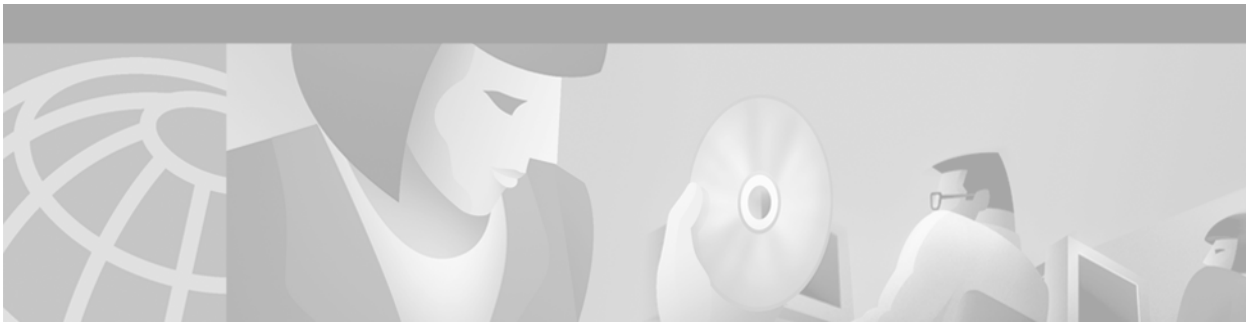


Overview of Basic SNMP Building Blocks

About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between a network management system (NMS), agents, and managed devices. SNMP uses the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

There are three versions of SNMP:

- **SNMP Version 1 (SNMPv1)**—The initial implementation of the SNMP protocol, which is described in RFC 1157 (http://www.ietf.org/rfc/rfc1157).
- **SNMP Version 2 (SNMPv2)**—An improved version of SNMPv1 that includes additional protocol operations. For the SNMPv2 Structure of Management Information (SMI), see RFC 1902 (http://www.ietf.org/rfc/rfc1902).
- **SNMP Version 3 (SNMPv3)**—SNMPv3 has yet to be standardized.

The case study in this guide describes how to create a dial NMS environment. To successfully manage the environment, you must be familiar with the SNMP feature set. The following NMS applications use SNMP to help manage the network devices in the case study:

- UCD-SNMP
- Multi-Router Traffic Grapher (MRTG)
- HP OpenView (HPOV)
- Cisco Works 2000 Resource Manager Essentials (CW2000 RME)

Table 1 Related SNMP Documentation and Sites

Site Description	URL
SNMP Technology TAC Page—Network design tips, implementation and operation guidelines, which are continually updated by Cisco TAC engineers.	http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:SNMP
The SimpleWeb—Public domain software packages, which are available on the Internet. Most of the software is a spin-off from SNMP related research.	http://penta.ufrgs.br/gereint/impl.htm
SNMP FAQ—Frequently asked questions about SNMP.	http://www.pantherdig.com/snmpfaq/ http://www.faqs.org/rfcs/rfc1382.html

