Chapter 11

Configuring CLI-Based Packet Mirroring

This chapter contains the following sections:

CLI-Based Packet Mirroring Overview

Packet mirroring enables you to send a copy of a packet to an external host for analysis. Packet mirroring has many uses, including traffic debugging and troubleshooting user networking problems.

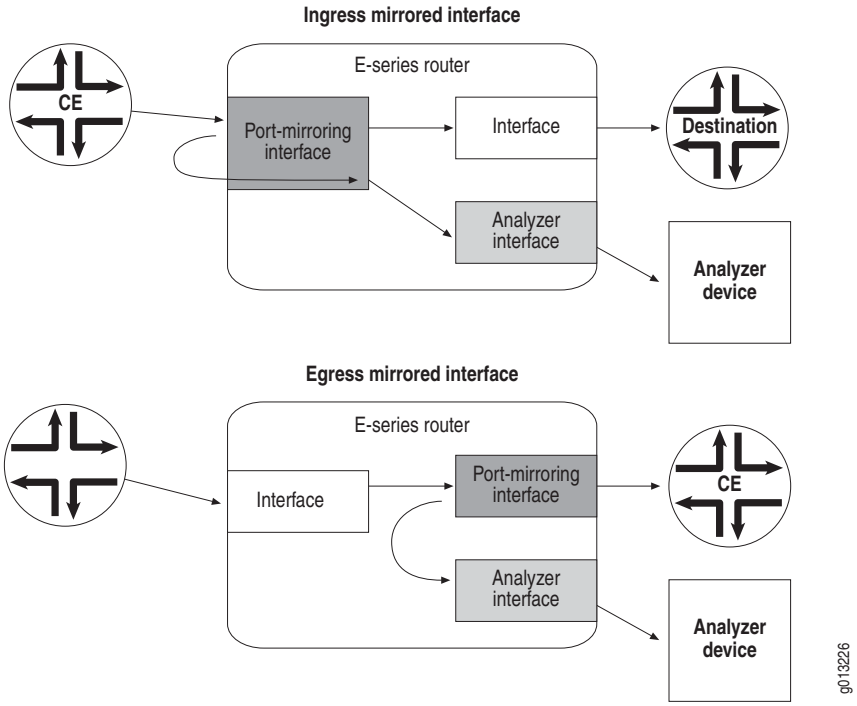
The JUNOSe software enables you to use CLI commands to configure and manage packet mirroring on specific static IP interfaces, or for a specific user. You use CLI commands to create a secure policy that specifies the analyzer device and how the mirrored traffic is treated.

When you mirror an interface, you can replicate ingress and egress traffic on the interface (traffic entering or exiting the E-series router through that interface). When you mirror a user, you can replicate all traffic to or from the user.

In both interface-specific and user-specific mirroring, the original traffic is forwarded to its intended destination as usual, while the replicated copy of the traffic is forwarded to an analyzer interface on the E-series router. The analyzer interface then directs the mirrored traffic to the specified analyzer device for analysis.

Figure 18 shows the traffic flow for ingress and egress IP interface mirroring.

Figure 18: CLI-Based Interface Mirroring



Enabling and Securing CLI-Based Packet Mirroring

The JUNOSe software enables you to create a secure environment for your packet mirroring operation by restricting access to the packet mirroring CLI commands and information. For example, when dealing with a critical diagnostic or troubleshooting procedure, you might want the packet mirroring feature to be available and visible to a subset of your network operations group. Or, if you are monitoring confidential traffic from a particular user, you might want the configuration and results of the mirroring operation to be available only to a unique group, such as the management group of the analyzer device.

By default, the packet mirroring configuration commands are hidden from all users. You must use the **mirror-enable** command to make the commands visible, which then enables you to configure the packet mirroring environment. The command applies only to the current CLI session. When you log off the current session and then log on again, the packet mirroring commands are no longer visible,

NOTE: The **no mirror-enable** command makes the packet mirroring commands no longer visible. However, any active mirroring sessions are unaffected and traffic continues to be mirrored.

To create a secure packet mirroring environment, you use a combination of the JUNOSe software authorization methods and the **mirror-enable** command. You configure the authorization method to control who can use the **mirror-enable** command. Authorized users can then issue the **mirror-enable** command, making the packet mirroring commands visible. However, the commands are still hidden from unauthorized users. Table 38 lists the commands whose visibility is controlled by the **mirror-enable** command.

