Chapter 14

Monitoring Packet Mirroring

This chapter contains the following topics:

Monitoring 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.

This topic describes the commands you can use to view your CLI-based and RADIUS-based packet mirroring environments.

Use the **baseline radius dynamic-request** command in RADIUS-based packet mirroring to set a statistics baseline for packet mirroring–related RADIUS statistics. The E-series router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics. Use the **delta** keyword with the **show radius statistics** command to show baselined statistics.

Related Topics

- **baseline radius dynamic-request** command
- **clear mirror log** command

Monitoring CLI-Based Packet Mirroring

Purpose Display brief or default (normal) information about your CLI-based packet mirroring environment, including interface analyzer information. To display secure packet mirroring information you must enable the **mirror-enable** command prior to using this command. This command displays a maximum of two secure policy attachments and statistics, if configured.

Action To display the default (normal) format for a specific interface, which is used as the default analyzer interface:

```
host1#show ip interface atm 5/0.1
ATM5/0.1 line protocol Atm1483 is up, ip is analyzer (default)
  Network Protocols: IP
  Internet address is 10.10.3.4/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
  Discontinuity Time = 0
  Router advertisement = disabled
  Proxy Arp = disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
  Access routing = disabled
  Multipath mode = hashed

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0
```

To display the format for a specific interface, showing secure policy attachments:

```
host1#show ip interface atm 4/1.1
ATM5/0.1 line protocol Atm1483 is up
  Network Protocols: IP
  Internet address is 10.10.7.14/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
  Discontinuity Time = 0
  Router advertisement = disabled
  Proxy Arp = disabled
  Administrative debounce-time = disabled
```

```
Operational debounce-time    = disabled
Access routing = disabled
Multipath mode = hashed

In Received Packets 0, Bytes 0
  Unicast Packets 0, Bytes 0
  Multicast Packets 0, Bytes 0
In Policed Packets 0, Bytes 0
In Error Packets 0
In Invalid Source Address Packets 0
In Discarded Packets 0
Out Forwarded Packets 0, Bytes 0
  Unicast Packets 0, Bytes 0
  Multicast Routed Packets 0, Bytes 0
Out Scheduler Dropped Packets 0, Bytes 0
Out Policed Packets 0, Bytes 0
Out Discarded Packets 0

IP policy secure-input ipSecureIn
  classifier-group secClassA entry 1
    0 packets, 0 bytes
    mirror analyzer-ip-address 10.10.3.14, analyzer-virtual-router default
  classifier-group secClassB entry 2
    0 packets, 0 bytes
    mirror analyzer-ip-address 10.10.3.14, analyzer-virtual-router vr200
IP policy secure-output ipSecureOut
  classifier-group secClassC entry 1
    0 packets, 0 bytes
    mirror analyzer-ip-address 10.10.7.104, analyzer-virtual-router vr300
```

Meaning Table 51 lists the secure packet mirroring-related fields.

Table 51: show ip interface Output Fields

Field Name	Field Description
IP Policy	Type (secure-input, secure-output) and name of the secure policy
classifier-group	Name of a CLACL attached to the interface and number of entry
packets	Number of packets classified by the CLACL
bytes	Number of bytes classified by the CLACL
mirror analyzer-ip-address	IP address of analyzer device
analyzer-virtual-router	Name of analyzer interface virtual router

Related Topics

- **show ip interface** command

Monitoring the Packet Mirroring Configuration of IP Interfaces

Purpose Display CLI-based packet mirroring configuration information for a specific interface or for all interfaces on which mirroring is enabled.

NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show secure policy-list** command.

Action To display information about a specific interface or for all interfaces:

```
host1#show ip mirror interface atm 5/0.1

    Interface          Analyzer Port      Analyzer next-hop
------------------- ------------------- ---------------------
ATM5/0.1            FastEthernet3/0       192.168.1.1
```

Meaning Table 52 lists the **show ip mirror interface** command output fields.

Table 52: show ip mirror interface Output Fields

Field Name	Field Description
Interface	Interface being mirrored
Analyzer Port	Interface to which the mirrored traffic is sent, and that then sends the traffic to the analyzer device
Analyzer next-hop	IP address of the next hop to the analyzer device; displayed when the analyzer interface is a shared medium

Related Topics

- **show ip mirror interface** command

Monitoring Failure Messages for Secure Policies

Purpose Display failure messages and information for secure policies. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. All normal E-series system log messages are suppressed for packet mirroring-related policy operations.