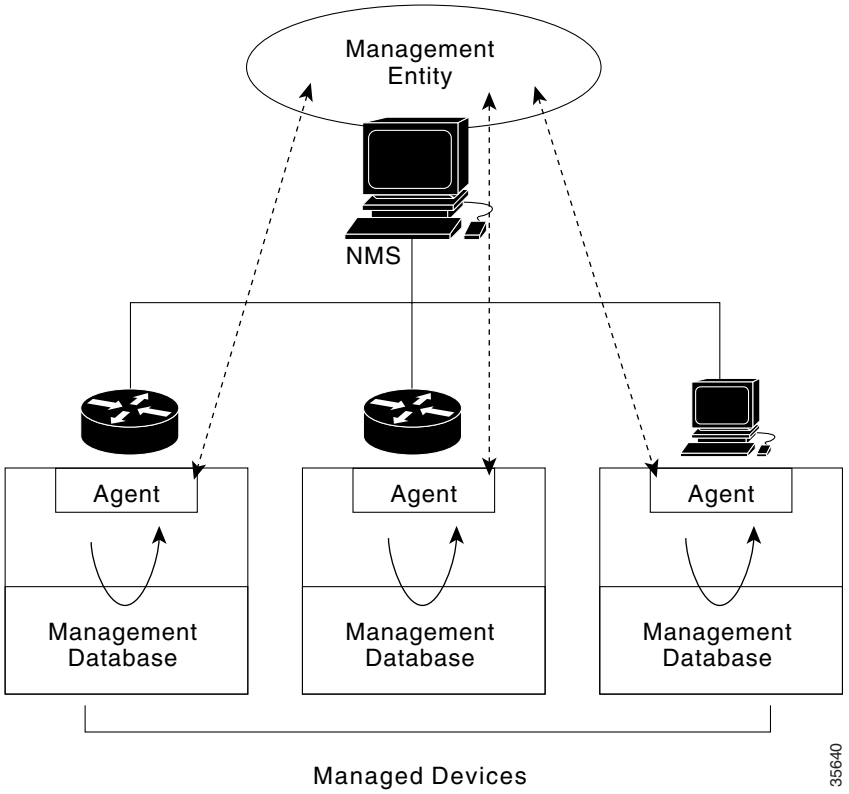
What are the Basic Components of SNMP?

An SNMP-managed network consists of three key components: managed devices, agents, and network management systems (NMS).

- **Managed devices**
  - Contain an SNMP agent and reside on a managed network.
  - Collect and store management information and make it available to NMS by using SNMP.
  - Include routers, access servers, switches, bridges, hubs, hosts, or printers.
- **Agent**—A network-management software module, such as the Cisco IOS software, that resides in a managed device. An agent has local knowledge of management information and makes that information available by using SNMP.
- **Network Management Systems (NMS)**—Run applications that monitor and control managed devices. NMS provide resources required for network management. In the case study, the NMS applications are:
  - UCD-SNMP
  - MRTG
  - HPOV
  - CW2000 RME

Figure 1 illustrates the relationship between the managed devices, the agent, and the NMS.

Figure 1 An SNMP-Managed Network



About Basic SNMP Message Types and Commands

There are three basic SNMP message types:

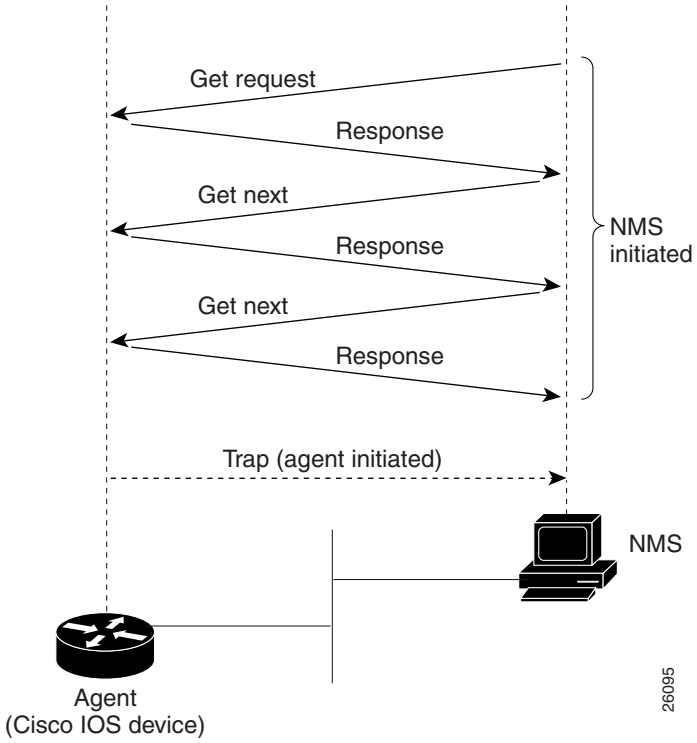
- **Get**—NMS-initiated requests used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.
- **Set**—NMS-initiated commands used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
- **Trap**—Agent-initiated messages sent from a managed device, which reports events to the NMS.

