CHAPTER 18

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454.

For SNMP setup information, refer to the *Cisco ONS 15454 Procedure Guide*.

Chapter topics include:

- 18.1 SNMP Overview, page 18-1
- 18.2 SNMP Basic Components, page 18-2
- 18.3 SNMP Proxy Support Over Firewalls, page 18-3
- 18.4 SNMP Version Support, page 18-4
- 18.5 SNMP Management Information Bases, page 18-4
- 18.6 SNMP Traps, page 18-6
- 18.7 SNMP Community Names, page 18-8
- 18.8 SNMP Remote Network Monitoring, page 18-8

18.1 SNMP Overview

SNMP is an application-layer communication protocol that allows network devices to exchange management information. SNMP enables network administrators to manage network performance, find and solve network problems, and plan network growth.

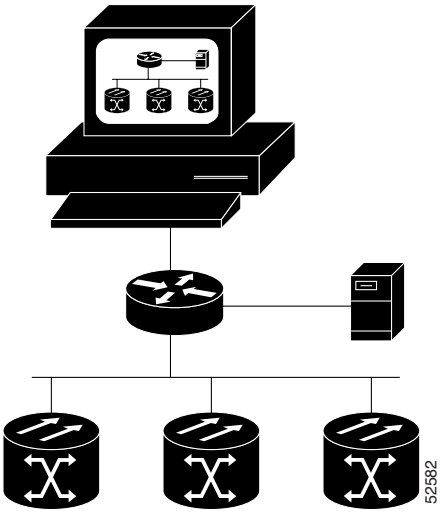
The ONS 15454 uses SNMP to provide asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows limited management of the ONS 15454 by a generic SNMP manager, for example, HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both versions share many features, but SNMPv2c includes additional protocol operations. This chapter describes both versions and explains how to configure SNMP on the ONS 15454.

Note The CERENT-MSDWDM-MIB.mib and CERENT-FC-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. However, the respective SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

Figure 18-1 illustrates a basic network managed by SNMP.

Figure 18-1 Basic Network Managed by SNMP

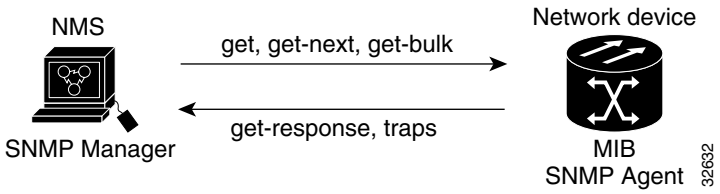


18.2 SNMP Basic Components

An SNMP-managed network consists of three primary components: managed devices, agents, and management systems. A managed device is a network node that contains an SNMP agent and resides on an SNMP-managed network. Managed devices collect and store management information and use SNMP to make this information available to management systems that use SNMP. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and network elements such as an ONS 15454.

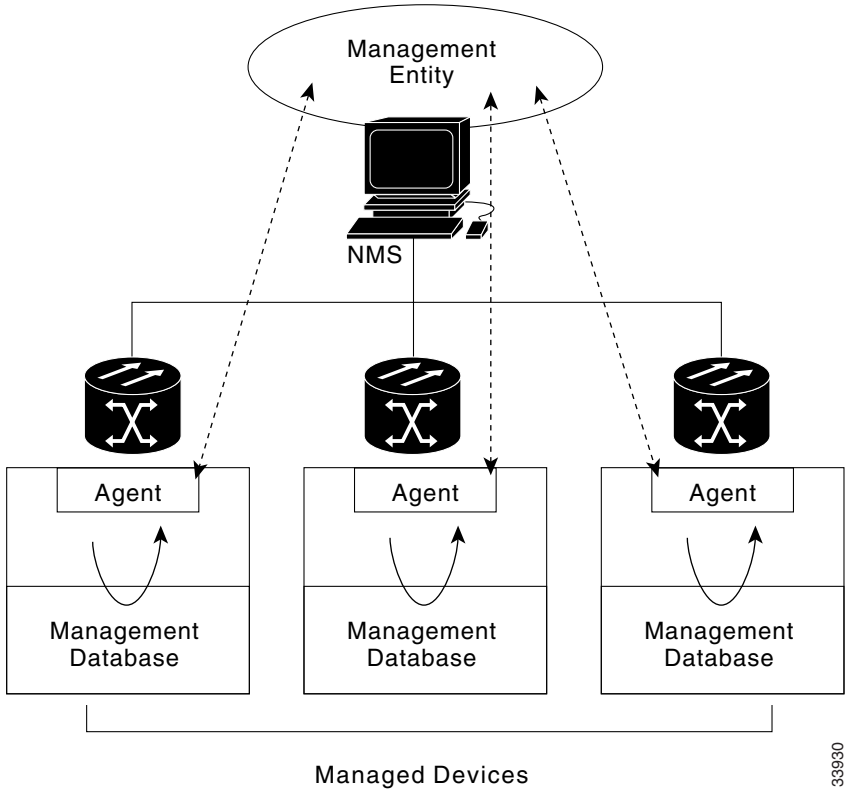
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for device parameter and network data. The agent can also send traps, which are notifications of certain events (such as changes), to the manager. Figure 18-2 on page 18-3 illustrates these SNMP operations.

