CHAPTER 13

SNMP

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

For SNMP setup information, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

13.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15600 SDH 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. Up to 10 SNMP trap destinations and five concurrent Cisco Transport Controller (CTC) user sessions are allowed per node.

The ONS 15600 SDH 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 SDH read-only management. 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 15600 SDH supports SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c), and SNMP Version 3 (SNMPv3). As compared to SNMPv1, SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. SNMPv3 provides authentication, encryption, and message integrity and is more secure. This chapter describes the SNMP versions and describes the configuration parameters for the ONS 15600 SDH.

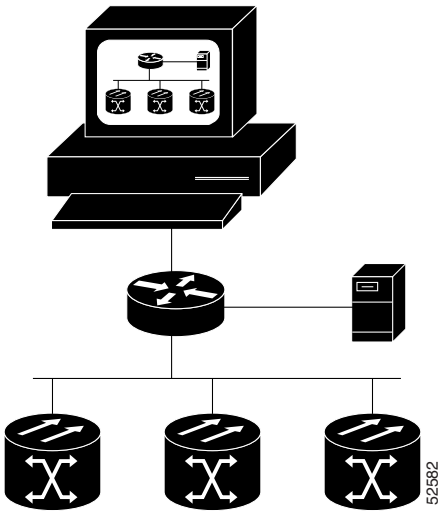
Note It is recommended that the SNMP Manager timeout value be set to 60 seconds. Under certain conditions, if this value is lower than the recommended time, the TCC card can reset. However, the response time depends on various parameters such as object being queried, complexity, and number of hops in the node, etc.

Note The CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. The 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.

Note When you switch multiplex-section shared protection ring (MS-SPRing) traffic from working to protect, the intermediate path performance monitoring (IPPM) TCAs and SDH near-end path PM values are available on the protect path. The protect TCA and PM values will not be available after the switch is cleared. Note that the protection channel access (PCA) TCAs and PM values are collected when the protect is not active.

Figure 13-1 illustrates the basic layout idea of an SNMP-managed network.