  The Cisco IOS generates SNMP traps for many distinct network conditions. Through SNMP traps, the Network Operations Center (NOC) is notified of network events, such as:

  - Link up/down changes
  - Configuration changes
  - Temperature thresholds
  - CPU overloads

Note For a list of Cisco-supported SNMP traps, go to http://www.cisco.com/public/mibs/traps/

Figure 2 SNMP Event Interactions Between the NMS and the Agent



What are SNMP MIBs?

A Management Information Base (MIB):

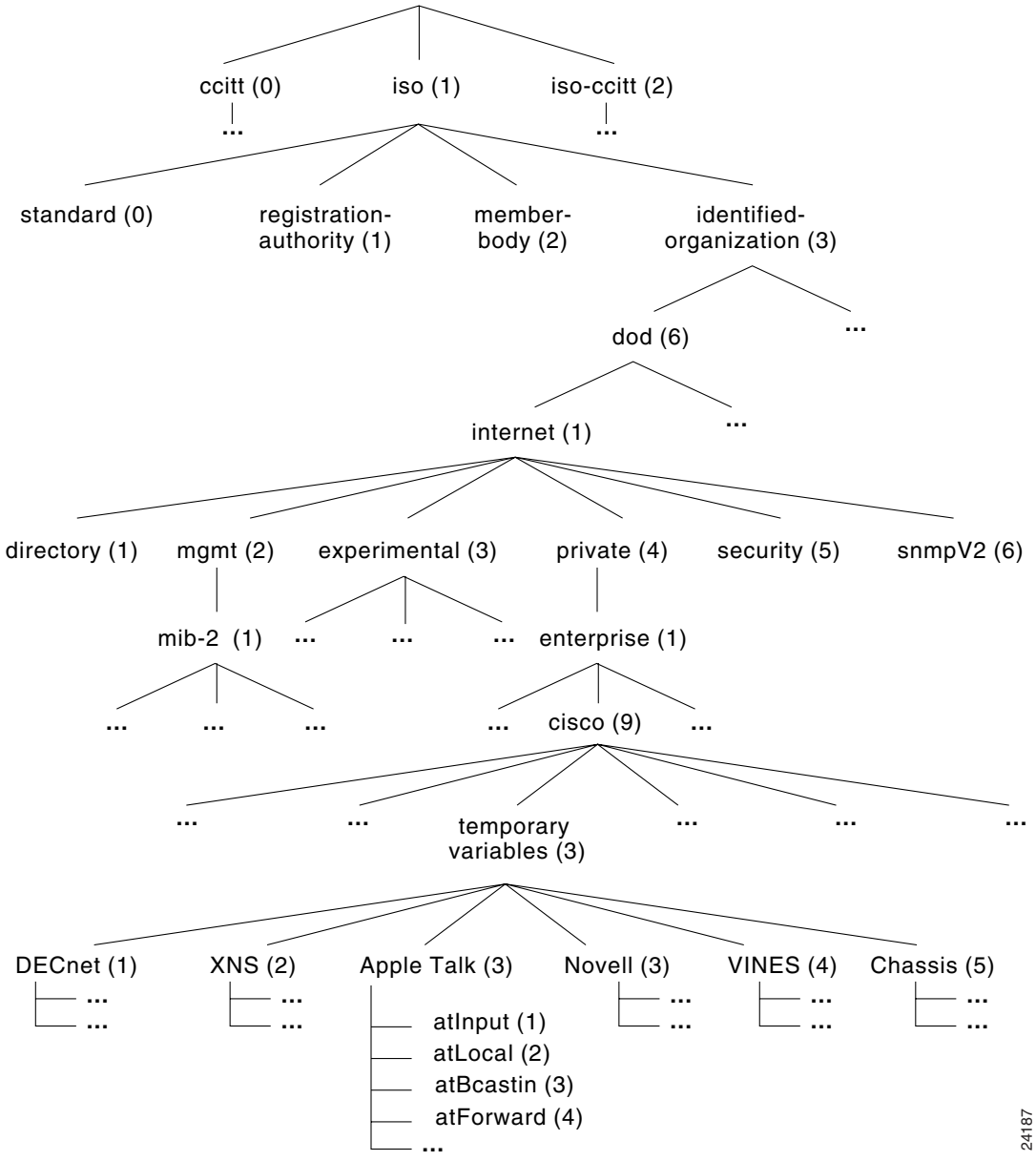
- Presents a collection of information that is organized hierarchically.
- Is accessed by using a network-management protocol, such as SNMP.
- References managed objects and object identifiers.

