Chapter 12

Configuring RADIUS-Based Mirroring

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.

This chapter contains the following sections:

RADIUS-Based Mirroring Overview

RADIUS-based packet mirroring enables you to mirror traffic related to a specific user, without regard to how often the user logs on or off, or which E-series router or interface the user uses. RADIUS-based mirroring is particularly appropriate for large networks, because you can use a single RADIUS server to provision mirroring on multiple E-series routers in a service provider's network. RADIUS-based mirroring is useful when debugging network problems related to mobile users, who do not always log on to a particular router.

You configure RADIUS-based mirroring independent of the actual mirroring session—you can configure the mirroring parameters at any time. RADIUS-based mirroring uses RADIUS and VSAs, rather than CLI commands, to specify the user whose traffic is to be mirrored. The VSAs specify attributes that are carried in Access-Accept messages and change-of-authorization messages from the RADIUS dynamic-request server to the E-series router.

NOTE: You cannot use RADIUS-initiated packet mirroring to mirror static interfaces, which might not be authenticated through RADIUS. To mirror static interfaces, you must use CLI-based mirroring.

NOTE: RADIUS-based packet mirroring is not supported on LAC L2TP sessions if the LAC uses domain maps to create tunnels or if authentication is disabled for both LAC and PPP termination.

RADIUS Attributes Used for Packet Mirroring

Table 42 lists the packet mirroring triggers. The triggers are RADIUS attributes that identify a user whose traffic is to be mirrored. A packet mirroring session starts when the router receives a RADIUS packet that contains mirroring attribute and then applies the mirroring configuration to the appropriate interface. For example, packet mirroring starts when a logon request occurs that contains a specified User-Name attribute.

The triggers also enable RADIUS-initiated mirroring to start when the user is already logged in.

Table 42: RADIUS Attributes Used as Packet Mirroring Triggers

Standard Number	Attribute Name
[1]	User-Name
[8]	Framed-IP-Address
[26-1]	Virtual-Router
[31]	Calling-Station-ID
[44]	Acct-Session-ID
[87]	Nas-Port-ID

You add the trigger to the RADIUS record of the user whose traffic will be mirrored. In addition, you must include the RADIUS VSAs listed in Table 43 in the mirrored user's RADIUS record.

NOTE: For IP mirroring, you must include both VSA 59 and 61 or neither. If you use only one of these two VSAs, the configuration fails.

Table 43: RADIUS-Based Mirroring Attributes

Standard Number	Attribute Name	Setting
[26-58]	LI-Action	0 = disable mirroring 1 = enable mirroring 2 = no action
[26-59]	Med-Dev-Handle	String (not null-terminated)
[26-60]	Med-IP-Address	IP address of analyzer device
[26-61]	Med-Port-Number	UDP port number of monitoring application in analyzer device

A Mirror-Action setting of 2 specifies that the router does not perform any packet mirroring–related configuration. This setting can provide additional security by confusing unauthorized users who attempt to access packet mirroring communication between the router and the RADIUS server.

RADIUS-Based Packet Mirroring Dynamically Created Secure Policies

RADIUS-based packet mirroring uses dynamically created secure policies, which are based on the RADIUS VSAs that an authorized RADIUS administrator creates. A policy is created when the packet mirroring action is initiated at the RADIUS server, and then applied to the interface that is dynamically created for the user. When the mirroring operation is disabled, the secure policy is deleted.

The E-series router creates a name for the dynamically created policies—the name consists of the string spl followed by a hexadecimal integer, such as spl_88000008. The name is displayed by the **show secure policy-list** command.

RADIUS-Based Packet Mirroring MLPPP Sessions

When you use RADIUS-based packet mirroring on MLPPP traffic, RADIUS authentication and authorization is performed on the individual links. The mirroring-related VSAs are returned with the RADIUS response. For user-initiated mirroring, which starts when the user logs on, a RADIUS response is returned for each successful authentication/authorization. For RADIUS-initiated mirroring of a user who is already logged in, a single RADIUS request is sent for each link.

