Simple Network Management Protocol

This chapter gives an overview of Simple Network Management Protocol (SNMP).

Overview

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes and routers. It comprises part of the TCP/IP suite. System administrators can remotely manage network performance, find and solve network problems, and plan for network growth by using SNMP.

Instead of defining a large set of commands, SNMP places all operations in a **get-request**, **get-next-request**, **get-bulk-request**, and **set-request** format. For example, an SNMP manager can get a value from an SNMP agent or store a value in that SNMP agent. The SNMP manager can comprise part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a router.

SNMP comprises of three parts—SNMP manager, SNMP agent, and MIBs. You can compile the Cisco MIB with your network management software.

The NMS uses the Cisco MIB variables to set device variables and to poll devices on the internetwork for specific information. The results of a poll can get graphed and analyzed to help you troubleshoot internetwork problems, increase network performance, verify the configuration of devices, and monitor traffic loads.

The SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The SNMP agent also can send traps (notifications) of certain events, to the SNMP manager. The Cisco host `//ftp.cisco.com` makes available the Cisco trap file, "mib.traps," which documents the format of Cisco traps.

The SNMP manager uses information in the MIB to perform the operations as described:

Operation	Description
get-request	Retrieve a value from a specific variable.
get-next-request	Retrieve the value following the named variable. Often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search gets performed to find the needed variable from within the MIB.
get-response	Reply to a get-request, get-next-request, get-bulk-request, and set-request that an NMS sent.
get-bulk-request	Fills the get-response with up to max-repetition number of get-next interactions, similar to get-next-request.
set-request	Store a value in a specific variable.
traps	Sent by an SNMP agent to an SNMP manager to indicate that some event occurred.

SNMP Versioning

Three versions of SNMP exist: version 1 (SNMPv1), version 2 (SNMPv2), and version 3 (SNMPv3). SNMPv1 represents the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI) and operates over protocols, such as User Datagram Protocol (UDP) and IP.

The SNMPv1 SMI defines highly structured MIB tables that are used to group objects that contain 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.

As with SNMPv1, SNMPv2c functions within the specifications of SMI. MIB modules contain definitions of interrelated managed objects. Be aware that 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 enables one NMS to send trap information to another NMS and to receive a response from the NMS.

SNMPv3 provides the following security features:

- Authentication—Verifying that the request comes from a genuine source.

- Privacy—Encrypting data.

- Authorization—Verifying that the user allows the requested operation.

- Access control—Verifying that the user has access to the objects that are requested.

SNMPv3 prevents packets from being exposed on the network. Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users.

Related Topics

SNMP and Cisco Unified CM Basics

A network that uses SNMP requires three key components—managed devices, agents, and network management software (NMS).

- Managed devices—Devices that contain SNMP agents and reside on a network. Managed devices collect and store information and make it available by using SNMP.

  - The first node in the Cisco Unified CM cluster acts as the managed device. In Cisco Unified CMBE, the server on which Cisco Unified CM is installed acts as the managed device.

- Agents—Software modules that contain local knowledge of management information and translates it into a form that is compatible with SNMP.

  - Cisco Unified CM 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. It contains a few Management Information Base (MIB) variables. The master agent also connects and disconnects subagents after the subagent completes necessary tasks.

  - Cisco Unified CM uses a subagent to interact with the local Cisco Unified CM only. The Cisco Unified CM subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- NMS—SNMP management application that runs on a PC and provides the bulk of the processing and memory resources that are required for network management. It 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

SNMP Limits

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

SNMP Basic Commands

Managed devices get monitored and controlled by using four basic SNMP commands: read, write, trap, and traversal operations.

- NMS uses the read command to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

- NMS uses the write command to control managed devices. The NMS changes the values of variables stored within managed devices.

- Managed devices use the trap command to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.

- NMS uses traversal operations to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

SNMP Community Strings and Users

Although SNMP community strings provide no security, the strings 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. It uses SNMP users that serve the same purpose as community strings but provide security because encryption or authentication is configured.

No default community string or user exists.