Table 38: Commands Made Visible by the mirror-enable Command

■ ip policy { secure-input | secure-output }	■ show ip interface (packet mirroring information)
■ clear mirror log	■ show mirror log
■ mirror acct-session-id	■ show mirror rules
■ mirror analyzer-ip-address	■ show mirror trap
■ mirror calling-station-id	■ show mirror subscribers
■ mirror disable	■ show secure classifier-list
■ mirror ip-address	■ show secure policy-list
■ mirror nas-port-id	■ show snmp secure-log
■ mirror trap-enable	■ show snmp trap (packet mirroring information)
■ mirror username	■ snmp-server clear secure-log
■ secure ip classifier-list	■ snmp-server secure-log
■ secure ip policy-list	■ snmp-server enable traps (packetMirror keyword)
■ secure l2tp policy-list	■ snmp-server host (packetMirror keyword)

To provide increased security, the **mirror-enable** command must be the only command at its access level (level 12 by default) and it also must be at a different privilege level than the other packet mirroring commands (level 13 by default) and other regular JUNOSe CLI commands. This separation enables you to control authorization to the **mirror-enable** command and to limit the visibility of packet mirroring commands. For example, if you are using TACACS+, the **mirror-enable** command is the only packet mirroring command that is sent to the TACACS+ server. You can also use TACACS+ to prevent unauthorized individuals from modifying the configuration of analyzed ports.

The following two examples describe techniques you might use to enable and secure your CLI-based packet mirroring environment. Example 1 uses a combination of TACACS+ authorization and virtual terminal (vty) access lists to secure the packet mirroring environment. Example 2 uses only vty access lists.

See *JUNOSe System Basics Configuration Guide, Chapter 9, Passwords and Security* for more information about access levels. See *JUNOSe Broadband Access Configuration Guide, Chapter 8, Configuring TACACS+* for information about TACACS+ authorization.

Reloading a CLI-Based Packet Mirroring Configuration

You can reload your packet mirroring configuration as part of a configuration file (.cnf) reload operation or when you run a script file (.scr) that you have saved from the **show configuration** command display. When you reload a .cnf file, the packet mirroring configuration is restored—no additional steps are required.

For a .scr file operation, the **mirror-enable** command must be enabled—before saving the scr. file from the **show configuration** display, and also before you run the script to reload the packet mirroring configuration. If the **mirror-enable** command is not enabled, the .scr file operation for the packet mirroring configuration fails.

Using TACACS+ and Vty Access Lists to Secure Packet Mirroring

The following example describes a procedure that uses TACACS+ and vty access lists to manage the users who have access to the **mirror-enable** command. An authorized user who issues the **mirror-enable** command then gains access to the packet mirroring CLI commands and information.

This technique enables you to restrict the visibility and use of packet mirroring commands to a controlled, authorized group of users.

1. Configure TACACS+ authorization for the access level of the **mirror-enable** command (level 12 by default).

   Configure the router either to allow or disallow authorization when the TACACS+ servers are not available.

2. Configure all vty lines and the console to use the TACACS+ authorization configuration from Step 1 for access level 12 commands.

This procedure ensures that packet mirroring commands are never sent out of the E-series router—only the **mirror-enable** command is sent. The packet mirroring configuration and all information about mirrored interfaces and subscribers are available only to users who are authorized for the packet mirroring CLI commands on the router.

Using Vty Access Lists to Secure Packet Mirroring

In this example, TACACS+ authorization is not used. However, you can still use vty access lists to control access to the **mirror-enable** command, which enables you to create isolation between the authorized packet mirroring users and unauthorized network operators.

1. Configure TACACS+ authorization for the **mirror-enable** command privilege level. Specify that authorization is denied if TACACS+ is not available. Because TACACS+ is not being used, authorization always fails.

2. Configure the *majority* of the vty lines and the console to use the authorization configuration from Step 1. (Users who use Telnet on these lines are denied access to the **mirror-enable** command.)

