly on the AAA server. The filter must include a term to match the destination IP address of the CWA server with the action `allow`.

  For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
        Session-Timeout = "300",
        Juniper-CWA-Redirect-URL = "https://10.10.10.10",
        Juniper-Switching-Filter = "Match Destination-ip 10.10.10.10 Action allow, Match ip-
protocol 17 Action allow, Match Destination-mac 00:01:02:33:44:55 Action deny"
```

  NOTE: The switch does not resolve the DNS queries for the redirect URL. You must configure the Juniper-Switching-Filter attribute to allow the destination IP address of the CWA server.

- To use the Filter-ID attribute for central Web authentication, enter JNPR_RSVD_FILTER_CWA as the value for the attribute on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required.

  For example:

```
001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
        Session-Timeout = "300",
        Juniper-CWA-Redirect-URL = "https://10.10.10.10",
        Filter-Id = "JNPR_RSVD_FILTER_CWA",
```

For more information about configuring dynamic firewall filters on the AAA server, see the documentation for your AAA server.

Configuring the Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. The redirect URL for central Web authentication can be configured on the AAA server or locally on the host interface.

- To configure the redirect URL on the AAA server, use the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter.

  For example:

  ```
  001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
          Session-Timeout = "300",
          Juniper-CWA-Redirect-URL = "https://10.10.10.10",
          Filter-Id = "JNPR_RSVD_FILTER_CWA",
  ```

  NOTE: When the special Filter-ID attribute JNPR_RSVD_FILTER_CWA is used for the dynamic firewall filter, the redirect URL must include the IP address of the AAA server, for example, **https://10.10.10.10**.

- To configure the redirect URL locally on the host interface, use the following CLI statement:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name redirect-url
  ```

  For example:

  ```
  user@switch# show protocols dot1x
  authenticator {
      authentication-name-profile auth1;
      interface {
          ge-0/0/1.0 {
              supplicant single;
              mac-radius;
              redirect-url https://10.10.10.10;
          }
  ```

```
    }
}
```

Guidelines for Configuring Central Web Authentication

Central Web authentication is triggered after the failure of MAC RADIUS authentication when the redirect URL and dynamic firewall filter are both present. The redirect URL and dynamic firewall filter can be configured in any of the following combinations:

1. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.

2. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the `redirect-url` CLI statement and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.

3. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR_RSVD_FILTER_CWA. The redirect URL must contain the IP address of the CWA server in this case.

4. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the `redirect-url` CLI statement and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value JNPR_RSVD_FILTER_CWA. The redirect URL must contain the IP address of the CWA server in this case.

NOTE: The `redirect-url` command statement is required in the CLI only if the RADIUS server is not sending the redirect URL in the "Juniper-CWA-Redirect" VSA.

RELATED DOCUMENTATION

- Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass

Dynamic VLAN Assignment for Colorless Ports

IN THIS SECTION

Enterprises typically have a variety of users and endpoints, which results in multiple use cases that need to be addressed by their policy infrastructure. The policy infrastructure should enable any supported user device to connect to any port on the access switch and to be authenticated based on the capabilities of the device, the authorization level of the user, or both.

Colorless ports support attaching any device t to any switch port because they all have the same initial configuration. The initial configuration places devices on a default VLAN that is used to authenticate and then profile the device or user. The colorless port concept relies on device profiling for VLAN assignment. Based on the type of the device that is connected to the port (AP, IP camera, or printer), the NAC server returns the appropriate VLAN using RADIUS attributes.

Benefits of Dynamic VLAN Assignment for Colorless Ports

- Allow any device to be connected to any port on an access switch.
- Deploy consistent security policies across the enterprise.

Overview

When 802.1X authentication is enabled on a port, the switch (known as the authenticator) blocks all traffic to and from the end device (known as a supplicant) until the supplicant's credentials are presented and matched on an NAC server. The NAC server is typically a RADIUS server or a policy manager that acts as a RADIUS server. After the supplicant is authenticated, the switch opens the port to the supplicant.

As part of the authentication process, a RADIUS server can return IETF-defined attributes that provide VLAN assignments to the switch. You can configure a policy manager to pass different RADIUS attributes back to the switch based on the endpoint access policy. The switch dynamically changes the VLAN assigned to the port according to the RADIUS attributes it receives.

Egress-VLAN attributes

To support both access and trunk ports as colorless ports, the RADIUS attribute must indicate if the frames on the VLAN for this port are to be represented in tagged or untagged format. The following attributes are supported for dynamically assigning a VLAN and also specifying the frame format:

- Egress-VLAN-ID
- Egress-VLAN-Name

The Egress-VLAN-ID or Egress-VLAN-Name attribute contains two parts; the first part indicates if frames on the VLAN for this port are to be represented in tagged or untagged format, the second part is the VLAN name.

For Egress-VLAN-ID:

- 0x31 = tagged
- 0x32 = untagged

For example, the following RADIUS profile includes one tagged and one untagged VLAN:

```
001094001177 Cleartext-Password := "001094001177“
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Egress-VLANID += 0x3100033,
    Egress-VLANID += 0x3200034,
```

For Egress-VLAN-Name:

- 1 = tagged
- 2 = untagged

In the example below, VLAN 1vlan-2 is tagged, and VLAN 2vlan-3 is untagged:

```
001094001144 Cleartext-Password := "001094001144“
      Tunnel-Type = VLAN,
```

```
Tunnel-Medium-Type = IEEE-802,
Egress-VLAN-Name += 1vlan-2,
Egress-VLAN-Name += 2vlan-3,
```

NOTE: It is mandatory to include the Tunnel-Type and Tunnel-Medium-Type attributes in the profile with Egress-VLAN-ID or Egress-VLAN-Name.

When the switch receives a VLAN assignment with "Egress-VLAN-ID," it checks if the VLAN is already present in the system. If not, it creates the dynamic VLAN. If the Egress-VLAN-Name is used, the VLAN should be already in the system.

Supplicant mode attributes

RADIUS attributes can also be used to change the supplicant mode for 802.1X authentication. Using a Juniper Networks vendor-specific attribute (VSA), you can set the supplicant mode to either single or single-secure:

- Juniper-AV-Pair = Supplicant-Mode-Single
- Juniper-AV-Pair = Supplicant-Mode-Single-Secure

When these attributes are received from the NAC server, the configured supplicant mode gets changed to match the VSA value after the session is authenticated. When the session ends, the supplicant mode reverts to the mode that was configured on the system before receiving the VSA from the NAC server. When a client receives the dynamic single supplicant attributes from the RADIUS server, it deletes all the other authenticated clients on that interface, effectively changing the interface mode from multiple to single supplicant.

VoIP on EX Series Switches

IN THIS SECTION

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. For more information, read this topic.

Understanding 802.1X and VoIP on EX Series Switches

IN THIS SECTION

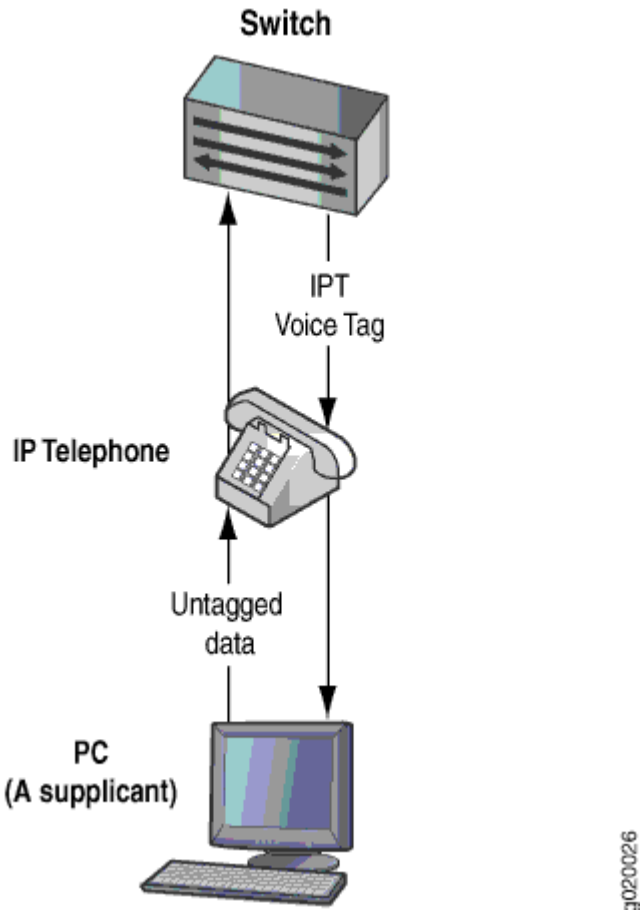
When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls by using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

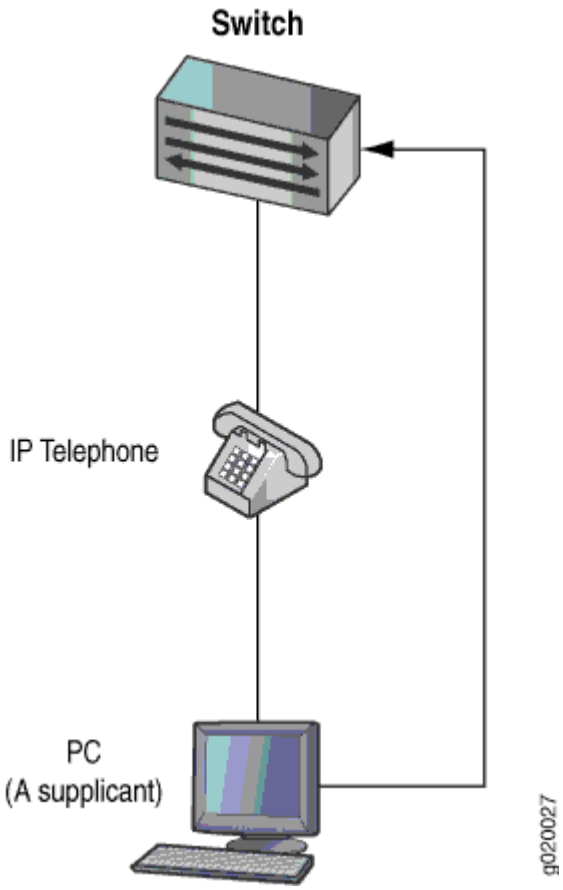
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 21 on page 555.

Figure 21: VoIP Multiple Supplicant Topology



If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single supplicant mode. In *single supplicant* mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see Figure 22 on page 556 .

Figure 22: VoIP Single Supplicant Topology



If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN.

Multi Domain 802.1X Authentication

Multi-domain 802.1X authentication is an extension of multiple supplicant mode that allows one default VoIP device and multiple data devices to authenticate on a single port. Multi-domain 802.1X authentication provides enhanced security over multiple supplicant mode by restricting the number of authenticated data and VoIP sessions on the port. In multiple supplicant mode, any number of VoIP or data sessions can be authenticated; the number of sessions can be restricted using MAC limiting, but there is no way to apply the limit specifically to either data or VoIP sessions.

With multi-domain 802.1X authentication, the single port is divided into two domains; one is the data domain and the other is the voice domain. Multi-domain 802.1X authentication maintains separate session counts based on the domain. You can configure the maximum number of authenticated data sessions allowed on the port. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed on the port.

If a new client attempts to authenticate on the interface after the maximum session count has been reached, the default action is to drop the packet and generate an error log message. You can also configure the action to shut down the interface. The port can be manually recovered from the down state by issuing the `clear dot1x recovery-timeout` command, or by can recover automatically after a configured recovery timeout period.

Multi-domain authentication does not enforce the order of device authentication. However, for the best results, the VoIP device should be authenticated before a data device on a multi domain 802.1X-enabled port. Multi-domain authentication is supported only in multiple supplicant mode.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | **711**

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch

IN THIS SECTION

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as the LLDP-MED protocol and 802.1X authentication:

NOTE: If your switch runs Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see "Example: Setting Up VoIP with

802.1X and LLDP-MED on an EX Series Switch with ELS Support" on page 593. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya 9620 IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See Installing and Connecting an EX3200 Switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- (Optional) Configured interface **ge-0/0/2** for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE Interfaces on EX Series Switches*.

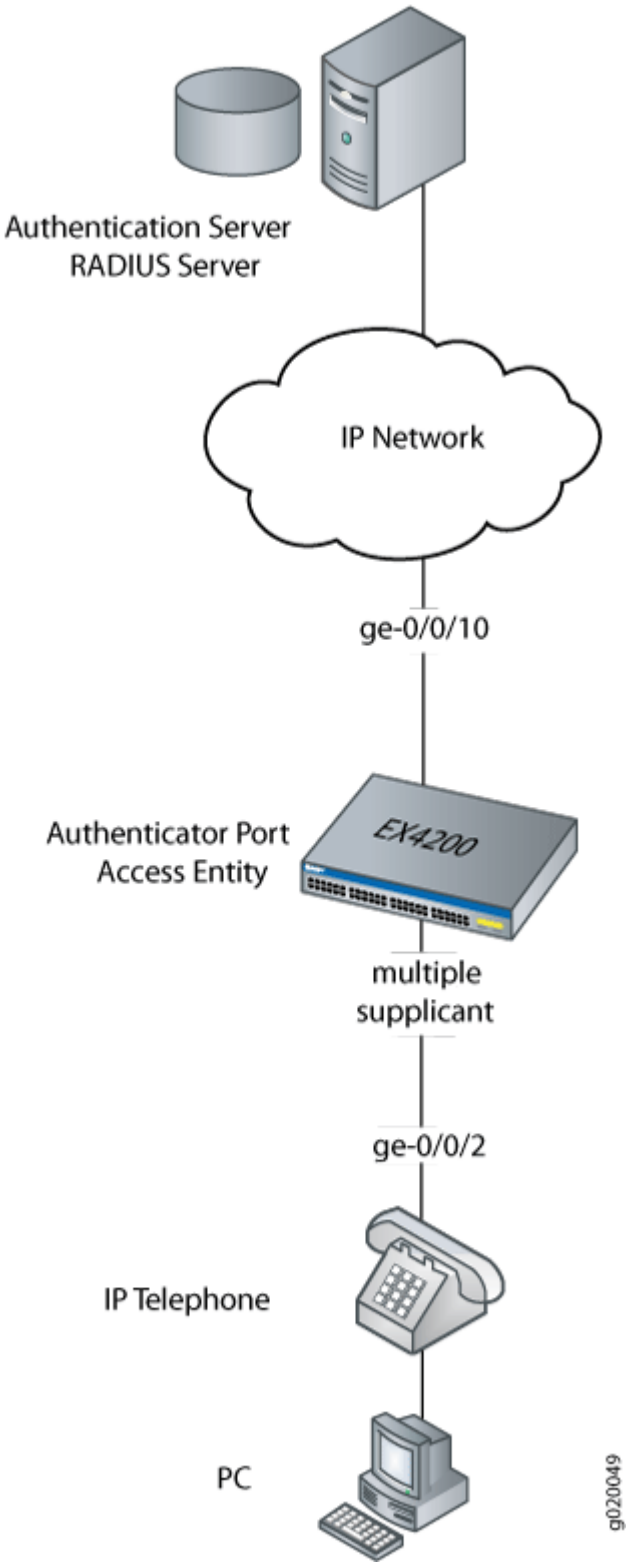
NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface **ge-0/0/2** on the EX4200 switch is connected to an Avaya 9620 IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on interface **ge-0/0/10** (see Figure 23 on page 560).

Figure 23: VoIP Topology



In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

Table 36 on page 561 describes the components used in this VoIP configuration example.

Table 36: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX4200 switch
VLAN names	**data-vlan** **voice-vlan**
Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE)	**ge-0/0/2**
One RADIUS server	Provides backend database connected to the switch through interface **ge-0/0/10**.

As well as configuring a VoIP for interface **ge-0/0/2**, you configure:

- 802.1X authentication. Authentication is set to **multiple** supplicant to support more than one supplicant's access to the LAN through interface **ge-0/0/2**.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

NOTE: A PoE configuration is not necessary if an IP telephone is using a power adapter.

Configuration

IN THIS SECTION

- Procedure | **562**

To configure VoIP, LLDP-MED, and 802.1X authentication:

Procedure

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Associate the VLAN **data-vlan** with the interface:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the **data-vlan** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode  access
```

4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2.0
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify **multiple** supplicant mode:

> **NOTE**: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant
multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
```

```
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
protocols {
    lldp-med {
        interface ge-0/0/2.0;
    }
    dot1x {
        authenticator {
            interface {
                ge-0/0/2.0 {
                    supplicant multiple;
                }
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        interface {
            ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
ethernet-switching options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
```

```
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying LLDP-MED Configuration

Purpose

Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch>                              show lldp detail
LLDP                    : Enabled
Advertisement interval : 30 Second(s)
Transmit delay          : 2 Second(s)
Hold timer              : 2 Second(s)
Config Trap Interval    : 300 Second(s)
Connection Hold timer   : 60 Second(s)

LLDP MED                : Enabled
MED fast start count    : 3 Packet(s)


Interface       LLDP       LLDP-MED    Neighbor count
all             Enabled    -           0
ge-0/0/2.0      -          Enabled     0
```

```
Interface     VLAN-id     VLAN-name
ge-0/0/0.0    0           default
ge-0/0/1.0    0           employee-vlan
ge-0/0/2.0    0           data-vlan
ge-0/0/2.0    99          voice-vlan
ge-0/0/3.0    0           employee-vlan
ge-0/0/8.0    0           employee-vlan
ge-0/0/10.0   0           default
ge-0/0/11.0   20          employee-vlan
ge-0/0/23.0   0           default

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port
VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

Meaning

The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the **ge-0/0/2.0** interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose

Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

Action

```
user@switch> show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
```

```
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The field **Role** shows that the **ge-0/0/2.0** interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose

Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

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

```
Interface   State    VLAN members          Blocking
ge-0/0/0.0  down     default               unblocked
ge-0/0/1.0  down     employee-vlan         unblocked
ge-0/0/5.0  down     employee-vlan         unblocked
ge-0/0/3.0  down     employee-vlan         unblocked
ge-0/0/8.0  down     employee-vlan         unblocked
ge-0/0/10.0 down     default               unblocked
ge-0/0/11.0 down     employee-vlan         unblocked
ge-0/0/23.0 down     default               unblocked
ge-0/0/2.0  up       voice-vlan            unblocked
                     data-vlan             unblocked
```

Meaning

The field **VLAN members** shows that the **ge-0/0/2.0** interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN. The **State** field shows that the interface is up.

SEE ALSO

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | **389**

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | **451**

Defining CoS Forwarding Classes (CLI Procedure)

Defining CoS Forwarding Classes (J-Web Procedure)

Configuring LLDP-MED (CLI Procedure) | **715**

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

IN THIS SECTION

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

Requirements

This example uses the following hardware and software components:

- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 13.2X50 or later for EX Series switches.

Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* .
- Configured the IP phone as a member of the voice VLAN.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE Interfaces on EX Series Switches*.

Overview

IN THIS SECTION

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support" on page 593.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the switch is connected to a non-LLDP-MED IP phone.

NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Topology

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Associate the VLAN `data-vlan` with the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

5. Specify the assured-forwarding forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        interface {
            ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
ethernet-switching options {
```

```
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
    }
}
```

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

IN THIS SECTION

- Procedure | 573

Procedure

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members voice-vlan;
                }
                native-vlan-id data-vlan;
            }
```

```
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
    }
    voice-vlan {
        vlan-id 99;
    }
}
```

Verification

IN THIS SECTION

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

Verifying the VLAN Association With the Interface

Purpose

Display the interface state and VLAN membership.

Action

```
user@switch>                              show ethernet-switching
interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
```

```
ge-0/0/8.0   down     employee-vlan          unblocked
ge-0/0/10.0  down     default                unblocked
ge-0/0/11.0  down     employee-vlan          unblocked
ge-0/0/23.0  down     default                unblocked
ge-0/0/2.0   up       voice-vlan             unblocked
                      data-vlan              unblocked
```

Meaning

The field `VLAN members` shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The `State` field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | **711**

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

IN THIS SECTION

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

Requirements

This example uses the following hardware and software components:

- One EX4200 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 9.1 or later for EX Series switches.

Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the IP phone as a member of the voice VLAN.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE Interfaces on EX Series Switches*.

Overview

IN THIS SECTION

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-

MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch" on page 557.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the EX4200 switch is connected to a non-LLDP-MED IP phone.

NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Topology

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
```

```
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure the VLAN **data-vlan** on the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        interface {
            ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
ethernet-switching options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
        }
    }
}
```

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members voice-vlan;
                }
                native-vlan-id data-vlan;
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
    }
    voice-vlan {
        vlan-id 99;
    }
}
```

Verification

IN THIS SECTION

- Verifying the VLAN Association With the Interface | 583

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

Verifying the VLAN Association With the Interface

Purpose

Display the interface state and VLAN membership.

Action

```
user@switch>                              show ethernet-switching
interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning

The field `VLAN members` shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The `State` field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 711

Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication

IN THIS SECTION

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication using static MAC bypass of authentication:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- An IP telephone

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- (Optional) Configured interface `ge-0/0/2` for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE Interfaces on EX Series Switches*.

NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface `ge-0/0/2` on the EX4200 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

IN THIS SECTION

To configure VoIP without 802.1X authentication:

Procedure

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP without 802.1X:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Associate the VLAN `data-vlan` with the interface:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the `data-vlan` VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
```

4. Configure VoIP on the interface and specify the `assured-forwarding` forwarding class to provide the most dependable class of service:

```
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2.0
```

6. Set the authentication profile (see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378 and "Configuring 802.1X RADIUS Accounting (CLI Procedure)" on page 448):

```
[edit protocols]
set dot1x authenticator authentication-profile-name auth-profile
```

7. Add the MAC address of the phone to the static MAC bypass list:

```
[edit protocols]
set dot1x authenticator static 00:04:f2:11:aa:a7
```

8. Set the supplicant mode to multiple:

```
[edit protocols]
set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
protocols {
    lldp-med {
        interface ge-0/0/2.0;
    }
    dot1x {
        authenticator {
            authentication-profile-name auth-profile;
                static {
                    00:04:f2:11:aa:a7;
                }
            }
            interface {
                ge-0/0/2.0 {
                    supplicant multiple;
                }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        interface {
            ge-0/0/2.0;
        }
```

```
    }
    voice-vlan {
        vlan-id 99;
    }
}
ethernet-switching options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying LLDP-MED Configuration

Purpose

Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch>                              show lldp detail
LLDP                    : Enabled
Advertisement interval : 30 Second(s)
Transmit delay          : 2 Second(s)
Hold timer              : 2 Second(s)
```

```
Config Trap Interval   : 300 Second(s)
Connection Hold timer  : 60 Second(s)

LLDP MED               : Enabled
MED fast start count   : 3 Packet(s)


Interface      LLDP       LLDP-MED    Neighbor count
all            Enabled    -           0
ge-0/0/2.0     -          Enabled     0

Interface     VLAN-id     VLAN-name
ge-0/0/0.0    0           default
ge-0/0/1.0    0           employee-vlan
ge-0/0/2.0    0           data-vlan
ge-0/0/2.0    99          voice-vlan
ge-0/0/3.0    0           employee-vlan
ge-0/0/8.0    0           employee-vlan
ge-0/0/10.0   0           default
ge-0/0/11.0   20          employee-vlan
ge-0/0/23.0   0           default

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port
VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.
```

Meaning

The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2.0` interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying Authentication for the Desktop PC

Purpose

Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.

Action

```
user@switch>  show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The field `Role` shows that the `ge-0/0/2.0` interface is in the authenticator state. The `Supplicant` field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose

Display the interface state and VLAN membership.

Action

```
user@switch> show ethernet-switching interfaces
 Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
                     data-vlan              unblocked
```

Meaning

The field `VLAN members` shows that the `ge-0/0/2.0` interface supports both the `data-vlan` VLAN and `voice-vlan` VLAN. The `State` field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 711

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch" on page 557. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can configure VoIP on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as how to configure the LLDP-MED protocol and 802.1X authentication:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2X50 or later for EX Series switches
- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see *Configuring PoE Interfaces on EX Series Switches*.

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

IN THIS SECTION

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic

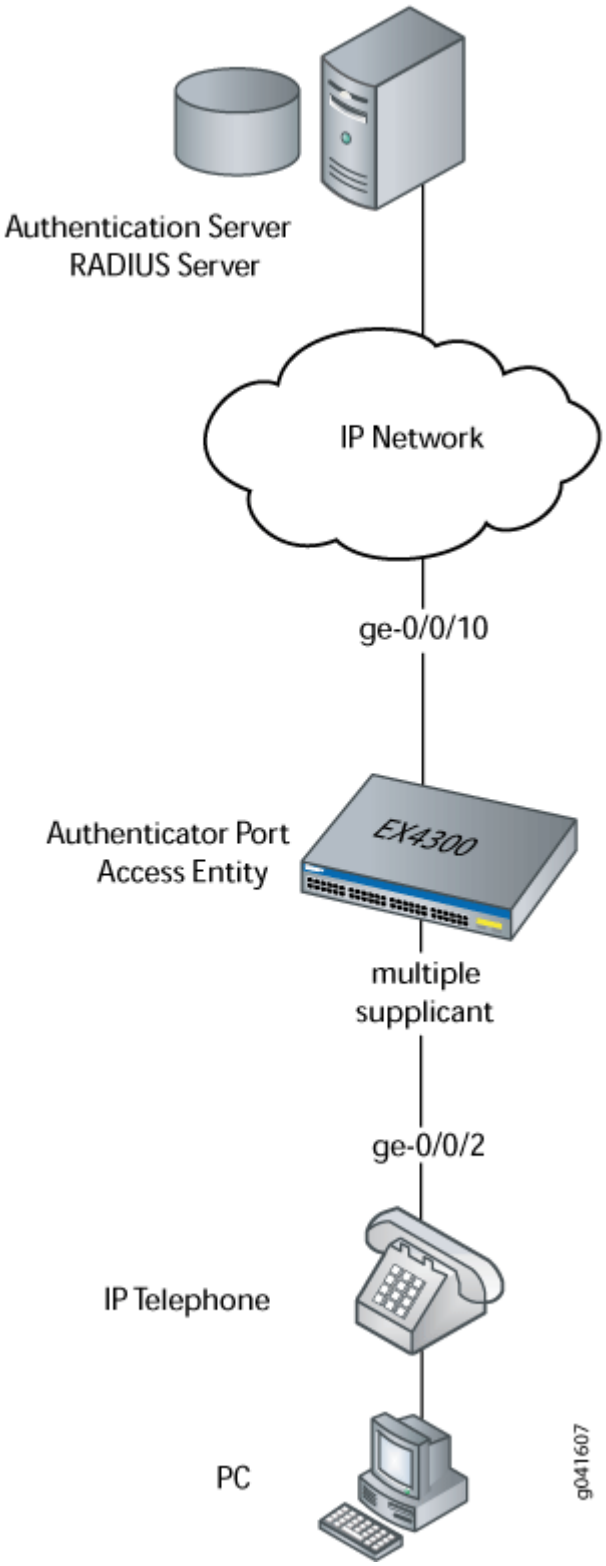
with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

NOTE: If a MAC addresses has been learned on both the data and voice VLANs, it remains active unless it ages out of both VLANs, or both VLANs are deleted.

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that enables you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see Figure 24 on page 596).

NOTE: This figure also applies to QFX5100 switches.

Figure 24: VoIP Topology



In this example, you configure VoIP parameters and specify the forwarding class `assured-forward` for voice traffic to provide the highest quality of service.

Table 37 on page 597 describes the components used in this VoIP configuration example.

Table 37: Components of the VoIP Configuration Topology

Property	Settings
Switch hardware	EX Series switch with support for ELS.
VLAN names and IDs	data-vlan, 77 voice-vlan, 99
Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE)	ge-0/0/2
One RADIUS server	Provides backend database connected to the switch through interface ge-0/0/10.

Besides configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to `multiple` supplicant mode to support more than one supplicant's access to the LAN through interface ge-0/0/2.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

> **NOTE**: A PoE configuration is not necessary if an IP telephone uses a power adapter.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Associate the VLAN **data-vlan** with the interface:

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the interface as a member of the **data-vlan** VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```

NOTE: You must not configure both data and voice on the same VLAN. If you configure data and voice on the same VLAN, the configuration will not be accepted.

If you have enabled 802.1X authentication on your switch and:

- The voice VLAN you have configured is the same as the data VLAN that the authentication server sends,
- The data VLAN you have configured is the same as the voice VLAN that the authentication server sends, or
- The data VLAN and the voice VLAN that the authentication server sends are the same

The client would move to HELD state.

4. Configure VoIP on the interface and specify the `assured-forwarding` forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify `multiple` supplicant mode:

> **NOTE**: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant
multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
protocols {
    lldp-med {
        interface ge-0/0/2;
    }
```

```
    dot1x {
        authenticator {
            interface {
                ge-0/0/2.0 {
                    supplicant multiple;
                }
            }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        switch-options {
            interface ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
switch-options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying LLDP-MED Configuration

Purpose

Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch>                              show lldp detail
LLDP                    : Enabled
Advertisement interval : 30 seconds
Transmit delay          : 2 seconds
Hold timer              : 120 seconds
Notification interval   : 0 Second(s)
Config Trap Interval    : 0 seconds
Connection Hold timer   : 300 seconds

LLDP MED                : Enabled
MED fast start count    : 3 Packets

Port ID TLV subtype     : locally-assigned

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
  Neighbor count
all            -                   Enabled     Enabled      Enabled
  0
ge-0/0/2       -                   -           Enabled      -
  0

Interface      Parent Interface    Vlan-id     Vlan-name
ge-0/0/0       -                   1           vlan-1
ge-0/0/1       -                   1           vlan-1
ge-0/0/2       -                   77          vlan-77
ge-0/0/2       -                   99          vlan-99
ge-0/0/3       -                   1           vlan-1
ge-0/0/4       -                   1           vlan-1
ge-0/0/5       -                   1           vlan-1
ge-0/0/6       -                   1           vlan-1
ge-0/0/7       -                   1           vlan-1
ge-0/0/8       -                   1           vlan-1
ge-0/0/9       -                   1           vlan-1
ge-0/0/10      -                   1           vlan-1
```

```
Basic Management TLVs supported:
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,
 System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,
 Port VLAN tag, Port VLAN name.
```

Meaning

The `show lldp detail` output shows that both `LLDP` and `LLDP-MED` are configured on the `ge-0/0/2` interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose

Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

Action

```
user@switch> show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
```

```
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The field **Role** shows that the `ge-0/0/2.0` interface is in the authenticator state. The **Supplicant mode** field shows that the interface is configured in `multiple` supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose

Display the interface's VLAN membership.

Action

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/2.0                    65535                                 untagged
             voice-vlan 99
                              65535    Discarding
             data-vlan  77
                              65535    Discarding
```

Meaning

The field **VLAN members** shows that the `ge-0/0/2.0` interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

SEE ALSO

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 389

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 451

Defining CoS Forwarding Classes (CLI Procedure)

Defining CoS Forwarding Classes (J-Web Procedure)

Configuring LLDP-MED (CLI Procedure) | 715

Example: Configuring VoIP on an EX Series Switch with ELS Support Without Including 802.1X Authentication

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication" on page 584. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication by using static MAC bypass of authentication:

Requirements

This example uses the following hardware and software components:

NOTE: This figure also applies to QFX5100 switches.

- One EX Series switch with support for ELS
- Junos OS Release 13.2 or later for EX Series switches
- An Avaya IP telephone

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 389.
- (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see *Configuring PoE Interfaces on EX Series Switches*.

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure VoIP without using 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure

To configure VoIP without 802.1X authentication:

1. Configure the VLANs for voice and data:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

2. Configure the interface as an access interface, configure support for Ethernet switching, and add the interface as a member of the `data-vlan` VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```

> **NOTE**: You must not configure both data and voice on the same VLAN. If you configure data and voice on the same VLAN, the configuration will not be accepted.

3. Configure VoIP on the interface and specify the `assured-forwarding` forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

4. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

5. Set the authentication profile with the name `auth-profile` (see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 378 and "Configuring 802.1X RADIUS Accounting (CLI Procedure)" on page 448):

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name auth-profile
```

6. Add the MAC address of the phone to the static MAC bypass list:

```
[edit protocols]
user@switch# set dot1x authenticator static 00:04:f2:11:aa:a7
```

7. Set the supplicant mode to multiple:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}
protocols {
    lldp-med {
        interface ge-0/0/2;
    }
    dot1x {
        authenticator {
            authentication-profile-name auth-profile;
                static {
                    00:04:f2:11:aa:a7;
                }
            }
            interface {
```

```
                ge-0/0/2.0 {
                    supplicant multiple;
                }
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        switch-options {
            interface ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
switch-options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying LLDP-MED Configuration

Purpose

Verify that LLDP-MED is enabled on the interface.

Action

```
user@switch>                              show lldp detail
LLDP                    : Enabled
Advertisement interval : 30 seconds
Transmit delay          : 2 seconds
Hold timer              : 120 seconds
Notification interval   : 0 Second(s)
Config Trap Interval    : 0 seconds
Connection Hold timer   : 300 seconds

LLDP MED                : Enabled
MED fast start count    : 3 Packets

Port ID TLV subtype     : locally-assigned

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
  Neighbor count
all            -                   Enabled     Enabled      Enabled
  0
ge-0/0/2       -                   -           Enabled      -
  0

Interface      Parent Interface    Vlan-id     Vlan-name
ge-0/0/0       -                   1           vlan-1
ge-0/0/1       -                   1           vlan-1
ge-0/0/2       -                   77          vlan-77
ge-0/0/2       -                   99          vlan-99
ge-0/0/3       -                   1           vlan-1
ge-0/0/4       -                   1           vlan-1
ge-0/0/5       -                   1           vlan-1
ge-0/0/6       -                   1           vlan-1
ge-0/0/7       -                   1           vlan-1
ge-0/0/8       -                   1           vlan-1
ge-0/0/9       -                   1           vlan-1
ge-0/0/10      -                   1           vlan-1
```

```
Basic Management TLVs supported:
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,
 System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,
 Port VLAN tag, Port VLAN name.
```

Meaning

The `show lldp detail` command output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2` interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

Verifying Authentication for the Desktop PC

Purpose

Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.

Action

```
user@switch>  show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
```

```
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The field `Role` shows that the `ge-0/0/2.0` interface is in the authenticator role. The `Supplicant Mode` field shows that the interface is configured in `multiple` supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose

Display the interface's VLAN membership.

Action

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/2.0                    65535                                 untagged
             voice-vlan 99
                               65535    Discarding
             data-vlan  77
                               65535    Discarding
```

Meaning

The `Vlan members` field shows that the `ge-0/0/2.0` interface supports both the `data-vlan` VLAN and `voice-vlan` VLAN.

SEE ALSO

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support | 593

Understanding 802.1X and VoIP on EX Series Switches | 554

Understanding LLDP and LLDP-MED on EX Series Switches | 711

RELATED DOCUMENTATION

RADIUS Server Configuration for Authentication | 345

802.1X Authentication | 369

Understanding LLDP-MED Bypass

SUMMARY

IN THIS SECTION

The LLDP-MED Bypass feature streamlines network access for LLDP-MED devices, such as VoIP phones, by allowing them to bypass the 802.1X authentication process on interfaces configured with dot1x. This functionality is crucial in environments where rapid and secure connectivity for multiple VoIP devices is essential. The bypass mechanism automatically adds the MAC addresses of LLDP-MED devices to the dot1x static MAC bypass list, facilitating seamless integration into VoIP VLANs. While this feature enhances efficiency for tagged VoIP traffic, it ensures that untagged data traffic still adheres to standard authentication procedures. Configuring and verifying LLDP-MED Bypass involves specific commands and is supported across all platforms with dot1x capability, providing a robust and flexible solution for managing VoIP device connectivity in sophisticated network environments.

Benefits of LLDP-MED Bypass

- Simplifies the deployment and management of VoIP devices by eliminating the need for 802.1X authentication, allowing for quicker and more efficient network access.

- Enhances operational efficiency by automatically adding LLDP-MED device MAC addresses to the dot1x static MAC bypass list, reducing manual configuration efforts.
- Ensures secure and streamlined connectivity for tagged VoIP traffic while maintaining standard authentication protocols for untagged data traffic, balancing security and ease of access.
- Provides compatibility across platforms that support dot1x, facilitating widespread adoption and integration into existing network environments.
- Minimizes the need for additional memory resources and ensures no significant impact on network performance, making it a cost-effective solution for managing multiple VoIP devices.

Configuration and Verification

When you enable the LLDP-MED Bypass feature, you streamline the connectivity process for LLDP-MED devices, such as VoIP phones, by allowing them to automatically bypass the 802.1X authentication process on dot1x-configured interfaces. This automation is crucial in environments with a high density of VoIP devices, ensuring rapid and secure network access. The mechanism works by automatically adding the MAC addresses of LLDP-MED devices to the dot1x static MAC bypass list, which eliminates the need for manual configuration and ensures that these devices are seamlessly integrated into VoIP VLANs.

To configure the LLDP-MED Bypass feature, you must use specific commands. For instance, you can enable LLDP-MED Bypass on a particular interface using the command `set protocols dot1x authenticator interface <interface> lldp-med-bypass`. If you need to enable this feature on all interfaces, the command `set protocols dot1x authenticator interface all lldp-med-bypass` should be used. Additionally, configuring VoIP VLAN on the interface is essential for proper functionality, which can be done using the command `set switch-options voip interface <interface> vlan voice`. These configurations ensure that LLDP-MED devices can bypass the authentication process and connect quickly and securely.

Verification of the LLDP-MED Bypass configuration can be done using the command `show dot1x authentication-bypassed-users`, which displays the MAC addresses of clients that have bypassed authentication. This ensures that you can monitor and manage the devices utilizing the bypass feature. To remove the LLDP-MED Bypass configuration from an interface, use the command `delete protocols dot1x authenticator interface <interface> lldp-med-bypass`.

In summary, the LLDP-MED Bypass feature simplifies the deployment and management of VoIP devices by automating the authentication bypass process. Proper configuration and regular verification are essential for leveraging the full benefits of this feature, ensuring that your network remains both secure and efficient.

How to Configure a Predefined Authentication Order

SUMMARY

The Dot1x Selective Server-Reject VLAN feature enhances the flexibility and security of 802.1X client authentication processes. When a RADIUS server rejects a client's authentication, the switch uses additional configured authentication methods, such as MAC RADIUS, before placing the client into a server-reject VLAN. This feature requires careful configuration of the authentication order and server-reject VLAN settings to maximize network access opportunities while maintaining robust security. Additionally, the feature introduces specific command-line interface (CLI) commands for configuring these behaviors and supports detailed customization of authentication sequences, providing a resilient and user-friendly authentication workflow.

IN THIS SECTION

Benefits of Configuring Multiple Authentication Methods

- Enhances network security by attempting multiple authentication methods before restricting client access, ensuring thorough verification of client legitimacy.
- Improves user experience by reducing unnecessary placement of clients into server-reject VLANs, allowing for alternative authentication methods to grant access.
- Increases flexibility in network access control by allowing configurable authentication sequences that adapt to different network policies and requirements.
- Ensures optimal use of network resources by preventing immediate client isolation, thus allowing for more efficient handling of authentication processes.
- Supports a resilient authentication workflow that maintains a balance between security and accessibility, even in re-authentication scenarios.

Overview

The Dot1x Selective Server-Reject VLAN feature significantly enhances the 802.1X client authentication mechanism by modifying how clients are handled upon authentication rejection by a RADIUS server. Instead of immediately placing rejected clients into a server-reject VLAN, the switch attempts other configured authentication methods, such as MAC RADIUS. This approach ensures a thorough verification process, potentially allowing clients to gain network access through alternative authentication paths before resorting to restrictive measures.

To utilize this feature, you must carefully configure the authentication order and the server-reject VLAN settings. The authentication order dictates the sequence in which the switch attempts different methods, ensuring that all potential avenues for client authentication are explored. For instance, you can set the order to try 802.1X first, followed by MAC RADIUS, depending on your network policies and requirements. The feature requires that the post-auth-order option be enabled on the interface, which directs the switch to try additional authentication methods before placing the client into the server-reject VLAN.

The CLI command `set protocols dot1x authenticator interface <INTF_NAME> server-reject-vlan post-auth-order` is central to configuring this feature. This command ensures that the switch attempts all configured authentication methods in the specified order before enforcing the server-reject VLAN. Note that this feature is not compatible with captive portal configurations on the same interface and requires that MAC RADIUS be configured. During re-authentication, the feature maintains a balance between flexibility and security by placing clients directly into the server-reject VLAN if the RADIUS server rejects them again, thus preventing potential security loopholes.

Configuration Example

To implement the Dot1x Selective Server-Reject VLAN feature, consider the following configuration example. Assume you have an interface that needs to support both 802.1X and MAC RADIUS authentication methods, and you want to ensure clients are given multiple chances to authenticate before being placed in the server-reject VLAN.

Configure MAC RADIUS and Dot1x on the Interface:

```
set protocols dot1x authenticator interface ge-0/0/1 mac-radius set protocols dot1x authenticator interface
ge-0/0/1
```

Set the Authentication Order:

```
set protocols dot1x authenticator interface ge-0/0/1 server-reject-vlan post-auth-order
```

Specify the Server-Reject VLAN:

```
set protocols dot1x authenticator interface ge-0/0/1 server-reject-vlan vlan10
```

In this example, the switch first tries 802.1X authentication. If the RADIUS server rejects the client, the switch then attempts MAC RADIUS authentication. Only if both methods fail will the client be placed in VLAN 10, the server-reject VLAN. This configuration ensures a flexible and secure authentication process, improving the overall network user experience.

CHAPTER 8

Configuring IEEE 802.1x Port-Based Network Access Control

IN THIS CHAPTER

IEEE 802.1x Port-Based Network Access Control Overview

MX Series routers support the IEEE 802.1x Port-Based Network Access Control (dot1x) protocol on Ethernet interfaces for validation of client and user credentials to prevent unauthorized access to a specified router port. Before authentication is complete, only 802.1x control packets are allowed and forwarded to the router control plane for processing. All other packets are dropped.

Authentication methods used must be 802.1x compliant. Authentication using RADIUS and Microsoft Active Directory servers is supported. The following user/client authentication methods are allowed:

- EAP-MD5 (RFC 3748)
- EAP-TTLS requires a server certificate (RFC 2716)
- EAP-TLS requires a client and server certificate
- PEAP requires only a server certificate

You can use both client and server certificates in all types of authentication except EAP-MD5.

NOTE: On the MX Series router, 802.1x can be enabled on bridged ports only and not on routed ports.

Dynamic changes to a user session are supported to allow the router administrator to terminate an already authenticated session by using the “RADIUS disconnect” message defined in RFC 3576.

RELATED DOCUMENTATION

Understanding the Administrative State of the Authenticator Port | **621**

Understanding the Administrative Mode of the Authenticator Port | **621**

Configuring the Authenticator | **622**

Viewing the dot1x Configuration | **623**

Ethernet Interfaces User Guide for Routing Devices

Understanding the Administrative State of the Authenticator Port

The administrative state of an authenticator port can take any of the following three states:

- Force authorized—Allows network access to all users of the port without requiring them to be authenticated. This is equivalent to not having any authentication enabled on the port.
- Force unauthorized—Denies network access to all users of the port. This is equivalent to disabling the port.
- Automatic—This is the default mode where the authentication server response determines if the port is opened for traffic or not. Only the successfully authenticated clients are allowed access, all others are denied.

In Junos OS, the default mode is “automatic.” The “force authorized” and “force unauthorized” admin modes are not supported. You can achieve the functionality of “force authorized” mode by disabling `dot1x` on the required port. You can achieve the functionality of “force unauthorized” mode by disabling the port itself.

RELATED DOCUMENTATION

IEEE 802.1x Port-Based Network Access Control Overview | **620**

Understanding the Administrative Mode of the Authenticator Port | **621**

Configuring the Authenticator | **622**

Viewing the dot1x Configuration | **623**

Ethernet Interfaces User Guide for Routing Devices

Understanding the Administrative Mode of the Authenticator Port

Junos OS supports the supplicant mode “single” and not the “single secure” nor “multiple” modes. The “Single” mode option authenticates only the first client that connects to a port. All other clients that connect later (802.1x compliant or noncompliant) are allowed free access on that port without any

further authentication. If the first authenticated client logs out, all other users are locked out until a client authenticates again.

RELATED DOCUMENTATION

- IEEE 802.1x Port-Based Network Access Control Overview | 620
- Understanding the Administrative State of the Authenticator Port | 621
- Configuring the Authenticator | 622
- Viewing the dot1x Configuration | 623
- Ethernet Interfaces User Guide for Routing Devices

Configuring the Authenticator

To configure the IEEE 802.1x Port-Based Network Access Control protocol on Ethernet interfaces you must configure the `authenticator` statement at the `[edit protocols dot1x]` hierarchy level. Use the `authentication-profile-name` *`access-profile-name`* statement to specify the authenticating RADIUS server, and use the `interface` statement to specify and configure the Gigabit Ethernet interface on the router specifically for IEEE 802.1x protocol use; both at the `[edit protocols dot1x authenticator]` hierarchy level.

```
[edit protocols dot1x]
authenticator {
    authentication-profile-name access-profile-name;
    interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) {
        maximum-requests seconds;
        quiet-period seconds;
        reauthentication (disable | interval seconds);
        retries integer;
        server-timeout seconds;
        supplicant (single);
        supplicant-timeout seconds;
        transmit-period seconds;
    }
}
```

RELATED DOCUMENTATION

- IEEE 802.1x Port-Based Network Access Control Overview | 620
- Understanding the Administrative State of the Authenticator Port | 621
- Understanding the Administrative Mode of the Authenticator Port | 621
- Viewing the dot1x Configuration | 623
- Ethernet Interfaces User Guide for Routing Devices

Viewing the dot1x Configuration

IN THIS SECTION

Purpose

To review and verify the dot1x configuration.

Action

To view all `dot1x` configurations, use the `show dot1x interface` operational mode command. To view a `dot1x` configuration for a specific interface, use the `show dot1x interface (xe-`*`fpc/pic/port`*` | ge-`*`fpc/pic/port`*` | fe-`*`fpc/pic/port`*`) detail` operational mode command. See the *Network Interfaces Command Reference* for more information about this command.

RELATED DOCUMENTATION

- IEEE 802.1x Port-Based Network Access Control Overview | 620
- Understanding the Administrative State of the Authenticator Port | 621
- Understanding the Administrative Mode of the Authenticator Port | 621

9

CHAPTER

Configuring IEEE 802.1x Port-Based Network Access Control in Enhanced LAN Mode

IN THIS CHAPTER

802.1X for MX Series Routers in Enhanced LAN Mode Overview

IN THIS SECTION

IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. Support is implemented for controlling access to your network through an MX Series router by using several different authentication methods, such as 802.1X, MAC RADIUS, or a captive portal.

This functionality is supported on the following MPCs in enhanced LAN mode:

- MPC4E with two 100-Gigabit Ethernet ports and eight 10-Gigabit Ethernet ports
- MPC4E with thirty-two 10-Gigabit Ethernet ports
- MPC3E that contains a 2-port 40-Gigabit Ethernet MIC with QSFP+
- MPC1E with forty 1-Gigabit Ethernet ports or twenty 1-Gigabit Ethernet ports

You must reboot the router when you configure or delete the enhanced LAN mode on the router. Configuring the `network-services lan` option implies that the system is running in the enhanced IP mode. When you configure a device to function in MX-LAN mode, only the supported configuration statements and operational show commands that are available for enabling or viewing in this mode are displayed in the CLI interface. If your system contains parameters that are not supported in MX-LAN mode in a configuration file, you cannot commit those unsupported attributes. You must remove the settings that are not supported and then commit the configuration. After the successful CLI commit, a system reboot is required for the attributes to be come effective. Similarly, if you remove the `network-services lan` statement, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. If your configuration file contains settings that are supported only in MX-LAN mode, you must remove those attributes before you commit the configuration. After the successful CLI commit, a system reboot will be required for the CLI settings to take effect. The Layer 2 Next-Generation CLI configuration settings are supported in MX-LAN mode. As a result, the typical MX Series-format of CLI configurations might differ in MX-LAN mode.

This functionality is supported on an MX Series Virtual Chassis combination that functions in enhanced LAN mode (by entering the `network-services lan` statement at the `[edit chassis]` hierarchy level). Port-based network access control is supported on devices with MPCs in both the MX-LAN mode and the non-MX-LAN mode (with other supported network services modes on MPCs on these routers). To configure the IEEE 802.1x port-based network access control (PNAC) protocol on Ethernet interfaces, you must configure the `authenticator` statement at the `[edit protocols authentication-access- control]` hierarchy level. You can also configure captive portal authentication on a router so that users connected to the switch are authenticated before being allowed to access the network.

How 802.1X Authentication Works

802.1X authentication works by using an *Authenticator Port Access Entity* (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in either *single* mode, *single-secure* mode, or *multiple* mode:

- **single**—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the end devices’ authentication.
- **single-secure**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.
- **multiple**—Allows multiple end devices to connect to the port. Each end device will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 354.

802.1X Features Overview

NOTE: The 802.1X features available on the MX Series routers depend upon which switch you are using.

802.1X features on Juniper Networks MX Series routers are:

- Guest VLAN—Provides limited access to a LAN, typically just to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected . Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access just to the Internet and to other guests' end devices.
- Server-reject VLAN—Provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.
- Server-fail VLAN—Provides limited access to a LAN, typically just to the Internet, for 802.1X end devices during a RADIUS server timeout.
- Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).
- Dynamic changes to a user session—Allows the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

Supported Features Related to 802.1X Authentication

802.1X does not replace other security technologies. 802.1X works together with port security features, such as DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting, to guard against spoofing.

Supported features related to authentication include:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.

- MAC RADIUS authentication—Provides a means to enable or disable MAC authentication independently of whether 802.1X authentication is enabled.

Understanding 802.1X and LLDP and LLDP-MED on MX Series Routers in Enhanced LAN Mode

MX Series routers use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the router to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Juniper Networks Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the router and the IP telephone.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the router to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the router interface to which it connects.

The router also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1Q tag information can be sent to the IP telephone.

Devices can support the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.

  NOTE: The Chassis ID TLV has a subtype for Network Address Family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

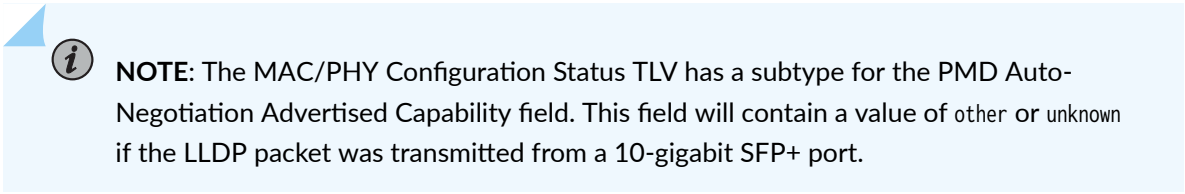
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV will contain the description

configured on the physical interface. For example, LAG member interfaces do not contain a logical unit, so only the description configured on the physical interface can be used.

- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.
- **Management Address**—The IPv4 or IPv6 management address of the local system.

Devices can support the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises MDI power support, PSE power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support. The information is not configurable, but based on the physical interface structure.



NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field will contain a value of `other` or `unknown` if the LLDP packet was transmitted from a 10-gigabit SFP+ port.

- **Link Aggregation**—A TLV that advertises if the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

Devices can support the following LLDP-MED TLVs:

- **LLDP MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
  - **0**— Capabilities
  - **1**— Network Policy
  - **2**— Location Identification
  - **3**— Extended Power via MDI-PSE

  - **4**— Inventory
  - **5–15**— Reserved
- LLDP-MED Device Class Values:
  - **0**— Class not defined.
  - **1**— Class 1 Device.
  - **2**— Class 2 Device.
  - **3**— Class 3 Device.
  - **4**— Network Connectivity Device
  - **5–255**— Reserved.
- **Network Policy**—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and Diffserv code points.
- **Endpoint Location**— A TLV that advertises the physical location of the endpoint.
- **Extended Power via MDI**— A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

Understanding 802.1X and RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

Juniper Networks MX Series routers support IETF RFC 2866, *RADIUS Accounting*. You can configure RADIUS accounting on an MX Series router which enables statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. In the event

that the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Juniper Networks Junos operating system (Junos OS).

The RADIUS accounting process between a switch and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.
2. The switch forwards an *accounting-request* packet containing an event record to the accounting server. For example, a supplicant is authenticated through 802.1X authentication and connected to the LAN. The event record associated with this supplicant contains an *Acct-Status-Type* attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request will contain an *Acct-Status-Type* attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.
3. The RADIUS accounting server logs these events as start-accounting or stop-accounting records. The records are in a file. On FreeRADIUS, the file name is the server's address; for example, 122.69.1.250.
4. The accounting server sends an *accounting-response* packet back to the switch confirming it has received the accounting request.
5. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

Understanding 802.1X and VoIP on MX Series Routers in Enhanced LAN Mode

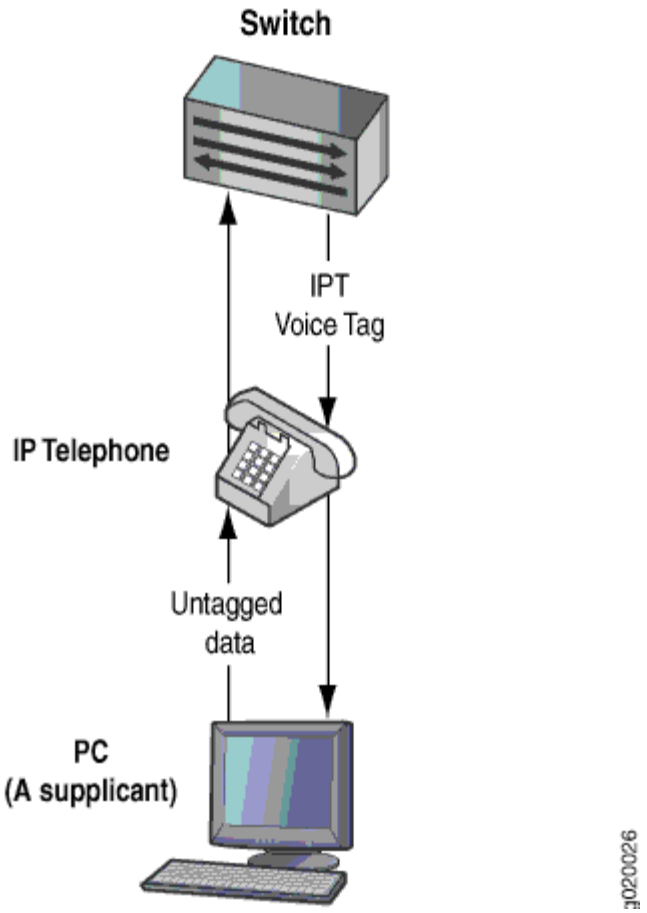
When you use Voice over IP (VoIP), you can connect IP telephones to the router and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

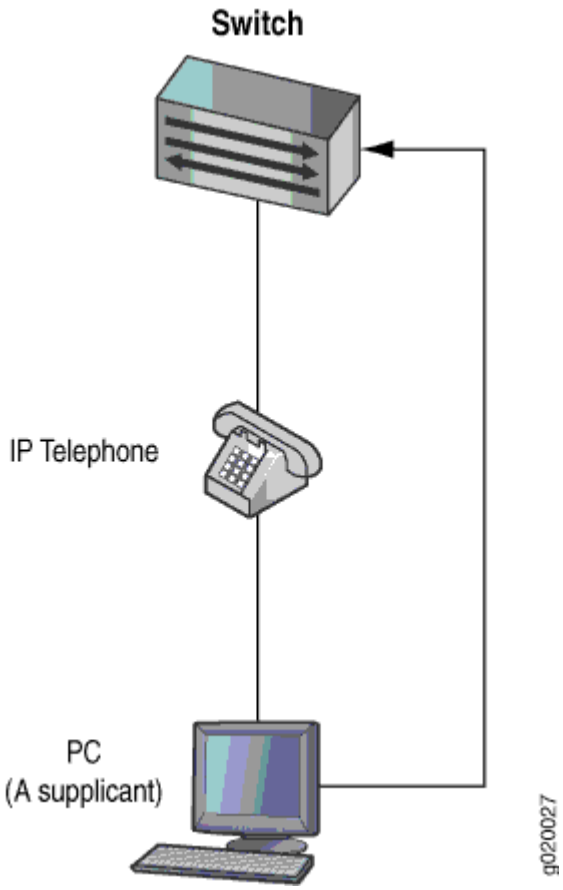
You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple-supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 25 on page 634.

Figure 25: VoIP Multiple Supplicant Topology



If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single-supplicant mode. In *single-supplicant* mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see Figure 26 on page 635 .

Figure 26: VoIP Single Supplicant Topology



If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN,

Understanding Guest VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled

- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants sending incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication.

Understanding Dynamic VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.

When this feature is configured on the RADIUS server, an end device or user authenticating on the RADIUS server is assigned to the VLAN configured for it. The end device or user becomes a member of a VLAN dynamically after successful 802.1X authentication. For information on configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

Successful authentication requires that the VLAN ID or VLAN name exist on the router and match the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is unauthenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

Understanding Server Fail Fallback and Authentication on MX Series Routers in Enhanced LAN Mode

Server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Juniper Networks MX Series routers in enhanced LAN mode use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication are configured on the interface, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the MX Series router opens the interface to permit access.

A RADIUS server timeout occurs if no RADIUS authentication servers are reachable when an end device logs in and attempts to access the LAN. Server fail fallback allows you to specify one of four actions to be taken toward end devices awaiting authentication when the server is timed out:

- *Permit* authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- *Deny* authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- *Move* the end device to a specified VLAN. (The VLAN must already exist on the router.)
- *Sustain* authenticated end devices that already have LAN access and *deny* unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device's first attempt at authentication through the RADIUS server.

Server fail fallback allows you to specify that an end device be moved to a specified VLAN if the router receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server.

Configuring 802.1X RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server.The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure basic RADIUS accounting using the CLI:

1. Specify the accounting servers to which the switch will forward accounting statistics:

```
[edit access ]
user@router# set profile profile1 radius accounting-server [122.69.1.250
122.69.1.252]
```

2. Define the RADIUS accounting servers:

```
[edit access]
user@router#   set radius-server 122.69.1.250 secret juniper
user@router# set radius-server 122.69.1.252 secret juniper1
```

3. Enable accounting for an access profile:

```
[edit access]
user@router# set profile profile1 accounting
```

4. Configure the RADIUS servers to use while sending accounting messages and updates:

```
[edit access]
user@router# set profile profile1 accounting order radius
```

5. Configure the statistics to be collected on the router and forwarded to the accounting server:

```
[edit access ]
user@router# set profile profile1 accounting accounting-stop-on-access-deny
```

```
user@router# set profile profile1 accounting accounting-stop-on-
failure
```

6. Display accounting statistics collected on the router:

```
user@router> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```

7. Open an accounting log on the RADIUS accounting server using the server's address, and view accounting statistics:

```
[root@freeradius]# cd /usr/local/var/log/radius/radacct/122.69.1.250
[root@freeradius 122.69.1.250]# ls

detail-20071214


[root@freeradius 122.69.1.250]# vi details-20071214


        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Stop
        Acct-Session-Id = "8O2.1x811912"
        Acct-Input-Octets = 17454
        Acct-Output-Octets = 4245
        Acct-Session-Time = 1221041249
        Acct-Input-Packets = 72
        Acct-Output-Packets = 53
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual
```

```
        User-Name = "000347e1bab9"
        NAS-Port = 67
        Acct-Status-Type = Start
        Acct-Session-Id = "802.1x811219"
        Called-Station-Id = "00-19-e2-50-52-60"
        Calling-Station-Id = "00-03-47-e1-ba-b9"
        Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
        NAS-Identifier = "esp48t-1b-01"
        NAS-Port-Type = Virtual
```

Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:

- You can also specify an 802.1X exclusion list to specify supplicants can that can bypass authentication and be automatically connected to the LAN.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.
- You cannot configure 802.1X user authentication on redundant trunk groups (RTGs).