Figure 13-1 Basic Network Managed by SNMP

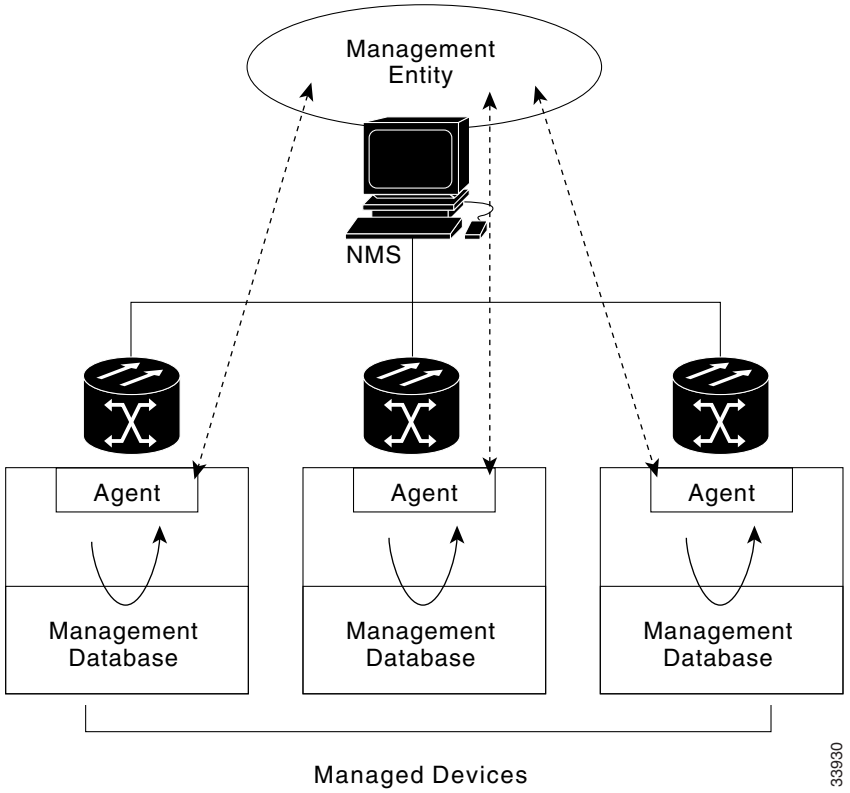


13.2 Basic SNMP Components

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

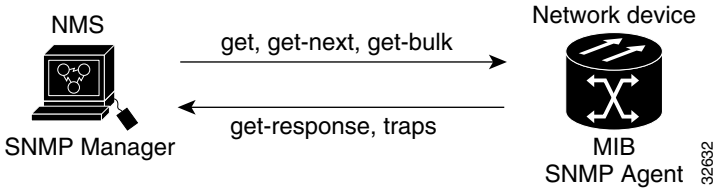
A network might be managed by one or several management systems. A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. Figure 13-2 illustrates the relationship between the network manager, SNMP agent, and the managed devices.

Figure 13-2 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 13-3 illustrates SNMP agent get-requests that transport data to the network management software.

Figure 13-3 Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from 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 SDH)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

13.3 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.

13.4 SNMP Version Support

The ONS 15600 SDH supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15600 SDH 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 SDH multiplexers using a supported MIB.

Note ONS 15600 SDH MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains three MIBs with 64-bit performance monitoring counters: CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib. The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

13.4.1 SNMPv3 Support

ONS 15600 SDH Software R9.0 and later supports SNMPv3 in addition to SNMPv1 and SNMPv2c. SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authentication and encryption packets over the network based on the User Based Security Model (USM) and the View-Based Access Control Model (VACM).

- **User-Based Security Model**—The User-Based Security Model (USM) uses the HMAC algorithm for generating keys for authentication and privacy. SNMPv3 authenticates data based on its origin, and ensures that the data is received intact. SNMPv1 and v2 authenticate data based on the plain text community string, which is less secure when compared to the user-based authentication model.

- **View-Based Access Control Model**—The view-based access control model controls the access to the managed objects. RFC 3415 defines the following five elements that VACM comprises:
  - Groups—A set of users on whose behalf the MIB objects can be accessed. Each user belongs to a group. The group defines the access policy, notifications that users can receive, and the security model and security level for the users.
  - Security level—The access rights of a group depend on the security level of the request.
  - Contexts—Define a named subset of the object instances in the MIB. MIB objects are grouped into collections with different access policies based on the MIB contexts.
  - MIB views—Define a set of managed objects as subtrees and families. A view is a collection or family of subtrees. Each subtree is included or excluded from the view.
  - Access policy—Access is determined by the identity of the user, security level, security model, context, and the type of access (read/write). The access policy defines what SNMP objects can be accessed for reading, writing, and creating.

  Access to information can be restricted based on these elements. Each view is created with different access control details. An operation is permitted or denied based on the access control details.

You can configure SNMPv3 on a node to allow SNMP get and set access to management information and configure a node to send SNMPv3 traps to trap destinations in a secure way. SNMPv3 can be configured in secure mode, non-secure mode, or disabled mode.

SNMP, when configured in secure mode, only allows SNMPv3 messages that have the authPriv security level. SNMP messages without authentication or privacy enabled are not allowed. When SNMP is configured in non-secure mode, it allows SNMPv1, SNMPv2, and SNMPv3 message types.

13.5 SNMP Message Types

The ONS 15600 SDH SNMP agent communicates with an SNMP management application using SNMP messages. Table 13-1 describes these messages.

Table 13-1 ONS 15600 SDH 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.

13.6 SNMP Management Information Bases

A managed object, sometimes called a MIB object, is one of many specific characteristics of a managed device. The MIB consists of hierarchically organized object instances (variables) that are accessed by network-management protocols such as SNMP. Section 13.6.1 lists the IETF standard MIBs implemented in the ONS 15600 SDH SNMP agent. Section 13.6.2 lists the proprietary MIBs implemented in the ONS 15600 SDH.

13.6.1 IETF-Standard MIBs for ONS 15600 SDH

Table 13-2 lists the IETF-standard MIBs implemented in the ONS 15600 SDH SNMP agents.

First compile the MIBs in Table 13-2. Next, compile the MIBs in the order given in Table 13-3.