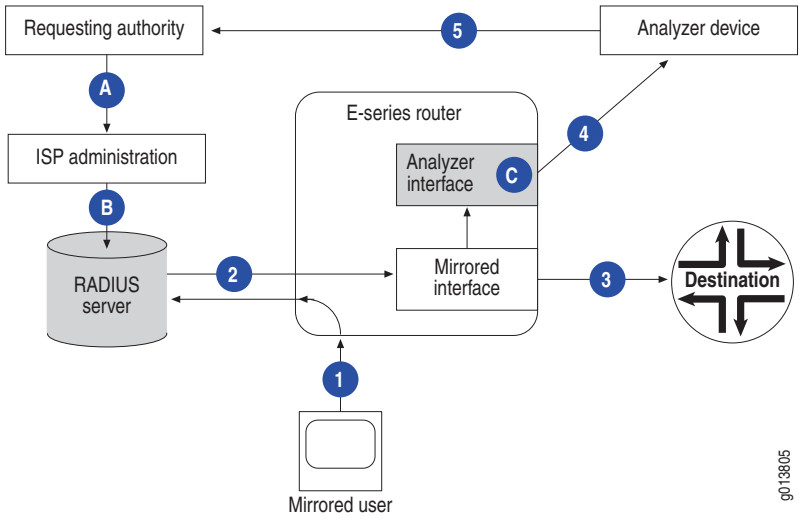
- If you are mirroring an L2TP session, the packet mirroring operation is enabled or disabled on a single link that is uniquely identified by the trigger you use (the RADIUS attributes for Acct-Session-ID or User-Name). For tunneled MLPPP, the individual links in the MLPPP bundle are mirrored separately. The packet mirroring configuration fails if you use the Acct-Multi-Session-ID attribute (RADIUS attribute 50) for the configuration.

- If you are mirroring an IP session, the packet mirroring operation is enabled or disabled on the MLPPP bundle as a whole. We recommend that you use the Account-Session-ID RADIUS attribute rather than the User-Name attribute as the trigger. Using the Account-Session-ID attribute is more efficient because the JUNOSe software creates one secure policy that packet mirroring uses for all links in the MLPPP bundle. If you use the User-Name attribute, a secure policy is created for the first link, then removed and re-created for every other link.

RADIUS-Based Mirroring Sequence of Events

Figure 20 on page 210 shows the sequence of events that take place during RADIUS-based mirroring. The tables after the figure describe the events indicated by the numbers and letters in the figure. Table 44 on page 210 describes the configuration process; Table 45 on page 211 describes the flow of traffic during a mirroring operation that is initiated when the user logs on; and Table 46 on page 211 describes the flow of traffic when mirroring a user who is already logged in.

Figure 20: RADIUS-Based Packet Mirroring



To create a RADIUS-based packet mirroring environment, you must complete the processes listed in Table 44.

Table 44: Setting Up the RADIUS-Based Packet Mirroring Environment

Process	Description
A	The authorized individual requests packet mirroring of the user's traffic and configures the analyzer device to receive mirrored traffic.
B	The ISP administration configures VSAs in the user's RADIUS record.
C	The E-series router administrator configures RADIUS server information and the analyzer interface connection to the analyzer device.

Table 45 indicates the sequence of steps for a packet mirroring operation that takes place when a user starts a new session.

Table 45: RADIUS-Based Mirroring During Session Start

Step	Description
1	The user logs on to an E-series router, requesting authentication by the RADIUS server. A trigger in the logon request starts the packet mirroring session.
2	■ The RADIUS server authenticates the user and sends packet mirroring VSAs and any other configured VSAs to the router. ■ The router creates a secure policy based on the VSAs and starts mirroring the user's traffic.
3	The router sends the user's original traffic to its intended destination.
4	The router sends the mirrored traffic to analyzer device.
5	The analyzer device provides information for the requesting individual.

Table 46 indicates the sequence of steps for a packet mirroring operation that is configured for a currently running session.

Table 46: RADIUS-Based Mirroring of Currently Running Session

Step	Description
1	The user logs on to the E-series router; no mirroring action is configured.
2	■ Packet mirroring is enabled on the RADIUS server. ■ The RADIUS server sends change-of-authorization messages containing packet mirroring VSAs to the router. ■ The router creates a secure policy based on the VSAs and starts mirroring the user's traffic.
3	The router sends the user's 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 RADIUS-Based Mirroring

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

Configuring the RADIUS Server

Table 43 on page 209 lists the VSAs that are included for both types of RADIUS-based mirroring—user-initiated (when the user logs on to start a new session), and RADIUS-initiated (when the user is already logged in).