Before you begin, specify the RADIUS server or servers to be used as the authentication server.

To configure 802.1X on an interface:

1. Configure the supplicant mode as **single** (authenticates the first supplicant), **single-secure** (authenticates only one supplicant), or **multiple** (authenticates multiple supplicants):

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 supplicant multiple
```

2. Enable reauthentication and specify the reauthentication interval:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5/0 dot1x reauthentication interval 5
```

3. Configure the interface timeout value for the response from the supplicant:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 dot1x supplicant-timeout 5
```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 server-timeout 5
```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 dot1x transmit-period 60
```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 dot1x maximum-requests 5
```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

```
[edit protocols authentication-access-control]
user@switch# set interface ge-0/0/5 retries 1
```

NOTE: This setting specifies the number of tries before the switch puts the interface in a “HELD” state.

Configuring LLDP-MED on MX Series Routers in Enhanced LAN Mode

IN THIS SECTION

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The router uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is turned on by default on MX Series routers.

This topic describes:

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@router# set interface (LLDP-MED) ge-0/0/2.0
```

Configuring Location Information Advertised by the Router

You can configure the location information that is advertised from the router to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

```
[edit protocols lldp-med]

user@router# set interface ge-0/0/2.0 location civic-based country-code
US
user@router# set interface ge-0/0/2.0 location civic-based ca-type 1 ca-value “El Dorado
County”
user@router# set interface ge-0/0/2.0 location civic-based ca-type 2 ca-value CA
user@router# set interface ge-0/0/2.0 location civic-based ca-type 3 ca-value Somerset
user@router# set interface ge-0/0/2.0 location civic-based ca-type 6 ca-value “Mount Aukum
Road”
user@router# set interface ge-0/0/2.0 location civic-based ca-type 19 ca-value 6450
user@router# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value “Holiday
Market”
```

- To specify a location using an **elin** string:

```
[edit protocols lldp-med]

user@router# set interface ge-0/0/2.0 location elin 4085551212
```

Configuring for Fast Start

You can specify the number of LLDP-MED advertisements sent from the router in the first second after it has detected an LLDP-MED device. The default is 3; to set it to another value:

```
[edit protocols lldp-med]
user@router# set fast-start 6
```

NOTE: If an interface is configured as a VoIP interface, then the router does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Configuring LLDP on MX Series Routers in Enhanced LAN Mode

IN THIS SECTION

Devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links.The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

```
[edit protocols lldp]
user@router# set interface all
```

- To configure LLDP on a specific interface:

```
[edit protocols lldp]
user@router# set interface interface-name
```

NOTE: On MX Series routers, LLDP cannot be configured on the management Ethernet interface. Issuing the command `set protocols lldp interfaceem0` generates the following error message:

```
error: name: 'em0': Invalid interface
error: statement creation failed: interface
```

Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

```
[edit protocols lldp]
user@router# set advertisement-interval seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@router# set advertisement-interval 45
```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the **advertisement-interval** value):

```
[edit protocols lldp]
user@router# set hold-multiplier seconds
```

For example, using the default value:

```
[edit protocols lldp]
user@router# set hold-multiplier 5
```

- To specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the **advertisement-interval** value is set to 8 seconds or more) or 1 second (if the **advertisement-interval** value is set to less than 8 seconds).

```
[edit protocols lldp]
user@router# set transmit-delay seconds
```

For example:

```
[edit protocols lldp]
user@router# set transmit-delay 2
```

NOTE: The **advertisement-interval** value must be greater than or equal to four times the **transmit-delay** value; otherwise, an error is returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to **0**, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

```
[edit protocols lldp]
user@router# set lldp-configuration-notification-interval seconds
```

For example:

```
[edit protocols lldp]
user@router# set lldp-configuration-notification-interval 600
```

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

```
[edit protocols lldp]
user@router# set ptopo-configuration-trap-interval seconds
```

For example:

```
[edit protocols lldp]
user@router# set ptopo-configuration-trap-interval 600
```

- To specify the holding time (used in combination with the **ptopo-configuration-trap-interval** value) to maintain dynamic topology entries (in seconds):

```
[edit protocols lldp]
user@router# set ptopo-configuration-maximum-hold-time seconds
```

For example:

```
[edit protocols lldp]
user@router# set ptopo-configuration-maximum-hold-time 2147483647
```

Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only out-of-band management addresses must be used as the value for the `management-address` statement.

To configure the management address:

```
[edit protocols lldp]
user@router# set management-address ip-address
```

NOTE: Ensure that the interface with the configured management address has LLDP enabled using the `set protocols lldp interface` command. If you configure a customized

management address for LLDP on an interface that has LLDP disabled, the `show lldp local-information` command output will not display the correct interface information.

Configuring Server Fail Fallback on MX Series Routers in Enhanced LAN Mode

Server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an *authenticator port access entity* (the router) to block all traffic to and from an end device at the interface until the end device's credentials are presented and matched on the *authentication server* (a RADIUS server). When the end device has been authenticated, the router stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the router, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the router and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the router does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. Server fail fallback allows you to configure authentication alternatives that permit the router to take appropriate actions toward end devices awaiting authentication or reauthentication.

NOTE: The authentication fallback method called *server-reject VLAN* provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

To configure basic server fail fallback options using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

```
[edit protocols authentication-access-control]
user@router# set interface ge-0/0/1 dot1x server-fail permit
```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

```
[edit protocols authentication-access-control]
user@router# set  interface ge-0/0/1 dot1x server-fail deny
```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs (in this case, the VLAN name is **vlan1**):

```
[edit protocols authentication-access-control]
user@router# set  interface ge-0/0/1 dot1x server-fail vlan-name
vlan1
```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

```
[edit protocols authentication-access-control]
user@router# set  interface ge-0/0/1 dot1x server-fail use-cache
```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the router (in this case, the VLAN name is **vlan-sf**):

```
[edit protocols authentication-access-control]
user@router# set  interface ge-0/0/1 dot1x server-reject-vlan vlan-sf
```

NOTE: If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

Understanding Captive Portal Authentication on the MX Series Routers

IN THIS SECTION

Captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on MX Series routers by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network.Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database using EAP-MD5, You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos Software for MX Series routers provides a template that allows you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time a client connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. Upon successful authentication, the user is allowed access to the network and to continue to the original page requested.

NOTE: If Hypertext Transfer Protocol Secure (HTTPS) is enabled, Hypertext Transfer Protocol (HTTP) requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the client is returned to the HTTP connection.

If there are clients that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC address to an authentication allowlist. (If the MAC address has already been learned on the interface, you must clear it using the **clear captive-portal interface** ***interface-name***) before adding it to the allowlist.)

When the user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Limitations of Captive Portal

Captive portal on MX Series routers has the following limitations:

- The captive portal interface must be configured for **family ethernet-switching** and set to port mode access. The VLAN must be configured with a *routed VLAN interface* (*RVI*).
- The DHCP gateway IP address for the switch must be configured as the IP address of the routed VLAN interface.
- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user is idle for more than about 5 minutes and there is no traffic passed, the user is required to log back in to the captive portal.

Understanding Authentication Session Timeout on MX Series Routers

You can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

For captive portal authentication, the length of the session depends on the value configured for the `session-expiry` statement. The remainder of this topic pertains only to 802.1X and MAC RADIUS authentication sessions.

For 802.1X and MAC RADIUS authentication sessions, the timeout of the session depends on the value of **reauthentication interval** for **dot1x authentication**. The authentication session might also end when the MAC table aging time expires because, unless you configure it not to, the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table.

Information about each 802.1X and MAC RADIUS authentication session—including the associated interfaces and VLANs for each MAC address that is authenticated by 802.1X authentication or MAC RADIUS authentication—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured **mac-table-aging-time** value, the switch removes the MAC address from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication database, with the result that the session ends.

You can control variables affecting timeout of authentication sessions in the following ways:

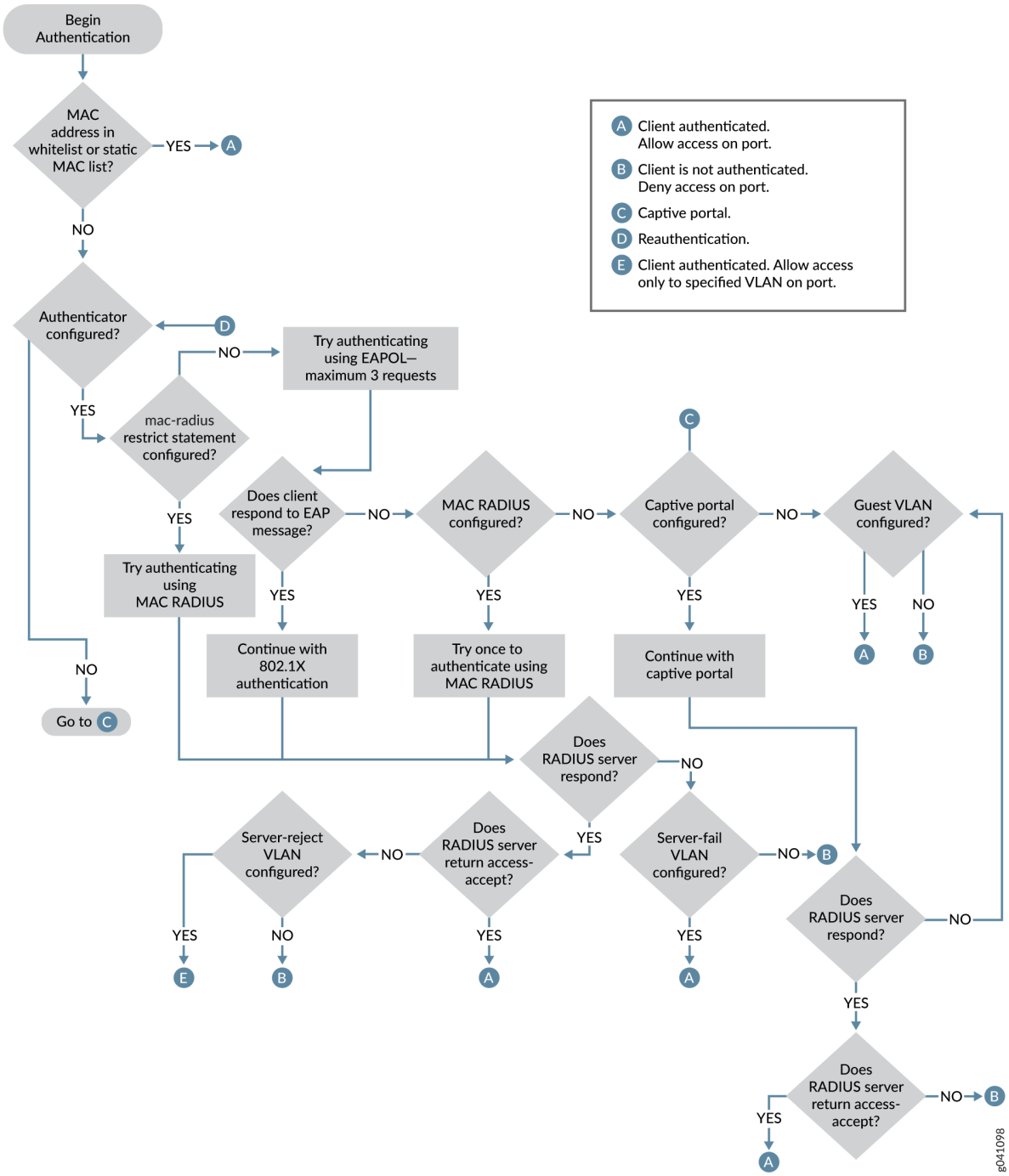
- Set the authentication session timeout on all interfaces or on selected interfaces using the `reauthentication` statement.
- Disassociate the authentication session table from the Ethernet switching table using the `no-mac-table-binding` statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.

Authentication Process Flow for MX Series Routers in Enhanced LAN Mode

You can control access to your network through an MX Series router by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

Figure 27 on page 653 illustrates the authentication process:

Figure 27: Authentication Process Flow for an MX Series Router



Specifying RADIUS Server Connections on an MX Series Router in Enhanced LAN Mode

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the *authentication server* (a RADIUS server). When the supplicant is authenticated, the router stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the router for each RADIUS server to which you will connect.

To configure a RADIUS server on the router:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the router must match the secret password on the server:

```
[edit access]
user@router# set radius-server 10.0.0.100 port 1812 secret abc
```

NOTE: Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the router is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the router.

```
[edit access]
user@router# set radius-server source-address 10.93.14.100
```

3. Configure the authentication order, making **radius** the first method of authentication:

```
[edit access]
user@router# set profile profile1 authentication-order radius
```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different sent of authentication servers.

```
[edit access profile]
user@router# set atlanta radius authentication-server 10.0.0.100 10.2.14.200
```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit access profile]
user@router# set protocols authentication-access-control authentication-profile-name denver
```

6. Configure the IP address of the MX Series router in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

Configuring Captive Portal Authentication on MX Series Routers in Enhanced LAN Mode

IN THIS SECTION

NOTE: This example uses Junos OS for MX Series routers with support for the Enhanced LAN mode configuration style. If your router does not run MX-LAN mode, you cannot configure port-based authentication settings in the same manner as described in this section. If you remove the network-services lan statement at the [edit chassis] hierarchy level, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. In such a scenario, you must use the statements at the `[edit protocols`

dot1x] hierarchy level to configure 802.1x and MAC RADIUS authentication, and the options at the [edit services captive-portal] hierarchy level to configure captive portal authentication. In MX-LAN mode, you can configure all the port-based network access control methodologies using the statements at the [edit protocols authentication-access-control] hierarchy level.

Configure captive portal authentication (hereafter referred to as captive portal) on an MX Series router so that users connected to the router are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the router:

```
[edit]
user@router# set system services web-management https local-certificate my-signed-cert
```

NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@router# set protocols custom-options-captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@router# set authentication-access-control interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@router# set authentication-access-control static 00:10:12:e0:28:22
```

NOTE: Optionally, you can use `set authentication-access-control static 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

NOTE: If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address` *`session-mac-addr`* command after adding its MAC address to the allowlist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Designing a Captive Portal Authentication Login Page on an MX Series Router

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access.Upon successful authentication, the user is allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the “Terms and Conditions of Use”. By clicking the Agree button, the user can access the captive portal login page.

Figure 28 on page 658 shows an example of a captive portal login page:

Figure 28: Example of a Captive Portal Login Page

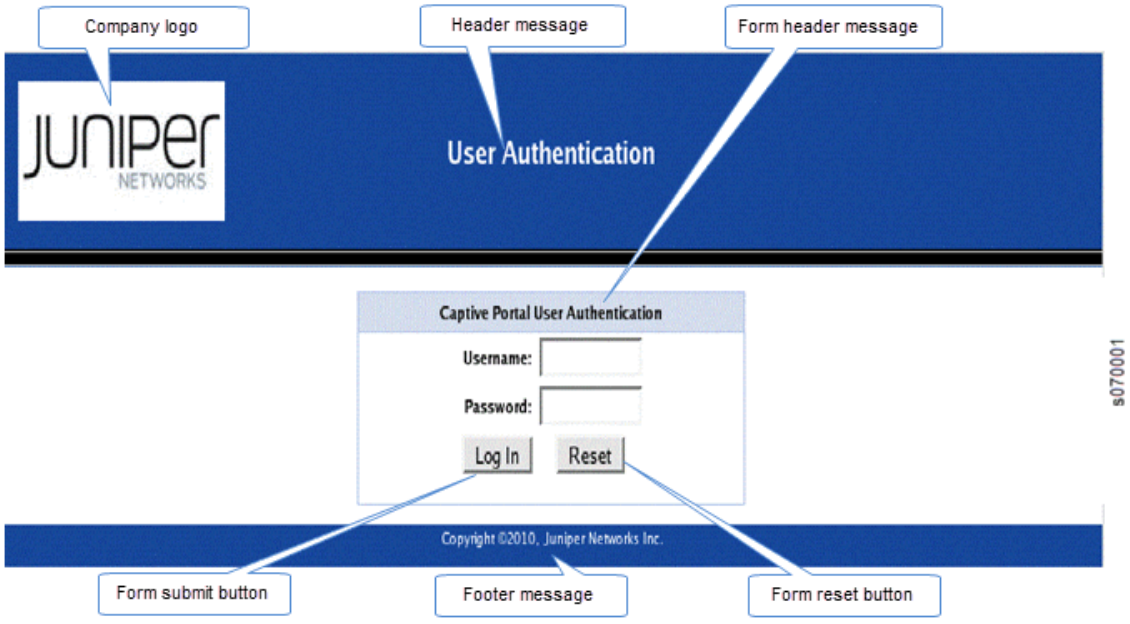


Table 38 on page 659 summarizes the configurable elements of a captive portal login page.

Table 38: Configurable Elements of a Captive Portal Login Page

Element	CLI Statement	Description
Footer background color	**footer-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the captive portal login page footer.
Footer message	**footer-message** *text-string*	Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy The default text shown in the footer is **Copyright @2010, Juniper Networks Inc.**
Footer text color	**footer- text-color** *color*	Color of the text in the footer. The default color is white.
Form header background color	**form-header-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.
Form header message	**form-header-message** *text-string*	Text displayed in the header of the captive portal login page. The default text is **Captive Portal User Authentication**
Form header text color	**form-header- text-color** *color*	Color of the text in the form header. The default color is black.
Form reset button label	**form-reset-label** *label-name*	Using the **Reset** button, the user can clear the username and password fields on the form.
Form submit button label	**form-submit-label** *label-name*	Using the **Login** button, the user can submit the login information.
Header background color	**header-bgcolor** *hex-color*	The HTML hexadecimal code for the background color of the captive portal login page header.

Table 38: Configurable Elements of a Captive Portal Login Page *(Continued)*

Element	CLI Statement	Description
Header logo	**header-logo** ***filename***	Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.
Header message	**header-message** ***text-string***	Text displayed in the page header. The default text is **User Authentication**.
Header text color	**header-text-color***color*	Color of the text in the header. The default color is white.
Post-authentication URL	**post-authentication-url** ***url***	URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

```
user@router> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

```
[edit protocols]
user@router# set captive-portal-custom-options header-bgcolor #006600
set captive-portal-custom-options header-message “Welcome to Our Network”
set captive-portal-custom-options banner-message “Please enter your username and
password”.The banner displays the message ”XXXXXXX” by default. The user can modify this
message.
set custom-options footer-message “Copyright ©2010, Our Network”
```

Now you can commit the configuration.

NOTE: For the custom options that you do not specify, the default value is used.

Configuring Static MAC Bypass of Authentication on MX Series Routers in Enhanced LAN Mode

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe
```

- Configure a supplicant to bypass authentication if connected through a particular interface:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5
```

- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

```
[edit protocols authentication-access-control]
user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment default-vlan
```

Controlling Authentication Session Timeouts on an MX Series Router in Enhanced LAN Mode

For 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the `reauthentication` statement.

The session might also end when the MAC table aging time expires, because the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table. In order to prevent the session from being removed from the authentication session table, you must disassociate the authentication table from the Ethernet switching table using the `no-mac-table-binding` statement.

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server.
- Configure 802.1X authentication on the router.

To configure the authentication session time on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control interface all dot1x reauthentication
seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@router# set protocols authentication-access-control interface interface-name dot1x
reauthentication seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface all;
```

To remove the binding on a single interface:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface
interface-name;
```

Configuring MAC RADIUS Authentication on MX Series Routers in Enhanced LAN Mode

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the MX Series router interfaces to which the hosts are connected.

NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the router first sends the host three EAPOL requests to the host. If there is no response from the host, the router sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the router that the MAC address is a permitted address, and the router opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the **mac-radius restrict** option), the router attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the MX Series router and the RADIUS server.
- Configured MX Series routers to function in enhanced LAN mode by entering the `network-services lan` statement at the `[edit chassis]` hierarchy level.

To configure MAC RADIUS authentication using the CLI:

- On the router, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the **restrict** qualifier for interface **ge-0/0/20** to have it use only MAC RADIUS authentication:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius
user@router# set protocols authentication-access-control interface ge-0/0/20 dot1x mac-radius
restrict
```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f**):

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
 0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

Example: Configuring MAC RADIUS Authentication on an MX Series Router

IN THIS SECTION

To permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the router interfaces to which the non-802.1X-enabled hosts are connected. When

MAC RADIUS authentication is configured, the router will attempt to authenticate the host with the RADIUS server using the host's MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

Requirements

This example uses the following hardware and software components:

- MX Series routers running in enhanced LAN mode.
- An MX Series router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

IN THIS SECTION

IEEE 802.1X Port-Based Network Access Control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the router using the 802.1X protocol (are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the

end device appears on the interface, the router consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the router opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is only connected to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication using the **mac-radius restrict** option, and thus avoid the delay that occurs while the router determines that the device is does not respond to EAP messages.

Two printers are connected to an MX Series router over interfaces, ge-0/0/19 and ge-0/0/20.

Table 39 on page 666 shows the components in the example for MAC RADIUS authentication.

Table 39: Components of the MAC RADIUS Authentication Configuration Topology

Property	Settings
Router hardware	Ports (ge-0/0/0 through ge-0/0/23)
VLAN name	sales
Connections to printers	ge-0/0/19, MAC address 00040ffdacfe ge-0/0/20, MAC address 0004aecd235f
RADIUS server	Connected to the router on interface **ge-0/0/10**

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the router, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the router attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the `mac radius restrict` option.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
  set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius

  set protocols authentication-access-control authenticator interface ge-0/0/20 dot1x mac-radius
restrict
```

NOTE: You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

Step-by-Step Procedure

Configure MAC RADIUS authentication on the router and on the RADIUS server:

1. On the router, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the **restrict** option on interface **ge-0/0/20**, so that only MAC RADIUS authentication is used:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius

  user@router# set protocols authentication-access-control authenticator interface ge-0/0/20
```

```
dot1x mac-radius restrict
```

2. On the RADIUS server, configure the MAC addresses **00040ffdacfe** and **0004aecd235f** as usernames and passwords:

```
[root@freeradius]#
                            edit /etc/raddb
                            vi users
                            00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
                            0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
```

Results

Display the results of the configuration on the router:

```
user@router> show configuration
protocols {
    authentication-access-control {
        authentication-profile-name profile52;
        interface {
            ge-0/0/19.0 {
                dot1x {
                    mac-radius;
                }
            }
            ge-0/0/20.0 {
                dot1x {
                    mac-radius {
                        restrict;
                    }
                }
            }
        }
    }
}
```

Verification

IN THIS SECTION

Verify that the supplicants are authenticated:

Verifying That the Supplicants Are Authenticated

Purpose

After supplicants are configured for MAC RADIUS authentication on the router and on the RADIUS server, verify that they are authenticated and display the method of authentication:

Action

Display information about 802.1X-configured interfaces **ge-0/0/19** and **ge-0/0/20**:

```
user@router> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
```

```
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds

user@router> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Enabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user102, 00:04:ae:cd:23:5f
      Operational state: Authenticated
      Authentcation method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The sample output from the `show dot1x interface detail` command displays the MAC address of the connected end device in the **Supplicant** field. On interface ge-0/0/19, the MAC address is **00:04:0f:fd:ac:fe**, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**. On interface **ge-0/0/20**, the MAC address is **00:04:ae:cd:23:5f**, which is the MAC address of the second printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**.

Example: Setting Up Captive Portal Authentication on an MX Series Router

IN THIS SECTION

You can set up captive portal authentication (hereafter referred to as captive portal) on a router to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an MX Series router:

Requirements

This example uses the following hardware and software components:

- An MX Series router that supports captive portal

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page. .

Overview and Topology

IN THIS SECTION

This example shows the configuration required on the router to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication allowlist. The MAC addresses in this list are permitted access on the interface without captive portal.

Topology

The topology for this example consists of one MX Series router connected to a RADIUS authentication server. One interface on the router is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

Configuration

IN THIS SECTION

To configure captive portal on your router:

CLI Quick Configuration

To quickly configure captive portal on the router after completing the tasks in the Requirements section, copy the following commands and paste them into the router terminal window:

```
[edit]
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set protocols captive-portal-custom-options secure-authentication https
set protocols authentication-access-control interface ge-0/0/10.0 supplicant multiple
set protocols authentication-access-control static 00:10:12:e0:28:22
set protocols captive-portal-custom-options post-authentication-url http://www.my-home-page.com
```

Procedure

Step-by-Step Procedure

To configure captive portal on the router:

1. Enable HTTP access on the router:

```
[edit]
user@router# set system services web-management http
```

2. To create a secure channel for Web access to the router, configure captive portal for HTTPS:

NOTE: You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

Step-by-Step Procedure

a. Associate the security certificate with the Web server and enable HTTPS access on the router:

```
[edit]
user@router# set system services web-management https local-certificate my-signed-cert
```

b. Configure captive portal to use HTTPS:

```
[edit]
user@router# set protocols captive-portal-custom-options secure-authentication https
```

3. Enable an interface for captive portal:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/10.0 supplicant
multiple
```

4. (Optional) Allow specific clients to bypass captive portal:

> **NOTE**: If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address` *mac-address* command after adding its MAC address to the allowlist. Otherwise the new entry for the MAC address will not be added to the Ethernet routering table and authentication bypass will not be allowed.

```
[edit]
user@router# set protocols authentication-access-control static 00:10:12:e0:28:22
```

> **NOTE**: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

5. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@router# set protocols captive-portal-custom-options post-authentication-url http://
www.my-home-page.com
```

Results

Display the results of the configuration:

```
[edit]
user@router> show
system {
    services {
        web-management {
            http;
            https {
                local-certificate my-signed-cert;
            }
        }
    }
}
security {
    certificates {
        local {
            my-signed-cert {
                "-----BEGIN RSA PRIVATE KEY-----\nMIICXwIBAAKBgQDk8sUggnXdDUmr7T vLv63yJq/
LRpDASfIDZlX3z9ZDe1Kfk5C9\nr/tkyvzv
 ...
Pt5YmvWDoGo0mSjoE/liH0BqYdh9YGqv3T2IEUfflSTQQHEOShS0ogWDHF\ nnyOb1O/vQtjk20X9NVQg JHBwidssY9eRp
\n-----END CERTIFICATE-----\n"; ## SECRET-DATA
            }
        }
    }
}
protocols {
    authentication-access-control {
    static 00:10:12:e0:28:22/48;
        interface {
            ge-0/0/10.0 {
                supplicant multiple;
            }
        }
    custom-captive-portal-options {
        secure-authentication https;
        post-authentication-url http://www.my-home-page.com;
```

```
    }
}
```

Verification

IN THIS SECTION

To confirm that captive portal is configured and working properly, perform these tasks:

Verifying That Captive Portal Is Enabled on the Interface

Purpose

Verify that captive portal is configured on interface ge-0/0/10.

Action

Use the operational mode command `show captive-portal interface` *`interface-name`* `detail`:

```
user@router> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning

The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose

Verify that captive portal is working on the router.

Action

Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

IN THIS SECTION

To troubleshoot captive portal, perform these tasks:

Troubleshooting Captive Portal

Problem

The router does not return the captive portal login page when a user connected to a captive portal interface on the router requests a Web page.

Solution

You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get

an IP address, check the router interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the router.

```
user@router> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                          Bytes              Packets
dot1x_ge-0/0/10_CP_arp         7616                  119
dot1x_ge-0/0/10_CP_dhcp           0                    0
dot1x_ge-0/0/10_CP_http           0                    0
dot1x_ge-0/0/10_CP_https          0                    0
dot1x_ge-0/0/10_CP_t_dns          0                    0
dot1x_ge-0/0/10_CP_u_dns          0                    0
```

Example: Connecting a RADIUS Server for 802.1X to an MX Series Router

IN THIS SECTION

802.1X is the IEEE standard for Port-Based Network Access Control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an MX Series router, and configure it for 802.1X:

Requirements

This example uses the following hardware and software components:

- MX Series routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 40: Components of the Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**

Table 40: Components of the Topology *(Continued)*

Property	Settings
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, connect the RADIUS server to access port **ge-0/0/10** on the MX Series router. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the MX Series router and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
 set access profile profile1 authentication-order radius
 set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:

```
[edit]
user@switch# set access radius-server 10.0.0.100 secret juniper
user@switch# set access radius-server 10.0.0.200 secret juniper
```

2. Configure the authentication order, making **radius** the first method of authentication:

```
[edit]
user@switch# set access profile profile1 authentication-order radius
```

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:

```
[edit]
user@switch# set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Results

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {

    10.0.0.100
        port 1812;

        secret "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
        }
    }
    profile profile1{
        authentication-order radius;
        radius {

            authentication-server 10.0.0.100 10.0.0.200;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verify That the Switch and RADIUS Server are Properly Connected

Purpose

Verify that the RADIUS server is connected to the switch on the specified port.

Action

Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning

ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether it is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an MX Series Router

IN THIS SECTION

802.1X on MX Series routers provides LAN access to users who do not have credentials in the RADIUS database.These users, referred to as guests, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

Requirements

This example uses the following hardware and software components:

- MX Series routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.

- Configured users on the RADIUS authentication server.

Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 41: Components of the Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**
One RADIUS server	Backend database with an address of **10.0.0.100** connected to the switch at port **ge-0/0/10**

In this example, access interface **ge-0/0/1** provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

IN THIS SECTION

Procedure

CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans bridge-domain-name vlan-id 300
 set protocols dot1x authenticator interface all guest-bridge-domain bridge-domain-name
```

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on MX Series routers:

1. Configure the VLAN ID for the guest VLAN:

```
[edit]
user@switch# set bridge-domains bridge-domain-name vlan-id 300
```

2. Configure the guest VLAN under dot1x protocols:

```
[edit]
user@switch# set protocols dot1x authenticator interface all guest-bridge-domain bridge-
domain-name
```

Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
    dot1x {
        authenticator {
        interface {
            all {
                    guest-bridge-domain {
                        bridge-domain-name;
```

```
                    }
                }
            }
        }
        }
    }
}
bridge-domains {
    bridge-domain-name {
        vlan-id 300;
    }
}
```

Verification

IN THIS SECTION

- Verifying That the Guest VLAN is Configured | 686

To confirm that the configuration is working properly, perform these tasks:

Verifying That the Guest VLAN is Configured

Purpose

Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.

Action

Use the operational mode commands:

```
user@switch> show bridge-domain

Instance                  Bridging Domain          Type
```

```
            Primary Table                                           Active
vs1                         dynamic                 bridge
            bridge.0                                                2
vs1                         guest                   bridge
            bridge.0                                                0
vs1                         guest-vlan              bridge
            bridge.0                                                0
vs1                         vlan_dyn                bridge
            bridge.0                                                0


user@switch> show dot1x interface ge-0/0/1.0 detail
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
  Number of connected supplicants: 1
    Supplicant: user1, 00:00:00:00:13:23
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning

The output from the `show bridge domain` command shows bridge-domain-name as the name of the VLAN and the VLAN ID as **300**.

The output from the `show dot1x interface ge-0/0/1.0 detail` command displays the bridge domain name , indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the bridge-domain-name.

Example: Configuring Static MAC Bypass of Authentication on an MX Series Router

IN THIS SECTION

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the MX Series router.The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the router without a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

Requirements

This example uses the following hardware and software components:

- MX Series routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

Overview and Topology

IN THIS SECTION

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

The interfaces shown in Table 42 on page 689 will be configured for static MAC authentication.

Table 42: Components of the Static MAC Authentication Configuration Topology

Property	Settings
Router hardware	MX Series router
VLAN name	**default**
Connections to integrated printer/fax/copier machines (no PoE required)	**ge-0/0/19**, MAC address 00:04:0f:fd:ac:fe **ge-0/0/20**, MAC address 00:04:ae:cd:23:5f

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface **ge-0/0/19**. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface **ge-0/0/20**. Both printers will be added to the static list and bypass 802.1X authentication.

Topology

Configuration

IN THIS SECTION

- Procedure | 690

Procedure

CLI Quick Configuration

To quickly configure static MAC authentication, copy the following commands and paste them into the router terminal window:

```
[edit]

set protocols authentication-access-control static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols authentication-access-control interface all supplicant multiple
set protocols authentication-access-control authenticaton-profile-name profile1
```

Step-by-Step Procedure

Configure static MAC authentication:

1. Configure MAC addresses **00:04:0f:fd:ac:fe** and **00:04:ae:cd:23:5f** as static MAC addresses:

```
[edit protocols]
user@router# set authentication-access-control static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
```

2. Configure the 802.1X authentication method:

```
[edit protocols]
user@router# set authentication-access-control interface all supplicant multiple
```

3. Configure the authentication profile name (access profile name) to use for authentication:

```
[edit protocols]
user@router# set authentication-access-control authentication-profile-name profile1
```

NOTE: Access profile configuration is required only for 802.1X clients, not for static MAC clients.

Results

Display the results of the configuration:

```
user@router> show
interfaces {
    ge-0/0/19 {
        unit 0 {
            family bridge {
                vlan-id 10;
            }
        }
    }
    ge-0/0/20 {
        unit 0 {
            family bridge {
                vlan-id 10;
            }
        }
    }
}
protocols {
    authentication-access-control {
        authentication-profile-name profile1;
        static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
```

```
        interface {
            all {
                supplicant multiple;
            }
        }
    }
}
```

Verification

IN THIS SECTION

- Verifying Static MAC Bypass of Authentication | **692**

To confirm that the configuration is working properly, perform these tasks:

Verifying Static MAC Bypass of Authentication

Purpose

Verify that the MAC address for both printers is configured and associated with the correct interfaces.

Action

Use the operational mode command:

```
user@switch> show dot1x static-mac-address

MAC address          VLAN-Assignment          Interface
00:04:0f:fd:ac:fe    default                  ge-0/0/19.0
00:04:ae:cd:23:5f    default                  ge-0/0/20.0
```

Meaning

The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on MX Series Routers

IN THIS SECTION

Firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server.The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following hardware and software components:

- One MX Series router
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the router and the RADIUS server.
- Configured 802.1X authentication on the router, with the authentication mode for interface **ge-0/0/2** set to **multiple**.
- Configured users on the RADIUS authentication server.

Overview and Topology

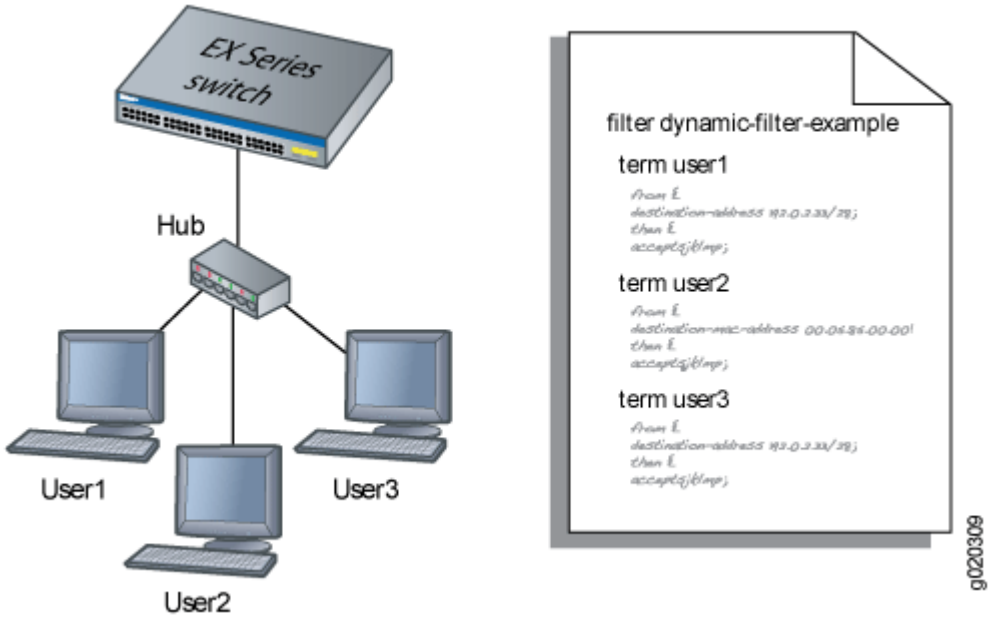
IN THIS SECTION

Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the router from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 29 on page 695, when User1 is authenticated by the MX Series router, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 29: Conceptual Model: Dynamic Filter Updated for Each New User

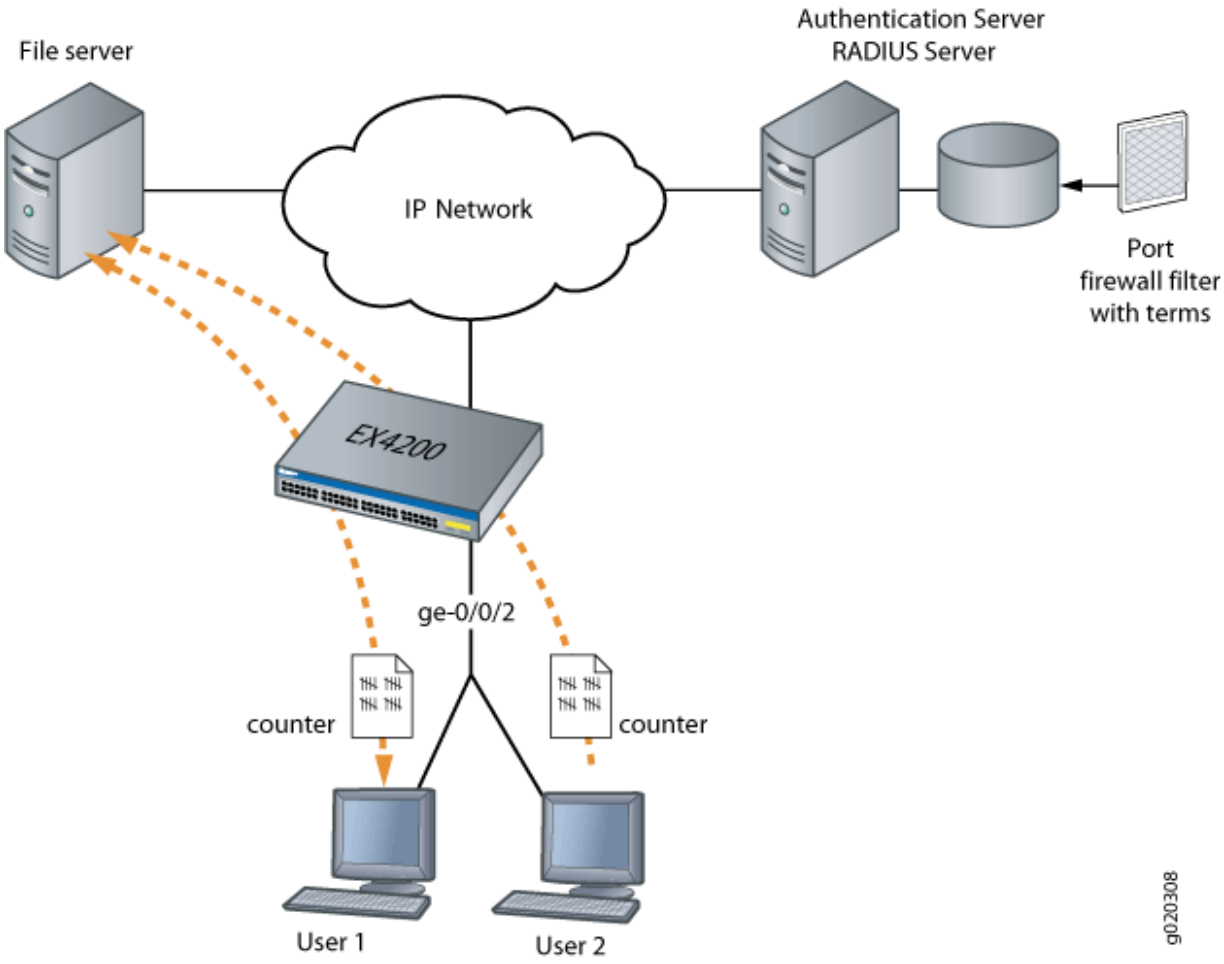


This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. Figure 30 on page 696 shows the network topology for this example.

Figure 30: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



Configuration

IN THIS SECTION

- Configuring Firewall Filters on Interfaces with Multiple Supplicants | **697**

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the router terminal window:

```
[edit]
                        set protocols authentication-access-control interface ge-0/0/2
supplicant multiple
                        set firewall family bridge filter filter1 term term1 from destination-
address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
                        set firewall family bridge filter filter1 term term1 then count
counter1
set firewall family bridge filter filter1 term term2 then policer p1
```

Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:

```
[edit protocols]
user@router# set authentication-access-control interface ge-0/0/2 supplicant
multiple
```

2. Set policer definition:

```
user@router# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family bridge]
user@router# set filter filter1 term term1 from destination-address 192.0.2.16/28
user@router# set filter filter1 term term1 then count counter1
user@router# set filter filter1 term term2 then policer p1
```

Results

Check the results of the configuration:

```
user@router> show configuration

firewall {
    family bridge {
        filter filter1 {
            term term1 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
                term term2 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
                burst-size-limit 1k;
            }
            then discard;
```

```
        }
}
protocols {
    authentication-access-control {
        interface ge-0/0/2 {
            supplicant multiple;
        }
    }
```

Verification

IN THIS SECTION

- Verifying Firewall Filters on Interfaces with Multiple Supplicants | 699

To confirm that the configuration is working properly, perform these tasks:

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose

Verify that firewall filters are functioning on the interface with multiple supplicants.

Action

1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on **ge-0/0/2**:

```
user@router> show dot1x firewall

Filter: dot1x_ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
```

2. When a second user, User2, is authenticated on the same interface, **ge-0/0/2**, you can verify that the filter includes the results for both of the users authenticated on the interface:

```
user@router>  show dot1x firewall

Filter: dot1x-filter-ge-0/0/0
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter1_dot1x_ge-0/0/2_user2 400
```

Meaning

The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

10
CHAPTER

Device Discovery

IN THIS CHAPTER

Device Discovery Using LLDP

IN THIS SECTION

The Link Layer Discovery Protocol (LLDP) is an industry-standard, vendor-neutral method to allow networked devices to advertise capabilities, identity, and other information onto a LAN. It also provides additional types, lengths, and values (TLVs) for capabilities discovery, network policy, Power over Ethernet (PoE), and inventory management. For more information, read this topic.

Understanding LLDP

The device uses LLDP to learn and to distribute device information on network links. The device uses this information to identify a variety of devices quickly. This quick identification results in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include specifics, such as the chassis identification, the port identification, the system name, and the system capabilities. The TLVs leverage this information from parameters that have already been configured in Junos OS.

The device supports the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—The user-configured port description. The port description can be a maximum of 256 characters.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.

- **System Description**—The system description containing information about the software and current image running on the system. This information is taken from the software. You cannot configure this information.
- **System Capabilities**—The primary function performed by the system, for example, bridge or router. This information cannot be configured, but is based on the model of the product.
- **Management Address**—The IP management address of the local system.

The device supports the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises media dependent interface (MDI) power support, power source equipment (PSE) power pair, and power class information.
- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure. You cannot configure this information.
- **Link Aggregation**—A TLV that advertises whether the port is aggregated and its aggregated port ID.
- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.
- **Port VLAN**—A TLV that advertises the VLAN name configured on the interface.

Configuring LLDP (CLI Procedure)

IN THIS SECTION

Follow these steps to configure LLDP on your device.

Enable LLDP on Interfaces

LLDP is enabled on all interfaces by default. If you disable it, you can re-enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

```
[edit protocols lldp]
user@device# set interface all
```

- To configure LLDP on a specific interface:

```
[edit protocols lldp]
user@device# set interface interface-name
```

Adjust LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. LLDP uses the default values when it is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

```
[edit protocols lldp]
user@device# set advertisement-interval seconds
```

  For example, using the default value of 30 seconds:

```
[edit protocols lldp]
user@device# set advertisement-interval 30
```

- To specify the number of seconds that LLDP information is held before it is discarded:

```
[edit protocols lldp]
user@device# set hold-multiplier number
```

For example, using the default value of 4:

```
[edit protocols lldp]
user@device# set hold-multiplier 4
```

The `hold-multiplier` value is used in combination with the `advertisement-interval` value. Using the default values means that the `advertisement-interval` value of 30 will be multiplied by the `hold-multiplier` value of 4. resulting in a LLDP hold time of 120 seconds.

- Set the transmit delay to specify the number of seconds the device waits before sending advertisements to neighbors after a change is made in a TLV (element in LLDP or in the state of the local system). A change in state of the local system includes a change in hostname or management address. The transmit delay is enabled by default to reduce the delay in notifying neighbors of a change in the local system. The default transmit delay is 1 second if the `advertisement-interval` value is set to less than 8 seconds. The default value is 2 seconds if the `advertisement-interval` value is set to 8 seconds or more.

