CHAPTER 14

Understanding Simple Network Management Protocol

This chapter provides information on the following topics:

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

You use Cisco Unified Serviceability to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. The settings that you configure in Cisco Unified Serviceability apply to the local node; however, if your Cisco Unified Communications Manager or Cisco Unity Connection configuration supports clusters, you can apply settings to all servers in the cluster with the “Apply to All Nodes” option in the SNMP configuration windows.

Tip *Unified CM only*: SNMP configuration parameters that you specified in Cisco Unified CallManager or Cisco Unified Communications Manager 4.X do not migrate during a Cisco Unified Communications Manager 6.0 and later upgrade. You must perform the SNMP configuration procedures again in Cisco Unified Serviceability.

This section contains information on the following topics:

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device—A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  Unified CM BE only: The server where Cisco Unified Communications Manager is installed acts as the managed device.

  Unified CM only: In a configuration that supports clusters, the first server in the cluster acts as the managed device.

- Agent—A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  Cisco Unified Communications Manager and Cisco Unity Connection use a master agent and subagent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few MIB variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Cisco Unified Communications Manager subagent interacts with the local Cisco Unified Communications Manager only. The Cisco Unified Communications Manager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- Network Management System (NMS)—A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Cisco Unified Communications Manager works with the following NMS:

- CiscoWorks
- HP OpenView
- Third-party applications that support SNMP and Cisco Unified Communications Manager SNMP interfaces

SNMP Configuration Requirements

The system provides no default SNMP configuration. You must configure SNMP settings after installation to access MIB information. Cisco supports SNMP V1, V2c, and V3 versions.

SNMP agent provides security with community names and authentication traps. You must configure a community name to access MIB information. Table 14-1 provides the required SNMP configuration settings.

Table 14-1 SNMP Configuration Requirements

Configuration	Cisco Unified Serviceability Page
V1/V2c Community String	**SNMP > V1/V2c >Community String**
V3 Community String	**SNMP > V3 > User**
System Contact and Location for MIB2	**SNMP > SystemGroup > MIB2 System Group**
Trap Destinations (V1/V2c)	**SNMP > V1/V2c > Notification Destination**
Trap Destinations (V3)	**SNMP > V3 > Notification Destination**

SNMP Version 1 Support

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In Cisco Unified Serviceability, you configure SNMP v1 support in the V1/V2c Configuration window.

SNMP Version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In Cisco Unified Serviceability, you configure SNMP v2c support in the V1/V2c Configuration window.

SNMP Version 3 Support

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the "SNMP Community Strings and Users" section on page 14-5.

In Cisco Unified Serviceability, you configure SNMP v3 support in the V3 Configuration window.

SNMP Services

The services in Table 14-2 support SNMP operations. For a description of each service, see the "Understanding Services" section on page 9-1.

Note SNMP Master Agent serves as the primary service for the MIB interface. You must manually activate Cisco CallManager SNMP service; all other SNMP services should be running after installation.

Table 14-2 SNMP Services

MIB	Service	Cisco Unified Serviceability Page
CISCO-CCM-MIB	Cisco CallManager SNMP service	**Tool > Control Center - Feature Services.** Choose a server; then, choose Performance and Monitoring category.
SNMP Agent	SNMP Master Agent	**Tool > Control Center - Network Services.** Choose a server; then, choose Platform Services category.
CISCO-CDP-MIB	Cisco CDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
Hardware MIBs	Native Agent Adaptor	

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the Cisco Unified Communications Manager network. Do not stop the services unless your technical support team tells you to do so.

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMP V1 and V2c only.

SNMP V3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In Cisco Unified Serviceability, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments. You configure the notification destinations by using the SNMP Notification Destination Configuration windows in Cisco Unified Serviceability.

Note Cisco Unified Communications Manager supports SNMP traps in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition systems. Cisco Unity Connection SNMP does not support traps.

For all notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, the CallManager alarms and system level log messages get sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages get logged locally in the syslog files and also get converted into SNMP traps/notifications.

The following list contains Cisco Unified Communications Manager SNMP trap/inform messages that are sent to a configured trap destination:

- Cisco Unified CallManager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

Tip Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string/user correctly.

You configure the SNMP trap destination by choosing **SNMP > V1/V2 > Notification Destination** or **SNMP > V3> Notification Destination** in Cisco Unified Serviceability.

Table 14-3 comprises information about Cisco Unified Communications Manager trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in Table 14-3 by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note All the parameters that are listed in Table 14-3 are part of CISCO-CCM-MIB except for the last two. The last two, clogNotificationsEnabled and clogMaxSeverity, comprise part of CISCO-SYSLOG-MIB.

Table 14-3 Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change **Note** Although you can configure a Cisco ATA 186 device as a phone in Cisco Unified Communications Manager Administration, when Cisco Unified Communications Manager sends SNMP traps for the Cisco ATA device, it sends a gateway type trap; for example, ccmGatewayFailed.	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600. See Configuring CISCO-CCM-MIB Trap Parameters, page 18-2.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600. See Configuring CISCO-CCM-MIB Trap Parameters, page 18-2.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.