Action To display information for secure policies:

```
host1#show mirror log

   Time       Mirror-ID      Session-ID   User          Error Status
----------- ---------------- ---------- ---------- ----------------------
TUE FEB 03  8976             1923       suresh@aol no secure polic
2004 18:35                              .com       ies available
:43 UTC

TUE FEB 03  8976             1924       219040@aol out of memory
2004 18:35                              .com
:39 UTC
```

```
TUE FEB 03  8976            1924       not applic analyzer 1.1.1.1 is unr
:30 UTC                                able       eachble in virtual rou
                                                  ter default
```

Meaning Table 53 lists the **show mirror log** command output fields.

Table 53: show mirror log Output Fields

Field Name	Field Description
Time	Day, date, and time of failure
Mirror-ID	Unique identifier of the mirrored session
Session-ID	Unique identifier of the user session
User	User login name
Error Status	Description of error condition

Related Topics

- **show mirror log** command

Monitoring Packet Mirroring Triggers

Purpose Display CLI-based packet mirroring information about all packet mirroring triggers (active and inactive) that are configured on the router. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command.

Action To display information about all packet mirroring triggers:

```
host1#show mirror rules

Total Mirror Rules Configured: 6

Subscriber ID                 Subscriber ID       Secure Policy  Secure Policy List  Sessions
                              Method              Type                               Mirrored
-------------------           ------------------  -------------  ------------------  --------
default: user@isp250.com      username            ip             securePolicyIp      4
vpn: fred@isp100.com          username            ip             securePolicyVpn     0
default: 192.168.10.1         ip address          ip             securePolicyIp      1
vpn: 10.10.2.2                ip address          l2tp           securePolicyVpn     0
5551212                       calling station id  l2tp           securePolicyL2tp    1
erx atm 2/1.2:0.42:0001048579 acct-session-id     ip             securePolicyIp      1
```

Meaning Table 54 lists **show mirror rules** command output fields.

Table 54: show mirror rules Output Fields

Field Name	Field Description
Subscriber ID	Identification of the subscriber
Subscriber ID Method	Method used to identify the subscriber
Secure Policy Type	Type of secure policy; IP or L2TP
Secure Policy List	Name of secure policy list used for packet mirroring
Sessions Mirrored	Number of sessions currently being mirrored

Related Topics

- **show mirror rules** command

Monitoring Packet Mirroring Subscriber Information

Purpose Display CLI-based packet mirroring information about the subscribers for whom packet mirroring is currently active. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command.

Action To display information about subscribers for whom packet mirroring is active:

```
host1#show mirror subscribers

Subscriber ID                Subscriber ID       Secure Policy  Secure Policy List  Sessions
                             Method              Type                               Mirrored
-----------------            ------------------  -------------  ------------------  --------
vpn: fred@isp100.com         username            l2tp           securePolicyL2tp    1
5551212                      calling station id  ip             securePolicyVpn     1
```

Meaning Table 55 lists **show mirror subscribers** command output fields.

Table 55: show mirror subscribers Output Fields

Field Name	Field Description
Subscriber ID	Subscriber being mirrored
Subscriber ID Method	Method used to identify the subscriber
Secure Policy Type	Type of secure policy; IP or L2TP
Secure Policy List	Name of secure policy list used for packet mirroring
Sessions Mirrored	Number of sessions being mirrored

Related Topics

- **show mirror subscribers** command

Monitoring RADIUS Dynamic-Request Server Information

Purpose Display RADIUS dynamic-request server configuration information and statistics.

Action To display RADIUS dynamic-request server configuration information:

```
host1#show radius dynamic-request servers

                RADIUS Request Configuration
                ----------------------------
                                          Change
                 Udp                        Of
 IP Address      Port   Disconnect   Authorization   Secret
-------------    ----   ----------   -------------   ------
192.168.2.3      1700   disabled     disabled        <NULL>
10.10.120.104    1700   disabled     disabled        mysecret

host1#show radius dynamic-request statistics
```

```
        RADIUS Request Statistics
        -------------------------
           Statistic              10.10.3.4
-----------------------------     -------
UDP Port                          1700
Disconnect Requests               0
Disconnect Accepts                0
Disconnect Rejects                0
Disconnect No Session ID          0
Disconnect Bad Authenticators     0
Disconnect Packets Dropped        0
CoA Requests                      0
CoA Accepts                       0
CoA Rejects                       0
CoA No Session ID                 0
CoA Bad Authenticators            0
CoA Packets Dropped               0
No Secret                         0
Unknown Request                   0

Invalid Addresses Received  :0
```

Meaning Table 56 lists **show rsdius dynamic-request statistics** command output fields.