Figure 18-2 SNMP Agent Gathering Data from a MIB and Sending Traps to the Manager



A management system such as HP OpenView executes applications that monitor and control managed devices. Management systems provide the bulk of the processing and memory resources required for network management. One or more management systems must exist on any managed network. Figure 18-3 illustrates the relationship between the three key SNMP components.

Figure 18-3 Example of the Primary SNMP Components



18.3 SNMP Proxy Support Over Firewalls

Firewalls, often used for isolating security risks inside networks or from outside, have traditionally prevented SNMP and other NMS monitoring and control applications from accessing NEs beyond a firewall.

Release 4.6 enables an application-level proxy at each firewall to transport SNMP protocol data units (PDU) between the NMS and NEs. This proxy, integrated into the firewall NE SNMP agent, exchanges requests and responses between the NMS and NEs and forwards NE autonomous messages to the NMS.

The usefulness of the proxy feature is that network operations centers (NOCs) can fetch performance monitoring data such as remote monitoring (RMON) statistics across the entire network with little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy interoperates with common NMS such as HP-OpenView. It is intended to be used with many NEs through a single NE gateway in a gateway network element-end network element (GNE-ENE) topology. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls.

For security reasons, the SNMP proxy feature must be turned on at all receiving and transmitting NEs to be enabled. For instructions to do this, refer to the *Cisco ONS 15454 Procedure Guide*. The feature does not interoperate with earlier ONS 15454 releases.

18.4 SNMP Version Support

The ONS 15454 supports SNMP v1 and SNMPv2c traps and get requests. The SNMP MIBs in the ONS 15454 define alarms, traps, and status. Through SNMP, NMS applications can query a management agent using a supported MIB. The functional entities include Ethernet switches and SONET multiplexers. Refer to the *Cisco ONS 15454 Procedure Guide* for procedures to set up or change SNMP settings.

18.5 SNMP Management Information Bases

A MIB is a hierarchically organized collection of information. It consists of managed objects and is identified by object identifiers. Network-management protocols, such as SNMP, are able to access to MIBs. The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP messages. Table 18-1 describes these messages.

Table 18-1 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.
set-request	Provides remote network monitoring (RMON) MIB.
trap	Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager.

A managed object (sometimes called a MIB object) is one of many specific characteristics of a managed device. Managed objects consist of one or more object instances (variables). Table 18-2 lists the IETF standard MIBs implemented in the ONS 15454 SNMP agent.

Table 18-2 IETF Standard MIBs Implemented in the ONS 15454 and ONS 15327 SNMP Agent

RFC[1] Number	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213	RFC1213-MIB-rfc1213.mib,	Management Information Base for Network
1907	SNMPV2-MIB-rfc1907.mib	Management of TCP/IP-based internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	OSPF Version 2 Management Information Base
1493	BRIDGE-MIB-rfc1493.mib	Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network (LAN) segments.)
2819	RMON-MIB-rfc2819.mib	Remote Network Monitoring Management Information Base
2737	ENTITY-MIB-rfc2737.mib	Entity MIB (Version 2)
2233	IF-MIB-rfc2233.mib	Interfaces Group MIB using SMIv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS3/E3 Interface Type
2558	SONET-MIB-rfc2558.mib	Definitions of Managed Objects for the SONET/SDH Interface Type
2674	P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions

1. RFC = Request for Comment

The ONS 15454 MIBs in Table 18-3 are included on the software CD that ships with the ONS 15454. Compile these MIBs in the order listed in Table 18-2 and then Table 18-3. If you do not follow the order, one or more MIB files might not compile.

Table 18-3 ONS Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib (for ONS 15454 only)
4	CERENT-GENERIC.mib (for ONS 15327 only)

Table 18-3 ONS Proprietary MIBs (continued)

MIB Number	Module Name
5	CISCO-SMI.mib
6	CISCO-VOA-MIB.mib
7	CERENT-MSDWDM-MIB.mib
8	CISCO-OPTICAL-MONITOR-MIB.mib
100	CERENT-FC-MIB.mib

If you cannot compile the ONS 15454 MIBs, call the Cisco Technical Assistance Center (Cisco TAC). Contact information for Cisco TAC is listed in the "About this Manual" section on page -xxxix.