```
[edit protocols lldp]
user@device# set transmit-delay seconds
```

For example:

```
[edit protocols lldp]
user@device# set transmit-delay 2
```

NOTE: The `advertisement-interval` value must be greater than or equal to four times the transmit-delay value; otherwise, an error is returned when you attempt to commit the configuration.

Adjust SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to 0, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

```
[edit protocols lldp]
user@device# set lldp-configuration-notification-interval seconds
```

For example:

```
[edit protocols lldp]
user@device# set lldp-configuration-notification-interval 600
```

- To configure how long SNMP trap notifications wait for topology changes (in seconds):

```
[edit protocols lldp]
user@device# set ptopo-configuration-trap-interval seconds
```

For example:

```
[edit protocols lldp]
user@device# set ptopo-configuration-trap-interval 600
```

- To specify the holding time (used in combination with the `ptopo-configuration-trap-interval` value) to maintain dynamic topology entries (in seconds):

```
[edit protocols lldp]
user@device# set ptopo-configuration-maximum-hold-time seconds
```

For example:

```
[edit protocols lldp]
user@device# set ptopo-configuration-maximum-hold-time 2147483647
```

Specify a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address TLV messages. An out-of-band management address must be used as the value for the `management-address` statement.

To configure the management address:

```
[edit protocols lldp]
user@device# set management-address ip-address
```

NOTE: Ensure that the interface with the configured management address has LLDP enabled using the `set protocols lldp interface` command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the `show lldp local-information` command output does not display the correct interface information.

Specify a Management Interface for the LLDP Management TLV

you can configure an interface to be used in the LLDP Management Address TLV messages.

NOTE: You cannot configure management address and management interface at the same time.

To configure the management interface:

```
[edit protocols lldp]
user@device# set management-interface interface-name
```

If the interface does not have an IP address, the IP address of the default management interfaces is used.

Configure LLDP Power Negotiation

LLDP power negotiation enables the device's Power over Ethernet (PoE) controller to dynamically allocate PoE power to PoE interfaces, based on the needs of the powered device, by negotiating with LLDP-enabled powered devices.

NOTE: LLDP power negotiation is not supported on EX3200 or EX4200 switches (except for the EX4200-PX models).

LLDP power negotiation is supported on devices running PoE controller software version 4.04 or later.

LLDP power negotiation is automatically enabled when the PoE management mode is set to `class`:

- ```
  [edit poe]
  user@device# set management class
  ```

To disable LLDP power negotiation:
  ```

- On all device interfaces:

```
[edit protocols lldp interface all power-negotiation]
user@device# set disable
```

- On a specific interface:

```
[edit protocols lldp interface interface-name power-negotiation]
user@device# set disable
```

Disable LLDP TLVs

LLDP sends TLV messages by default. You can configure LLDP to disable non-mandatory TLVs. The mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- `tlv-select`—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
- `tlv-filter`—Filter the TLVs that should not be advertised by LLDP. Use this option if you want to filter only a few TLVs and allow everything else.

NOTE: The `tlv-select` and `tlv-filter` options are mutually exclusive and cannot be used on the same configuration stanza at the same time.

You can disable TLVs on specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over the global configuration.

To select which TLVs are allowed to be advertised by LLDP:

- On all interfaces:

```
[edit protocols lldp]
user@device# set tlv-select tlv-name
```

- On a specific interface:

```
[edit protocols lldp]
user@device# set interface interface-name tlv-select tlv-name
```

To filter TLVs that should not be advertised by LLDP:

- On all interfaces:

```
[edit protocols lldp]
user@device# set tlv-filter tlv-name
```

- On a specific interface:

```
[edit protocols lldp]
user@device# set interface interface-name tlv-filter tlv-name
```

The following example disables all TLVs except port-description:

```
[edit protocols lldp]
user@device# set tlv-select port-description
```

The following example disables the system-description TLV on the ge-2/1/1 interface:

```
[edit protocols lldp]
user@device# set interface ge-2/1/1 tlv-filter system-description
```

The following example disables all TLVs except port-description and system-description on all interfaces except on the ge-0/0/1 interface, where it disables only the system-name TLV:

```
[edit protocols lldp]
user@device# set tlv-select [port-description system-description]
user@device# set interface ge-0/0/1 tlv-filter system-name
```

Configuring LLDP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Use the LLDP Configuration page to configure LLDP global and port settings for an EX Series switch on the J-Web interface.

To configure LLDP:

1. Select **Configure** > **Switching** > **LLDP**.

   The LLDP Configuration page displays LLDP Global Settings and Port Settings.

   The second half of the screen displays operational details for the selected port.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options** > **Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. For an EX8200 Virtual Chassis configuration, select the member and the slot (FPC) from the list.
3. To modify LLDP Global Settings, click **Global Settings**.

   Enter information as described in Table 43 on page 710.
4. To modify Port Settings, click **Edit** in the Port Settings section.

   Enter information as described in Table 44 on page 711.

Table 43: Global Settings

Field	Function	Your Action
Advertising interval	Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.	Type the number of seconds.
Hold multiplier	Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.	Type the required number in the field.

Table 43: Global Settings *(Continued)*

Field	Function	Your Action
Fast start count	Specifies the number of LLDP advertisements sent in the first second after the device connects. The default is 3. Increasing this number results in the port initially advertising LLDP–MED at a faster rate for a limited time.	Type the Fast start count.

Table 44: Edit Port Settings

Field	Function	Your Action
LLDP Status	Specifies whether LLDP has been enabled on the port.	Select one: **Enabled**, **Disabled**, or **None**.
LLDP-MED Status	Specifies whether LLDP–MED has been enabled on the port.	Select **Enable** from the list.

Understanding LLDP and LLDP-MED on EX Series Switches

IN THIS SECTION

EX Series Ethernet Switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

Benefits of LLDP and LLDP-MED

- Enables the switch to quickly identify a variety of devices.
- Provides PoE power management capabilities.
- Ensures that voice traffic gets tagged and prioritized with the correct values at the source itself.

LLDP and LLDP-MED Overview

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone.

NOTE: If your IP telephone is configured for VoIP (VoIP), the switch automatically detects the configuration and assigns the telephone to the voice VLAN. The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the switch to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the switch interface to which it connects.

The switch also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

Supported LLDP TLVs

EX Series switches and QFX5100 switches support the following basic management TLVs:

- Chassis ID—The MAC address associated with the local system.

> **NOTE**: The Chassis ID TLV has a subtype for the network address family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the `show lldp neighbors` command, but is not assigned to the VLAN.

- Port ID—The port identification for the specified port in the local system.
- Time to Live—The length of time that the received information should remain valid.
- Port Description—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV contains the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit; therefore, only the description configured on the physical interface can be used.
- System Name—The user-configured name of the local system. The system name can be a maximum of 256 characters. The system name field contains the host name and the domain name in the following format: *host-name.domain-name.*
- System Description—The system description that contains information about the software and current image running on the system. This information is not configurable, but taken from the software.
- System Capabilities—The primary function performed by the system. The capabilities that the system supports—for example, bridge or router. This information is not configurable, but based on the model of the product.
- Management Address—The IPv4 or IPv6 management address of the local system.

EX Series switches and QFX5100 switches support the following organizationally defined TLVs:

- Power via MDI—A TLV that advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.
- MAC/PHY Configuration Status—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type. The information is not configurable, but based on the physical interface structure.

> **NOTE**: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field contains a value of `other` or `unknown` if the LLDP packet is transmitted from a 10-gigabit SFP+ port.

- Link Aggregation—A TLV that advertises whether the port is aggregated and its aggregated port ID.

- Maximum Frame Size—A TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.
- Port Vlan—A TLV that advertises the VLAN name configured on the interface.

Supported LLDP-MED TLVs

EX Series switches and QFX5100 switches support the following LLDP-MED TLVs:

- LLDP-MED Capabilities—A TLV that advertises the primary function of the port. The values of capabilities range from 0 through 15:
  - 0—Capabilities
  - 1—Network Policy
  - 2—Location Identification
  - 3—Extended Power via MDI-PSE
  - 4—Inventory
  - 5-15—Reserved
- LLDP-MED Device Class Values—Categorizes media endpoint devices into classes:
  - 0—Class not defined
  - 1—Class 1 (generic endpoints). This class definition is applicable to all endpoints that require the base LLDP discovery services.
  - 2—Class 2 (media endpoints). This class includes endpoints that have IP media capabilities.
  - 3—Class 3 (communication endpoints). Devices acting as end user communication applicances
  - 4—Network Connectivity Device
  - 5-255—Reserved
- Network Policy—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
- Endpoint Location— A TLV that advertises the physical location of the endpoint.
- Extended Power via MDI— A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

Disabling TLVs

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live. All other TLVs can be disabled, either on specific interfaces or on a global basis. See "Configuring LLDP (CLI Procedure)" on page 703 and "Configuring LLDP-MED (CLI Procedure)" on page 715 for more information.

SEE ALSO

Understanding PoE on EX Series Switches

Configuring LLDP-MED (CLI Procedure)

IN THIS SECTION

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The EX Series switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is enabled by default on EX Series switches.

This topic describes:

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

NOTE: On switches running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, configure LLDP-MED on the physical interface–for example, on ge-0/0/2. For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name
```

Configuring Location Information Advertised by the Switch

You can configure the location information that is advertised from the switch to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

```
[edit protocols lldp-med]

user@switch# set interface ge-0/0/2.0 location civic-based country-code country-
code
user@switch# set interface ge-0/0/2.0 location civic-based ca-type ca-type ca-value ca-
value
```

- To specify a location by using an `elin` string:

```
[edit protocols lldp-med]

user@switch# set interface ge-0/0/2.0 location elin 4085551212
```

Configuring a Fast Start for LLDP-MED

When the switch detects an LLDP-MED capable device, it begins to send LLDP advertisements from the port connected to the device. The fast start count indicates how many advertisements will be send in

the first second after the switch detects the LLDP-MED device. The default is 3; to set it to another value:

```
[edit protocols lldp-med]
user@switch# set fast-start seconds
```

For example:

```
[edit protocols lldp-med]
user@switch# set fast-start 6
```

NOTE: If an interface is configured as a VoIP interface, then the switch does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Disabling LLDP-MED TLVs

LLDP-MED sends TLV messages by default. You can configure LLDP-MED to disable non-mandatory TLVs. Mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- `tlv-select`—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
- `tlv-filter`—Filter the TLVs that should not be advertised by LLDP. This approach is useful if you want to filter only few TLVs, and allow everything else.

NOTE: The `tlv-select` and `tlv-filter` are mutually exclusive and cannot be used on the same configuration stanza at the same time.

You can disable TLVs on a specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over global the global configuration.

To select which TLVs are allowed to be advertised by LLDP-MED:

- On all interfaces:

```
[edit protocols lldp-med]
user@switch# set tlv-select tlv-name
```

- On a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name tlv-select tlv-name
```

To filter TLVs that should not be advertised by LLDP-MED:

- On all interfaces:

```
[edit protocols lldp-med]
user@switch# set tlv-filter tlv-name
```

- On a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface interface-name tlv-filter tlv-name
```

The following example disables all TLVs except location-id:

```
[edit protocols lldp-med]
user@switch# set tlv-select location-id
```

The following example disables the ext-power-via-mdi TLV on ge-2/1/1 interface:

```
[edit protocols lldp-med]
user@switch# set interface ge-2/1/1 tlv-filter ext-power-via-mdi
```

The following example disables all TLVs except location-id and ext-power-via-mdi on all interfaces except on the ge-0/0/1 interface, where it disables only the network-policy TLV:

```
[edit protocols lldp-med]
user@switch# set tlv-select [location-id ext-power-via-mdi]
user@switch# set interface ge-0/0/1 tlv-filter network-policy
```

You can also disable TLVs for the LLDP protocol. See "Configuring LLDP (CLI Procedure)" on page 703 for more information.

RELATED DOCUMENTATION

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 557

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support | 593

NetBIOS Snooping on EX Series Switches

IN THIS SECTION

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch. The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database. for more information, read this topic.

Understanding NetBIOS Snooping

IN THIS SECTION

NetBIOS snooping allows Juniper Networks EX Series Ethernet Switches to discover NetBIOS hosts that are connected to the switch.

What Is a NetBIOS Name?

A NetBIOS name is a key element in communications between NetBIOS resources. A NetBIOS name identifies a NetBIOS resource on the network. A NetBIOS name is either a unique (exclusive) name or a group (nonexclusive) name. When a NetBIOS resource communicates with one other NetBIOS resource, a unique name is used in that communication. When a NetBIOS resource communicates with multiple resources, a group name is used.

The NetBIOS name of each NetBIOS resource is stored on the NetBIOS Name Server (NBNS). The NetBIOS name of a NetBIOS resource is mapped to its IP address.

A NetBIOS name is a 16-byte address. The first 15 bytes contain the name and the last byte contains the name type.

The NetBIOS name service is supported over UDP port 137.

How NetBIOS Snooping Works

You can enable NetBIOS snooping on the switch so that the switch can identify NetBIOS resources that are connected to it.

When a host connected to the switch initializes itself, it attempts to register its NetBIOS name by sending a NetBIOS name registration request message. The host can opt for either a unique or a group NetBIOS name. For a unique NetBIOS name, the host either broadcasts a NetBIOS name query message on the local network or unicasts it to the NBNS to check whether the requested name is already being used by another host. If so, the host that previously registered the name or the NBNS responds with a negative name registration response. If the host receives no negative response, it broadcasts the NetBIOS name registration packet to confirm the name. For a NetBIOS group name, the host sends a

NetBIOS name registration packet, which generates no responses from other hosts because multiple hosts can use the same group name at the same time.

The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 711

Configuring NetBIOS Snooping (CLI Procedure)

IN THIS SECTION

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch.

This topic describes:

Enabling NetBIOS Snooping

To enable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# set netbios-snooping
```

Disabling NetBIOS Snooping

To disable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# delete netbios-snooping
```

RELATED DOCUMENTATION

show lldp neighbors

RELATED DOCUMENTATION

lldp

CHAPTER 11

Domain Name Security

IN THIS CHAPTER

DNSSEC Overview

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

RELATED DOCUMENTATION

DNS Overview

Example: Configuring Keys for DNSSEC | **731**

Example: Configuring Secure Domains and Trusted Keys for DNSSEC | **727**

Configuring the TTL Value for DNS Server Caching

IN THIS SECTION

This section describes how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

Requirements

No special configuration beyond device initialization is required before performing this task.

Overview

IN THIS SECTION

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

Topology

Configuration

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds. (In this example, 86400 seconds equals 24 hours.)

```
[edit]
user@host# set system services dns max-cache-ttl 86400
```

2. Specify the maximum TTL value for negative cached responses, in seconds.

```
[edit]
user@host# set system services dns max-ncache-ttl 86400
```

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

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

Verification

To verify the configuration is working properly, enter the `show system services` command.

RELATED DOCUMENTATION

DNS Overview

Example: Configuring DNSSEC

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]
set system services dns dnssec disable
```

RELATED DOCUMENTATION

DNSSEC Overview | 724

Example: Configuring Secure Domains and Trusted Keys for DNSSEC

IN THIS SECTION

This example shows how to configure secure domains and trusted keys for DNSSEC.

Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See "Example: Configuring DNSSEC" on page 727 for more information.

Overview

IN THIS SECTION

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.

Topology

Configuration

IN THIS SECTION

Procedure

CLI Quick Configuration

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

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.ABC123ABCh
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Step-by-Step Procedure

To configure secure domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

```
[edit]
user@host# set system services dns dnssec secure-domains domain1.net
user@host# set system services dns dnssec secure-domains domain2.net
```

2. Configure trusted keys to domain1.net.

```
[edit]
user@host# set system services dns dnssec trusted-keys key "domain1.net.ABC123ABCh"
```

3. Attach a root zone div.isc.org as a trusted anchor to a secure domain.

```
[edit]
user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Results

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

```
dns {
    dnssec {
        trusted-keys {
            key domain1.net.ABC123ABCh; ## SECRET-DATA
        }
        dlv {
            domain domain2.net trusted-anchor dlv.isc.org;
        }
        secure-domains {
            domain1.net;
            domain2.net;
        }
    }
}
```

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

RELATED DOCUMENTATION

DNSSEC Overview | 724

Example: Configuring Keys for DNSSEC | 731

Example: Configuring Keys for DNSSEC

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key “...pasted-text...”
```

If you are done loading the keys from the file or terminal, click `commit` in the CLI editor.

RELATED DOCUMENTATION

DNSSEC Overview | 724

Example: Configuring Secure Domains and Trusted Keys for DNSSEC | 727

DNS Proxy Overview

IN THIS SECTION

A domain name system (DNS) proxy allows clients to use an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DNS proxy server. A DNS proxy improves domain lookup

performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.

If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the `clear system services dns-proxy cache` command , or the cache will automatically expire along with TTL when it goes to zero.

DNS Proxy with Split DNS

The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate then with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

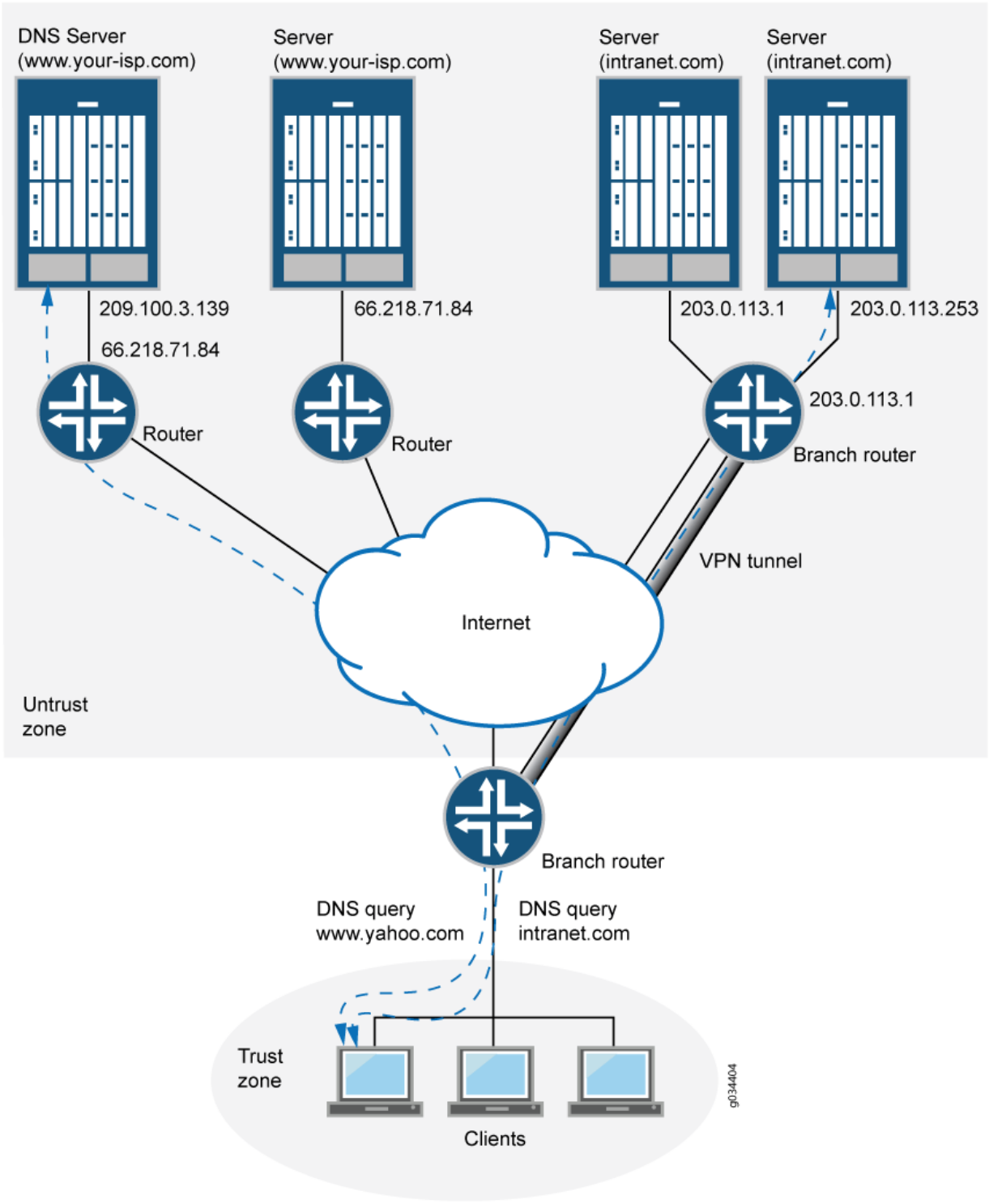
You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

Figure 31 on page 733 shows how the split DNS proxy works in a corporate network.

Figure 31: DNS Proxy with Split DNS



In the corporate network shown in Figure 31 on page 733, a PC client that points to the SRX Series Firewall as its DNS server makes two queries—to www.your-isp.com and to www.intranet.com, The DNS proxy redirects the www.intranet.com, query to the www.intranet.com DNS server (203.0.113.253), while the www.your-isp.com query is redirected to the ISP DNS server (209.100.3.130). Although the query for www.your-isp.com is sent to the ISP DNS server as a regular DNS query using clear text protocols (TCP/UDP), the query for the www.intranet.com domain goes to the intranet's DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as acme.com) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.
- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

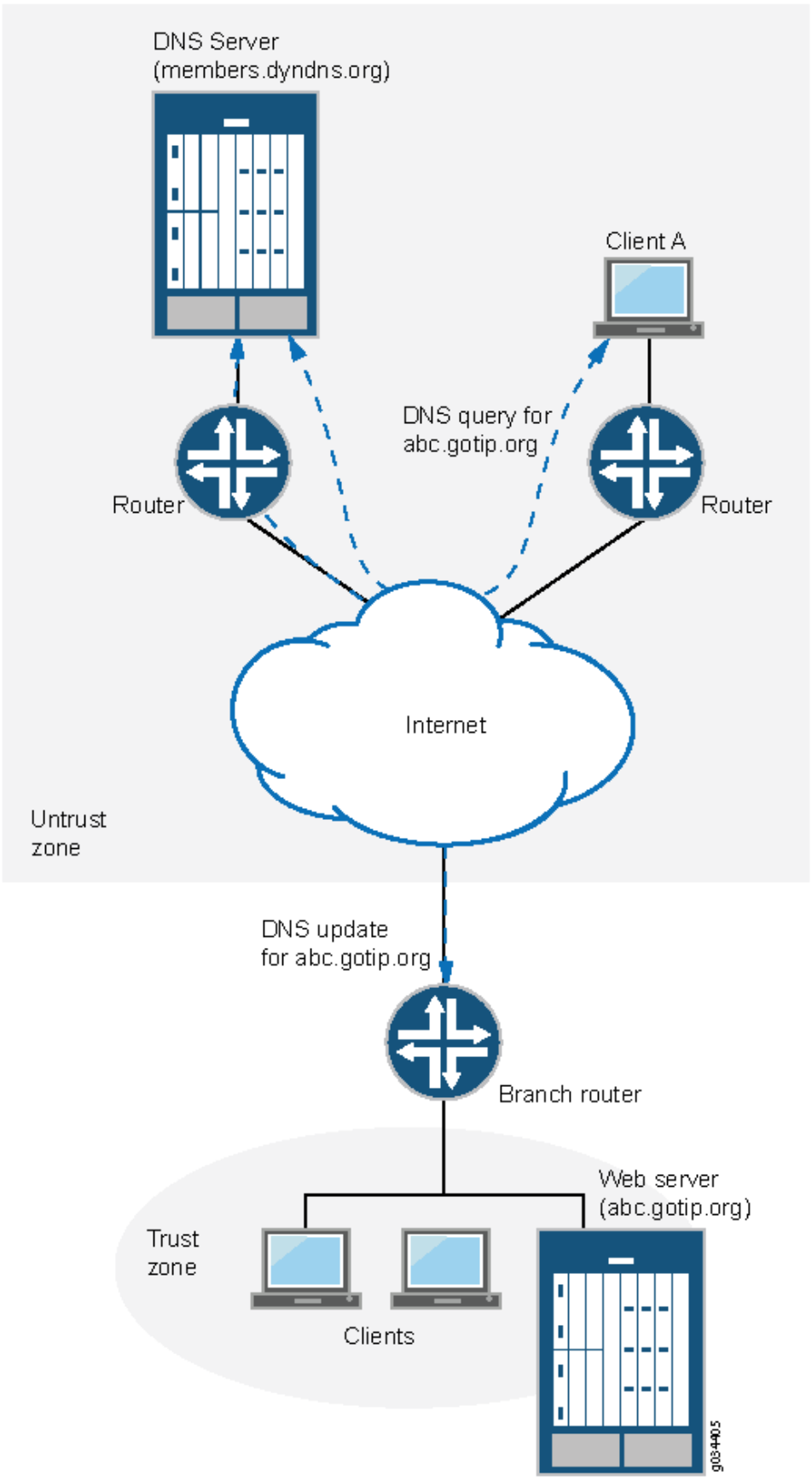
Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as dyndns.org and ddo.jp

Figure 32 on page 735 illustrates how the DDNS client works.

Figure 32: Dynamic DNS



The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the untrust zone interface on the device. The hostname abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in Figure 32 on page 735 needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

RELATED DOCUMENTATION

Configuring the Device as a DNS Proxy | **736**

Configuring the Device as a DNS Proxy

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device to reference locations by domain name (such as www.example.net) in addition to using the routable IP address.

DNS features include:

- DNS proxy cache—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series Firewall. DNS proxy improves domain lookup performance by using caching.
- Split DNS—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.
- Dynamic DNS (DDNS) client—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).

To configure the device as a DNS proxy, you enable DNS on a *logical interface* and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, ge-2/0/0.0—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

1. DNS proxy with non-split dns configuration

   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-0/0/3.0
     ```

   - Set dns resolver to forward received dns query.

     ```
     [edit]
     user@host# set system services dns forwarders 192.0.2.0
     ```

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

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

     To verify if the configuration is working properly, execute the show command.

     ```
     user@host# show system services dns-proxy statistics
     ```

2. DNS proxy with split dns configuration

   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-2/0/0.0
     ```

- Configure view for split DNS, specify the internal IP interface to handle the DNS query and view the logical subnet address.

```
[edit]
user@host# set system services dns dns-proxy view internal match-clients 10.1.1.0/24
```

- Set a default internal domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

```
[edit]
user@host# set system services dns dns-proxy view internal domain aa.internal.com
forwarders 10.1.1.1
user@host# set system services dns dns-proxy view internal domain bb.internal.com
forwarders 10.2.2.2
```

- Configure view for split DNS, specify the external IP interface to handle the DNS query and view the logical subnet address.

```
[edit]
user@host# set system services dns dns-proxy view external match-clients 10.11.1.0/24
```

- Set a default external domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

```
[edit]
user@host# set system services dns dns-proxy view external domain aa.external.com
forwarders 10.3.3.3
user@host# set system services dns dns-proxy view external domain bb.external.com
forwarders 10.4.4.4
```

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

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

To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns-proxy statistics
```

3. DNS proxy cache configuration

   - Configure the dns proxy static cache entries to specify the host's IPv4 address.

```
[edit]
user@host# set system services dns dns-proxy cache aa.example.net inet 10.10.10.10
user@host# set system services dns dns-proxy cache bb.example.net inet 10.20.20.20
```

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

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

   To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns-proxy cache
```

4. Dynamic DNS proxy configuration

   - Enable client.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface
ge-2/0/0.0 username test password test123
```

   - Configure the server.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface
ge-2/0/0.0 username test password test123 server ddo
user@host# set system services dynamic-dns client abc.com agent juniper interface
ge-2/0/0.0 username test password test123 server dyndns
```

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

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

To verify if the configuration is working properly

```
user@host# show system services dynamic-dns client
```

RELATED DOCUMENTATION

Configuring the Device as a DNS Proxy | 736

12
CHAPTER

Permission Flags

IN THIS CHAPTER

access

Can view the access configuration in configuration mode.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
```

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

```
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
```

```
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
```

```
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

Configuration Hierarchy Levels

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

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- access-control | 748

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 access radsec]
[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 Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- access | 743

admin

Can view user account information in configuration mode.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
```

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

```
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
```

```
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
```

```
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
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 authorized-keys-command]
[edit system services ssh authorized-keys-command-user]
[edit system services ssh ciphers]
[edit system services ssh client-alive-count-max]
```

```
[edit system services ssh client-alive-interval]]
[edit system services ssh fingerprint-hash]
[edit system services ssh hostkey-algorithm]
[edit system services ssh  key-exchange]
[edit system services ssh macs]
[edit system services ssh max-sessions-per-connection]
[edit system services ssh no-tcp-fowarding]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
[edit system services ssh tcp-fowarding]
[edit unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- admin-control | 754

admin-control

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

Commands

```
show system audit
```

Configuration Hierarchy Levels

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

```
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh ciphers]
[edit system services ssh hostkey-algorithm]
[edit system services ssh  key-exchange]
[edit system services ssh macs]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- admin | 749

all

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

Commands

All CLI commands.

Configuration Hierarchy Levels

All CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53

clear

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

Commands

```
clear
clear access-security
clear access-security router-advertisement-entries
<clear-as-router-advetisement-entry>
clear amt
clear amt statistics
<clear-amt-statistics>
clear amt tunnel
clear-amt-tunnel
clear amt tunnel gateway-address
<clear amt tunnel gateway-address>
clear amt tunnel statistics
<clear-amt-tunnel-statistics>
clear amt tunnel statistics gateway-address
<clear-amt-tunnel-gateway-address-statistics>
clear amt tunnel statistics tunnel-interface
<clear-amt-tunnel-interface-statistics>
clear amt tunnel tunnel-interface
<clear-amt-tunnel-interface<>
clear ancp
clear ancp neighbor
 <clear-ancp-neighbor-connection>
clear ancp statistics
<clear-ancp-statistics>
clear ancp subscriber
<clear-ancp-subscriber-connection>
clear-appqos-counter
<clear-appqos-rate-limiters-statistics>
```

```
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 evpn nd-table
<clear-bridge-evpn-nd-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 bridge satellite
clear bridge satellite logging
```

```
<clear-satellite-control-logging>
clear bridge satellite vlan-auto-sense
<clear-satellite-control-plane-vlan-auto-sense>
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 all-fiber-channel-enode
clear ddos-protection protocols all-fiber-channel-enode aggregate
clear ddos-protection protocols all-fiber-channel-enode aggregate culprit-flows
<clear-ddos-all-fc-enode-aggregate-flows>
clear ddos-protection protocols all-fiber-channel-enode aggregate states
<clear-ddos-all-fc-enode-aggregate-states>
clear ddos-protection protocols all-fiber-channel-enode aggregate statistics
<clear-ddos-all-fc-enode-aggregate-statistics>
clear ddos-protection protocols all-fiber-channel-enode culprit-flows
<clear-ddos-all-fc-enode-flows>
clear ddos-protection protocols all-fiber-channel-enode states
<clear-ddos-all-fc-enode-states>
clear ddos-protection protocols all-fiber-channel-enode statistics
<clear-ddos-all-fc-enode-statistics>
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-snoop
clear ddos-protection protocols arp-snoop aggregate
clear ddos-protection protocols arp-snoop aggregate culprit-flows
<clear-ddos-arp-snoop-aggregate-flows>
clear ddos-protection protocols arp-snoop aggregate states
<clear-ddos-arp-snoop-aggregate-states>
```

```
clear ddos-protection protocols arp-snoop aggregate statistics
<clear-ddos-arp-snoop-aggregate-statistics>
clear ddos-protection protocols arp-snoop culprit-flows
<clear-ddos-arp-snoop-flows>
clear ddos-protection protocols arp-snoop states
<clear-ddos-arp-snoop-states>
clear ddos-protection protocols arp-snoop statistics
<clear-ddos-arp-snoop-statistics>
clear ddos-protection protocols arp culprit-flows
clear ddos-protection protocols atm
clear ddos-protection protocols atm aggregate
clear ddos-protection protocols atm aggregate culprit-flows
clear ddos-protection protocols atm aggregate states
<clear-ddos-atm-aggregate-states>
clear ddos-protection protocols atm aggregate statistics
<clear-ddos-atm-aggregate-statistics>
clear ddos-protection protocols atm culprit-flows
clear ddos-protection protocols bfd aggregate culprit-flows
clear ddos-protection protocols atm states
clear-ddos-atm-states
clear ddos-protection protocols atm statistics
clear-ddos-atm-statistics
clear ddos-protection protocols bfd
clear ddos-protection protocols bfd aggregate
clear ddos-protection protocols bfd culprit-flows
clear ddos-protection protocols bfd aggregate states
clear-ddos-bfd-aggregate-states
 clear ddos-protection protocols bfd aggregate statistics
clear-ddos-bfd-aggregate-statistics
 clear ddos-protection protocols bfd states
clear-ddos-bfd-states
clear ddos-protection protocols bfd statistics
clear-ddos-bfd-statistics
clear ddos-protection protocols bfdv6
clear ddos-protection protocols bfdv6 aggregate
clear ddos-protection protocols bfdv6 culprit-flows
clear ddos-protection protocols bfdv6 aggregate states
clear-ddos-bfdv6-aggregate-states
clear ddos-protection protocols bfdv6 aggregate statistics
clear-ddos-bfdv6-aggregate-statistics
clear ddos-protection protocols bfdv6 states
clear-ddos-bfdv6-states
clear ddos-protection protocols bfdv6 statistics
```

```
clear-ddos-bfdv6-statistics
clear ddos-protection protocols bgp
clear ddos-protection protocols bgp aggregate
clear ddos-protection protocols bgp aggregate culprit-flows
clear ddos-protection protocols bgp aggregate states
clear-ddos-bgp-aggregate-states
clear ddos-protection protocols bgp aggregate statistics
clear ddos-protection protocols bgp culprit-flows
clear ddos-protection protocols bgp states
clear-ddos-bgp-states
clear ddos-protection protocols bgp statistics
clear-ddos-bgp-statistics
clear ddos-protection protocols bgpv6
clear ddos-protection protocols bgpv6 aggregate
clear ddos-protection protocols bgpv6 aggregate culprit-flows
clear ddos-protection protocols bgpv6 aggregate states
clear-ddos-bgpv6-aggregate-states
clear ddos-protection protocols bgpv6 aggregate statistics
clear-ddos-bgpv6-aggregate-statistics
clear ddos-protection protocols bgpv6 states
clear-ddos-bgp-aggregate-states
clear-ddos-bgp-aggregate-statistics
clear-ddos-bgp-states
clear-ddos-bgp-statistics
clear-ddos-bgpv6-aggregate-states
clear-ddos-bgpv6-aggregate-statistics
clear-ddos-bgpv6-states
clear ddos-protection protocols bgpv6 statistics
<clear-ddos-bgpv6-statistics>
clear ddos-protection protocols bridge-control
clear ddos-protection protocols bridge-control aggregate
clear ddos-protection protocols bridge-control aggregate culprit-flows
<clear-ddos-brg-ctrl-aggregate-flows>
clear ddos-protection protocols bridge-control aggregate states
<clear-ddos-brg-ctrl-aggregate-states>
clear ddos-protection protocols bridge-control aggregate statistics
<clear-ddos-brg-ctrl-aggregate-statistics>
clear ddos-protection protocols bridge-control culprit-flows
<clear-ddos-brg-ctrl-flows>
clear ddos-protection protocols bridge-control states
<clear-ddos-brg-ctrl-states>
clear ddos-protection protocols bridge-control statistics
<clear-ddos-brg-ctrl-statistics>
```

```
clear ddos-protection protocols culprit-flows
clear ddos-protection protocols demux-autosense
clear ddos-protection protocols demux-autosense aggregate
clear ddos-protection protocols demux-autosense aggregate culprit-flows
clear ddos-protection protocols demux-autosense aggregate states
clear-ddos-demuxauto-aggregate-states
clear ddos-protection protocols demux-autosense aggregate statistics
clear ddos-protection protocols demux-autosense culprit-flows
clear ddos-protection protocols demux-autosense states
clear-ddos-demuxauto-states
clear ddos-protection protocols demux-autosense statistics
clear-ddos-demuxauto-statistics
clear ddos-protection protocols dhcpv4
clear ddos-protection protocols dhcpv4 ack
clear ddos-protection protocols dhcpv4 ack culprit-flows
clear ddos-protection protocols dhcpv4 ack states
clear ddos-protection protocols dhcpv4 ack statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4v6
clear ddos-protection protocols dhcpv4v6 aggregate
clear ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<clear-ddos-dhcpv4v6-aggregate-flows>
clear ddos-protection protocols dhcpv4v6 aggregate states
<clear-ddos-dhcpv4v6-aggregate-states>
clear ddos-protection protocols dhcpv4v6 aggregate statistics
<clear-ddos-dhcpv4v6-aggregate-statistics>
clear ddos-protection protocols dhcpv4v6 culprit-flows
<clear-ddos-dhcpv4v6-flows>
clear ddos-protection protocols dhcpv4v6 states
<clear-ddos-dhcpv4v6-states>
clear ddos-protection protocols dhcpv4v6 statistics
<clear-ddos-dhcpv4v6-statistics>
clear-ddos-demuxauto-aggregate-states
clear-ddos-demuxauto-aggregate-statistics
clear-ddos-demuxauto-states
clear-ddos-demuxauto-statistics
clear-ddos-dhcpv4-ack-states
clear ddos-protection protocols dhcpv4 ack statistics
clear-ddos-dhcpv4-ack-statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4 aggregate states
clear-ddos-dhcpv4-aggregate-states
clear ddos-protection protocols dhcpv4 aggregate statistics
```

```
clear-ddos-dhcpv4-aggregate-statistics
clear ddos-protection protocols dhcpv4 bad-packets
clear ddos-protection protocols dhcpv4 bad-packets states
clear-ddos-dhcpv4-bad-pack-states
clear ddos-protection protocols dhcpv4 bad-packets statistics
clear-ddos-dhcpv4-bad-pack-statistics
clear ddos-protection protocols dhcpv4 bootp
clear ddos-protection protocols dhcpv4 bootp states
clear-ddos-dhcpv4-bootp-states
clear ddos-protection protocols dhcpv4 bootp statistics
clear-ddos-dhcpv4-bootp-statistics
clear ddos-protection protocols dhcpv4 decline
clear ddos-protection protocols dhcpv4 decline culprit-flows
clear ddos-protection protocols dhcpv4 decline states
clear-ddos-dhcpv4-decline-states
clear ddos-protection protocols dhcpv4 decline statistics
clear-ddos-dhcpv4-decline-statistics
clear ddos-protection protocols dhcpv4 discover
clear ddos-protection protocols dhcpv4 discover states
clear-ddos-dhcpv4-discover-states
clear ddos-protection protocols dhcpv4 discover statistics
clear-ddos-dhcpv4-discover-statistics
clear ddos-protection protocols dhcpv4 force-renew
clear ddos-protection protocols dhcpv4 force-renew culprit-flows
clear ddos-protection protocols dhcpv4 force-renew states
clear-ddos-dhcpv4-forcerenew-states
clear ddos-protection protocols dhcpv4 force-renew statistics
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 inform
clear ddos-protection protocols dhcpv4 inform culprit-flows
clear ddos-protection protocols dhcpv4 inform states
clear-ddos-dhcpv4-decline-states
clear-ddos-dhcpv4-decline-statistics
clear-ddos-dhcpv4-discover-states
clear-ddos-dhcpv4-discover-statistics
clear-ddos-dhcpv4-forcerenew-states
clear-ddos-dhcpv4-forcerenew-statistics
clear ddos-protection protocols dhcpv4 unclassified culprit-flows
clear ddos-protection protocols dhcpv4 unclassified states
clear-ddos-dhcpv4-unclass-states
clear ddos-protection protocols dhcpv4 unclassified statistics
clear-ddos-dhcpv4-unclass-statistics
clear ddos-protection protocols dhcpv6
```

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

```
clear ddos-protection protocols garp-reply culprit-flows
<clear-ddos-garp-reply-flows>
clear ddos-protection protocols garp-reply states
<clear-ddos-garp-reply-states>
clear ddos-protection protocols garp-reply statistics
<clear-ddos-garp-reply-statistics>
clear ddos-protection protocols gre hbc
clear ddos-protection protocols gre hbc culprit-flows
<clear-ddos-gre-hbc-flows>
clear ddos-protection protocols gre hbc states
<clear-ddos-gre-hbc-states>
clear ddos-protection protocols gre hbc statistics
<clear-ddos-gre-hbc-statistics>
clear ddos-protection protocols gre punt
clear ddos-protection protocols gre punt culprit-flows
<clear-ddos-gre-punt-flows>
clear ddos-protection protocols gre punt states
<clear-ddos-gre-punt-states>
clear ddos-protection protocols gre punt statistics
<clear-ddos-gre-punt-statistics>
clear ddos-protection protocols ipmc-reserved
clear ddos-protection protocols ipmc-reserved aggregate
clear ddos-protection protocols ipmc-reserved aggregate culprit-flows
<clear-ddos-ipmc-reserved-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate states
<clear-ddos-ipmc-reserved-aggregate-states>
clear ddos-protection protocols ipmc-reserved aggregate statistics
<clear-ddos-ipmc-reserved-aggregate-statistics>
clear ddos-protection protocols ipmc-reserved culprit-flows
<clear-ddos-ipmc-reserved-flows>
clear ddos-protection protocols ipmc-reserved states
<clear-ddos-ipmc-reserved-states>
clear ddos-protection protocols ipmc-reserved statistics
<clear-ddos-ipmc-reserved-statistics>
clear ddos-protection protocols ipmcast-miss
clear ddos-protection protocols ipmcast-miss aggregate
clear ddos-protection protocols ipmcast-miss aggregate culprit-flows
<clear-ddos-ipmcast-miss-aggregate-flows>
clear ddos-protection protocols ipmcast-miss aggregate states
<clear-ddos-ipmcast-miss-aggregate-states>
clear ddos-protection protocols ipmcast-miss aggregate statistics
<clear-ddos-ipmcast-miss-aggregate-statistics>
clear ddos-protection protocols ipmcast-miss culprit-flows
```

```
<clear-ddos-ipmcast-miss-flows>
clear ddos-protection protocols ipmcast-miss states
<clear-ddos-ipmcast-miss-states>
clear ddos-protection protocols ipmcast-miss statistics
<clear-ddos-ipmcast-miss-statistics>
clear ddos-protection protocols l3dest-miss
clear ddos-protection protocols l3dest-miss aggregate
clear ddos-protection protocols l3dest-miss aggregate culprit-flows
<clear-ddos-l3dest-miss-aggregate-flows>
clear ddos-protection protocols l3dest-miss aggregate states
<clear-ddos-l3dest-miss-aggregate-states>
clear ddos-protection protocols l3dest-miss aggregate statistics
<clear-ddos-l3dest-miss-aggregate-statistics>
clear ddos-protection protocols l3dest-miss culprit-flows
<clear-ddos-l3dest-miss-flows>
clear ddos-protection protocols l3dest-miss states
<clear-ddos-l3dest-miss-states>
clear ddos-protection protocols l3dest-miss statistics
<clear-ddos-l3dest-miss-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-aggregate-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate states
<clear-ddos-l3mc-sgv-hit-icl-aggregate-states>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate statistics
<clear-ddos-l3mc-sgv-hit-icl-aggregate-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl culprit-flowsclear ddos-protection protocols
l3mc-sgv-hit-icl culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl states
<clear-ddos-l3mc-sgv-hit-icl-states>
clear ddos-protection protocols l3mc-sgv-hit-icl statistics
<clear-ddos-l3mc-sgv-hit-icl-statistics>
clear ddos-protection protocols l3mtu-fail
clear ddos-protection protocols l3mtu-fail aggregate
clear ddos-protection protocols l3mtu-fail aggregate culprit-flows
<clear-ddos-l3mtu-fail-aggregate-flows>
clear ddos-protection protocols l3mtu-fail aggregate states
<clear-ddos-l3mtu-fail-aggregate-states>
clear ddos-protection protocols l3mtu-fail aggregate statistics
<clear-ddos-l3mtu-fail-aggregate-statistics>
clear ddos-protection protocols l3mtu-fail culprit-flows
```

```
<clear-ddos-l3mtu-fail-flows>
clear ddos-protection protocols l3mtu-fail states
<clear-ddos-l3mtu-fail-states>
clear ddos-protection protocols l3mtu-fail statistics
<clear-ddos-l3mtu-fail-statistics>
clear ddos-protection protocols l3nhop
clear ddos-protection protocols l3nhop aggregate
clear ddos-protection protocols l3nhop aggregate culprit-flows
<clear-ddos-l3nhop-aggregate-flows>
clear ddos-protection protocols l3nhop aggregate states
<clear-ddos-l3nhop-aggregate-states>
clear ddos-protection protocols l3nhop aggregate statistics
<clear-ddos-l3nhop-aggregate-statistics>
clear ddos-protection protocols l3nhop culprit-flows
<clear-ddos-l3nhop-flows>
clear ddos-protection protocols l3nhop states
<clear-ddos-l3nhop-states>
clear ddos-protection protocols l3nhop statistics
<clear-ddos-l3nhop-statistics>
clear ddos-protection protocols localnh
clear ddos-protection protocols localnh aggregate
clear ddos-protection protocols localnh aggregate culprit-flows
<clear-ddos-localnh-aggregate-flows>
clear ddos-protection protocols localnh aggregate states
<clear-ddos-localnh-aggregate-states>
clear ddos-protection protocols localnh aggregate statistics
<clear-ddos-localnh-aggregate-statistics>
clear ddos-protection protocols localnh culprit-flows
<clear-ddos-localnh-flows>
clear ddos-protection protocols localnh states
<clear-ddos-localnh-states>
clear ddos-protection protocols localnh statistics
<clear-ddos-localnh-statistics>
clear-ddos-dhcpv4-unclass-states
clear-ddos-dhcpv4-unclass-statistics
clear-ddos-dhcpv6-advertise-states
clear-ddos-dhcpv6-advertise-statistics
clear-ddos-dhcpv6-aggregate-states
clear-ddos-dhcpv6-aggregate-statistics
clear-ddos-dhcpv6-confirm-states
clear-ddos-dhcpv6-confirm-statistics
clear-ddos-dhcpv6-decline-states
clear-ddos-dhcpv6-decline-statistics
```

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

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

```
clear-ddos-dhcpv6-relay-for-states
clear-ddos-dhcpv6-relay-for-statistics
clear-ddos-dhcpv6-relay-rep-states
clear-ddos-dhcpv6-relay-rep-statistics
clear-ddos-dhcpv6-release-states
clear-ddos-dhcpv6-release-statistics
clear-ddos-dhcpv6-renew-states
clear-ddos-dhcpv6-renew-statistics
clear-ddos-dhcpv6-reply-states
clear-ddos-dhcpv6-reply-statistics
clear-ddos-dhcpv6-request-states
clear-ddos-dhcpv6-request-statistics
clear-ddos-dhcpv6-solicit-states
clear-ddos-dhcpv6-solicit-statistics
clear-ddos-dhcpv6-states
clear-ddos-dhcpv6-statistics
clear-ddos-dhcpv6-unclass-states
clear-ddos-dhcpv6-unclass-statistics
clear-ddos-diameter-aggregate-states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-diameter-aggregate-statistics
clear ddos-protection protocols diameter states
clear-ddos-diameter-states
clear ddos-protection protocols diameter statistics
clear-ddos-diameter-statistics
clear ddos-protection protocols dns
clear ddos-protection protocols dns aggregate
clear ddos-protection protocols dns aggregate states
clear-ddos-dns-aggregate-states
clear ddos-protection protocols dns aggregate statistics
clear-ddos-dns-aggregate-statistics
clear ddos-protection protocols dns states
clear-ddos-dns-states
clear ddos-protection protocols dns statistics
clear-ddos-dns-statistics
clear ddos-protection protocols dtcp
clear ddos-protection protocols dtcp aggregate
clear ddos-protection protocols dtcp aggregate culprit-flows
clear ddos-protection protocols dtcp aggregate states
clear-ddos-dtcp-aggregate-states
clear ddos-protection protocols dtcp aggregate statistics
clear ddos-protection protocols dtcp culprit-flows
clear ddos-protection protocols dtcp states
```

```
clear-ddos-dtcp-states
clear ddos-protection protocols dtcp statistics
clear-ddos-dtcp-statistics
clear ddos-protection protocols dynamic-vlan
clear ddos-protection protocols dynamic-vlan aggregate
clear ddos-protection protocols dynamic-vlan aggregate culprit-flows
clear ddos-protection protocols dynamic-vlan aggregate states
clear-ddos-dynvlan-aggregate-states
clear ddos-protection protocols dynamic-vlan aggregate statistics
clear-ddos-dynvlan-aggregate-statistics
clear ddos-protection protocols dynamic-vlan states
clear-ddos-dynvlan-states
clear ddos-protection protocols dynamic-vlan statistics
clear-ddos-dynvlan-statistics
clear ddos-protection protocols egpv6
clear ddos-protection protocols egpv6 aggregate
clear ddos-protection protocols egpv6 aggregate culprit-flows
clear ddos-protection protocols egpv6 aggregate states
clear-ddos-egpv6-aggregate-states
clear ddos-protection protocols egpv6 aggregate statistics
clear-ddos-egpv6-aggregate-statistics
clear ddos-protection protocols egpv6 states
clear-ddos-egpv6-states
clear ddos-protection protocols egpv6 statistics
clear-ddos-egpv6-statistics
clear ddos-protection protocols eoam
clear ddos-protection protocols eoam aggregate
clear ddos-protection protocols eoam aggregate culprit-flows
clear ddos-protection protocols eoam aggregate states
clear-ddos-eoam-aggregate-states
clear ddos-protection protocols eoam aggregate statistics
clear-ddos-eoam-aggregate-statistics
clear ddos-protection protocols eoam states
clear-ddos-eoam-states
clear ddos-protection protocols eoam statistics
clear-ddos-eoam-statistics
clear ddos-protection protocols esmc
clear ddos-protection protocols esmc aggregate
clear ddos-protection protocols esmc aggregate culprit-flows
clear ddos-protection protocols esmc aggregate states
clear-ddos-esmc-aggregate-states
clear ddos-protection protocols esmc aggregate statistics
clear ddos-protection protocols esmc culprit-flows
```

```
clear ddos-protection protocols esmc states
clear-ddos-esmc-states
clear ddos-protection protocols esmc statistics
<clear-ddos-esmc-statistics>
clear ddos-protection protocols ethernet-tcc
clear ddos-protection protocols ethernet-tcc aggregate
clear ddos-protection protocols ethernet-tcc aggregate culprit-flows
<clear-ddos-eth-tcc-aggregate-flows>
clear ddos-protection protocols ethernet-tcc aggregate states
<clear-ddos-eth-tcc-aggregate-states>
clear ddos-protection protocols ethernet-tcc aggregate statistics
<clear-ddos-eth-tcc-aggregate-statistics>
clear ddos-protection protocols ethernet-tcc culprit-flows
<clear-ddos-eth-tcc-flows>
clear ddos-protection protocols ethernet-tcc states
<clear-ddos-eth-tcc-states>
clear ddos-protection protocols ethernet-tcc statistics
<clear-ddos-eth-tcc-statistics>
clear ddos-protection protocols exceptions
clear ddos-protection protocols exceptions aggregate
clear ddos-protection protocols exceptions aggregate culprit-flows
<clear-ddos-exception-aggregate-flows>
clear ddos-protection protocols exceptions aggregate states
<clear-ddos-exception-aggregate-states>
clear ddos-protection protocols exceptions aggregate statistics
<clear-ddos-exception-aggregate-statistics>
clear ddos-protection protocols exceptions culprit-flows
<clear-ddos-exception-flows>
clear ddos-protection protocols exceptions mcast-rpf-err
clear ddos-protection protocols exceptions mcast-rpf-err culprit-flows
<clear-ddos-exception-mcast-rpf-flows>
clear ddos-protection protocols exceptions mcast-rpf-err states
<clear-ddos-exception-mcast-rpf-states>
clear ddos-protection protocols exceptions mcast-rpf-err statistics
<clear-ddos-exception-mcast-rpf-statistics>
clear ddos-protection protocols exceptions mtu-exceeded
clear ddos-protection protocols exceptions mtu-exceeded culprit-flows
<clear-ddos-exception-mtu-exceed-flows>
clear ddos-protection protocols exceptions mtu-exceeded states
<clear-ddos-exception-mtu-exceed-states>
clear ddos-protection protocols exceptions mtu-exceeded statistics
<clear-ddos-exception-mtu-exceed-statistics>
clear ddos-protection protocols exceptions states
```

```
<clear-ddos-exception-states>
clear ddos-protection protocols exceptions statistics
<clear-ddos-exception-statistics>
clear ddos-protection protocols exceptions unclassified
clear ddos-protection protocols exceptions unclassified culprit-flows
<clear-ddos-exception-unclass-flows>
clear ddos-protection protocols exceptions unclassified states
<clear-ddos-exception-unclass-states>
clear ddos-protection protocols exceptions unclassified statistics
<clear-ddos-exception-unclass-statistics>
clear ddos-protection protocols fab-probe
clear ddos-protection protocols fab-probe aggregate
clear ddos-protection protocols fab-probe aggregate states
clear ddos-protection protocols fab-probe aggregate statistics
<clear-ddos-fab-probe-aggregate-statistics>
clear ddos-protection protocols martian-address
clear ddos-protection protocols martian-address aggregate
clear ddos-protection protocols martian-address aggregate culprit-flows
<clear-ddos-martian-address-aggregate-flows>
clear ddos-protection protocols martian-address aggregate states
<clear-ddos-martian-address-aggregate-states>
clear ddos-protection protocols martian-address aggregate statistics
<clear-ddos-martian-address-aggregate-statistics>
clear ddos-protection protocols martian-address culprit-flows
<clear-ddos-martian-address-flows>
clear ddos-protection protocols martian-address states
<clear-ddos-martian-address-states>
clear ddos-protection protocols martian-address statistics
<clear-ddos-martian-address-statistics>
clear-ddos-diameter-statistics
clear-ddos-dns-aggregate-states
clear-ddos-dns-aggregate-statistics
clear-ddos-dns-states
clear-ddos-dns-statistics
clear-ddos-dtcp-aggregate-states
clear-ddos-dtcp-aggregate-statistics
clear-ddos-dtcp-states
clear-ddos-dtcp-statistics
clear-ddos-dynvlan-aggregate-states
clear-ddos-dynvlan-aggregate-statistics
clear-ddos-dynvlan-states
clear-ddos-dynvlan-statistics
clear-ddos-egpv6-aggregate-states
```

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

