GLOSSARY

A

AAA Authentication, authorization, and accounting.

Alarm The word alarm represents a condition that causes a trap to be generated.

Alarm Severity Each alarm type defined by a vendor type and employed by the system is assigned an associated severity. See critical, major, minor and informational for severity types.

ATM Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

ATM-AAL5 ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented variable bit rate (VBR) services and is used predominantly for the transfer of classical IP over ATM and LAN emulation (LANE) traffic. AAL5 uses simple and efficient AAL (SEAL) and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

B

Bandwidth The difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.

Broadcast storm Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

C

CANA Cisco Assigned Numbers Authority.   The central clearing house for allocation of unique names and numbers that are embedded in Cisco software.

Columnar object One type of managed object that defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects, (for example, ifTable in the IF-MIB defines the interface).

Community Name Defines an access environment for a group of NMSs. NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

Critical alarm severity type Indicates a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week. For example, online insertion and removal of line cards or loss of signal failure when a physical port link is down.

D

Display String A printable ASCII string. It is typically a name or description. For example, the variable netConfigName provides the name of the network configuration file for a device.

DS0 Digital signal level 0. Framing specification used in transmitting digital signals at 64 Kbps. Twenty-four DS0s equal one DS1.

DS1 Digital signal level 1. Framing specification used in transmitting digital signals at 1.544 Mbps on a T1 facility.

DS3 Digital signal level 3. Framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility.

E

EHSA Enhanced High System Availability.

EMS Element Management System. An EMS manages a specific portion of the network. For example the SunNet Manager, an SNMP management application, is used to manage SNMP manageable elements. Element Managers may manage async lines, multiplexers, PABX's, proprietary systems or an application.

Encapsulation The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

F

FRU Field Replaceable Unit. Term applied to the Cisco 6400 components that can be replaced in the field, including the NLC, NSP, NRP, and PEM units, plus the blower fans.

Forwarding Process of sending a frame toward its ultimate destination by way of an internetworking device.

Frame Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment are also used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

G

Gb gigabit

Gbps gigabits per second

GB gigabyte

GBps gigabytes per second

H

HSRP Hot Standby Routing Protocol. Protocol used among a group of routers for selecting an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met.)

I

IEEE 802.2 IEEE LAN protocol that specifies an implementation of the LLC sublayer of the data link layer. IEEE 802.2 handles errors, framing, flow control, and the network layer (Layer 3) service interface. Used in IEEE 802.3 and IEEE 802.5 LANs. See also IEEE 802.3 and IEEE 802.5.

IEEE 802.3 IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet.

IEEE 802.5 IEEE LAN protocol that specifies an implementation of the physical layer and MAC sublayer of the data link layer. IEEE 802.5 uses token passing access at 4 or 16 Mbps over STP cabling and is similar to IBM Token Ring. See also Token Ring.

Info Notification about a condition that could lead to an impending problem or notification of an event that improves operation.

Informs Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

ifIndex Each row of the interfaces table has an associated number, called an ifIndex. You use the ifIndex number to get a specific instance of an interfaces group object. For example, ifInNUcastPkts.1 would find you the number of broadcast packets received on interface number one. You can then find the description of interface number one by looking at the object which holds the interface description (from MIB-II) ifDescr.

Integer A numeric value that can be an actual number. For example, the number of lost IP packets on an interface. It also can be a number that represents a nonnumeric value. For example, the variable tsLineType returns the type of terminal services line to the SNMP manager.

Interface Counters Interface management over SNMP is based on two tables: ifTable and its extension, ifXTable described in RFC1213/RFC2233. Interfaces can have several layers, depending on the media, and each sub-layer is represented by a separate row in the table. The relationship between the higher layer and lower layers is described in the ifStackTable.

The ifTable defines 32-bit counters for inbound and outbound octets (ifInOctets / ifOutOctets), packets (ifInUcastPkts / ifOutUcastPkts, ifInNUcastPkts / ifOutNUcastPkts), errors, and discards.

The ifXTable provides similar 64-bit counters, also called high capacity (HC) counters: ifHCInOctets / ifHCOutOctets, and ifHCInUcastPkts / ifHCOutUcastPkts.

Internetwork Collection of networks interconnected by routers and other devices that functions as a single network. Sometimes called an internet, which is not to be confused with the Internet.

Interoperability Ability of computing equipment manufactured by different vendors to communicate with one another successfully over a network.

IP Address The variable hostConfigAddr indicates the IP address of the host that provided the host configuration file for a device.

J

K

Keepalive message Message sent by one network device to inform another network device that the virtual circuit between the two is still active.

L

label A short, fixed-length identifier that is used to determine the forwarding of a packet.

LDP Label Distribution Protocol.

LSR Label Switching Router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

LSP Label Switched Path.