Table 14-3 Cisco Unified Communications Manager Trap/Inform Configuration Parameters (continued)

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmQualityReportAlarmEnable	True	**Note** This trap gets generated only if the Cisco Extended Functions service is activated and running on the server; or, in the case of a cluster configuration (Cisco Unified Communications Manager only), on the local Cisco Unified Communications Manager server. ccmQualityReport	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True. See Configuring CISCO-SYSLOG-MIB Trap Parameters, page 18-1.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when Cisco Unified Communications Manager applications generate a syslog message with at least a warning severity level.Configuring CISCO-SYSLOG-MIB Trap Parameters, page 18-1.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

Note Cisco Unified Communications Manager supports the following MIBs in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition systems. Cisco Unity Connection supports the following MIBs except for CISCO-CCM-MIB.

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CCM-MIB
- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

The Simple Network Management Protocol (SNMP) extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In the case of a cluster configuration, the SNMP extension agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

For vendor-specific supported hardware MIBS, refer to the "Vendor-Specific MIBs" section.

Cisco Unified Communications Manager SNMP Interface supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco Unified Communications Manager CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco Unified Communications Manager to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun
- sysApplMap

- sysApplInstallElmt
- sysApplElmtRun

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the Cisco Unified Communications Manager and its associated devices, such as phones, gateways, and so on, that are visible on this Cisco Unified Communications Manager node. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

Note Cisco Unified Communications Manager supports this MIB in Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition systems. Cisco Unity Connection does not support this MIB.

To view the support lists for the CISCO-CCM-MIB and MIB definitions, go to the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

To view MIB dependencies and MIB contents, including obsolete objects, across Cisco Unified Communications Manager releases, go to the following link: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

Note Because IPv6 is not supported in this release, CISCO-CCM-MIB attributes that support IPv6, such as IPv6 address, address preferences, and active load ID, do not get populated.

Dynamic tables (see Table 14-4) get populated only if the Cisco CallManager service is up and running (or the local Cisco CallManager service in the case of a Cisco Unified Communications Manager cluster configuration); static tables (see Table 14-5) get populated when the Cisco CallManager SNMP Service is running.

Table 14-4 Cisco-CCM-MIB Dynamic Tables

Table(s)	Contents
ccmTable	This table stores the version and installation ID for the local CallManager. The table also stores information about all the CallManagers in a cluster that the local CallManager knows about but shows “unknown” for the version detail. If the local CallManager is down, the table remains empty, except for the version and installation ID values.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match Cisco Unified Communications Manager/RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone. The ccmPhoneExtnTable uses a combined index, ccmPhoneIndex and ccmPhoneExtnIndex, for relating the entries in the ccmPhoneTable and ccmPhoneExtnTable.
ccmCTIDevice, ccmCTIDeviceDirNum	The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Cisco Unified Communications Manager MIB get updated.
ccmSIPDevice	The CCMSIPDeviceTable stores each SIP trunk as one device.

Table 14-4 Cisco-CCM-MIB Dynamic Tables (continued)

Table(s)	Contents
ccmH323Device	The ccmH323DeviceTable contains the list of H323 devices for which Cisco Unified Communications Manager contains information (or the local Cisco Unified Communications Manager in the case of a cluster configuration). For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Cisco Unified Communications Manager. Cisco Unified Communications Manager generates the H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H323 trunk information.
ccmVoiceMailDevice, ccmVoiceMailDirNum	For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable includes one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisco Unified Communications Manager MIB get updated.
ccmGateway	The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively. Cisco Unified Communications Manager generates alarms at the device or port level. The ccmGatewayTable, based on CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports. Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.
ccmMediaDeviceInfo	The table contains a list of all media devices which have tried to register with the local CallManager at least once.
ccmGroup	This tables contains the Cisco Unified CM groups in a Cisco Unified Communications Manager cluster.
ccmGroupMapping	This table maps all Cisco Unified CMs in a cluster to a Cisco Unified CM group. The table remains empty when the local Cisco Unified CM node is down

Table 14-5 CISCO-CCM-MIB Static Tables

Table(s)	Content
ccmProductType	The table contains the list of product types that are supported with Cisco Unified Communications Manager (or cluster, in the case of a Cisco Unified Communications Manager cluster configuration), including phone types, gateway types, media device types, H323 device types, CTI device types, voice-messaging device types, and SIP device types.
ccmRegion, ccmRegionPair	ccmRegionTable contains the list of all geographically separated regions in a Cisco Communications Network (CCN) system. The ccmRegionPairTable contains the list of geographical region pairs for a Cisco Unified Communications Manager cluster. Geographical region pairs are defined by Source region and Destination region.
ccmTimeZone	The table contains the list of all time zone groups in a Cisco Unified Communications Manager cluster.
ccmDevicePool	The tables contains the list of all device pools in a Cisco Unified Communications Manager cluster. Device pools are defined by Region, Date/Time Group, and Cisco Unified CM Group.