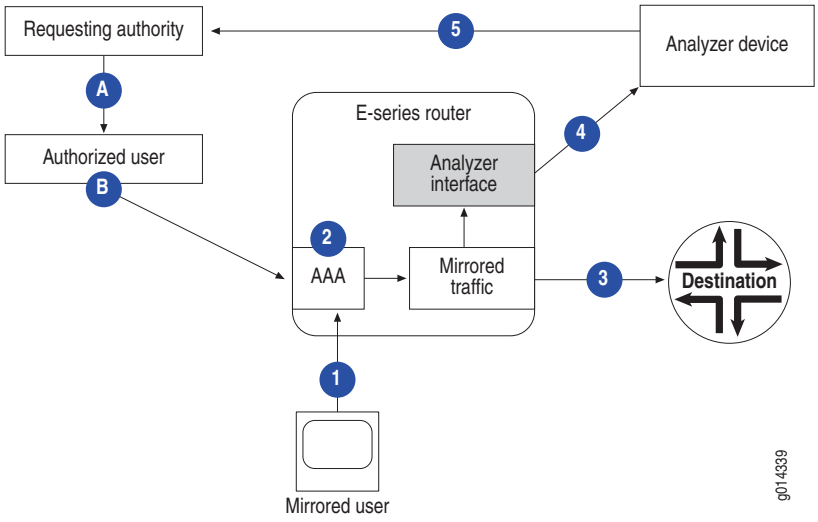
3. On the remaining vty lines (without the TACACS+ authorization) create an access list that contains the IP addresses of the users that you want to grant access to these vty lines—these users are granted access to the **mirror-enable** command, and therefore, the packet mirroring feature.

This configuration grants access to the packet mirroring CLI commands to the users from the specified IP addresses. The packet mirroring commands remain hidden for all other users.

CLI-Based Packet Mirroring Sequence of Events

Figure 19 shows the sequence of events that take place during CLI-based mirroring. The tables after the figure describe the events indicated by the numbers and letters in the figure. Table 39 on page 199 describes the configuration process; Table 40 on page 200 describes the flow of traffic during a mirroring operation that is initiated when the user logs on; and Table 41 on page 200 describes the flow of traffic when mirroring a user who is already logged in or when mirroring a static interface.

Figure 19: CLI-Based Packet Mirroring



To create a CLI-based packet mirroring environment, you must complete the processes listed in Table 39.

Table 39: Setting Up the CLI-Based Packet Mirroring Environment

Process	Description
A	The authorized individual requests packet mirroring of a user's or interface's traffic and configures the analyzer device to receive mirrored traffic.
B	An individual who is authorized to use the packet mirroring CLI commands configures the packet mirroring environment, including the secure policy, analyzer interface connection to the analyzer device, and the interface or trigger information.

Table 40 indicates the sequence of steps for a packet mirroring operation that takes place when a user starts a new session.

Table 40: CLI-Based User-Specific Mirroring During Session Start

Step	Description
1	The user logs on to an E-series router, requesting authentication by AAA.
2	AAA authenticates the user, and the router starts mirroring the user's traffic.
3	The router sends the user's original traffic to the intended destination.
4	The router sends the mirrored traffic to the analyzer device.
5	The analyzer device provides information to the requesting individual.

Table 41 indicates the sequence of steps for a packet mirroring operation that is configured for an interface or for a user who is already logged in.

Table 41: CLI-Based Mirroring of Currently Running Session

Step	Description
1	For user-specific mirroring, the user logs on to the E-series router; no mirroring action is configured.
2	■ CLI-based packet mirroring is configured and enabled on the router. ■ For interface-specific mirroring, the router starts mirroring all traffic for the interface. ■ For user-specific mirroring, AAA verifies that the mirrored user is already logged in, then starts mirroring all subsequent traffic to or from the user.
3	The router sends the original traffic to its intended destination.
4	The router sends mirrored traffic to the analyzer device.
5	The analyzer device provides information for the requesting individual.

Configuring CLI-Based Mirroring

To configure the CLI-based packet mirroring environment, you must coordinate the mirroring operations of two devices in the network: the E-series router and the analyzer device. The configuration of the analyzer device is mentioned in this section for reference only. The actual configuration procedures depend on the policies and guidelines established by the responsible organizations.

The **ip policy** command is visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. If you enter the **ip policy** command with the **secure-input** or **secure-output** keyword and the policy list does not exist, the router creates a policy list with a default mirror rule that disables mirroring. If you attach this policy list to an interface, there is no packet mirroring. When you use this command to create a secure policy list, statistics-related keywords are not supported.

The **secure ip classifier-list** command creates or modifies a secure IP classifier control list, which can then be included in a secure policy list.

NOTE: Do not use the asterisk (*) for the name of a classifier list. The asterisk is used as a wildcard for the **classifier-group** command.

