SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15600.

For SNMP set up information, refer to the *Cisco ONS 15600 Procedure Guide*.

Chapter topics include:

- 5.1 SNMP Overview, page 5-1
- 5.2 Basic SNMP Components, page 5-2
- 5.3 SNMP External Interface Requirement, page 5-4
- 5.4 SNMP Version Support, page 5-4
- 5.5 SNMP Message Types, page 5-4
- 5.6 SNMP Management Information Bases, page 5-4
- 5.7 SNMP Trap Content, page 5-6
- 5.8 SNMP Community Names, page 5-13

5.1 SNMP Overview

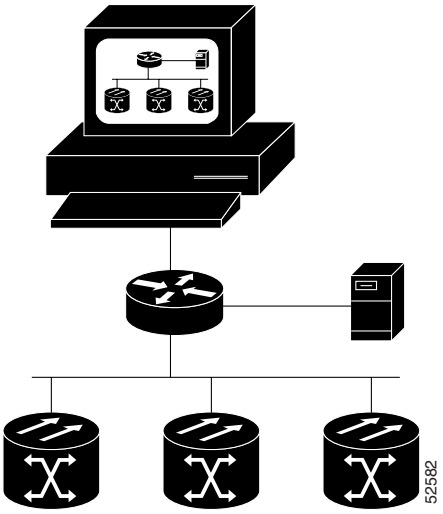
SNMP is an application-layer communication protocol that allows ONS 15600 network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

The ONS 15600 uses SNMP for 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 a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15600s support SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both of these versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15600.

Figure 5-1 illustrates the basic layout idea of an SNMP-managed network.

Figure 5-1 Basic Network Managed by SNMP

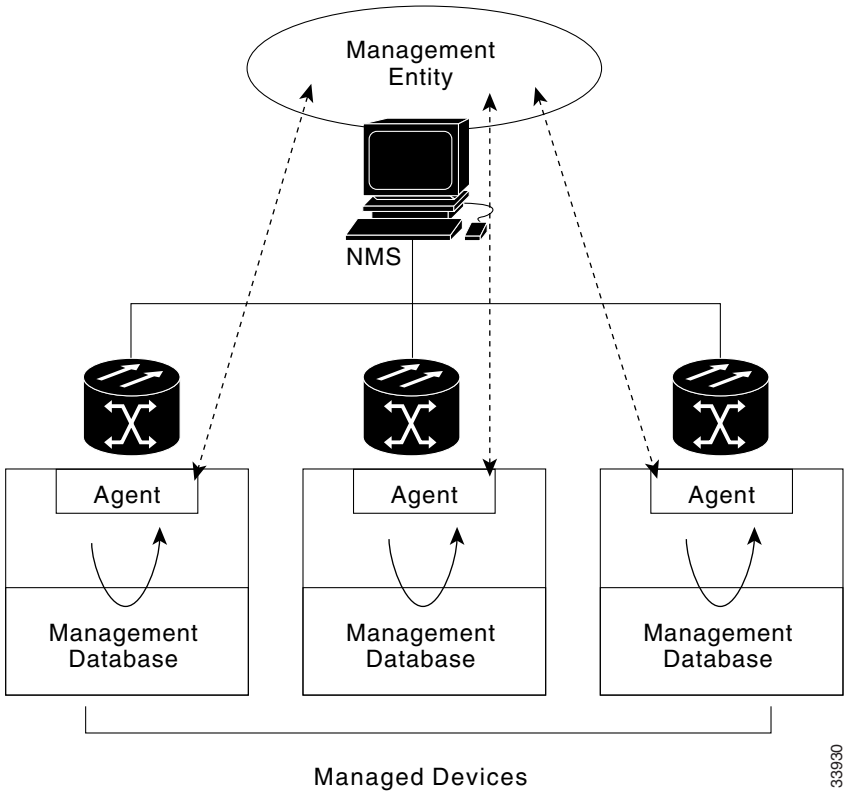


5.2 Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

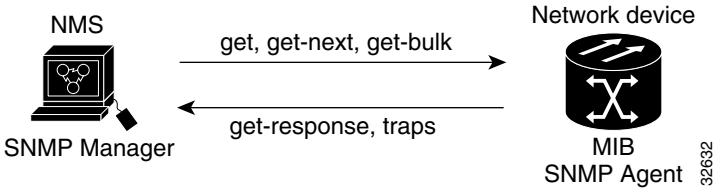
A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or more management systems. Figure 5-2 illustrates the relationship between the network manager, SNMP agent, and the managed devices.

Figure 5-2 Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. Figure 5-3 illustrates SNMP agent get-requests that transport data to the network management software.

Figure 5-3 Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from management information bases, or MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15600)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available via SNMP to other management systems having the same protocol compatibility.

5.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-part SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

5.4 SNMP Version Support

The ONS 15600 supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15600 SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SONET multiplexers using a supported MIB.

5.5 SNMP Message Types

The ONS 15600 SNMP agent communicates with an SNMP management application using SNMP messages. Table 5-1 describes these messages.

Table 5-1 ONS 15600 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.

