Implementing SNMP

Simple Network Management Protocol (SNMP) for Cisco Unified Border Element (SP Edition) is defined in the following MIBs:

- CISCO-SESSION-BORDER-CONTROLLER-EVENT-MIB—Defines SNMP notifications and alarms that are generated by Cisco Unified Border Element (SP Edition). This MIB sends the notifications and traps that are generated by Cisco Unified Border Element (SP Edition) to the SNMP manager.
- CISCO-SESSION-BORDER-CONTROLLER-STATS-MIB—Defines the SNMP statistics information for Cisco Unified Border Element (SP Edition). The two types are call statistics and media statistics. The calls are categorized as Session Initiation Protocol (SIP) calls and H.323 calls; the media statistics refer to RTP.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

Feature History for Implementing SNMP

Release	Modification
Cisco IOS XE Release 2.4	Implementing Simple Network Management Protocol (SNMP) was introduced on the Cisco IOS XR.

Contents

Prerequisites for Implementing SNMP

The following prerequisites are required to implement SNMP for Cisco Unified Border Element (SP Edition):

- You must have sufficient user privileges to modify the running configuration of the router.
- You must have configured Cisco Unified Border Element (SP Edition).
- Before you can access the SNMP MIBs to perform SNMPv2 polling for the SBC MIB statistics or to configure the SNMP users and groups for SNMPv3 polling, you must configure the SNMP read-only community string by using the **snmp-server community** command in Cisco IOS XR. For more information about the **snmp-server community** command, see the *Cisco IOS Network Management Command Reference*.

Information About Implementing SNMP

This section describes how to implement SNMP for SBC:

- SNMP Notifications, page 43-2
- SNMP Statistics, page 43-3

SNMP Notifications

Table 43-1 lists the types of SNMP notifications.

Table 43-1 List of SNMP Notifications

Type	Description
Source Alert Notification	Specifies that the media is received from an unexpected source.
Blacklist Notification	Adds or removes the source from the blacklist table.
Adjacency Status Notification	Attaches or detaches the adjacency from the SBC.
SLA Violation Notification	Specifies that the violations of the Service Level Agreement (SLA) are described in the policy tables. SLAs can include the maximum number of calls allowed, maximum call rate, maximum bandwidth, and so forth.
Radius Connection Status Notification	Specifies that the SBC connection to a RADIUS server is either lost or restored.
H.248 Controller Status	Specifies if an H.248 controlled entity, either a data border element (DBE) or remote transcoder, is connected or detached from the SBC. See other sections of the documentation for supported H.248 controlled entities.

SNMP Statistics

Table 43-2 lists the types of SNMP statistics.

Table 43-2 List of SNMP Statistics

Type	Description
Global call statistics	Represents the global call-related statistics such as call rates, media flows, signaling flows, and so forth. The **show sbc dbe media-stats** command displays output for the global call statistics.
Periodic statistics	Represents the information for the SBC call statistics for a particular time interval such as current 5 minutes, previous 5 minutes, current 15 minutes, previous 15 minutes, current hour, and previous hour. The **show sbc sbe call-stats** command displays output for the periodic statistics.
Per flow statistics	Represents the SBC media flow statistics. These media statistics are used for each of the current ongoing call flows. The **show sbc dbe media-flow-stats** command displays output for the per-flow statistics.
H.248 statistics	Represents the information for the H.248 call-related statistics when the H.248 controller is associated with SBC. The **show sbc dbe controllers** command displays output for the H.248 statistics.

Implementing SNMP for Cisco Unified Border Element (SP Edition)

This section describes how to implement SNMP for Cisco Unified Border Element (SP Edition):

- Configuring SNMP Notifications, page 43-3

Configuring SNMP Notifications

Perform this task to configure SNMP notifications for Cisco Unified Border Element (SP Edition).

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server enable traps sbc** {**adj-status** | **blacklist** | **h248-ctrlr-status** | **qos-statistics** | **radius-conn-status** | **sla-violation** | **source-alert**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 2	**snmp-server enable traps sbc** {**adj-status** | **blacklist** | **congestion-alarm** | **h248-ctrlr-status** | **media-source** | **qos-statistics** | **radius-conn-status** | **sla-violation** | **source-alert**} **Example:** `Router(config)# snmp-server enable traps sbc blacklist`	Specifies the SBC notification type to be enabled. • Use the **adj-status** keyword to enable the SNMP SBC Adjacency Status trap when an adjacency is attached to or detached from the SBE. • Use the **blacklist** keyword to enable the SNMP SBC Dynamic Blacklist trap when a source is added or removed from the blacklist table. • Use the **congestion-alarm** keyword to enable the SNMP SBC Congestion Alarm trap. • Use the **h248-ctrlr-status** keyword to enable the SNMP SBC H.248 Controller Status trap. For a distributed deployment model, a DBE is attached or detached from the SBC. • Use the **media-source** keyword to enable the SNMP SBC Media Source Alert traps. • Use the **qos-statistics** keyword to enable the QoS statistics traps. See the ?$paranum>Implementing QoS Demarcation? section on page 39-10 for more information about the procedure. • Use the **radius-conn-status** keyword to enable the SNMP SBC Radius Connection Status trap when the connection is changed for the RADIUS server. • Use the **sla-violation** keyword to enable the SNMP SBC SLA Violation trap when there is an SLA violation in the policy tables. SLAs include the maximum number of calls allowed, maximum call rate, maximum bandwidth, and so on. • Use the **source-alert** keyword to enable the SNMP SBC Source Alert trap when media is received from an unexpected source. See the ?$paranum>Alarm Logs? section on page 44-6 for information about configuring logging for some of these alarms.
Step 3	**end** **Example:** `Router(config)# end`	Exits the configuration command.

Configuration Example for Implementing SNMP

This section provides the following configuration example for implementing SNMP for Cisco Unified Border Element (SP Edition):

Configuring SNMP Notifications: Example

The following example shows how to configure the SNMP blacklist notification for Cisco Unified Border Element (SP Edition):

```
configure terminal
 snmp-server enable traps sbc blacklist
 end
```