Main page: Cisco Unified Presence, Release 7.x

Contents

- 1 Previous Topic
- 2 About Simple Network Management Protocol Support
  - 2.1 SNMP Basics
    - 2.1.1 Related Topics
  - 2.2 SNMP version 1 Support
    - 2.2.1 Related Topics
  - 2.3 SNMP version 2c Support
    - 2.3.1 Related Topics
  - 2.4 SNMP version 3 Support
    - 2.4.1 Related Topics
  - 2.5 SNMP Services
    - 2.5.1 Related Topics
  - 2.6 SNMP Community Strings and Users
    - 2.6.1 Related Topics
  - 2.7 SNMP Management Information Base (MIB)
    - 2.7.1 CISCO-CDP-MIB
    - 2.7.2 SYSAPPL-MIB
    - 2.7.3 MIB-II
    - 2.7.4 HOST-RESOURCES MIB
    - 2.7.5 CISCO-SYSLOG-MIB
    - 2.7.6 CISCO-CCM-MIB
    - 2.7.7 Related Topics
    - 2.7.8 Vendor-Specific MIBs
    - 2.7.9 Table: IBM MIBs
    - 2.7.10 Table: HP MIBs
    - 2.7.11 Related Topics
  - 2.8 SNMP Traps and Informs
    - 2.8.1 Table: Cisco Unified Communications Manager Trap/Inform Configuration Parameters
    - 2.8.2 Related Topics
- 3 SNMP Configuration Checklist
  - 3.1 Table: SNMP Configuration Checklist
  - 3.2 Related Topics
- 4 Troubleshooting SNMP
  - 4.1 Related Topics

Previous Topic

- Cisco Unified Serviceability Administration for Cisco Unified Presence

- About Simple Network Management Protocol Support

- SNMP Configuration Checklist

- Troubleshooting SNMP

About Simple Network Management Protocol Support

- SNMP Basics
- SNMP Version 1 Support
- SNMP version 2c Support
- SNMP version 3 Support
- SNMP Services
- SNMP Community Strings and Users
- SNMP Management Information Base (MIB)
- SNMP Traps and Informs

SNMP Basics

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. Likewise, in the SNMP configuration windows, you can apply the settings to all nodes in the cluster.

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 Communications Manager 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 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 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:

- CiscoWorks2000
- HP OpenView
- Third-party applications that support SNMP and Cisco Unified Communications Manager SNMP interfaces

Related Topics

- Getting More Information

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.

Related Topics

- How to Configure SNMP V1/V2c in Cisco Unified Serviceability
- Getting More Information

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.

Related Topics

- How to Configure SNMP V1/V2c in Cisco Unified Serviceability
- Getting More Information

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.

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

Related Topics

- How to Configure SNMP V3 in Cisco Unified Serviceability
- SNMP Community Strings and Users
- Getting More Information

SNMP Services

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

- SNMP Master Agent
- MIB2 Agent
- Host Resources Agent
- System Application Agent
- Native Agent Adaptor
- Cisco CDP Agent
- Cisco Syslog Agent

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.

Related Topics

- About Feature and Network Services in Cisco Unified Serviceability
- Getting More Information

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.

Related Topics

- How to Configure SNMP V1/V2c in Cisco Unified Serviceability
- How to Configure SNMP V3 in Cisco Unified Serviceability
- Getting More Information

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 Simple Network Management Protocol (SNMP) extension agent resides in each Cisco Unified Presence node. Cisco Unified Presence supports the following MIBs.

CISCO-CDP-MIB

Use the Cisco Unified Presence CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco Unified Presence 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:

- 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

CISCO-CCM-MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the local Cisco Unified Communications Managerand 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 support lists for the CISCO-CCM-MIB, go to 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 Unified Communications Manager/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 Unified Communications Manager 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 Communications Manager 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 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.

- 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 Unified Presence 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 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.

- ccmProductTypeTable

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

- ccmMediaDeviceInfo Table

  The table contains a list of all media devices which have tried to register with the local CallManager at least once.

Note: The "ccmAlarmConfigInfo" and "ccmQualityReportAlarmConfigInfo" groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications.

Related Topics

SNMP Traps and Informs

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 are developed by the hardware vendors; for example, HP Systems Insight Manager (SIM) and IBM Director Server+Console. For information about 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: IBM MIBs-Describes supported IBM MIBs

- Table: HP MIBs-Describes supported HP MIBs

Table: 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: 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

Related Topics

- Getting More Information

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.

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

The following SNMP trap/inform message is sent to a configured trap destination:

- 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: Cisco Unified Communications Manager Trap/Inform Configuration Parameters comprises information about Cisco Unified Presence trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in the table below by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note: Be aware that the parameters that are listed in the table below are part of CISCO-SYSLOG-MIB.

Table: Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
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 Communications Manager applications generate a syslog message with at least a warning severity level.

Related Topics

- Getting More Information

SNMP Configuration Checklist

Table: SNMP Configuration Checklist provides an overview of the steps for configuring SNMP.

Table: SNMP Configuration Checklist

	Configuration Steps	Related Procedures and Topics
1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
2	In the Control Center-Network Services window, verify that the system started the SNMP services.	• SNMP Services • About Feature and Network Services in Cisco Unified Serviceability
3	If you are using SNMP v1/v2c, configure the community string.	Configuring a Community String
4	If you are using SNMP v3, configure the SNMP user.	Configuring an SNMP User
5	Configure the notification destination for traps or informs.	• For SNMP v1/v2c- ♦ How to Configure SNMP V1/V2c in Cisco Unified Serviceability • For SNMP v3- ♦ How to Configure SNMP V3 in Cisco Unified Serviceability ♦ SNMP Traps and Informs
6	Configure the system contact and location for the MIB2 system group.	Configuring the MIB2 System Group
7	Restart the Master Agent service.	• SNMP Services • About Feature and Network Services in Cisco Unified Serviceability.
8	On the NMS, configure the Cisco Unified Communications Manager trap parameters.	• SNMP Traps and Informs • SNMP product documentation that supports the NMS

Related Topics

- Getting More Information

Troubleshooting SNMP

Review this section for troubleshooting tips. Make sure that all of the feature and network services are running.

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

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

Problem: Cannot receive any notifications from the system This condition means that the notification destination is not configured correctly on the system.

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

Related Topics

- SNMP Services
- Getting More Information