```
clear ddos-protection protocols frame-relay statistics
clear ddos-protection protocols ftp
clear ddos-protection protocols ftp aggregate
clear ddos-protection protocols ftp aggregate culprit-flows
clear ddos-protection protocols ftp aggregate states
clear-ddos-ftp-aggregate-states
clear ddos-protection protocols ftp aggregate statistics
clear-ddos-ftp-aggregate-statistics
clear ddos-protection protocols ftp states
clear-ddos-ftp-states
clear ddos-protection protocols ftp statistics
clear-ddos-ftp-statistics
clear ddos-protection protocols ftpv6
clear ddos-protection protocols ftpv6 aggregate
clear ddos-protection protocols ftpv6 aggregate culprit-flows
clear ddos-protection protocols ftpv6 aggregate states
clear-ddos-ftpv6-aggregate-states
clear ddos-protection protocols ftpv6 aggregate statistics
clear-ddos-ftpv6-aggregate-statistics
clear ddos-protection protocols ftpv6 states
clear-ddos-ftpv6-states
clear ddos-protection protocols ftpv6 statistics
clear-ddos-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 gre aggregate statistics
clear-ddos-gre-aggregate-statistics
clear ddos-protection protocols gre states
clear-ddos-gre-states
clear ddos-protection protocols gre statistics
clear-ddos-gre-statistics
clear ddos-protection protocols icmp
clear ddos-protection protocols icmp aggregate
clear ddos-protection protocols icmp aggregate states
```

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

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

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

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

```
clear-ddos-ipv4-uncls-aggregate-states
clear-ddos-isis-aggregate-states
clear ddos-protection protocols isis aggregate statistics
<clear-ddos-isis-aggregate-statistics>
clear ddos-protection protocols isis culprit-flows
clear ddos-protection protocols isis states
clear-ddos-isis-states
clear ddos-protection protocols isis statistics
clear-ddos-isis-statistics
clear ddos-protection protocols iso-tcc
clear ddos-protection protocols iso-tcc aggregate
clear ddos-protection protocols iso-tcc aggregate culprit-flows
<clear-ddos-iso-tcc-aggregate-flows>
clear ddos-protection protocols iso-tcc aggregate states
<clear-ddos-iso-tcc-aggregate-states>
clear ddos-protection protocols iso-tcc aggregate statistics
<clear-ddos-iso-tcc-aggregate-statistics>
clear ddos-protection protocols iso-tcc culprit-flows
<clear-ddos-iso-tcc-flows>
clear ddos-protection protocols iso-tcc states
<clear-ddos-iso-tcc-states>
clear ddos-protection protocols iso-tcc statistics
<clear-ddos-iso-tcc-statistics>
clear ddos-protection protocols jfm
clear ddos-protection protocols jfm aggregate
clear ddos-protection protocols jfm aggregate culprit-flows
clear ddos-protection protocols jfm aggregate states
clear-ddos-jfm-aggregate-states
clear ddos-protection protocols jfm aggregate statistics
clear-ddos-jfm-aggregate-statistics
clear ddos-protection protocols jfm states
clear-ddos-jfm-states
clear ddos-protection protocols jfm statistics
<clear-ddos-jfm-statistics>
clear ddos-protection protocols keepalive
clear ddos-protection protocols keepalive aggregate
clear ddos-protection protocols keepalive aggregate culprit-flows
clear ddos-protection protocols keepalive aggregate states
clear ddos-protection protocols keepalive aggregate statistics
clear ddos-protection protocols keepalive culprit-flows
clear ddos-protection protocols keepalive states
clear ddos-protection protocols keepalive statistics
clear ddos-protection protocols l2pt
```

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

```
clear-ddos-lacp-states
clear-ddos-lacp-statistics
clear-ddos-ldp-aggregate-states
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp statistics
clear ddos-protection protocols ldp statistics
clear-ddos-ldp-statistics
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate statistics
clear ddos-protection protocols ldpv6 aggregate statistics
clear-ddos-ldpv6-aggregate-statistics
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp states
clear ddos-protection protocols lldp states
clear-ddos-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-lmpv6-states
clear ddos-protection protocols lmpv6 statistics
clear-ddos-lmpv6-statistics
clear ddos-protection protocols mac-host
clear ddos-protection protocols mac-host aggregate
clear ddos-protection protocols mac-host aggregate culprit-flows
clear ddos-protection protocols mac-host aggregate states
clear-ddos-mac-host-aggregate-states
clear ddos-protection protocols mac-host aggregate statistics
clear-ddos-mac-host-aggregate-statistics
clear ddos-protection protocols mac-host states
clear-ddos-mac-host-states
clear ddos-protection protocols mac-host statistics
clear ddos-protection protocols mcast-snoop
clear ddos-protection protocols mcast-snoop aggregate
clear ddos-protection protocols mcast-snoop aggregate culprit-flows
clear ddos-protection protocols mcast-snoop aggregate states
clear ddos-protection protocols mcast-snoop aggregate statistics
```

```
clear ddos-protection protocols mcast-snoop culprit-flows
clear ddos-protection protocols mcast-snoop igmp
clear ddos-protection protocols mcast-snoop igmp culprit-flows
<clear-ddos-mcast-snoop-igmp-flows>
clear ddos-protection protocols mcast-snoop igmp states
<clear-ddos-mcast-snoop-igmp-states>
clear ddos-protection protocols mcast-snoop igmp statistics
<clear-ddos-mcast-snoop-igmp-statistics>
clear ddos-protection protocols mcast-snoop mld
clear ddos-protection protocols mcast-snoop mld culprit-flows
<clear-ddos-mcast-snoop-mld-flows>
clear ddos-protection protocols mcast-snoop mld states
<clear-ddos-mcast-snoop-mld-states>
clear ddos-protection protocols mcast-snoop mld statistics
<clear-ddos-mcast-snoop-mld-statistics>
clear ddos-protection protocols mld
clear ddos-protection protocols mld aggregate
clear ddos-protection protocols mld aggregate culprit-flows
<clear-ddos-mld-aggregate-flows>
clear ddos-protection protocols mld aggregate states
<clear-ddos-mld-aggregate-states>
clear ddos-protection protocols mld aggregate statistics
<clear-ddos-mld-aggregate-statistics>
clear ddos-protection protocols mld culprit-flows
<clear-ddos-mld-flows>
clear ddos-protection protocols mld states
<clear-ddos-mld-states>
clear ddos-protection protocols mld statistics
<clear-ddos-mld-statistics>
clear ddos-protection protocols mlp
clear ddos-protection protocols mlp add
clear ddos-protection protocols mlp add culprit-flows
<clear-ddos-mlp-add-flows>
clear ddos-protection protocols mlp add states
<clear-ddos-mlp-add-states>
clear ddos-protection protocols mlp add statistics
<clear-ddos-mlp-add-statistics>
clear ddos-protection protocols mlp aggregate
clear ddos-protection protocols mlp aggregate culprit-flows
clear ddos-protection protocols mlp aggregate states
clear-ddos-mlp-aggregate-states
clear ddos-protection protocols mlp aggregate statistics
clear-ddos-mlp-aggregate-statistics
```

```
clear ddos-protection protocols mlp aging-exception
clear ddos-protection protocols mlp aging-exception culprit-flows
clear ddos-protection protocols mlp aging-exception states
clear-ddos-mlp-aging-exc-states
clear ddos-protection protocols mlp aging-exception statistics
clear-ddos-mlp-aging-exc-statistics
clear ddos-protection protocols mlp packets
clear ddos-protection protocols mlp packets states
clear-ddos-mlp-packets-states
clear ddos-protection protocols mlp packets statistics
clear-ddos-mlp-packets-statistics
clear ddos-protection protocols mlp macpin-exception
clear ddos-protection protocols mlp macpin-exception culprit-flows
<clear-ddos-mlp-mac-pinning-flows>
clear ddos-protection protocols mlp macpin-exception states
<clear-ddos-mlp-mac-pinning-states>
clear ddos-protection protocols mlp macpin-exception statistics
<clear-ddos-mlp-mac-pinning-statistics>
clear ddos-protection protocols mlp states
clear-ddos-mlp-states
clear ddos-protection protocols mlp statistics
clear-ddos-mlp-statistics
clear ddos-protection protocols mlp unclassified
clear ddos-protection protocols mlp unclassified states
clear-ddos-mlp-unclass-states
clear ddos-protection protocols mlp unclassified statistics
clear-ddos-mlp-unclass-statistics
clear ddos-protection protocols msdp
clear ddos-protection protocols msdp aggregate
clear ddos-protection protocols msdp aggregate states
clear-ddos-msdp-aggregate-states
clear ddos-protection protocols msdp aggregate statistics
clear ddos-protection protocols msdp culprit-flows
clear ddos-protection protocols msdp states
clear-ddos-msdp-states
clear ddos-protection protocols msdp statistics
clear-ddos-msdp-statistics
clear ddos-protection protocols msdpv6
clear ddos-protection protocols msdpv6 aggregate
clear ddos-protection protocols msdpv6 aggregate culprit-flows
clear ddos-protection protocols msdpv6 aggregate states
clear-ddos-msdpv6-aggregate-states
clear ddos-protection protocols msdpv6 aggregate statistics
```

```
clear-ddos-msdpv6-aggregate-statistics
clear ddos-protection protocols msdpv6 states
clear-ddos-msdpv6-states
clear ddos-protection protocols msdpv6 statistics
clear-ddos-msdpv6-statistics
clear ddos-protection protocols multicast-copy
clear ddos-protection protocols multicast-copy aggregate
clear ddos-protection protocols multicast-copy aggregate states
clear-ddos-mcast-copy-aggregate-states
clear ddos-protection protocols multicast-copy aggregate statistics
clear-ddos-mcast-copy-aggregate-statistics
clear ddos-protection protocols multicast-copy states
clear-ddos-mcast-copy-states
clear ddos-protection protocols multicast-copy statistics
clear-ddos-mcast-copy-statistics
clear ddos-protection protocols mvrp
clear ddos-protection protocols mvrp aggregate
clear ddos-protection protocols mvrp aggregate states
clear-ddos-mvrp-aggregate-states
clear ddos-protection protocols mvrp aggregate statistics
clear ddos-protection protocols mvrp culprit-flows
clear ddos-protection protocols mvrp states
clear-ddos-mvrp-states
clear ddos-protection protocols mvrp statistics
clear-ddos-mvrp-statistics
clear ddos-protection protocols ndpv6
clear ddos-protection protocols ndpv6 aggregate
clear ddos-protection protocols ndpv6 aggregate states
clear ddos-protection protocols ndpv6 aggregate statistics
clear ddos-protection protocols ndpv6 neighbor-advertisement
clear ddos-protection protocols ndpv6 neighbor-advertisement culprit-flows
<clear-ddos-ndpv6-neighb-adv-flows>
clear ddos-protection protocols ndpv6 neighbor-advertisement states
<clear-ddos-ndpv6-neighb-adv-states>
clear ddos-protection protocols ndpv6 neighbor-advertisement statistics
<clear-ddos-ndpv6-neighb-adv-statistics>
clear ddos-protection protocols ndpv6 neighbor-solicitation
clear ddos-protection protocols ndpv6 neighbor-solicitation culprit-flows
<clear-ddos-ndpv6-neighb-sol-flows>
clear ddos-protection protocols ndpv6 neighbor-solicitation states
<clear-ddos-ndpv6-neighb-sol-states>
clear ddos-protection protocols ndpv6 neighbor-solicitation statistics
<clear-ddos-ndpv6-neighb-sol-statistics>
```

```
clear ddos-protection protocols ndpv6 redirect
clear ddos-protection protocols ndpv6 redirect culprit-flows
<clear-ddos-ndpv6-redirect-flows>
clear ddos-protection protocols ndpv6 redirect states
<clear-ddos-ndpv6-redirect-states>
clear ddos-protection protocols ndpv6 redirect statistics
<clear-ddos-ndpv6-redirect-statistics>
clear ddos-protection protocols ndpv6 router-advertisement
clear ddos-protection protocols ndpv6 router-advertisement culprit-flows
<clear-ddos-ndpv6-router-adv-flows>
clear ddos-protection protocols ndpv6 router-advertisement states
<clear-ddos-ndpv6-router-adv-states>
clear ddos-protection protocols ndpv6 router-advertisement statistics
<clear-ddos-ndpv6-router-adv-statistics>
clear ddos-protection protocols ndpv6 router-solicitation
clear ddos-protection protocols ndpv6 router-solicitation culprit-flows
<clear-ddos-ndpv6-router-sol-flows>
clear ddos-protection protocols ndpv6 router-solicitation states
<clear-ddos-ndpv6-router-sol-states>
clear ddos-protection protocols ndpv6 router-solicitation statistics
<clear-ddos-ndpv6-router-sol-statistics>
clear ddos-protection protocols ndpv6 states
clear ddos-protection protocols ndpv6 statistics
clear ddos-protection protocols nonucast-switch
clear ddos-protection protocols nonucast-switch aggregate
clear ddos-protection protocols nonucast-switch aggregate culprit-flows
<clear-ddos-nonucast-switch-aggregate-flows>
clear ddos-protection protocols nonucast-switch aggregate states
<clear-ddos-nonucast-switch-aggregate-states>
clear ddos-protection protocols nonucast-switch aggregate statistics
<clear-ddos-nonucast-switch-aggregate-statistics>
clear ddos-protection protocols nonucast-switch culprit-flows
<clear-ddos-nonucast-switch-flows>
clear ddos-protection protocols nonucast-switch states
<clear-ddos-nonucast-switch-states>
clear ddos-protection protocols nonucast-switch statistics
<clear-ddos-nonucast-switch-statistics>
clear ddos-protection protocols ntp aggregate
clear ddos-protection protocols ntp aggregate states
clear-ddos-ntp-aggregate-states
clear ddos-protection protocols ntp aggregate statistics
clear ddos-protection protocols ntp culprit-flows
clear ddos-protection protocols ntp states
```

```
clear-ddos-ntp-states
clear ddos-protection protocols ntp statistics
clear-ddos-ntp-statistics
clear ddos-protection protocols oam-cfm
clear ddos-protection protocols oam-cfm aggregate
clear ddos-protection protocols oam-cfm aggregate culprit-flows
<clear-ddos-oam-cfm-aggregate-flows>
clear ddos-protection protocols oam-cfm aggregate states
<clear-ddos-oam-cfm-aggregate-states>
clear ddos-protection protocols oam-cfm aggregate statistics
<clear-ddos-oam-cfm-aggregate-statistics>
clear ddos-protection protocols oam-cfm culprit-flows
<clear-ddos-oam-cfm-flows>
clear ddos-protection protocols oam-cfm states
<clear-ddos-oam-cfm-states>
clear ddos-protection protocols oam-cfm statistics
<clear-ddos-oam-cfm-statistics>
clear ddos-protection protocols oam-lfm
clear ddos-protection protocols oam-lfm aggregate
clear ddos-protection protocols oam-lfm aggregate states
clear-ddos-oam-lfm-aggregate-states
clear ddos-protection protocols oam-lfm aggregate statistics
clear-ddos-oam-lfm-aggregate-statistics
clear ddos-protection protocols oam-lfm states
clear-ddos-oam-lfm-states
clear ddos-protection protocols oam-lfm statistics
clear-ddos-oam-lfm-statistics
clear ddos-protection protocols ospf
clear ddos-protection protocols ospf aggregate
clear ddos-protection protocols ospf aggregate culprit-flows
clear ddos-protection protocols ospf aggregate states
clear-ddos-ospf-aggregate-states
clear ddos-protection protocols ospf aggregate statistics
clear-ddos-ospf-aggregate-statistics
clear ddos-protection protocols ospf states
clear ddos-protection protocols ospf statistics
clear ddos-protection protocols ospf-hello
clear ddos-protection protocols ospf-hello aggregate
clear ddos-protection protocols ospf-hello aggregate culprit-flows
<clear-ddos-ospf-hello-aggregate-flows>
clear ddos-protection protocols ospf-hello aggregate states
<clear-ddos-ospf-hello-aggregate-states>
clear ddos-protection protocols ospf-hello aggregate statistics
```

```
<clear-ddos-ospf-hello-aggregate-statistics>
clear ddos-protection protocols ospf-hello culprit-flows
<clear-ddos-ospf-hello-flows>
clear ddos-protection protocols ospf-hello states
<clear-ddos-ospf-hello-states>
clear ddos-protection protocols ospf-hello statistics
<clear-ddos-ospf-hello-statistics>
clear ddos-protection protocols ospfv3v6
clear ddos-protection protocols ospfv3v6 aggregate
clear ddos-protection protocols ospfv3v6 aggregate culprit-flows
clear ddos-protection protocols ospfv3v6 aggregate states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear ddos-protection protocols ospfv3v6 states
clear ddos-protection protocols ospfv3v6 statistics
clear-ddos-ldp-states
<clear-ddos-ldp-states>
clear ddos-protection protocols ldp-hello
clear ddos-protection protocols ldp-hello aggregate
clear ddos-protection protocols ldp-hello aggregate culprit-flows
<clear-ddos-ldp-hello-aggregate-flows>
clear ddos-protection protocols ldp-hello aggregate states
<clear-ddos-ldp-hello-aggregate-states>
clear ddos-protection protocols ldp-hello aggregate statistics
<clear-ddos-ldp-hello-aggregate-statistics>
clear ddos-protection protocols ldp-hello culprit-flows
<clear-ddos-ldp-hello-flows>
clear ddos-protection protocols ldp-hello states
<clear-ddos-ldp-hello-states>
clear ddos-protection protocols ldp-hello statistics
<clear-ddos-ldp-hello-statistics>
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-protection protocols multihop-bfd
clear ddos-protection protocols multihop-bfd aggregate
clear ddos-protection protocols multihop-bfd aggregate culprit-flows
<clear-ddos-mhop-bfd-aggregate-flows>
clear ddos-protection protocols multihop-bfd aggregate states
<clear-ddos-mhop-bfd-aggregate-states>
clear ddos-protection protocols multihop-bfd aggregate statistics
<clear-ddos-mhop-bfd-aggregate-statistics>
clear ddos-protection protocols multihop-bfd culprit-flows
<clear-ddos-mhop-bfd-flows>
clear ddos-protection protocols multihop-bfd states
<clear-ddos-mhop-bfd-states>
clear ddos-protection protocols multihop-bfd statistics
<clear-ddos-mhop-bfd-statistics>
clear-ddos-mvrp-aggregate-states
clear-ddos-mvrp-aggregate-statistics
clear-ddos-mvrp-states
clear-ddos-mvrp-statistics
clear-ddos-ntp-aggregate-states
clear-ddos-ntp-aggregate-statistics
clear-ddos-ntp-states
clear-ddos-ntp-statistics
clear-ddos-oam-lfm-aggregate-states
clear-ddos-oam-lfm-aggregate-statistics
clear-ddos-oam-lfm-states
clear-ddos-oam-lfm-statistics
clear-ddos-ospf-aggregate-states
clear-ddos-ospf-aggregate-statistics
clear-ddos-ospf-states
clear-ddos-ospf-statistics
clear-ddos-ospfv3v6-aggregate-states
clear ddos-protection protocols ospfv3v6 aggregate statistics
clear-ddos-ospfv3v6-aggregate-statistics
clear ddos-protection protocols ospfv3v6 states
clear-ddos-ospfv3v6-states
 clear ddos-protection protocols pimv6
 clear-ddos-pim-statistics
clear ddos-protection protocols pim-ctrl
clear ddos-protection protocols pim-ctrl aggregate
clear ddos-protection protocols pim-ctrl aggregate culprit-flows
<clear-ddos-pim-ctrl-aggregate-flows>
clear ddos-protection protocols pim-ctrl aggregate states
<clear-ddos-pim-ctrl-aggregate-states>
```

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

```
clear ddos-protection protocols pimv6 aggregate
clear ddos-protection protocols pimv6 aggregate culprit-flows
clear ddos-protection protocols pimv6 aggregate states
clear ddos-protection protocols pimv6 aggregate statistics
clear ddos-protection protocols pimv6 states
clear ddos-protection protocols pimv6 statistics
clear ddos-protection protocols pkt-inject
clear ddos-protection protocols pkt-inject aggregate
clear ddos-protection protocols pkt-inject aggregate culprit-flows
<clear-ddos-pkt-inject-aggregate-flows>
clear ddos-protection protocols pkt-inject aggregate states
<clear-ddos-pkt-inject-aggregate-states>
clear ddos-protection protocols pkt-inject aggregate statistics
<clear-ddos-pkt-inject-aggregate-statistics>
clear ddos-protection protocols pkt-inject culprit-flows
<clear-ddos-pkt-inject-flows>
clear ddos-protection protocols pkt-inject states
<clear-ddos-pkt-inject-states>
clear ddos-protection protocols pkt-inject statistics
<clear-ddos-pkt-inject-statistics>clear ddos-protection protocols pmvrp
clear ddos-protection protocols pmvrp aggregate
clear ddos-protection protocols pmvrp aggregate states
clear-ddos-pmvrp-aggregate-states
clear ddos-protection protocols pmvrp aggregate statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols pmvrp states
clear-ddos-pmvrp-states
clear ddos-protection protocols pmvrp statistics
clear-ddos-pmvrp-statistics
clear ddos-protection protocols pos
clear ddos-protection protocols pos aggregate
clear ddos-protection protocols pos aggregate states
clear-ddos-pos-aggregate-states
clear ddos-protection protocols pos aggregate statistics
clear-ddos-pos-aggregate-statistics
clear ddos-protection protocols pos states
clear-ddos-pos-states
```

```
clear ddos-protection protocols pos statistics
clear-ddos-pos-statistics
clear ddos-protection protocols ppp
clear ddos-protection protocols ppp aggregate
clear ddos-protection protocols ppp aggregate states
clear-ddos-ppp-aggregate-states
clear ddos-protection protocols ppp aggregate statistics
clear-ddos-ppp-aggregate-statistics
clear ddos-protection protocols ppp authentication
clear ddos-protection protocols ppp authentication states
clear-ddos-ppp-auth-states
clear ddos-protection protocols ppp authentication statistics
clear-ddos-ppp-auth-statistics
clear ddos-protection protocols ppp ipcp
clear ddos-protection protocols ppp ipcp states
clear-ddos-ppp-ipcp-states
clear ddos-protection protocols ppp ipcp statistics
clear-ddos-ppp-ipcp-statistics
clear ddos-protection protocols ppp ipv6cp
clear ddos-protection protocols ppp ipv6cp states
clear-ddos-ppp-ipv6cp-states
clear ddos-protection protocols ppp ipv6cp statistics
clear-ddos-ppp-ipv6cp-statistics
clear ddos-protection protocols ppp isis
clear ddos-protection protocols ppp isis states
clear-ddos-ppp-isis-states
clear ddos-protection protocols ppp isis statistics
clear-ddos-ppp-isis-statistics
clear ddos-protection protocols ppp lcp
clear ddos-protection protocols ppp lcp states
clear-ddos-ppp-lcp-states
clear ddos-protection protocols ppp lcp statistics
clear-ddos-ppp-lcp-statistics
clear ddos-protection protocols ppp mplscp
clear ddos-protection protocols ppp mplscp states
clear-ddos-ppp-mplscp-states
clear ddos-protection protocols ppp mplscp statistics
clear-ddos-ppp-mplscp-statistics
clear ddos-protection protocols ppp states
clear-ddos-ppp-states
clear ddos-protection protocols ppp statistics
clear-ddos-ppp-statistics
clear ddos-protection protocols ppp unclassified
```

```
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
<clear-ddos-ppp-unclass-statistics>
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
clear ddos-protection protocols pppoe aggregate states
clear-ddos-pppoe-aggregate-states
clear ddos-protection protocols pppoe aggregate statistics
clear-ddos-pppoe-aggregate-statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear-ddos-pppoe-padi-states
clear ddos-protection protocols pppoe padi statistics
clear-ddos-pppoe-padi-statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear-ddos-pppoe-padm-states
clear ddos-protection protocols pppoe padm statistics
clear-ddos-pppoe-padm-statistics
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
clear-ddos-pppoe-padn-states
clear ddos-protection protocols pppoe padn statistics
clear-ddos-pppoe-padn-statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear-ddos-pppoe-pado-states
clear ddos-protection protocols pppoe pado statistics
clear-ddos-pppoe-pado-statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear-ddos-pppoe-padr-states
clear ddos-protection protocols pppoe padr statistics
clear-ddos-pppoe-padr-statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear-ddos-pppoe-pads-states
clear ddos-protection protocols pppoe pads statistics
clear-ddos-pppoe-pads-statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear-ddos-pppoe-padt-states
clear ddos-protection protocols pppoe padt statistics
```

```
clear-ddos-pppoe-padt-statistics
clear ddos-protection protocols pppoe states
clear-ddos-pppoe-states
clear ddos-protection protocols pppoe statistics
clear-ddos-pppoe-statistics
clear ddos-protection protocols proto-802-1x
clear ddos-protection protocols proto-802-1x aggregate
clear ddos-protection protocols proto-802-1x aggregate culprit-flows
<clear-ddos-8021x-aggregate-flows>
clear ddos-protection protocols proto-802-1x aggregate states
<clear-ddos-8021x-aggregate-states>
clear ddos-protection protocols proto-802-1x aggregate statistics
<clear-ddos-8021x-aggregate-statistics>
clear ddos-protection protocols proto-802-1x culprit-flows
<clear-ddos-8021x-flows>
clear ddos-protection protocols proto-802-1x states
<clear-ddos-8021x-states>
clear ddos-protection protocols proto-802-1x statistics
<clear-ddos-8021x-statistics>
clear ddos-protection protocols ptp
clear ddos-protection protocols ptp aggregate
clear ddos-protection protocols ptp aggregate states
clear-ddos-ptp-aggregate-states
clear ddos-protection protocols ptp aggregate statistics
clear-ddos-ptp-aggregate-statistics
clear ddos-protection protocols ptp states
clear-ddos-ptp-states
clear ddos-protection protocols ptp statistics
clear-ddos-ptp-statistics
clear ddos-protection protocols ptpv6
clear ddos-protection protocols ptpv6 aggregate
clear ddos-protection protocols ptpv6 aggregate culprit-flows
<clear-ddos-ptpv6-aggregate-flows>
clear ddos-protection protocols ptpv6 aggregate states
<clear-ddos-ptpv6-aggregate-states>
clear ddos-protection protocols ptpv6 aggregate statistics
<clear-ddos-ptpv6-aggregate-statistics>
clear ddos-protection protocols ptpv6 culprit-flows
<clear-ddos-ptpv6-flows>
clear ddos-protection protocols ptpv6 states
<clear-ddos-ptpv6-states>
clear ddos-protection protocols ptpv6 statistics
<clear-ddos-ptpv6-statistics>
```

```
clear ddos-protection protocols pvstp
clear ddos-protection protocols pvstp aggregate
clear ddos-protection protocols pvstp aggregate states
clear-ddos-pvstp-aggregate-states
clear ddos-protection protocols pvstp aggregate statistics
clear-ddos-pvstp-aggregate-statistics
clear ddos-protection protocols pvstp states
clear-ddos-pvstp-states
clear ddos-protection protocols pvstp statistics
clear-ddos-pvstp-statistics
clear ddos-protection protocols radius
clear ddos-protection protocols radius accounting
clear ddos-protection protocols radius accounting states
clear-ddos-radius-account-states
clear ddos-protection protocols radius accounting statistics
clear-ddos-radius-account-statistics
clear ddos-protection protocols radius aggregate
clear ddos-protection protocols radius aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius aggregate statistics
clear-ddos-radius-aggregate-statistics
clear ddos-protection protocols radius authorization
clear ddos-protection protocols radius authorization states
clear ddos-protection protocols radius authorization statistics
clear-ddos-ospfv3v6-statistics
clear-ddos-pfe-alive-aggregate-states
clear-ddos-pfe-alive-aggregate-statistics
clear-ddos-pfe-alive-states
clear-ddos-pfe-alive-statistics
clear-ddos-pim-aggregate-states
clear-ddos-pim-aggregate-statistics
clear-ddos-pim-states
clear-ddos-pmvrp-aggregate-states
clear-ddos-pmvrp-aggregate-statistics
clear-ddos-pmvrp-states
clear-ddos-pmvrp-statistics
clear-ddos-pos-aggregate-states
clear-ddos-pos-aggregate-statistics
clear-ddos-pos-states
clear-ddos-pos-statistics
clear-ddos-ppp-aggregate-states
clear-ddos-ppp-aggregate-statistics
clear-ddos-ppp-auth-states
```

```
clear-ddos-ppp-ipcp-states
clear-ddos-ppp-ipcp-statistics
clear-ddos-ppp-ipv6cp-states
clear-ddos-ppp-ipv6cp-statistics
clear-ddos-ppp-isis-states
clear-ddos-ppp-isis-statistics
clear-ddos-ppp-lcp-states
clear-ddos-ppp-lcp-statistics
clear-ddos-ppp-mplscp-states
clear-ddos-ppp-mplscp-statistics
clear-ddos-pppoe-aggregate-states
clear-ddos-pppoe-aggregate-statistics
clear-ddos-pppoe-padi-states
clear-ddos-pppoe-padi-statistics
clear-ddos-pppoe-padm-states
clear-ddos-pppoe-padm-statistics
clear-ddos-pppoe-padn-states
clear-ddos-pppoe-padn-statistics
clear-ddos-pppoe-pado-states
clear-ddos-pppoe-pado-statistics
clear-ddos-pppoe-padr-states
clear-ddos-pppoe-padr-statistics
clear-ddos-pppoe-pads-states
clear-ddos-pppoe-pads-statistics
clear-ddos-pppoe-padt-states
clear-ddos-pppoe-padt-statistics
clear-ddos-pppoe-states
clear-ddos-pppoe-statistics
clear-ddos-ppp-states
clear-ddos-ppp-statistics
clear-ddos-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-protection protocols radius authorization statistics
clear-ddos-radius-auth-statistics
clear ddos-protection protocols pmvrp culprit-flows
clear ddos-protection protocols radius server
clear ddos-protection protocols radius server states
clear-ddos-radius-server-states
clear ddos-protection protocols radius server statistics
clear-ddos-radius-server-statistics
clear ddos-protection protocols radius states
clear-ddos-radius-states
clear ddos-protection protocols radius statistics
clear-ddos-radius-statistics
clear ddos-protection protocols redirect
clear ddos-protection protocols redirect aggregate
clear ddos-protection protocols redirect aggregate states
clear-ddos-redirect-aggregate-states
clear ddos-protection protocols redirect aggregate statistics
clear-ddos-redirect-aggregate-statistics
clear ddos-protection protocols redirect states
clear-ddos-redirect-states
clear ddos-protection protocols redirect statistics
clear-ddos-redirect-statistics
clear ddos-protection protocols reject
clear ddos-protection protocols reject aggregate
clear ddos-protection protocols reject aggregate states
clear ddos-protection protocols reject aggregate statistics
clear ddos-protection protocols reject states
clear ddos-protection protocols reject statistics
clear ddos-protection protocols rip
clear ddos-protection protocols rip aggregate
clear ddos-protection protocols rip aggregate states
clear-ddos-rip-aggregate-states
clear ddos-protection protocols rip aggregate statistics
clear-ddos-rip-aggregate-statistics
clear ddos-protection protocols rip states
clear-ddos-rip-states
clear ddos-protection protocols rip statistics
clear-ddos-rip-statistics
clear ddos-protection protocols ripv6
clear ddos-protection protocols ripv6 aggregate
clear ddos-protection protocols ripv6 aggregate states
clear-ddos-ripv6-aggregate-states
clear ddos-protection protocols ripv6 aggregate statistics
```

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

```
<clear-ddos-sample-sflow-flows>
clear ddos-protection protocols sample sflow states
<clear-ddos-sample-sflow-states>
clear ddos-protection protocols sample sflow statistics
<clear-ddos-sample-sflow-statistics>
clear ddos-protection protocols sample states
<clear-ddos-sample-states>
clear ddos-protection protocols sample statistics
<clear-ddos-sample-statistics>
clear ddos-protection protocols sample syslog
clear ddos-protection protocols sample syslog culprit-flows
clear ddos-protection protocols sample syslog states
<clear-ddos-sample-syslog-states>
clear ddos-protection protocols sample syslog statistics
<clear-ddos-sample-syslog-statistics>
clear ddos-protection protocols sample tap
clear ddos-protection protocols sample tap states
clear ddos-protection protocols sample-dest
clear ddos-protection protocols sample-dest aggregate
clear ddos-protection protocols sample-dest aggregate culprit-flows
<clear-ddos-sample-dest-aggregate-flows>
clear ddos-protection protocols sample-dest aggregate states
<clear-ddos-sample-dest-aggregate-states>
clear ddos-protection protocols sample-dest aggregate statistics
 <clear-ddos-sample-dest-aggregate-statistics>
clear ddos-protection protocols sample-dest culprit-flows
<clear-ddos-sample-dest-flows>
clear ddos-protection protocols sample-dest states
<clear-ddos-sample-dest-states>
clear ddos-protection protocols sample-dest statistics
<clear-ddos-sample-dest-statistics>
clear ddos-protection protocols sample-source
clear ddos-protection protocols sample-source aggregate
clear ddos-protection protocols sample-source aggregate culprit-flows
<clear-ddos-sample-source-aggregate-flows>
clear ddos-protection protocols sample-source aggregate states
<clear-ddos-sample-source-aggregate-states>
clear ddos-protection protocols sample-source aggregate statistics
<clear-ddos-sample-source-aggregate-statistics>
clear ddos-protection protocols sample-source culprit-flows
<clear-ddos-sample-source-flows>
clear ddos-protection protocols sample-source states
<clear-ddos-sample-source-states>
```

```
clear ddos-protection protocols sample-source statistics
 <clear-ddos-sample-source-statistics>
clear ddos-protection protocols sample tap statistics
<clear-ddos-sample-tap-statistics>
clear ddos-protection protocols services
clear ddos-protection protocols services aggregate
clear ddos-protection protocols services aggregate states
clear-ddos-services-aggregate-states
clear ddos-protection protocols services aggregate statistics
clear ddos-protection protocols services bsdt
clear ddos-protection protocols services bsdt culprit-flows
<clear-ddos-services-BSDT-flows>
clear ddos-protection protocols services bsdt states
<clear-ddos-services-BSDT-states>
clear ddos-protection protocols services bsdt statistics
<clear-ddos-services-BSDT-statistics>
clear ddos-protection protocols services culprit-flows
<clear-ddos-services-flows>
clear ddos-protection protocols services packet
clear ddos-protection protocols services packet culprit-flows
<clear-ddos-services-packet-flows>
clear ddos-protection protocols services packet states
<clear-ddos-services-packet-states>
clear ddos-protection protocols services packet statistics
<clear-ddos-services-packet-statistics>
clear ddos-protection protocols services states
clear-ddos-services-states
clear ddos-protection protocols services statistics
clear-ddos-services-statistics
clear ddos-protection protocols snmp
clear ddos-protection protocols snmp aggregate
clear ddos-protection protocols snmp aggregate states
clear-ddos-snmp-aggregate-states
clear ddos-protection protocols snmp aggregate statistics
clear ddos-protection protocols snmp culprit-flows
clear ddos-protection protocols snmp states
clear-ddos-snmp-states
clear ddos-protection protocols snmp statistics
clear-ddos-snmp-statistics
clear ddos-protection protocols snmpv6
clear ddos-protection protocols snmpv6 aggregate
clear ddos-protection protocols snmpv6 aggregate states
clear-ddos-snmpv6-aggregate-states
```

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

```
clear-ddos-tacacs-aggregate-states
clear ddos-protection protocols tacacs aggregate statistics
clear-ddos-tacacs-aggregate-statistics
clear ddos-protection protocols tacacs states
clear-ddos-tacacs-states
clear ddos-protection protocols tacacs statistics
clear-ddos-tacacs-statistics
clear ddos-protection protocols tcc
clear ddos-protection protocols tcc aggregate
clear ddos-protection protocols tcc aggregate culprit-flows
<clear-ddos-tcc-aggregate-flows>
clear ddos-protection protocols tcc aggregate states
<clear-ddos-tcc-aggregate-states>
clear ddos-protection protocols tcc aggregate statistics
<clear-ddos-tcc-aggregate-statistics>
clear ddos-protection protocols tcc culprit-flows
<clear-ddos-tcc-flows>
clear ddos-protection protocols tcc ethernet-tcc
clear ddos-protection protocols tcc ethernet-tcc culprit-flows
<clear-ddos-tcc-ethernet-tcc-flows>
clear ddos-protection protocols tcc ethernet-tcc states
<clear-ddos-tcc-ethernet-tcc-states>
clear ddos-protection protocols tcc ethernet-tcc statistics
<clear-ddos-tcc-ethernet-tcc-statistics>
clear ddos-protection protocols tcc iso-tcc
clear ddos-protection protocols tcc iso-tcc culprit-flows
<clear-ddos-tcc-iso-tcc-flows>
clear ddos-protection protocols tcc iso-tcc states
<clear-ddos-tcc-iso-tcc-states>
clear ddos-protection protocols tcc iso-tcc statistics
<clear-ddos-tcc-iso-tcc-statistics>
clear ddos-protection protocols tcc states
<clear-ddos-tcc-states>
clear ddos-protection protocols tcc statistics
<clear-ddos-tcc-statistics>
clear ddos-protection protocols tcc unclassified
clear ddos-protection protocols tcc unclassified culprit-flows
<clear-ddos-tcc-unclass-flows>
clear ddos-protection protocols tcc unclassified states
<clear-ddos-tcc-unclass-states>
clear ddos-protection protocols tcc unclassified statistics
<clear-ddos-tcc-unclass-statistics>
clear ddos-protection protocols tcp-flags
```

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

```
clear-ddos-telnetv6-states
clear ddos-protection protocols telnetv6 statistics
clear-ddos-telnetv6-statistics
clear ddos-protection protocols ttl
clear ddos-protection protocols ttl aggregate
clear ddos-protection protocols ttl aggregate culprit-flows
clear ddos-protection protocols ttl aggregate states
clear-ddos-ttl-aggregate-states
clear ddos-protection protocols ttl aggregate statistics
clear-ddos-ttl-aggregate-statistics
clear ddos-protection protocols ttl states
clear-ddos-ttl-states
clear ddos-protection protocols ttl statistics
clear-ddos-ttl-statistics
clear ddos-protection protocols tunnel-fragment
clear ddos-protection protocols tunnel-fragment aggregate
clear ddos-protection protocols tunnel-fragment aggregate states
clear-ddos-tun-frag-aggregate-states
clear ddos-protection protocols tunnel-fragment aggregate statistics
clear-ddos-tun-frag-aggregate-statistics
clear ddos-protection protocols tunnel-fragment states
clear-ddos-tun-frag-states
clear ddos-protection protocols tunnel-fragment statistics
clear-ddos-tun-frag-statistics
clear ddos-protection protocols unclassified
clear ddos-protection protocols unclassified aggregate
clear ddos-protection protocols unclassified aggregate states
clear ddos-protection protocols unclassified aggregate statistics
clear ddos-protection protocols unclassified control-layer2
clear ddos-protection protocols unclassified control-layer2 culprit-flows
clear ddos-protection protocols unclassified control-layer2 states
clear ddos-protection protocols unclassified control-layer2 statistics
clear ddos-protection protocols unclassified control-v4
clear ddos-protection protocols unclassified control-v4 culprit-flows
clear ddos-protection protocols unclassified control-v4 states
clear ddos-protection protocols unclassified control-v4 statistics
clear ddos-protection protocols unclassified control-v6
clear ddos-protection protocols unclassified control-v6 culprit-flows
clear ddos-protection protocols unclassified control-v6 states
clear ddos-protection protocols unclassified control-v6 statistics
clear ddos-protection protocols unclassified filter-v4 culprit-flows
clear ddos-protection protocols unclassified filter-v4 states
clear ddos-protection protocols unclassified filter-v4 statistics
```

```
clear ddos-protection protocols unclassified filter-v6
clear ddos-protection protocols unclassified filter-v6 culprit-flows
clear ddos-protection protocols unclassified filter-v6 states
clear ddos-protection protocols unclassified filter-v6 statistics
clear ddos-protection protocols unclassified fw-host
clear ddos-protection protocols unclassified fw-host culprit-flows
<clear-ddos-uncls-fw-host-flows>
clear ddos-protection protocols unclassified fw-host states
<clear-ddos-uncls-fw-host-states>
clear ddos-protection protocols unclassified fw-host statistics
<clear-ddos-uncls-fw-host-statistics>
clear ddos-protection protocols unclassified host-route-v4
clear ddos-protection protocols unclassified host-route-v4 culprit-flows
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 statistics
clear ddos-protection protocols unclassified host-route-v6
clear ddos-protection protocols unclassified host-route-v6 culprit-flows
clear ddos-protection protocols unclassified host-route-v6 states
clear ddos-protection protocols unclassified host-route-v6 statistics
clear ddos-protection protocols unclassified mcast-copy
clear ddos-protection protocols unclassified mcast-copy culprit-flows
<clear-ddos-uncls-mcast-copy-flows>
clear ddos-protection protocols unclassified mcast-copy states
<clear-ddos-uncls-mcast-copy-states>
clear ddos-protection protocols unclassified mcast-copy statistics
<clear-ddos-uncls-mcast-copy-statistics>
clear ddos-protection protocols unknown-l2mc
clear ddos-protection protocols unknown-l2mc aggregate
clear ddos-protection protocols unknown-l2mc aggregate culprit-flows
<clear-ddos-unknown-l2mc-aggregate-flows>
clear ddos-protection protocols unknown-l2mc aggregate states
 <clear-ddos-unknown-l2mc-aggregate-states>
clear ddos-protection protocols unknown-l2mc aggregate statistics
<clear-ddos-unknown-l2mc-aggregate-statistics>
 clear ddos-protection protocols unknown-l2mc culprit-flows
<clear-ddos-unknown-l2mc-flows>
clear ddos-protection protocols unknown-l2mc states
<clear-ddos-unknown-l2mc-states>
 clear ddos-protection protocols unknown-l2mc statistics
<clear-ddos-unknown-l2mc-statistics>
clear ddos-protection protocols urpf-fail
clear ddos-protection protocols urpf-fail aggregate
```

```
clear ddos-protection protocols urpf-fail aggregate culprit-flows
<clear-ddos-urpf-fail-aggregate-flows>
clear ddos-protection protocols urpf-fail aggregate states
<clear-ddos-urpf-fail-aggregate-states>
 clear ddos-protection protocols urpf-fail aggregate statistics
<clear-ddos-urpf-fail-aggregate-statistics>
clear ddos-protection protocols urpf-fail culprit-flows
<clear-ddos-urpf-fail-flows>
clear ddos-protection protocols urpf-fail states
<clear-ddos-urpf-fail-states>
clear ddos-protection protocols urpf-fail statistics
<clear-ddos-urpf-fail-statistics>
clear ddos-protection protocols vcipc-udp
clear ddos-protection protocols vcipc-udp aggregate
clear ddos-protection protocols vcipc-udp aggregate culprit-flows
 <clear-ddos-vcipc-udp-aggregate-flows>
 clear ddos-protection protocols vcipc-udp aggregate states
<clear-ddos-vcipc-udp-aggregate-states>
clear ddos-protection protocols vcipc-udp aggregate statistics
<clear-ddos-vcipc-udp-aggregate-statistics>
 clear ddos-protection protocols vcipc-udp culprit-flows
<clear-ddos-vcipc-udp-flows>
clear ddos-protection protocols vcipc-udp states
<clear-ddos-vcipc-udp-states>
<clear-ddos-vcipc-udp-statistics>
clear ddos-protection protocols unclassified other
clear ddos-protection protocols unclassified other culprit-flows
clear ddos-protection protocols unclassified other states
clear ddos-protection protocols unclassified other statistics
clear ddos-protection protocols unclassified resolve-v4
clear ddos-protection protocols unclassified resolve-v4 culprit-flows
clear ddos-protection protocols unclassified resolve-v4 states
clear ddos-protection protocols unclassified resolve-v4 statistics
clear ddos-protection protocols unclassified resolve-v6
clear ddos-protection protocols unclassified resolve-v6 culprit-flows
clear ddos-protection protocols unclassified resolve-v6 states
clear ddos-protection protocols unclassified resolve-v6 statistics
clear ddos-protection protocols unclassified states
clear ddos-protection protocols unclassified statistics
<clear-ddos-uncls-statistics>
clear ddos-protection protocols virtual-chassis
clear ddos-protection protocols virtual-chassis aggregate
clear ddos-protection protocols virtual-chassis aggregate culprit-flows
```

```
clear ddos-protection protocols virtual-chassis aggregate states
clear-ddos-protocols-states
clear-ddos-protocols-statistics
clear-ddos-radius-server-states
clear-ddos-radius-server-statistics
clear-ddos-radius-states
clear-ddos-radius-statistics
clear ddos-protection protocols re-services
 clear ddos-protection protocols re-services aggregate
clear ddos-protection protocols re-services aggregate culprit-flows
<clear-ddos-re-services-aggregate-flows>
clear ddos-protection protocols re-services aggregate states
<clear-ddos-re-services-aggregate-states>
clear ddos-protection protocols re-services aggregate statistics
<clear-ddos-re-services-aggregate-statistics>
clear ddos-protection protocols re-services captive-portal
clear ddos-protection protocols re-services captive-portal culprit-flows
<clear-ddos-re-services-captive-portal-flows>
clear ddos-protection protocols re-services captive-portal states
<clear-ddos-re-services-captive-portal-states>
clear ddos-protection protocols re-services captive-portal statistics
<clear-ddos-re-services-captive-portal-statistics>
clear ddos-protection protocols re-services culprit-flows
<clear-ddos-re-services-flows>
clear ddos-protection protocols re-services states
<clear-ddos-re-services-states>
clear ddos-protection protocols re-services statistics
<clear-ddos-re-services-statistics>
clear ddos-protection protocols re-services-v6
clear ddos-protection protocols re-services-v6 aggregate
clear ddos-protection protocols re-services-v6 aggregate culprit-flows
<clear-ddos-re-services-v6-aggregate-flows>
clear ddos-protection protocols re-services-v6 aggregate states
<clear-ddos-re-services-v6-aggregate-states>
clear ddos-protection protocols re-services-v6 aggregate statistics
<clear-ddos-re-services-v6-aggregate-statistics>
clear ddos-protection protocols re-services-v6 captive-portal
clear ddos-protection protocols re-services-v6 captive-portal culprit-flows
<clear-ddos-re-services-v6-captive-portal-v6-flows>
clear ddos-protection protocols re-services-v6 captive-portal states
<clear-ddos-re-services-v6-captive-portal-v6-states>
clear ddos-protection protocols re-services-v6 captive-portal statistics
<clear-ddos-re-services-v6-captive-portal-v6-statistics>
```

```
clear ddos-protection protocols re-services-v6 culprit-flows
<clear-ddos-re-services-v6-flows>
clear ddos-protection protocols re-services-v6 states
<clear-ddos-re-services-v6-states>
clear ddos-protection protocols re-services-v6 statistics
<clear-ddos-re-services-v6-statistics>
clear-ddos-redirect-aggregate-states
clear-ddos-redirect-states
clear-ddos-redirect-statistics
clear-ddos-rip-aggregate-states
clear-ddos-rip-aggregate-statistics
clear-ddos-rip-states
clear-ddos-rip-statistics
clear-ddos-ripv6-aggregate-states
clear-ddos-ripv6-aggregate-statistics
clear-ddos-ripv6-states
clear-ddos-ripv6-statistics
clear-ddos-rsvp-aggregate-states
clear-ddos-rsvp-aggregate-statistics
clear-ddos-rsvp-states
clear-ddos-rsvp-statistics
clear-ddos-rsvpv6-aggregate-states
clear-ddos-rsvpv6-aggregate-statistics
clear-ddos-rsvpv6-states
clear-ddos-rsvpv6-statistics
clear-ddos-services-aggregate-states
clear-ddos-services-aggregate-statistics
clear-ddos-services-states
clear-ddos-services-statistics
clear-ddos-snmp-aggregate-states
clear-ddos-snmp-aggregate-statistics
clear-ddos-snmp-states
clear-ddos-snmp-statistics
clear-ddos-snmpv6-aggregate-states
clear-ddos-snmpv6-aggregate-statistics
clear-ddos-snmpv6-states
clear-ddos-snmpv6-statistics
clear-ddos-ssh-aggregate-states
clear-ddos-ssh-aggregate-statistics
clear-ddos-ssh-states
clear-ddos-ssh-statistics
clear-ddos-sshv6-aggregate-states
clear-ddos-sshv6-aggregate-statistics
```

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

```
clear-ddos-ttl-aggregate-statistics
clear-ddos-ttl-states
clear-ddos-ttl-statistics
clear-ddos-tun-frag-aggregate-states
clear-ddos-tun-frag-aggregate-statistics
clear-ddos-tun-frag-states
clear-ddos-tun-frag-statistics
clear ddos-protection protocols tunnel-ka
clear ddos-protection protocols tunnel-ka aggregate
clear ddos-protection protocols tunnel-ka aggregate culprit-flows
<clear-ddos-tunnel-ka-aggregate-flows>
clear ddos-protection protocols tunnel-ka aggregate states
<clear-ddos-tunnel-ka-aggregate-states>
clear ddos-protection protocols tunnel-ka aggregate statistics
<clear-ddos-tunnel-ka-aggregate-statistics>
clear ddos-protection protocols tunnel-ka culprit-flows
<clear-ddos-tunnel-ka-flows>
clear ddos-protection protocols tunnel-ka states
<clear-ddos-tunnel-ka-states>
clear ddos-protection protocols tunnel-ka statistics
<clear-ddos-tunnel-ka-statistics>
clear-ddos-vchassis-aggregate-states
clear ddos-protection protocols virtual-chassis aggregate statistics
clear-ddos-vchassis-aggregate-statistics
clear ddos-protection protocols virtual-chassis control-high
clear ddos-protection protocols virtual-chassis control-high states
clear-ddos-vchassis-control-hi-states
clear ddos-protection protocols virtual-chassis control-high statistics
clear-ddos-vchassis-control-hi-statistics
clear ddos-protection protocols virtual-chassis control-low
clear ddos-protection protocols virtual-chassis control-low states
clear-ddos-vchassis-control-lo-states
clear ddos-protection protocols virtual-chassis control-low statistics
clear-ddos-vchassis-control-lo-statistics
clear ddos-protection protocols virtual-chassis states
clear-ddos-vchassis-states
clear ddos-protection protocols virtual-chassis statistics
clear-ddos-vchassis-statistics
clear ddos-protection protocols virtual-chassis unclassified
clear ddos-protection protocols virtual-chassis unclassified culprit-flows
clear ddos-protection protocols virtual-chassis unclassified states
clear-ddos-vchassis-unclass-states
clear ddos-protection protocols virtual-chassis unclassified statistics
```