Managed object—A characteristic of a managed device. Managed objects reference one or more object instances (variables). Two types of managed objects exist:

- Scalar objects—Define a single object instance.
- Tabular objects—Define multiple-related object instances that are grouped together in MIB tables.

Object identifier (or object ID)—Identifies a managed object in the MIB hierarchy. The MIB hierarchy is depicted as a tree with a nameless root. The levels of the tree are assigned by different organizations and vendors.

Figure 3 The MIB Tree and Its Various Hierarchies



As shown in Figure 3, top-level MIB object IDs belong to different standards organizations while low-level object IDs are allocated by associated organizations. Vendors define private branches that include managed objects for products. Non standard MIBs are typically in the experimental branch.

A managed object has these unique identities:

- **The object name**—For example, iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput

  or

- **The equivalent object descriptor**—For example, 1.3.6.1.4.1.9.3.3.1.

SNMP must account for and adjust to incompatibilities between managed devices. Different computers use different data-representation techniques, which can compromise the ability of SNMP to exchange information between managed devices.

What is SNMPv1?

SNMPv1 is the initial implementation of the SNMP protocol and is described in RFC 1157 (http://www.ietf.org/rfc/rfc1157).

SNMPv1:

- Functions within the specifications of the Structure of Management Information (SMI).
- Operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX).
- Is the de facto network-management protocol in the Internet community.

The SMI defines the rules for describing management information by using Abstract Syntax Notation One (ASN.1). The SNMPv1 SMI is defined in RFC 1155 (http://www.ietf.org/rfc/rfc1155). The SMI makes three specifications:

- ASN.1 data types
- SMI-specific data types
- SNMP MIB tables

SNMPv1 and ASN1 Data Types

The SNMPv1 SMI specifies that all managed objects must have a subset of associated ASN.1 data types. Three ASN.1 data types are required:

- **Name**—Serves as the object identifier (object ID).
- **Syntax**—Defines the data type of the object (for example, integer or string). The SMI uses a subset of the ASN.1 syntax definitions.
- **Encoding**—Describes how information associated with a managed object is formatted as a series of data items for transmission over the network.

SNMPv1 and SMI-Specific Data Types

The SNMPv1 SMI specifies the use of many SMI-specific data types, which are divided into two categories:

- **Simple data types**—Including these three types:
  - Integers—A signed integer in the range of -2,147,483,648 to 2,147,483,647.
  - Octet strings—Ordered sequences of zero to 65,535 octets.
  - Object IDs— Come from the set of all object identifiers allocated according to the rules specified in ASN.1.

- **Application-wide data types**—Including these seven types:
  - Network addresses—Represent addresses from a protocol family. SNMPv1 supports only 32-bit IP addresses.
  - Counters—Nonnegative integers that increase until they reach a maximum value; then, the integers return to zero. In SNMPv1, a 32-bit counter size is specified.
  - Gauges—Nonnegative integers that can increase or decrease but retain the maximum value reached.
  - Time ticks—A hundredth of a second since some event.
  - Opaques—An arbitrary encoding that is used to pass arbitrary information strings that do not conform to the strict data typing used by the SMI.
  - Integers—Signed integer-valued information. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.
  - Unsigned integers—Unsigned integer-valued information that is useful when values are always nonnegative. This data type redefines the integer data type, which has arbitrary precision in ASN.1 but bounded precision in the SMI.