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

Table 13-2 IETF Standard MIBs Implemented in the ONS 15600 SDH 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 Internet: 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 SNMPv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	(Not applicable to the ONS 15600 SDH) Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Not applicable to the ONS 15600 SDH
2496	DS3-MIB-rfc2496.mib	Not applicable to the ONS 15600 SDH
2558	SDH-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

Table 13-2 IETF Standard MIBs Implemented in the ONS 15600 SDH System (continued)

RFC[1] Number	Module Name	Title/Comments
3273	HC-RMON-MIB	The MIB module for managing RMON device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513, and RMON-2 MIB as specified in RFC 2021
	CISCO-DOT3-OAM-MIB	A Cisco proprietary MIB defined for IEEE 802.3ah ethernet OAM.
3413	SNMP-NOTIFICATION-MIB	Defines the MIB objects that provide mechanisms to remotely configure the parameters used by an SNMP entity for generating notifications.
3413	SNMP-TARGET-MIB	Defines the MIB objects that provide mechanisms to remotely configure the parameters that are used by an SNMP entity for generating SNMP messages.
3413	SNMP-PROXY-MIB	Defines MIB objects that provide mechanisms to remotely configure the parameters used by a proxy forwarding application.
3414	SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-Based Security Model.
3415	SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-Based Access Control Model for SNMP.

1. RFC = Request for Comment

13.6.2 Proprietary ONS 15600 SDH MIBs

Each ONS 15600 SDH is shipped with a software CD containing applicable proprietary MIBs. The MIBs in Table 13-3 lists the proprietary MIBs for the ONS 15600 SDH.

Table 13-3 ONS 15600 SDH Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-600.mib
4	CERENT-GENERIC.mib
5	CISCO-SMI.mib
6	CISCO-VOA-MIB.mib
7	CERENT-MSDWDM-MIB.mib
8	CERENT-OPTICAL-MONITOR-MIB.mib
9	CERENT-HC-RMON-MIB.mib
10	CERENT-ENVMON-MIB.mib
11	CERENT-GENERIC-PM-MIB.mib

Table 13-3 ONS 15600 SDH Proprietary MIBs (continued)

MIB Number	Module Name
12	BRIDGE-MIB.my
13	CERENT-454-MIB.mib
14	CERENT-ENVMON-MIB.mib
15	CERENT-FC-MIB.mib
16	CERENT-GENERIC-MIB.mib
17	CERENT-GENERIC-PM-MIB.mib
18	CERENT-GLOBAL-REGISTRY.mib
19	CERENT-HC-RMON-MIB.mib
20	CERENT-IF-EXT-MIB.mib
21	CERENT-MSDWDM-MIB.mib
22	CERENT-OPTICAL-MONITOR-MIB.mib
23	CERENT-TC.mib
24	CISCO-IGMP-SNOOPING-MIB.mib
25	CISCO-OPTICAL-MONITOR-MIB.mib
26	CISCO-OPTICAL-PATCH-MIB.mib
27	CISCO-SMI.mib
28	CISCO-VOA-MIB.mib
29	CISCO-VTP-MIB.mib
30	INET-ADDRESS-MIB.mib
31	OLD-CISCO-TCP-MIB.my
32	OLD-CISCO-TS-MIB.my
33	RFC1155-SMI.my
34	RFC1213-MIB.my
35	RFC1315-MIB.my
36	BGP4-MIB.my
37	CERENT-454-MIB.mib
38	CERENT-ENVMON-MIB.mib
39	CERENT-FC-MIB.mib
40	CERENT-GENERIC-MIB.mib
41	CERENT-GENERIC-PM-MIB.mib
42	CERENT-GLOBAL-REGISTRY.mib
43	CERENT-HC-RMON-MIB.mib
44	CERENT-IF-EXT-MIB.mib
45	CERENT-MSDWDM-MIB.mib
46	CERENT-OPTICAL-MONITOR-MIB.mib
47	CERENT-TC.mib

Table 13-3 ONS 15600 SDH Proprietary MIBs (continued)

