SNMP

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

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

Chapter topics include:

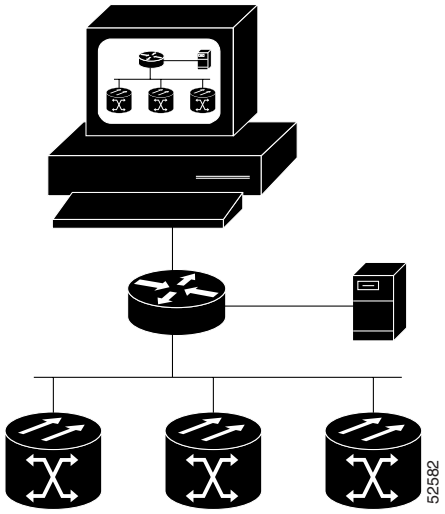
14.1 SNMP Overview

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. Figure 14-1 on page 14-2 illustrates a basic network managed by SNMP.

Figure 14-1 A Basic Network Managed by SNMP

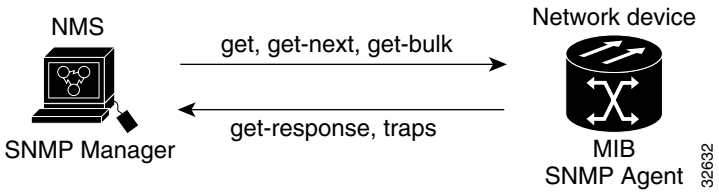


14.2 SNMP Basic Components

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.

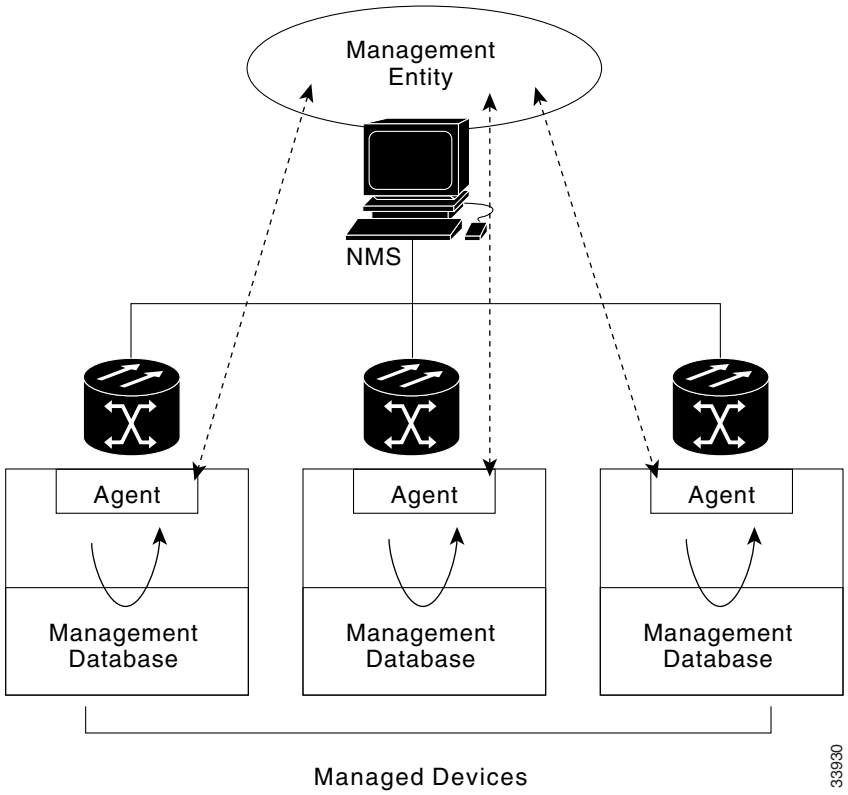
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for device parameter and network data. The agent can also send traps, which are notifications of certain events (such as changes), to the manager. Figure 14-2 illustrates these SNMP operations.

Figure 14-2 SNMP Agent Gathering Data from an 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 14-3 on page 14-3 illustrates the relationship between the three key SNMP components.

Figure 14-3 Example of the Primary SNMP Components



14.3 SNMP Support

The ONS 15454 supports SNMP v1 and v2c 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.

14.4 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 14-1 on page 14-4 describes these messages.

Table 14-1 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	The reply to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS
get-bulk-request	Similar to a get-next-request, but this operation fills the get-response with up to the max-repetition number of get-next interactions
set-request	Set-request processing is enabled to provide remote network monitoring (RMON) MIB.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that an event has occurred

A managed object (sometimes called a MIB object) is one of any specific characteristics of a managed device. Managed objects consist of one or more object instances (variables). Table 14-3 lists the IETF standard MIBs implemented in the ONS 15454 SNMP Agent.