Table 56: show radius dynamic-request statistics Output Fields

Field Name	Field Description
IP Address	IP address of the RADIUS server
Udp Port	Port on which the router listens for RADIUS server
Disconnect	Status of RADIUS-initiated disconnect feature, enabled or disabled
Change of Authorization	Status of change of authorization feature, enabled or disabled
Secret	Secret (key) used to connect to RADIUS server
Disconnect or CoA Requests	Number of RADIUS-initiated disconnect or CoA requests received
Disconnect or CoA Accepts	Number of RADIUS-initiated disconnect or CoA requests accepted
Disconnect or CoA Rejects	Number of RADIUS-initiated disconnect or CoA requests rejected
Disconnect or CoA No Session ID	Number of RADIUS-initiated disconnect or CoA messages rejected because the request did not include a session ID attribute
Disconnect or CoA Bad Authenticators	Number of RADIUS-initiated disconnect or CoA messages rejected because the calculated authenticator in the authenticator field of the request did not match
Disconnect or CoA Packets Dropped	Number of RADIUS-initiated disconnect or CoA packets dropped because of queue overflow
No Secret	Number of messages rejected because a secret was not present in the authenticator field
Unknown Request	Number of packets received with an invalid RADIUS code for RADIUS disconnect or change of authorization
Invalid Addresses Received	Number of invalid addresses received

Related Topics

- **show radius servers** command
- **show radius statistics** command

Monitoring Secure CLACL Configurations

Purpose Display information about only secure CLACL configurations. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. Use the **brief** or **detail** keywords with the **show secure classifier-list** command to display different levels of information.

Action To display a list of secure CLACLs

```
host1#show secure classifier-list

                        Classifier Control List Table
                        ---------- ------- ---- -----
Secure IP secClassA.1 ip any any
Secure IP secClassB.1 ip any not 10.10.10.1 255.255.255.255
Secure IP secClass25.1 user-packet-class 8 source-route-class 100 ip
192.168.44.103 255.255.255.255 any
```

Displays details of each secure CLACL

```
host1#show secure classifier-list secClass25 detailed

                        Classifier Control List Table
                        ---------- ------- ---- -----
Secure IP Classifier Control List secClass25
   Reference count:      0
   Entry count:          1

   Classifier-List secClass25 Entry 1
      User Packet Class:          8
      Source Route Class:         100
      Protocol:                   ip
      Not Protocol:               false
      Source IP Address:          192.168.44.103
      Source IP WildcardMask:     255.255.255.255
      Not Source Ip Address:      false
      Destination IP Address:     0.0.0.0
      Destination IP WildcardMask:255.255.255.255
      Not Destination Ip Address: false
```

Meaning Table 57 lists **show secure classifier-list** command output fields.

Table 57: show secure classifier-list Output Fields

Field Name	Field Description
Reference count	Number of times the CLACL is referenced by policies
Entry count	Number of entries in the classifier list
Classifier-List	Name of the classifier list
Entry	Entry number of the classifier list rule
Color	Packet color to match: green, yellow, or red

Table 57: show secure classifier-list Output Fields (continued)

Field Name	Field Description
Protocol	Protocol type
Not Protocol	If true, matches any protocol except the preceding protocol; if false, matches the preceding protocol
Source IP Address	Address of the network or host from which the packet is sent
Source IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set
Not Source Ip Address	If true, matches any source IP address and mask except the preceding source IP address and mask; if false, matches the preceding source IP address and mask
Destination IP Address	Number of the network or host from which the packet is sent
Destination IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set
Not Destination Ip Address	If true, matches any destination IP address and mask except the preceding destination IP address and mask; if false, matches the preceding destination IP address and mask
Traffic Class	Name of the traffic class to match
User Packet Class	User packet value to match
DS Field	DS field value to match
TOS Byte	ToS value to match
Precedence	Precedence value to match
User Priority bits	User priority bits value to match
Traffic Class Field	Traffic class field value to match
EXP Bits	MPLS EXP bit value to match
EXP Mask	Mask applied to EXP bits before matching
DE Bit	Frame Relay DE bit value to match
Destination Route Class	Route class used to classify packets based on the packet's destination address
Source Route Class	Route class used to classify packets based on the packet's source address
Local	If true, matches packets destined to a local interface; if false, matches packets that are traversing the router