MIB Number	Module Name
48	CISCO-CDP-MIB.my
49	CISCO-CLASS-BASED-QOS-MIB.my
50	CISCO-CONFIG-COPY-MIB.my
51	CISCO-CONFIG-MAN-MIB.my
52	CISCO-ENTITY-ASSET-MIB.my
53	CISCO-ENTITY-EXT-MIB.my
54	CISCO-ENTITY-VENDORTYPE-OID-MI
55	CISCO-FRAME-RELAY-MIB.my
56	CISCO-FTP-CLIENT-MIB.my
57	CISCO-HSRP-EXT-MIB.my
58	CISCO-HSRP-MIB.my
59	CISCO-IGMP-SNOOPING-MIB.mib
60	CISCO-IMAGE-MIB.my
61	CISCO-IP-STAT-MIB.my
62	CISCO-IPMROUTE-MIB.my
63	CISCO-MEMORY-POOL-MIB.my
64	CISCO-OPTICAL-MONITOR-MIB.mib
65	CISCO-OPTICAL-PATCH-MIB.mib
66	CISCO-PING-MIB.my
67	CISCO-PORT-QOS-MIB.my
68	CISCO-PROCESS-MIB.my
69	CISCO-PRODUCTS-MIB.my
70	CISCO-RTTMON-MIB.my
71	CISCO-SMI.mib
72	CISCO-SMI.my
73	CISCO-SYSLOG-MIB.my
74	CISCO-TC.my
75	CISCO-TCP-MIB.my
76	CISCO-VLAN-IFTABLE-RELATIONSHI
77	CISCO-VOA-MIB.mib
78	CISCO-VTP-MIB.mib
79	CISCO-VTP-MIB.my
80	ENTITY-MIB.my
81	ETHERLIKE-MIB.my
82	HC-PerfHist-TC-MIB.my
83	HC-RMON-MIB.my

Table 13-3 ONS 15600 SDH Proprietary MIBs (continued)

MIB Number	Module Name
84	HCNUM-TC.my
85	IANA-RTPROTO-MIB.my
86	IANAifType-MIB.my
87	IEEE-802DOT17-RPR-MIB.my
88	IEEE8023-LAG-MIB.my
89	IF-MIB.my
90	IGMP-MIB.my
91	INET-ADDRESS-MIB.my
92	IPMROUTE-STD-MIB.my
93	OSPF-MIB.my
94	PIM-MIB.my
95	RMON-MIB.my
96	RMON2-MIB.my
97	SNMP-FRAMEWORK-MIB.my
98	SNMP-NOTIFICATION-MIB.my
99	SNMP-TARGET-MIB.my
100	SNMPv2-MIB.my
101	SNMPv2-SMI.my
102	SNMPv2-TC.my
103	TCP-MIB.my
104	TOKEN-RING-RMON-MIB.my
105	UDP-MIB.my
106	BRIDGE-MIB-rfc1493.mib
107	DS1-MIB-rfc2495.mib
108	DS3-MIB-rfc2496.mib
109	ENTITY-MIB-rfc2737.mib
110	EtherLike-MIB-rfc2665.mib
111	HC-RMON-rfc3273.mib
112	HCNUM-TC.mib
113	IANAifType-MIB.mib
114	IF-MIB-rfc2233.mib
115	INET-ADDRESS-MIB.mib
116	P-BRIDGE-MIB-rfc2674.mib
117	PerfHist-TC-MIB-rfc2493.mib
118	Q-BRIDGE-MIB-rfc2674.mib
119	RFC1213-MIB-rfc1213.mib

Table 13-3 ONS 15600 SDH Proprietary MIBs (continued)

MIB Number	Module Name
120	RFC1253-MIB-rfc1253.mib
121	RIPv2-MIB-rfc1724.mib
122	RMON-MIB-rfc2819.mib
123	RMON2-MIB-rfc2021.mib
124	RMONTOK-rfc1513.mib
125	SNMP-FRAMEWORK-MIB-rfc2571.mib
126	SNMP-MPD-MIB.mib
127	SNMP-NOTIFY-MIB-rfc3413.mib
128	SNMP-PROXY-MIB-rfc3413.mib
129	SNMP-TARGET-MIB-rfc3413.mib
130	SNMP-USER-BASED-SM-MIB-rfc3414.mib
131	SNMP-VIEW-BASED-ACM-MIB-rfc3415.mib
132	SNMPv2-MIB-rfc1907.mib
133	SONET-MIB-rfc2558.mib

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

13.7 SNMP Trap Content

The ONS 15600 SDH uses SNMP traps to generate all alarms and events, such as raises and clears. The traps contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; virtual container [VC], or MS-SPRing).
- Severity and service effect of the alarm (Critical [CR], Major [MJ], Minor [MN], or event; Service-Affecting [SA] or Non Service Affecting [NSA]).
- Date and time stamp showing when the alarm occurred.