```
clear-ddos-vchassis-unclass-statistics
clear ddos-protection protocols virtual-chassis vc-packets
clear ddos-protection protocols virtual-chassis vc-packets states
clear-ddos-vchassis-vc-packets-states
clear ddos-protection protocols virtual-chassis vc-packets statistics
clear-ddos-vchassis-vc-packets-statistics
clear ddos-protection protocols virtual-chassis vc-ttl-errors
clear ddos-protection protocols virtual-chassis vc-ttl-errors states
clear-ddos-vchassis-vc-ttl-err-states
clear ddos-protection protocols virtual-chassis vc-ttl-errors statistics
clear-ddos-vchassis-vc-ttl-err-statistics
clear ddos-protection protocols vrrp
clear ddos-protection protocols vrrp aggregate
clear ddos-protection protocols vrrp aggregate states
clear-ddos-vrrp-aggregate-states
clear ddos-protection protocols vrrp aggregate statistics
clear ddos-protection protocols vrrp culprit-flows
clear ddos-protection protocols vrrp statistics
clear-ddos-vrrp-statistics
clear ddos-protection protocols vrrpv6
clear ddos-protection protocols vrrpv6 aggregate
clear ddos-protection protocols vrrpv6 aggregate states
clear-ddos-vrrpv6-aggregate-states
clear ddos-protection protocols vrrpv6 aggregate statistics
clear-ddos-vrrpv6-aggregate-statistics
clear ddos-protection protocols vrrpv6 states
clear-ddos-vrrpv6-states
clear ddos-protection protocols vrrpv6 statistics
clear-ddos-uncls-host-rt-v4-flows
clear-ddos-vchassis-aggregate-statistics
clear-ddos-vchassis-control-hi-states
clear-ddos-vchassis-control-hi-statistics
clear-ddos-vchassis-control-lo-states
clear-ddos-vchassis-control-lo-statistics
clear-ddos-vchassis-states
clear-ddos-vchassis-statistics
clear-ddos-vchassis-unclass-states
clear-ddos-vchassis-unclass-statistics
clear-ddos-vchassis-vc-packets-states
clear-ddos-vchassis-vc-packets-statistics
clear-ddos-vchassis-vc-ttl-err-states
clear-ddos-vchassis-vc-ttl-err-statistics
clear-ddos-vrrp-aggregate-states
```

```
clear-ddos-vrrp-aggregate-statistics
clear-ddos-vrrp-states
clear-ddos-vrrp-statistics
clear-ddos-vrrpv6-aggregate-states
clear-ddos-vrrpv6-aggregate-statistics
clear-ddos-vrrpv6-states
clear-ddos-vrrpv6-statistics
clear ddos-protection protocols vxlan
clear ddos-protection protocols vxlan aggregate
clear ddos-protection protocols vxlan aggregate culprit-flows
clear-ddos-vxlan-aggregate-flows
clear ddos-protection protocols vxlan aggregate states
<clear-ddos-vxlan-aggregate-states>
clear ddos-protection protocols vxlan aggregate statistics
<clear-ddos-vxlan-aggregate-statistics>
clear ddos-protection protocols vxlan culprit-flows
<clear-ddos-vxlan-flows>
clear ddos-protection protocols vxlan states
<clear-ddos-vxlan-states>
clear ddos-protection protocols vxlan statistics
<clear-ddos-vxlan-statistics>
clear dhcp
clear dhcp client
clear dhcp client binding
<clear-dhcp-client-binding-information>
clear dhcp client statistics
<clear-client-statistics-information>
clear dhcp proxy-client
clear dhcp proxy-client statistics
clear dhcp relay
clear dhcp relay binding
 <clear-dhcp-relay-binding-information>
clear dhcp relay binding interface
<clear-dhcp-interface-bindings>
clear dhcp relay statistics
 <clear-dhcp-relay-statistics-information>
<clear-dhcp-security-binding>
<clear-dhcp-security-binding-interface>
<clear-dhcp-security-binding-ip-address>
<clear-dhcp-security-binding-statistics>
<clear-dhcp-security-binding-vlan>
clear dhcp relay statistics bulk-leasequery-connections
<clear-dhcp-relay-bulk-leasequery-conn-statistics>
```

```
clear dhcp relay statistics leasequery
<clear-dhcp-relay-leasequery-statistics>
clear dhcp server
clear dhcp server binding
 <clear-dhcp-server-binding-information>
clear dhcp server binding interface
<clear-dhcp-server-binding-interface>
clear dhcp server statistics
 <clear-server-statistics-information>
clear dhcp statistics
<clear-dhcp-service-statistics-information>
clear dhcp-security statistics
<clear-dhcp-security-statistics>
clear dhcpv6
clear dhcpv6 client
clear dhcpv6 client binding
<clear-dhcpv6-client-binding-information>
clear dhcpv6 client statistics
<clear-dhcpv6-client-statistics-information>
clear dhcpv6 proxy-client
clear dhcpv6 proxy-client statistics
 <clear-dhcpv6-proxy-client-statistics-information>
clear dhcpv6 relay
clear dhcpv6 relay binding
clear dhcpv6 relay binding interface
clear dhcpv6 relay statistics
<clear-dhcpv6-relay-statistics-information>
clear dhcpv6 relay statistics bulk-leasequery-connections
<clear-dhcpv6-relay-bulk-leasequery-conn-statistics>
clear dhcpv6 relay statistics leasequery
<clear-dhcpv6-relay-leasequery-statistics>
clear dhcpv6 server
clear dhcpv6 server binding
<clear-dhcpv6-server-binding-information>
clear dhcpv6 server binding interface
<clear-dhcpv6-server-binding-interface>
clear dhcpv6 server statistics
<clear-dhcpv6-server-statistics-information>
clear dhcpv6 server statistics bulk-leasequery-connections
<clear-dhcpv6-server-bulk-leasequery-statistics>
clear dhcpv6 statistics
<clear-dhcpv6-service-statistics-information>
clear diameter
```

```
clear diameter function
 <clear-diameter-function>
clear diameter peer
 <clear-diameter-peer>
<clear-dhcp-binding-information>
<clear-dhcp-conflict-information>
<clear-dhcp-statistics-information>
clear system subscriber-management
clear system subscriber-management arp
<clear-subscriber-management-arp>
clear system subscriber-management arp address
<clear-subscriber-management-arp-address>
clear system subscriber-management arp interface
<clear-subscriber-management-arp-interface>
clear system subscriber-management ipv6-neighbors
<clear-subscriber-management-ipv6-neighbors>
clear system subscriber-management ipv6-neighbors address
<clear-subscriber-management-ipv6-neighbor-address>clear system subscriber-management ipv6-
neighbors interface
<clear-subscriber-management-ipv6-neighbor-interface>
clear system subscriber-management statistics
<clear-subscriber-management-statistics>
clear dot1x
clear dot1x eapol-block
clear dot1x eapol-block interface
<clear-dot1x-eapol-block-interface-session>
clear dot1x eapol-block mac-address
<clear-dot1x-eapol-block-mac-session>
clear dot1x firewall
<clear-dot1x-firewall>
clear dot1x firewall interface
<clear-dot1x-firewall-interface>
clear dot1x interface
 <clear-dot1x-interface-session>
clear dot1x mac-address
 <clear-dot1x-mac-session>
clear dot1x statistics
<clear-dot1x-statistics>
clear dot1x statistics interface
<clear-dot1x-statistics-interface>
clear error
clear error bpdu
clear error bpdu interface
```

```
<clear-bpdu-error>
clear error loop-detect
clear error loop-detect interface
<clear-loop-detect-error>
clear error mac-rewrite
clear error mac-rewrite interface
 <clear-mac-rewrite-error>
clear esis
clear esis adjacency
<clear-esis-adjacency>
clear esis statistics
<clear-esis-statistics>
clear ethernet-switching
clear ethernet-switching evpn
clear ethernet-switching evpn arp-table
<clear-ethernet-switching-evpn-arp-table>
clear ethernet-switching mac-learning-log
<clear-ethernet-switching-mac-learning-log>
clear ethernet-switching recovery-timeout
<clear-ethernet-switching-recovery>
clear ethernet-switching recovery-timeout interface
<clear-ethernet-switching-recovery-interface>
clear ethernet-switching satellite
clear ethernet-switching satellite logging
<clear-satellite-control-logging>
clear ethernet-switching satellite vlan-auto-sense
<clear-satellite-control-plane-vlan-auto-sense>
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 evpn nd-table
<clear-evpn-nd-table>
clear extensible-subscriber-services
clear extensible-subscriber-services counters
<clear-extensible-subscriber-services-counters>
clear extensible-subscriber-services sessions
<clear-extensible-subscriber-services-sessions>
clear fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-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 layer2-map
<clear-isis-layer2-map-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 evpn nd-statistics
<clear-evpn-nd-statistics>
clear l2-learning evpn nd-statistics interface
<clear-evpn-nd-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 l2circuit
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 loop-detect
clear loop-detect statistics
clear loop-detect statistics interface
<clear-loop-detect-statistics-information>
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 address-assignment
clear network-access address-assignment preserved
<clear-address-assignment-preserved>
```

```
clear network-access ocs
clear network-access ocs statistics
<clear-ocs-statistics-information>
clear network-access pcrf
clear network-access pcrf statistics
<clear-pcrf-statistics-information>
clear network-access pcrf subscribers
<clear-pcrf-subscribers>
clear network-access requests
clear network-access requests pending
 <clear-authentication-pending-table>
clear network-access requests statistics
 <clear-authentication-statistics>
clear network-access securid-node-secret-file
 <clear-node-secret-file>
clear oam
clear oam ethernet
clear oam ethernet connectivity-fault-management
clear oam ethernet connectivity-fault-management continuity-measurement
 <clear-cfm-continuity-measurement>
clear oam ethernet connectivity-fault-management delay-statistics
 <clear-cfm-delay-statistics>
clear oam ethernet connectivity-fault-management event
<clear-cfm-action-profile-event>
clear oam ethernet connectivity-fault-management loss-statistics
 <clear-cfm-loss-statistics>
clear oam ethernet connectivity-fault-management path-database
 <clear-cfm-linktrace-path-database>
clear oam ethernet connectivity-fault-management policer
<clear-cfm-policer-statistics>
clear oam ethernet connectivity-fault-management sla-iterator-history
<clear-cfm-iterator-history>
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-ospf-database-protection>
clear ospf3 io-statistics
   <clear-ospf3-io-statistics-information>
clear ospf3 neighbor
 <clear-ospf3-neighbor-information>
clear ospf3 overload
 <clear-ospf3-overload-information>
clear ospf3 statistics
 <clear-ospf3-io-statistics-information>
clear ovsdb
clear ovsdb commit
clear ovsdb commit failures
<clear-ovsdb-commit-failure-information>
clear ovsdb statistics
clear ovsdb statistics interface
clear ovsdb statistics interface all
<clear-ovsdb-interfaces-statistics-all>
clear performance-monitoring
clear performance-monitoring mpls
clear performance-monitoring mpls lsp
<clear-pm-mpls-lsp-information>
```

```
clear pfe
clear pfe statistics
clear pfe statistics fabric
clear pfe statistics traffic detail
clear pfe statistics traffic egress-queues fpc
clear pfe statistics traffic multicast
clear pfe statistics traffic multicast fpc
clear pfe tcam-errors
clear pfe tcam-errors all-tcam-stages
<clear-pfe-tcam-errors-all-tcam-stages>
clear pfe tcam-errors app
<clear-pfe-tcam-errors-app>
clear pfe tcam-errors app bd-dtag-validate
<clear-pfe-tcam-errors-app-bd-dtag-validate>
clear pfe tcam-errors app bd-dtag-validate detail
clear pfe tcam-errors app bd-dtag-validate list-related-apps
clear pfe tcam-errors app bd-dtag-validate list-shared-apps
clear pfe tcam-errors app bd-dtag-validate shared-usage
clear pfe tcam-errors app bd-dtag-validate shared-usage detail
clear pfe tcam-errors app bd-tpid-swap
<clear-pfe-tcam-errors-app-bd-tpid-swap>
clear pfe tcam-errors app bd-tpid-swap detail
clear pfe tcam-errors app bd-tpid-swap list-related-apps
clear pfe tcam-errors app bd-tpid-swap list-shared-apps
clear pfe tcam-errors app bd-tpid-swap shared-usage
clear pfe tcam-errors app bd-tpid-swap shared-usage detail
 clear pfe tcam-errors app cfm-bd-filter
<clear-pfe-tcam-errors-app-cfm-bd-filter>
clear pfe tcam-errors app cfm-bd-filter detail
clear pfe tcam-errors app cfm-bd-filter list-related-apps
clear pfe tcam-errors app cfm-bd-filter list-shared-apps
clear pfe tcam-errors app cfm-bd-filter shared-usage
clear pfe tcam-errors app cfm-bd-filter shared-usage detail
clear pfe tcam-errors app cfm-filter
<clear-pfe-tcam-errors-app-cfm-filter>
clear pfe tcam-errors app cfm-filter detail
clear pfe tcam-errors app cfm-filter list-related-apps
clear pfe tcam-errors app cfm-filter list-shared-apps
clear pfe tcam-errors app cfm-filter shared-usage
clear pfe tcam-errors app cfm-filter shared-usage detail
clear pfe tcam-errors app cfm-vpls-filter
<clear-pfe-tcam-errors-app-cfm-vpls-filter>
clear pfe tcam-errors app cfm-vpls-filter detail
```

```
clear pfe tcam-errors app cfm-vpls-filter list-related-apps
clear pfe tcam-errors app cfm-vpls-filter list-shared-apps
clear pfe tcam-errors app cfm-vpls-filter shared-usage
clear pfe tcam-errors app cfm-vpls-filter shared-usage detail
clear pfe tcam-errors app cfm-vpls-ifl-filter
<clear-pfe-tcam-errors-app-cfm-vpls-ifl-filter>
clear pfe tcam-errors app cfm-vpls-ifl-filter detail
clear pfe tcam-errors app cfm-vpls-ifl-filter list-related-apps
clear pfe tcam-errors app cfm-vpls-ifl-filter list-shared-apps
clear pfe tcam-errors app cfm-vpls-ifl-filter shared-usage
clear pfe tcam-errors app cfm-vpls-ifl-filter shared-usage detail
clear pfe tcam-errors app cos-fc
<clear-pfe-tcam-errors-app-cos-fc>
clear pfe tcam-errors app cos-fc detail
clear pfe tcam-errors app cos-fc list-related-apps
clear pfe tcam-errors app cos-fc list-shared-apps
clear pfe tcam-errors app cos-fc shared-usage
clear pfe tcam-errors app cos-fc shared-usage detail
clear pfe tcam-errors app fw-ccc-in
<clear-pfe-tcam-errors-app-fw-ccc-in>
clear pfe tcam-errors app fw-ccc-in detail
clear pfe tcam-errors app fw-ccc-in list-related-apps
clear pfe tcam-errors app fw-ccc-in list-shared-apps
clear pfe tcam-errors app fw-ccc-in shared-usage
clear pfe tcam-errors app fw-ccc-in shared-usage detail
clear pfe tcam-errors app fw-family-out
<clear-pfe-tcam-errors-app-fw-family-out>
clear pfe tcam-errors app fw-family-out detail
clear pfe tcam-errors app fw-family-out list-related-apps
clear pfe tcam-errors app fw-family-out list-shared-apps
clear pfe tcam-errors app fw-family-out shared-usage
clear pfe tcam-errors app fw-family-out shared-usage detail
clear pfe tcam-errors app fw-fbf
<clear-pfe-tcam-errors-app-fw-fbf>
clear pfe tcam-errors app fw-fbf detail
clear pfe tcam-errors app fw-fbf list-related-apps
clear pfe tcam-errors app fw-fbf list-shared-apps
clear pfe tcam-errors app fw-fbf shared-usage
clear pfe tcam-errors app fw-fbf shared-usage detail
clear pfe tcam-errors app fw-fbf-inet6
<clear-pfe-tcam-errors-app-fw-fbf-inet6>
clear pfe tcam-errors app fw-fbf-inet6 detail
clear pfe tcam-errors app fw-fbf-inet6 list-related-apps
```

```
clear pfe tcam-errors app fw-fbf-inet6 list-shared-apps
clear pfe tcam-errors app fw-fbf-inet6 shared-usage
clear pfe tcam-errors app fw-fbf-inet6 shared-usage detail
clear pfe tcam-errors app fw-ifl-in
<clear-pfe-tcam-errors-app-fw-ifl-in>
clear pfe tcam-errors app fw-ifl-in detail
clear pfe tcam-errors app fw-ifl-in list-related-apps
clear pfe tcam-errors app fw-ifl-in list-shared-apps
clear pfe tcam-errors app fw-ifl-in shared-usage
clear pfe tcam-errors app fw-ifl-in shared-usage detail
clear pfe tcam-errors app fw-ifl-out
<clear-pfe-tcam-errors-app-fw-ifl-out>
clear pfe tcam-errors app fw-ifl-out detail
clear pfe tcam-errors app fw-ifl-out list-related-apps
clear pfe tcam-errors app fw-ifl-out list-shared-apps
clear pfe tcam-errors app fw-ifl-out shared-usage
clear pfe tcam-errors app fw-ifl-out shared-usage detail
clear pfe tcam-errors app fw-inet-ftf
<clear-pfe-tcam-errors-app-fw-inet-ftf>
clear pfe tcam-errors app fw-inet-ftf detail
clear pfe tcam-errors app fw-inet-ftf list-related-apps
clear pfe tcam-errors app fw-inet-ftf list-shared-apps
clear pfe tcam-errors app fw-inet-ftf shared-usage
clear pfe tcam-errors app fw-inet-ftf shared-usage detail
clear pfe tcam-errors app fw-inet-in
<clear-pfe-tcam-errors-app-fw-inet-in>
clear pfe tcam-errors app fw-inet-in detail
clear pfe tcam-errors app fw-inet-in list-related-apps
clear pfe tcam-errors app fw-inet-in list-shared-apps
clear pfe tcam-errors app fw-inet-in shared-usage
clear pfe tcam-errors app fw-inet-in shared-usage detail
clear pfe tcam-errors app fw-inet-pm
<clear-pfe-tcam-errors-app-fw-inet-pm>
clear pfe tcam-errors app fw-inet-pm detail
clear pfe tcam-errors app fw-inet-pm list-related-apps
clear pfe tcam-errors app fw-inet-pm list-shared-apps
clear pfe tcam-errors app fw-inet-pm shared-usage
clear pfe tcam-errors app fw-inet-pm shared-usage detail
clear pfe tcam-errors app fw-inet-rpf
<clear-pfe-tcam-errors-app-fw-inet-rpf>
clear pfe tcam-errors app fw-inet-rpf detail
clear pfe tcam-errors app fw-inet-rpf list-related-apps
clear pfe tcam-errors app fw-inet-rpf list-shared-apps
```

```
clear pfe tcam-errors app fw-inet-rpf shared-usage
clear pfe tcam-errors app fw-inet-rpf shared-usage detail
clear pfe tcam-errors app fw-inet-rpf
<clear-pfe-tcam-errors-app-fw-inet-rpf>
clear pfe tcam-errors app fw-inet-rpf detail
clear pfe tcam-errors app fw-inet-rpf list-related-apps
clear pfe tcam-errors app fw-inet-rpf list-shared-apps
clear pfe tcam-errors app fw-inet-rpf shared-usage
clear pfe tcam-errors app fw-inet-rpf shared-usage detail
clear pfe tcam-errors app fw-inet6-family-out
<clear-pfe-tcam-errors-app-fw-inet6-family-out>
clear pfe tcam-errors app fw-inet6-family-out detail
clear pfe tcam-errors app fw-inet6-family-out list-related-apps
clear pfe tcam-errors app fw-inet6-family-out list-shared-apps
clear pfe tcam-errors app fw-inet6-family-out shared-usage
clear pfe tcam-errors app fw-inet6-family-out shared-usage detail
clear pfe tcam-errors app fw-inet6-ftf
<clear-pfe-tcam-errors-app-fw-inet6-ftf>
clear pfe tcam-errors app fw-inet6-ftf detail
clear pfe tcam-errors app fw-inet6-ftf list-related-apps
clear pfe tcam-errors app fw-inet6-ftf list-shared-apps
clear pfe tcam-errors app fw-inet6-ftf shared-usage
clear pfe tcam-errors app fw-inet6-ftf shared-usage detail
clear pfe tcam-errors app fw-inet6-in
<clear-pfe-tcam-errors-app-fw-inet6-in>
clear pfe tcam-errors app fw-inet6-in detail
clear pfe tcam-errors app fw-inet6-in list-related-apps
clear pfe tcam-errors app fw-inet6-in list-shared-apps
clear pfe tcam-errors app fw-inet6-in shared-usage
clear pfe tcam-errors app fw-inet6-in shared-usage detail
clear pfe tcam-errors app fw-inet6-rpf
<clear-pfe-tcam-errors-app-fw-inet6-rpf>
clear pfe tcam-errors app fw-inet6-rpf detail
clear pfe tcam-errors app fw-inet6-rpf list-related-apps
clear pfe tcam-errors app fw-inet6-rpf list-shared-apps
clear pfe tcam-errors app fw-inet6-rpf shared-usage
clear pfe tcam-errors app fw-inet6-rpf shared-usage detail
clear pfe tcam-errors app fw-l2-in
<clear-pfe-tcam-errors-app-fw-l2-in>
clear pfe tcam-errors app fw-l2-in detail
clear pfe tcam-errors app fw-l2-in list-related-apps
clear pfe tcam-errors app fw-l2-in list-shared-apps
clear pfe tcam-errors app fw-l2-in shared-usage
```

```
clear pfe tcam-errors app fw-l2-in shared-usage detail
clear pfe tcam-errors app fw-mpls-in
<clear-pfe-tcam-errors-app-fw-mpls-in>
clear pfe tcam-errors app fw-mpls-in detail
clear pfe tcam-errors app fw-mpls-in list-related-apps
clear pfe tcam-errors app fw-mpls-in list-shared-apps
clear pfe tcam-errors app fw-mpls-in shared-usage
clear pfe tcam-errors app fw-mpls-in shared-usage detail
clear pfe tcam-errors app fw-semantics
<clear-pfe-tcam-errors-app-fw-semantics>
clear pfe tcam-errors app fw-semantics detail
clear pfe tcam-errors app fw-semantics list-related-apps
clear pfe tcam-errors app fw-semantics list-shared-apps
clear pfe tcam-errors app fw-semantics shared-usage
clear pfe tcam-errors app fw-semantics shared-usage detail
clear pfe tcam-errors app fw-vpls-in
<clear-pfe-tcam-errors-app-fw-vpls-in>
clear pfe tcam-errors app fw-vpls-in detail
clear pfe tcam-errors app fw-vpls-in list-related-apps
clear pfe tcam-errors app fw-vpls-in list-shared-apps
clear pfe tcam-errors app fw-vpls-in shared-usage
clear pfe tcam-errors app fw-vpls-in shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-egr
<clear-pfe-tcam-errors-app-gr-ifl-statistics-egr>
clear pfe tcam-errors app gr-ifl-stats-egr detail
clear pfe tcam-errors app gr-ifl-stats-egr list-related-apps
clear pfe tcam-errors app gr-ifl-stats-egr list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-egr shared-usage
clear pfe tcam-errors app gr-ifl-stats-egr shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-ing
<clear-pfe-tcam-errors-app-gr-ifl-statistics-ing>
clear pfe tcam-errors app gr-ifl-stats-ing detail
clear pfe tcam-errors app gr-ifl-stats-ing list-related-apps
clear pfe tcam-errors app gr-ifl-stats-ing list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-ing shared-usage
clear pfe tcam-errors app gr-ifl-stats-ing shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-preing
<clear-pfe-tcam-errors-app-gr-ifl-statistics-preing>
clear pfe tcam-errors app gr-ifl-stats-preing detail
clear pfe tcam-errors app gr-ifl-stats-preing list-related-apps
clear pfe tcam-errors app gr-ifl-stats-preing list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-preing shared-usage
clear pfe tcam-errors app gr-ifl-stats-preing shared-usage detail
```

```
< clear pfe tcam-errors app ifd-src-mac-fil
<clear-pfe-tcam-errors-app-ifd-src-mac-fil>
clear pfe tcam-errors app ifd-src-mac-fil detail
clear pfe tcam-errors app ifd-src-mac-fil list-related-apps
clear pfe tcam-errors app ifd-src-mac-fil list-shared-apps
clear pfe tcam-errors app ifd-src-mac-fil shared-usage
clear pfe tcam-errors app ifd-src-mac-fil shared-usage detail
clear pfe tcam-errors app ifl-statistics-in
<clear-pfe-tcam-errors-app-ifl-statistics-in>
clear pfe tcam-errors app ifl-statistics-in detail
clear pfe tcam-errors app ifl-statistics-in list-related-apps
clear pfe tcam-errors app ifl-statistics-in list-shared-apps
clear pfe tcam-errors app ifl-statistics-in shared-usage
clear pfe tcam-errors app ifl-statistics-in shared-usage detail
clear pfe tcam-errors app ifl-statistics-out
<clear-pfe-tcam-errors-app-ifl-statistics-out>
clear pfe tcam-errors app ifl-statistics-out detail
clear pfe tcam-errors app ifl-statistics-out list-related-apps
clear pfe tcam-errors app ifl-statistics-out list-shared-apps
clear pfe tcam-errors app ifl-statistics-out shared-usage
clear pfe tcam-errors app ifl-statistics-out shared-usage detail
clear pfe tcam-errors app ing-out-iff
<clear-pfe-tcam-errors-app-ing-out-iff>
clear pfe tcam-errors app ing-out-iff detail
clear pfe tcam-errors app ing-out-iff list-related-apps
clear pfe tcam-errors app ing-out-iff list-shared-apps
clear pfe tcam-errors app ing-out-iff shared-usage
clear pfe tcam-errors app ing-out-iff shared-usage detail
 clear pfe tcam-errors app ip-mac-val
<clear-pfe-tcam-errors-app-ip-mac-val>
clear pfe tcam-errors app ip-mac-val detail
clear pfe tcam-errors app ip-mac-val list-related-apps
clear pfe tcam-errors app ip-mac-val list-shared-apps
clear pfe tcam-errors app ip-mac-val shared-usage
clear pfe tcam-errors app ip-mac-val shared-usage detail
 clear pfe tcam-errors app ip-mac-val-bcast
<clear-pfe-tcam-errors-app-ip-mac-val-bcast>
clear pfe tcam-errors app ip-mac-val-bcast detail
clear pfe tcam-errors app ip-mac-val-bcast list-related-apps
clear pfe tcam-errors app ip-mac-val-bcast list-shared-apps
clear pfe tcam-errors app ip-mac-val-bcast shared-usage
clear pfe tcam-errors app ip-mac-val-bcast shared-usage detail
clear pfe tcam-errors app ipsec-reverse-fil
```

```
<clear-pfe-tcam-errors-app-ipsec-reverse-fil>
clear pfe tcam-errors app ipsec-reverse-fil detail
clear pfe tcam-errors app ipsec-reverse-fil list-related-apps
clear pfe tcam-errors app ipsec-reverse-fil list-shared-apps
clear pfe tcam-errors app ipsec-reverse-fil shared-usage
clear pfe tcam-errors app ipsec-reverse-fil shared-usage detail
clear pfe tcam-errors app irb-cos-rw
<clear-pfe-tcam-errors-app-irb-cos-rw>
clear pfe tcam-errors app irb-cos-rw detail
clear pfe tcam-errors app irb-cos-rw list-related-apps
clear pfe tcam-errors app irb-cos-rw list-shared-apps
clear pfe tcam-errors app irb-cos-rw shared-usage
clear pfe tcam-errors app irb-cos-rw shared-usage detail
clear pfe tcam-errors app irb-fixed-cos
<clear-pfe-tcam-errors-app-irb-fixed-cos>
clear pfe tcam-errors app irb-fixed-cos detail
clear pfe tcam-errors app irb-fixed-cos list-related-apps
clear pfe tcam-errors app irb-fixed-cos list-shared-apps
clear pfe tcam-errors app irb-fixed-cos shared-usage
clear pfe tcam-errors app irb-fixed-cos shared-usage detail
clear pfe tcam-errors app irb-inet6-fil
<clear-pfe-tcam-errors-app-irb-inet6-fil>
clear pfe tcam-errors app irb-inet6-fil detail
clear pfe tcam-errors app irb-inet6-fil list-related-apps
clear pfe tcam-errors app irb-inet6-fil list-shared-apps
clear pfe tcam-errors app irb-inet6-fil shared-usage
clear pfe tcam-errors app irb-inet6-fil shared-usage detail
clear pfe tcam-errors app lfm-802.3ah-in
<clear-pfe-tcam-errors-app-lfm-802.3ah-in>
clear pfe tcam-errors app lfm-802.3ah-in detail
clear pfe tcam-errors app lfm-802.3ah-in list-related-apps
clear pfe tcam-errors app lfm-802.3ah-in list-shared-apps
clear pfe tcam-errors app lfm-802.3ah-in shared-usage
clear pfe tcam-errors app lfm-802.3ah-in shared-usage detail
clear pfe tcam-errors app lfm-802.3ah-out
<clear-pfe-tcam-errors-app-lfm-802.3ah-out>
clear pfe tcam-errors app lfm-802.3ah-out detail
clear pfe tcam-errors app lfm-802.3ah-out list-related-apps
clear pfe tcam-errors app lfm-802.3ah-out list-shared-apps
clear pfe tcam-errors app lfm-802.3ah-out shared-usage
clear pfe tcam-errors app lfm-802.3ah-out shared-usage detail
clear pfe tcam-errors app lo0-inet-fil
<clear-pfe-tcam-errors-app-lo0-inet-fil>
```

```
clear pfe tcam-errors app lo0-inet-fil detail
clear pfe tcam-errors app lo0-inet-fil list-related-apps
clear pfe tcam-errors app lo0-inet-fil list-shared-apps
clear pfe tcam-errors app lo0-inet-fil shared-usage
clear pfe tcam-errors app lo0-inet-fil shared-usage detail
clear pfe tcam-errors app lo0-inet6-fil
<clear-pfe-tcam-errors-app-lo0-inet6-fil>
clear pfe tcam-errors app lo0-inet6-fil detail
clear pfe tcam-errors app lo0-inet6-fil list-related-apps
clear pfe tcam-errors app lo0-inet6-fil list-shared-apps
clear pfe tcam-errors app lo0-inet6-fil shared-usage
clear pfe tcam-errors app lo0-inet6-fil shared-usage detail
clear pfe tcam-errors app mac-drop-cnt
<clear-pfe-tcam-errors-app-mac-drop-cnt>
clear pfe tcam-errors app mac-drop-cnt detail
clear pfe tcam-errors app mac-drop-cnt list-related-apps
clear pfe tcam-errors app mac-drop-cnt list-shared-apps
clear pfe tcam-errors app mac-drop-cnt shared-usage
clear pfe tcam-errors app mac-drop-cnt shared-usage detail
clear pfe tcam-errors app mrouter-port-in
<clear-pfe-tcam-errors-app-mrouter-port-in>
clear pfe tcam-errors app mrouter-port-in detail
clear pfe tcam-errors app mrouter-port-in list-related-apps
clear pfe tcam-errors app mrouter-port-in list-shared-apps
clear pfe tcam-errors app mrouter-port-in shared-usage
clear pfe tcam-errors app mrouter-port-in shared-usage detail
 clear pfe tcam-errors app napt-reverse-fil
<clear-pfe-tcam-errors-app-napt-reverse-fil>
clear pfe tcam-errors app napt-reverse-fil detail
clear pfe tcam-errors app napt-reverse-fil list-related-apps
clear pfe tcam-errors app napt-reverse-fil list-shared-apps
clear pfe tcam-errors app napt-reverse-fil shared-usage
clear pfe tcam-errors app napt-reverse-fil shared-usage detail
clear pfe tcam-errors app no-local-switching
<clear-pfe-tcam-errors-app-no-local-switching>
clear pfe tcam-errors app no-local-switching detail
clear pfe tcam-errors app no-local-switching list-related-apps
clear pfe tcam-errors app no-local-switching list-shared-apps
clear pfe tcam-errors app no-local-switching shared-usage
clear pfe tcam-errors app no-local-switching shared-usage detail
clear pfe tcam-errors app ptpoe-cos-rw
<clear-pfe-tcam-errors-app-ptpoe-cos-rw>
clear pfe tcam-errors app ptpoe-cos-rw detail
```

```
clear pfe tcam-errors app ptpoe-cos-rw list-related-apps
clear pfe tcam-errors app ptpoe-cos-rw list-shared-apps
clear pfe tcam-errors app ptpoe-cos-rw shared-usage
clear pfe tcam-errors app ptpoe-cos-rw shared-usage detail
clear pfe tcam-errors app rfc2544-layer2-in
<clear-pfe-tcam-errors-app-rfc2544-layer2-in>
clear pfe tcam-errors app rfc2544-layer2-in detail
clear pfe tcam-errors app rfc2544-layer2-in list-related-apps
clear pfe tcam-errors app rfc2544-layer2-in list-shared-apps
clear pfe tcam-errors app rfc2544-layer2-in shared-usage
clear pfe tcam-errors app rfc2544-layer2-in shared-usage detail
clear pfe tcam-errors app rfc2544-layer2-out
<clear-pfe-tcam-errors-app-rfc2544-layer2-out>
clear pfe tcam-errors app rfc2544-layer2-out detail
clear pfe tcam-errors app rfc2544-layer2-out list-related-apps
clear pfe tcam-errors app rfc2544-layer2-out list-shared-apps
clear pfe tcam-errors app rfc2544-layer2-out shared-usage
clear pfe tcam-errors app rfc2544-layer2-out shared-usage detail
clear pfe tcam-errors app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
clear pfe tcam-errors app vpls-mesh-group-mcast detail
clear pfe tcam-errors app vpls-mesh-group-mcast list-related-apps
clear pfe tcam-errors app vpls-mesh-group-mcast list-shared-apps
clear pfe tcam-errors app vpls-mesh-group-mcast shared-usage
clear pfe tcam-errors app vpls-mesh-group-mcast shared-usage detail
clear pfe tcam-errors app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
clear pfe tcam-errors app vpls-mesh-group-ucast detail
clear pfe tcam-errors app vpls-mesh-group-ucast list-related-apps
clear pfe tcam-errors app vpls-mesh-group-ucast list-shared-apps
clear pfe tcam-errors app vpls-mesh-group-ucast shared-usage
clear pfe tcam-errors app vpls-mesh-group-ucast shared-usage detail
clear pfe tcam-errors tcam-stage
clear pfe tcam-errors tcam-stage egress
<clear-pfe-tcam-errors-egress-tcam-stage>
clear pfe tcam-errors tcam-stage egress app
clear-pfe-tcam-errors-egress-app
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate
<clear-pfe-tcam-errors-egress-app-bd-dtag-validate>
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate detail
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate list-related-appsclear pfe tcam-
errors tcam-stage egress app bd-dtag-validate list-shared-apps
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate shared-usage
```

```
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate shared-usage detail
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap
<clear-pfe-tcam-errors-egress-app-bd-tpid-swap>
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap detail
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap list-related-apps
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap list-shared-apps
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap shared-usage
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-family-out
<clear-pfe-tcam-errors-egress-app-fw-family-out>
clear pfe tcam-errors tcam-stage egress app fw-family-out detail
clear pfe tcam-errors tcam-stage egress app fw-family-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-family-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-family-out shared-usage
clear pfe tcam-errors tcam-stage egress app fw-family-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-ifl-out
<clear-pfe-tcam-errors-egress-app-fw-ifl-out>
clear pfe tcam-errors tcam-stage egress app fw-ifl-out detail
clear pfe tcam-errors tcam-stage egress app fw-ifl-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-ifl-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-ifl-out shared-usage
clear pfe tcam-errors tcam-stage egress app fw-ifl-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out
<clear-pfe-tcam-errors-egress-app-fw-inet6-family-out>
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out detail
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out shared-usage
 clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out shared-usage detail
 clear pfe tcam-errors tcam-stage egress app ifl-statistics-out
<clear-pfe-tcam-errors-egress-app-ifl-statistics-out>
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out detail
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out list-related-apps
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out shared-usage
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app irb-cos-rw
<clear-pfe-tcam-errors-egress-app-irb-cos-rw>
clear pfe tcam-errors tcam-stage egress app irb-cos-rw detail
clear pfe tcam-errors tcam-stage egress app irb-cos-rw list-related-apps
clear pfe tcam-errors tcam-stage egress app irb-cos-rw list-shared-apps
clear pfe tcam-errors tcam-stage egress app irb-cos-rw shared-usage
clear pfe tcam-errors tcam-stage egress app irb-cos-rw shared-usage detail
```

```
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out
<clear-pfe-tcam-errors-egress-app-lfm-802.3ah-out>
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out detail
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out list-related-apps
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw
<clear-pfe-tcam-errors-egress-app-ptpoe-cos-rw>
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw detail
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw list-related-apps
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw list-shared-apps
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw shared-usage
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw shared-usage detail
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out
<clear-pfe-tcam-errors-egress-app-rfc2544-layer2-out>
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out detail
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out list-related-apps
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out shared-usage
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out shared-usage detail
clear pfe tcam-errors tcam-stage ingress
<clear-pfe-tcam-errors-ingress-tcam-stage>
clear pfe tcam-errors tcam-stage ingress app
<clear-pfe-tcam-errors-ingress-app>
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter
<clear-pfe-tcam-errors-ingress-app-cfm-bd-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter detail
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter shared-usage detail
clear pfe tcam-errors tcam-stage ingress app cfm-filter
<clear-pfe-tcam-errors-ingress-app-cfm-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-filter detail
clear pfe tcam-errors tcam-stage ingress app cfm-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-filter shared-usage detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter
<clear-pfe-tcam-errors-ingress-app-cfm-vpls-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter list-related-apps
```

```
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter shared-usage detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter
<clear-pfe-tcam-errors-ingress-app-cfm-vpls-ifl-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-ifl-filter shared-usage detail
 clear pfe tcam-errors tcam-stage ingress app fw-ccc-in
<clear-pfe-tcam-errors-ingress-app-fw-ccc-in>
clear pfe tcam-errors tcam-stage ingress app fw-ccc-in detail
clear pfe tcam-errors tcam-stage ingress app fw-ccc-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-ccc-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-ccc-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-ccc-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in
<clear-pfe-tcam-errors-ingress-app-fw-ifl-in>
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in detail
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-ifl-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf
<clear-pfe-tcam-errors-ingress-app-fw-inet-ftf>
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-ftf shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-in
<clear-pfe-tcam-errors-ingress-app-fw-inet-in>
clear pfe tcam-errors tcam-stage ingress app fw-inet-in detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm
<clear-pfe-tcam-errors-ingress-app-fw-inet-pm>
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm list-shared-apps
```

```
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf
<clear-pfe-tcam-errors-ingress-app-fw-inet-rpf>
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf
<clear-pfe-tcam-errors-ingress-app-fw-inet6-ftf>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in
<clear-pfe-tcam-errors-ingress-app-fw-inet6-in>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf
<clear-pfe-tcam-errors-ingress-app-fw-inet6-rpf>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-l2-in
<clear-pfe-tcam-errors-ingress-app-fw-l2-in>
clear pfe tcam-errors tcam-stage ingress app fw-l2-in detail
clear pfe tcam-errors tcam-stage ingress app fw-l2-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-l2-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-l2-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-l2-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in
<clear-pfe-tcam-errors-ingress-app-fw-mpls-in>
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in detail
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in shared-usage
```

```
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in
<clear-pfe-tcam-errors-ingress-app-fw-vpls-in>
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in detail
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr
<clear-pfe-tcam-errors-ingress-app-gr-ifl-statistics-egr>
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing
<clear-pfe-tcam-errors-ingress-app-gr-ifl-statistics-ing>
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing
<clear-pfe-tcam-errors-ingress-app-gr-ifl-statistics-preing>
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing shared-usage detail
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in
<clear-pfe-tcam-errors-ingress-app-ifl-statistics-in>
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in detail
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in shared-usage
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil
<clear-pfe-tcam-errors-ingress-app-ipsec-reverse-fil>
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil detail
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil shared-usage detail
```

```
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos
<clear-pfe-tcam-errors-ingress-app-irb-fixed-cos>
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos detail
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos list-related-apps
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos list-shared-apps
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos shared-usage
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos shared-usage detail
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil
<clear-pfe-tcam-errors-ingress-app-irb-inet6-fil>
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil detail
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in
<clear-pfe-tcam-errors-ingress-app-lfm-802.3ah-in>
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in detail
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in shared-usage
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil
<clear-pfe-tcam-errors-ingress-app-lo0-inet-fil>
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil
<clear-pfe-tcam-errors-ingress-app-lo0-inet6-fil>
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt
<clear-pfe-tcam-errors-ingress-app-mac-drop-cnt>
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt detail
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt list-related-apps
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt list-shared-apps
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt shared-usage
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt shared-usage detail
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in
```

```
<clear-pfe-tcam-errors-ingress-app-mrouter-port-in>
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in detail
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in shared-usage
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil
<clear-pfe-tcam-errors-ingress-app-napt-reverse-fil>
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil detail
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app no-local-switching
<clear-pfe-tcam-errors-ingress-app-no-local-switching>
clear pfe tcam-errors tcam-stage ingress app no-local-switching detail
clear pfe tcam-errors tcam-stage ingress app no-local-switching list-related-apps
clear pfe tcam-errors tcam-stage ingress app no-local-switching list-shared-apps
clear pfe tcam-errors tcam-stage ingress app no-local-switching shared-usage
clear pfe tcam-errors tcam-stage ingress app no-local-switching shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress
<clear-pfe-tcam-errors-pre-ingress-tcam-stage>
clear pfe tcam-errors tcam-stage pre-ingress app
<clear-pfe-tcam-errors-pre-ingress-app>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc detail
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 list-shared-apps
```

```
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics detail
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil detail
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff
<clear-pfe-tcam-errors-pre-ingress-app-ing-out-iff>
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff detail
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val
<clear-pfe-tcam-errors-pre-ingress-app-ip-mac-val>
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast
<clear-pfe-tcam-errors-pre-ingress-app-ip-mac-val-bcast>
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in
<clear-pfe-tcam-errors-pre-ingress-app-rfc2544-layer2-in>
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in detail
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in shared-usage
```

```
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage detail
clear passive-monitoring
 <clear-passive-monitoring>
clear passive-monitoring statistics
 <clear-passive-monitoring-statistics>
clear pgm
clear pgm negative-acknowledgments
<clear-pgm-negative-acknowledgments>
clear pgm source-path-messages
<clear-pgm-source-path-messages>
clear pgm statistics
<clear-pgm-statistics>
clear pim
clear pim join
<clear-pim-join-state>
clear pim join-distribution
<clear-pim-join-distribution>
clear pim register
<clear-pim-register-state>
clear pim snooping
clear pim snooping join
clear pim snooping statistics
clear pim statistics
<clear-pim-statistics>
clear poe
clear poe telemetries
clear poe telemetries interface
<clear-poe-telemetries-information>
clear ppp
```

```
clear ppp statistics
 <clear-ppp-statistics-information>
clear pppoe
clear pppoe lockout
<clear-pppoe-lockout-timers>
clear pppoe lockout atm-identifier
<clear-pppoe-lockout-timers-atm>
clear pppoe lockout vlan-identifier
clear pppoe sessions
<clear-pppoe-sessions-information>
clear-pppoe-lockout-timers-vlan
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 group
<clear-gvpn-group-information>
clear security group-vpn member ike
clear security group-vpn member ike security-associations
<clear-group-vpn-ike-security-associations>
clear security group-vpn member ipsec
clear security group-vpn member ipsec security-associations
<clear-gvpn-ipsec-security-association>
clear security group-vpn member ipsec security-associations statistics
<clear-gvpn-ipsec-security-association-statistics>
clear security group-vpn member ipsec statistics
<clear-gvpn-ipsec-statistics>
clear services
clear services accounting flow inline-jflow
<clear-services-accounting-inline-jflow-flows>
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 ha
clear services ha statistics
<clear-service-ha-statistics-information>
clear services hcm
clear services hcm pic-statistics
<clear-services-hcm-pic-statistics>
clear services hcm statistics
<clear-services-hcm-statistics>
clear services ids
<clear-services-ids-tables>
clear services ids destination-table
<clear-services-ids-destination-table>
clear services ids pair-table
```

```
<clear-services-ids-pair-table>
clear services ids source-table
<clear-services-ids-source-table>
clear services inline
clear services inline nat
clear services inline nat pool
<clear-inline-nat-pool-information>
clear services inline nat statistics
<clear-inline-nat-statistics>
clear services inline softwire
clear services inline softwire statistics
<clear-inline-softwire-statistics>
clear services ipsec-vpn
clear services ipsec-vpn ipsec
clear services ipsec-vpn ipsec security-associations
<clear-services-ipsec-vpn-security-associations>
clear services ipsec-vpn ike
clear services ipsec-vpn ike security-associations
<clear-services-ike-security-associations>
clear services ipsec-vpn ike statistics
<clear-services-ike-statistics>
clear services pcp
clear services pcp epoch
clear services pcp statistics
clear services ipsec-vpn ipsec statistics
<clear-ipsec-vpn-statistics>
clear services l2tp
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp multilink
<clear-l2tp-multilink-information>
clear services l2tp session
<clear-l2tp-session-information>
clear services l2tp destination
<clear-l2tp-destinations-information>
clear services l2tp disconnect-cause-summary
<clear-l2tp-disconnect-cause-summary>
clear services l2tp tunnel
<clear-l2tp-tunnel-information>
clear services l2tp user
<clear-l2tp-user-session-information>
clear services local-policy-decision-function
```

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

```
<clear-service-video-monitoring-mdi-information>
clear services video-monitoring mdi alarm
<clear-service-video-monitoring-mdi-alarm-information>
clear services video-monitoring mdi alarm errors
<clear-services-video-monitoring-mdi-alarm-errors>
clear services video-monitoring mdi alarm stats
<clear-services-video-monitoring-mdi-alarm-statistics>
clear services video-monitoring mdi errors
<clear-service-video-monitoring-mdi-errors>
clear services video-monitoring mdi statistics
<clear-service-video-monitoring-mdi-statistics>
clear services sessions analysis
<clear-service-msp-session-analysis-information>
clear services softwire
clear services softwire statistics
<clear-services-softwire-statistics>
clear services stateful-firewall
clear services stateful-firewall flow-analysis
<clear-service-flow-analysis>
clear services stateful-firewall flows
<clear-service-sfw-flow-table-information>
clear services pgcp
clear services pgcp gates
 <clear-service-pgcp-gates>
clear services pgcp gates gateway
 <clear-service-pgcp-gates-gateway>
clear services pgcp statistics
 <clear-service-pgcp-statistics>
clear services pgcp statistics gateway
 <clear-service-pgcp-statistics-gateway>
<clear-rfc2544-information>
<clear-aborted-tests-information>
<clear-active-tests-information>
<clear-completed-tests-information>
clear sflow
clear sflow collector
clear sflow collector statistics
<clear-sflow-collector-statistics>
clear shmlog
clear shmlog all-info
<clear-shmlog-all-information>
clear shmlog entries
<clear-shmlog-entries>
```

```
clear shmlog statistics
<clear-shmlog-statistics>
clear snmp
clear snmp history
<clear-snmp-history>
<clear-health-monitor-routing-engine-history>.
clear snmp statistics
<clear-snmp-statistics>
clear spanning-tree
clear spanning-tree protocol-migration
clear spanning-tree protocol-migration interface
<clear-interface-stp-protocol-migration>
clear spanning-tree statistics
<clear-stp-interface-statistics>
clear spanning-tree statistics bridge
clear spanning-tree statistics interface
clear spanning-tree statistics routing-instance
<clear-stp-routing-instance-statistics>
clear spanning-tree stp-buffer
clear spanning-tree topology-change-counter
<clear-stp-topology-change-counter>
clear synchronous-ethernet
clear synchronous-ethernet esmc
clear synchronous-ethernet esmc statistics
clear system
clear system boot-media
<clear-boot-media>
clear system login
 clear system login lockout
< clear-system-login-lockout>
clear-twamp-information
clear-twamp-server-information
clear-twamp-server-connection-information
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
```

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

```
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
```

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

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

```
<get-mobile-gateways-sgw-call-trace-stop-information>
```

Configuration Hierarchy Levels

No asscociated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

configure

Can enter configuration mode.

Commands

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

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Access Privilege Levels Overview | 53

Example: Configure User Permissions with Access Privilege Levels | 59

Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91

Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

control

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

Commands

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

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Access Privilege Levels Overview | 53

Example: Configure User Permissions with Access Privilege Levels | 59

Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91

Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

field

Can view field debug commands.

Commands

No associated CLI commands.

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

firewall

Can view the firewall filter configuration in configuration mode.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
```

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

```
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
```

```
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
```

```
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show firewall
    <get-firewall-information>

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

show firewall filter
```

```
    <get-firewall-filter-information>

show firewall filter version
    <get-filter-version>

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

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

show policer
<get-policer-information>
```

Configuration Hierarchy Levels

```
[edit chassis satellite-management]
[edit firewall][edit dynamic-profiles firewall]
[edit firewall]
[edit logical-systems firewall]
[edit unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- firewall-control | 861

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

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

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

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

show firewall filter version
    <get-filter-version>

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

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

show policer
```

Configuration Hierarchy Levels

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

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- firewall | 856

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

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

flow-tap

Can view the flow-tap configuration in configuration mode.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
```

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

```
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
```

```
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
```

```
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

Configuration Hierarchy Levels

```
[edit services flow-tap]
[edit services radius-flow-tap]
[edit system services flow-tap-dtcp]
[edit unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- flow-tap-control | 868

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

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- flow-tap | 863

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

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

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

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
```

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

```
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
```

```
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
```

```
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

Configuration Hierarchy Levels

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

RELATED DOCUMENTATION

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 system services dhcp-local-server]
```

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

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- interface | 870

maintenance

Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell, viewing configuration files in the CLI and the shell, and halting or rebooting the router.