SNMP and Cisco MIBs

You can access the Cisco MIB variables by using SNMP which facilitates the exchange of management information between network devices. The SNMP system comprises three parts: SNMP manager, SNMP agent, and MIB.

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, get-bulk-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or store a value in that SNMP agent. The SNMP manager can comprise part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a router. You can compile the Cisco MIB with your network management software. If SNMP is configured on a router, the SNMP agent can respond to MIB-related queries that are being sent by the NMS.

The NMS uses the Cisco MIB variables to set device variables and to poll devices on the internetwork for specific information. The results of a poll can get graphed and analyzed to help you troubleshoot internetwork problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

The SNMP agent gathers data from the MIB, which provides the repository for information about device parameters and network data. The SNMP agent also can send traps (notifications) of certain events, to the SNMP manager. The Cisco host `//ftp.cisco.com` makes available the Cisco trap file, "mib.traps," which documents the format of Cisco traps.

The SNMP manager uses information in the MIB to perform the operations as described:

Operation	Description
get-request	Retrieve a value from a specific variable.
get-next-request	Retrieve the value following the named variable. Often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within the MIB.
get-response	The reply to a get-request, get-next-request, get-bulk-request, and set-request sent by an NMS.
get-bulk-request	Similar to get-next-request, but fills the get-response with up to max-repetition number of get-next interactions.
set-request	Store a value in a specific variable.
traps	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred.

SNMP Traps and Informs

An SNMP agent sends notifications 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.

Note Cisco Unity Connection does not support SNMP traps.

For all notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, the Cisco Unified CM 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 CM SNMP trap and inform messages that are sent to a configured trap destination:

- Cisco Unified CM 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

SNMP Trace Configuration

For Cisco Unified CM, you can configure traces for the SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco Unified CM 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 command line interface (CLI) to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

SNMP Tips

Refer to the CISCO-CCM-CAPABILITY-MIB at http://tools.cisco.com/Support/SNMP/do/ BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY or to the CISCO-CCM-CAPABILITY MIB topic in the related topics section.

As stated in the CISCO-CCM-CAPABILITY-MIB, ccmPhoneDevicePoolIndex does not get supported, so it returns a 0. The Callmanager device registration alarm currently does not contain the device pool information.

If Cisco CallManager SNMP service is not running, only the following tables in the MIB respond:

- ccmGroupTable

- ccmRegionTable

- ccmRegionPairTable

- ccmDevicePoolTable

- ccmProductTypeTable

- ccmQualityReportAlarmConfigInfo

- ccmGlobalInfo

To get Cisco CallManager SNMP service running, activate and start the service in Cisco Unified Serviceability. Query the following tables in the SYSAPPL-MIB:

- SysApplInstallPkgTable to get an inventory of Cisco Unified Communications Manager applications that are installed on the system.

- SysApplRunTable to get an inventory of Cisco Unified Communications Manager applications that are running on the system.

Note Cisco Unified Communications Manager uses the following Web application services and servlets: Cisco CallManager Admin, Cisco CallManager Cisco IP Phone Services, Cisco CallManager Personal Directory, Cisco CallManager Serviceability, Cisco CallManager Serviceability RTMT, Cisco Extension Mobility, Cisco Extension Mobility Application, Cisco RTMT Reporter Servlet, Cisco Tomcat Stats Servlet, Cisco Trace Collection Servlet, Cisco AXL Web Service, Cisco Unified Mobile Voice Access Service, Cisco Extension Mobility, Cisco IP Manager Assistant, Cisco Web Dialer Service, Cisco CAR Web Service, and Cisco Dialed Number Analyzer.

Related Topics

CISCO-CCM-CAPABILITY

SNMP Troubleshooting

In general ensure that all the feature and network services are running and verify that the community string or SNMP user is properly configured on the Cisco Unified CM system. You configure the SNMP community string or user by choosing **SNMP** > **V1/V2** > **Community String or SNMP** > **V3** > **User** in Cisco Unified Serviceability.

Other tips are as follows:

- 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. Check the configuration and reconfigure if necessary.

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

- 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.