13.7.1 Generic and IETF Traps

Table 13-4 contains information about the generic threshold and performance monitoring MIBs that can be used to monitor any network element (NE) contained in the network. The ONS 15600 SDH supports the generic IETF traps listed in Table 13-4.

Table 13-4 Supported Generic IETF Traps

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

13.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. Variable bindings for the ONS 15600 SDH are listed in Table 13-5. For each group (such as Group A), all traps within the group are associated with all of the group's variable bindings.

Table 13-5 Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings

Group	Associated Trap Name(s)	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
A	dsx1LineStatusChange (from RFC 2495, not applicable to ONS 15600 SDH but applicable to other platforms)	(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 (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA).
		(5)	snmpTrapAddress	The address of the SNMP trap.

Table 13-5 Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Associated Trap Name(s)	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
B	dsx3LineStatusChange (from RFC 2496, not applicable to ONS 15600 SDH but applicable to other platforms)	(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 reinitialization 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 (MN), Major (MJ), and Critical (CR). 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 (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA).
	newRoot (from RFC)	(3)	snmpTrapAddress	The address of the SNMP trap (not supported for ONS 15600 SDH).
	topologyChange (from RFC)	—	—	(Not supported for ONS 15600 SDH)
	entConfigChange (from RFC 2737)	—	—	—
	authenticationFailure (from RFC 1907)	—	—	—

Table 13-5 Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Associated Trap Name(s)	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
D	failureDetectedExternal ToTheNE (from CERENT-600-mib)	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA).
		(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)	cerentGenericAlarmSlot Number	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerentGenericAlarmPort Number	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerentGenericAlarmLine Number	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)	cerentGenericAlarm AdditionalInfo	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 13-5 Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Associated Trap Name(s)	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
E	performanceMonitorThresholdCrossingAlert (from CERENT-600-mib)	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA).
		(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 13-5 Supported ONS 15600 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Associated Trap Name(s)	(Variable Binding Number)	SNMPv2 Variable Bindings	Description
F	All other traps (from CERENT-600-MIB) not listed above	(1)	cerentGenericNodeTime	The time that an event occurred.
		(2)	cerentGenericAlarmState	The alarm severity and service-affecting status. Severities are Minor (MN), Major (MJ), and Critical (CR). Service-affecting statuses are Service-Affecting (SA) and Non-Service Affecting (NSA).
		(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)	cerentGenericAalrmSlot Number	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerentGenericAlarmPort Number	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerentGenericAlarmLine Number	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.

13.8 SNMPv1/v2 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or outside networks. CTC enables network operations centers (NOCs) to access performance monitoring data such as remote monitoring (RMON) statistics or autonomous messages across firewalls by using an SNMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

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

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

13.9 SNMPv3 Proxy Configuration

The GNE can act as a proxy for the ENEs and forward SNMP requests to other SNMP entities (ENEs) irrespective of the types of objects that are accessed. For this, you need to configure two sets of users, one between the GNE and NMS, and the other between the GNE and ENE. In addition to forwarding requests from the NMS to the ENE, the GNE also forwards responses and traps from the ENE to the NMS.