Related Topics

- **show secure classifier-list** command

Monitoring Secure Policy Lists

Purpose Display information about only secure policy lists. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. Use the **name** keyword to display information for a specific secure policy list.

Action To display information about secure policy lists:

```
host1#show secure policy-list

                                  Policy Table
                                  ------ -----
Secure IP Policy secureIpPolicy
   Administrative state: enable
   Reference count:      2
   Classifier control list: secClassA
      mirror analyzer-ip-address 192.168.1.1 analyzer-virtual-router default
analyzer-udp-port 3000 mirror-id 6789 session-id 6543

   Referenced by interface(s):
      ATM5/0.1  secure-input policy, statistics disabled, virtual-router
default
      ATM5/0.1  secure-output policy, statistics disabled, virtual-router
default

L2TP Secure Policy secureL2tpPolicy
   Administrative state: enable
   Reference count:      2
   Classifier control list: *
      mirror analyzer-ip-address 192.168.2.1 analyzer-virtual-router default
analyzer-udp-port 3000 mirror-id 6789 session-id 6543 (unreachable)

   Referenced by interface(s):
      TUNNEL l2tp:1/msn.pwh.com/1  secure-input policy, statistics disabled
      TUNNEL l2tp:1/msn.pwh.com/1  secure-output policy, statistics disabled
```

Meaning Table 58 lists **show secure policy-list** command output fields.

Table 58: show secure policy-list Output Fields

Field Name	Field Description
Policy	Type (IP or L2TP) and name of the policy list
Administrative state	Status of administrative state, enable or disable; set to enable when the policy list is created
Reference count	Number of attachments to interfaces or profiles
Classifier control list	Name of the classifier control list
Mirror analyzer-ip-address	IP address of analyzer device
Analyzer-virtual-router	Analyzer interface virtual router
Analyzer-udp-port	UDP port used to communicate with analyzer device
Mirror-id	Unique identifier of the mirrored session
Session-id	Unique identifier of the user session

Table 58: show secure policy-list Output Fields (continued)

Field Name	Field Description
Referenced by interface(s)	List of interfaces to which the policy is attached; indicates whether the attachment is at secure input or secure output of interface
Referenced by profile(s)	Not currently supported: always null
Statistics	Not currently supported: always disabled

Related Topics

- **show secure policy-list** command

Monitoring Information for Secure Policies

Purpose Display failure messages and information for secure policies. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled prior to using this command. All normal E-series system log messages are suppressed for packet mirroring-related policy operations.

Action To display information for secure policies:

```
host1#show mirror log

  Time              Mirror-ID      Session-ID   User           Error Status
-----------        ---------------- ---------- --------------  --------------
TUE FEB 03         8976             1923       suresh@aol.com  no secure policies available
2005 18:35:43 UTC

TUE FEB 03         8976             1924       219040@aol.com  out of memory
2005 18:35:39 UTC

TUE FEB 03         8976             1924       not applicable  analyzer unreachable
2005 18:35:30 UTC
```

Meaning

- Table 59 lists the **show mirror log** command output fields.

Table 59: show mirror log Output Fields

Field Name	Field Description
Time	Day, date, and time of failure
Mirror-ID	Unique identifier of the mirrored session
Session-ID	Unique identifier of the user session
User	User login name
Error Status	Description of the error condition

Related Topics

- **clear mirror log** command
- **show mirror log** command

Monitoring SNMP Secure Packet Mirroring Traps

Purpose Display configuration information about SNMP traps and trap destinations. The PacketMirror trap category is displayed only when the **mirror enable** command has been configured. The Secure Trap Logging status is displayed only when the **mirror enable** command has been issued and secure audit logs have been configured.Text in bold indicates secure packet mirroring trap configuration information.