Commands

```
clear system commit synchronize-server pending-jobs
    <clear-pending-commit-sync-jobs>
clear system reboot
    <clear-reboot>
clear-system-services-reverse-information
file archive
    <file-archive>
file change-owner
    <file-change-owner>
file show
```

```
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 fan-tray
request chassis feb
    <request-feb>
request chassis fpc
    <request-chassis-fpc>
request chassis fpc optical-module
    <request-fpc-optical-module>
request chassis fpc optical-module amplifier-chain
    <request-fpc-optical-module-amplifier-chain>
request chassis fpc optical-module amplifier-chain ila
    <request-fpc-optical-module-ila>
request chassis fpc optical-module amplifier-chain ila firmware-upgrade
    <request-fpc-optical-module-ila-firmware-upgrade>
request chassis fpc optical-module amplifier-chain ila hard-reset
    <request-fpc-optical-module-ila-hard-reset>
request chassis fpc optical-module amplifier-chain ila soft-reset
    <request-fpc-optical-module-ila-soft-reset>
request chassis fpc optical-module firmware-upgrade
    <request-fpc-optical-module-firmware-upgrade>
request chassis fpm
request chassis mcs
request chassis mic
request chassis optics
request chassis pcg
request chassis pic
```

```
    <request-chassis-pic>
request chassis port-led
request chassis port-led start
    <request-chassis-port-led-switch-on>
request chassis port-led stop
    <request-chassis-port-led-switch-off>
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 satellite device-mode
request chassis satellite disable
    <request-chassis-satellite-disable>
request chassis satellite enable
    <request-chassis-satellite-enable>
request chassis satellite file-copy
    <request-chassis-satellite-file-copy>
request chassis satellite install
    <request-chassis-satellite-install>
request chassis satellite interface
request chassis satellite login
    <request-chassis-satellite-login>
request chassis satellite reboot
    <request-chassis-satellite-reboot>
request chassis satellite restart
    <request-chassis-satellite-restart>
request chassis satellite restart process
request chassis satellite shell-command
    <request-chassis-satellite-shell-command>
request chassis scg
request chassis sfb
request chassis sfm
request chassis sfm master
request chassis sib
    <request-chassis-sib>
request chassis sib f13
request chassis sib f2s
request chassis sib optics
request chassis spmb
    <request-chassis-spmb>
```

```
request chassis ssb
request chassis ssb master
request chassis synchronization
request chassis synchronization force
request chassis synchronization force automatic-switching
request chassis synchronization force mark-failed
request chassis synchronization force unmark-failed
request chassis synchronization switch
request chassis tfeb
request chassis vcpu
request chassis vnpu
request diagnostics
request diagnostics tdr
request diagnostics tdr abort
request diagnostics tdr abort interface
    <abort-tdr-interface-diagnostics>
request diagnostics tdr start
request diagnostics tdr start interface
    <request-tdr-interface-diagnostics>
request extension-service
request extension-service start
    <extension-service-start>
request extension-service stop
    <extension-service-stop>
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 security-package offline-download
    <request-idp-security-package-offline-download>
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 decrypt
    <security-decrypt-password>
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 cb
    <request-fpc-fpga-upgrade>
request system firmware downgrade cb i2c
    <request-i2c-fpga-upgrade>
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 cb i2c
    <request-i2c-fpga-upgrade>
request system firmware upgrade feb
request system firmware upgrade fpc
request system firmware upgrade fpga
request system firmware upgrade fpga cb
    <request-cb-fpga-upgrade>
request system firmware upgrade fpga fpc
request system firmware upgrade fpga fpd
    <request-fpd-fpga-upgrade>
request system firmware upgrade fpga ftc
    <request-ftc-fpga-upgrade>
request system firmware upgrade fpga re
    <request-re-fpga-upgrade>
request system firmware upgrade fpga scb
    <request-scb-fpga-upgrade>
request system firmware upgrade fpga sib
    <request-sib-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 logs
    <request-system-logs-copy>
request system partition
request system partition abort
request system partition compact-flash
request system partition hard-disk
request system power-off
    <request-power-off>
request system power-on
    <request-power-on-other-re>
request system process
request system process terminate
    <request-process-terminate>
request system reboot
    <request-reboot>
request system recover
request system scripts
request system scripts add
    <request-scripts-package-add>
request system scripts convert
request system scripts convert slax-to-xslt
request system scripts convert xslt-to-slax
request system scripts delete
    <request-scripts-package-delete>
request system scripts event-scripts
request system scripts event-scripts reload
    <reload-event-scripts>
request system scripts refresh-from
   <request-script-refresh-from>
request system scripts rollback
    <request-scripts-package-rollback>
request system scripts synchronize
    <request-scripts-synchronize>
request system snapshot
    <request-snapshot>
request system software
request system software abort
request system software abort in-service-upgrade
    <abort-in-service-upgrade>
request system software add
    <request-package-add>
request system software delete
    <request-package-delete>
```

```
request system software delete-backup
    <request-package-delete-backup>
request system software in-service-upgrade
    <request-package-in-service-upgrade>
request system software nonstop-upgrade
   <request-package-nonstop-upgrade>
request system software recovery-package
request system software recovery-package add
request system software recovery-package delete
request system software recovery-package extract
request system software recovery-package extract ex-8200-package
request system software recovery-package extract ex-xre200-package
request system software rollback
    <request-package-rollback>
request system software validate
    <request-package-validate>
request system software validate in-service-upgrade
    <check-in-service-upgrade>
request system storage
request system storage cleanup
    <request-system-storage-cleanup>
request system storage cleanup qfabric
   <remove-qfabric-repository-contents>
request system storage mount
    <request-mount>
request system storage unified-edge
request system storage unified-edge charging
request system storage unified-edge charging media
request system storage unified-edge media
request system storage unified-edge media eject
request system storage unified-edge media prepare
request system storage unmount
    <request-unmount>
request system subscriber-management
request system subscriber-management new-sessions-disable
    <request-sm-new-sessions-disable>
request system subscriber-management new-sessions-enable
    <request-sm-new-sessions-enable>
request system yang enable
    <request-yang-enable>
request system yang update
    <request-yang-update>
request system yang validate
```

```
    <request-yang-validate>
request system zeroize
request vmhost
request vmhost cleanup
    <request-vmhost-file-cleanup>
request vmhost file-copy
    <request-vmhost-file-copy>
request vmhost halt
    <request-vmhost-halt>
request vmhost hard-disk-test
    <request-vmhost-hard-disk-test>
request vmhost power-off
    <request-vmhost-poweroff>
request vmhost power-on
    <request-power-on-other-re>
request vmhost reboot
    <request-vmhost-reboot>
request vmhost snapshot
    <request-vmhost-snapshot>
request vmhost snapshot partition
    <request-vmhost-snapshot-partition>
request vmhost snapshot recovery
    <request-vmhost-snapshot-recovery>
request vmhost snapshot recovery partition
    <request-vmhost-snapshot-recovery-partition>
request vmhost software
request vmhost software abort
request vmhost software abort in-service-upgrade
    <abort-in-service-upgrade>
request vmhost software add
    <request-vmhost-package-add>
request vmhost software in-service-upgrade
    <request-vmhost-package-in-service-upgrade>
request vmhost software rollback
    <request-package-rollback>
request vmhost zeroize
    <request-vmhost-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 ipsect trusted-channel]
[edit services dynamic-flow-capture traceoptions]
[edit services ggsn]
[edit system fips]
[edit services ggsn rule-space]
[edit system processes daemon-process command]
[edit system scripts]
[edit system scripts commit]
[edit system scripts op]
[edit system scripts snmp]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

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

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

show host
show interfaces level-extra descriptions
show multicast 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>
traceroute overlay
<request-traceroute-overlay>
```

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

pgcp-session-mirroring

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

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
```

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

```
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
```

```
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
```

```
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show services pgcp gates gate-way display session-mirroring
```

Configuration Hierarchy Levels

```
[edit services pgcp gateway session-mirroring]
[edit services pgcp session-mirroring]
[edit unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- pgcp-session-mirroring-control | 895

pgcp-session-mirroring-control

Can modify PGCP session mirroring configuration

Commands

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

Configuration Hierarchy Levels

```
[edit services pgcp gateway session-mirroring]
[edit services pgcp session-mirroring]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- pgcp-session-mirroring | 890

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

```
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 satellite install 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>
```

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Access Privilege Levels Overview | 53

Example: Configure User Permissions with Access Privilege Levels | 59

Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91

Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

rollback

Can roll back to previous configurations.

Commands

`rollback`

Configuration Hierarchy Levels

```
[edit]
```

RELATED DOCUMENTATION

Access Privilege Levels Overview | 53

Example: Configure User Permissions with Access Privilege Levels | 59

Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91

Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

routing

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

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
```

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

```
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
```

```
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
```

```
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

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 rsvp]
[edit logical-systems routing-instances instance protocols rsvp lsp-set 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]
sho[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 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 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]
```

```
[ed[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 unified-edge]
[edit vlans]
[edit vlans vlan multicast-snooping-options]
[edit vlans vlan multicast-snooping-options traceoptions]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- routing-control | 907

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 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 forwarding-options satellite]
[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 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 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 Levels Overview | **53**
- Example: Configure User Permissions with Access Privilege Levels | **59**
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | **91**
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | **103**
- routing | **897**

secret

Can view passwords and other authentication keys in the configuration.

Commands

No associated CLI commands.

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
```

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

```
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
```

```
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
```

```
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

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

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

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- secret-control | 918

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

```
[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 Levels Overview | **53**
- Example: Configure User Permissions with Access Privilege Levels | **59**
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | **91**
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | **103**
- secret | **913**

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 counters action
clear security idp counters application-ddos
clear security idp counters application-identification
clear security idp counters dfa
clear security idp counters flow
clear security idp counters http-decoder
clear security idp counters ips
clear security idp counters log
clear security idp counters memory
clear security idp counters packet
clear security idp counters packet-log
clear security idp counters pdf-decoder
clear security idp counters policy-manager
clear security idp counters ssl-inspection
clear security idp counters tcp-reassembler


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>
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
```

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

```
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
```

```
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
    <request-idp-policy-load>
request security idp security-package
request security idp security-package download
    <request-idp-security-package-download>

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

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

request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
```

```
    <request-idp-ssl-key-add>

request security idp ssl-inspection key delete
    <request-idp-ssl-key-delete>
request security idp storage-cleanup
   <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
    <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
    <load-pki-ca-certificate>
request security pki crl
request security pki crl load
    <request security pki crl load>
request security pki generate-certificate-request
    <generate-pki-certificate-request>
request security pki generate-key-pair
   <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
    <verify-pki-local-certificate>
request security pki verify-integrity-status
<verify-integrity-status>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
    <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
    <load-pki-local-certificate>
request system set-encryption-key
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
```

```
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
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 counters action
show security idp counters application-ddos
show security idp counters application-identification
show security idp counters dfa
show security idp counters flow
show security idp counters http-decoder
show security idp counters ips
show security idp counters log
show security idp counters memory
show security idp counters packet
show security idp counters packet-log
show security idp counters pdf-decoder
show security idp counters policy-manager
show security idp counters ssl-inspection
show security idp counters tcp-reassembler

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][edit security ssh-known-hosts][edit
unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- security-control | 929

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 security-package offline-download
<request-idp-security-package-offline-download>
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 counters action
show security idp counters application-ddos
show security idp counters application-identification
```

```
show security idp counters dfa
show security idp counters flow
show security idp counters http-decoder
show security idp counters ips
show security idp counters log
show security idp counters memory
show security idp counters packet
show security idp counters packet-log
show security idp counters pdf-decoder
show security idp counters policy-manager
show security idp counters ssl-inspection
show security idp counters tcp-reassembler

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][edit security ssh-known-hosts]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- security | 919

shell

IN THIS SECTION

Can create a UNIX-level shell.

Juniper Networks does not provide support for operations in the shell.

Commands

```
start shell csh
start shell csh user
start shell sh
start shell sh user
```

RELATED DOCUMENTATION

start shell

snmp

Can view Simple Network Management Protocol (SNMP) configuration.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
```

```
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
```

```
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
```

```
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
```

```
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
```

Configuration Hierarchy Levels

```
[edit snmp]
[edit unified-edge]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

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 Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

snmp | 934

system

Can view system-level configuration information.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
```

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

```
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
```

```
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
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 path-computation-client retry-delegation
<request-path-computation-retry-delegation>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
```

```
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
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 network-slices]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit fabric virtual-chassis]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems protocols uplink-failure-detection]
[edit logical-systems routing-instances instance forwarding-options helpers bootp]
[edit logical-systems routing-instances instance forwarding-options helpers domain]
[edit logical-systems routing-instances instance forwarding-options helpers port]
[edit logical-systems routing-instances instance forwarding-options helpers tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit logical-systems system syslog]
[edit poe]
[edit protocols uplink-failure-detection]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
```

```
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system boot loader authentication]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-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-hidden-commands]
[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 unified-edge]
[edit virtual-chassis]
[edit virtual-chassis locality-bias]
[edit vlans]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- system-control | 947

system-control

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

Configuration Hierarchy Levels

```
[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
```

```
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems routing-instances instance forwarding-options helpers bootp]
[edit logical-systems routing-instances instance forwarding-options helpers domain]
[edit logical-systems routing-instances instance forwarding-options helpers port]
[edit logical-systems routing-instances instance forwarding-options helpers tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit poe]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system dgasp-in]
[edit system dgasp-usb]
[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 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 Levels Overview | **53**
- Example: Configure User Permissions with Access Privilege Levels | **59**
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | **91**
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | **103**
- system | **940**

trace

Can view trace file settings and configure trace file properties.

Commands

```
clear log
   <clear-log>
clear log satellite
<clear-log-satellite>
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
```

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

```
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
```

```
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
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
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
```

```
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show log
<get-log>
show log user
    <get-syslog-events>
```

Configuration Hierarchy Levels

```
[edit unified-edge]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit class-of-service application-traffic-control traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
```

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

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

```
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp lsp-set traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server interface-
traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
```

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

```
[edit routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit services l2tp traceoptions]
[edit services server-load-balance traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system ddos-protection traceoptions]
[edit system license traceoptions]
[edit system processes 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 system services web-management traceoptions]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- trace-control | 960

trace-control

Can modify trace file settings and configure trace file properties.

Configuration Hierarchy Levels

```
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit demux traceoptions]
```

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

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

```
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options dhcp-relay
interface-traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options dhcp-relay
traceoptions]
[edit logical-systems routing-instances instance vlans domain multicast-snooping-options
traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols igmp-snooping
traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server interface-
traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
```

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

```
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay interface-
traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay interface-traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance system services dhcp-local-server interface-traceoptions]
[edit routing-instances instance system services dhcp-local-server traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit system ddos-protection traceoptions]
[edit services l2tp traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services server-load-balance traceoptions]
```

```
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services dhcp-local-server traceoptions]
[edit system services dhcp-local-server interface-traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]
[edit unified-edge aaa traceoptions]
[edit unified-edge gateways tdf charging traceoptions]
```

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103
- trace | 950

view

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

Commands

```
clear ipv6 router-advertisement
<clear-ipv6-router-advertisement-information>clear l2circuit auto-sensing
<clear-l2ckt-pw-auto-sensing>
clear services redundancy-group
<clear-services-redundancy-group>
clear services redundancy-group statistics
<clear-services-redundancy-group-statistics>
<clear-services-redundancy-set>
clear services service-sets statistics ids
clear services service-sets statistics ids drops
<clear-service-set-ids-drops-statistics>
clear services traffic-load-balance
clear services traffic-load-balance statistics
<clear-service-traffic-load-balance-statistics>
<request-validation-policy>
show
show access-cac interface-set
<get-access-cac-iflset>
show access-security
show access-security router-advertisement-guard
show access-security router-advertisement-guard entries
<show-as-router-advetisement-entry>
show access-security router-advertisement-guard state
<show-as-ra-state>
show access-security router-advertisement-guard statistics
<get-as-router-advertisement-statistics>
show access-security router-advertisement-guard statistics interface
<get-as-router-advertisement-interface>
show accounting

show accounting profile
    <get-accounting-profile-information>

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

show amt
show amt statistics
 <get-amt-statistics>
```

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

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

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

show ancp subscriber identifier
   <get-ancp-subscriber-identifier-information>show ancp subscriber ip-address
<get-ancp-subscriber-neighbor-information>
show ancp subscriber system-name
<get-ancp-subscriber-mac-information>
show ancp subscriber neighbor
show app-engine
show app-engine information
show app-engine packages
show app-engine packages remote
<get-virtual-machine-package-remote>
show app-engine packages system
<get-virtual-machine-package-system>
show app-engine processes
show app-engine resource-usage
show app-engine route-table
show app-engine routing-instance
```

```
show app-engine routing-instance compute-clusters
show app-engine routing-instance virtual-machines
show app-engine status
show app-engine virtual-machine package
<get-virtual-machine-package-information>
show application-monitor
<get-application-monitor-information>
show application-monitor probe
show application-monitor probe flows
<get-application-monitor-probe-flows-information>
show application-monitor probe measurements
<get-application-monitor-probe-measurements>
show application-monitor probe mirrors
<get-application-monitor-probe-mirrors>
show app-engine virtual-machine vm-instance
show aps
   <get-aps-information>

show aps group
   <get-aps-group-information>
show aps interface
   <get-aps-interface-information>
show arp
    <get-arp-table-information>

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

show bfd session address
   <get-bfd-session-address>
show bfd session client
<get-bfd-session-client>
```

```
show bfd session client rsvp-oam
<get-bfd-session-client-rsvp>
show bfd session client vpls-oam
<get-bfd-session-client-vpls>
show bfd session client vpls-oam instance
<get-bfd-session-client-vpls-instance>
show bfd session discriminator
   <get-bfd-session-discriminator>
show bfd session prefix
   <get-bfd-session-prefix>
show bfd subscriber
show bfd subscriber session
<get-bfd-subscriber-session>
show bgp
show bgp bmp
<get-bgp-monitoring-protocol-statistics>
show bgp group
    <get-bgp-group-information>
show bgp group output-queues
<get-bgp-group-output-queue-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 neighbor output-queue
<get-bgp-output-queue-information>
show bgp output-scheduler

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 domain satellite
<get-satellite-control-bridge-domain>
show bridge evpn
show bridge evpn arp-table
<get-bridge-evpn-arp-table>
show bridge evpn nd-table
<get-bridge-evpn-nd-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 next-hops
show bridge flood next-hops satellite
<get-satellite-control-composite-next-hop>
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 flood satellite
<get-satellite-control-flood-ethernet>
show bridge interface
show bridge interface satellite
<get-satellite-control-bridge-interface>
show bridge mac-table
    <get-bridge-mac-table>
show bridge mac-table interface
    <get-bridge-interface-mac-table>
```

```
show bridge mac-table satellite
<get-satellite-control-bridge-mac-table>
show bridge satellite
show bridge satellite device
<get-satellite-device-db>
show bridge satellite events
<get-satellite-control-history-information>
show bridge satellite logging
<get-satellite-control-logging-information>
show bridge satellite summary
<get-satellite-control-bridge-summary>

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 alarms satellite
<get-chassis-alarm-satellite-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 fpc satellite
<get-chassis-environment-fpc-satellite-info>
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 pem satellite
<get-chassis-environment-pem-satellite-info>
show chassis environment psm
show chassis environment psu
    <get-environment-psu-information>
show chassis environment routing-engine
    <get-environment-re-information>
show chassis environment routing-engine satellite
<get-chassis-environment-re-satellite-info>
show chassis environment satellite
<get-chassis-environment-satellite-information>
show chassis environment scg
    <get-environment-scg-information>
show chassis environment service-node
<get-environment-service-node-information>
show chassis environment sfb
show chassis environment sfm
    <get-environment-sfm-information>

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

show chassis environment sib f13
show chassis environment sib f2s
show chassis ethernet-switch
show chassis ethernet-switch errors
show chassis ethernet-switch statistics
show chassis ethernet-switch temperature
show chassis fabric
```

```
show chassis fabric degraded-fabric-reachability
show chassis fabric device
    <get-chassis-fabric-information-device>
show chassis fabric connectivity
<get-chassis-fabric-connectivity-information>
show chassis fabric degradation
<get-fm-degradation-information>
show chassis fabric degradation actions
<get-fm-degradation-information-details>
show chassis fabric destinations
<get-fm-fabric-destinations-state>
show chassis fabric errors
show chassis fabric errors autoheal
<get-fm-plane-autoheal-errors>
show chassis fabric errors fpc
    <get-fm-fpc-errors>

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

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

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

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

```
show chassis fabric topology
    <get-chassis-fabric-topology-information>
show chassis fabric unreachable-destinations
   <get-fm-unreachable-dest-information>
show chassis fan
show chassis fan satellite
get-chassis-fan-satellite-information
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 firmware satellite
<get-chassis-firmware-satellite-information>
show chassis forwarding
    <get-fwdd-information>

show chassis fpc
    <get-fpc-information>

show chassis fpc errors
    <get-fpc-error-information>
show chassis fpc optical-properties
<get-fpc-optical-information>
show chassis fpc optical-properties alarms
<get-fpc-optical-alarms-information>
show chassis fpc optical-properties amplifier-chain
show chassis fpc optical-properties amplifier-chain ila
<get-fpc-optical-amplifier-chain-information>
show chassis fpc optical-properties amplifier-chain ila alarms
<get-fpc-optical-ila-alarms-information>
show chassis fpc optical-properties amplifier-chain ila edfa
<get-fpc-optical-ila-edfa-information>
show chassis fpc optical-properties amplifier-chain ila osc
<get-fpc-optical-ila-osc-information>
show chassis fpc optical-properties amplifier-chain ila pm-current
```

```
<get-fpc-optical-ila-pm-current-information>
show chassis fpc optical-properties amplifier-chain ila pm-currentday
<get-fpc-optical-ila-pm-currentday-information>
show chassis fpc optical-properties amplifier-chain ila pm-interval
<get-fpc-optical-ila-pm-interval-information>
show chassis fpc optical-properties amplifier-chain ila pm-previousday
<get-fpc-optical-ila-pm-previousday-information>
show chassis fpc optical-properties amplifier-chain ila summary
<get-fpc-optical-ila-summary-information>
show chassis fpc optical-properties amplifier-chain ila voa
<get-fpc-optical-ila-voa-information>
show chassis fpc optical-properties amplifier-topology
<get-fpc-optical-amplifier-topology-information>
show chassis fpc optical-properties edfa
<get-fpc-optical-edfa-information>
show chassis fpc optical-properties mfg-info
<get-fpc-optical-mfg-info-information>
show chassis fpc optical-properties ocm
<get-fpc-optical-ocm-information>
show chassis fpc optical-properties pm-current
<get-fpc-optical-pm-current-information>
show chassis fpc optical-properties pm-currentday
<get-fpc-optical-pm-currentday-information>
show chassis fpc optical-properties pm-interval
<get-fpc-optical-pm-interval-information>
show chassis fpc optical-properties pm-previousday
<get-fpc-optical-pm-previousday-information>
show chassis fpc optical-properties status
<get-fpc-optical-status-information>
show chassis fpc optical-properties topology
<get-fpc-optical-topology-information>
show chassis fpc optical-properties wss
<get-fpc-optical-wss-information>
show chassis fpc pic-status
    <get-pic-information>
show chassis fpc port-status
<get-fpc-port-information>
show chassis fpc-feb-connectivity
    <get-fpc-feb-connectivity-information>

show chassis hardware
    <get-chassis-inventory>
show chassis hardware satellite
```

```
<get-chassis-hardware-satellite-information>
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 jam-test
<get-jam-test-information>
show chassis lcc-mode
<get-chassis-lcc-mode-information>

show chassis lccs
    <get-fru-information>
<get-chassis-led-satellite-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 network-slices
<get-gnf-information>

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 routing-engine bios satellite
<get-chassis-routing-engine-bios-satellite-info>
show chassis routing-engine errors
<get-chassis-routing-engine-errors>
show chassis routing-engine satellite
<get-chassis-routing-engine-satellite-information>
show chassis satellite
<get-chassis-satellite-information>
show chassis satellite extended-port
<get-chassis-satellite-extended-port-information>
show chassis satellite interface
<get-chassis-satellite-interface-information>
show chassis satellite neighbor
<get-chassis-satellite-neighbor-information>
show chassis satellite neighbor statistics
<get-chassis-satellite-neighbor-statistics>
 show chassis satellite power-budget-statistics
```

```
<get-power-budget-information>
show chassis satellite redundancy-group
<get-chassis-satellite-redundancy-group-info>
show chassis satellite redundancy-group devices
<get-chassis-satellite-redundacy-grp-devices-info>
show chassis satellite redundancy-group devices history
<get-chassis-satellite-redundancy-grp-dev-history>
show chassis satellite software
<get-satellite-management-software-information>
show chassis satellite statistics
<get-chassis-satellite-statistics>
 show chassis satellite unprovision
 <get-chassis-satellite-unprovision-information>
 show chassis satellite upgrade-group
<get-chassis-satellite-upgrade-group-information>
show chassis satellite-cluster
<get-chassis-satellite-cluster-information>
 show chassis satellite-cluster route
<get-chassis-satellite-cluster-route>
show chassis satellite-cluster statistics
<get-chassis-satellite-cluster-statistics>
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 errors
<get-spmb-error-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 gnss
show chassis synchronization master
show chassis system-mode
<get-system-mode-information>
show chassis temperature-thresholds
    <get-temperature-threshold-information>
show chassis temperature-thresholds satellite
<get-chassis-temp-thresholds-satellite-info>
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 rate-limiters
show class-of-service application-traffic-control rate-limiters rl-all
<get-appqos-swrl-stat-all>
show class-of-service application-traffic-control rate-limiters rl-name
<get-appqos-swrl-stat-name>
show class-of-service application-traffic-control rate-limiters summary
<get-appqos-swrl-stat-summary>
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 bind-point
<get-cos-bind-point-feature-information>
show class-of-service bind-point interface
<get-cos-interface-feature-information>
show class-of-service bind-point interface-set
<get-cos-interface-set-feature-information>
show class-of-service bind-point routing-instance
```

```
<get-cos-routing-instance-feature-information>
show class-of-service bind-point-ownership
<get-cos-bind-point-ownership-summary>
show class-of-service classifier
    <get-cos-classifier-information>
show class-of-service client
show class-of-service client internal-id
<get-cos-junos-client-information>
show class-of-service client name
<get-cos-junos-client-information>
show class-of-service client summary
<get-cos-junos-client-summary>

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

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

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

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

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

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

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

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

show class-of-service forwarding-table classifier mapping
```

```
    <get-cos-classifier-table-map-information>

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

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

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

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

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

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

show class-of-service forwarding-table loss-priority-rewrite
   <get-cos-loss-priority-rewrite-table-information>
show class-of-service forwarding-table loss-priority-rewrite mapping
   <get-cos-loss-priority-rewrite-table-binding-information>
show class-of-service forwarding-table policer
    <get-cos-policer-table-map-information>
show class-of-service forwarding-table policy-map
<get-cos-policy-map-table-information>
show class-of-service forwarding-table policy-map mapping
<get-cos-policy-map-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 scheduler-map mapping
<get-scheduler-map-table-map-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 multi-destination classifier-binding
<get-cos-multi-destination-classifier-binding-information>

show class-of-service packet-buffer
<get-cos-packet-buffer-information>
show class-of-service packet-buffer usage
<get-cos-packet-buffer-usage-information>
show class-of-service policy-map
<get-cos-policy-map-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 commands
show cli commands
show cli directory
<get-current-working-directory>
show cli history
show cloud-analytics
show cloud-analytics connections
<get-cloud-analytics-connections>
show cloud-analytics discovery-service
<get-cloud-analytics-discovery-service>
show cloud-analytics linecard
<get-cloud-analytics-lc>
show cloud-analytics resources
<get-cloud-analytics-resources>
show cloud-analytics resources-sampling
<get-cloud-analytics-resources-sampling>
show cloud-analytics resources-summary
<get-cloud-analytics-resources-summary>
show cloud-analytics sensors
```

```
<sensor-information>
show cloud-analytics streaming-policies
<get-cloud-analytics-streaming-policies>
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 all-fiber-channel-enode
<get-ddos-all-fc-enode-information>
show ddos-protection protocols all-fiber-channel-enode aggregate
<get-ddos-all-fc-enode-aggregate>
show ddos-protection protocols all-fiber-channel-enode aggregate culprit-flows
<get-ddos-all-fc-enode-aggregate-flows>
show ddos-protection protocols all-fiber-channel-enode culprit-flows
<get-ddos-all-fc-enode-flows>
show ddos-protection protocols all-fiber-channel-enode flow-detection
<get-ddos-all-fc-enode-flow-parameters>
show ddos-protection protocols all-fiber-channel-enode parameters
<get-ddos-all-fc-enode-parameters>
show ddos-protection protocols all-fiber-channel-enode statistics
<get-ddos-all-fc-enode-statistics>
show ddos-protection protocols all-fiber-channel-enode violations
<get-ddos-all-fc-enode-violations>
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 arp-snoop
<get-ddos-arp-snoop-information>
show ddos-protection protocols arp-snoop aggregate
<get-ddos-arp-snoop-aggregate>
show ddos-protection protocols arp-snoop aggregate culprit-flows
<get-ddos-arp-snoop-aggregate-flows>
```

```
show ddos-protection protocols arp-snoop culprit-flows
<get-ddos-arp-snoop-flows>
show ddos-protection protocols arp-snoop flow-detection
<get-ddos-arp-snoop-flow-parameters>
show ddos-protection protocols arp-snoop parameters
<get-ddos-arp-snoop-parameters>
 show ddos-protection protocols arp-snoop statistics
<get-ddos-arp-snoop-statistics>
show ddos-protection protocols arp-snoop violations
<get-ddos-arp-snoop-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 bridge-control
<get-ddos-brg-ctrl-information>
show ddos-protection protocols bridge-control aggregate
<get-ddos-brg-ctrl-aggregate>
show ddos-protection protocols bridge-control aggregate culprit-flows
<get-ddos-brg-ctrl-aggregate-flows>
show ddos-protection protocols bridge-control culprit-flows
<get-ddos-brg-ctrl-flows>
show ddos-protection protocols bridge-control flow-detection
<get-ddos-brg-ctrl-flow-parameters>
show ddos-protection protocols bridge-control parameters
<get-ddos-brg-ctrl-parameters>
show ddos-protection protocols bridge-control statistics
<get-ddos-brg-ctrl-statistics>
show ddos-protection protocols bridge-control violations
<get-ddos-brg-ctrl-violations>show ddos-protection protocols demux-autosense
    get-ddos-demuxauto-information
show ddos-protection protocols demux-autosense aggregate
    get-ddos-demuxauto-aggregate
show ddos-protection protocols demux-autosense parameters
    get-ddos-demuxauto-parameters
show ddos-protection protocols demux-autosense statistics
    get-ddos-demuxauto-statistics
show ddos-protection protocols demux-autosense violations
    get-ddos-demuxauto-violations
show ddos-protection protocols dhcpv4
```

```
    get-ddos-dhcpv4-information
show ddos-protection protocols dhcpv4 ack
    get-ddos-dhcpv4-ack
show ddos-protection protocols dhcpv4 aggregate
    get-ddos-dhcpv4-aggregate
show ddos-protection protocols dhcpv4 bad-packets
    get-ddos-dhcpv4-bad-pack
show ddos-protection protocols dhcpv4 bootp
    get-ddos-dhcpv4-bootp
show ddos-protection protocols dhcpv4 decline
    get-ddos-dhcpv4-decline
show ddos-protection protocols dhcpv4 discover
    get-ddos-dhcpv4-discover
show ddos-protection protocols dhcpv4 force-renew
    get-ddos-dhcpv4-forcerenew
show ddos-protection protocols dhcpv4 inform
    get-ddos-dhcpv4-inform
show ddos-protection protocols dhcpv4 lease-active
    get-ddos-dhcpv4-leaseact
show ddos-protection protocols dhcpv4 lease-query
    get-ddos-dhcpv4-leasequery
show ddos-protection protocols dhcpv4 lease-unassigned
    get-ddos-dhcpv4-leaseuna
show ddos-protection protocols dhcpv4 lease-unknown
    get-ddos-dhcpv4-leaseunk
show ddos-protection protocols dhcpv4 nak
    get-ddos-dhcpv4-nak
show ddos-protection protocols dhcpv4 no-message-type
    get-ddos-dhcpv4-no-msgtype
show ddos-protection protocols dhcpv4 offer
    get-ddos-dhcpv4-offer
show ddos-protection protocols dhcpv4 offer culprit-flows
show ddos-protection protocols dhcpv4 parameters
    get-ddos-dhcpv4-parameters
show ddos-protection protocols dhcpv4 release
    get-ddos-dhcpv4-release
show ddos-protection protocols dhcpv4 renew
    get-ddos-dhcpv4-renew
show ddos-protection protocols dhcpv4 request
    get-ddos-dhcpv4-request
show ddos-protection protocols dhcpv4 statistics
    get-ddos-dhcpv4-statistics
show ddos-protection protocols dhcpv4 unclassified
```

```
    get-ddos-dhcpv4-unclass
show ddos-protection protocols dhcpv4 violations
    get-ddos-dhcpv4-violations
show ddos-protection protocols dhcpv4v6
<get-ddos-dhcpv4v6-information>
show ddos-protection protocols dhcpv4v6 aggregate
<get-ddos-dhcpv4v6-aggregate>
show ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<get-ddos-dhcpv4v6-aggregate-flows>
show ddos-protection protocols dhcpv4v6 culprit-flows
<get-ddos-dhcpv4v6-flows>
show ddos-protection protocols dhcpv4v6 flow-detection
<get-ddos-dhcpv4v6-flow-parameters>
show ddos-protection protocols dhcpv4v6 parameters
<get-ddos-dhcpv4v6-parameters>
show ddos-protection protocols dhcpv4v6 statistics
<get-ddos-dhcpv4v6-statistics>
show ddos-protection protocols dhcpv4v6 violations
<get-ddos-dhcpv4v6-violations>
show ddos-protection protocols dhcpv6
    get-ddos-dhcpv6-information
show ddos-protection protocols dhcpv6 advertise
    get-ddos-dhcpv6-advertise
show ddos-protection protocols dhcpv6 advertise culprit-flows
show ddos-protection protocols dhcpv6 aggregate
    get-ddos-dhcpv6-aggregate
show ddos-protection protocols dhcpv6 confirm
    get-ddos-dhcpv6-confirm
show ddos-protection protocols dhcpv6 decline
    get-ddos-dhcpv6-decline
show ddos-protection protocols dhcpv6 information-request
    get-ddos-dhcpv6-info-req
show ddos-protection protocols dhcpv6 leasequery
    get-ddos-dhcpv6-leasequery
show ddos-protection protocols dhcpv6 leasequery culprit-flows
show ddos-protection protocols dhcpv6 leasequery-data
    get-ddos-dhcpv6-leaseq-da
show ddos-protection protocols dhcpv6 leasequery-done
    get-ddos-dhcpv6-leaseq-do
show ddos-protection protocols dhcpv6 leasequery-reply
    get-ddos-dhcpv6-leaseq-re
show ddos-protection protocols dhcpv6 parameters
    get-ddos-dhcpv6-parameters
```

```
show ddos-protection protocols dhcpv6 rebind
    get-ddos-dhcpv6-rebind
show ddos-protection protocols dhcpv6 reconfigure
    get-ddos-dhcpv6-reconfig
show ddos-protection protocols dhcpv6 relay-forward
    get-ddos-dhcpv6-relay-for
show ddos-protection protocols dhcpv6 relay-reply
    get-ddos-dhcpv6-relay-rep
show ddos-protection protocols dhcpv6 release
    get-ddos-dhcpv6-release
show ddos-protection protocols dhcpv6 renew
    get-ddos-dhcpv6-renew
show ddos-protection protocols dhcpv6 reply
    get-ddos-dhcpv6-reply
show ddos-protection protocols dhcpv6 request
    get-ddos-dhcpv6-request
show ddos-protection protocols dhcpv6 solicit
    get-ddos-dhcpv6-solicit
show ddos-protection protocols dhcpv6 statistics
    get-ddos-dhcpv6-statistics
show ddos-protection protocols dhcpv6 unclassified
    get-ddos-dhcpv6-unclass
show ddos-protection protocols dhcpv6 unclassified culprit-flows
show ddos-protection protocols dhcpv6 violations
    get-ddos-dhcpv6-violations
show ddos-protection protocols diameter
    get-ddos-diameter-information
show ddos-protection protocols diameter aggregate
    get-ddos-diameter-aggregate
show ddos-protection protocols diameter parameters
    get-ddos-diameter-parameters
show ddos-protection protocols diameter statistics
    get-ddos-diameter-statistics
show ddos-protection protocols diameter violations
    get-ddos-diameter-violations
show ddos-protection protocols dns
    get-ddos-dns-information
show ddos-protection protocols dns aggregate
    get-ddos-dns-aggregate
show ddos-protection protocols dns parameters
    get-ddos-dns-parameters
show ddos-protection protocols dns statistics
    get-ddos-dns-statistics
```

```
show ddos-protection protocols dns violations
    get-ddos-dns-violations
show ddos-protection protocols dtcp
    get-ddos-dtcp-information
show ddos-protection protocols dtcp aggregate
    get-ddos-dtcp-aggregate
show ddos-protection protocols dtcp aggregate culprit-flows
show ddos-protection protocols dtcp parameters
    get-ddos-dtcp-parameters
show ddos-protection protocols dtcp statistics
    get-ddos-dtcp-statistics
show ddos-protection protocols dtcp violations
    get-ddos-dtcp-violations
show ddos-protection protocols dynamic-vlan
    get-ddos-dynvlan-information
show ddos-protection protocols dynamic-vlan aggregate
    get-ddos-dynvlan-aggregate
show ddos-protection protocols dynamic-vlan parameters
    get-ddos-dynvlan-parameters
show ddos-protection protocols dynamic-vlan statistics
    get-ddos-dynvlan-statistics
show ddos-protection protocols dynamic-vlan violations
    get-ddos-dynvlan-violations
show ddos-protection protocols egpv6
    get-ddos-egpv6-information
show ddos-protection protocols egpv6 aggregate
    get-ddos-egpv6-aggregate
show ddos-protection protocols egpv6 parameters
    get-ddos-egpv6-parameters
show ddos-protection protocols egpv6 statistics
    get-ddos-egpv6-statistics
show ddos-protection protocols egpv6 violations
    get-ddos-egpv6-violations
show ddos-protection protocols eoam
    get-ddos-eoam-information
show ddos-protection protocols eoam aggregate
    get-ddos-eoam-aggregate
show ddos-protection protocols eoam parameters
    get-ddos-eoam-parameters
show ddos-protection protocols eoam statistics
    get-ddos-eoam-statistics
show ddos-protection protocols eoam violations
    get-ddos-eoam-violations
```

```
show ddos-protection protocols esmc
    get-ddos-esmc-information
show ddos-protection protocols esmc aggregate
    get-ddos-esmc-aggregate
show ddos-protection protocols esmc parameters
    get-ddos-esmc-parameters
show ddos-protection protocols esmc statistics
    get-ddos-esmc-statistics
show ddos-protection protocols esmc violations
    get-ddos-esmc-violations
show ddos-protection protocols ethernet-tcc
<get-ddos-eth-tcc-information>
show ddos-protection protocols ethernet-tcc aggregate
<get-ddos-eth-tcc-aggregate>
show ddos-protection protocols ethernet-tcc aggregate culprit-flows
<get-ddos-eth-tcc-aggregate-flows>
show ddos-protection protocols ethernet-tcc culprit-flows
<get-ddos-eth-tcc-flows>
show ddos-protection protocols ethernet-tcc flow-detection
<get-ddos-eth-tcc-flow-parameters>
show ddos-protection protocols ethernet-tcc parameters
<get-ddos-eth-tcc-parameters>
show ddos-protection protocols ethernet-tcc statistics
<get-ddos-eth-tcc-statistics>
show ddos-protection protocols ethernet-tcc violations
<get-ddos-eth-tcc-violations>
show ddos-protection protocols exceptions
<get-ddos-exception-information>
show ddos-protection protocols exceptions aggregate
<get-ddos-exception-aggregate>
show ddos-protection protocols exceptions aggregate culprit-flows
<get-ddos-exception-aggregate-flows>
show ddos-protection protocols exceptions culprit-flows
<get-ddos-exception-flows>
show ddos-protection protocols exceptions flow-detection
<get-ddos-exception-flow-parameters>
show ddos-protection protocols exceptions mcast-rpf-err
<get-ddos-exception-mcast-rpf>
show ddos-protection protocols exceptions mcast-rpf-err culprit-flows
<get-ddos-exception-mcast-rpf-flows>
show ddos-protection protocols exceptions mtu-exceeded
<get-ddos-exception-mtu-exceed>
show ddos-protection protocols exceptions mtu-exceeded culprit-flows
```

```
<get-ddos-exception-mtu-exceed-flows>
show ddos-protection protocols exceptions parameters
<get-ddos-exception-parameters>
show ddos-protection protocols exceptions statistics
<get-ddos-exception-statistics>
show ddos-protection protocols exceptions unclassified
<get-ddos-exception-unclass>
show ddos-protection protocols exceptions unclassified culprit-flows
<get-ddos-exception-unclass-flows>
show ddos-protection protocols exceptions violations
<get-ddos-exception-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-ftpv6-information
show ddos-protection protocols ftpv6 aggregate
    get-ddos-ftpv6-aggregate
show ddos-protection protocols ftpv6 parameters
    get-ddos-ftpv6-parameters
show ddos-protection protocols ftpv6 statistics
    get-ddos-ftpv6-statistics
show ddos-protection protocols ftpv6 violations
    get-ddos-ftpv6-violations
show ddos-protection protocols garp-reply
<get-ddos-garp-reply-information>
show ddos-protection protocols garp-reply aggregate
<get-ddos-garp-reply-aggregate>
show ddos-protection protocols garp-reply aggregate culprit-flows
<get-ddos-garp-reply-aggregate-flows>
show ddos-protection protocols garp-reply culprit-flows
<get-ddos-garp-reply-flows>
show ddos-protection protocols garp-reply flow-detection
<get-ddos-garp-reply-flow-parameters>
show ddos-protection protocols garp-reply parameters
<get-ddos-garp-reply-parameters>
show ddos-protection protocols garp-reply statistics
<get-ddos-garp-reply-statistics>
show ddos-protection protocols garp-reply violations
<get-ddos-garp-reply-violations>
show ddos-protection protocols gre
    get-ddos-gre-information
show ddos-protection protocols gre aggregate
    get-ddos-gre-aggregate
show ddos-protection protocols gre hbc
<get-ddos-gre-hbc>
show ddos-protection protocols gre hbc culprit-flows
<get-ddos-gre-hbc-flows>
show ddos-protection protocols gre parameters
    get-ddos-gre-parameters
show ddos-protection protocols gre punt
<get-ddos-gre-punt>
show ddos-protection protocols gre punt culprit-flows
<get-ddos-gre-punt-flows>
show ddos-protection protocols gre statistics
    get-ddos-gre-statistics
```

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

```
show ddos-protection protocols igmp-snoop violations
    get-ddos-igmp-snoop-violations
show ddos-protection protocols igmpv4v6
    get-ddos-igmpv4v6-information
show ddos-protection protocols igmpv4v6 aggregate
    get-ddos-igmpv4v6-aggregate
show ddos-protection protocols igmpv4v6 aggregate culprit-flows
show ddos-protection protocols igmpv4v6 parameters
    get-ddos-igmpv4v6-parameters
show ddos-protection protocols igmpv4v6 statistics
    get-ddos-igmpv4v6-statistics
show ddos-protection protocols igmpv4v6 violations
    get-ddos-igmpv4v6-violations
show ddos-protection protocols igmpv6
    get-ddos-igmpv6-information
show ddos-protection protocols igmpv6 aggregate
    get-ddos-igmpv6-aggregate
show ddos-protection protocols igmpv6 parameters
    get-ddos-igmpv6-parameters
show ddos-protection protocols igmpv6 statistics
    get-ddos-igmpv6-statistics
show ddos-protection protocols igmpv6 violations
    get-ddos-igmpv6-violations
show ddos-protection protocols ip-fragments
    get-ddos-ip-frag-information
show ddos-protection protocols ip-fragments aggregate
    get-ddos-ip-frag-aggregate
show ddos-protection protocols ip-fragments first-fragment
    get-ddos-ip-frag-first-frag
show ddos-protection protocols ip-fragments parameters
    get-ddos-ip-frag-parameters
show ddos-protection protocols ip-fragments statistics
    get-ddos-ip-frag-statistics
show ddos-protection protocols ip-fragments trail-fragment
    get-ddos-ip-frag-trail-frag
show ddos-protection protocols ip-fragments violations
    get-ddos-ip-frag-violations
show ddos-protection protocols ip-options
    get-ddos-ip-opt-information
show ddos-protection protocols ip-options aggregate
    get-ddos-ip-opt-aggregate
show ddos-protection protocols ip-options non-v4v6
<get-ddos-ip-opt-non-v4v6>
```

```
show ddos-protection protocols ip-options parameters
    get-ddos-ip-opt-parameters
show ddos-protection protocols ip-options router-alert
    get-ddos-ip-opt-rt-alert
show ddos-protection protocols ip-options statistics
    get-ddos-ip-opt-statistics
show ddos-protection protocols ip-options unclassified
    get-ddos-ip-opt-unclass
show ddos-protection protocols ipmc-reserved culprit-flows
<get-ddos-ipmc-reserved-flows>
show ddos-protection protocols ipmc-reserved flow-detection
<get-ddos-ipmc-reserved-flow-parameters>
show ddos-protection protocols ipmc-reserved parameters
<get-ddos-ipmc-reserved-parameters>
show ddos-protection protocols ipmc-reserved statistics
<get-ddos-ipmc-reserved-statistics>
show ddos-protection protocols ipmc-reserved violations
<get-ddos-ipmc-reserved-violations>
show ddos-protection protocols ipmcast-miss
<get-ddos-ipmcast-miss-information>
show ddos-protection protocols ipmcast-miss aggregate
<get-ddos-ipmcast-miss-aggregate>
show ddos-protection protocols ipmcast-miss aggregate culprit-flows
<get-ddos-ipmcast-miss-aggregate-flows>
show ddos-protection protocols ipmcast-miss culprit-flows
<get-ddos-ipmcast-miss-flows>
show ddos-protection protocols ipmcast-miss flow-detection
<get-ddos-ipmcast-miss-flow-parameters>
show ddos-protection protocols ipmcast-miss parameters
<get-ddos-ipmcast-miss-parameters>
show ddos-protection protocols ipmcast-miss statistics
<get-ddos-ipmcast-miss-statistics>
show ddos-protection protocols ipmcast-miss violations
<get-ddos-ipmcast-miss-violations>
show ddos-protection protocols ip-options violations
    get-ddos-ip-opt-violations
show ddos-protection protocols ipv4-unclassified
    get-ddos-ipv4-uncls-information
show ddos-protection protocols ipv4-unclassified aggregate
    get-ddos-ipv4-uncls-aggregate
show ddos-protection protocols ipv4-unclassified parameters
    get-ddos-ipv4-uncls-parameters
show ddos-protection protocols ipv4-unclassified statistics
```

```
    get-ddos-ipv4-uncls-statistics
show ddos-protection protocols ipv4-unclassified violations
    get-ddos-ipv4-uncls-violations
show ddos-protection protocols ipv6-unclassified
    get-ddos-ipv6-uncls-information
show ddos-protection protocols ipv6-unclassified aggregate
    get-ddos-ipv6-uncls-aggregate
show ddos-protection protocols ipv6-unclassified parameters
    get-ddos-ipv6-uncls-parameters
show ddos-protection protocols ipv6-unclassified statistics
    get-ddos-ipv6-uncls-statistics
show ddos-protection protocols ipv6-unclassified violations
    get-ddos-ipv6-uncls-violations
show ddos-protection protocols isis
    get-ddos-isis-information
show ddos-protection protocols isis aggregate
    get-ddos-isis-aggregate
show ddos-protection protocols isis parameters
    get-ddos-isis-parameters
show ddos-protection protocols isis statistics
    get-ddos-isis-statistics
show ddos-protection protocols isis violations
    get-ddos-isis-violations
show ddos-protection protocols iso-tcc
<get-ddos-iso-tcc-information>
show ddos-protection protocols iso-tcc aggregate
<get-ddos-iso-tcc-aggregate>
show ddos-protection protocols iso-tcc aggregate culprit-flows
<get-ddos-iso-tcc-aggregate-flows>
show ddos-protection protocols iso-tcc culprit-flows
<get-ddos-iso-tcc-flows>
show ddos-protection protocols iso-tcc flow-detection
<get-ddos-iso-tcc-flow-parameters>
show ddos-protection protocols iso-tcc parameters
<get-ddos-iso-tcc-parameters>
show ddos-protection protocols iso-tcc statistics
<get-ddos-iso-tcc-statistics>
show ddos-protection protocols iso-tcc violations
<get-ddos-iso-tcc-violations>
show ddos-protection protocols jfm
    get-ddos-jfm-information
show ddos-protection protocols jfm aggregate
    get-ddos-jfm-aggregate
```

```
show ddos-protection protocols jfm parameters
    get-ddos-jfm-parameters
show ddos-protection protocols jfm statistics
    get-ddos-jfm-statistics
show ddos-protection protocols jfm violations
    get-ddos-jfm-violations
show ddos-protection protocols l2tp
    get-ddos-l2tp-information
show ddos-protection protocols l2tp aggregate
    get-ddos-l2tp-aggregate
show ddos-protection protocols l2tp parameters
    get-ddos-l2tp-parameters
show ddos-protection protocols l2tp statistics
    get-ddos-l2tp-statistics
show ddos-protection protocols l2tp violations
    get-ddos-l2tp-violations
show ddos-protection protocols l3dest-miss
      <get-ddos-l3dest-miss-information>
show ddos-protection protocols l3dest-miss aggregate
      <get-ddos-l3dest-miss-aggregate>
show ddos-protection protocols l3dest-miss aggregate culprit-flows
      <get-ddos-l3dest-miss-aggregate-flows>
show ddos-protection protocols l3dest-miss culprit-flows
      <get-ddos-l3dest-miss-flows>
show ddos-protection protocols l3dest-miss flow-detection
      <get-ddos-l3dest-miss-flow-parameters>
show ddos-protection protocols l3dest-miss parameters
      <get-ddos-l3dest-miss-parameters>
show ddos-protection protocols l3dest-miss statistics
      <get-ddos-l3dest-miss-statistics>
show ddos-protection protocols l3dest-miss violations
      <get-ddos-l3dest-miss-violations>
show ddos-protection protocols l3mc-sgv-hit-icl
      <get-ddos-l3mc-sgv-hit-icl-information>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate
      <get-ddos-l3mc-sgv-hit-icl-aggregate>
show ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
      <get-ddos-l3mc-sgv-hit-icl-aggregate-flows>
show ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
      <get-ddos-l3mc-sgv-hit-icl-flows>
show ddos-protection protocols l3mc-sgv-hit-icl flow-detection
      <get-ddos-l3mc-sgv-hit-icl-flow-parameters>
show ddos-protection protocols l3mc-sgv-hit-icl parameters
```

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

```
show ddos-protection protocols lacp statistics
<get-ddos-lacp-statistics>
show ddos-protection protocols lacp violations
<get-ddos-lacp-violations>
show ddos-protection protocols ldp
<get-ddos-ldp-information>
show ddos-protection protocols ldp aggregate
<get-ddos-ldp-aggregate>
show ddos-protection protocols ldp parameters
<get-ddos-ldp-parameters>
show ddos-protection protocols ldp statistics
<get-ddos-ldp-statistics>
show ddos-protection protocols ldp violations
<get-ddos-ldp-violations>
show ddos-protection protocols ldp-hello
<get-ddos-ldp-hello-information>
show ddos-protection protocols ldp-hello aggregate
<get-ddos-ldp-hello-aggregate>
show ddos-protection protocols ldp-hello aggregate culprit-flows
<get-ddos-ldp-hello-aggregate-flows>
show ddos-protection protocols ldp-hello culprit-flows
<get-ddos-ldp-hello-flows>
show ddos-protection protocols ldp-hello flow-detection
<get-ddos-ldp-hello-flow-parameters>
show ddos-protection protocols ldp-hello parameters
<get-ddos-ldp-hello-parameters>
show ddos-protection protocols ldp-hello statistics
<get-ddos-ldp-hello-statistics>
show ddos-protection protocols ldp-hello violations
<get-ddos-ldp-hello-violations>
show ddos-protection protocols ldpv6
<get-ddos-ldpv6-information>
show ddos-protection protocols ldpv6 aggregate
<get-ddos-ldpv6-aggregate>
show ddos-protection protocols ldpv6 parameters
<get-ddos-ldpv6-parameters>
show ddos-protection protocols ldpv6 statistics
<get-ddos-ldpv6-statistics>
show ddos-protection protocols ldpv6 violations
<get-ddos-ldpv6-violations>
show ddos-protection protocols lldp
<get-ddos-lldp-information>
show ddos-protection protocols lldp aggregate
```