The ONS 15454 MIBs in Table 14-2 are included on the software CD that ships with the ONS 15454. Compile these MIBs in the following order. If you do not follow the order, one or more MIB files might not compile.

Table 14-2 ONS 15454 Proprietary MIBs

MIB#	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)

If you cannot compile the ONS 15454 MIBs, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Table 14-3 IETF Standard MIBs Implemented in the ONS 15454 and ONS 15327 SNMP Agent

RFC#	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213	RFC1213-MIB-rfc1213.mib,	Management Information Base for Network Management of TCP/IP-based internets:MIB-II
1907	SNMPV2-MIB-rfc1907.mib	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	OSPF Version 2 Management Information Base

Table 14-3 IETF Standard MIBs Implemented in the ONS 15454 and ONS 15327 SNMP Agent (continued)

RFC#	Module Name	Title/Comments
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).
1757	RMON-MIB-rfc1757.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

14.5 SNMP Traps

The ONS 15454 can receive SNMP requests from a number of SNMP managers and send traps to eleven 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, STS, VT, BLSR, STP, etc.). The traps give the severity of the alarm (critical, major, minor, event, etc.) 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 eleven variable bindings listed in Table 14-4 for the ONS 15454. Table 14-5 on page 14-6 lists the variable bindings for the ONS 15327.

Table 14-4 SNMP Trap Variable Bindings for ONS 15454

Number	Name	Description
1	sysUpTime	The first variable binding in the variable binding list of an SNMPv2-Trap-PDU.
2	snmpTrapOID	The second variable binding in the variable binding list of an SNMPv2-Trap-PDU.
3	cerentNodeTime	This variable gives the time that an event occurred.

Table 14-4 SNMP Trap Variable Bindings for ONS 15454 (continued)

Number	Name	Description
4	cerent454AlarmState	This variable specifies alarm severity and service-affecting status. Severities are minor, major and critical. Service- affecting statuses are service-affecting and non-service affecting.
5	cerent454AlarmObjectType	This variable provides 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	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.
7	cerent454AlarmSlotNumber	This variable indicates 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	This variable provides 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	This variable provides the object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
10	cerent454AlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

Table 14-5 SNMP Trap Variable Bindings used in ONS 15327

Number	Name	Description
1	sysUpTime	This table holds all the currently raised alarms. When an alarm is raised, it appears as a new entry in the table. When an alarm is cleared, it is removed from the table and all the subsequent entries move up by one row.
2	snmpTrapID	This variable uniquely identifies each entry in an alarm table. When an alarm in the alarm table clears, the alarm indexes change for each alarm located subsequent to the cleared alarm.
3	cerentNodeTime	This variable gives the time that an event occurred.
4	cerentGenericAlarmState	This variable specifies alarm severity and service-affecting status. Severities are minor, major and critical. Service- affecting statuses are service-affecting and non-service affecting.

Table 14-5 SNMP Trap Variable Bindings used in ONS 15327 (continued)

Number	Name	Description
5	cerentGenericAlarmObjectType	This variable provides 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	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.
7	cerentGenericAlarmSlotNumber	This variable indicates the slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
8	cerentGenericAlarmPortNumber	This variable provides the port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
9	cerentGenericAlarmLineNumber	This variable provides the object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
10	cerentGenericAlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

The ONS 15454 supports the generic and IETF traps listed in Table 14-6.

Table 14-6 Traps Supported in the ONS 15454

Trap	From RFC# 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 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 (ex. DS-3), no traps for the DS-1 are sent.

Table 14-6 Traps Supported in the ONS 15454 (continued)

Trap	From RFC# MIB	Description
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 (ex. DS-1), no traps for the lower-level are sent.
risingAlarm	RFC1757/ 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	RFC1757/ 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.

14.6 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box in 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.

14.7 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, see 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 Request for Comment (RFC)1757. The ONS 15454 implements five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

14.7.1 Ethernet Statistics Group

The Ethernet Statistics group contains the basic statistics for each monitored subnetwork in a single table named etherstats.

14.7.2 History Control Group

The History Control group defines sampling functions for one or more monitor interfaces. RFC 1757 defines the historyControlTable.

14.7.3 Ethernet History Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 1757, within the bounds of the historyControlTable.

14.7.4 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.

14.7.5 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 1757.