Note ‘The “ccmAlarmConfigInfo” and “ccmQualityReportAlarmConfigInfo” groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that the “SNMP Management Information Base (MIB)” section on page 14-7 describes.

Vendor-Specific MIBs

The following MIBs exist on various Cisco MCS, depending on vendor and model number. To query these MIBS, you can use the standard MIB browsers that the hardware vendors develop; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information on using the MIB browsers, refer to the documentation that the hardware vendor provides.

To review the vendor-specific MIB information, see the following tables:

- Table 14-6—Describes supported IBM MIBs
- Table 14-7—Describes supported HP MIBs

Table 14-6 IBM MIBs

MIB	OID	Description
Supported for browsing only		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	Provides temperature, voltage, and fan status
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	Provides hardware component asset data
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	Provides temperature, voltage, and fan details
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Provides Network Interface Card (NIC) status
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	Provides physical memory details
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	Provides power supply details
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	Provides CPU asset/status data
Supported for system traps		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	Provides temperature, voltage, fan, disk, NIC, memory, power supply, and CPU details
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	Provides RAID status

Table 14-7 HP MIBs

MIB	OID	Description
Supported for browsing and system traps		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	Provides hardware component configuration data
CPQSINFO-MIB	1.3.6.1.4.1.232.2	Provides hardware component asset data
CPQIDA-MIB	1.3.6.1.4.1.232.3	Provides RAID status/events
CPQHLTH-MIB	1.3.6.1.4.1.232.6	Provides hardware components status/events
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	Provides storage (disk) systems status/events
CPQSM2-MIB	1.3.6.1.4.1.232.9	Provides iLO status/events
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	Provides alarm threshold management
CPQHOST-MIB	1.3.6.1.4.1.232.11	Provides operating system information
CPQIDE-MIB	1.3.6.1.4.1.232.14	Provides IDE (CD-ROM) drive status/events
CPQNIC-MIB	1.3.6.1.4.1.232.18	Provides Network Interface Card (NIC) status/events

SNMP Trace Configuration

For Cisco Unified Communications Manager, you can configure trace for the Cisco CallManager SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco CallManager SNMP Service in the Performance and Monitoring Services service group. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you use the CLI to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For Cisco Unity Connection, you can configure trace for the Connection SNMP agent in the Trace Configuration window in Cisco Unity Connection Serviceability by choosing the Connection SNMP Agent component.

SNMP Configuration Checklist

Table 14-8 provides an overview of the steps for configuring SNMP.

Table 14-8 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the Control Center—Network Services window, verify that the system started the SNMP services.	• SNMP Services, page 14-4 • Understanding Services, page 9-1 • Configuring Services, page 11-1
Step 3	*Unified CM and Unified CM BE only:* In the Service Activation window, activate the Cisco CallManager SNMP service. *Connection only:* The Connection SNMP Agent service automatically activates.	• SNMP Services, page 14-4 • Understanding Services, page 9-1 • Activating and Deactivating Feature Services, page 11-1
Step 4	If you are using SNMP V1/V2c, configure the community string.	Configuring a Community String, page 15-2
Step 5	If you are using SNMP V3, configure the SNMP user.	Configuring the SNMP User, page 16-2
Step 6	Configure the notification destination for traps or informs.	• For SNMP v1/v2c—Configuring a Notification Destination for SNMP V1/V2c, page 15-6 • For SNMP v3—Configuring a Notification Destination for SNMP V3, page 16-6 • SNMP Management Information Base (MIB), page 14-7
Step 7	Configure the system contact and location for the MIB2 system group.	Configuring the MIB2 System Group, page 17-1
Step 8	*Unified CM and Unified BE only:* Configure trap settings for CISCO-SYSLOG-MIB and CISCO-CCM-MIB.	• Configuring CISCO-SYSLOG-MIB Trap Parameters, page 18-1 • Configuring CISCO-CCM-MIB Trap Parameters, page 18-2

Table 14-8 SNMP Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 9	Restart the Master Agent service.	• SNMP Services, page 14-4 • Understanding Services, page 9-1 • Understanding Services, page 9-1
Step 10	On the NMS, configure the Cisco Unified Communications Manager trap parameters.	• SNMP Management Information Base (MIB), page 14-7 • SNMP product documentation that supports the NMS

Where to Find More Information

Related Topics

- Understanding Services, page 9-1
- Configuring Services, page 11-1
- Configuring SNMP V1/V2c, page 15-1
- Configuring SNMP V3, page 16-1
- Configuring SNMP System Group, page 17-1
- Configuring SNMP Trap/Inform Parameters, page 18-1
- Troubleshooting, page 19-1