CHAPTER 12

Using SNMP

Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a device (a host, gateway, server, and so on).

A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device provides information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the MIB. The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol, together with the MIB, provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. The MIB information used by Cisco netManager is contained in MIB files in the MIB directory.

For basic steps on how to enable SNMP on a Cisco device, go to

http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/dial_nms/snmpios.html#wp1049705

Monitoring SNMP Service

You can select SNMP on a device's **Services** dialog box (**Properties > Services**) and monitor it just as you can monitor any TCP service. SNMP monitoring checks to see if the SNMP service is running on the device.

Assigning SNMP Active Monitor to a Device

Step 1 In the Device Properties Active Monitor dialog box, click **Add**. The Active Monitor Properties dialog box opens.

Step 2 Select the SNMP Active Monitor, then click **Next**.

Step 3 Set the polling properties for the monitor, then click **Next**.

Step 4 Set up an Action for the monitor state changes.

Step 5 Click **Finish** to add the monitor to the device.

Note An SNMP-manageable device is identified on the map by a star in the upper-right corner of the device.

About the SNMP Agent or Manager

SNMP agent or manager software must be installed and enabled on any devices for which you want to receive SNMP information. Windows NT 4.0 and Windows 98, 2000, ME, and XP provide an SNMP agent. Network system manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

About the SNMP MIB

The MIB contains the essential objects that make up the *management information* for the device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

The MIB is structured as a hierarchical object tree divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:

- **System**. Contains general information about the device; for example, sysDescr (description), sysContact (person responsible), and sysName (device name).
- **Interfaces**. Contains information about network interfaces, such as Ethernet adapters or point-to-point links; for example, ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).
- **IP**. Contains information about the processing of IP packets, such as routing table information; for example, ipRouteDest (the destination) and ipRouteNextHop (the next hop of the route entry).
- Other groups provide information about the operation of a specific protocol for example, tcp, udp, icmp, snmp and egp.
- The **enterprise** group contains vendor-provided objects that are extensions of the MIB.

Each object of the MIB is identified by a numeric object identifier (OID) and each OID can be referred to by its text label. For example, the system group contains an object named sysDescr, which provides a description of the device. The sysDescr object has the following object identifier:

iso.org.dod.Internet.mgmt.mib.system.sysDescr

1.3.6.1.2.1.1.1

This object identifier would be 1.3.6.1.2.1.1.1 to which is appended an instance subidentifier of 0. That is, 1.3.6.1.2.1.1.1.0 identifies the only instance of sysDescr.

All of the MIB-II objects (for TCP/IP networks) are under the MIB sub ree (so all these objects will have an identifier that starts with 1.3.6.1.2.1).

For a detailed description of the MIB, see RFC 1213.

About SNMP Object Names and Identifiers

Each SNMP object has a name and numeric identifier. For example, in the *system* group, the network object named *SysDescr* with object identifier 1.3.6.1.2.1.1.1 contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the *ifPhysAddress* object, which has object identifier 1.3.6.1.2.1.2.2.1.6. In this case, you need to specify an instance number at the end of the object identifier (such as 1.3.6.1.2.1.2.2.1.6.1). If you do not specify an instance, it defaults to zero.

About SNMP Operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

- **Get**. Gets a specified SNMP object for a device.
- **Get next**. Gets the next object in a table or list.
- **Set**. Sets the value of an SNMP object on a device.
- **Trap**. Sends a message about an event (that occurs on the device) to the management application.

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using User Datagram Protocol (UDP). Trap messages, which are unsolicited messages from a device, are sent to port 162.

Note If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.

About SNMP Security

In Cisco netManager, credentials are used like passwords to limit access to a device's SNMP data. The credentials system supports SNMPv1 and SNMPv2.

Credentials are configured and stored in the Credentials Library (found on the web interface menu at **GO > Configure > Credentials Library**) and used in several places throughout the application. They can be assigned to devices in **Device Properties > Credentials**, or through the Credentials Bulk Field Change option.

Devices need SNMP credentials assigned to them before SNMP-based Active Monitors will work.

Using the Trap Definition Import Tool

This tool lets you import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your Cisco netManager MIB folder: `\Program Files\Ipswitch\WhatsUp\Data\Mibs`.

The SNMP Trap monitors that are listed are based on one of three things:

- **Passive monitors already in the database**. By default, the passive monitor database comes with a few of the most Common SNMP traps already in it.
- **Passive monitors automatically created by** the Cisco netManager **Trap Definition Import Tool**. Use the Trap Definition Import Tool to create SNMP Traps from MIB files stored in `\Program Files\Ipswitch\WhatsUp\Data\Mibs` folder.
- **Passive monitors that you define yourself.** You can do this either by copying and pasting actual trap information directly from your existing logs, or by browsing the MIB for OID values that you are interested in and adding the Generic type (Major) and Specific type (Minor) information if required.

To import SNMP trap definitions into the Passive Monitor Library:

Step 1 In the Cisco netManager console, click **Tools > Trap Definition Import Tool**. The Trap Definition Import Tool dialog opens.

Step 2 Click to select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog opens and provides a message about the import results. Traps that already exist in the database are not imported again.

Configuring Global SNMP Timeout and Retry Settings

If an SNMP query does not respond in time, Cisco netManager will time out. It will then retry contacting the device for as many times as listed under the snmpretries attribute in the configuration file. The timeout period is doubled for every subsequent retry. For example, if the timeout value is 4 seconds and the retries value is 3, Cisco netManager waits for 4 seconds before the first retry, 8 seconds before the second retry, and 16 seconds before the third retry. The SNMP timeout and retries are global settings.

Step 1 Select **GO > Configure > Default SNMP Timeout**.

Step 2 Enter the following:

- **Timeout** (milliseconds)—Enter the timeout in milliseconds (ms). If a device does not respond to the scan within this time, the scan continues to the next IP address. The timeout should be set to 300 ms or greater.
- **Retry count**—This is the number of times to try to discover a device at a given IP address, before continuing to the next device.