CHAPTER 10

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.

Note SNMP configuration parameters that you specified in Cisco Unified CallManager 4.0 or Cisco Unified CallManager 4.1 do not migrate during the Cisco Unified CallManager 5.0 installation. You must perform the SNMP configuration procedures again.

In previous releases of Cisco Unified CallManager, no graphical user interface existed in Cisco Unified CallManager Serviceability for configuring Cisco Unified CallManager SNMP settings. In Cisco Unified CallManager 5.0, you use Cisco Unified CallManager Serviceability to configure

SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. Likewise, in the SNMP configuration windows, you can apply the settings to all servers in the cluster; that is, if you want to do so.

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.

  The first node in the Cisco Unified CallManager 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 CallManager uses 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 CallManager subagent interacts with the local Cisco CallManager only. The Cisco CallManager 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 CallManager works with the following NMS:
  - CiscoWorks2000
  - HP OpenView
  - Third-party applications that support SNMP and Cisco CallManager SNMP interfaces

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 CallManager 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 CallManager 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 10-4.

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

Cisco CallManager SNMP Services

To support SNMP, Cisco Unified CallManager uses the following services, which display in the Service Activation and/or Control Center windows in Cisco Unified CallManager Serviceability.

- Cisco CCM SNMP service—This service provides SNMP access to provisioning and statistics information that is available for Cisco Unified CallManager and implements the CISCO-CCM-MIB.

  If you use SNMP, activate this service on all servers in the cluster.

- SNMP Master Agent—This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in Cisco Unified CallManager Serviceability, you must restart the SNMP Master Agent service in the Control Center—Network Features window.

- MIB2 Agent—This service provides SNMP access to variables that are defined in RFC 1213; for example, system, interfaces, IP and so on.
- Host Resources Agent—This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. This service implements the HOST-RESOURCES-MIB.
- System Application Agent—This service implements the SYSAPPL-MIB to provide a system-level view of the installed applications and their status.
- Native Agent Adaptor—This service allows you to forward requests from an SNMP Master agent to a Native SNMP agent running on the same system. Native SNMP agent supports vendor MIBs only.
- Cisco CDP Agent—This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the Cisco Unified CallManager node. This service implements the CISCO-CDP-MIB.
- Cisco Syslog Agent—This service supports gathering of syslog messages that various Cisco Unified CallManager components generate and enables syslog messages to be converted to SNMP traps. This service implements the CISCO-SYSLOG-MIB.

Caution Stopping any Cisco CallManager SNMP service may result in loss of data because the network management system no longer monitors the Cisco Unified CallManager network. Do not stop the services unless the Cisco Technical Assistance Center 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 CallManager 5.0, 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 acknowlegments from the destination whereas informs do receive acknowlegments. You must configure the notification destinations by using the SNMP Notification Destination Configuration windows.

The following list contains Cisco Unified CallManager 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

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

Table 10-1 comprises information about Cisco Unified CallManager trap/Inform parameters.

Table 10-1 Cisco Unified CallManager 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	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.

Table 10-1 Cisco Unified CallManager Trap/Inform Configuration Parameters (continued)

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmQualityReportAlarmEnable	True	ccmQualityReport **Note** This trap gets generated only if the Cisco Extended Functions service is activated and running on the local Cisco Unified CallManager node.	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when Cisco Unified CallManager applications generate a syslog message with at least a warning severity level.

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).

The Cisco Unified CallManager Simple Network Management Protocol (SNMP) extension agent resides in each Cisco Unified CallManager node and exposes the CISCO-CCM-MIB that provides detailed information about devices that are known to the node. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the node (not the cluster).

Cisco Unified CallManager supports the following MIBs.

CISCO-CDP-MIB

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

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

- CdpGlobalDeviceId
- CdpInterfaceEnable
- CdpInterfaceMessageInterval
- CdpGlobalRun

- CdpGlobalMessageInterval
- CdpGlobalHoldTime

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:

- sysApplInstalled
- sysApplRun
- sysApplMap

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

The system supports trap functionality only. The Cisco Syslog Agent supports only the following objects of CISCO-SYSLOG-MIB:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores

- clogMsgDrops

Vendor-Specific MIBs from HP

CPQAPLI.MIB, CPQCLUS.MIB, CPQCR.MIB, CPQFCA.MIB, CPQHLTH.MIB, CPQHOST.MIB, CPQIDA.MIB, CPQIDE.MIB, CPQNIC.MIB, CPQRECOV.MIB, CPQSCSI.MIB, CPQSINFO.MIB, CPQSM2.MIB, CPQSTAT.MIB, CPQSTDEQ.MIB, CPQSTSYS.MIB, CPQTHRSH.MIB, CPQUPS.MIB, ETHER.MIB, SVRCLU.MIB, SVRNTC.MIB, TOKEN.MIB