Except for the following considerations, secure IP classifier lists are created and function the same as standard IP classifier lists—see the *Chapter 2, Creating Classifier Control Lists for Policies* for information:

- This command is visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command.
- Secure IP classifier lists are the only type of classifier lists allowed in secure policy lists
- Secure IP classifier lists cannot be used in non-secure policy lists.

The **secure ip policy-list** and **secure l2tp policy-list** commands create or modify a secure IP or L2TP policy list. These commands are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. These commands enter Policy List Configuration mode, enabling you to specify the parameters of the secure policy list. If you enter Policy List Configuration mode and then type **exit** without specifying any parameters, the router creates a policy list with a mirror disable rule. Attaching this policy list to an interface results in no packet mirroring. Secure IP classifier lists are the only type of classifier lists allowed in secure IP policy lists. Secure L2TP policies do not support classification. Therefore, the only classifier group you can use for secure L2TP policies is **classifier-group *****. You cannot delete a secure policy list that is currently attached to an interface.

Related Topics

- **classifier-group** command
- **ip analyzer** command
- **ip mirror** command
- **ip policy** command
- **mirror** command
- **mirror analyzer-ip-address** command
- **mirror disable** command
- **mirror-enable** command
- **secure ip classifier-list** command
- **secure ip policy-list** command
- **secure l2tp policy-list** command

Configuring the Analyzer Device

The analyzer device must be configured to receive the mirrored traffic from the E-series router's analyzer interface. You can use the **default** keyword to configure an interface as the virtual router's default analyzer interface; it is then used when an analyzer interface is not explicitly specified in the **ip mirror** command. You cannot configure multiaccess interfaces, such as IP over Ethernet, as default analyzer interfaces.

You can configure any type of IP interface on the E-series router as an analyzer interface, except for special interfaces such as SRP interfaces, null interfaces, and loopback interfaces. An interface cannot be both an analyzer interface and a mirrored interface at the same time. A single analyzer interface can serve multiple mirrored sessions.

The receive side of an analyzer interface is disabled; all traffic attempting to access the router through an analyzer interface is dropped. Analyzer interfaces drop all nonmirrored traffic.

Policies are not supported on analyzer interfaces. When you configure an analyzer interface, existing policies are disabled, and no new policies are accepted.

Configuring the E-series Router

To configure the router to support CLI-based packet mirroring:

1. Configure the analyzer interface, the route to the analyzer device, and any static ARP entries.
2. Allow authorized users to have access to the **mirror-enable** command. The users can then make the packet mirroring CLI commands visible and perform the following steps.
3. Configure the secure policy that forwards the mirrored traffic to the analyzer device.
4. (Optional) For increased security, create an IPSec tunnel between the analyzer interface and the analyzer device.
5. For interface-specific mirroring, attach the secure policy to the interface.
6. For user-specific mirroring, configure the trigger that identifies the user.

Configuring CLI-Based Interface-Specific Mirroring

This example shows the configuration of a CLI-based packet mirroring session for a particular static IP interface. The configuration results in all traffic through the interface being replicated and the replicated traffic then sent through an IPSec tunnel to the analyzer device.

1. Enable the visibility and use of the packet mirroring CLI commands.

   host1#**mirror-enable**

2. Configure the analyzer interface and a route to reach the analyzer device at 192.168.125.29.

NOTE: If the analyzer interface is Ethernet-based, you must configure a static ARP entry for the analyzer device.

```
host1(config)#virtual-router vr1
host1:vr1(config)#interface tunnel ipsec:Diag transport-virtual-router default
host1:vr1(config-if)#ip analyzer
host1:vr1(config-if)#exit
host1:vr1(config)#ip route 192.168.125.29 255.255.255.255 tunnel ipsec:Diag
```

3. Configure the secure IP policy that forwards the mirrored traffic to the analyzer device at 192.168.125.29.

   In this example, the configured mirror rule does not include the **analyzer-udp-port** keyword. Therefore, the rule sets the mirror header to **disable**, which means that the mirror header is not prepended to the mirrored packets. See *Understanding the Prepended Header During a Packet Mirroring Session* on page 216 for information about the prepended mirror header. The **classifier-group** command uses a previously configured classifier list, secClassA.

```
host1:vr1(config)#secure ip policy-list secureIpPolicy1
host1:vr1(config-policy-list)#classifier-group secClassA
host1:vr1(config-policy-list-classifier-group)#mirror analyzer-ip-address
192.168.125.29 analyzer-virtual-router vr1
```