The proxy forwarder application is defined in RFC 3413. Each entry in the Proxy Forwarder Table consists of the following parameters:

- Proxy Type—Defines the type of message that may be forwarded based on the translation parameters defined by this entry. If the Proxy Type is read or write, the proxy entry is used for forwarding SNMP requests and their response between the NMS and the ENE. If the Proxy Type is trap, the entry is used for forwarding SNMP traps from the ENE to the NMS.
- Context Engine ID/Context Name—Specifies the ENE to which the incoming requests should be forwarded or the ENE whose traps should be forwarded to the NMS by the GNE.
- TargetParamsIn—Points to the Target Params Table that specifies the GNE user who proxies on behalf of an ENE user. When the proxy type is read or write, TargetParamsIn specifies the GNE user who receives requests from an NMS, and forwards requests to the ENE. When the proxy type is trap, TargetParamsIn specifies the GNE user who receives notifications from the ENE and forwards them to the NMS. TargetParamsIn and the contextEngineID or the contextName columns are used to determine the row in the Proxy Forwarder Table that could be used for forwarding the received message.
- Single Target Out—Refers to the Target Address Table. After you select a row in the Proxy Forwarder Table for forwarding, this object is used to get the target address and the target parameters that are used for forwarding the request. This object is used for requests with proxy types read or write, which only requires one target.
- Multiple Target Out (Tag)—Refers to a group of entries in the Target Address Table. Notifications are forwarded using this tag. The Multiple Target Out tag is only relevant when proxy type is Trap and is used to send notifications to one or more NMSs.

13.10 Remote Monitoring

The ONS 15600 SDH incorporates RMON to allow network operators to monitor Ethernet facility performance and events. Software Releases 7.0 and later provide remote data communications channel (DCC) monitoring using 64-bit RMON over the DCC to gather historical and statistical Ethernet data. In general, the ONS 15600 SDH system RMON is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

Note Typical RMON operations, other than threshold provisioning, are invisible to the CTC user.

13.10.1 64-Bit RMON Monitoring over DCC

The ONS 15600 SDH DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system monitors Ethernet equipment history and statistics using RMON. RMON DCC monitoring for IP and Ethernet is used to check the health of remote DCC connections.

RMON DCC contains two MIBs for DCC interfaces. They are:

- cMediaIndependentTable—Standard, RFC 3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- cMediaIndependentHistoryTable—Proprietary MIB used to support history

13.10.1.1 Row Creation in MediaIndependentTable

The mediaIndependentTable is created automatically when the Ethernet facility is created on the ONS 15600 SDH ASAP card.

13.10.1.2 Row Creation in cMediaIndependentHistoryControlTable

SNMP row creation and deletion for the cMediaIndependentHistoryControlTable follows the same processes as for the MediaIndependentTable; only the variables differ.

In order to create a row, the SetRequest PDU should contain the following:

- cMediaIndependentHistoryControlDataSource and its desired value
- cMediaIndependentHistoryControlOwner and its desired value
- cMediaIndependentHistoryControlStatus with a value of createRequest (2)

13.10.2 HC-RMON-MIB Support

For the ONS 15600 SDH, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for this support. All of these elements are accessible by any third-party SNMP client should have the ability to upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

13.10.3 Ethernet Statistics RMON Group

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

13.10.3.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note EtherStatsTable entries are not preserved if the SNMP agent is restarted.

13.10.3.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15600 SDH Ethernet facilities.

13.10.3.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus value of 4 (invalid). The OID marks the row for deletion. If required, a deleted row can be recreated.

13.10.4 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

13.10.4.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 13-6 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods.

Table 13-6 RMON History Control Periods and History Categories

Sampling Periods (historyControlValue Variable)	Total Values, or Buckets (historyControl Variable)
15 minutes	32
24 hours	7
1 minute	60
60 minutes	24

13.10.4.2 Row Creation in historyControlTable

The etherStats table and historyControl table are automatically created when the Ethernet facility is created. History size is based upon the default history bucket located in Table 13-6.

13.10.4.3 Get Requests and GetNext Requests

These PDUs are not restricted.

13.10.4.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

13.10.4.5 Ethernet History RMON Group

The ONS 15600 SDH implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

13.10.4.6 64-Bit etherHistoryHighCapacityTable

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

13.10.5 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

13.10.5.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

13.10.5.2 Get Requests and GetNext Requests

These PDUs are not restricted.

13.10.5.3 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

13.10.6 Event RMON Group

The event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15600 SDH implements the logTable as specified in RFC 2819.

13.10.6.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always “log-and-trap (4)”.
- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be sent to all provisioned destinations.
- The eventOwner column value is always “monitor.”
- The eventStatus column value is always “valid(1)”.

13.10.6.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.