M

Major alarm severity type Used for hardware or software conditions. Indicates a serious disruption of service or the malfunctioning or failure of important hardware. Requires immediate attention and response of a technician to restore or maintain system stability. The urgency is less than in critical situations because of a lesser effect on service or system performance. For example, a minor alarm is generated if a secondary NSE-100 or NPE-G100 card fails or it is removed.

Minor alarm severity type Used for troubles that do not have a serious effect on service to customers or for alarms in hardware that are not essential to the operation of the system.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIB II MIB-II is the follow on to MIB-I which was the original standard SNMP MIB. MIB-II provided some much needed enhancements to MIB-I. MIB-II is very old, and most of it has been updated (that which has not is mostly obsolete). It includes objects that describe system related data, especially data related to a system’s interfaces.

MPLS Multiprotocol Label Switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS Interface An interface on which MPLS traffic is enabled. MPLS is the standardized version of Cisco original tag switching proposal. It uses a label forwarding paradigm (forward packets based on labels).

MTU Maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

N

NAS Network access server. Cisco platform or collection of platforms such as an AccessPath system which interfaces between the Internet and the circuit world (the PSTN).

NMS Network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

NHLFE Next Hop Label Forwarding Entry.

O

OID Object identifier. Values are defined in specific MIB modules. The Event MIB allows you or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, you or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and Boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

OIR Online Insertion and Removal.

P

PAP Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but identifies the remote end. The router or access server determines if that user is allowed access. PAP is supported only on PPP lines.

PEM Power Entry Module.

Polling Access method in which a primary network device inquires, in an orderly fashion, whether secondaries have data to transmit. The inquiry occurs in the form of a message to each secondary that gives the secondary the right to transmit.

PPP Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

Q

QoS Quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

RADIUS Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Read-only This variable can be used to monitor information only. For example, the locIPUnreach variable, whose access is read-only, indicates whether Internet Control Message Protocol (ICMP) packets concerning an unreachable address will be sent.

Read-write This variable can be used to monitor information and to set a new value for the variable. For example, the tsMsgSend variable, whose access is read-write, determines what action to take after a message has been sent.

The possible integer values for this variable follow:

1 = nothing

2 = reload

3 = message done

4 = abort

RFC Requests for Comments, started in 1969, form a series of notes about the Internet (originally the ARPANET). The notes discuss many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts, but also include meeting notes, opinions, and sometimes humor.

The RFC Editor is the publisher of RFCs and is responsible for the final editorial review of the documents. The RFC Editor also maintains a master file of RFCs, the RFC index, that you can search online here.

The specification documents of the Internet protocol suite, as defined by the Internet Engineering Task Force (IETF) and its steering group, the Internet Engineering Steering Group (IESG), are published as RFCs. Thus, the RFC publication process plays an important role in the Internet standards process. Go to the following URL for details:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios103/mib_doc/80516.htm#xtocid13

RMON The Remote Network Monitoring MIB is a SNMP MIB for remote management of networks. RMON is one of the many SNMP based MIBs that are IETF Standards. RMON allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

RSVP Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP depends on IPv4. Also known as Resource Reservation Setup Protocol.

S

Scalar Object One type of managed object which is a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB)

SNMPv1 The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings. SNMPv1 uses a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address Access Control List and password.

SNMPv2

The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.

SNMPv2c support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported:

- no such object exceptions
- no such instance exceptions
- end of MIB view exceptions

SNMPv3

SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:

- Message integrity—Ensuring that a packet has not been tampered with in transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMP Agent

A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent.

SNMP Manager

A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

SONET

Synchronous Optical Network. A physical layer interface standard for fiber optic transmission. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

T

TE

Traffic Engineered

Time Stamp

Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.

TLV

Type Length Value. Dynamic format for storing data in any order. Used by Cisco’s Generic ID PROM for storing asset information.

Traffic engineering tunnel
A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

Trap
An trap is an unsolicited (device initiated) message. The contents of the message might be simply informational, but it is mostly used to report real-time trap information. Since a trap is a UDP datagram, sole reliance upon them to inform you of network problems (i.e. passive network monitoring) is not wise. They can be used in conjunction with other SNMP mechanisms as in trap-directed polling or the SNMP inform mechanism can be used when a reliable fault reporting system is required.

Tunnel
A secure communication path between two peers, such as routers.

U

UBR
Unspecified bit rate. QOS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network, but there are no guarantees in terms of cell loss rate and delay. Compare with ABR (available bit rate), CBR, and VBR.

UDP
User Datagram Protocol. A connections, non-reliable IP based transport protocol.

V

VBR
Variable bit rate. QOS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QOS.

VRF
VPN Routing and Forwarding Tables.

W

Write-only
This variable can be used to set a new value for the variable only. For example, the writeMem variable, whose access is write-only, writes the current (running) router configuration into nonvolatile memory where it can be stored and retained even if the router is reloaded. If the value is set to 0, the writeMem variable erases the configuration memory