- Cannot receive SNMP traps from Cisco Unified Communications Manager node—Verify that you configured the following MIB Object IDentifiers (OIDs) that relate to phone registration/deregistration/failure to the following values (the default for both values equals 0):

    ◦ ccmPhoneFailedAlarmInterval (1.3.6.1.4.1. 9.9.156.1.9.2) set to 30-3600. You can use this CLI command: **snmpset -c** *<community string>* **-v2c** *<transmitter ipaddress>* **1.3.6.1.4.1.9.9.156.1.9.2 .0 i** *<value>*

    ◦ ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) set to 30-3600. You can use this CLI command: **snmpset -c** *<community string>* **-v2c** *<transmitter ipaddress>* **1.3.6.1.4.1.9.9.156.1.9.4.0 i** *<value>*

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

    Verify that you configured the community string/user privileges correctly, including Notify permissions, in the Community String (V1/V2c) or User (V3) Configuration window.

Because System Application Agent cannot show services that are activated and deactivated or monitor Web App services or servlets, use this approach to monitor system health and service status for Cisco Unified Communications Manager applications:

- Use the Serviceability API **getservicestatus** to provide complete status information, including activation status, for both Web applications and non-Web applications. See the AXL Serviceability API Guide for more details.

- Check service status with this CLI command: **utils service list**

- Monitor the servM-generated messages with Syslog (see the following example):

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service
Activated. Service
Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager
Cluster ID: Node
ID:ciscart26
```

If an SNMP request specifies multiple OIDs and the variables are pointing to empty tables, you may get a NO_SUCH_NAME (for SNMP V1) or GENERIC ERROR (for SNMP V2c or V3) due to a timeout problem. A timeout can occur as a result of throttling enhancements to protect the Cisco Unified Communications Manager processing engine.

You can retrieve the count of entries in CCMH323DeviceTable and ccmSIPDeviceTable by using scalar objects, so the SNMP Manager (the client) can avoid unnecessary get/getnext operations on these tables when no entries exist. As an SNMP developer, you can use the following workaround for this problem:

- Use the available scalar variables (1.3.6.1.4.1.9.9.156.1.5) to determine table size before accessing the table or perform the **get** operation on the desired table; then, query the non-empty tables.

- Reduce the number of variables that are queried in a single request; for example, for empty tables, if the management application has the timeout set to 3 seconds, specify only 1 OID. (For non-empty tables, it takes 1 second to retrieve one row of data.)

- Increase the response timeout.

- Reduce the number of retries.

- Avoid using **getbulk** SNMP API. The **getbulk** API retrieves the number of records that is specified by MaxRepetitions, so even if the next object goes outside the table or MIB, it gets those objects. Empty tables cause even more delay. Use **getbulk** API for non-empty tables with a known number of records. In these circumstances, set MaxRepetitions to 5 seconds to require a response within 5 seconds.

- Structure SNMP queries to adapt to existing limits.

- Avoid performing multiple **getbulks** to walk the PhoneTable periodically in case a large number of phones are registered to Cisco CallManager. You can use the ccmPhoneStatusUpdateTable, which updates whenever there is a Phone update, to decide whether to walk the PhoneTable.

Related Topics

Cisco Management Information Base
Industry-Standard Management Information Base

SNMP/R MIBs

When SNMP/R binaries spike the CPU, collect the following logs and information for analysis:

- Note the processes that are experiencing high CPU usage.

- Check to see if any SNMP polling is occurring and get the polling interval of the application.

- Note the SNMP versions by using the **show packages active snmp** command.

- Execute the **show process using-most cpu** command and collect the output.

- Collect the Perfmon logs by executing the **file get activelog /cm/log/ris/csv/** command.

- Collect the traces for SNMP Master Agent, and other binaries experiencing high CPU.

- Send the above information to Support for further troubleshooting.

When the SNMP Master Agent does not start, check to see if port 161 is open. If the port is open, collect the SNMP Master Agent traces for further analysis.

When migrating from Windows to Linux Cisco Unified CM, the ccmH323DevRmtCM1InetAddress has been defined as OctetString in Cisco Unified CM Release 5.x and later. So, the IP Address displays as Hexadecimal instead of the dotted decimal format as displayed in Cisco Unified CM Release 4.x.