The SNMPv1 SMI defines structured tables that are used to group the instances of a tabular object (an object that contains multiple variables). Tables contain zero or more rows that are indexed to allow SNMP to retrieve or alter an entire row with a single **Get**, **GetNext**, or **Set** command.

SNMPv1 Protocol Operations

SNMP is a simple request-response protocol. The NMS issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations:

- **Get**—Used by the NMS to retrieve the value of one or more object instances from an agent. If the agent responding to the Get operation cannot provide values for all the object instances in a list, the agent does not provide any values.
- **GetNext**—Used by the NMS to retrieve the value of the next object instance in a table or list within an agent.
- **Set**—Used by the NMS to set the values of object instances within an agent.
- **Trap**—Used by agents to asynchronously inform the NMS of a significant event.

What is SNMPv2?

SNMPv2 is an improved version of SNMPv1. Originally, SNMPv2 was published as a set of proposed Internet standards in 1993; currently, it is a Draft Standard. As with SNMPv1, SNMPv2 functions within the specifications of the SMI. SNMPv2 offers many improvements to SNMPv1, including additional protocol operations.

SNMPv2 and SMI

The SMI defines the rules for describing management information by using ASN.1.

RFC 1902 (http://www.ietf.org/rfc/rfc1902) describes the SNMPv2 SMI and enhances the SNMPv1 SMI-specific data types by including:

- **Bit strings**—Comprise zero or more named bits that specify a value.
- **Network addresses**—Represent an address from a protocol family. SNMPv1 supports 32-bit IP addresses, but SNMPv2 can support other types of addresses too.
- **Counters**—Non-negative integers that increase until they reach a maximum value; then, the integers return to zero. In SNMPv1, a 32-bit counter size is specified. In SNMPv2, 32-bit and 64-bit counters are defined.

SMI Information Modules

The SNMPv2 SMI specifies information modules, which include a group of related definitions. Three types of SMI information modules exist:

- **MIB modules**—Contain definitions of interrelated managed objects.
- **Compliance statements**—Provide a systematic way to describe a group of managed objects that must conform to a standard.
- **Capability statements**—Used to indicate the precise level of support that an agent claims with respect to a MIB group. An NMS can adjust its behavior towards agents according to the capability statements associated with each agent.

SNMPv2 Protocol Operations

The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. SNMPv2, however, adds and enhances protocol operations. The SNMPv2 trap operation, for example, serves the same function as the one used in SNMPv1. However, a different message format is used.

SNMPv2 also defines two new protocol operations:

- **GetBulk**—Used by the NMS to efficiently retrieve large blocks of data, such as multiple rows in a table. GetBulk fills a response message with as much of the requested data as fits.
- **Inform**—Allows one NMS to send trap information to another NMS and receive a response. If the agent responding to GetBulk operations cannot provide values for all the variables in a list, the agent provides partial results.

About SNMP Management

SNMP is a distributed-management protocol. A system can operate exclusively as an NMS or an agent, or a system can perform the functions of both.

When a system operates as both an NMS and an agent, another NMS can require the system to:

- Query managed devices and provide a summary of the information learned.
- Report locally stored management information.

About SNMP Security

SNMP lacks authentication capabilities, which results in a variety of security threats:

- **Masquerading**—An unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity.
- **Modification of information**—An unauthorized entity attempting to alter a message generated by an authorized entity, so the message results in unauthorized accounting management or configuration management operations.
- **Message sequence and timing modifications**—Occurs when an unauthorized entity reorders, delays, or copies and later replays a message generated by an authorized entity.
- **Disclosure**—Results when an unauthorized entity extracts values stored in managed objects. The entity can also learn of notifiable events by monitoring exchanges between managers and agents.

Note Because SNMP does not implement authentication, many vendors do not implement **Set** operations, which reduce SNMP to a monitoring facility.