Action To display secure packet mirroring traps:

```
host1#show snmp trap

Enabled Categories: CliSecurity, PacketMirror, Sonet
SNMP authentication failure trap is disabled
Trap Source: FastEthernet 6/0, Trap Source Address:192.168.120.78
Trap Proxy: enabled
Secure Trap Logging is enabled

Global Trap Severity Level: 6 - informational

Address          Security String                  Ver  Port   Trap Categories
---------------  -------------------------------  ---  -----  ----------------
10.1.1.1         host1                            v1     162  Cli
10.12.12.12      secureHost                       v3     162  CliOspfPacketMirrorSonet
192.168.57.162   host2                            v3     162  Sonet


Address         TrapSeverityFilter  Ping    Maximum    Queue    Queue Full
                                    TimeOut QueueSize DrainRate discrd methd
--------------- ------------------- ------- --------- --------- -------------
10.1.1.1        5 - notice          1       32        0         dropLastIn
10.12.12.12     2 - critical        1       32        0         dropLastIn
192.168.57.162  2 - critical        1       32        0         dropLastIn
```

Meaning Table 60 lists the **show snmp trap** command output fields.

Table 60: show snmp trap Output Fields

Field Name	Field Description
Enabled Categories	Trap categories that are enabled on the router
SNMP authentication failure trap	Enabled or disabled
Trap Source	Interface whose IP address is used as the source address for all SNMP traps
Trap Source Address	IP address used as the source address for all SNMP traps
Trap Proxy	Enabled or disabled
Secure Trap Logging	Enabled or disabled
Global Trap Severity Level	Global severity level filter; if a trap does not meet this severity level, it is discarded
Address	IP address of the trap recipient
Security String	Name of the SNMP community
Ver	SNMP version (v1 or v2) of the SNMP trap packet
Port	UDP port on which the trap recipient accepts traps

Table 60: show snmp trap Output Fields (continued)

Field Name	Field Description
Trap Categories	Types of traps that the trap recipient can receive
TrapSeverityFilter	Severity level filter for this SNMP host
Ping TimeOut	Configured ping timeout in minutes
Maximum QueueSize	Maximum number of traps to be kept in the trap queue
Queue DrainRate	Maximum number of traps per second to be sent to the host
Queue Full discrd methd	Method used to discard traps when the queue is full:
dropFirstIn	Oldest trap in the queue is dropped
dropLastIn	Most recent trap is dropped

Related Topics

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

NOTE: Secure packet mirroring trap configuration information appears in the Enabled Categories and Trap Categories fields only if the **mirror-enable** command is enabled.

Monitoring SNMP Secure Audit Logs

Purpose Display output when the secure audit log data is available.

Action To display the contents of the SNMP secure audit log:

```
host1#show snmp secure-log

Agent's Context    LogData
---------------    ------------------------------------------------------------
SnmpRouterAgent1   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=3, errSts=0, errIndx=0, msgID=2, msgMaxSize=1500, msgFlags=0,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
securityName=jbond, engineBoots=0, engineTime=0, varCnt=13, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.3], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.5 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.4 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.3 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.14 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.1 [1], 1.3.6.1.4.1.4874.2.2.77.3.1.2 [1],
```

```
1.3.6.1.4.1.4874.2.2.77.3.1.11 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.12 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.15 [0], 1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [5],

SnmpRouterAgent44   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=5, errSts=0, errIndx=0, msgID=4, msgMaxSize=1500, msgFlags=0,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
securityName=jbond, engineBoots=0, engineTime=0, varCnt=14, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.1], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.5 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.4 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.3 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.14 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.10 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.1 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.2 [1], 1.3.6.1.4.1.4874.2.2.77.3.1.6 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.8 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.7 [f],
1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [3],

SnmpRouterAgent22   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=8, errSts=0, errIndx=0, msgID=7, msgMaxSize=1500, msgFlags=3,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
securityName=jbond, engineBoots=1, engineTime=8602, varCnt=6, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.4], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.9 [192.168.7.120], 1.3.6.1.4.1.4874.2.2.77.3.1.14
[1], 1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [4],
```

Meaning

- Table 61 lists the **show snmp secure-log** command output fields.

Table 61: show snmp secure-log Output Fields

Field Name	Field Description
Agent's Context	Owner of the secure log entry
LogData	Contents of the secure audit log

Related Topics

- **snmp-server clear secure-log** command
- **show snmp secure-log** command