18.6 SNMP Traps

The ONS 15454 can receive SNMP requests from a number of SNMP managers and send traps to 10 trap receivers. The ONS 15454 generates all alarms and events as SNMP traps. The ONS 15454 generates traps containing an object ID that uniquely identifies the alarm. An entity identifier uniquely identifies the entity that generated the alarm (slot, port, synchronous transport signal [STS], Virtual Tributary [VT], bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], and so on). The traps give the severity of the alarm (critical, major, minor, event, and so on) and indicate whether the alarm is service affecting or non-service affecting. The traps also contain a date/time stamp that shows the date and time the alarm occurred. The ONS 15454 also generates a trap for each alarm when the alarm condition clears. Each SNMP trap contains ten variable bindings, listed in Table 18-4.

Table 18-4 SNMPv2 Trap Variable Bindings

Number	ONS 15454 Name	ONS 15327 Name	Description
1	sysUpTime	sysUpTime	The first variable binding in the variable binding list of an SNMPv2-Trap-PDU.
2	snmpTrapOID	snmpTrapOID	The second variable binding in the variable binding list of an SNMPv2-Trap-PDU.
3	cerent454NodeTime	cerentGenericNodeTime	The time that an event occurred
4	cerent454AlarmState	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are minor, major, and critical. Service- affecting statuses are service-affecting and non-service affecting.
5	cerent454AlarmObjectType	cerentGenericAlarmObjectType	The entity type that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
6	cerent454AlarmObjectIndex	cerentGenericAlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of the objects in each table; if the alarm is interface related, this is the index of the interfaces in the interface table.

Table 18-4 SNMPv2 Trap Variable Bindings (continued)

Number	ONS 15454 Name	ONS 15327 Name	Description
7	cerent454AlarmSlotNumber	cerentGenericAlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
8	cerent454AlarmPortNumber	cerentGenericAlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
9	cerent454AlarmLineNumber	cerentGenericAlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
10	cerent454AlarmObjectName	cerentGenericAlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.

The ONS 15454 supports the generic and IETF traps listed in Table 18-5.

Table 18-5 Traps Supported in the ONS 15454

Trap	From RFC No. MIB	Description
coldStart	RFC1907-MIB	Agent up, cold start.
warmStart	RFC1907-MIB	Agent up, warm start.
authenticationFailure	RFC1907-MIB	Community string does not match.
newRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree.
topologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking.
entConfigChange	RFC2737/ ENTITY-MIB	The entLastChangeTime value has changed.
dsx1LineStatusChange	RFC2495/ DS1-MIB	A dsx1LineStatusChange trap is sent when the value of an instance of dsx1LineStatus changes. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (for example, a DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	A dsx3LineStatusLastChange trap is sent when the value of an instance of dsx3LineStatus changes. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (for example, a DS-1), no traps for the lower-level are sent.
risingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

18.7 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box in Cisco Transport Controller (CTC). In effect, SNMP considers any request valid that uses a community name matching a community name on the list of provisioned SNMP trap destinations. Otherwise, SNMP considers the request invalid and drops it.

If an SNMP request contains an invalid community name, the request silently drops and the MIB variable (snmpInBadCommunityNames) increments. All MIB variables managed by the agent grant access to all SNMP requests containing a validated community name.

18.8 SNMP Remote Network Monitoring

The ONS 15454 incorporates RMON to allow network operators to monitor the ONS 15454 Ethernet cards. This feature is not apparent to the typical CTC user, because RMON interoperates with an NMS. However, with CTC you can provision the RMON alarm thresholds. For the procedure, refer to the *Cisco ONS 15454 Procedure Guide*. CTC also monitors the five RMON groups implemented by the ONS 15454.

ONS 15454 RMON implementation is based on the IETF-standard MIB RFC2819. The ONS 15454 implements five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

18.8.1 Ethernet Statistics Group

The Ethernet Statistics group contains the basic statistics for each monitored subnetwork in a single table named etherstats. The group also contains 64-bit statistics in the etherStatsHighCapacityTable.

18.8.2 History Control Group

The History Control group defines sampling functions for one or more monitor interfaces. RFC 2819 defines the historyControlTable.

18.8.3 Ethernet History Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 2819, within the bounds of the historyControlTable. It also implements 64-bit Ethernet history in the etherHistoryHighCapacityTable.

18.8.4 Alarm Group

The Alarm group consists of a single alarm table. This table provides the network performance alarm thresholds for the network management application. With CTC, you can provision the thresholds in the table.

18.8.5 Event Group

The Event group consists of two tables, eventTable and logTable. The eventTable is read-only. The ONS 15454 implements the logTable as specified in RFC 2819.