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

```
show ddos-protection protocols mac-host
      <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
      <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host aggregate culprit-flows
      <get-ddos-mac-host-aggregate-flows>
show ddos-protection protocols mac-host culprit-flows
      <get-ddos-mac-host-flows>
show ddos-protection protocols mac-host flow-detection
      <get-ddos-mac-host-flow-parameters>
show ddos-protection protocols mac-host parameters
      <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
      <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
      <get-ddos-mac-host-violations>
show ddos-protection protocols martian-address
      <get-ddos-martian-address-information>
show ddos-protection protocols martian-address aggregate
      <get-ddos-martian-address-aggregate>
show ddos-protection protocols martian-address aggregate culprit-flows
      <get-ddos-martian-address-aggregate-flows>
show ddos-protection protocols martian-address culprit-flows
      <get-ddos-martian-address-flows>
show ddos-protection protocols martian-address flow-detection
      <get-ddos-martian-address-flow-parameters>
show ddos-protection protocols martian-address parameters
      <get-ddos-martian-address-parameters>
show ddos-protection protocols martian-address statistics
      <get-ddos-martian-address-statistics>
show ddos-protection protocols martian-address violations
      <get-ddos-martian-address-violations>
show ddos-protection protocols mac-host
   <get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
    <get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host parameters
    <get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
    <get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
    <get-ddos-mac-host-violations>
show ddos-protection protocols mcast-snoop mld
```

```
<get-ddos-mcast-snoop-mld>
show ddos-protection protocols mcast-snoop mld culprit-flows
<get-ddos-mcast-snoop-mld-flows>
show ddos-protection protocols mld
<get-ddos-mld-information>
show ddos-protection protocols mld aggregate
<get-ddos-mld-aggregate>
show ddos-protection protocols mld aggregate culprit-flows
show ddos-protection protocols mld culprit-flows
<get-ddos-mld-flows>
show ddos-protection protocols mld flow-detection
<get-ddos-mld-flow-parameters>
show ddos-protection protocols mld parameters
<get-ddos-mld-parameters>
show ddos-protection protocols mld statistics
<get-ddos-mld-statistics>
show ddos-protection protocols mld violations
<get-ddos-mld-violations>
show ddos-protection protocols mlp
    <get-ddos-mlp-information>
show ddos-protection protocols mlp add
<get-ddos-mlp-add>
show ddos-protection protocols mlp add culprit-flows
<get-ddos-mlp-add-flows>
show ddos-protection protocols mlp aggregate
    <get-ddos-mlp-aggregate>
show ddos-protection protocols mlp aggregate culprit-flows
<get-ddos-mlp-aggregate-flows>
show ddos-protection protocols mlp culprit-flows
<get-ddos-mlp-flows>
show ddos-protection protocols mlp delete
<get-ddos-mlp-delete>
show ddos-protection protocols mlp delete culprit-flows
get-ddos-mlp-delete-flows
show ddos-protection protocols mlp flow-detection
get-ddos-mlp-flow-parameters
show ddos-protection protocols mlp lookup
<get-ddos-mlp-lookup>
show ddos-protection protocols mlp lookup culprit-flows
<get-ddos-mlp-lookup-flows>
show ddos-protection protocols mlp macpin-exception
<get-ddos-mlp-mac-pinning>
show ddos-protection protocols mlp macpin-exception culprit-flows
```

```
<get-ddos-mlp-mac-pinning-flows>
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 multihop-bfd
<get-ddos-mhop-bfd-information>
show ddos-protection protocols multihop-bfd aggregate
<get-ddos-mhop-bfd-aggregate>
show ddos-protection protocols multihop-bfd aggregate culprit-flows
<get-ddos-mhop-bfd-aggregate-flows>
show ddos-protection protocols multihop-bfd culprit-flows
<get-ddos-mhop-bfd-flows>
show ddos-protection protocols multihop-bfd flow-detection
<get-ddos-mhop-bfd-flow-parameters>
```

```
show ddos-protection protocols multihop-bfd parameters
<get-ddos-mhop-bfd-parameters>
show ddos-protection protocols multihop-bfd statistics
<get-ddos-mhop-bfd-statistics>
show ddos-protection protocols multihop-bfd violations
<get-ddos-mhop-bfd-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 ndpv6
<get-ddos-ndpv6-information>
show ddos-protection protocols ndpv6 aggregate
<get-ddos-ndpv6-aggregate>
show ddos-protection protocols ndpv6 aggregate culprit-flows
<get-ddos-ndpv6-aggregate-flows>
show ddos-protection protocols ndpv6 culprit-flows
<get-ddos-ndpv6-flows>
show ddos-protection protocols ndpv6 flow-detection
<get-ddos-ndpv6-flow-parameters>
show ddos-protection protocols ndpv6 neighbor-advertisement
<get-ddos-ndpv6-neighb-adv>
show ddos-protection protocols ndpv6 neighbor-advertisement culprit-flows
<get-ddos-ndpv6-neighb-adv-flows>
show ddos-protection protocols ndpv6 neighbor-solicitation
<get-ddos-ndpv6-neighb-sol>
show ddos-protection protocols ndpv6 neighbor-solicitation culprit-flows
<get-ddos-ndpv6-neighb-sol-flows>
```

```
show ddos-protection protocols ndpv6 parameters
<get-ddos-ndpv6-parameters>
show ddos-protection protocols ndpv6 redirect
<get-ddos-ndpv6-redirect>
show ddos-protection protocols ndpv6 redirect culprit-flows
<get-ddos-ndpv6-redirect-flows>
show ddos-protection protocols ndpv6 router-advertisement
<get-ddos-ndpv6-router-adv>
show ddos-protection protocols ndpv6 router-advertisement culprit-flows
<get-ddos-ndpv6-router-adv-flows>
show ddos-protection protocols ndpv6 router-solicitation
<get-ddos-ndpv6-router-sol>
show ddos-protection protocols ndpv6 router-solicitation culprit-flows
<get-ddos-ndpv6-router-sol-flows>
show ddos-protection protocols nonucast-switch
<get-ddos-nonucast-switch-information>
show ddos-protection protocols nonucast-switch aggregate
<get-ddos-nonucast-switch-aggregate>
show ddos-protection protocols nonucast-switch aggregate culprit-flows
<get-ddos-nonucast-switch-aggregate-flows>
show ddos-protection protocols nonucast-switch culprit-flows
<get-ddos-nonucast-switch-flows>
show ddos-protection protocols nonucast-switch flow-detection
<get-ddos-nonucast-switch-flow-parameters>
show ddos-protection protocols nonucast-switch parameters
<get-ddos-nonucast-switch-parameters>
show ddos-protection protocols nonucast-switch statistics
<get-ddos-nonucast-switch-statistics>
show ddos-protection protocols nonucast-switch violations
<get-ddos-nonucast-switch-violations>
show ddos-protection protocols ntp
    get-ddos-ntp-information
show ddos-protection protocols ntp aggregate
    get-ddos-ntp-aggregate
show ddos-protection protocols ntp parameters
    get-ddos-ntp-parameters
show ddos-protection protocols ntp statistics
    get-ddos-ntp-statistics
show ddos-protection protocols ntp violations
    get-ddos-ntp-violations
show ddos-protection protocols oam-cfm
get-ddos-oam-cfm-information
show ddos-protection protocols oam-cfm aggregate
```

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

```
show ddos-protection protocols ospf-hello parameters
<get-ddos-ospf-hello-parameters>
show ddos-protection protocols ospf-hello statistics
<get-ddos-ospf-hello-statistics>
show ddos-protection protocols ospf-hello violations
<get-ddos-ospf-hello-violations>
show ddos-protection protocols ospfv3v6
    get-ddos-ospfv3v6-information
show ddos-protection protocols ospfv3v6 aggregate
    get-ddos-ospfv3v6-aggregate
show ddos-protection protocols ospfv3v6 parameters
    get-ddos-ospfv3v6-parameters
show ddos-protection protocols ospfv3v6 statistics
    get-ddos-ospfv3v6-statistics
show ddos-protection protocols ospfv3v6 violations
    get-ddos-ospfv3v6-violations
show ddos-protection protocols parameters
    get-ddos-protocols-parameters
show ddos-protection protocols pfe-alive
    get-ddos-pfe-alive-information
show ddos-protection protocols pfe-alive aggregate
    get-ddos-pfe-alive-aggregate
show ddos-protection protocols pfe-alive parameters
    get-ddos-pfe-alive-parameters
show ddos-protection protocols pfe-alive statistics
    get-ddos-pfe-alive-statistics
show ddos-protection protocols pfe-alive violations
    get-ddos-pfe-alive-violations
show ddos-protection protocols pim
    get-ddos-pim-information
show ddos-protection protocols pim aggregate
    get-ddos-pim-aggregate
show ddos-protection protocols pim aggregate culprit-flows
show ddos-protection protocols pim parameters
    get-ddos-pim-parameters
show ddos-protection protocols pim statistics
    get-ddos-pim-statistics
show ddos-protection protocols pim violations
    get-ddos-pim-violations
show ddos-protection protocols pim-ctrl
      <get-ddos-pim-ctrl-information>
show ddos-protection protocols pim-ctrl aggregate
      <get-ddos-pim-ctrl-aggregate>
```

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

```
show ddos-protection protocols pkt-inject aggregate culprit-flows
<get-ddos-pkt-inject-aggregate-flows>
show ddos-protection protocols pkt-inject culprit-flows
<get-ddos-pkt-inject-flows>
show ddos-protection protocols pkt-inject flow-detection
<get-ddos-pkt-inject-flow-parameters>
show ddos-protection protocols pkt-inject parameters
<get-ddos-pkt-inject-parameters>
show ddos-protection protocols pkt-inject statistics
<get-ddos-pkt-inject-statistics>
show ddos-protection protocols pkt-inject violations
<get-ddos-pkt-inject-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 proto-802-1x
<get-ddos-8021x-information>
show ddos-protection protocols proto-802-1x aggregate
<get-ddos-8021x-aggregate>
show ddos-protection protocols proto-802-1x aggregate culprit-flows
get-ddos-8021x-aggregate-flows
show ddos-protection protocols proto-802-1x culprit-flows
<get-ddos-8021x-flows>
show ddos-protection protocols proto-802-1x flow-detection
<get-ddos-8021x-flow-parameters>
show ddos-protection protocols proto-802-1x parameters
<get-ddos-8021x-parameters>
show ddos-protection protocols proto-802-1x statistics
<get-ddos-8021x-statistics>
show ddos-protection protocols proto-802-1x violations
<get-ddos-8021x-violations>
show ddos-protection protocols ptp
    get-ddos-ptp-information
show ddos-protection protocols ptp aggregate
    get-ddos-ptp-aggregate
show ddos-protection protocols ptp aggregate culprit-flows
show ddos-protection protocols ptp parameters
    get-ddos-ptp-parameters
show ddos-protection protocols ptp statistics
    get-ddos-ptp-statistics
show ddos-protection protocols ptp violations
    get-ddos-ptp-violations
show ddos-protection protocols ptpv6
<get-ddos-ptpv6-information>
show ddos-protection protocols ptpv6 aggregate
<get-ddos-ptpv6-aggregate>
show ddos-protection protocols ptpv6 aggregate culprit-flows
<get-ddos-ptpv6-aggregate-flows>
show ddos-protection protocols ptpv6 culprit-flows
<get-ddos-ptpv6-flows>
show ddos-protection protocols ptpv6 flow-detection
<get-ddos-ptpv6-flow-parameters>
show ddos-protection protocols ptpv6 parameters
<get-ddos-ptpv6-parameters>
show ddos-protection protocols ptpv6 statistics
<get-ddos-ptpv6-statistics>
show ddos-protection protocols ptpv6 violations
```

```
<get-ddos-ptpv6-violations>
show ddos-protection protocols pvstp
    get-ddos-pvstp-information
show ddos-protection protocols pvstp aggregate
    get-ddos-pvstp-aggregate
show ddos-protection protocols pvstp parameters
    get-ddos-pvstp-parameters
show ddos-protection protocols pvstp statistics
    get-ddos-pvstp-statistics
show ddos-protection protocols pvstp violations
    get-ddos-pvstp-violations
show ddos-protection protocols radius
    get-ddos-radius-information
show ddos-protection protocols radius accounting
    get-ddos-radius-account
show ddos-protection protocols radius aggregate
    get-ddos-radius-aggregate
show ddos-protection protocols radius accounting culprit-flows
show ddos-protection protocols radius authorization
    get-ddos-radius-auth
show ddos-protection protocols radius parameters
    get-ddos-radius-parameters
show ddos-protection protocols radius server
    get-ddos-radius-server
show ddos-protection protocols radius statistics
    get-ddos-radius-statistics
show ddos-protection protocols radius violations
    get-ddos-radius-violations
show ddos-protection protocols re-services
      <get-ddos-re-services-information>
show ddos-protection protocols re-services aggregate
      <get-ddos-re-services-aggregate>
show ddos-protection protocols re-services aggregate culprit-flows
      <get-ddos-re-services-aggregate-flows>
show ddos-protection protocols re-services captive-portal
      <get-ddos-re-services-captive-portal>
show ddos-protection protocols re-services captive-portal culprit-flows
      <get-ddos-re-services-captive-portal-flows>
show ddos-protection protocols re-services culprit-flows
      <get-ddos-re-services-flows>
show ddos-protection protocols re-services flow-detection
      <get-ddos-re-services-flow-parameters>
show ddos-protection protocols re-services parameters
```

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


show ddos-protection protocols reject
   <get-ddos-reject-information>
show ddos-protection protocols reject aggregate
   <get-ddos-reject-aggregate>
show ddos-protection protocols reject parameters
   <get-ddos-reject-parameters>
```

```
show ddos-protection protocols reject statistics
   <get-ddos-reject-statistics>
show ddos-protection protocols reject violations
   <get-ddos-reject-violations>
show ddos-protection protocols rejectv6show ddos-protection protocols rejectv6 aggregate
show ddos-protection protocols rejectv6 aggregate culprit-flows
show ddos-protection protocols rejectv6 flow-detection
show ddos-protection protocols rejectv6 parameters
show ddos-protection protocols rejectv6 statistics
show ddos-protection protocols rejectv6 violations
show ddos-protection protocols rip
    get-ddos-rip-information
show ddos-protection protocols rip aggregate
    get-ddos-rip-aggregate
show ddos-protection protocols rip aggregate culprit-flows
show ddos-protection protocols rip culprit-flows
show ddos-protection protocols rip parameters
    get-ddos-rip-parameters
show ddos-protection protocols rip statistics
    get-ddos-rip-statistics
show ddos-protection protocols rip violations
    get-ddos-rip-violations
show ddos-protection protocols ripv6
    get-ddos-ripv6-information
show ddos-protection protocols ripv6 aggregate
    get-ddos-ripv6-aggregate
show ddos-protection protocols ripv6 aggregate culprit-flows
show ddos-protection protocols ripv6 parameters
    get-ddos-ripv6-parameters
show ddos-protection protocols ripv6 statistics
    get-ddos-ripv6-statistics
show ddos-protection protocols ripv6 violations
    get-ddos-ripv6-violations
show ddos-protection protocols rsvp
    get-ddos-rsvp-information
show ddos-protection protocols rsvp aggregate
    get-ddos-rsvp-aggregate
show ddos-protection protocols rsvp aggregate culprit-flows
show ddos-protection protocols rsvp parameters
    get-ddos-rsvp-parameters
show ddos-protection protocols rsvp statistics
    get-ddos-rsvp-statistics
show ddos-protection protocols rsvp violations
```

```
    get-ddos-rsvp-violations
show ddos-protection protocols rsvpv6
    get-ddos-rsvpv6-information
show ddos-protection protocols rsvpv6 aggregate
    get-ddos-rsvpv6-aggregate
show ddos-protection protocols rsvpv6 aggregate culprit-flows
show ddos-protection protocols rsvpv6 parameters
    get-ddos-rsvpv6-parameters
show ddos-protection protocols rsvpv6 statistics
    get-ddos-rsvpv6-statistics
show ddos-protection protocols rsvpv6 violations
    get-ddos-rsvpv6-violations
show ddos-protection protocols sample
<get-ddos-sample-information>
show ddos-protection protocols sample aggregate
<get-ddos-sample-aggregate>
show ddos-protection protocols sample aggregate culprit-flows
show ddos-protection protocols sample host
<get-ddos-sample-host>
show ddos-protection protocols sample parameters
<get-ddos-sample-parameters>
show ddos-protection protocols sample pfe
<get-ddos-sample-pfe>
show ddos-protection protocols sample pfe culprit-flows
show ddos-protection protocols sample sflow
<get-ddos-sample-sflow>
show ddos-protection protocols sample sflow culprit-flows
<get-ddos-sample-sflow-flows>
show ddos-protection protocols sample statistics
<get-ddos-sample-statistics>
show ddos-protection protocols sample syslog
show ddos-protection protocols sample tap
<get-ddos-sample-tap>
show ddos-protection protocols sample tap culprit-flows
show ddos-protection protocols sample violations
<get-ddos-sample-violations>
show ddos-protection protocols services
    get-ddos-services-information
show ddos-protection protocols sample-dest
<get-ddos-sample-dest-information>
show ddos-protection protocols sample-dest aggregate
<get-ddos-sample-dest-aggregate>
show ddos-protection protocols sample-dest aggregate culprit-flows
```

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

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

```
    get-ddos-sshv6-aggregate
show ddos-protection protocols sshv6 parameters
    get-ddos-sshv6-parameters
show ddos-protection protocols sshv6 statistics
    <get-ddos-sshv6-statistics>
show ddos-protection protocols sshv6 violations
    <get-ddos-sshv6-violations>
show ddos-protection protocols statistics
    <get-ddos-protocols-statistics>
show ddos-protection protocols stp
    <get-ddos-stp-information>
show ddos-protection protocols stp aggregate
    <get-ddos-stp-aggregate>
show ddos-protection protocols stp parameters
    <get-ddos-stp-parameters>
show ddos-protection protocols stp statistics
    <get-ddos-stp-statistics>
show ddos-protection protocols stp violations
    <get-ddos-stp-violations>
show ddos-protection protocols tacacs
    <get-ddos-tacacs-information>
show ddos-protection protocols tacacs aggregate
    <get-ddos-tacacs-aggregate>
show ddos-protection protocols tacacs parameters
    <get-ddos-tacacs-parameters>
show ddos-protection protocols tacacs statistics
    <get-ddos-tacacs-statistics>
show ddos-protection protocols tacacs violations
    <get-ddos-tacacs-violations>

show ddos-protection protocols tcc
<get-ddos-tcc-information>
show ddos-protection protocols tcc aggregate
<get-ddos-tcc-aggregate>
show ddos-protection protocols tcc aggregate culprit-flows
<get-ddos-tcc-aggregate-flows>
show ddos-protection protocols tcc culprit-flows
<get-ddos-tcc-flows>
show ddos-protection protocols tcc ethernet-tcc
<get-ddos-tcc-ethernet-tcc>
show ddos-protection protocols tcc ethernet-tcc culprit-flows
<get-ddos-tcc-ethernet-tcc-flows>
show ddos-protection protocols tcc flow-detection
```

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

```
    <get-ddos-telnetv6-information>
show ddos-protection protocols telnetv6 aggregate
    <get-ddos-telnetv6-aggregate>
show ddos-protection protocols telnetv6 aggregate culprit-flows
show ddos-protection protocols telnetv6 parameters
    <get-ddos-telnetv6-parameters>
show ddos-protection protocols telnetv6 statistics
    <get-ddos-telnetv6-statistics>
show ddos-protection protocols telnetv6 violations
    <get-ddos-telnetv6-violations>
show ddos-protection protocols ttl
    <get-ddos-ttl-information>
show ddos-protection protocols ttl aggregate
    <get-ddos-ttl-aggregate>
show ddos-protection protocols ttl parameters
    <get-ddos-ttl-parameters>
show ddos-protection protocols ttl statistics
    <get-ddos-ttl-statistics>
show ddos-protection protocols ttl violations
    <get-ddos-ttl-violations>
show ddos-protection protocols tunnel-fragment
    <get-ddos-tun-frag-information>
show ddos-protection protocols tunnel-fragment aggregate
    <get-ddos-tun-frag-aggregate>
show ddos-protection protocols tunnel-fragment aggregate culprit-flows
show ddos-protection protocols tunnel-fragment parameters
    <get-ddos-tun-frag-parameters>
show ddos-protection protocols tunnel-fragment statistics
    <get-ddos-tun-frag-statistics>
show ddos-protection protocols tunnel-fragment violations
    <get-ddos-tun-frag-violations>
show ddos-protection protocols tunnel-ka
      <get-ddos-tunnel-ka-information>
show ddos-protection protocols tunnel-ka aggregate
      <get-ddos-tunnel-ka-aggregate>
show ddos-protection protocols tunnel-ka aggregate culprit-flows
      <get-ddos-tunnel-ka-aggregate-flows>
show ddos-protection protocols tunnel-ka culprit-flows
      <get-ddos-tunnel-ka-flows>
show ddos-protection protocols tunnel-ka flow-detection
      <get-ddos-tunnel-ka-flow-parameters>
show ddos-protection protocols tunnel-ka parameters
      <get-ddos-tunnel-ka-parameters>
```

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

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

```
    get-ddos-vchassis-vc-ttl-err
show ddos-protection protocols virtual-chassis violations
    get-ddos-vchassis-violations
show ddos-protection protocols vrrp
    get-ddos-vrrp-information
show ddos-protection protocols vrrp aggregate
    get-ddos-vrrp-aggregate
show ddos-protection protocols vrrp aggregate culprit-flows
show ddos-protection protocols vrrp parameters
    get-ddos-vrrp-parameters
show ddos-protection protocols vrrp statistics
    get-ddos-vrrp-statistics
show ddos-protection protocols vrrp violations
    get-ddos-vrrp-violations
show ddos-protection protocols vrrpv6
    get-ddos-vrrpv6-information
show ddos-protection protocols vrrpv6 aggregate
    get-ddos-vrrpv6-aggregate
show ddos-protection protocols vrrpv6 aggregate culprit-flows
show ddos-protection protocols vrrpv6 parameters
    get-ddos-vrrpv6-parameters
show ddos-protection protocols vrrpv6 statistics
    get-ddos-vrrpv6-statistics
show ddos-protection protocols vrrpv6 violations
    get-ddos-vrrpv6-violations
show ddos-protection statistics
    get-ddos-statistics-information
show ddos-protection version
    get-ddos-version
show ddos-protection protocols vxlan
      <get-ddos-vxlan-information>
show ddos-protection protocols vxlan aggregate
      <get-ddos-vxlan-aggregate>
show ddos-protection protocols vxlan aggregate culprit-flows
      <get-ddos-vxlan-aggregate-flows>
show ddos-protection protocols vxlan culprit-flows
      <get-ddos-vxlan-flows>
show ddos-protection protocols vxlan flow-detection
      <get-ddos-vxlan-flow-parameters>
show ddos-protection protocols vxlan parameters
      <get-ddos-vxlan-parameters>
show ddos-protection protocols vxlan statistics
      <get-ddos-vxlan-statistics>
```

```
show ddos-protection protocols vxlan violations
      <get-ddos-vxlan-violations>
show dhcp
show dhcp proxy-client
show dhcp proxy-client binding
show dhcp proxy-client servers
show dhcp proxy-client statistics
   <get-proxy-dhcp-client-statistics-information>
show dhcp relay
show dhcp relay binding
    <get-dhcp-relay-binding-information>

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

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

show dhcp server binding interface
<get-dhcp-relay-binding-interface>
show dhcp server binding lease-time-violation
<get-dhcp-server-binding-ltv-information>
show dhcp server statistics
    <get-dhcp-server-statistics-information>
show dhcp statistics
    <get-dhcp-service-statistics-information>
show dhcp-security
<get-dhcp-security-arp-inspection-statistics>
show dhcp-security binding
<get-dhcp-security-binding>
show dhcp-security binding interface
<get-dhcp-security-binding-interface>
show dhcp-security binding ip-address
<get-dhcp-security-binding-ip-address>
```

```
show dhcp-security binding ip-source-guard
<get-dhcp-security-ip-source-guard>
show dhcp-security binding statistics
<get-dhcp-security-binding-statistics>
show dhcp-security binding vlan
get-dhcp-security-binding-vlan
show dhcp-security ipv6
show dhcp-security ipv6 binding
<get-dhcpv6-security-binding>
show dhcp-security ipv6 binding interface
<get-dhcpv6-security-binding-interface>
show dhcp-security ipv6 binding ipv6-address
<get-dhcpv6-security-binding-ip-address>
show dhcp-security ipv6 binding vlan
<get-dhcpv6-security-binding-vlan>
show dhcp-security ipv6 statistics
<get-dhcp-ipv6-statistics>
show dhcp-security neighbor-discovery-inspection
show dhcp-security neighbor-discovery-inspection statistics
<get-dhcp-security-nd-inspection-statistics>
show dhcp-security neighbor-discovery-inspection statistics interface
<get-dhcp-security-ndi-interface>
show dhcp-security statistics
<get-dhcp-security-statistics>

show dhcpv6
show dhcpv6 client
show dhcpv6 client binding
get-dhcpv6-client-binding-information
show dhcpv6 client binding interface
<get-dhcpv6-client-binding-information-by-interface>
show dhcpv6 client statistics
<get-dhcpv6-client-statistics-information>
show dhcpv6 proxy-client
show dhcpv6 proxy-client binding
show dhcpv6 proxy-client statistics
   <get-proxy-dhcpv6-client-statistics-information>
show dhcpv6 relay
show dhcpv6 relay binding
   <get-dhcpv6-relay-binding-information>
show dhcpv6 relay binding interface
<get-dhcpv6-relay-binding-interface>
show dhcpv6 relay binding lease-time-violation
```

```
<get-dhcpv6-relay-binding-ltv-information>
show dhcpv6 relay statistics
   <get-dhcpv6-relay-statistics-information>
show dhcpv6 relay statistics bulk-leasequery-connections
<get-dhcpv6-relay-bulk-leasequery-conn-statistics>
show dhcpv6 relay statistics leasequery
<get-dhcpv6-relay-leasequery-statistics>
show dhcpv6 server
show dhcpv6 server binding
   <get-dhcpv6-server-binding-information>

