

Using SNMP Secure Packet Mirroring Traps

SNMP secure packet mirroring traps enable you to capture and report packet mirroring information to an external device; you can then view the secure information on the remote device. The secure packet mirroring traps feature is an extension of the router's standard SNMP implementation, and is only available to SNMPv3 users who are authorized to use packet mirroring.

You can also log mirror traps to local volatile memory for debugging purposes by enabling the SNMP secure log feature. See Capturing SNMP Secure Audit Logs for details of secure audit logging. Normal console and syslog audit logs for packet mirroring traps and packet Mirror-MIB accesses are suppressed due to security concerns.



NOTE: The contents of secure logs are not preserved across a reboot.

The **mirror-enable** command must be enabled to make packet mirroring-related commands, command options, and **show** command output visible.



NOTE: You must use the CLI to configure the secure packet mirroring trap category to allow transmission of secure packet mirroring traps through the router—you cannot use SNMP to configure the secure packet mirroring trap category. However, after you have configured the secure packet mirroring trap category using the CLI, you can then use SNMP (juniPacketMirrorMIB.mi2) to enable and disable secure packet mirroring traps.

Table 1 on page 1 indicates the events that trigger secure packet-mirroring traps and lists the information sent in the trap for each event.

Table 1: Packet-Mirroring SNMP Traps

Trap Information Sent	Event That Triggers the Trap			
	A secure policy failed during CoA-based or RADIUS-initiated packet mirroring	A secure policy failed during CLI trigger or CLI-based packet mirroring	An interface with secure policies attached is deleted	An analyzer is unreachable
Analyzer address	–	–	–	✓
Application name	✓	✓	–	–
Configuration source	✓	✓	✓	–
Date and time of event	–	✓	✓	✓
Error cause	✓	✓	–	–

Table 1: Packet-Mirroring SNMP Traps *(continued)*

Trap Information Sent	Event That Triggers the Trap			
	A secure policy failed during CoA-based or RADIUS-initiated packet mirroring	A secure policy failed during CLI trigger or CLI-based packet mirroring	An interface with secure policies attached is deleted	An analyzer is unreachable
Error string	✓	✓	–	–
Mirror ID	✓	–	✓	–
Mirroring direction	–	–	✓	–
Secure policy name	–	✓	✓	–
Secure policy UID	–	✓	✓	–
Session ID	✓	–	✓	–
Trigger event	✓	✓	✓	–
Trigger type	✓	✓	✓	–
Username	✓	–	–	–
Virtual router (0 for L2TP)	✓	✓	✓	✓

Additional Packet-Mirroring Traps for CALEA Compliance

You can use the packet-mirroring traps shown in Table 2 on page 2 to help support compliance with the Communications Assistance for Law Enforcement Act (CALEA), which defines electronic surveillance guidelines for telecommunications companies. For example, a third-party vendor of mediation devices might receive packet mirroring traps from the router and convert the traps to messages that comply with CALEA, such as Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard For Telecommunications messages. Individual traps might map to multiple LAES messages to provide additional compliance-related information.

Table 2: Packet-Mirroring Traps for CALEA Compliance

Trap	Description
juniPacketMirrorSessionStart	A grant has been issued to a mirrored subscriber.
juniPacketMirrorSessionEnd	A mirrored session has been terminated; includes the termination reason.
juniPacketMirrorInterfaceSessionActivated	A secure policy has been attached to an existing interface or to an existing session.

Table 2: Packet-Mirroring Traps for CALEA Compliance (continued)

Trap	Description
juniPacketMirrorInterfaceSessionDeactivated	A secure policy has been detached from an interface, not including interface or session termination.
juniPacketMirrorSessionReject	A deny has been issued because the potential mirrored user was not allowed on the network for some reason. However, the user would have been mirrored if access to the network had been allowed.
juniPacketMirrorSessionFailed	The user session was terminated before the secure policy was attached. For example, no resources were available to create the interface. The termination reason is included.

Packet Mirroring Trap Severity Levels

Table 3 on page 3 lists the default severity levels for packet mirroring traps. See the *JUNOS System Basics Configuration Guide* for descriptions of the severity levels.

Table 3: Packet Mirroring Trap Severity Levels

Trap	Default Severity Level
juniPacketMirrorAnalyzerUnreachable	Warning
juniPacketMirrorCliTriggerBasedMirroringFailure	Error
juniPacketMirrorInterfaceDeleted	Notice
juniPacketMirrorInterfaceSessionActivated	Info
juniPacketMirrorInterfaceSessionDeactivated	Info
juniPacketMirrorRadiusBasedMirroringFailure	Error
juniPacketMirrorSessionEnd	Info
juniPacketMirrorSessionFailed	Info
juniPacketMirrorSessionStart	Info
juniPacketMirrorSessionReject	Info

- Related Topics**
- See Configuring SNMP in *JUNOS System Basics Configuration Guide* for information about JUNOS software SNMP support.
 - Configuring SNMP Secure Packet Mirroring Traps
 - mirror trap-enable
 - snmp-server clear secure-log

- snmp-server enable traps
- snmp-server host
- snmp-server secure-log
- show mirror trap
- show snmp secure-log