5.6 SNMP Management Information Bases

Table 5-2 lists the IETF-standard MIBs implemented in the ONS 15600 SNMP agents.

First compile the MIBs in Table 5-2. Next, compile the mibs in the order given in Table 5-3.

Caution If you do not compile MIBs in the correct order, one or more might not compile correctly.

Table 5-2 IETF Standard MIBs Implemented in the ONS 15600 System

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 (not applicable to the ONS 15600)
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (not applicable to the ONS 15600)
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS3/E3 Interface Type (not applicable to the ONS 15600)
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
3273	HC-RMON-MIB	The MIB module for managing remote monitoring device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513 and RMON-2 MIB as specified in RFC 2021

1. RFC = Request for Comment

Each ONS system is shipped with a software CD containing applicable proprietary MIBs. The MIBs in Table 5-3 are used with the ONS 15600.

Table 5-3 ONS 15600 Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib
4	CERENT-GENERIC.mib

Note If you cannot compile the proprietary MIBs correctly, log into the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/techsupport or call Cisco TAC (800) 553-2447.

5.7 SNMP Trap Content

The ONS 15600 generates all alarms and events, such as raises and clears, as SNMP traps. These contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; synchronous transport signal [STS] and Virtual Tributary [VT]; bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], etc.).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service affecting).
- Date and time stamp showing when the alarm occurred.

5.7.1 Generic and IETF Traps

The ONS 15600 supports the generic IETF traps listed in Table 5-4.

Table 5-4 ONS 15600 Generic Traps

Trap	From RFC No. MIB	Description
coldStart	RFC1213-MIB	Agent up, cold start.
warmStart	RFC1213-MIB	Agent up, warm start.
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	RFC2037/ ENTITY-MIB	The entLastChangeTime value has changed.

Table 5-4 ONS 15600 Generic Traps (continued)

Trap	From RFC No. MIB	Description
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.

5.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. Variable bindings for the ONS 15600 are listed in Table 5-5. For each group (such as Group A), all traps within the group are associated with all of its variable bindings.

Table 5-5 15600 SNMPv2 Trap Variable Bindings

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
A	dsx1LineStatusChange (from RFC 2495)	(1)	dsx1LineStatus	This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information.
		(2)	dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent re-initialization, the value of this object is zero.
		(3)	cerentGenericNodeTime	The time that an event occurred.
		(4)	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)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
B	dsx3LineStatusChange (from RFC 2496)	(1)	dsx3LineStatus	This variable indicates the line status of the interface. It contains loopback state information and failure state information.
		(2)	dsx3LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then the value is zero.
		(3)	cerentGenericNodeTime	The time that an event occurred.
		(4)	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)	snmpTrapAddress	The address of the SNMP trap.
C	coldStart (from RFC 1907)	(1)	cerentGenericNodeTime	The time that an event occurred.
	warmStart (from RFC 1907)	(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
	newRoot (from RFC)	(3)	snmpTrapAddress	The address of the SNMP trap.
	topologyChange (from RFC)		—	—
	entConfigChange (from RFC 2737)		—	—
	authenticationFailure (from RFC 1907)		—	—

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
D1	risingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmRisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is greater than or equal to this threshold.
		(6)	cerentGenericNodeTime	The time that an event occurred.
		(7)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
D2	fallingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmFallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is less than or equal to this threshold.
		(6)	cerentGenericNodeTime	The time that an event occurred.
		(7)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
E	failureDetectedExternal ToTheNE (from CERENT-454-mib)	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerentGenericAlarmObject Type	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerentGenericAlarmObject Index	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerentGenericAlarmSlotNu mber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerentGenericAlarmPortN umber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerentGenericAlarmLineN umber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerentGenericAlarmObject Name	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerentGenericAlarmAdditi onalInfo	Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero.
		(10)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
F	performanceMonitorThresholdCrossingAlert (from CERENT-454-mib)	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerentGenericAlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerentGenericAlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerentGenericAlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerentGenericAlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerentGenericAlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerentGenericAlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerentGenericThresholdMonitorType	This object indicates the type of metric being monitored.
		(10)	cerentGenericThresholdLocation	Indicates whether the event occurred at the near- or far end.
		(11)	cerentGenericThresholdPeriod	Indicates the sampling interval period.
		(12)	cerentGenericThresholdSetValue	The value of this object is the threshold provisioned by the NMS.
		(13)	cerentGenericThresholdCurrentValue	
		(14)	cerentGenericThresholdDetectType	
		(15)	snmpTrapAddress	The address of the SNMP trap.

Table 5-5 15600 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
G	All other traps (from CERENT-454-MIB) not listed above	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerentGenericAlarmObject Type	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerentGenericAlarmObject Index	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerentGenericAalrmSlotNu mber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerentGenericAlarmPortN umber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerentGenericAlarmLineN umber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerentGenericAlarmObject Name	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	snmpTrapAddress	The address of the SNMP trap.

5.8 SNMP Community Names

Community names are used to group SNMP trap destinations. All ONS 15600 trap destinations can be provisioned as part of SNMP communities in Cisco Transport Controller (CTC). When community names are assigned to traps, the ONS 15600 treats the request as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.