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

```
    <get-diameter-peer-statistics>
show diameter route
    <get-diameter-route-information>
show dot1x
show dot1x accounting-attributes
get-dot1x-accounting-attributes
show dot1x accounting-attributes interface
<get-dot1x-interface-accounting-attributes>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-addresess>
show dot1x static-mac-address interface
    <get-dot1x-interface-mac-addresses>
show dvmrp
show dvmrp interfaces
    <get-dvmrp-interfaces-information>
show dvmrp neighbors
    <get-dvmrp-neighbors-information>
show dvmrp prefix
    <get-dvmrp-prefix-information>
show dvmrp prunes
    <get-dvmrp-prunes-information>
show dynamic-profile
     <get-dynamic-profile>
show dynamic-profile session
<get-dynamic-profile-session-information>
show dynamic-tunnels
show dynamic-tunnels database
<get-dynamic-tunnels-database>
show ethernet-switching mac-learning-log
<get-ethernet-switching-log-information>
show ethernet-switching mac-notification
<get-ethernet-switching-mac-notification-information>
show ethernet-switching flood next-hops
show ethernet-switching flood next-hops satellite
<get-satellite-control-composite-next-hop>
show ethernet-switching flood satellite
<get-satellite-control-flood>
show ethernet-switching nh-learn-entity
<get-l2-learning-nh-learn-entries>
show ethernet-switching redundancy-groups
```

```
<get-ethernet-switching-redundancy-groups>
show ethernet-switching satellite
show ethernet-switching satellite device
<get-satellite-device-db>
show ethernet-switching satellite events
<get-satellite-control-history-information>
show ethernet-switching satellite logging
<get-satellite-control-logging-information>
show ethernet-switching satellite summary
<get-satellite-control-bridge-summary>
show ethernet-switching table satellite
<get-satellite-control-bridge-mac-table>
show ethernet-switching vxlan-tunnel-end-point esi
<get-ethernet-switching-vxlan-esi-info>
show ethernet-switching vxlan-tunnel-end-point remote
<get-ethernet-switching-vxlan-rvtep-info>
show ethernet-switching vxlan-tunnel-end-point remote esi
<get-ethernet-switching-vxlan-esi-info>
show ethernet-switching vxlan-tunnel-end-point remote vtep-source-interface
<get-ethernet-switching-vxlan-remote-svtep-ip-information>
show ethernet-switching vxlan-tunnel-end-point source ip
<get-ethernet-switching-vxlan-svtep-ip-information>
show ephemeral-configuration
show esis
show esis adjacency
    <get-esis-adjacency-information>
show esis interface
    <get-esis-interface-information>
show esis statistics
    <get-esis-statistics-information>
show event-options
show event-options event-scripts
show event-options event-scripts policies
   <get-event-scripts-policies>
<get-event-summary>
show evpn
show evpn arp-table
<get-evpn-arp-table>
show evpn flood
<get-evpn-flood-information>
show evpn flood event-queue
<get-evpn-event-queue-information>
show evpn flood route
```

```
show evpn flood route all-ce-flood
<get-evpn-all-ce-flood-route-information>
show evpn flood route all-flood
<get-evpn-all-flood-route-information>
show evpn flood route alt-root-flood
<get-evpn-alt-root-flood-route-information>
show evpn flood route ce-flood
<get-evpn-ce-flood-route-information>
show evpn flood route mlp-flood
<get-evpn-mlp-flood-route-information>
show evpn flood route re-flood
<get-evpn-re-flood-route-information>
show evpn instance
<get-evpn-instance-information>show evpn ip-prefix-database
<get-evpn-ip-prefix-database-information>
show evpn l3-context
<get-evpn-l3-context-information>
show evpn mac-table
<get-evpn-mac-table>
show evpn mac-table interface
<get-evpn-interface-mac-table>
show evpn nd-table
<get-evpn-nd-table>
show evpn peer-gateway-macs
<get-evpn-peer-gateway-mac>
show evpn statistics
<get-evpn-statistics-information>
show evpn vpws-instance
<get-evpn-vpws-information>
show extensible-subscriber-services
show extensible-subscriber-services accounting
<get-extensible-subscriber-services-accounting>
show extensible-subscriber-services counters
<get-extensible-subscriber-services-counters>
show extensible-subscriber-services dictionary
<get-extensible-subscriber-services-dictionary>
show extensible-subscriber-services services
<get-extensible-subscriber-services-services>
show extensible-subscriber-services sessions
<get-extensible-subscriber-services-sessions>
show extension-provider
show extension-provider system
show extension-provider system connections
```

```
    <get-mspinfo-connections>
show extension-provider system packages
    <get-mspinfo-packages>
show extension-provider system processes
    <get-mspinfo-processes>
show extension-provider system processes brief
    <get-mspinfo-processes-brief>
show extension-provider system processes extensive
    <get-mspinfo-processes-extensive>
show extension-provider system uptime
    <get-mspinfo-uptime>
show extension-provider system virtual-memory
 <get-core-key-list>
 <get-fabric-summary-information>
 <get-key-vg-binding>
 <get-mac-ip-binding-information>
<get-mc-ccpc-cache-ccpc-select>
<get-mc-ccpc-cache-root-candidates>
<get-mc-ccpc-cache-spf>
 <get-mc-ccpc-src-mod-filters>
<get-mc-edge-cache-ccpc-select>
 <get-mc-edge-map-to-key-binding>
 <get-mc-edge-key-to-map-binding>
 <get-mc-edge-vg-portmap>
 <get-mc-nsf>
<get-mc-root-cache-trunk>
 <get-mc-root-key-to-map-binding>
<get-layer2-group-membership-entries>
<get-layer3-group-membership-entries>
<get-layer3-multicast-pending-routes>
<get-layer3-multicast-receivers>
 <get-mc-root-map-to-key-binding>
 <get-mc-root-vg-pfemap>
<get-fabric-multicast-statistics>
 <get-mc-vccpdf-adjacency-database>
 <get-mspinfo-virtual-memory>
get-fabric-statistics
get-fabric-summary-information
 <get-vlan-domain-map-information>
show fabric multicast dirty-key-info
<get-mc-dirty-key-info>
show fabric multicast edge corekey-ifls-filters
<get-mc-edge-corekey-ifls-filters>
```

```
show fabric multicast edge ine-ifls-filters
<get-mc-edge-ine-ifls-filters>
show fabric multicast edge src-mod-filters
<get-mc-edge-src-mod-filters>
show fabric multicast graph
show fabric multicast graph core-tree
<get-fabric-multicast-graph>
show fabric multicast steal-key-info
<get-mc-steal-key-info>
show forwarding-options
show forwarding-options enhanced-hash-key
show forwarding-options enhanced-hash-key fpc
show forwarding-options hyper-mode
<get forwarding-options hyper-mode>
show forwarding-options load-balance
show forwarding-options next-hop-group
<get-forwarding-options-next-hop-group>
show forwarding-options port-mirroring
<get-forwarding-options-port-mirroring>
show helper
show helper statistics
    <get-helper-statistics-information>
show hfrr
show hfrr profiles
show iccp
   <get-inter-chassis-control-protocol-information>
show igmp
show igmp group
    <get-igmp-group-information>
show igmp interface
    <get-igmp-interface-information>
show igmp output-group
    <get-igmp-output-group-information>
show igmp snooping
show igmp snooping interface
    <get-igmp-snooping-interface-information>
show igmp snooping interface bridge-domain
<get-igmp-snooping-bridge-domain-interface>
show igmp snooping membership
    <get-igmp-snooping-membership-information>
show igmp snooping membership bridge-domain
show igmp snooping options
<get-igmp-snooping-options-information>
```

```
show igmp snooping options
get-igmp-snooping-options-information
show igmp snooping statistics
    <get-igmp-snooping-statistics-information>
show igmp snooping statistics bridge-domain
<get-igmp-snooping-bridge-domain-membership>
show igmp statistics
    <get-igmp-statistics-information>

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

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

show interfaces destination-class all
<get-all-destination-class-statistics>
show interfaces diagnostics
show interfaces diagnostics optics
    <get-interface-optics-diagnostics-information>
show interfaces diagnostics optics satellite
<show-interface-optics-diagnostics-satellite>
show interfaces distribution-list
<get-distribution-list-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 lib-clients
<get-dcd-lib-client-data>
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 bgp-orr
<get-isis-bgporr-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 interface-group
<get-isis-interface-group-information>
show isis layer2-map
<get-isis-layer2-map-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 evpn nd-statistics
<get-evpn-nd-statistics>
show l2-learning evpn nd-statistics interface
<get-evpn-nd-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 esi
<get-l2-learning-vxlan-esi-info>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 auto-sensing
<get-l2ckt-pw-auto-sensing-information>
show l2circuit connections
    <get-l2ckt-connection-information>
```

```
show l2cpd
show l2cpd task
<get-l2cpd-task-information>
show l2cpd task io
   <get-l2cpd-tasks-io-statistics>
show l2cpd task memory
   <get-l2cpd-task-memory>
show l2cpd task replication
   <get-l2cpd-replication-information>
show l2vpn
show l2vpn connections
    <get-l2vpn-connection-information>

show lacp
show lacp interfaces
    <get-lacp-interface-information>
show lacp statistics
show lacp statistics interfaces
    <get-lacp-interface-statistics>
show lacp timeouts
show ldp
show ldp database
    <get-ldp-database-information>

show ldp fec-filters
    <get-ldp-fec-filters-information>

show ldp interface
    <get-ldp-interface-information>

show ldp neighbor
    <get-ldp-neighbor-information>

show ldp oam
<get-ldp-oam-information>
show ldp overview
   <get-ldp-overview-information>
show ldp p2mp
show ldp p2mp fec
  <get-ldp-p2mp-fec-information>
show ldp p2mp path
  <get-ldp-p2mp-path-information>
show ldp p2mp tunnel
```

```
<get-ldp-p2mp-tunnel-information>
show ldp path
    <get-ldp-path-information>

show ldp rib-groups
<get-ldp-rib-groups-information>
show ldp route
    <get-ldp-route-information>

show ldp session
    <get-ldp-session-information>

show ldp statistics
    <get-ldp-statistics-information>

show ldp traffic-statistics
    <get-ldp-traffic-statistics-information>

show link-management
    <get-lm-information>

show link-management peer
    <get-lm-peer-information>

show link-management routing
    <get-lm-routing-information>

show link-management routing peer
    <get-lm-routing-peer-information>

show link-management routing resource
    <get-lm-routing-resource-information>

show link-management routing te-link
    <get-lm-routing-te-link-information>

show lldp
    <get-lldp-information>

show lldp detail
    <get-lldp-information-detail>

show lldp local-information
```

```
    <get-lldp-local-info>

show lldp neighbors
    <get-lldp-neighbors-information>

show lldp neighbors interface
<get-lldp-interface-neighbors>
show lldp remote-global-statistics
    <get-lldp-remote-global-statistics>

show lldp statistics
    <get-lldp-statistics-information>

show lldp statistics interface
<get-lldp-interface-statistics>
show loop-detect
show loop-detect interface
<get-loop-detect-interface-information>
show loop-detect statistics
show loop-detect statistics interface
<get-loop-detect-interface-statistics-information>
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 abstract-hop-membership
<get-mpls-abstract-hop-membership-information>
show mpls admin-groups
    <get-mpls-admin-group-information>

show mpls admin-groups-extended
    <get-mpls-admin-group-extended-information>
show mpls association
show mpls association iif
<get-mpls-association-iif-information>
show mpls association oif
<get-mpls-association-oif-information>
show mpls association path
<get-mpls-association-path-information>
show mpls call-admission-control
    <get-mpls-call-admission-control-information>

show mpls context-identifier
    <get-mpls-context-identifier-information>
show mpls correlation
show mpls correlation label
<get-mpls-correlation-label-information>
show mpls correlation nexthop-id
<get-mpls-correlation-nexthop-information>

show network-access address-assignment preserved
<get-address-assignment-preserved-table>
show network-access domain-map
show network-access domain-map statistics
    <get-domain-map-statistics>
show mpls cspf
```

```
    <get-mpls-cspf-information>

show mpls diffserv-te
    <get-mpls-diffserv-te-information>
show mpls egress-protection
show mpls interface
    <get-mpls-interface-information>
show mpls label
<get mpls-label-space>
show mpls label usage
<get mpls-label-space-usage>

show mpls lsp
    <get-mpls-lsp-information>
show mpls lsp abstract-computation
<get-mpls-lsp-abstract-computation>

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 multi-chassis
show multi-chassis mc-lag
show multi-chassis mc-lag configuration-consistency
<get-mclag-config-consistency-information>
show multi-chassis mc-lag configuration-consistency global-config
<get-mclag-global-config-consistency-information>
show multi-chassis mc-lag configuration-consistency icl-config
<get-mclag-icl-config-consistency-information>
show multi-chassis mc-lag configuration-consistency list-of-parameters<get-mclag-config-
consistency-information-params>
show multi-chassis mc-lag configuration-consistency mcae-config
get-mclag-config-consistency-information-mcae
show multi-chassis mc-lag configuration-consistency vlan-config
<get-mclag-vlan-config-consistency-information>
show multi-chassis mc-lag configuration-consistency vrrp-config
<get-mclag-vrrp-config-consistency-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 ecid-mapping
show multicast ecid-mapping satellite
<get-satellite-control-ecid>
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 next-hops satellite
<get-satellite-control-next-hop>
```

```
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 next-hops satellite
<get-satellite-control-indirect-next-hop>
show multicast snooping route
    <get-multicast-snooping-route-information>
show multicast snooping route satellite
get-satellite-control-multicast


show multicast statistics
    <get-multicast-statistics-information>
show multicast statistics satellite
<get-satellite-control-statistics>
show multicast summary
show multicast summary satellite
<get-satellite-control-summary>

show multicast usage
    <get-multicast-usage-information>

show mvpn
```

```
show mvpn c-multicast
<get-mvpn-c-multicasti-route>
show mvpn instance
    <get-mvpn-instance-information>

show mvpn neighbor
<get-mvpn-neighbor-information>
show mvpn suppressed
get-mvpn-suppressed-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 nasreq
show network-access nasreq statistics
get-nasreq-counters
show network-access ocs
show network-access ocs state
<get-ocs-state-information>
show network-access ocs statistics
<get-ocs-statistics-information>
show network-access pcrf
show network-access pcrf state
<get-pcrf-state-information>
show network-access pcrf statistics
<get-pcrf-statistics-information>

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 sla-iterator-history
<get-cfm-iterator-history>
show oam ethernet connectivity-fault-management
show oam ethernet connectivity-fault-management adjacencies
<get-cfm-adjacency-information>
show oam ethernet connectivity-fault-management delay-statistics
    <get-cfm-delay-statistics>

show oam ethernet connectivity-fault-management forwarding-state
show oam ethernet connectivity-fault-management forwarding-state instance
    <get-cfm-forwarding-state-instance-information>

show oam ethernet connectivity-fault-management forwarding-state interface
    <get-cfm-forwarding-state-interface-information>

show oam ethernet connectivity-fault-management interfaces
    <get-cfm-interfaces-information>
show oam ethernet connectivity-fault-management loss-statistics
    <get-cfm-loss-statistics>
show oam ethernet connectivity-fault-management mep-database
    <get-cfm-mep-database>

show oam ethernet connectivity-fault-management mep-statistics
    <get-cfm-mep-statistics>

show oam ethernet connectivity-fault-management mip
    <get-cfm-mip-information>
```

```
show oam ethernet connectivity-fault-management path-database
    <get-cfm-linktrace-path-database>

show oam ethernet connectivity-fault-management policer
   <get-evc-information>

show oam ethernet connectivity-fault-management sla-iterator-statistics
    <get-cfm-iterator-statistics>
show oam ethernet evc
    <get-evc-infromation>
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 bgp-orr
<get-ospf-bgporr-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 bgp-orr
<get-ospf-bgporr-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 overlay
<get-cloud-analytics-overlay-information>
show overlay vxlan
<get-cloud-analytics-overlay-vxlan-information>
show overlay vxlan vni
<get-application-monitor-overlay-vxlan-information>
show overlay vxlan vtep
<get-application-monitor-overlay-vtep-information>
show ovsdb
```

```
show ovsdb commit
show ovsdb commit failures
<get-ovsdb-commit-failure-information>

show ovsdb tunnels
<get-ovsdb-tunnels-information>
show ovsdb virtual-tunnel-end-point
<get-ovsdb-vtep-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 lsp-retry-pending
<get-path-computation-client-lsp-retry-pending>
show path-computation-client statistics
show performance-monitoring
show performance-monitoring mpls
show performance-monitoring mpls lsp
<get-pm-mpls-lsp-information>
show pfe
show pfe cfeb
show pfe data
<get-pfe-data>
show pfe feb
show pfe filter
show pfe filter hw
show pfe filter hw summary
show pfe fpc
```

```
show pfe fwdd
show pfe lcc
show pfe next-hop
show pfe pfem
show pfe pfem detail
show pfe pfem extensive
show pfe route
show pfe route clnp
show pfe route clnp table
show pfe route inet6
show pfe route inet6 hw
show pfe route inet6 hw host
show pfe route inet6 hw lpm
show pfe route inet6 hw multicast

show pfe route inet6 table
show pfe route ip
show pfe route ip table
show pfe route iso
show pfe route iso table
show pfe scb
show pfe sfm
show pfe ssb
show pfe statistics
show pfe statistics exceptions
show pfe statistics fabric
show pfe statistics ip
show pfe route ip hw
show pfe route ip hw host
show pfe route ip hw lpm
show pfe route ip hw multicast
show pfe route summary
show pfe route summary hw
show pfe statistics ip6
show pfe statistics traffic
    <get-pfe-statistics>
show pfe statistics traffic bandwidth
<get-pfe-traffic-statistics-bandwidth>

show pfe statistics traffic cpu
show pfe statistics traffic cpu fpe
show pfe statistics traffic detail
<get-pfe-traffic-statistics>
```

```
show pfe statistics traffic egress-queues
show pfe statistics traffic egress-queues fpc
show pfe statistics traffic multicast
show pfe statistics traffic multicast fpcshow pfe statistics traffic protocol
show pfe tcam
show pfe tcam app
<get-pfe-tcam-app-list>
show pfe tcam app bd-dtag-validate
<get-pfe-tcam-app-list-bd-dtag-validate>
show pfe tcam app bd-dtag-validate detail
show pfe tcam app bd-dtag-validate list-related-apps
show pfe tcam app bd-dtag-validate list-shared-apps
show pfe tcam app bd-dtag-validate shared-usage
show pfe tcam app bd-dtag-validate shared-usage detail
show pfe tcam app bd-tpid-swap
<get-pfe-tcam-app-list-bd-tpid-swap>
show pfe tcam app bd-tpid-swap detail
show pfe tcam app bd-tpid-swap list-related-apps
show pfe tcam app bd-tpid-swap list-shared-apps
show pfe tcam app bd-tpid-swap shared-usage
show pfe tcam app bd-tpid-swap shared-usage detail
show pfe tcam app cfm-bd-filter
<get-pfe-tcam-app-list-cfm-bd-filter>
show pfe tcam app cfm-bd-filter detail
show pfe tcam app cfm-bd-filter list-related-apps
show pfe tcam app cfm-bd-filter list-shared-apps
show pfe tcam app cfm-bd-filter shared-usage
show pfe tcam app cfm-bd-filter shared-usage detail
show pfe tcam app cfm-filter
<get-pfe-tcam-app-list-cfm-filter>
show pfe tcam app cfm-filter list-related-apps
show pfe tcam app cfm-filter list-shared-apps
show pfe tcam app cfm-filter shared-usage
show pfe tcam app cfm-filter shared-usage detail
show pfe tcam app cfm-vpls-filter
<get-pfe-tcam-app-list-cfm-vpls-filter>
show pfe tcam app cfm-vpls-filter detail
show pfe tcam app cfm-vpls-filter list-related-apps
show pfe tcam app cfm-vpls-filter list-shared-apps
show pfe tcam app cfm-vpls-filter shared-usage
show pfe tcam app cfm-vpls-filter shared-usage detail
show pfe tcam app cfm-vpls-ifl-filter
<get-pfe-tcam-app-list-cfm-vpls-ifl-filter>
```

```
show pfe tcam app cfm-vpls-ifl-filter detail
show pfe tcam app cfm-vpls-ifl-filter list-related-apps
show pfe tcam app cfm-vpls-ifl-filter list-shared-apps
show pfe tcam app cfm-vpls-ifl-filter shared-usage
show pfe tcam app cfm-vpls-ifl-filter shared-usage detail
 show pfe tcam app cos-fc
<get-pfe-tcam-app-list-cos-fc>
show pfe tcam app cos-fc detail
show pfe tcam app cos-fc list-related-apps
show pfe tcam app cos-fc list-shared-apps
show pfe tcam app cos-fc shared-usage
show pfe tcam app cos-fc shared-usage detail
show pfe tcam app fw-ccc-in
<get-pfe-tcam-app-list-fw-ccc-in>
show pfe tcam app fw-ccc-in detail
show pfe tcam app fw-ccc-in list-related-apps
show pfe tcam app fw-ccc-in list-shared-apps
show pfe tcam app fw-ccc-in shared-usage
show pfe tcam app fw-ccc-in shared-usage detail
 show pfe tcam app fw-family-out
<get-pfe-tcam-app-list-fw-family-out>
show pfe tcam app fw-family-out detail
show pfe tcam app fw-family-out list-related-apps
show pfe tcam app fw-family-out list-shared-apps
show pfe tcam app fw-family-out shared-usage
show pfe tcam app fw-family-out shared-usage detail
show pfe tcam app fw-fbf
<get-pfe-tcam-app-list-fw-fbf>
show pfe tcam app fw-fbf detail
show pfe tcam app fw-fbf list-related-apps
show pfe tcam app fw-fbf list-shared-apps
show pfe tcam app fw-fbf shared-usage
show pfe tcam app fw-fbf shared-usage detail
 show pfe tcam app fw-fbf-inet6
<get-pfe-tcam-app-list-fw-fbf-inet6>
show pfe tcam app fw-fbf-inet6 detail
show pfe tcam app fw-fbf-inet6 list-related-apps
show pfe tcam app fw-fbf-inet6 list-shared-apps
show pfe tcam app fw-fbf-inet6 shared-usage
show pfe tcam app fw-fbf-inet6 shared-usage detail
show pfe tcam app fw-ifl-in
<get-pfe-tcam-app-list-fw-ifl-in>
show pfe tcam app fw-ifl-in detail
```

```
show pfe tcam app fw-ifl-in list-related-apps
show pfe tcam app fw-ifl-in list-shared-apps
show pfe tcam app fw-ifl-in shared-usage
show pfe tcam app fw-ifl-in shared-usage detail
show pfe tcam app fw-ifl-out
<get-pfe-tcam-app-list-fw-ifl-out>
show pfe tcam app fw-ifl-out detail
show pfe tcam app fw-ifl-out list-related-apps
show pfe tcam app fw-ifl-out list-shared-apps
show pfe tcam app fw-ifl-out shared-usage
show pfe tcam app fw-ifl-out shared-usage detail
show pfe tcam app fw-inet-ftf
<get-pfe-tcam-app-list-fw-inet-ftf>
show pfe tcam app fw-inet-ftf detail
show pfe tcam app fw-inet-ftf list-related-apps
show pfe tcam app fw-inet-ftf list-shared-apps
show pfe tcam app fw-inet-ftf shared-usage
show pfe tcam app fw-inet-ftf shared-usage detail
show pfe tcam app fw-inet-in
<get-pfe-tcam-app-list-fw-inet-in>
show pfe tcam app fw-inet-in detail
show pfe tcam app fw-inet-in list-related-apps
show pfe tcam app fw-inet-in list-shared-apps
show pfe tcam app fw-inet-in shared-usage
show pfe tcam app fw-inet-in shared-usage detail
show pfe tcam app fw-inet-pm
<get-pfe-tcam-app-list-fw-inet-pm>
show pfe tcam app fw-inet-pm detail
show pfe tcam app fw-inet-pm list-related-apps
show pfe tcam app fw-inet-pm list-shared-apps
show pfe tcam app fw-inet-pm shared-usage
show pfe tcam app fw-inet-pm shared-usage detail
show pfe tcam app fw-inet-rpf
<get-pfe-tcam-app-list-fw-inet-rpf>
show pfe tcam app fw-inet-rpf detail
show pfe tcam app fw-inet-rpf list-related-apps
show pfe tcam app fw-inet-rpf list-shared-apps
show pfe tcam app fw-inet-rpf shared-usage
show pfe tcam app fw-inet-rpf shared-usage detail
show pfe tcam app fw-inet6-family-out
<get-pfe-tcam-app-list-fw-inet6-family-out>
show pfe tcam app fw-inet6-family-out detail
show pfe tcam app fw-inet6-family-out list-related-apps
```

```
show pfe tcam app fw-inet6-family-out list-shared-apps
show pfe tcam app fw-inet6-family-out shared-usage
show pfe tcam app fw-inet6-family-out shared-usage detail
show pfe tcam app fw-inet6-ftf
<get-pfe-tcam-app-list-fw-inet6-ftf>
show pfe tcam app fw-inet6-ftf detail
show pfe tcam app fw-inet6-ftf list-related-apps
show pfe tcam app fw-inet6-ftf list-shared-apps
show pfe tcam app fw-inet6-ftf shared-usage
show pfe tcam app fw-inet6-ftf shared-usage detail
show pfe tcam app fw-inet6-in
<get-pfe-tcam-app-list-fw-inet6-in>
 show pfe tcam app fw-inet6-in detail
show pfe tcam app fw-inet6-in list-related-apps
show pfe tcam app fw-inet6-in list-shared-apps
show pfe tcam app fw-inet6-in shared-usage
 show pfe tcam app fw-inet6-in shared-usage detail
show pfe tcam app fw-inet6-rpf
<get-pfe-tcam-app-list-fw-inet6-rpf>
show pfe tcam app fw-inet6-rpf detail
show pfe tcam app fw-inet6-rpf list-related-apps
show pfe tcam app fw-inet6-rpf list-shared-apps
show pfe tcam app fw-inet6-rpf shared-usage
show pfe tcam app fw-inet6-rpf shared-usage detail
show pfe tcam app fw-l2-in
<get-pfe-tcam-app-list-fw-l2-in>
show pfe tcam app fw-l2-in detail
show pfe tcam app fw-l2-in list-related-apps
show pfe tcam app fw-l2-in list-shared-apps
show pfe tcam app fw-l2-in shared-usage
show pfe tcam app fw-l2-in shared-usage detail
show pfe tcam app fw-mpls-in
<get-pfe-tcam-app-list-fw-mpls-in>
show pfe tcam app fw-mpls-in detail
show pfe tcam app fw-mpls-in list-related-apps
show pfe tcam app fw-mpls-in list-shared-apps
show pfe tcam app fw-mpls-in shared-usage
show pfe tcam app fw-mpls-in shared-usage detail
show pfe tcam app fw-semantics
<get-pfe-tcam-app-list-fw-semantics>
show pfe tcam app fw-semantics detail
show pfe tcam app fw-semantics list-related-apps
show pfe tcam app fw-semantics list-shared-apps
```

```
show pfe tcam app fw-semantics shared-usage
show pfe tcam app fw-semantics shared-usage detail
show pfe tcam app fw-vpls-in
<get-pfe-tcam-app-list-fw-vpls-in>
show pfe tcam app fw-vpls-in detail
 show pfe tcam app fw-vpls-in list-related-apps
show pfe tcam app fw-vpls-in list-shared-apps
show pfe tcam app fw-vpls-in shared-usage
 show pfe tcam app fw-vpls-in shared-usage detail
show pfe tcam app gr-ifl-stats-egr
<get-pfe-tcam-app-list-gr-ifl-statistics-egr>
show pfe tcam app gr-ifl-stats-egr detail
show pfe tcam app gr-ifl-stats-egr list-related-apps
show pfe tcam app gr-ifl-stats-egr list-shared-apps
show pfe tcam app gr-ifl-stats-egr shared-usage
show pfe tcam app gr-ifl-stats-egr shared-usage detail
show pfe tcam app gr-ifl-stats-ing
<get-pfe-tcam-app-list-gr-ifl-statistics-ing>
show pfe tcam app gr-ifl-stats-ing detail
show pfe tcam app gr-ifl-stats-ing list-related-apps
show pfe tcam app gr-ifl-stats-ing list-shared-apps
show pfe tcam app gr-ifl-stats-ing shared-usage
show pfe tcam app gr-ifl-stats-ing shared-usage detail
show pfe tcam app gr-ifl-stats-preing
<get-pfe-tcam-app-list-gr-ifl-statistics-preing>
show pfe tcam app gr-ifl-stats-preing detail
show pfe tcam app gr-ifl-stats-preing list-related-apps
show pfe tcam app gr-ifl-stats-preing list-shared-apps
show pfe tcam app gr-ifl-stats-preing shared-usage
show pfe tcam app gr-ifl-stats-preing shared-usage detail
show pfe tcam app ifd-src-mac-fil
<get-pfe-tcam-app-list-ifd-src-mac-fil>
show pfe tcam app ifd-src-mac-fil detail
show pfe tcam app ifd-src-mac-fil list-related-apps
show pfe tcam app ifd-src-mac-fil list-shared-apps
show pfe tcam app ifd-src-mac-fil shared-usage
show pfe tcam app ifd-src-mac-fil shared-usage detail
show pfe tcam app ifl-statistics-in
<get-pfe-tcam-app-list-ifl-statistics-in>
show pfe tcam app ifl-statistics-in detail
show pfe tcam app ifl-statistics-in list-related-apps
show pfe tcam app ifl-statistics-in list-shared-apps
show pfe tcam app ifl-statistics-in shared-usage
```

```
show pfe tcam app ifl-statistics-in shared-usage detail
show pfe tcam app ifl-statistics-out
<get-pfe-tcam-app-list-ifl-statistics-out>
 show pfe tcam app ifl-statistics-out detail
show pfe tcam app ifl-statistics-out list-related-apps
show pfe tcam app ifl-statistics-out list-shared-apps
show pfe tcam app ifl-statistics-out shared-usage
show pfe tcam app ifl-statistics-out shared-usage detail
show pfe tcam app ing-out-iff
<get-pfe-tcam-app-list-ing-out-iff>
show pfe tcam app ing-out-iff detail
show pfe tcam app ing-out-iff list-related-apps
show pfe tcam app ing-out-iff list-shared-apps
show pfe tcam app ing-out-iff shared-usage
show pfe tcam app ing-out-iff shared-usage detail
show pfe tcam app ip-mac-val
<get-pfe-tcam-app-list-ip-mac-val>
show pfe tcam app ip-mac-val detail
show pfe tcam app ip-mac-val list-related-apps
show pfe tcam app ip-mac-val list-shared-apps
show pfe tcam app ip-mac-val shared-usage
show pfe tcam app ip-mac-val shared-usage detail
show pfe tcam app ip-mac-val-bcast
<get-pfe-tcam-app-list-ip-mac-val-bcast>
show pfe tcam app ip-mac-val-bcast detail
show pfe tcam app ip-mac-val-bcast list-related-apps
show pfe tcam app ip-mac-val-bcast list-shared-apps
show pfe tcam app ip-mac-val-bcast shared-usage
show pfe tcam app ip-mac-val-bcast shared-usage detail
show pfe tcam app ipsec-reverse-fil
<get-pfe-tcam-app-list-ipsec-reverse-fil>
show pfe tcam app ipsec-reverse-fil detail
show pfe tcam app ipsec-reverse-fil list-related-apps
show pfe tcam app ipsec-reverse-fil list-shared-apps
show pfe tcam app ipsec-reverse-fil shared-usage
show pfe tcam app ipsec-reverse-fil shared-usage detail
show pfe tcam app irb-cos-rw
<get-pfe-tcam-app-list-irb-cos-rw>
show pfe tcam app irb-cos-rw detail
show pfe tcam app irb-cos-rw list-related-apps
show pfe tcam app irb-cos-rw list-shared-apps
show pfe tcam app irb-cos-rw shared-usage
show pfe tcam app irb-cos-rw shared-usage detail
```

```
show pfe tcam app irb-fixed-cos
<get-pfe-tcam-app-list-irb-fixed-cos>
show pfe tcam app irb-fixed-cos detail
show pfe tcam app irb-fixed-cos list-related-apps
show pfe tcam app irb-fixed-cos list-shared-apps
show pfe tcam app irb-fixed-cos shared-usage
show pfe tcam app irb-fixed-cos shared-usage detail
show pfe tcam app irb-inet6-fil
<get-pfe-tcam-app-list-irb-inet6-fil>
show pfe tcam app irb-inet6-fil detail
show pfe tcam app irb-inet6-fil list-related-apps
show pfe tcam app irb-inet6-fil list-shared-apps
show pfe tcam app irb-inet6-fil shared-usage
show pfe tcam app irb-inet6-fil shared-usage detail
show pfe tcam app lfm-802.3ah-in
<get-pfe-tcam-app-list-lfm-802.3ah-in>
show pfe tcam app lfm-802.3ah-in detail
show pfe tcam app lfm-802.3ah-in list-related-apps
show pfe tcam app lfm-802.3ah-in list-shared-apps
 show pfe tcam app lfm-802.3ah-in shared-usage
show pfe tcam app lfm-802.3ah-in shared-usage detail
show pfe tcam app lfm-802.3ah-out
<get-pfe-tcam-app-list-lfm-802.3ah-out>
show pfe tcam app lfm-802.3ah-out detail
show pfe tcam app lfm-802.3ah-out list-related-apps
show pfe tcam app lfm-802.3ah-out list-shared-apps
show pfe tcam app lfm-802.3ah-out shared-usage
show pfe tcam app lfm-802.3ah-out shared-usage detail
show pfe tcam app lo0-inet-fil
<get-pfe-tcam-app-list-lo0-inet-fil>
show pfe tcam app lo0-inet-fil detail
show pfe tcam app lo0-inet-fil list-related-apps
show pfe tcam app lo0-inet-fil list-shared-apps
show pfe tcam app lo0-inet-fil shared-usage
show pfe tcam app lo0-inet-fil shared-usage detail
show pfe tcam app lo0-inet6-fil
<get-pfe-tcam-app-list-lo0-inet6-fil>
show pfe tcam app lo0-inet6-fil detail
show pfe tcam app lo0-inet6-fil list-related-apps
show pfe tcam app lo0-inet6-fil list-shared-apps
show pfe tcam app lo0-inet6-fil shared-usage
show pfe tcam app lo0-inet6-fil shared-usage detail
show pfe tcam app mac-drop-cnt
```

```
<get-pfe-tcam-app-list-mac-drop-cnt>
show pfe tcam app mac-drop-cnt detail
show pfe tcam app mac-drop-cnt list-related-apps
show pfe tcam app mac-drop-cnt list-shared-apps
show pfe tcam app mac-drop-cnt shared-usage
show pfe tcam app mac-drop-cnt shared-usage detail
show pfe tcam app mrouter-port-in
<get-pfe-tcam-app-list-mrouter-port-in>
show pfe tcam app mrouter-port-in detail
show pfe tcam app mrouter-port-in list-related-apps
show pfe tcam app mrouter-port-in list-shared-apps
show pfe tcam app mrouter-port-in shared-usage
show pfe tcam app mrouter-port-in shared-usage detail
show pfe tcam app napt-reverse-fil
<get-pfe-tcam-app-list-napt-reverse-fil>
show pfe tcam app napt-reverse-fil detail
show pfe tcam app napt-reverse-fil list-related-apps
show pfe tcam app napt-reverse-fil list-shared-apps
show pfe tcam app napt-reverse-fil shared-usage
show pfe tcam app napt-reverse-fil shared-usage detail
show pfe tcam app no-local-switching
<get-pfe-tcam-app-list-no-local-switching>
show pfe tcam app no-local-switching detail
show pfe tcam app no-local-switching list-related-apps
show pfe tcam app no-local-switching list-shared-apps
show pfe tcam app no-local-switching shared-usage
show pfe tcam app no-local-switching shared-usage detail
show pfe tcam app ptpoe-cos-rw
<get-pfe-tcam-app-list-ptpoe-cos-rw>
show pfe tcam app ptpoe-cos-rw detail
show pfe tcam app ptpoe-cos-rw list-related-apps
show pfe tcam app ptpoe-cos-rw list-shared-apps
show pfe tcam app ptpoe-cos-rw shared-usage
show pfe tcam app ptpoe-cos-rw shared-usage detail
show pfe tcam app rfc2544-layer2-in
<get-pfe-tcam-app-list-rfc2544-layer2-in>
 show pfe tcam app rfc2544-layer2-in detail
show pfe tcam app rfc2544-layer2-in list-related-apps
 show pfe tcam app rfc2544-layer2-in list-shared-apps
show pfe tcam app rfc2544-layer2-in shared-usage
show pfe tcam app rfc2544-layer2-in shared-usage detail
show pfe tcam app rfc2544-layer2-out
<get-pfe-tcam-app-list-rfc2544-layer2-out>
```

```
show pfe tcam app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam app vpls-mesh-group-mcast detail
show pfe tcam app vpls-mesh-group-mcast list-related-apps
show pfe tcam app vpls-mesh-group-mcast list-shared-apps
show pfe tcam app vpls-mesh-group-mcast shared-usage
show pfe tcam app vpls-mesh-group-mcast shared-usage detail
show pfe tcam app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam app vpls-mesh-group-ucast detail
show pfe tcam app vpls-mesh-group-ucast list-related-apps
show pfe tcam app vpls-mesh-group-ucast list-shared-apps
show pfe tcam app vpls-mesh-group-ucast shared-usage
show pfe tcam app vpls-mesh-group-ucast shared-usage detail
show pfe tcam app cfm-filter detail
show pfe tcam errors app fw-inet-rpf
<get-pfe-tcam-errors-app-fw-inet-rpf>
show pfe tcam errors app fw-inet-rpf detail
show pfe tcam errors app fw-inet-rpf list-related-apps
show pfe tcam errors app fw-inet-rpf list-shared-apps
show pfe tcam errors app fw-inet-rpf shared-usage
show pfe tcam errors app fw-inet-rpf shared-usage detail
show pfe tcam errors app fw-inet6-rpf
<get-pfe-tcam-errors-app-fw-inet6-rpf>
show pfe tcam errors app fw-inet6-rpf detail
show pfe tcam errors app fw-inet6-rpf list-related-apps
show pfe tcam errors app fw-inet6-rpf list-shared-apps
show pfe tcam errors app fw-inet6-rpf shared-usage
show pfe tcam errors app fw-inet6-rpf shared-usage detail
show pfe tcam errors app gr-ifl-stats-egr
<get-pfe-tcam-errors-app-gr-ifl-statistics-egr>
show pfe tcam errors app gr-ifl-stats-egr detail
show pfe tcam errors app gr-ifl-stats-egr list-related-apps
show pfe tcam errors app gr-ifl-stats-egr list-shared-apps
show pfe tcam errors app gr-ifl-stats-egr shared-usage
show pfe tcam errors app gr-ifl-stats-egr shared-usage detail
show pfe tcam errors app gr-ifl-stats-ing
<get-pfe-tcam-errors-app-gr-ifl-statistics-ing>
show pfe tcam errors app gr-ifl-stats-ing detail
show pfe tcam errors app gr-ifl-stats-ing list-related-apps
show pfe tcam errors app gr-ifl-stats-ing list-shared-apps
show pfe tcam errors app gr-ifl-stats-ing shared-usage
show pfe tcam errors app gr-ifl-stats-ing shared-usage detail
```

```
show pfe tcam errors app gr-ifl-stats-preing
<get-pfe-tcam-errors-app-gr-ifl-statistics-preing>
show pfe tcam errors app gr-ifl-stats-preing detail
show pfe tcam errors app gr-ifl-stats-preing list-related-apps
show pfe tcam errors app gr-ifl-stats-preing list-shared-apps
show pfe tcam errors app gr-ifl-stats-preing shared-usage
show pfe tcam errors app gr-ifl-stats-preing shared-usage detail
show pfe tcam errors app ing-out-iff
<get-pfe-tcam-errors-app-ing-out-iff>
show pfe tcam errors app ing-out-iff detail
show pfe tcam errors app ing-out-iff list-related-apps
show pfe tcam errors app ing-out-iff list-shared-apps
show pfe tcam errors app ing-out-iff shared-usage
show pfe tcam errors app ing-out-iff shared-usage detail
show pfe tcam errors app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam errors app vpls-mesh-group-mcast detail
show pfe tcam errors app vpls-mesh-group-mcast list-related-apps
show pfe tcam errors app vpls-mesh-group-mcast list-shared-apps
show pfe tcam errors app vpls-mesh-group-mcast shared-usage
show pfe tcam errors app vpls-mesh-group-mcast shared-usage detail
show pfe tcam errors app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam errors app vpls-mesh-group-ucast detail
show pfe tcam errors app vpls-mesh-group-ucast list-related-apps
show pfe tcam errors app vpls-mesh-group-ucast list-shared-apps
show pfe tcam errors app vpls-mesh-group-ucast shared-usage
show pfe tcam errors app vpls-mesh-group-ucast shared-usage detail
show pfe tcam errors tcam-stage ingress app fw-inet-rpf
<get-pfe-tcam-errors-ingress-tcam-stage-fw-inet-rpf>
show pfe tcam errors tcam-stage ingress app fw-inet-rpf detail
show pfe tcam errors tcam-stage ingress app fw-inet-rpf list-related-apps
show pfe tcam errors tcam-stage ingress app fw-inet-rpf list-shared-apps
show pfe tcam errors tcam-stage ingress app fw-inet-rpf shared-usage
show pfe tcam errors tcam-stage ingress app fw-inet-rpf shared-usage detail
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf
<get-pfe-tcam-errors-ingress-tcam-stage-fw-inet6-rpf>
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf detail
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf list-related-apps
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf list-shared-apps
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf shared-usage
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr
```

```
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-egr>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr shared-usage
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-ing>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing shared-usage
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-preing>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing shared-usage
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing shared-usage detail
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff
<get-pfe-tcam-errors-pre-ingress-app-ing-out-iff>
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff detail
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff list-related-apps
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff shared-usage
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff shared-usage detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-related-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-related-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage detail
show pfe tcam usage app fw-inet-rpf
<get-pfe-tcam-usage-app-fw-inet-rpf>
```

```
show pfe tcam usage app fw-inet-rpf detail
show pfe tcam usage app fw-inet-rpf list-related-apps
show pfe tcam usage app fw-inet-rpf list-shared-apps
show pfe tcam usage app fw-inet-rpf shared-usage
show pfe tcam usage app fw-inet-rpf shared-usage detail
show pfe tcam usage app fw-inet6-rpf
<get-pfe-tcam-usage-app-fw-inet6-rpf>
show pfe tcam usage app fw-inet6-rpf detail
show pfe tcam usage app fw-inet6-rpf list-related-apps
show pfe tcam usage app fw-inet6-rpf list-shared-apps
show pfe tcam usage app fw-inet6-rpf shared-usage
show pfe tcam usage app fw-inet6-rpf shared-usage detail
show pfe tcam usage app gr-ifl-stats-egr
<get-pfe-tcam-usage-app-gr-ifl-statistics-egr>
show pfe tcam usage app gr-ifl-stats-egr detail
show pfe tcam usage app gr-ifl-stats-egr list-related-apps
show pfe tcam usage app gr-ifl-stats-egr list-shared-apps
show pfe tcam usage app gr-ifl-stats-egr shared-usage
show pfe tcam usage app gr-ifl-stats-egr shared-usage detail
show pfe tcam usage app gr-ifl-stats-ing
<get-pfe-tcam-usage-app-gr-ifl-statistics-ing>
show pfe tcam usage app gr-ifl-stats-ing detail
show pfe tcam usage app gr-ifl-stats-ing list-related-apps
show pfe tcam usage app gr-ifl-stats-ing list-shared-apps
show pfe tcam usage app gr-ifl-stats-ing shared-usage
show pfe tcam usage app gr-ifl-stats-ing shared-usage detail
show pfe tcam usage app gr-ifl-stats-preing
<get-pfe-tcam-usage-app-gr-ifl-statistics-preing>
show pfe tcam usage app gr-ifl-stats-preing detail
show pfe tcam usage app gr-ifl-stats-preing list-related-apps
show pfe tcam usage app gr-ifl-stats-preing list-shared-apps
show pfe tcam usage app gr-ifl-stats-preing shared-usage
show pfe tcam usage app gr-ifl-stats-preing shared-usage detail
show pfe tcam usage app ing-out-iff
<get-pfe-tcam-usage-app-ing-out-iff>
show pfe tcam usage app ing-out-iff detail
show pfe tcam usage app ing-out-iff list-related-apps
show pfe tcam usage app ing-out-iff list-shared-apps
show pfe tcam usage app ing-out-iff shared-usage
show pfe tcam usage app ing-out-iff shared-usage detail
show pfe tcam usage app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam usage app vpls-mesh-group-mcast detail
```

```
show pfe tcam usage app vpls-mesh-group-mcast list-related-apps
show pfe tcam usage app vpls-mesh-group-mcast list-shared-apps
show pfe tcam usage app vpls-mesh-group-mcast shared-usage
show pfe tcam usage app vpls-mesh-group-mcast shared-usage detail
show pfe tcam usage app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam usage app vpls-mesh-group-ucast detail
show pfe tcam usage app vpls-mesh-group-ucast list-related-apps
show pfe tcam usage app vpls-mesh-group-ucast list-shared-apps
show pfe tcam usage app vpls-mesh-group-ucast shared-usage
show pfe tcam usage app vpls-mesh-group-ucast shared-usage detail
show pfe tcam usage tcam-stage egress app rfc2544-layer2-out shared-usage detail
show pfe tcam usage tcam-stage egress detail
get-pfe-tcam-usage-egress-tcam-stage-detail
show pfe tcam usage tcam-stage ingress
<get-pfe-tcam-usage-ingress-tcam-stage>
show pfe tcam usage tcam-stage ingress app
<get-pfe-tcam-usage-ingress-app>
show pfe tcam usage tcam-stage ingress app cfm-bd-filter
<get-pfe-tcam-usage-ingress-app-cfm-bd-filter>
show pfe tcam usage tcam-stage ingress app cfm-bd-filter detail
show pfe tcam usage tcam-stage ingress app cfm-bd-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-bd-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-bd-filter shared-usage
show pfe tcam usage tcam-stage ingress app cfm-bd-filter shared-usage detail
show pfe tcam usage tcam-stage ingress app cfm-filter
<get-pfe-tcam-usage-ingress-app-cfm-filter>
show pfe tcam usage tcam-stage ingress app cfm-filter detail
show pfe tcam usage tcam-stage ingress app cfm-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-filter shared-usage
show pfe tcam usage tcam-stage ingress app cfm-filter shared-usage detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter
<get-pfe-tcam-usage-ingress-app-cfm-vpls-filter>
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter shared-usage
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter shared-usage detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter
<get-pfe-tcam-usage-ingress-app-cfm-vpls-ifl-filter>
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter list-related-apps
```

```
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter shared-usage
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-ccc-in
<get-pfe-tcam-usage-ingress-app-fw-ccc-in>
show pfe tcam usage tcam-stage ingress app fw-ccc-in detail
show pfe tcam usage tcam-stage ingress app fw-ccc-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-ccc-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-ccc-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-ccc-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-ifl-in
<get-pfe-tcam-usage-ingress-app-fw-ifl-in>
show pfe tcam usage tcam-stage ingress app fw-ifl-in detail
show pfe tcam usage tcam-stage ingress app fw-ifl-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-ifl-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-ifl-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-ifl-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet-ftf
<get-pfe-tcam-usage-ingress-app-fw-inet-ftf>
show pfe tcam usage tcam-stage ingress app fw-inet-ftf detail
show pfe tcam usage tcam-stage ingress app fw-inet-ftf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-ftf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-ftf shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet-ftf shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet-in
<get-pfe-tcam-usage-ingress-app-fw-inet-in>
show pfe tcam usage tcam-stage ingress app fw-inet-in detail
show pfe tcam usage tcam-stage ingress app fw-inet-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet-pm
<get-pfe-tcam-usage-ingress-app-fw-inet-pm>
show pfe tcam usage tcam-stage ingress app fw-inet-pm detail
show pfe tcam usage tcam-stage ingress app fw-inet-pm list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-pm list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-pm shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet-pm shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet-rpf
<get-pfe-tcam-usage-ingress-app-fw-inet-rpf>
show pfe tcam usage tcam-stage ingress app fw-inet-rpf detail
show pfe tcam usage tcam-stage ingress app fw-inet-rpf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-rpf list-shared-apps
```

```
show pfe tcam usage tcam-stage ingress app fw-inet-rpf shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet-rpf shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf
<get-pfe-tcam-usage-ingress-app-fw-inet6-ftf>
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf detail
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet6-in
<get-pfe-tcam-usage-ingress-app-fw-inet6-in>
show pfe tcam usage tcam-stage ingress app fw-inet6-in detail
show pfe tcam usage tcam-stage ingress app fw-inet6-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet6-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf
<get-pfe-tcam-usage-ingress-app-fw-inet6-rpf>
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf detail
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf shared-usage
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-l2-in
<get-pfe-tcam-usage-ingress-app-fw-l2-in>
show pfe tcam usage tcam-stage ingress app fw-l2-in detail
show pfe tcam usage tcam-stage ingress app fw-l2-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-l2-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-l2-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-l2-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-mpls-in
<get-pfe-tcam-usage-ingress-app-fw-mpls-in>
show pfe tcam usage tcam-stage ingress app fw-mpls-in detail
show pfe tcam usage tcam-stage ingress app fw-mpls-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-mpls-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-mpls-in shared-usage
show pfe tcam usage tcam-stage ingress app fw-mpls-in shared-usage detail
show pfe tcam usage tcam-stage ingress app fw-vpls-in
<get-pfe-tcam-usage-ingress-app-fw-vpls-in>
show pfe tcam usage tcam-stage ingress app fw-vpls-in detail
show pfe tcam usage tcam-stage ingress app fw-vpls-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-vpls-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-vpls-in shared-usage
```

```
show pfe tcam usage tcam-stage ingress app fw-vpls-in shared-usage detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-egr>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr shared-usage
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr shared-usage detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-ing>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing shared-usage
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing shared-usage detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-preing>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing shared-usage
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing shared-usage detail
show pfe tcam usage tcam-stage ingress app ifl-statistics-in
<get-pfe-tcam-usage-ingress-app-ifl-statistics-in>
show pfe tcam usage tcam-stage ingress app ifl-statistics-in detail
show pfe tcam usage tcam-stage ingress app ifl-statistics-in list-related-apps
show pfe tcam usage tcam-stage ingress app ifl-statistics-in list-shared-apps
show pfe tcam usage tcam-stage ingress app ifl-statistics-in shared-usage
show pfe tcam usage tcam-stage ingress app ifl-statistics-in shared-usage detail
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil
<get-pfe-tcam-usage-ingress-app-ipsec-reverse-fil>
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil detail
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil list-related-apps
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil shared-usage
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil shared-usage detail
show pfe tcam usage tcam-stage ingress app irb-fixed-cos
<get-pfe-tcam-usage-ingress-app-irb-fixed-cos>
show pfe tcam usage tcam-stage ingress app irb-fixed-cos detail
show pfe tcam usage tcam-stage ingress app irb-fixed-cos list-related-apps
show pfe tcam usage tcam-stage ingress app irb-fixed-cos list-shared-apps
show pfe tcam usage tcam-stage ingress app irb-fixed-cos shared-usage
show pfe tcam usage tcam-stage ingress app irb-fixed-cos shared-usage detail
```

```
show pfe tcam usage tcam-stage ingress app irb-inet6-fil
<get-pfe-tcam-usage-ingress-app-irb-inet6-fil>
show pfe tcam usage tcam-stage ingress app irb-inet6-fil detail
show pfe tcam usage tcam-stage ingress app irb-inet6-fil list-related-apps
show pfe tcam usage tcam-stage ingress app irb-inet6-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app irb-inet6-fil shared-usage
show pfe tcam usage tcam-stage ingress app irb-inet6-fil shared-usage detail
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in
<get-pfe-tcam-usage-ingress-app-lfm-802.3ah-in>
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in detail
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in list-related-apps
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in list-shared-apps
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in shared-usage
show pfe tcam usage tcam-stage ingress app lfm-802.3ah-in shared-usage detail
show pfe tcam usage tcam-stage ingress app lo0-inet-fil
<get-pfe-tcam-usage-ingress-app-lo0-inet-fil>
show pfe tcam usage tcam-stage ingress app lo0-inet-fil detail
show pfe tcam usage tcam-stage ingress app lo0-inet-fil list-related-apps
show pfe tcam usage tcam-stage ingress app lo0-inet-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app lo0-inet-fil shared-usage
show pfe tcam usage tcam-stage ingress app lo0-inet-fil shared-usage detail
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil
<get-pfe-tcam-usage-ingress-app-lo0-inet6-fil>
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil detail
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil list-related-apps
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil shared-usage
show pfe tcam usage tcam-stage ingress app lo0-inet6-fil shared-usage detail
show pfe tcam usage tcam-stage ingress app mac-drop-cnt
<get-pfe-tcam-usage-ingress-app-mac-drop-cnt>
show pfe tcam usage tcam-stage ingress app mac-drop-cnt detail
show pfe tcam usage tcam-stage ingress app mac-drop-cnt list-related-apps
show pfe tcam usage tcam-stage ingress app mac-drop-cnt list-shared-apps
show pfe tcam usage tcam-stage ingress app mac-drop-cnt shared-usage
show pfe tcam usage tcam-stage ingress app mac-drop-cnt shared-usage detail
<get-pfe-tcam-usage-ingress-app-mrouter-port-in>
show pfe tcam usage tcam-stage ingress app mrouter-port-in detail
show pfe tcam usage tcam-stage ingress app mrouter-port-in list-related-apps
show pfe tcam usage tcam-stage ingress app mrouter-port-in list-shared-apps
show pfe tcam usage tcam-stage ingress app mrouter-port-in shared-usage
show pfe tcam usage tcam-stage ingress app mrouter-port-in shared-usage detail
show pfe tcam usage tcam-stage ingress app napt-reverse-fil
```

```
<get-pfe-tcam-usage-ingress-app-napt-reverse-fil>
show pfe tcam usage tcam-stage ingress app napt-reverse-fil detail
show pfe tcam usage tcam-stage ingress app napt-reverse-fil list-related-apps
show pfe tcam usage tcam-stage ingress app napt-reverse-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app napt-reverse-fil shared-usage
show pfe tcam usage tcam-stage ingress app napt-reverse-fil shared-usage detail
show pfe tcam usage tcam-stage ingress app no-local-switching
<get-pfe-tcam-usage-ingress-app-no-local-switching>
show pfe tcam usage tcam-stage ingress app no-local-switching detail
show pfe tcam usage tcam-stage ingress app no-local-switching list-related-apps
show pfe tcam usage tcam-stage ingress app no-local-switching list-shared-apps
show pfe tcam usage tcam-stage ingress app no-local-switching shared-usage
show pfe tcam usage tcam-stage ingress app no-local-switching shared-usage detail
show pfe tcam usage tcam-stage ingress detail
<get-pfe-tcam-usage-ingress-tcam-stage-detail>
show pfe tcam usage tcam-stage pre-ingress
<get-pfe-tcam-usage-pre-ingress-tcam-stage>
show pfe tcam usage tcam-stage pre-ingress app
<get-pfe-tcam-usage-pre-ingress-app>
show pfe tcam usage tcam-stage pre-ingress app cos-fc
<get-pfe-tcam-usage-pre-ingress-app-cos-fc>
show pfe tcam usage tcam-stage pre-ingress app cos-fc detail
show pfe tcam usage tcam-stage pre-ingress app cos-fc list-related-apps
show pfe tcam usage tcam-stage pre-ingress app cos-fc list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app cos-fc shared-usage
show pfe tcam usage tcam-stage pre-ingress app cos-fc shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app fw-fbf
<get-pfe-tcam-usage-pre-ingress-app-fw-fbf>
show pfe tcam usage tcam-stage pre-ingress app fw-fbf detail
show pfe tcam usage tcam-stage pre-ingress app fw-fbf list-related-apps
show pfe tcam usage tcam-stage pre-ingress app fw-fbf list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app fw-fbf shared-usage
show pfe tcam usage tcam-stage pre-ingress app fw-fbf shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6
<get-pfe-tcam-usage-pre-ingress-app-fw-fbf-inet6>
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6 detail
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6 list-related-apps
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6 list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6 shared-usage
show pfe tcam usage tcam-stage pre-ingress app fw-fbf-inet6 shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app fw-semantics
<get-pfe-tcam-usage-pre-ingress-app-fw-semantics>
show pfe tcam usage tcam-stage pre-ingress app fw-semantics detail
```

```
show pfe tcam usage tcam-stage pre-ingress app fw-semantics list-related-apps
show pfe tcam usage tcam-stage pre-ingress app fw-semantics list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app fw-semantics shared-usage
show pfe tcam usage tcam-stage pre-ingress app fw-semantics shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app ifd-src-mac-fil
<get-pfe-tcam-usage-pre-ingress-app-ifd-src-mac-fil>
show pfe tcam usage tcam-stage pre-ingress app ifd-src-mac-fil detail
show pfe tcam usage tcam-stage pre-ingress app ifd-src-mac-fil list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app ifd-src-mac-fil shared-usage
show pfe tcam usage tcam-stage pre-ingress app ifd-src-mac-fil shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff
<get-pfe-tcam-usage-pre-ingress-app-ing-out-iff>
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff detail
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff list-related-apps
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff shared-usage
show pfe tcam usage tcam-stage pre-ingress app ing-out-iff shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val
<get-pfe-tcam-usage-pre-ingress-app-ip-mac-val>
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val detail
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val list-related-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val shared-usage
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast
<get-pfe-tcam-usage-pre-ingress-app-ip-mac-val-bcast>
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast detail
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast list-related-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast shared-usage
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in
<get-pfe-tcam-usage-pre-ingress-app-rfc2544-layer2-in>
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in detail
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in list-related-apps
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in shared-usage
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast list-related-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast list-shared-apps
```

```
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast list-related-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage detail
show pfe tcam usage tcam-stage pre-ingress detail
<get-pfe-tcam-usage-pre-ingress-tcam-stage-detail>
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 lockout atm-identifier
<get-pppoe-lockout-atm-information>
show pppoe lockout vlan-identifier
<get-pppoe-lockout-vlan-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 programmable-rpd
show programmable-rpd clients
<get-programmable-rpd-client-information>

show protection-group
show protection-group ethernet-aps
    <show-protection-group-ethernet-aps>
show protection-group ethernet-ring
show protection-group ethernet-ring aps
   <get-raps-pdu-information>
show protection-group ethernet-ring data-channel
   <get-ring-data-channel-information>
show protection-group ethernet-ring interface
   <get-ring-interface-information>
show protection-group ethernet-ring node-state
   <get-raps-state-machine-information>
show protection-group ethernet-ring node-state
show protection-group ethernet-ring statistics
   <get-ring-tatistics>
show protection-group ethernet-ring vlan
   <get-ring-vlan-information>
show ptp
show ptp clock
   get-ptp-clock>
show ptp global-information
   get-ptp-global-information>
show ptp hybrid
```

```
show ptp hybrid config
<get-ptp-hybrid-mapping>
show ptp hybrid status
<get-ptp-hybrid-status>
show ptp last-tod-update
<get-last-tod-update>
show ptp lock-status
   get-ptp-lock-status>
show ptp master
<get-ptp-master>
show ptp path-trace
<get-ptp-path-trace>
show ptp port
   <get-ptp-port>
show ptp quality-level-mapping
<get-ptp-quality-level-mapping>
show ptp slave
   <get-ptp-slave>
show ptp stateful
<get-ptp-stateful>
show ptp statistics
   <get-ptp-statistics>
show r2cp
show r2cp interfaces
    <get-r2cp-interface-information>
show r2cp radio
    <get-r2cp-radio-information>
show r2cp sessions
    <get-r2cp-session-information>
show r2cp statistics
    <get-r2cp-statistics>
show redundant-power-system
show redundant-power-system led
show redundant-power-system multi-backup
<get-rps-scale-information>
show redundant-power-system network
<get-rps-network-information>
show redundant-power-system power-supply
show redundant-power-system status
show redundant-power-system upgrade
<get-rps-upgrade-information>
show redundant-power-system version
show rip
```

```
show rip general-statistics
    <get-rip-general-statistics-information>

show rip neighbor
    <get-rip-neighbor-information>

show rip statistics
    <get-rip-statistics-information>
show rip statistics peer
<get-rip-peer-information>
show ripng
show ripng general-statistics
   <get-ripng-general-statistics-information>

show ripng neighbor
   <get-ripng-neighbor-information>
show ripng statistics
   <get-ripng-statistics-information>
show route
    <get-route-information>

show route cumulative
    <get-route-cumulative>

show route export
    <get-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 route-session-id
<get-rsvp-route-session-id-information>

show rsvp session
    <get-rsvp-session-information>

show rsvp statistics
    <get-rsvp-statistics-information>

show rsvp version
    <get-rsvp-version-information>

show sap
show sap listen
    <get-sap-listen-information>
```

```
show security group-vpn member kek
show security group-vpn member kek security-associations
<get-gvpn-kek-security-associations-information>

show services
show services accounting
    <get-service-accounting-information>

show services accounting aggregation
    <get-service-accounting-aggregation-information>

show services accounting aggregation as
    <get-service-accounting-aggregation-as-information>

show services accounting aggregation destination-prefix
    <get-service-accounting-aggregation-destination-prefix-information>

show services accounting aggregation protocol-port
    <get-service-accounting-aggregation-protocol-port-information>

show services accounting aggregation source-destination-prefix
    <get-service-accounting-aggregation-source-destination-prefix-information>

show services accounting aggregation source-prefix
    <get-service-accounting-aggregation-source-prefix-information>

show services accounting aggregation template
    <get-service-accounting-aggregation-template-information>

show services accounting errors
    <get-service-accounting-errors-information>

show services accounting flow
    <get-service-accounting-flow-information>

show services accounting flow-detail
    <get-service-accounting-flow-detail>

show services accounting memory
    <get-service-accounting-memory-information>

show services accounting packet-size-distribution
    <get-packet-distribution-information>
```

```
show services accounting status
    <get-service-accounting-status-information>

show services accounting usage
    <get-service-accounting-usage-information>

show services alg
show services alg conversations
    <get-service-msp-alg-conversation-information>
show services alg sip-globals
<get-service-msp-alg-sip-globals-information>
show services alg statistics
show services application-aware-access-list
show services application-aware-access-list flows
show services application-aware-access-list flows interface
   <get-application-aware-access-list-flows-interface>
show services application-aware-access-list flows subscriber
   <get-application-aware-access-list-flows-subscriber>
show services application-aware-access-list statistics
show services application-aware-access-list statistics interface
   <get-application-aware-access-list-statistics-interface>
show services application-aware-access-list statistics subscriber
   <get-application-aware-access-list-statistics-subscriber>
show services application-identification
show services application-identification application
show services application-identification application detail
   <get-appid-application-signature-detail>
show services application-identification application summary
   <get-appid-application-signature-summary>
show services application-identification application-system-cache
    <get-appid-application-system-cache>

show services application-identification counter
    <get-appid-counter>
show services application-identification counter ssl-encrypted-sessions
<get-appid-counter-encrypted>
show services application-identification group
show services application-identification group detail

   <get-appid-application-group-detail>
show services application-identification group summary
   <get-appid-application-group-summary>
```

```
show services application-identification statistics
show services application-identification statistics application-groups
   <get-appid-application-group-statistics>
show services application-identification statistics applications
   <get-appid-application-statistics>
show services application-identification status
<get-appid-staus-information>
show services application-identification version
     <get-appid-package-version>

show services border-signaling-gateway
show services border-signaling-gateway accounting
show services border-signaling-gateway accounting statistics
    <get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway accounting status
    <get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway admission-control
    <get-service-border-signaling-gateway-statistics-admission-control>

show services border-signaling-gateway by-call-context-id
    <get-service-bsg-information-by-call-context-id>

show services border-signaling-gateway by-contact
    <get-service-border-signaling-gateway-information-by-contact>

show services border-signaling-gateway by-request-uri
    <get-service-border-signaling-gateway-information-by-request-uri>

show services border-signaling-gateway calls
    <get-service-border-signaling-gateway-statistics-calls>

show services border-signaling-gateway calls-duration
    <get-service-border-signaling-gateway-calls-duration>

show services border-signaling-gateway calls-failed


how services border-signaling-gateway charging
show services border-signaling-gateway charging statistics
    <get-service-border-signaling-gateway-charging-statistics>
show services border-signaling-gateway charging status
    <get-service-border-signaling-gateway-charging-status>
show services border-signaling-gateway denied-messages
```

```
    <get-service-bsg-denied-messages>

show services border-signaling-gateway embedded-spdf
    <get-service-border-signaling-gateway-embedded-spdf>

show services border-signaling-gateway embedded-spdf status
    <get-service-border-signaling-gateway-embedded-spdf-status>

show services border-signaling-gateway name-resolution-cache

show services border-signaling-gateway name-resolution-cache all
    <get-service-border-signaling-gateway-name-resolution-cache-all>

show services border-signaling-gateway name-resolution-cache by-fqdn
<get-border-signaling-gateway-name-resolution-cache-by-fqdn>
show services border-signaling-gateway status
    <get-service-bsg-status-information>
show services captive-portal-content-delivery
show services captive-portal-content-delivery pic
   <get-cpcd-pic-information>
show services captive-portal-content-delivery profile
   <get-cpcd-profile>
show services captive-portal-content-delivery rule
   <get-cpcd-rule>
show services captive-portal-content-delivery ruleset
   <get-cpcd-rule-set>
show services captive-portal-content-delivery sset
   <get-cpcd-service-set>
show services captive-portal-content-delivery statistics
   <get-cpcd-pic-statistics>
show services captive-portal-content-delivery statistics interface
show services capture
<get-service-capture>
show services cos
show services cos statistics
    <get-service-cos-statistics-information>

show services cos statistics diffserv
    <get-service-cos-diffserv-statistics>

show services cos statistics forwarding-class
    <get-service-cos-forwarding-class-statistics>
```

```
show services crtp
    <get-service-crtp-params-information>

show services crtp extensive
    <get-service-crtp-extensive-information>

show services crtp flows
    <get-service-crtp-flow-table-information>

show services dynamic-flow-capture
show services dynamic-flow-capture content-destination
    <get-services-dynamic-flow-capture-content-destination-information>

show services dynamic-flow-capture control-source
    <get-services-dynamic-flow-capture-control-source-information>

show services dynamic-flow-capture statistics
   <get-services-dfc-statistics-information>
show extension-service
show extension-service status
<jet-application-status>
show services fips
show system commit synchronize-server pending-jobs
<get-pending-commit-sync-jobs>
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 ha
<get-service-ha-info>
show services hcm
show services hcm pic-statistics
  <get-service-hcm-pic-statistics-information>
show services ids
show services ids destination-table
    <get-service-ids-destination-table-information>

show services ids pair-table
    <get-service-ids-pair-table-information>

show services ids source-table
    <get-service-ids-source-table-information>

show services inline
show services inline ip-reassembly
show services inline ip-reassembly statistics
show services inline nat
show services inline nat mappings
show services inline nat mappings nptv6
<get-inline-nat-mapping-nptv6-information>
show services inline nat pool
   <get-inline-nat-pool-information>
show services inline nat statistics
   <get-inline-nat-statistics-information>
show services inline softwire
show services inline softwire statistics
<get-inline-service-sw-statistics-information>
show services inline stateful-firewall
show services inline stateful-firewall flows
<get-inline-sfw-flow-table-information>
show services inline stateful-firewall statistics
<get-inline-sfw-statistics-information>
show services ipsec-vpn
show services ipsec-vpn ike
show services ipsec-vpn ike security-associations
    <get-ike-services-security-associations-information>

show services ipsec-vpn ike statistics
```

```
<get-ike-services-statistics>
show services ipsec-vpn ipsec
show services ipsec-vpn ipsec security-associations
    <get-services-security-associations-information>

show services ipsec-vpn ipsec statistics
    <get-services-ipsec-statistics-information>

show services l2tp
show services l2tp client
<get-l2tp-client-information>
show services l2tp destination
    <get-l2tp-destination-information>
show services l2tp destination lockout
<get-services-l2tp-destination-lockout>
show services l2tp disconnect-cause-summary<
<get-l2tp-disconnect-cause-summary>
show services l2tp multilink
    <get-l2tp-multilink-information>

show services l2tp radius
show services l2tp radius accounting
show services l2tp radius accounting servers
    <get-services-l2tp-radius-accounting-servers-information>

show services l2tp radius accounting statistics
    <get-services-l2tp-radius-accounting-statistics-information>

show services l2tp radius authentication
show services l2tp radius authentication servers
    <get-services-l2tp-radius-authentication-servers-information>

show services l2tp radius authentication statistics
    <get-services-l2tp-radius-authentication-statistics-information>

show services l2tp radius servers
    <get-services-l2tp-radius-authentication-accounting-servers-information>

show services l2tp radius statistics
    <get-services-l2tp-radius-authentication-accounting-statistics-information>

show services l2tp session
    <get-l2tp-session-information>
```

```
show services l2tp session-limit-group
<get-l2tp-session-limit-group-information>

show services l2tp summary
    <get-l2tp-summary-information>

show services l2tp tunnel
    <get-l2tp-tunnel-information>
show services l2tp tunnel-group
<get-l2tp-tunnel-group-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 match-policies
<get-services-match-policies>
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 redundancy-group
<get-services-redundancy-group-information>
show services redundancy-group rg-id
<get-services-redundancy-group-id-information>

show services rpm
show services rpm active-servers
    <get-active-servers>

show services rpm history-results
    <get-history-results>

show services rpm probe-results
    <get-probe-results>

show services rpm twamp
   <twamp-information>
show services rpm twamp client
<twamp-client-information>
show services rpm twamp client connection
```

```
<twamp-client-connection-information>
show services rpm twamp client history-results
<twamp-get-history-results>
show services rpm twamp client probe-results
<twamp-get-probe-results>
show services rpm twamp client session
<twamp-client-test-session>
show services rpm twamp server
   <twamp-server-information>
show services rpm twamp server connection
   <twamp-server-connection-information>
show services rpm twamp server session
   <twamp-server-session-information>
show services server-load-balance
show services server-load-balance external-manager
show services server-load-balance external-manager information
show services server-load-balance external-manager statistics
   <get-external-manager-statistics-information>
show services server-load-balance hash-table
   <get-hash-table-information>
show services server-load-balance health-monitor
show services server-load-balance health-monitor information
   <get-real-server-health-monitor-information>
show services server-load-balance health-monitor statistics
   <get-real-server-health-monitor-statistics-information>
show services server-load-balance real-server
show services server-load-balance real-server statistics
   <get-real-server-statistics-information>
show services server-load-balance real-server-group
show services server-load-balance real-server-group information
   <get-real-server-group-information>
show services server-load-balance real-server-group statistics
   <get-real-server-group-statistics-information>
show services server-load-balance sticky
   <get-sticky-table-information>
show services server-load-balance virtual-server
show services server-load-balance virtual-server information
   <get-virtual-server-information>
show services server-load-balance virtual-server statistics
   <get-virtual-server-statistics-information>
show services service-identification
show services service-identification header-redirect
show services service-identification header-redirect statistics
```

```
    <get-header-redirect-set-statistics-information>

show services service-identification statistics
    <get-service-identification-statistics-information>

show services service-identification uri-redirect
show services service-identification uri-redirect statistics
    <get-uri-redirect-set-statistics-information>

show services service-sets
show services service-sets cpu-usage
    <get-service-set-cpu-statistics>

show services service-sets memory-usage
    <get-service-set-memory-statistics>

show services service-sets memory-usage zone
show services service-sets plug-ins
    <get-service-set-plugin-summary>

show services service-sets statistics
show services service-sets statistics drop-flow-limit
<get-service-set-drop-flow-statistics>
show services service-sets statistics ids
show services service-sets statistics ids drops
<get-service-set-ids-drops-statistics>
show services service-sets statistics jflow-log
<get-service-set-jflow-log-statistics>
show services service-sets statistics packet-drops
    <get-service-set-packet-drop-statistics>

show services service-sets statistics syslog
    <get-service-set-syslog-statistics>
show services service-sets statistics tcp
<get-service-set-tcp-tracker-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 sessions analysis
<show-service-msp-session-analysis-information>
show services sessions count
<get-service-msp-sess-count-information>
show services sessions utilization
<get-services-sessions-utilization>

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 traffic-detection-function
show services traffic-detection-function hcm
show services traffic-detection-function hcm statistics
<get-service-tdf-hcm-sessions-stats>
show services traffic-detection-function sessions
<get-service-tdf-sessions-information>
show services traffic-load-balance
show services traffic-load-balance statistics
<get-traffic-load-balance-statistics>
show services unified-access-control
show services unified-access-control authentication-table
<get-uac-auth-table>
show services unified-access-control counters
<get-uac-counters>
show services unified-access-control policies
<get-uac-policies>
show services unified-access-control roles
<get-uac-role-entries>
show services unified-access-control status
<get-uac-status>
show services video-monitoring
<get-service-video-monitoring-information>
show services video-monitoring mdi
<get-service-video-monitoring-mdi-information
show services video-monitoring mdi alarms
<get-services-video-monitoring-mdi-alarms-information>
show services video-monitoring mdi alarms errors
```

```
<get-services-video-monitoring-mdi-alarms-errors-information>
show services video-monitoring mdi alarms stats
<get-services-video-monitoring-mdi-alarms-stats-information>
show services video-monitoring mdi errors>
<get-service-video-monitoring-mdi-errors-information>
show services video-monitoring mdi flow
<get-service-video-monitoring-mdi-flows-information>
show services video-monitoring mdi stats
<get-service-video-monitoring-mdi-stats-information>
show shmlog
show shmlog argument-mappings
<get-shmlog-argument-mappings>
show shmlog configuration
<show-shmlog-configuration>
show shmlog entries
<show-shmlog-entries>
show shmlog logs-summary
<show-shmlog-logsummary>
show shmlog statistics
<show-shmlog-statistics>
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 health-monitor routing-engine
show snmp health-monitor routing-engine history
<get-health-monitor-routing-engine-history>
show snmp health-monitor routing-engine history cpu
<get-routing-engine-cpu-history>
show snmp health-monitor routing-engine history memory
<get-routing-engine-memory-history>
show snmp health-monitor routing-engine history open-files-count
<get-routing-engine-fd-history>
show snmp health-monitor routing-engine history process-count
<get-routing-engine-pcount-history>
show snmp health-monitor routing-engine history storage
<get-routing-engine-storage-history>
show snmp health-monitor routing-engine history temperature
```

```
<get-routing-engine-temperature-history>
show snmp health-monitor routing-engine status
<get-health-monitor-routing-engine-information>
show snmp health-monitor routing-engine status detail

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 spanning-tree stp-buffer see-all
```

```
show ssl-certificates
<get-ssl-certificate-information>
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 ephemeral
<get-ephemeral-commit-information>
show system commit server queue
<get-commit-server-queue-information>
show system commit synchronize-server
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 satellite
<get-core-file-satellite>
show system core-dumps transfer-status
show system diagnostics
show system diagnostics inventory
show system diagnostics usage
show system directory-usage
    <get-directory-usage-information>

show system firmware
    <get-system-firmware-information>
show system khms-stats


show system license
    <get-license-summary-information>

show system license installed
    <get-license-information>
show system license key-content
show system license keys
    <get-license-key-information>

show system license usage
    <get-license-usage-summary>
show system login
show system login lockout
   <get-system-login-lockout-information>
show system memory
<show system processes
show system processes brief
show system processes esc-node
show system processes extensive
show system processes health
    <get-process-health-information>

show system processes providers
show system processes host-processes detail
```

```
show system processes 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>
<get-resource-monitor-fpc-information>
<get-resource-monitor-fpc-slot-information>

show system rollback
    <get-rollback-information>

show system services
show system services dhcp
show system services dhcp binding
    <get-dhcp-binding-information>

show system services dhcp conflict
    <get-dhcp-conflict-information>

show system services dhcp global
    <get-dhcp-global-information>

show system services dhcp pool
    <get-dhcp-pool-information>

show system services dhcp statistics
    <get-dhcp-statistics-information>

show system services reverse
    <get-system-services-reverse-information>

show system services service-deployment
    <get-service-deployment-service-information>

show system snapshot
    <get-snapshot-information>

show system software
show system software backup
```

```
<get-package-backup-information>
<get-software-installation-status>
show system software recovery-package
show system software rollback
<show-package-rollback>

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 storage satellite
<get-system-storage-satellite>
show system subscriber-management
show system subscriber-management arp
<get-subscriber-management-arp>
show system subscriber-management arp address
<get-subscriber-management-arp-address>
show system subscriber-management arp interface
<get-subscriber-management-arp-interface>
show system subscriber-management ipv6-neighbors
<get-subscriber-management-ipv6-neighbors>
show system subscriber-management ipv6-neighbors address
<get-subscriber-management-ipv6-neighbor-address>
show system subscriber-management ipv6-neighbors interface
<get-subscriber-management-ipv6-neighbor-interface>.
show system subscriber-management route
<get-subscriber-management-route>
show system subscriber-management route next-hop
<get-subscriber-management-route-nh>
show system subscriber-management route prefix
show system subscriber-management route summary
<get-subscriber-management-route-summary>
show system subscriber-management statistics
<get-subscriber-management-statistics>
show system subscriber-management summary
show system switchover
```

```
    <get-switchover-information>

show system uptime
    <get-system-uptime-information>

show system users
    <get-system-users-information>

show system virtual-memory
show system yang
show system yang package
<get-system-yang-packages>
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
<get-mobile-serving-gateway-interface-service-mode>
show unified-edge tdf
show unified-edge tdf aaa
show unified-edge tdf aaa radius
show unified-edge tdf aaa radius client
show unified-edge tdf aaa radius client statistics
<radius-client-statistics>
show unified-edge tdf aaa radius client status
show unified-edge tdf aaa radius network-element
show unified-edge tdf aaa radius network-element statistics
<get-aaa-radius-element-statistics>
show unified-edge tdf aaa radius network-element status>
<get-aaa-radius-element-status>
show unified-edge tdf aaa radius server
show unified-edge tdf aaa radius server statistics
radius-server-statistics
show unified-edge tdf aaa radius server status
<get-aaa-radius-server-status>
show unified-edge tdf aaa radius snoop-segment
show unified-edge tdf aaa radius snoop-segment statistics
<radius-snoop-segment-statistics>
show unified-edge tdf aaa statistics
<get-tdf-gateway-aaa-statistics>
show unified-edge tdf address-assignment
show unified-edge tdf address-assignment pool
<get-tdf-gateway-sm-ippool-pool-information>
show unified-edge tdf address-assignment service-mode
<get-tdf-address-assign-service-mode>
show unified-edge tdf address-assignment statistics
<get-tdf-gateway-sm-ippool-statistics>
show unified-edge tdf call-admission-control
show unified-edge tdf call-admission-control statistics
<get-tdf-cac-statistics>
show unified-edge tdf call-rate
show unified-edge tdf call-rate statistics
<get-tdf-call-rate-statistics>
show unified-edge tdf diameter
show unified-edge tdf diameter network-element
show unified-edge tdf diameter network-element statistics
<get-diameter-network-element-statistics>
```

```
show unified-edge tdf diameter network-element status
<get-diamieter-network-element-status>
show unified-edge tdf diameter pcc-gx
show unified-edge tdf diameter pcc-gx statistics
<get-diameter-statistics-gx>
show unified-edge tdf diameter peer
show unified-edge tdf diameter peer statistics
<get-gateway-diameter-peer-statistics>
show unified-edge tdf diameter peer status
<get-diameter-peer-status>
show unified-edge tdf domain
show unified-edge tdf domain service-mode
<get-mobile-gateways-domain-service-mode>
show unified-edge tdf domain statistics
<get-mobile-gateways-domain-statistics>
show unified-edge tdf resource-manager
show unified-edge tdf resource-manager clients
<get-mobile-gateway-tdf-client-status-information>
show unified-edge tdf service-mode
<get-tdf-gateway-service-mode>
show unified-edge tdf statistics
<get-tdf-statistics>
show unified-edge tdf status
<get-tdf-gateway-status>
show unified-edge tdf status subscriber-state
<get-tdf-gateways-status-state>
show unified-edge tdf subscribers
<get-tdf-gateway-subscribers>
show unified-edge tdf subscribers data-plane
<get-tdf-gateway-subscriber-dataplane-statistics>
show unified-edge tdf subscribers stuck
<get-tdf-gateway-stuck-subscribers>
show unified-edge tdf system
show unified-edge tdf system interfaces
<get-tdf-interfaces-information>
show unified-edge tdf system interfaces service-mode
<get-mobile-tdf-interface-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 vlans satellite
<get-satellite-control-bridge-domain>
show vmhost
show vmhost bridge
<get-vmhost-bridge-information>
```

```
show vmhost crash
<get-vmhost-crash-information>
show vmhost hardware
<get-vmhost-hardware>
show vmhost information
<get-vmhost-information>
show vmhost logs
<get-vmhost-logs-information>
show vmhost management-if
<get-vmhost-management-if-info>
show vmhost netstat
<get-vmhost-netstat>
show vmhost processes
<get-vmhost-processes-information>
show vmhost resource-usage
<get-vmhost-resource-usage-information>
show vmhost snapshot
<get-vmhost-snapshot-information>
show vmhost status
<get-vmhost-staus>
show vmhost uptime
<get-vmhost-uptime>
show vmhost version
<get-vmhost-version-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 Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

view-configuration

Can view all of the configuration (not including secrets).

Commands

```
No associated CLI commands.
```

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Access Privilege Levels Overview | 53
- Example: Configure User Permissions with Access Privilege Levels | 59
- Example: Configure User Permissions with Access Privileges for Operational Mode Commands | 91
- Example: Configure User Permissions with Access Privileges for Configuration Statements and Hierarchies | 103

13

CHAPTER

Configuration Statements and Operational Commands

IN THIS CHAPTER

show snmp

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- `show snmp health-monitor`, which displays the health monitor log and alarm information.
- `show snmp mib`, which displays information from the MIBs, such as device and system information.
- `show snmp statistics`, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- `show snmp rmon`, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the `show snmp health-monitor` command:

```
user@switch> show snmp health-monitor
Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                       58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                        0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                          0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                      35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                      0 active
       Chassis daemon                                  50 active
       Firewall daemon                                  0 active
       Interface daemon                                 5 active
       SNMP daemon                                     11 active
       MIB2 daemon                                     42 active
       ...
```

The following example provides sample output from the `show snmp mib` command:

```
user@switch> show snmp mib walk system

sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx
Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the `show snmp statistics` command:

```
user@switch> show snmp statistics

SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
    Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

RELATED DOCUMENTATION

- show snmp mib

show snmp statistics

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Read this guide to learn about the syntax and options that make up the statements and commands. Also understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands