Chapter 9

Passwords and Security

Passwords and security are of utmost importance for the security of your router. This chapter provides the information you need to configure your E-series router to be secure for all levels of users.

This chapter contains the following sections:

Overview

One of your major management responsibilities is to secure your router. To do this, assign passwords or secrets to the router. In Global Configuration mode, you can set passwords or secrets to prevent unauthorized users from accessing the router in Privileged Exec mode.

Passwords and secrets have the same degree of security on your router, and they are used interchangeably. You can define either a password or a secret for your router, but not both.

Platform Considerations

Passwords and security are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Setting Basic Password Parameters

This section shows how to set up basic passwords and secrets on your router. You cannot create your own encrypted passwords and secrets. You must use encrypted passwords and secrets that the router generates.

NOTE: See *Setting and Erasing Passwords* on page 445 for additional commands for erasing and monitoring passwords.

Creating Encrypted Passwords

This example encrypts password *t1meout1* and creates a password for privilege level 10.

1. Enable and configure the password. The **0** keyword specifies that you are entering an unencrypted password.

   host1(config)#**enable password level 10 0 t1meout1**

2. Display the encrypted password.

```
host1(config)#exit
host1#show secret
               Current Password Settings
               -------------------------
         encryption          encrypted
level       type          password/secret         mode
-----   ------------   --------------------   ----------
0
1
2
3
4
5
6
7
8
9
10      7 (password)   dq]XG`,%N"SS7d}o)_?Y   configured
11      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
12      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
```

```
13      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
14      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
15      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
```

You or users with high privilege levels can now use the encrypted password, *dq]XG`,%N"SS7d}o)_?Y*, with the **password** command.

Creating Secrets

This example generates a secret for the password *rocket*, and creates a secret for privilege level 15.

1. Enable and configure the secret. The **0** keyword specifies that you are entering an unencrypted secret.

   host1(config)#**enable secret level 15 0 rocket**

2. Display the secret.

```
host1(config)#exit
host1#show secret
              Current Password Settings
              -------------------------
        encryption        encrypted
level      type        password/secret         mode
-----   ----------   --------------------   ----------
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15      5 (secret)   bcA";+1aeJD8)/[1ZDP6   configured
```

You or users with high privilege levels can now use the encrypted password, *bcA";+1aeJD8)/[1ZDP6*, with the **password** command.

Encrypting Passwords in Configuration File

You can also direct the system software to encrypt passwords saved in the configuration file by using the **service password-encryption** command. This command is useful to keep unauthorized individuals from viewing your password in your configuration file. It is important to remember that this command uses a simple cipher and is not intended to protect against serious analysis. You can tell if a string is encrypted if it is preceded by an 8.

Commands and Guidelines

Use the following commands and guidelines to set passwords or secrets for the privilege levels.

enable password

- Use to set a password, which controls access to Privileged Exec mode and some configuration modes.
- Enter the password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- The first time you define a password, you must enter it in plain text. To view its encrypted form, use the **show config** display. To redefine the password at a later date, you can enter the password in its encrypted form.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted password
  - **7**—Specifies an encrypted password
- Example 1 (unencrypted password)

  host1(config)#**enable password 0 mypassword**

- Example 2 (encrypted password)

  host1(config)#**enable password 7 x13_2**

- Use the **no** version to remove the password.

enable secret

- Use to set a secret, which controls access to the Privileged Exec mode and some configuration modes.
- Enter the secret in plain text (its unencrypted form) or cipher text (its encrypted form). In either case, the system stores the secret as encrypted.
- The first time you define a secret, you must enter it in plain text. To view its encrypted form, use the **show config** display. To redefine the secret at a later date, you can enter the secret in its encrypted form.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted secret
  - **5**—Specifies an encrypted secret
- Example 1 (unencrypted secret)

  host1(config)#**enable secret 0 yalta45**

- Example 2 (encrypted secret)

  host1(config)#**enable secret 5 y13_x**

- Use the **no** version to remove the secret.

service password-encryption

- Use to encrypt passwords that are saved in the system's configuration file. The command converts plain text to cipher text. The default is no encryption.
- Use of this command prevents casual observers from viewing passwords, for example, in data obtained from **show config** displays. The command is not intended to provide protection from serious analysis.
- This command does *not* apply to passwords set with **enable secret**, **enable password**, or **password** (Line Configuration mode).
- This command does apply to authentication key passwords and BGP neighbor passwords.
- Example

  host1(config)#**service password-encryption**

- Use the **no** version to remove the encryption assignment.

Setting and Erasing Passwords

You can set the following passwords:

- Enable passwords that control access to different groups of commands.
- A console password that controls access to the console.
- Passwords for individual vty lines or groups of vty lines.

Privilege Levels

Different groups of commands are associated with privilege levels (Table 51). You can set enable passwords to allow users to access commands at different privilege levels.

Table 51: Commands Available at Different Privilege Levels

Privilege Level	Commands Available
0	**help**, **exit**, **enable**, and **disable** commands
1	User Exec commands plus commands at level 0
5	Privileged Exec **show** commands plus commands at levels 0 and 1
10	All commands except support commands
15	Support commands that Juniper Networks Technical Support may provide and all other commands

To maximize security and usability, set different passwords for levels 1, 5, 10, and 15. By default, no **enable** passwords exist.

Accessing Privilege Levels

If users have access to the console, they automatically have access to privilege level 0. To access higher levels of privilege, they must enter the **enable** *privilege-level* command. When users specify a privilege level, the system determines whether there is a password at that level. If there is not, the system prompts the user for the password for the lower level closest to the requested level.

Setting Enable Passwords

To set up enable passwords, use the commands described in *Setting Basic Password Parameters* on page 442.

Erasing Enable Passwords

If you forget an e**nable** password or secret, you can erase all **enable** passwords and secrets.

Two commands allow you to erase passwords and secrets: **erase secrets** and **service unattended-password-recovery.** It is important to fully understand the purpose of these commands and how they work with each other.

The **erase secrets** command can be used to delete all existing passwords. To use this command, you must be physically present at the router to complete the operation. After the command has been executed, you have a finite number of seconds to press the software reset button on the SRP module. You can execute this command from the console or any vty.

The **service unattended-password-recovery** command provides you with a way to delete existing passwords and secrets without physically being present at the router. You must have the proper privilege level to execute the command, and you can execute it from either the console or any vty.

When you execute **service unattended-password-recovery**, you change the behavior of **erase secrets**. You can now delete passwords and secrets from the console by executing **erase secrets** without a time restraint or having to be physically present at the router. When you use the **no** version of **service unattended-password-recovery**, you revert the functionality of erase secrets to the factory default setting.

To erase all enable passwords or secrets:

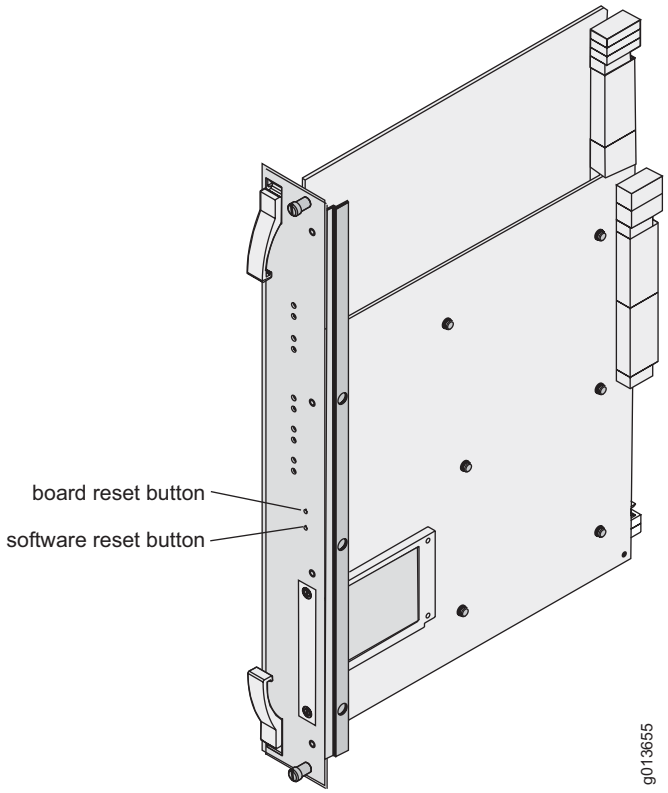
1. Log in to the router.

2. Erase the existing enable password or secret. Specify the number of seconds to allow for the erase operation.

   host1>**erase secrets 60**

3. Within the time limit that you specified for the **erase secrets** command, press the recessed software reset button on the primary SRP module (see Figure 28 on page 447).

Figure 28: Location of the Software Reset Button



NOTE: If you do not press the software reset button within the time limit, the system will not erase the password, and you will need to repeat the process.

erase secrets

- Use to delete all CLI passwords and secrets.
- After you issue this command, press the software reset button (see Figure 28) within the time you specify for this command.
- Allows you to set the number of seconds (1–60) for this procedure to be accomplished.
- Allows you to set a new password when you have forgotten your password.
- Can be used with the **service unattended-password-recovery** command.
- Example

  host1>**erase secrets 60**

- There is no **no** version.

service unattended-password-recovery

- Use to allow you to delete all passwords and secrets from the console without being physically present at the router.
- When executed, this command changes the behavior of the **erase secrets** command, which will not take any parameters and will not be available through a vty session.
- Example

  host1(config)#**service unattended-password-recovery**

- Use the **no** version to revert **erase secrets** to factory default settings.

Setting a Console Password

By default, there is no console password. To set a console password:

1. Make sure that you know the enable password for the system.

   If you need to reset the enable password, see *Privilege Levels* on page 445.

2. Access Privileged Exec mode, and enter the enable password if prompted.
3. Access Global Configuration mode.
4. Access Line Configuration mode.

   host1(config)#**line console 0**

5. Enable password checking at login.

   host1(config-line)#**login**

6. Specify a password.

   host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

line

- Use to specify the vty lines or the console.
- Example

  host1(config)#**line vty 1 4**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login

- Use to enable password checking at login.
- The default setting is to enable a password.
- Example

  host1(config)#**line vty 1 4**
  host1(config-line)#**login**

- Use the **no** version to disable password checking and allow access without a password.

password

- Use to specify a password on the console, a line, or a range of lines.
- If you enable password checking, but do not configure a password, the system will not allow you to access virtual terminals.
- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 bcA";+1aeJD8)/[1ZDP6**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

- Use the **no** version to remove the password. By default, no password is specified.

Erasing the Console Password

If you forget the console password, you can erase the existing value and configure a new one. This action deletes all authentication for the console line. To erase existing passwords:

1. Reboot the router by pressing the recessed software reset button on the primary SRP module (see Figure 28 on page 447) and then pressing the mb key sequence during the countdown.

2. Disable authentication at the console level.

   :boot##**disable console authentication**

   If you remember the password at this point, you can override this action by entering:

   :boot##**no disable console authentication**

3. Reload the operating system.

   :boot##**reload**

When the operating system reloads, you can access the console without a password.

NOTE: You will be able to log in to the console without a password until you set a new password.

Monitoring Passwords

You can use the **show secrets** command to view all current passwords and secrets.

show secrets

- Use to display all passwords and secrets.
- Passwords and secrets appear in their encrypted form.
- In the mode column, *inherited* indicates whether a secret was inherited from a lower password level. The **show secrets** command displays only secrets configured by the user; it does not display inherited secrets.
- Example

```
host1#show secrets
                Current Password Settings
                -------------------------
         encryption          encrypted
level       type          password/secret          mode
-----   ------------   --------------------   ----------
0
1
2
3
4
5       7 (password)   zRFj_6>^]1OkZR@e!|S$   configured
6       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
7       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
```

```
8       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
9       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
10      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
11      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
12      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
13      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
14      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
```

Vty Line Authentication and Authorization

The router supports 30 virtual tty (vty) lines for Telnet, Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty line. You can add security to your router by configuring the software to validate login requests. There are two modes of authentication for a vty line:

- Simple authentication—Password-only authentication through the local configuration
- AAA authentication—Username and password authentication through a set of authentication servers

You can enable AAA authorization, which allows you to limit the services available to a user. Based on information retrieved from a user's profile, the user is either granted or denied access to the requested server.

Configuring Simple Authentication

To configure simple authentication:

1. Specify a vty line or a range of vty lines on which you want to enable the password.

   host1(config)#**line vty 8 13**
   host1(config-line)#

2. Specify the password for the vty lines.

   host1(config-line)#**password 0 mypassword**

3. Enable login authentication on the lines.

   host1(config-line)#**login**

4. Display your vty line configuration.

   host1#**show line vty 8**
   no access-class in
   data-character-bits 8
   exec-timeout never
   exec-banner enabled
   motd-banner enabled
   login-timeout 30 seconds

line

- Use to specify the vty line(s) on which you want to enable the password.
- You can set a single line or a range of lines. The range is 0–29.
- Example

  host1(config)#**line vty 8 13**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login

- Use to enable password checking at login.
- The default setting is to enable a password.
- Example

  host1(config-line)#**login**

- Use the **no** version to disable password checking and allow access without a password.

password

- Use to specify a password on a single line or a range of lines.
- If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals.
- Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 bcA";+1aeJD8)/[1ZDP6**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

- Use the **no** version to remove the password. By default, no password is specified.

show line vty

- Use to display the configuration of a vty line.
- Field descriptions
  - access-class—Access-class associated with the vty line
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the message of the day (MOTD) banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show line vty 0
no access-class in
data-character-bits 8
exec-timeout 3w 3d 7h 20m 0s
exec-banner enabled
motd-banner enabled
login-timeout 30 seconds
```

Configuring AAA Authentication and AAA Authorization

Before you configure AAA authentication and AAA authorization, you need to configure a RADIUS and/or TACACS+ authentication server. Note that several of the steps in the configuration procedure are optional.

To configure AAA new model authentication and authorization for inbound sessions to vty lines on your router:

1. Specify AAA new model authentication.

   host1(config)#**aaa new-model**

2. Create an authentication list that specifies the type(s) of authentication methods allowed.

   host1(config)#**aaa authentication login my_auth_list tacacs+ line enable**

3. (Optional) Specify the privilege level by defining a method list for authentication.

   host1(config)**aaa authentication enable default tacacs+ radius enable**

4. (Optional) Enable authorization, and create an authorization method list.

   host1(config)**aaa authorization commands 15 boston if-authenticated tacacs+**

5. (Optional) Disable authorization for all Global Configuration commands.

   host1(config)#**no aaa authorization config-commands**

6. Specify the range of vty lines.

   host1(config)#**line vty 6 10**
   host1(config-line)#

7. (Optional) Apply an authorization list to a vty line or a range of vty lines.

   host1(config-line)#**authorization commands 15 boston**

8. Specify the password for the vty lines.

   host1(config-line)#**password xyz**

9. Apply the authentication list to the vty lines you specified on your router.

   host1(config-line)#**login authentication my_auth_list**

aaa authentication enable default

- Use to allow privilege determination to be authenticated through the TACACS+ or RADIUS server. This command specifies a list of authentication methods that are used to determine whether a user is granted access to the privilege command level.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.
- Requests sent to a TACACS+ or RADIUS server include the username that is entered for login authentication.
- If the authentication method list is empty, the local **enable** password is used.
- Example

  host1(config)#**aaa authentication enable default tacacs+ radius**

- Use the **no** version to empty the list.

aaa authentication login

- Use to set AAA authentication at login. This command creates a list that specifies the methods of authentication.
- After you have specified **aaa new-model** as the authentication method for vty lines, an authentication list called "default" is automatically assigned to the vty lines. To allow users to access the vty lines, you must create an authentication list and either:
  - Name the list "default."
  - Assign a different name to the authentication list, and assign the new list to the vty line using the **login authentication** command.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- The system traverses the list of authentication methods to determine whether a user is allowed to start a Telnet session. If a specific method is available but the user information is not valid (such as an incorrect password), the system does not continue to traverse the list and denies the user a session.
- If a specific method is unavailable, the system continues to traverse the list. For example, if **tacacs+** is the first authentication type element on the list and the TACACS+ server is unreachable, the system attempts to authenticate with the next authentication type on the list, such as **radius**.
- The system assumes an implicit denial of service if it reaches the end of the authentication list without finding an available method.
- Example

  host1(config)#**aaa authentication login my_auth_list tacacs+ radius line none**

- Use the **no** version to remove the authentication list from your configuration.

aaa authorization

- Use to set the parameters that restrict access to a network.
- Use the keyword **exec** to determine if the user is allowed to run Exec mode commands. The commands that you can execute from Exec mode provide only user-level access.
- Use the keyword **commands** to run authorization for all commands at the specified privilege level (0–15). See Table 51 on page 445 for a description of privilege levels.
- You can enter up to three authorization types to use in an authorization method list. Options include: **if-authenticated, none**, and **tacacs+**.

NOTE: For information about TACACS+, see *JUNOSe Broadband Access Configuration Guide, Chapter 9, Configuring TACACS+*.

- Authorization method lists define the way authorization is performed and the sequence in which the methods are performed. You can designate one or more security protocols in the method list to be used for authorization. If the initial method fails, the next method in the list is used. The process continues until either there is successful communication with a listed authorization method or all methods defined are exhausted.
- Example

  host1(config)#**aaa authorization exec**

- Use the **no** version to delete the method list.

aaa authorization config-commands

- Use to reestablish the default created when the **aaa authorization commands** command was issued.
- After the **aaa authorization commands** command has been issued, **aaa authorization config-commands** is enabled by default, which means that all configuration commands are authorized.
- Example

  host1(config)#**aaa new-model**
  host1(config)#**aaa authorization command 15 parks tacacs+ none**
  host1(config)#**no aaa authorization config-commands**

- Use the **no** version to disable AAA configuration command authorization.

aaa new-model

- Use to specify AAA new model as the authentication method for the vty lines on your router.
- If you specify AAA new model and you do not create an authentication list, users will not be able to access the router through a vty line.
- Example

  host1(config)#**aaa new-model**

- Use the **no** version to restore simple authentication.

authorization

- Use to apply AAA authorization to a specific vty line or group of lines.
- Use the **exec** keyword to apply this authorization to CLI access in general.
- Use the **commands** keyword to apply this authorization to user commands of the privilege level you specify.
- You can specify the name of an authorization method list; if no method list is specified, the default is used.
- After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined list to the appropriate lines for authorization to take place.
- Example

  host1(config)#**line vty 6**
  host1(line-config)#**authorization commands 15 sonny**

- Use the **no** version to disable authorization.

line

- Use to specify the virtual terminal lines.
- You can set a single line or a range of lines. The range is 0–29.
- Example

  host1(config)#**line vty 6 10**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login authentication

- Use to apply an authentication list to the vty lines you specified on your router.
- Example

  host1(config-line)#**login authentication my_auth_list**

- Use the **no** version to specify that the system should use the default authentication list.

password

- Use to specify a password on a line or a range of lines if you specified the line option with the **aaa authentication login** command.
- If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals.

- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 bcA";+1aeJD8)/[1ZDP6**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

- Use the **no** version to remove the password. By default, no password is specified.

Virtual Terminal Access Lists

You can provide additional security for your router by using access lists to restrict access to vty lines.

When the router attempts to authenticate a user, it always selects the first vty line that has an access class that permits that user's host. The vty line's configuration must authenticate the user to allow access. Otherwise, the user can never gain access. Consequently, we recommend that you use identical authentication configurations for all vtys that have the same access class list.

To set up access lists:

- Associate the access list with inbound Telnet sessions.

  host1(config)#**line vty 12 15**
  host1(config-line)#**access-class boston in**

- Configure an access list.

  host1(config)#**access-list boston permit any**

access-class in

- Use to associate the access list with vty lines.
- Example—This example sets the virtual terminal lines to which you want to restrict access and specifies an access class to grant access to incoming requests.

  host1(config)#**line vty 12 15**
  host1(config-line)#**access-class boston in**

- Use the **no** version to remove access restrictions.

access-list

- Use to configure an access list.
- Example

  host1(config)#**access-list boston permit any**

- Use the **no** version to remove the access list.

Secure System Administration with SSH

The system supports the SSH protocol version 2 as a secure alternative to Telnet for system administration.

NOTE: Versions earlier than 2.0.12 of the SSH protocol client are not supported. The SSH server embedded within the router recognizes SSH clients that report an SSH protocol version of 1.99, with the expectation that such clients are compatible with SSH protocol version 2.0. Clients that report an SSH protocol version of 1.99 apparently do so to determine the protocol version supported by the server.

SSH provides the following major features:

- Server authentication through a Diffie-Hellman key exchange—Protects against hackers interjecting mimics to obtain your password. You can be confident that you are connected to your own router.
- User authentication—Ensures that the router is allowing connection from a permitted host and remote user.

NOTE: Digital Signature Standard (DSS) public key user authentication for SSH is not supported. RADIUS password authentication is the only method of user authentication currently supported. It is enabled by default. If RADIUS authentication is disabled, then all SSH clients that pass protocol negotiation are accepted.

- Data encryption and key-protected hashing—Provides a secure, trustable session to the upper-layer user interface. Encryption provides confidentiality by preventing unauthorized persons from listening in on management traffic. Encryption and hashing ensure data integrity to obstruct man-in-the-middle attacks, in which unauthorized persons access messages and modify them without detection.

Transport

The SSH transport layer handles algorithm negotiation between the server and client over TCP/IP. Negotiation begins when the SSH client and server send each other textual information that identifies their SSH version. If they both agree that the versions are compatible, the client and server exchange lists that specify the algorithms that they support for key exchange, encryption, data integrity through a message authentication code (MAC), and compression. Each party sends two lists. One list has the algorithms supported for transmission; the other has the algorithms supported for receipt. The algorithms are specified in order of preference in each list. The client and server use the algorithm for each process that matches the client's highest preference and is supported by the server. If no intersection is found, the negotiation attempt fails and the connection is terminated.

If algorithm negotiation is successful, the server sends its public host key to the client for authentication so the client can be certain that it is connected to the intended host rather than to an imposter. The client compares the key to its host key database. The client authenticates the server if the key is found in the database. If the key is not present, then the client can accept or reject this new, unknown key depending on how you have configured the client. For more information, see *Host Key Management* on page 461.

When the client authenticates the server's host key, it begins the transport key exchange process by sending the key data required by the negotiated set of algorithms. The server responds by sending its own key data set. If both sides agree that the keys are consistent and authentic, the keys are applied so that all subsequent messages between client and server are encrypted, authenticated, and compressed according to the negotiated algorithms.

User Authentication

User authentication begins after the transport keys are applied. The client typically asks the server which authentication methods it supports. The server responds with a list of supported methods with no preference.

The client specifies a user authentication method. If the chosen method is supported by the server, the client then challenges the user—that is, the client prompts the user for a password or public-key pass phrase. The client sends the challenge response from the user and the username to the server. The server authenticates the user based on this response.

The system software currently supports only RADIUS password authentication, which is enabled by default. The RADIUS server validates the username and password from its database. If user authentication is disabled, then all SSH clients that pass protocol negotiation are accepted.

Connection

The SSH connection layer creates the user session when the user is authenticated. The server waits for a connection request. The router currently supports only shell requests, which the server interprets as a request for entry into a CLI session. The server ignores any other requests, such as X11 or TCP/IP tunneling.

Key Management

The E-series router implementation of SSH provides for management of user keys and host keys.

User Key Management

Key administration is still under development for the server environment.

Host Key Management

You create a host key for the SSH server with the **crypto key generate dss** command. If a host key already exists, this command replaces it with a new key and terminates all ongoing SSH sessions. Any SSH clients that previously accepted the old host key reject the new key the next time the client and server connect. The client then typically instructs the end user to delete the locally cached host key and to try to connect again.

CAUTION: Use caution issuing the **crypto key generate dss** command from an SSH client. Issuing this command will terminate that SSH session; it will be the last command you send from that session.

The public half of the host key is sent from the server to the client as part of the transport layer negotiation. The client attempts to find a match for this key with one stored locally and assigned to the server. If the client does not find a match, it can accept or reject the key sent from the server. Refer to your client documentation for detailed information. You typically configure the client to do one of the following:

- Never accept an unknown key.
- Always accept an unknown key.
- Query the administrator before accepting an unknown key.

If you do not want the client ever to trust the server when it sends an unknown key, you must manually copy—using the **copy** command—the host key from each server to each intended client. This is the only way to be certain that each client has a local copy of the necessary keys for matching during negotiation.

If you configure the client to accept unknown keys—either automatically or with administrator approval—this acceptance policy applies only to the first time the client receives a key from a particular server. When the SSH client accepts a host key, it stores the key locally and uses it for all future comparisons with keys received from that host. If the client subsequently receives a different key—a new unknown—from that server, it is rejected.

You cannot configure an SSH client to accept a new key after it has accepted a key from an SSH server. You must delete the old key before a new key can be accepted.

Performance

Generating a host key is computationally intensive and can take up to several minutes depending on the load of the system. The system cannot accept any CLI inputs from that session while it is generating the key.

Encryption, data integrity validation, and compression are all computationally intensive. These features can affect router performance in the following ways:

- Reduce the effective baud rate compared with Telnet or the local CLI. Users are unlikely to notice this performance degradation because user interaction is inherently slow compared with other system operations.
- Increase the general load on the system CPU.

Security Concerns

You might be concerned about security with the current support of SSH for the following reasons:

- Only RADIUS user authentication is supported. If you disable user authentication, all users are accepted if the client and server successfully complete negotiation.
- Because the load on the system CPU increases with use of SSH, you might be concerned about denial-of-service attacks. However, the forwarding engine takes care of this issue, because it limits the rate at which it sends packets to the system controller. A flood of packets from a packet generator does not cause problems regardless of whether SSH is enabled.

Before You Configure SSH

You must obtain and install a commercial SSH client on the host from which you want to administer the system. Versions earlier than 2.0.12 of the SSH client are not supported.

Determine your Telnet policy before you configure SSH on your system. Effective use of SSH implies that you should severely limit Telnet access to the system. To limit Telnet access, create access control lists that prevent almost all Telnet usage, permitting only trusted administrators to access the system through Telnet. For example, you might limit access to administrators who need to Telnet to the system from a remote host that does not have the SSH client installed.

You must install and configure a RADIUS server on a host machine before you configure SSH on your router. Refer to your RADIUS server documentation for information about choosing a host machine and installing the server software. You must also configure the RADIUS client on your router. See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access* for more information.

SSH Configuration Tasks

You configure SSH on individual virtual routers, rather than on the global system. To configure SSH:

1. Access the context of the virtual router.
2. Configure encryption.(Optional)
3. Configure user authentication, including connection parameters.
4. Configure message authentication.(Optional)
5. Enable SSH.
6. Display SSH to verify configuration.

Configuring Encryption

The embedded SSH server and external SSH client maintain separate lists of the encryption algorithms that each supports. Lists are kept for inbound and outbound algorithms. For the server:

- Inbound means the algorithms that the server supports for information coming in from a client.
- Outbound means the algorithms that the server supports for information it sends out to a client.

You must configure each list separately. By default, all of the supported encryption algorithms are available. You need to configure encryption only if you need to specifically remove or add any supported algorithm from the list. Refer to your SSH client documentation for details on configuring encryption on your client. The system supports the following SSH algorithms for encryption:

- 3des-cbc—A triple DES block cipher with 8-byte blocks and 24 bytes of key data. The first 8 bytes of the key data are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
- blowfish-cbc—A block cipher with 8-byte blocks and 128-bit keys that provides strong encryption and is faster than DES.
- twofish-cbc—A block cipher with 16-byte blocks and 256-bit keys that is stronger and faster than Blowfish encryption.

Although it is not recommended, you can also specify **none**. In this case, the system does not perform encryption.

ip ssh crypto

- Use to add an encryption algorithm to the specified support list for the SSH server.

  Example 1—This example adds the blowfish-cbc algorithm to the list of supported inbound algorithms.

  host1(config)#**ip ssh crypto client-to-server blowfish-cbc**

  Example 2—This example removes the 3des-cbc algorithm from the list of supported outbound algorithms.

  host1(config)#**ip ssh crypto server-to-client no 3des-cbc**

- The **default** version restores the specified list to the factory default, which includes all supported algorithms (3des-cbc, twofish-cbc, and blowfish-cbc). The default list does not include the **none** option.

  Example

  host1(config)#**ip ssh crypto server-to-client default 3des-cbc**

- If you do not specify a direction (client-to-server or server-to-client), the command applies the algorithm to both inbound and outbound lists.
- Use the **no** version to remove or exclude an algorithm from the specified list.

Configuring User Authentication

The router supports RADIUS for user authentication. RADIUS authentication is enabled by default. You must have previously configured a RADIUS server on a host machine and the RADIUS client on your system.

You can specify timeout and retry limits to control the SSH connection process. The limits apply only from the time the user first tries to connect until the user has been successfully authenticated. The timeout limits are independent of any limits configured for virtual terminals (vtys). The following limits are supported:

- SSH timeout—Maximum time allowed for a user to be authenticated, starting from the receipt of the first SSH protocol packet.
- Authentication retry—Number of times a user can try to correct incorrect information—such as a bad password—in a given connection attempt.
- Sleep—Prevents a user that has exceeded the authentication retry limit from connecting from the same host within the specified period.

ip ssh authentication-retries

- Use to set the number of times that a user can retry a failed authentication, such as trying to correct a wrong password. The SSH server terminates the connection when the limit is exceeded.
- Specify an integer from 0–20.
- Example

  host1(config)#**ip ssh authentication-retries 3**

- Use the **no** version to restore the default value, 20 retry attempts.

ip ssh disable-user-authentication

- Use to disable RADIUS password authentication. If you disable RADIUS authentication, all SSH clients that pass protocol negotiation are accepted.
- RADIUS authentication is enabled by default.
- Example

  host1(config)#**ip ssh disable-user-authentication**

- Use the **no** version to restore RADIUS authentication.

ip ssh sleep

- Use to set a sleep period in seconds for users that have exceeded the authentication retry limit. Connection attempts from the user at the same host are denied until this period expires.
- Specify any nonnegative integer.
- Example

  host1(config)#**ip ssh sleep 300**

- Use the **no** version to restore the default value, 600 seconds.

ip ssh timeout

- Use to set a timeout period in seconds. The SSH server terminates the connection if protocol negotiation—including user authentication—is not completed within this timeout.
- Specify an integer from 10–600.
- Example

  host1(config)#**ip ssh timeout 480**

- Use the **no** version to restore the default value, 600 seconds.

Configuring Message Authentication

The SSH server and SSH client maintain separate lists of the message authentication algorithms that each supports. Lists are kept for *inbound* and *outbound* algorithms. For the server, *inbound* means the algorithms that the server supports for information coming in from a client. For the server, *outbound* means the algorithms that the server supports for information it sends out to a client. You must configure each list separately. By default, all of the supported encryption algorithms are available. You need to configure encryption only if you need to specifically remove or add any supported algorithm from the list. The system supports the following SSH algorithms for hash function-based message authentication:

- hmac-sha1—Uses Secure Hash Algorithm 1 (SHA-1) to create a 160-bit message digest from which it generates the MAC.
- hmac-sha1-96—Uses the first 96 bits of the SHA-1 message digest to generate the MAC.
- hmac-md5—Uses MD5 hashing to create a 128-bit message digest from which it generates the MAC.

Although it is not recommended, you can also specify **none**. In this case, the system does not verify the integrity of the data.

ip ssh mac

- Use to add a message authentication algorithm to the specified support list for the SSH server.

  Example 1—This example adds the hmac-md5 algorithm to the list of supported outbound algorithms.

  ```
  host1(config)#ip ssh mac server-to-client hmac-md5
  ```

- If you to not specify a direction (client-to-server or server-to-client), the command applies the algorithm to both inbound and outbound lists.
- The **default** version restores the specified list to the factory default, which includes all supported algorithms (hmac-md5, hmac-sha1, and hmac-sha1-96). The default list does not include the *none* option.
- Example 2—This example restores the hmac-sha1 algorithm to the list of supported inbound algorithms.

  ```
  host1(config)#ip ssh mac client-to-server default hmac-sha1
  ```

- Use the **no** version to remove or exclude an algorithm from the specified list.

  Example 3—This example removes the hmac-sha1 algorithm from the list of supported inbound algorithms.

  ```
  host1(config)#ip ssh mac client-to-server no hmac-sha1
  ```

Enabling and Disabling SSH

The SSH server daemon starts only if the server host key exists when the router boots. The host key resides in NVS and is persistent across system reboots. After it has started, the daemon listens for traffic on TCP port 22. The server daemon is disabled by default.

crypto key dss

- Use the **generate** keyword to create the SSH server host key and enable the daemon.
- Example

  host1(config)#**crypto key generate dss**

- Use the **zeroize** keyword to remove the SSH server host key and stop the SSH daemon if it is running. Issuing this command terminates any active client sessions. The next time the router boots after this command is issued, the SSH server daemon is not started.
- The command is not displayed by the **show configuration** command.

NOTE: SSH can be enabled or disabled regardless of the state of the Telnet daemon. If SSH is enabled, use access control lists to limit access through Telnet. See *Virtual Terminal Access Lists* on page 458 for information about using access control lists.

- Example

  host1(config)#**crypto key zeroize dss**

- There is no **no** version.

Displaying SSH Status

You can monitor the current state of the SSH server with the **show ip ssh** command.

show ip ssh

- Use to display the current state of the SSH server.
- Use the **detail** keyword to display the encryption and MAC algorithm lists for the client and server. For each active session, **detail** shows the version of SSH running on the client and the algorithms in use for encryption and message authentication.
- Field descriptions
  - daemon status—Indicates whether the SSH server is enabled; if so, how long it has been up
  - supported encryption, inbound—Encryption algorithms supported inbound from the client
  - supported encryption, outbound—Encryption algorithms supported outbound to the client
  - supported MAC, inbound—Message authentication code algorithms supported inbound from the client

- supported MAC outbound—Message authentication code algorithms supported outbound to the client
- connections since last system reset—Number of connections made through SSH since the last time the system was reset
- connections since daemon startup—Number of connections made since the SSH server was enabled
- active sessions—Number of SSH sessions currently active
  - id—Session ID number
  - username—Username for the remote user that initiated the session
  - host—IP address of the remote client
  - uptime (d:h:m:s)—Duration of the session
  - client version—Version of the SSH software run by the remote client
  - ciphers inbound/outbound—Encryption algorithms used by the client and the system for this session
  - MAC inbound/outbound—Message authentication code algorithms used by the client and the system for this session

- Example

```
host1#show ip ssh detail

SSH Server version: SSH-2.0-2.0.12

daemon status: enabled, up since MON NOV 08 1999 14:38:19 UTC

supported encryption, inbound: 3des-cbc,blowfish-cbc,twofish-cbc
supported encryption, outbound: 3des-cbc,blowfish-cbc,twofish-cbc
supported MAC, inbound: hmac-sha1,hmac-sha1-96,hmac-md5
supported MAC, outbound: hmac-sha1,hmac-sha1-96,hmac-md5

connections since last system reset: 4 out of 4 attempts
connections since daemon startup:    4 out of 4 attempts

active sessions: 1
```

id	username	host	uptime (d:h:m:s)	client version	ciphers inbound/outbound	MAC inbound/outbound
3	mcarr	10.0.0.145	0:00:00:19	SSH-2.0-2.0.12 F-SECURE SSH	3des-cbc/3des-cbc	hmac-md5/hmac-md5

- To view failed connection attempts and other protocol errors logged at the error severity level, use the **show log data** command:

  host1#**show log data category ssh severity error**

Terminating an SSH Session

You can use the session identifier to terminate an SSH session.

disconnect ssh

- Use to terminate an active SSH session.
- Use the **show ip ssh** command to determine the session identifier for the session to terminate.
- Example

  host1(config)#**disconnect ssh 12**

NOTE: You can also use the **clear line vty** terminal command to terminate SSH sessions. In that case, use the **show users** command to determine the virtual terminal number to specify with the **clear line vty** terminal command.

- There is no **no** version.

Restricting User Access

Users who are authenticated through RADIUS or TACACS+ can be restricted to certain sets of commands and virtual routers (VRs). The levels of access are shown in Table 52. For information about TACACS+, see *JUNOSe Broadband Access Configuration Guide, Chapter 9, Configuring TACACS+*.

Table 52: CLI User Access Levels

Access Level	Commands Available
0	**disable**, **enable**, **exit**, and **help** commands
1	Level 0 commands and all other commands available in User Exec mode
5	Level 1 commands and all Privileged **show** commands
10	All commands except support and privilege change commands
15	Commands that Juniper Networks Technical Support may provide and all other commands

Restricting Access to Commands with RADIUS

You can use RADIUS authentication to specify a level of commands that a user is allowed. If you do not configure RADIUS authentication for the console or virtual terminals, all users who successfully log in are automatically granted Level 1 access.

The vendor-specific attribute (VSA) Admin-Auth-Level supports the levels of access shown in Table 52. In addition to VSA access level support, the software provides access to levels 1 and 10 through the Initial-Auth-Level in the standard RADIUS Service-Type attribute. If the RADIUS Service-Type attribute is included in the RADIUS Access-Accept message, the standard attribute overrides any VSA setting.

If you are using the RADIUS Service-Type attribute to assign access levels, the system sets the Initial-Auth-Level as follows:

- If the Service-Type attribute is set to "administrative," then the Initial-Auth-Level is set to 10.
- If the Service-Type attribute is set to "nas prompt" or "login," the Initial-Auth-Level is set to 1.

Per-User Enable Authentication

After a user has been authenticated through RADIUS, the RADIUS server provides the E-series router with the names of the privilege levels (for example, "10") that the user has **enable** access to. When the user attempts to access a privilege level through the **enable** command, the system either denies or approves the user's request.

The decision to deny or approve the user's request is based on the list the system received through RADIUS. See Table 53.

Table 53: Juniper Networks–Specific CLI Access VSA Descriptions

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Initial-CLI- Access-Level	Specifies the initial level of access to CLI commands.	26	len	18	sublen	Single attribute; enter only: 0, 1, 5, 10, or 15
Alt-CLI- Access-Level	Specifies level of access to CLI commands.	26	len	20	sublen	Single attribute; enter only: 0, 1, 5, 10, or 15

NOTE: All levels to which a user can have access must explicitly be specified in the Admin-Auth-Set VSA.

The user is not prompted for a password, because the system knows whether or not the user should have access to the requested level. If the user is not authenticated through RADIUS, the router uses the system-wide **enable** passwords instead.

Restricting Access to Virtual Routers

You can use RADIUS authentication to specify whether users can access all virtual routers (VRs), one specific VR, or a set of specific VRs.

NOTE: This classification is independent of the command access levels configurable through the Initial-CLI-Access-Level VSA.

The VSA Allow-All-VR-Access controls access; the VSA Virtual-Router controls the VR to which the user logs in, and the VSA Alt-CLI-Virtual-Router-Name specifies which VRs other than the VR specified by the VSA virtual-router are accessible to restricted users. See Table 54.

Table 54: Juniper Networks–Specific Virtual Router Access VSA Descriptions

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Allow-All-VR-Access	Specifies user access to all virtual routers.	26	len	19	sublen	Integer: 0 – disable, 1 – enable
Virtual-Router	Specifies the VR to which the user logs in or the only VR to which a user has access. The default setting is the default VR.	26	len	1	sublen	String: *virtual-router-name*
Alt-CLI-Virtual-Router-Name	Specifies a VR, other than the VR specified by the Virtual-Router VSA, to which the user has access. You can define this VSA multiple times to define a set of VRs to which a user has access.	26	len	21	sublen	String: *virtual-router-name*

VSA Configuration Examples

Consider a router on which five VRs have been configured. The VRs are called Boston, Chicago, Detroit, Los Angeles, and San Francisco. The following examples illustrate how to use the VSAs to control a user's access to these VRs.

Example 1 In this example, you want the user to have access to all VRs and to log in to the default VR. Accept the default setting or set the following VSA:

- Allow-All-VR-Access—1

Example 2 In this example, you want the user to have access to all VRs and to log in to the VR Boston. Set the VSAs as follows:

- Allow-All-VR-Access—1
- Virtual-Router—Boston

Example 3 In this example, you want the user to have access only to the VR Boston. Set the VSAs as follows:

- Allow-All-VR-Access—0
- Virtual-Router—Boston

Example 4 In this example, you want the user to log in to VR Boston, and to have access to VRs Chicago, Los Angeles, and San Francisco. Set the VSAs as follows:

- Allow-All-VR-Access—0
- Virtual-Router—Boston
- Alt-CLI-Virtual-Router-Name—Chicago

- Alt-CLI-Virtual-Router-Name—Los Angeles
- Alt-CLI-Virtual-Router-Name—San Francisco

Commands Available to Users

If you do not configure RADIUS authentication for the console or virtual terminals, there are no restrictions on VR access for any user who successfully logs in to the router. For example, nonrestricted users can:

- Issue the **virtual-router** command in Privileged Exec mode, to switch to another previously created virtual router.
- Issue the **virtual-router** command in Global Configuration mode to create a new virtual router and switch to its context.
- Access Global Configuration mode to configure the router and virtual routers.
- View all settings for the router and all virtual routers.

User restricted to one or a set of specific VRs can see and use only a limited set of commands to monitor the status of those VRs and view some configuration settings on those VRs. More specifically, such users:

- Can issue the **virtual-router** command in Privileged Exec mode to switch to another previously configured VR to which they have access.
- Cannot create new VRs or access VRs other than those to which they have access.
- Cannot access Global Configuration mode and cannot configure VRs to which they have access.
- Cannot see or use any commands associated with the file system, boot settings, or system configuration.

The following table lists some, but not all, commands accessed from Exec mode that are available only to users with no VR restriction:

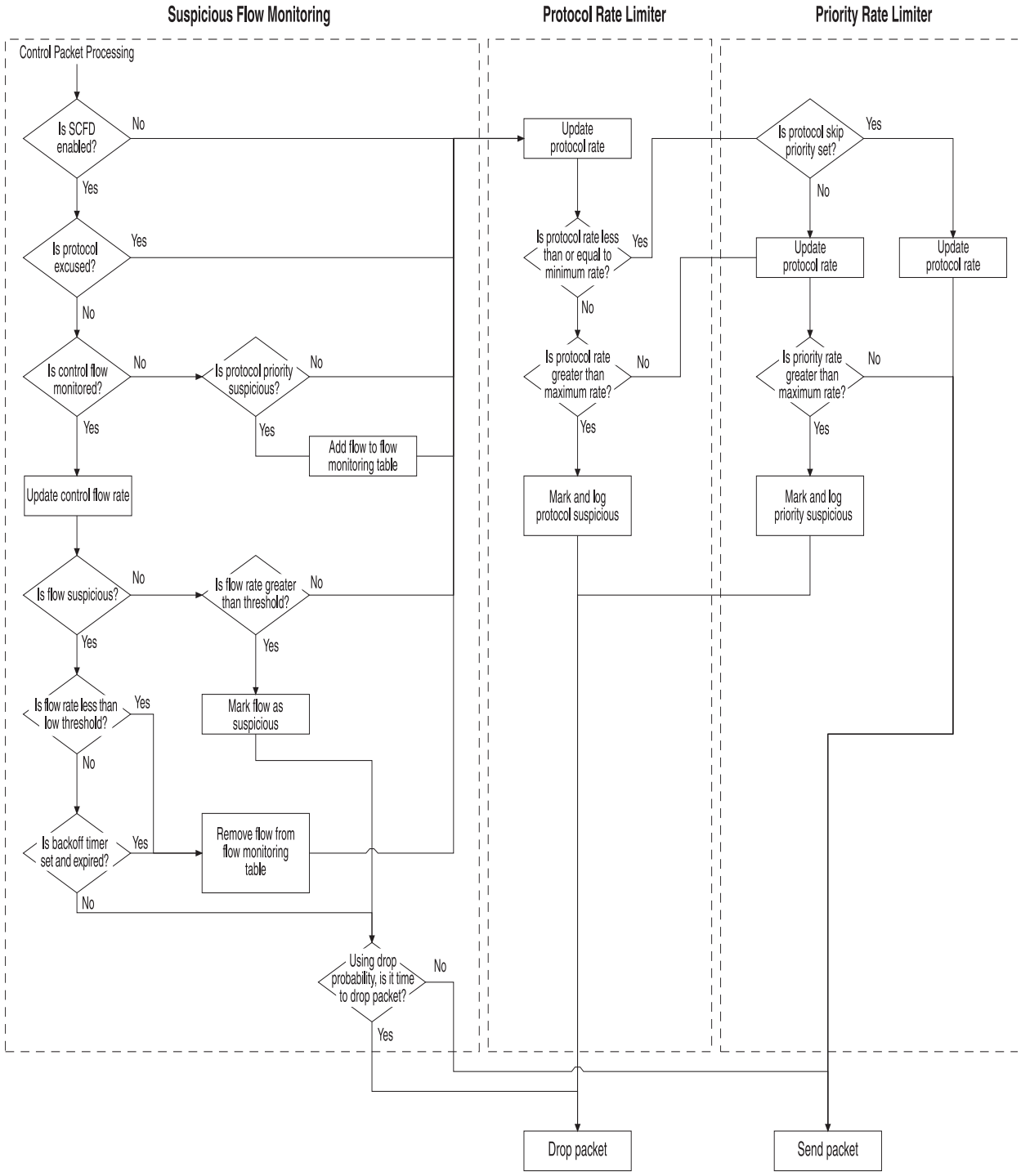
clear line	reload	show redundancy
clock set	reload slot	show secrets
copy	rename	show subsystems
copy running-configuration	redundancy force-switchover	show timing
delete	redundancy revert	show users
dir	show boot	show utilization
disconnect ssh	show config	srp switch
configure	show exception dump	synchronize
erase secrets	show ip ssh	–
halt	show line	–

Denial of Service (DoS) Protection

A denial-of-service (DoS) attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Denial of service protection provides reactive prevention from attack and determines whether the source of traffic is valid or invalid. DoS protection includes diagnostic tools and configuration options. DoS protection groups provide a simple policy that can be applied to interfaces, which can specify a set of parameters to tune behavior.

Figure 29 shows an example of the state of a flow with DoS protection using suspicious control flow detection (SCFD).

Figure 29: Typical Control Packet Processing



Suspicious Control Flow Detection

To reduce the chance of a successful denial of service (DoS) attack and to provide diagnostic abilities while undergoing an attack, the system can detect suspicious control flows and keep state on those flows. A flow is a specific control protocol on a specific interface from a particular source. When the system determines that a control flow is suspicious, it can take corrective action on that control flow.

Keeping full state on each control flow can use a large number of resources. Instead, the system detects which flows have suspicious traffic. If a control flow is marked as suspicious, every packet associated with the flow is considered suspicious. When a packet is marked as suspicious, it is dropped based on drop probability before being delivered to the control processor.

When a distributed DoS attack occurs on a line module, suspicious flow control resources can be exhausted. To provide further counter measures, you can enable the group feature, where flows are grouped together and treated as a whole. If you do not use the group feature, suspicious flows can fill up the suspicious flow table and prevent detection of additional attacking flows.

Suspicious Control Flow Monitoring

Each protocol has a per-protocol rate limit. The rate limiter is used to limit the rate of packets that proceed to the control processor for the specific protocol. Per-protocol rate limiting is also used to begin the process by which flows of the specific protocol are monitored.

Each priority has a per-priority rate limit. The rate limiter limits the rate of packets that proceed to the control processor for the specific priority. It also begins the process by which flows of the specific priority are monitored.

All protocols on each line module have a rate limit. Each protocol is associated with a given priority, which is also provided with a rate limit. When a slot comes under attack, the first lines of defense are the protocol and priority rate limiters. If the line module determines that a specific protocol or priority is under attack (because the rate has been exceeded), it proceeds to monitor all flows from the problem protocol or priority. Initially, a control flow is marked as nonsuspicious.

After a control flow is placed in the suspicious flow table, the system inspects all packets that belong to the flow. The interface controller (IC) and forwarding controller (FC) monitor the table to determine whether the suspicious flow has a packet rate above the suspicious level. If the packet rate is above this level, the flow is marked as suspicious. Marking a control flow as suspicious affects only a particular protocol on a particular interface. When a flow is marked as suspicious, all packets belonging to that flow are marked as suspicious and trapped at the forwarding controller.

Suspicious control flows are continually monitored. The flow can be restored if the flow goes below the low threshold level. The flow can also be restored based on a backoff timer. The flow is removed from the suspicious flow table if the related interface is removed.

Approximately 2000 flows can be monitored as suspicious at any time for each line module. When the suspicious flow table on a particular line module reaches its maximum and the system is not set to group flows, flows that should be marked as suspicious proceed as nonsuspicious. When you return a suspicious flow to a nonsuspicious state or delete it, the flows that did not fit into the table are added to the table.

By default, the system groups flows when the suspicious flow table size is exceeded on a line module. When the flow table is full, instead of marking a specific flow in that group as suspicious and providing information on each flow on that line module, the system groups flows based on group membership and provides information on the group instead of each flow. This flow information is useful under severe distributed DoS attacks. Group membership is based on physical port and control protocol; all flows in that group are considered suspicious.

Configurable Options

You can configure the following options for suspicious flow detection:

- Global on or off. When the option is set to off, flows or packets are not marked as suspicious. The default is on.
- Actions a line module takes when the suspicious flow table on the line module overflows:
  - Overflow—Stop recognizing new suspicious flows
  - Group—Group flows into logical groupings where some individual flows are monitored as a group
- Suspicious threshold for each protocol. The threshold is the rate in packets per second at which a flow becomes suspicious. A zero setting disables suspicious flow detection for the protocol. Flows are subject to protocol and priority rate limits, but not to suspicious flow detection.
- Low threshold for each protocol. The threshold rate determines whether an interface transitions from suspicious back to nonsuspicious. A zero setting means that the flow does not transition back to nonsuspicious based on packet rate.
- Backoff time in seconds for each protocol. After this period expires, the flow transitions to nonsuspicious regardless of the current rate. When set to zero, an interface does not return to the nonsuspicious state using a time mechanism.

You can also clear the following:

- All suspicious flows from the suspicious flow table for a specific slot.
- Suspicious flows from the suspicious flow table for the entire system.
- A single suspicious flow; returns the flow to the nonsuspicious state.

Display Options

For monitoring purposes, you can:

- Display all suspicious control flows when the system has recognized an attack.
- Display the current state and the number of transitions into suspicious state for the protocol and priority.
- Display historical counts about the number of flows made suspicious.
- View a trap or log generated when a control flow is considered suspicious.
- View a trap or log generated when a control flow is no longer suspicious.

Traps and Logs

The system generates a trap and a log message under the following conditions:

- A control flow transitions into a suspicious state; another trap and log message is generated on removal from a suspicious state.
- A protocol transitions to or from the suspicious state.
- A priority transitions to or from the suspicious state.
- The suspicious flow control system is overflowing or grouping flows on a line module.

You can control trap and log messages using CLI or SNMP commands.

Suspicious Control Flow Commands

Use the commands described in this section to regulate suspicious control flows.

baseline suspicious-control-flow-detection counts

- Use to set a baseline for statistics for suspicious control flow detection.
- Example

  host1#**baseline suspicious-control-flow-detection counts**

- There is no **no** version.

clear suspicious-control-flow-detection

- Use to clear the active state for suspicious control detection.
- If you do not specify a slot or interface, clears all suspicious flows.
- If you specify a slot, clears all specified suspicious flows on that slot.
- If you specify an interface and protocol, and source mac-address. clears that specific flow.

- Example

  host1#**clear suspicious-control-flow-detection interface atm 1/0.1 ppp Control address 0000.0001.0002**

- There is no **no** version.

suspicious-control-flow-detection grouping-off

- Use to turn off overflow protection for suspicious control flow detection, enabling flows to be grouped into larger entities when the line module flow table overflows.
- Example

  host1(config)#**suspicious-control-flow-detection grouping-off**

- Use the **no** version to turn on overflow protection.

suspicious-control-flow-detection off

- Use to turn off the suspicious control flow detection.
- Example

  host1(config)#**suspicious-control-flow-detection off**

- Use the **no** version to turn on suspicious control flow detection, which is the default.

suspicious-control-flow-detection protocol backoff-time

- Use to set the backoff time in seconds for a specific protocol that triggers the suspicious flow to return to a nonsuspicious state.
- When set to zero, a suspicious control flow for a protocol does not return to a nonsuspicious state using a time mechanism.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi backoff-time 300**

- Use the **no** version to restore the defaults for the protocol, 300 seconds.

suspicious-control-flow-detection protocol low-threshold

- Use to set a threshold for a specific protocol; if the flow rate falls below this rate, a suspicious flow changes to the nonsuspicious state.
- Low threshold is the rate in packets per second at which a suspicious flow becomes no longer suspicious.
- When set to zero, a suspicious flow cannot change to the nonsuspicious state by means of a low threshold rate. To clear this flow, you must use the **clear suspicious-control-flow-detection** command.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi low-threshold 512**

- Use the **no** version to restore the defaults for the protocol.

suspicious-control-flow-detection protocol threshold

- Use to set the threshold in packets per second for a specific protocol, which triggers the flow to become a suspicious flow.
- When set to zero, a suspicious flow cannot change to the nonsuspicious state via a threshold rate.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi threshold 1024**

- Use the **no** version to restore the defaults for the protocol.

Monitoring Suspicious Control Flow

Use the commands described in this section to monitor suspicious control flows.

show suspicious-control-flow-detection counts

- Use to display statistics for suspicious control flow detection. When a slot is specified, displays only information for the specific slot. If no slot is specified, displays information for all slots.
- The **delta** keyword displays statistics for the current baseline.
- Field descriptions
  - Number of suspicious flows total—Total number of suspicious flows, current and past
  - Number of suspicious flows current—Number of suspicious flows currently detected and monitored
  - Number of groups total—Total number of groups, current and past
  - Number of groups current—Number of groups currently detected and monitored
  - Number of false negatives total—Total number of flows monitored that have not become suspicious (exceeded their threshold)
  - Number of false negatives current—Current number of flows monitored that have not become suspicious (exceeded their threshold)
  - Number of table overflows—Number of times a flow table overflows
- Example

```
host1(config)#show suspicious-control-flow-detection counts
Suspicious Flow Detection System Counts
        Number of suspicious flows total: 0
        Number of suspicious flows current: 0
        Number of groups total: 0
        Number of groups current: 0
        Number of false negatives total: 0
        Number of false negatives current: 0
        Number of table overflows: 0
```

show suspicious-control-flow-detection flows

- Use to display suspicious flows.
- Field descriptions
  - Interface—Interface for the flow
  - Protocol—Control protocol of the flow
  - MAC address—Source MAC address of the flow
  - InSlot—For certain flows detected on egress, the possible ingress slot of the flow
  - Rate (pps)—Rate of the flow
  - Peak Rate (pps)—Peak rate of the flow
  - Time Since Created—Time since the flow was determined to be suspicious, in hh:mm:sec format
- Example

```
host1(config)#show suspicious-control-flow-detection flows
Suspicious Flow Detection System Flows
                                                    Peak            Time
                                              In    Rate    Rate    since
Interface             Protocol        MAC address Slot (pps)   (pps)   Create
------------------    -------         ------------  ----- ---    -------  -------
GigabitEthernet 1/0/7 Ethernet ARP    0000.0100.0002 ---  1000030 1000050 00:00:32

*group 3 slot 1       EthernetArpMiss 0000.0100.0003 ---  1000    3000    00:10:10
```

show suspicious-control-flow-detection info

- Use to display information about suspicious flows.
- You can specify the following keywords:
  - **delta**—Displays statistics for the current baseline
  - **brief**—Displays only suspicious information
  - **slot**—Displays information for the specific slot
- Field descriptions
  - Protocol Information
    - Protocol—Control protocol of the flow
    - State
      - OK—Protocol is currently not receiving an excess amount of traffic.
      - Suspicious—Protocol detected as receiving an excess amount of traffic within the last backoff time in number of seconds.
    - Transitions—Number of times this protocol or priority has transitioned to the suspicious state
  - Priority Information
    - Priority—Priorities map to a specific queue and color; priority groups are Hi-Green, Hi-Yellow, Lo-Green and Lo-Yellow.

- State:
  - OK—Protocol is currently not receiving an excess amount of traffic
  - Suspicious—Protocol detected as receiving an excess amount of traffic within the last backoff time in number of seconds.
- Transitions—Number of times this protocol or priority has transitioned to the suspicious state

- Example

```
host1(config)#show suspicious-control-flow-detection info slot 2
Suspicious Flow Detection System Information
        Suspicious Flow Detection System is enabled

        Using Groups

The suspicious control flow system is not in overflow state or using groups
Protocol Information
Protocol                                 State      Transitions
---------------------------------------- ---------- -----------
Ppp Echo Request                         OK         0
Ppp Echo Reply                           OK         0
Ppp Echo Reply Fastpath                  OK         0
Ppp Control                              OK         0
Atm Control (ILMI)                       OK         0
Atm OAM                                  OK         0
Atm Dynamic Interface Column Creation    OK         0
Atm Inverse ARP                          OK         0
Frame Relay LMI Control                  OK         0
Frame Relay Inverse Arp                  OK         0
Pppoe Control                            OK         0
Pppoe Config Dynamic Interface Column    OK         0
 Creation
Ethernet ARP Miss                        OK         0
Ethernet ARP                             OK         0
Ethernet LACP packet                     OK         0
Ethernet Dynamic Interface Column        OK         0
 Creation
Slep SLARP                               OK         0
MPLS TTL Exceeded On Receive             OK         0
MPLS TTL Exceeded On Transmit            OK         0
MPLS MTU Exceeded                        OK         0
Ipsec Transport Mode L2tp Control        OK         0
NAT/Firewall Payload                     OK         0
NAT/Firewall Update Table                OK         0
DHCP External                            OK         0
IP OSI                                   OK         0
IP TTL Expired                           OK         0
IP Options Other                         OK         0
IP Options Router Alert                  OK         0
IP Multicast/Broadcast Other             OK         0
IP Multicast DHCP (SC)                   OK         0
IP Multicast Control (SC)                OK         0
IP Multicast Control (IC)                OK         0
IP Multicast VRRP                        OK         0
IP Mulitcast Cache Miss                  OK         0
IP Multicast Cache Miss Auto Reply       OK         0
IP Multicast Wrong Interface             OK         0
IP Local DHCP (SC)                       OK         0
IP Local Dhcp (IC)                       OK         0
IP Local Icmp Echo                       OK         0
```

```
IP Local Icmp Other                     OK         0
IP Local LDP                            OK         0
IP Local BGP                            OK         0
IP Local OSPF                           OK         0
IP Local RSVP                           OK         0
IP Local PIM                            OK         0
IP Local COPS                           OK         0
IP Local L2tp Control (SC)              OK         0
IP Local L2tp Control (IC)              OK         0
IP Local Other                          OK         0
IP Local Subscriber Interface Miss      OK         0
IP Route To SRP Ethernet                OK         0
IP Route No Route Exists                OK         0
IP Normal Path MTU                      OK         0
IP Neighbor Discovery                   OK         0
IP Neighbor Discovery Miss              OK         0
IP Search Error                         OK         0
IP MLD                                  OK         0
IP Local PIM Assert                     OK         0
IP Local BFD                            OK         0
IP IKE                                  OK         0
IP Reassembly                           OK         0
IP Local Icmp Frag                      OK         0
IP Local Frag                           OK         0
IP Application Classifier HTTP Redirect OK         0

Priority Information
Priority     State    Transitions
------------ ---------- -----------
Hi-Green-IC  OK         0
Hi-Yellow-IC OK         0
Lo-Green-IC  OK         0
Lo-Yellow-IC OK         1
Hi-Green-SC  OK         0
Hi-Yellow-SC OK         0
Lo-Green-SC  OK         0
Lo-Yellow-SC OK         0
```

show suspicious-control-flow-detection protocol

- Use to display protocol information for suspicious control flows.
- Field descriptions
  - Protocol—Control protocol
  - Threshold—Threshold in packets per second
  - Lo-Threshold—Low threshold in packets per second
  - Backoff-Time—Backoff time in seconds
- Example

```
host1(config)#show suspicious-control-flow-detection protocol
Protocol                        Threshold Lo-Threshold Backoff-Time
------------------------------ --------- ------------ ------------
Ppp Echo Request                       10            5          300
Ppp Echo Reply                         10            5          300
Ppp Echo Reply Fastpath                10            5          300
Ppp Control                            10            5          300
Atm Control (ILMI)                     10            5          300
Atm OAM                                10            5          300
Atm Dynamic Interface Column           10            5          300
 Creation
```

Atm Inverse ARP	10	5	300
Frame Relay LMI Control	10	5	300
Frame Relay Inverse Arp	10	5	300
Pppoe Control	512	256	300
Pppoe Config Dynamic Interface Column Creation	10	5	300
Ethernet ARP Miss	128	64	300
Ethernet ARP	128	64	300
Ethernet LACP packet	10	5	300
Ethernet Dynamic Interface Column Creation	512	256	300
Slep SLARP	128	64	300
MPLS TTL Exceeded On Receive	10	5	300
MPLS TTL Exceeded On Transmit	10	5	300
MPLS MTU Exceeded	10	5	300
Ipsec Transport Mode L2tp Control	2048	1024	300
NAT/Firewall Payload	512	256	300
NAT/Firewall Update Table	512	256	300
DHCP External	1024	512	300
IP OSI	2048	1024	300
IP TTL Expired	10	5	300
IP Options Other	512	256	300
IP Options Router Alert	2048	1024	300
IP Multicast/Broadcast Other	512	256	300
IP Multicast DHCP (SC)	512	256	300
IP Multicast Control (SC)	2048	1024	300
IP Multicast Control (IC)	512	256	300
IP Multicast VRRP	512	256	300
IP Mulitcast Cache Miss	128	64	300
IP Multicast Cache Miss Auto Reply	128	64	300
IP Multicast Wrong Interface	10	5	300
IP Local DHCP (SC)	512	256	300
IP Local Dhcp (IC)	512	256	300
IP Local Icmp Echo	512	256	300
IP Local Icmp Other	128	64	300
IP Local LDP	2048	1024	300
IP Local BGP	2048	1024	300
IP Local OSPF	64	32	300
IP Local RSVP	2048	1024	300
IP Local PIM	2048	1024	300
IP Local COPS	2048	1024	300
IP Local L2tp Control (SC)	2048	1024	300
IP Local L2tp Control (IC)	512	256	300
IP Local Other	512	256	300
IP Local Subscriber Interface Miss	512	256	300
IP Route To SRP Ethernet	512	256	300
IP Route No Route Exists	10	5	300
IP Normal Path MTU	10	5	300
IP Neighbor Discovery	128	64	300
IP Neighbor Discovery Miss	128	64	300
IP Search Error	10	5	300
IP MLD	512	256	300
IP Local PIM Assert	512	256	300
IP Local BFD	1024	512	300
IP IKE	512	256	300
IP Reassembly	2048	1024	300
IP Local Icmp Frag	512	256	300
IP Local Frag	512	256	300
IP Application Classifier HTTP Redirect	128	64	300

show snmp interfaces

- Use to display a list of interface types that are compressed in the interface tables and the interface numbering method configured on the router.
- Field descriptions
  - Compressed(Removed) Interface Types—List of interface types that are removed from the ifTable and ifStackTable
  - Armed Interface Numbering Mode—Interface numbering method configured on the router: RFC1213, RFC2863
  - maxIfIndex—Maximum value that the system will allocate to the ifIndex field
  - maxIfNumber—Maximum number of interfaces allowed in the ifTable
  - Interface Description Setting—Method used to encode the ifDescr and ifName objects: common, legacy, proprietary
- Example

```
host1#show snmp interfaces
Compressed(Removed) Interface Types:
HDLC, FT1, ATM, ATM1483
Armed Interface Numbering Mode:
RFC1213, maxIfIndex=65535, maxIfNumber=65535
Interface Description Setting: proprietary
```

Denial-of-Service Protection Groups

A DoS protection group provides a simple policy that can be applied to interfaces. This policy can specify a complete set of parameters to tune the behavior of the DoS protection groups. The system uses these parameters to determine the priority and rates for various control protocols. The rate of traffic for a particular protocol is unlikely to be the same on all ports in the system. A configuration can have several types of interfaces, such as DHCP access clients, PPPoE access clients, and uplink interfaces. Each of these interfaces requires a different DoS configuration. All interfaces are associated with a default DoS protection group, which has standard system defaults. The maximum rates are per line module, and the drop probability is 100 percent (all suspicious packets are dropped).

Group Parameters

DoS protection groups support the following set of parameters:

- Protocol-to-priority mapping enables you to map a protocol to one of four priorities.
- Protocol burst enables you to configure the burst level for the protocol. The burst is configurable in packets, and defaults to a value in packets that is one half of the maximum rate.

- Protocol maximum rate limit (per line module) enables you to map a protocol to a maximum rate limit. This rate limit applies to all packets for a particular protocol for interfaces belonging to this particular DoS protection group on a line module. By having a DoS protection group on a single line module, the total maximum rate for a protocol can be up to the sum of the four rates configured, depending on the DoS group attached to an interface. You can set a maximum rate of zero for protocols that are not used. The actual rate never exceeds the maximum rate, but the actual rate allowed can be less than the configured maximum rate because of the weighting of protocols within a DoS protection group and the use of multiple DoS protection groups.

- Protocol weight with respect to other protocols in the DoS protection group enables you to balance the priority of the protocols. For each priority grouping, weight determines the effective minimum rate that each protocol receives. Within each priority, the sum of the minimum rates for all protocols using that priority is equal to or less than the priority rate times the over-subscription value. Each priority has a separate rate for each DoS protection group.

- Protocol drop probability for suspicious packets enables you to map a protocol to a specific drop probability. The drop probability is the percentage probability that a suspicious packet is dropped.

- Protocol skip priority rate limiter enables you to configure the system so that the specified protocol is not subject to the priority rate limiter for the priority and DoS protection group selected. The default is off—the protocol is subject to priority rate limiting.

- Priority rate sets the rate of the priority in packets per second for the line module. If this rate is exceeded, it triggers DoS suspicious control flow detection.

- Priority burst enables you to set the number of packets allowed to exceed the maximum rate before packets are dropped and DoS suspicious control flow detection is triggered.

- Priority oversubscription enables you to set an oversubscription factor for the priority rate limiter. In addition to the priority rate, it calculates the minimum rate limits for protocols with a priority grouping and allows for oversubscription of the priority rate. The value indicates a percentage that the priority rate limiter is allowed to be oversubscribed, in the range 100–1000.

Attaching Groups

By default, each interface belongs to the default DoS protection group. The name is the only non-configurable aspect of the default DoS protection group.

The DoS protection group is a configurable parameter for all Layer 2 and IP interfaces. Similar to other configurable interface parameters, the DoS protection group can be set using profiles.

Because all newly created interfaces default to using the default DoS protection group, they do not inherit any DoS protection group association from a higher or lower interface binding. The DoS group applies to all types of control flows for the specific interface. For example, an IP interface supports a variety of control protocols, each of which can be separately mapped to a priority and drop probability, but to a single DoS protection group.

Protocol Mapping

Table 55 and Table 56 list the protocols mapped within DoS protection groups.

Table 55: Layer 2-Related Protocols

CLI Name	Description of Flow
atmControl	ATM ILMI packets
atmOAM	ATM OAM packets
atmDynamicIf	ATM dynamic interface column creation
atmInverseArp	ATM inverse ARP packets
dhcpExternal	DHCP external packets
ethernetArpMiss	Ethernet/Bridged Ethernet request to send ARP
ethernetArp	Ethernet/Bridged Ethernet reception of ARP packet
ethernetLacp	Ethernet LACP packet
ethernetDynamicIf	Ethernet/Bridged Ethernet dynamic VLAN interface creation
flisInPayload	Firewall/NAT payload
flisInPayloadUpdateTbl	Firewall/NAT payload and update table
frameRelayControl	Frame Relay LMI packets
frameRelayArp	Frame Relay inverse ARP packets
itmL2tpControl	IPSec transport mode L2TP control packets
mplsTtlOnRx	MPLS TTL expired on ingress
mplsTtlOnTx	MPLS TTL expired on egress
mplsMtu	MPLS MTU exceeded
pppEchoRequest	PPP echo request packets destined for the IC
pppEchoReply	PPP echo reply packets destined for the IC
pppEchoReplyFast	PPP echo request packets generating an FC-based reply
pppControl	other PPP control packets
pppoeControl	PPPoE PADx packets

Table 55: Layer 2-Related Protocols (continued)

CLI Name	Description of Flow
pppoePppConfig	PPPoE handling of PPP LCP packets for dynamic interface creation
slepSlarp	Serial Line Interface SLARP packets

Table 56: IP-Related Protocols

CLI Name	Description of Flow
ipAppClassifierHttpRedirect	IP Application Classifier (HTTP redirect) packets
ipIke	IP IKE packet
ipLocalBfd	IP BFD packets
ipLocalBgp	IP BGP packets
ipLocalCops	IP COPS packets
ipLocalDemuxMiss	IP Subscriber Interface Miss packets
ipLocalDhcpIc	IP DHCP packets destined for the IC (not broadcast)
ipLocalDhcpSc	IP DHCP packets destined for the SC (broadcast and IC not enabled)
ipLocalFrag	IP fragments not classifiable
ipLocalIcmpEcho	IP ICMP echo request and reply
ipLocalIcmpFrag	IP ICMP packets that are not further classifiable (most likely large ping packets)
ipLocalIcmpOther	IP ICMP except echo request and reply
ipLocalL2tpControlIC	IP L2TP control packets for IC
ipLocalL2tpControlSC	IP L2TP control packets for SC
ipLocalLDP	IP LDP packets
ipLocalOspf	IP OSPF packets
ipLocalOther	IP Local packets not otherwise classified
ipLocalPim	IP PIM packets (except typeAssert)
ipLocalPimAssert	IP PIM assert type packets
ipLocalRsvp	IP RSVP packets
ipMld	IP Multicast listener packet
ipMulticastBroadcastOther	Ip Multicast/Broadcast not otherwise classified
ipMulticastCacheMiss	IP Multicast route table misses
ipMulticastCacheMissAutoRp	IP Multicast route table Auto-RP misses
ipMulticastControlIc	IP IGMP packets for the IC
ipMulticastControlSc	IP Multicast control packet not otherwise classified
ipMulticastDhcpSc	IP Multicast DHCP destined for SC
ipMulticastVrrp	IP VRRP packets
ipMulticastWrongIf	IP Multicast on wrong interface
ipNeighborDiscovery	IPv6 Neighbor Discovery

Table 56: IP-Related Protocols (continued)

CLI Name	Description of Flow
ipNeighborDiscoveryMiss	IPv6 Neighbor Discovery miss
ipNormalPathMtu	IP Path MTU request
ipOptionsOther	IP options not otherwise classified
ipOptionsRouterAlert	IP Router Alert
ipOsi	OSI packets
ipReassembly	IP packets that have been reassembled on a server card
ipRouteNoRoute	IP packets with no route indication
ipRouteToSrpEthernet	Packets routed to the SRP Ethernet
ipTtlExpired	IP TTL expired

DoS Protection Group Configuration Example

NOTE: To configure a DoS protection group for an interface, you must configure the settings under the default group, which is the only group that is currently supported.

To configure a DoS protection group for an interface:

```
host1(config)#dos-protection-group default
host1(config-dos-protection)#protocol AtmOam rate 512
host1(config-dos-protection)#protocol PppoeControl rate 512
host1(config-dos-protection)#protocol IpLocalOther rate 512
```

To display the configuration:

```
host1#show dos-protection-group default
           default (canned-group: defaultCanned)  *modified -- no references

      Protocol       Dest Mod Rate  Burst Weight DropProb Priority  Skip
-------------------- ---- --- ----- ----- ------ -------- --------- ----
Ppp Echo Request     IC     -  2048  1024    100      100 HI green  Y
Ppp Echo Reply       IC     -  2048  1024    100      100 HI green  Y
Ppp Echo Reply Fastp FC     -     0     0    100      100 Data path Y
path
Ppp Control          IC     -  2048  1024    100      100 HI green  N
Atm Control (ILMI)   IC     -  2048  1024    100      100 HI green  Y
Atm OAM              IC     *   512   512    100      100 LO green  N
Atm Dynamic Interfac IC     -  1024   512    100      100 HI yellow N
e Column Creation
Atm Inverse ARP      IC     -   256   128    100      100 LO yellow N
Frame Relay Control  IC     -  2048  1024    100      100 HI green  Y
(LMI)
Frame Relay Inverse  IC     -   256   128    100      100 LO yellow N
Arp
Pppoe Control        IC     *   512   512    100      100 HI yellow N
Pppoe Ppp Config Dyn IC     -  1024   512    100      100 HI yellow N
amic Interface Colum
n Creation
Ethernet ARP Miss    IC     -   256   128    100      100 LO yellow N
Ethernet ARP         IC     -   256   128    100      100 LO yellow N
```

DoS Protection Group Commands

Use the commands described in this section to create DoS protection groups and attach them to different types of interfacesatm dos-protection-group

- Use to attach an ATM DoS protection group to an interface.
- Example

  host1(config-if)#**atm dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

bridge1483 dos-protection-group

- Use to attach a bridge 1483 DoS protection group to an interface.
- Example

  host1(config-if)#**bridge1483 dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

dos-protection-group

- Use to create a DoS protection group and enter DoS Protection Group Configuration mode.
- A group named default always exists.
- Example

  host1(coonfig)#**dos-protection-group default**

- Use the **no** version to remove the DoS protection group.

ethernet dos-protection-group

- Use to attach an Ethernet DoS protection group to an interface.
- Example

  host1(config-if)#**ethernet dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

frame-relay dos-protection-group

- Use to attach a Frame Relay DoS protection group to an interface.
- Example

  host1(config-if)#**frame-relay dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

hdlc dos-protection-group

- Use to attach an HDLC DoS protection group to an interface.
- Example

  host1(config-if)#**hdlc dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ip dos-protection-group

- Use to attach an IP DoS protection group to an interface.
- Example 1

  host1(config-if)#**ip dos-protection-group group1**

- Example 2

  host1(config)#**dos-protection-group default**
  host1(config-dos-protection)#**protocol Atm0am rate 512**
  host1(config-dos-protection)#**protocol PppoeControl rate 512**
  host1(config-dos-protection)#**protocol IpLocalOther rate 512**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ipv6 dos-protection-group

- Use to attach an IPv6 DoS protection group to an interface.
- Example

  host1(config-if)#**ipv6 dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

lag dos-protection-group

- Use to attach a LAG DoS protection group to an interface.
- Example

  host1(config-if)#**lag dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ppp dos-protection-group

- Use to attach a PPP DoS protection group to an interface.
- Example

  host1(config-if)#**ppp dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

pppoe dos-protection-group

- Use to attach a PPPoE DoS protection group to an interface.
- Example

  host1(config-if)#**pppoe dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

priority burst

- Use to set the burst size in packets for the priority.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC burst 32**

- Use the **no** version to return to the default value.

priority over-subscription-factor

- Use to set the oversubscription value for the priority rate limiter.
- The oversubscription value and the priority rate are used to calculate the minimum rate limits for port compression.
- Allows an oversubscription of the priority rate because all protocols within a priority are not generally used simultaneously.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC over-subscription-factor 100**

- Use the **no** version to return no oversubscription value.

priority rate

- Use to set the rate in packets-per-second for the priority.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC rate 6000**

- Use the **no** version to return to the default value of 0.

protocol burst

- Use to set the burst size in packets-per-second for the protocol.
- The default value is one half the maximum rate in packets.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc burst 65535**

- Use the **no** version to set the default value, which is equal to half of the configured maximum rate.

protocol drop-probability

- Use to map a protocol to a specific drop probability, which is the percentage probability of an exceeded packet being dropped.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc drop-probability 100**

- Use the **no** version to set the drop probability to the value specified in the associated default group.

protocol priority

- Use to set the priority for the protocol.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc priority hiGreen**

- Use the **no** version to set the priority to the value specified in the associated default group.

protocol rate

- Use to map a protocol to a maximum rate limit.
- The rate limit applies to all packets of the protocol for interfaces belonging to the DoS protection group.
- A particular protocol can be up to the sum of the four rates configured, depending on the DoS group attached to an interface.
- Use a maximum rate of 0 for protocols that are not used.
- The actual rate never exceeds the maximum rate, but can be less than the configured maximum rate due to the weighting of the protocols within a DoS protection group and the use of multiple DoS protection groups.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc rate 100**

- Use the **no** version to set the value to the value specified in the associated default group.

protocol skip-priority-rate-limiter

- Use to set the skip priority rate limiter for the protocol.
- The specified protocol is not subject to the priority rate limiter for the priority and DoS protection group selected.
- The default sets the protocol such that it is subject to priority rate limiting.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc skip-priority-rate-limiter**

- Use the **no** version to set the value to the default, which is not to use skip-priority-rate-limiter.

protocol weight

- Use to set the weight for the protocol.
- For each port compression, weight determines the effective minimum rate that each protocol receives.
- Within each port compression, the sum of the minimum rates for all protocols is equal to or less than the priority rate.
- For each priority, there is a separate rate for each DoS protection group.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc weight 100**

- Use the **no** version to set the weight to the value specified in the associated default group.

use canned-group

- Use to create a DoS protection group that uses a pre-programmed set of parameters.
- Use the **revert** keyword to return the values to the canned group values
- Example

  host1#**use canned-group group1**

- Use the **no** version to associate the group with the default canned group settings.

vlan dos-protection-group

- Use to attach a VLAN DoS protection group to an interface.
- Example

  host1(config-if)#**vlan dos-protection-group**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

Monitoring DoS Protection Groups

Use the commands described in this section to monitor DoS protection groups.

show dos-protection-group

- Use to display DoS protection groups.
- If you do not specify a group, displays the names of the currently configured DoS protection groups.
- If you specify a group, displays information about the specified group.
- If you do not specify the **brief** keyword, displays a list of references (interfaces and templates) to the DoS protection group,
- When *modified* appears next to the name of the DoS protection group. the group or protocol within the group has changed from the preprogrammed value of the associated group.

- Example

```
host1(config)#show dos-protection-group
DOS Protection Groups:
        Default (canned-group: “default”)  *modified*
        Uplink  (canned-group: “link” }
        ATM     (canned-group: “pppoe” )   *modified*
        VLAN    (canned-group: “mixed-access”)
```