Chapter 10

Packet Mirroring Overview

This chapter contains the following sections:

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 provides two methods that you can use to configure and manage your packet mirroring environment—CLI-based and RADIUS-based.

- CLI-based packet mirroring—An authorized user uses the router's CLI commands to configure and manage packet mirroring. You can mirror traffic related to a specific IP or L2TP interface or traffic related to a particular user. You also use CLI commands to create secure policies that identify the traffic to be mirrored and specify how the mirrored traffic is treated.

- RADIUS-based packet mirroring—A RADIUS administrator uses RADIUS attributes to configure packet mirroring of a particular user's traffic. The router creates dynamic secure policies for the mirroring operation.

In both the CLI-based and the RADIUS-based packet mirroring methods, the original traffic is sent to its intended destination and the mirrored traffic is sent to an analyzer (the mediation device). The mirroring operations are transparent to the user whose traffic is being mirrored.

NOTE: Packet mirroring operations require some system resources. To avoid performance degradation, limit the amount of mirrored traffic to a maximum of 5 percent of the E-series router's total traffic.

Packet mirroring is supported on ASIC-based modules. See *ERX Module Guide*, *Appendix A*, *Module Protocol Support* for information about modules supported on ERX routers. See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about modules supported on the E120 and E320 routers.

Comparing CLI-Based Mirroring and RADIUS-Based Mirroring

This section compares the characteristics of CLI-based and RADIUS-based mirroring techniques. You can use CLI-based mirroring for both interface-specific and user-specific mirroring; RADIUS-based mirroring is used for user-specific mirroring. This section highlights differences in configuration, security, and application of the CLI-based and RADIUS-based mirroring methods.

Configuration

This section describes differences in the configuration processes for CLI-based and RADIUS-based mirroring:

- CLI-based packet mirroring—You use CLI commands to configure and manage packet mirroring of specific interfaces and users. For interface-specific mirroring, you enable the static configuration after the IP interface is created. The interface method mirrors only the traffic on the specific interface.

  In user-specific mirroring, authentication, authorization, and accounting (AAA) uses RADIUS attributes as triggers to identify the user whose traffic is to be mirrored. The mirroring session starts when the user logs on. If the user is already logged in, AAA immediately starts the mirroring session when you enable packet mirroring.

- RADIUS-based packet mirroring—This dynamic method uses RADIUS and vendor-specific attributes (VSAs), rather than CLI commands, to identify a user whose traffic is to be mirrored and to trigger the mirroring session. A RADIUS administrator configures and enables the mirroring separate from the user's session. You can use a single RADIUS server to provision packet mirroring operations on multiple E-series routers in a service provider's network.

  There are two variations of RADIUS-based packet mirroring. For both types, the mirroring feature is initiated without regard to the user location, router, interface, or type of traffic.

  - User-initiated mirroring—If the user is not currently logged in, the mirroring session starts when the user logs on and is authenticated by RADIUS.

  - RADIUS-initiated mirroring—If the user is already logged in, the JUNOSe RADIUS dynamic-request server uses RADIUS-initiated change-of-authorization (CoA) messages to immediately start the mirroring session when the packet mirroring is enabled.

NOTE: Packet mirroring is not supported on IPv6 interfaces.

Security

The following list highlights security features provided by CLI-based and RADIUS-based mirroring:

- CLI-based packet mirroring—All packet mirroring commands are hidden by default. You must execute the **mirror-enable** command to make the mirroring commands visible. You can optionally configure authorization methods to control access to the **mirror-enable** command, which makes the packet mirroring commands available only to authorized users. The **mirror-enable** command is in privilege level 12 by default and the mirroring commands are in privilege level 13 by default. You can change the privilege levels of these commands; however, we recommend that you always put the **mirror-enable** command at a different privilege level than the mirroring commands.

- RADIUS-based packet mirroring—Access to RADIUS-based mirroring functionality is unrestricted. However, the display of mirroring functionality is restricted to privilege level 13 users by default. In addition, the user must execute the **mirror-enable** command to make the packet mirroring-related **show** commands visible.

  RADIUS-based mirroring uses dynamically created secure policies based on certain RADIUS VSAs. You attach the secure policies to the interface used by the mirrored user. The packet mirroring VSAs that the RADIUS server sends to the E-Series router are MD5 salt-encrypted.

Application

The following list compares the different types of packet mirroring methods:

- CLI-based packet mirroring—Is useful when organizations want to provide separation between the typical network operations personnel and the mirroring operations personnel. For example, if security is essential, you might perform the entire packet-mirroring configuration on the mediation device, separate from the normal network operations role. This way, only the authorized personnel on the mediation device are aware of the mirroring operation. If this level of security is not required, the network operations personnel can perform the configuration and management on the router as usual.

  - CLI-based interface-specific mirroring—Can be useful in small networks with few E-series routers and in static environments where a user typically logs on to the same router through the same interface.
  - CLI-based user-specific mirroring—Is useful in B-RAS environments, in which users log in and log out frequently.

- RADIUS-based user-specific mirroring—Is triggered when needed, either user-initiated when the specified user logs on, or RADIUS-initiated when the user is already logged in. RADIUS-based mirroring also provides an excellent solution for B-RAS networks, for example to troubleshoot traffic problems related to mobile users.

CLI-based user-specific and RADIUS-based user-specific mirroring are also useful to mirror L2TP traffic at the L2TP access concentrator (LAC). If the L2TP network server (LNS) and the LAC belong to different service providers, mirroring at the LAC enables mirroring to take place close to the user's domain.

Packet Mirroring Terms

Table 37 defines terms used in this discussion of packet mirroring.

Table 37: Packet-Mirroring Terminology

Term	Meaning
Analyzer device	Device that receives the mirrored traffic from the E-series router. Also called the mediation device.
Analyzer interface	IP interface in analyzer mode on the E-series router that is used to direct mirrored traffic to the analyzer device.
CLI access class	Security level that grants access to specific CLI commands.
Mirrored interface	Statically or dynamically configured interface on which traffic is being mirrored.
Mirrored user	User whose traffic is being mirrored.
Requesting authority	Group that is authorized to request or conduct packet mirroring.
Salt encryption	Random string of data used to modify a password hash.
Secure policy	Policies created with a mirror action and that contain information about where to forward mirrored traffic.
Trigger	RADIUS attribute that identifies a user whose traffic is to be mirrored. Packet mirroring starts when a trigger is detected. An E-series router supports a maximum of 100 mirror trigger rules.

Packet Mirroring Platform Considerations

For information about modules that support packet mirroring on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support packet mirroring.

For detailed information about the modules that support packet mirroring on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that support packet mirroring.

Packet Mirroring References

For more information about RADIUS-based packet mirroring, consult the following resources:

- RFC 3576—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (July 2003)
- Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications, version PTSC-LAES-2006-084R6