Disabling RADIUS-Based Mirroring

To disable mirroring, you include the RADIUS attribute (for example, Acct-Session-ID) and set the Mirror-Action attribute to 0 in the mirrored user's RADIUS record.

You can also use the **mirror disable** CLI commands to disable RADIUS-based mirroring. You must use the version of the **mirror disable** command that corresponds to the RADIUS attribute that was used to identify the user. For example, if you used the RADIUS Calling-Station-ID attribute to create the mirroring session, you must use the **mirror disable calling-station-id** command to disable the session.

NOTE: All RADIUS-based mirroring sessions that start when a user logs on are considered to use the Acct-Session-ID attribute. Therefore, you must use the **mirror disable acct-session-id** command to disable these sessions. For RADIUS-based sessions of a user that is already logged in, you use the **mirror disable** command with the same keyword you used to configure the session.

Configuring the Analyzer Device

The analyzer device must be configured to receive the mirrored traffic from the E-series router's analyzer interface. The analyzer interface directs mirrored traffic to the specified analyzer device for analysis. You can configure the interface as the virtual router's default analyzer interface. You cannot configure multiaccess interfaces, such as IP over Ethernet, as default analyzer interfaces.

When mirroring an IP interface, the analyzer interface must reside in the same virtual router as the mirrored interface. When mirroring an L2TP interface, the analyzer interface must reside in the default virtual router.

NOTE: You must configure a static route to reach the analyzer device through the analyzer interface. If the analyzer interface is an IP over Ethernet interface, you must also configure a static Address Resolution Protocol (ARP) entry to reach the analyzer device.

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 support multiple mirrored interfaces.The receive side of the 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. When you configure an analyzer interface, existing policies are disabled, and no new policies are accepted.

Related Topics

- **authorization change** command
- **ip analyzer** command
- **key** command

- **mirror disable** command
- **radius dynamic-request server** command
- **udp-port** command

Configuring Router to Start Mirroring When User Logs On

To configure the router to support RADIUS-based mirroring that starts when the user logs on:

1. Configure RADIUS server authentication information in the router. See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access* for information.
2. Ensure that the analyzer interface is configured to send the mirrored traffic to the analyzer device.
3. (Optional) For increased security, create an IPSec tunnel between the analyzer interface and the analyzer device.

Configuring Router to Mirror Users Already Logged On

To configure the router to support RADIUS-initiated mirroring when the user is already logged in:

1. Specify the RADIUS server that sends change-of-authorization messages to the router.
2. Specify the UDP port used to communicate with the RADIUS server.
3. Configure the key used when communicating with the RADIUS server.
4. Enable the router to receive change-of-authorization messages from the RADIUS server.
5. Ensure that the analyzer interface is configured to send the mirrored traffic to the analyzer device.
6. (Optional) For increased security, create an IPSec tunnel between the analyzer interface and the analyzer device.

Configuring RADIUS-Initiated Mirroring When Users Are Logged On

When a mirroring operation is initiated for a user who is already logged on, the RADIUS server uses change-of-authorization messages and passes the required RADIUS attributes and the identifier of the currently running session to the E-series router. The router uses this information to create the secure policy and attaches it to the interface that is created for the user. The E-series router must be configured to accept change-of-authorization messages from the RADIUS server.

1. Specify the RADIUS dynamic-request server, and enter RADIUS configuration mode.

   host1(config)#**radius dynamic-request server 192.168.11.0**

2. Specify the UDP port used to communicate with the RADIUS server.

   host1(config-radius)#**udp-port 3799**

3. Create the key used to communicate with the RADIUS server.

   host1(config-radius)#**key mysecret**

4. Configure the router to receive change-of-authorization messages from the RADIUS server.

   host1(config-radius)#**authorization change**
   host1(config-radius)#**exit**
   host1(config)#**exit**

5. Verify your RADIUS-initiated mirroring configuration.

```
host1#show radius dynamic-request servers

               RADIUS Request Configuration
               ----------------------------
                                        Change
                Udp                       Of
 IP Address     Port   Disconnect   Authorization   Secret
-------------   ----   ----------   -------------   ------
 10.10.3.4      3799   enabled      enabled         mysecret
```

6. Create the analyzer interface.

   host1(config)#**interface fastEthernet 4/0**
   host1(config-if)#**ip analyzer**