Vendor-Specific MIBs from IBM

UMSEVENT-MIB, UMSLMSSENSOR-MIB, HW-ENV-MONITORING-MIB

CISCO-CCM-MIB

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

To view the supports lists for the CISCO-CCM-MIB, click the following link:

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

The following list of tables exists in the CISCO-CCM-MIB:

- ccmPhoneFailedTable, ccmPhoneStatusUpdateTable, ccmPhoneExtnTable, ccmPhoneTable

  For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match Cisco CallManager/ RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone.

- ccmCTIDeviceTable, ccmCTIDeviceDirNumTable

  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 CallManager MIB get updated.

- ccmSIPDeviceTable

  The CCMSIPDeviceTable stores each SIP trunk as one device.

- ccmH323Device

  The ccmH323DeviceTable contains the list of H323 devices for which the local Cisco Unified CallManager contains information. 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 CallManager. Cisco Unified CallManager generates 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.

- ccmVoiceMailDeviceTable, ccmVoiceMailDirNumTable

  For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable has one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisco CallManager MIB get updated.

- ccmGatewayTable

  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 CallManager generates alarms at the device or port level. The ccmGatewayTable, based on Cisco Unified 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.

- ccmProductTypeTable

  The table contains the list of product types that are supported in a Cisco Unified CallManager cluster, including phone types, gateway types, media device types, H323 device types, CTI device types, voice-messaging device types and SIP device types.

Note The dynamic tables such as phoneTable, gatewayTable, and so on, get populated only if the local Cisco CallManager service is up and running. The static tables such as region, timezone, devicepool, and so on, in the Cisco CallManager MIB, get populated when the Cisco CallManager SNMP service is running.

Note The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that the "SNMP Traps and Informs" section on page 10-4 describes.

SNMP Trace Configuration

In Cisco Unified CallManager Serviceability, you can configure trace for Cisco CCM agent. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you can use CLI to change trace settings.

SNMP Configuration Checklist

Table 10-2 provides an overview of the steps for configuring SNMP.

Table 10-2 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 window, verify that the system started the Cisco CallManager SNMP services.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco Unified CallManager Serviceability Administration Guide*

Table 10-2 SNMP Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	In the Service Activation window, activate the Cisco CCM SNMP service.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco Unified CallManager Serviceability Administration Guide*
Step 4	If you are using SNMP v1/v2c, configure the community string.	SNMP Community String Configuration, *Cisco Unified CallManager Serviceability Administration Guide*
Step 5	If you are using SNMP v3, configure the SNMP user.	SNMP User Configuration, *Cisco Unified CallManager Serviceability Administration Guide*
Step 6	Configure the notification destination for traps or Informs.	• For SNMP v1/v2c—SNMP Notification Destination Configuration for V1/V2c, *Cisco Unified CallManager Serviceability Administration Guide* • For SNMP v3—SNMP Notification Destination Configuration for V3, *Cisco Unified CallManager Serviceability Administration Guide* • SNMP Traps and Informs, page 10-4
Step 7	Configure the system contact and location for the MIB2 system group.	MIB2 System Group Configuration, *Cisco Unified CallManager Serviceability Administration Guide*
Step 8	Restart the Master Agent service.	• Cisco CallManager SNMP Services, page 10-3 • Service Management, page 2-1 • Managing Services, *Cisco Unified CallManager Serviceability Administration Guide*
Step 9	On the NMS, configure the Cisco Unified CallManager trap parameters.	SNMP product documentation that supports the NMS

Troubleshooting

Review this section for troubleshooting tips.

Make sure that all of the feature and network services listed in "Cisco CallManager SNMP Services" section on page 10-3 are running.

Cannot poll any MIBs from the system

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system.

Note By default, no community string or user is configured on the system.

Check whether the community string or snmp user is properly configured on the system by using the SNMP configuration windows.

Cannot receive any notifications from the system

This condition means that the notification destination is not configured correctly on the system.

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.

Where to Find More Information

Related Topics

- Service Management, page 2-1
- Managing Services, *Cisco Unified CallManager Serviceability Administration Guide*
- SNMP V1/V2c Configuration, *Cisco Unified CallManager Serviceability Administration Guide*
- SNMP V3 Configuration, *Cisco Unified CallManager Serviceability Administration Guide*
- MIB2 System Group Configuration, *Cisco Unified CallManager Serviceability Administration Guide*