The Cisco Unified MeetingPlace SNMP feature lets you monitor Cisco Unified MeetingPlace the same way you manage other devices on the network. By using a Simple Network Management Protocol (SNMP) management tool, and configuring it appropriately, you can obtain network status information and gain access to the system.

The SNMP feature supports all the standard "MIB II" queries and a set of Cisco Unified MeetingPlace MIB traps. The MIB II queries include information such as the Cisco Unified MeetingPlace server name, location, and contact name, plus various statistics regarding the network interface.

Table: Cisco Unified MeetingPlace SNMP describes the conditions that generate Cisco Unified MeetingPlace MIB traps.

Contents

- 1 Table: Table D-1 Cisco Unified MeetingPlace SNMP
- 2 Setting Up Contact and Location Information
  - 2.1 To Set Up Contact and Location Information
- 3 Setting Up Community Information
  - 3.1 To Set Up Community Information

Table: Table D-1 Cisco Unified MeetingPlace SNMP

This Alarm	Is Generated Whenever
T1 status	A T1 line goes down
Gateway System Integrity Manager (SIM)	The Gateway SIM registers an alarm
Server startup	The server restarts or crashes (cold start)
Major hardware alarm	A major hardware failure occurs
Major software alarm	A major software failure occurs
Minor hardware alarm	A minor hardware failure occurs
Minor software alarm	A minor software failure occurs

Each major and minor hardware and software notification includes an integer alarm code that indicates which software module and server reported the alarm. For hardware alarms, four additional codes identify the device type, the device address, slot number, and port number. The MIB defines these fields.

A MIB file, named CISCO-LATITUDE-MIB, contains all the MIB alarms. You must load this MIB file into

your monitoring system and configure it to enable the trap messages to display properly. To download this file and for more information, go to: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-LATITUDE-MIB.

For a list of major and minor alarms, see the *MeetingPlace Server Alarm Reference* document, at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_tech_notes_list.html.

Remember the following:

- Normally, each alarm instance generates a separate notification. In some cases, however, one specific incident could trigger multiple types of alarms.
- The *MeetingPlaceConfs* MIB is reserved for future use. It responds to queries but contains no information about conferences on the Cisco Unified MeetingPlace servers.

Setting Up Contact and Location Information

With the Cisco Unified MeetingPlace SNMP option installed, you can see Cisco Unified MeetingPlace servers from any SNMP Management station without supplying special configuration information. To control access to the SNMP module and set up SNMP data exchange, however, you must supply information in the Network Management Information and Network Management Communities topics of the Configure tab.

Network Management Information controls high-level access to the SNMP module and allows Cisco Unified MeetingPlace to exchange SNMP data with the rest of your network. To ensure the SNMP system administrator contacts the right person for any issues related to the Cisco Unified MeetingPlace system, enter data in the System contact and System location fields.

Tip: The Cisco Unified MeetingPlace system contact and location can also be set from the SNMP management station.

To Set Up Contact and Location Information

1. In MeetingTime, select the **Configure** tab.
2. Select the **Network Management Info** topic, and configure the following parameters.

Parameter	Configure
IP Port Number	The port on which Cisco Unified MeetingPlace can find incoming SNMP messages. Port 161 is most commonly used.
System Contact	The name of the Cisco Unified MeetingPlace system administrator.
System Location	The physical location of the Cisco Unified MeetingPlace system.
	The ability to turn off all SNMP queries.

Table: Table D-1 Cisco Unified MeetingPlace SNMP

Disable SNMP Queries	

Setting Up Community Information

Using the Network Management Communities topic in the Configure tab, you can define SNMP communities for controlling access to Cisco Unified MeetingPlace through SNMP. The Network Management Communities topic also shows you the network information available from the SNMP module.

You can configure two types of network management communities:

- Trap community-Defines a host to which Cisco Unified MeetingPlace sends standard MIB II traps.
- Non-trap community-Controls the type of access that is provided in response to an SNMP message: read-write, read only, or no access.

If a problem exists, contact the administrator of hosting.

Caution! The SNMP agent does not accept queries on trap communities. So, for example, to make queries using the public community, do not designate *public* to be a trap community.

To Set Up Community Information

1. In MeetingTime, select the **Configure** tab.
2. Select the **Network Mgmt Communities** topic.
   You will configure the following attributes (described in these steps).

Attribute	Configure
Name	The name of the network management community. Standard "public" and "private" communities are predefined. They are called *MeetingPlace-public* and *MeetingPlace-private* . You may use these values or replace them with your own.
IP Address	The IP address to which traps are sent for trap communities. This parameter is ignored for non-trap communities.
Read-Write	When set to *Yes* , SNMP messages for this community can modify stored SNMP data. (Ignored for trap communities.) Typically, administrators choose read-only in the public community; private communities are often used for read-write access.
Is It a Trap	SNMP agents can proactively notify the administrator through a "trap" (for example, "I am restarting"). The SNMP module can activate traps when the system restarts, when a network link changes state, or when an SNMP message that fails authentication is received.

3. Delete the private community and rename the public and trap communities, as shown in the following table.

To	Do This
Delete the private community	Click the **Query** button, then click the **<** or **>** button to find the private community. Click **Delete** , then click **Save Changes** .
Rename the public community	Click the **Query** button, and click the **<** or **>** button to find the public community. Enter the following name exactly as shown (it is case sensitive): **rwcHP1** Then click **Save Changes** . **Note:** This value is the same on all servers; it does not change.
Rename the trap community	Set the IP address to the current server value. Then click **Save Changes** .

4. Restart the Cisco Unified MeetingPlace 8106 or 8112 for these changes to take effect.

Traps appear on SNMP management tools as events with a trap code. Because most SNMP management tools permit configuration of both the event message and the alarm severity, we recommend that system administrators configure T1 and Gateway SIM traps so that they are easy to spot and understand. For a list of generic codes, see the About SNMP Traps.