4. Attach the secure policy to the interfaces whose traffic you want to mirror. This example mirrors input traffic at interface ATM 5/0.1 and output traffic at interface ATM 5/0.2.

```
host1:vr1(config)#interface atm 5/0.1
host1:vr1(config-if)#ip policy secure-input secureIpPolicy1
```

```
host1:vr1(config)#interface atm 5/0.2
host1:vr1(config-if)#ip policy secure-output secureIpPolicy1
```

5. Verify the secure policy configuration.

```
host1#show secure policy-list name secureIpPolicy1

                                Policy Table
                                ------ -----
Secure IP Policy secureIpPolicy1
 Administrative state: enable
 Reference count:      2
 Classifier control list: secClassA
  mirror analyzer-ip-address 192.168.125.29 analyzer-virtual-router vr1

 Referenced by interface(s):
  ATM5/0.1  secure-input policy, virtual-router vr1
  ATM5/0.2  secure-output policy, virtual-router vr1
```

Configuring CLI-Based User-Specific Mirroring

In user-specific packet mirroring, you use triggers to identify the user whose traffic you want to mirror and to start the mirroring session. The triggers are similar to the RADIUS attributes used in RADIUS-based mirroring. However, for CLI-based mirroring, AAA can use any supported authentication method, including RADIUS.

NOTE: An E-series router supports a maximum of 100 mirror trigger rules.

You can use the following triggers to identify users:

- Username (virtual router specific)
- IP address (virtual router specific)
- Calling station ID
- Account session ID

The following considerations apply to trigger rules:

- A new trigger rule is not applied to matching connected subscribers if any of the subscribers is mirrored by another rule.
- When you remove a rule, mirroring is terminated for all affected subscribers.
- CLI-initiated mirroring per account session ID creates a rule that continues to exist after the subscriber logs out.
- RADIUS CoA messages do not create rules and affect only currently connected subscribers.

This example shows the configuration of a CLI-based packet mirroring session for an L2TP user. The configuration uses the username as the trigger to identify the user and start the mirroring session. The mirroring session replicates all traffic associated with the user, and then sends the replicated traffic through an IPSec tunnel to the analyzer device.

1. Enable the visibility and use of the packet mirroring CLI commands.

   host1#**mirror-enable**

2. Create the analyzer interface and the route to the analyzer device at address 192.168.99.2.

   host1(config)# **interface tunnel ipsec:mirror3 transport-virtual-router default**
   host1(config-if)#**ip analyzer**
   host1(config-if)#**exit**
   host1(config)#**ip route 192.168.99.2 255.255.255.255 tunnel ipsec:mirror3**

3. Configure the secure L2TP policy that forwards the mirrored traffic to the analyzer device at 192.168.99.2, port 6500. The **classifier-group** command uses the default classifier list, which is indicated by the asterisk character (*****).

```
hosts1(config)#secure l2tp policy-list l2tp_toMirrorHQ
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#mirror analyzer-ip-address 192.168.99.2
analyzer-virtual-router default analyzer-udp-port 6500 mirror-identifier 1
session-identifier 1
```

4. Configure packet mirroring for the subscriber identified by username jwbooth@isptheatre.com and associate the secure policy with the user.

```
host1(config)#virtual-router lac
host1:lac(config)#mirror username jwbooth@isptheatre.com l2tp
secure-policy-list l2tp_toMirrorHQ
```

Now, when subscriber jwbooth@isptheatre.com logs in, the packet mirroring session starts and the subscriber's replicated traffic is sent through the secure IPSec tunnel to the remote analyzer device.

5. Verify the packet mirroring configuration.

```
host1#show mirror subscribers

Subscriber ID                Subscriber ID       Secure Policy  Secure Policy List  Sessions
                             Method              Type                               Mirrored
-----------------            ------------------  -------------  ------------------  --------
lac:jwbooth@isptheatre.com   username            l2tp           l2tp_toMirrorHQ     1
```

6. Verify the configuration of the secure L2TP policy.

```
host1#show secure policy-list name l2tp_toMirrorHQ

                                  Policy Table
                                  ------ -----
Secure L2TP Policy l2tp_toMirrorHQ
 Administrative state: enable
 Reference count:      2
 Classifier control list: *
  mirror analyzer-ip-address 192.168.99.2 analyzer-virtual-router default
analyzer-udp-port 6500 mirror-id 1 session-id 1

 Referenced by interface(s):
  TUNNEL l2tp:5/1/5  secure-input policy
  TUNNEL l2tp:5/1/5  secure-output policy
```