Net Management Chapter 4

Network protocols management

Assume that you are the network administrator of a network that is made up of several different types of devices, including workstations, routers, bridges, switches, and hubs. The operation of the network has been going on smoothly for some time, but then suddenly, the network begins to experience problems. It becomes sluggish, and users start calling you and complaining of poor network response times. Is there something you can do to monitor or analyze the network without leaving your office and running from room to room or building to building?

Of course, there is — **if all or most of the devices on the network support a network management protocol**. **A network management protocol facilitates the exchange of management information between network devices**. This information can be deployed to monitor network performance, find network problems, and as well solve those problems — all without having any network personnel physically touch the affected device.

Even though a number of different protocols exist to support network management, one protocol stands out as the simplest to operate, easiest to implement, and most widely used: **Simple Network Management Protocol**. Simple Network Management Protocol (SNMP) is an industry standard created by the Internet Engineering Task Force (IETF) and designed originally to manage Internet components, it is now also being used to manage wide area network and telecommunications systems. Certain weak points arose in the protocol and a version two has been developed and fielded, called SNMPv.2. Even this version has been subsequently upgraded to SNMPv.3. So, currently, SNMP is in its third version.

CMIP (Common Management Information Protocol) is another network managment protocol that has been developed for the OSI environment. It is more versatile but requires about five times the memory of SNMP. In the next sections, we are going to examine these network managment protocols

Simple Network Management Protocol (SNMP) - An Overview of SNMP.

SNMP is perhaps the dominant method for devices on a network to relay network management information to centralized management consoles that are designed to provide a comprehensive operational view of the network. Having come into existence in about 1990, literally thousands of SNMP systems have been deployed. The latest version of SNMP is v.3, which is described in RFC 3410, dated December 2002.

There are three components of the SNMP protocol:

- The management protocol itself
- The MIB (management information base)
- The SMI (structure management information)

Figure 21.5 (Freeman) depicts the typical client–server model. The client runs the *managing* system. It makes requests and is typically called the *Network Management System* (NMS) or *Network Operation Center* (NOC). The server is in the *managed* system. It executes requests and is called the *agent*.

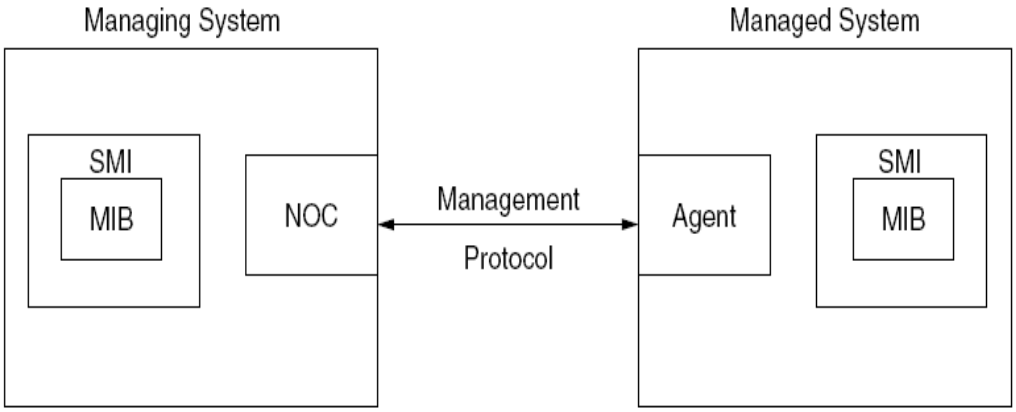

Figure 21.5 SNMP management architecture. SMI, structure of management information; NOC, network operations center. MIB, management information base.

SMI. Structure of Management Information (SMI) defines the general framework within which an MIB can be defined. In other words, SMI is the set of rules that define MIB objects, including generic types used to describe management information. The SNMP SMI uses a subset of Abstract Syntax Notation One (ASN.1) specification language that the ISO (International Standards Organization) developed for communications above the OSI Presentation Layer. Layer 7, for example, may use ASN.1 standards such as ITU-T Recs. X.400 and X.500. It was designed this way so that SNMP could be aligned with the OSI environment. The SMI organizes MIB objects into an upside-down tree for naming purposes.

Simple Network Management Protocol Version 1 (SNMPv1)

SNMP was developed for use as a network management tool for networks and internetworks operating TCP/IP. It has since been expanded for use in all types of networking environments. The term simple network management protocol (SNMP) is actually used to refer to a collection of specifications for network management that include the protocol itself, the definition of a database, and associated concepts.

Basic Concepts The model of network management that is used for SNMP

includes the following key elements:

- Management station, or manager
- Agent
- Management information base
- Network management protocol

The management station is generally a standalone device, but may be a capability implemented on a shared system. In either case, the management station serves as the interface for the human network manager into the network management system.The management station will have, at minimum,

- A set of management applications for data analysis, fault recovery, and so on
- An interface by which the network manager may monitor and control the network

- The capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network
- A database of network management information extracted from the databases of all the managed entities in the network

Only the last two elements are the subject of SNMP standardization.

The other active element in the network management system is the management agent. Key platforms, such as hosts, bridges, routers, and hubs, may be equipped with agent software so that they may be managed from a management station. The agent responds to requests for information from a management station, responds to requests for actions from the management station, and may asynchronously provide the management station with important but unsolicited information.

To manage resources in the network, each resource is represented as an object. An object is, essentially, a data variable that represents one aspect of the managed agent.The collection of objects is referred to as a management information base (MIB). The MIB functions as a collection of access points at the agent for the management station. These objects are standardized across systems of a particular class (e.g., bridges all support the same management objects). A management station carries out the monitoring function by retrieving the value of MIB objects. A management station can cause an action to take place at an agent or can change the configuration settings of an agent by modifying the value of specific variables.

The management station and agents are linked by a network management protocol. The protocol used for the management of TCP/IP networks is the Simple Network Management Protocol (SNMP). An enhanced version of SNMP, known as SNMPv2, is intended for both TCP/IP- and OSI-based networks. Each of these protocols includes the following key capabilities:

- Get: Enables the management station to retrieve the value of objects at the agent
- Set: Enables the management station to set the value of objects at the agent
- Notify: Enables an agent to send unsolicited notifications to the management station of significant events

In a traditional centralized network management scheme, one host in the configuration has the role of a network management station; there may be one or two other management stations in a backup role. The remainder of the devices on the network contain agent software and a MIB, to permit monitoring and control from the management station. As networks grow in size and traffic load, such a centralized system is unworkable. Too much burden is placed on the management station, and there is too much traffic, with reports from every single agent having to wend their way across the entire network to headquarters. In such circumstances, a decentralized, distributed approach works best (e.g., Figure 22.3- Stallings, 2007).

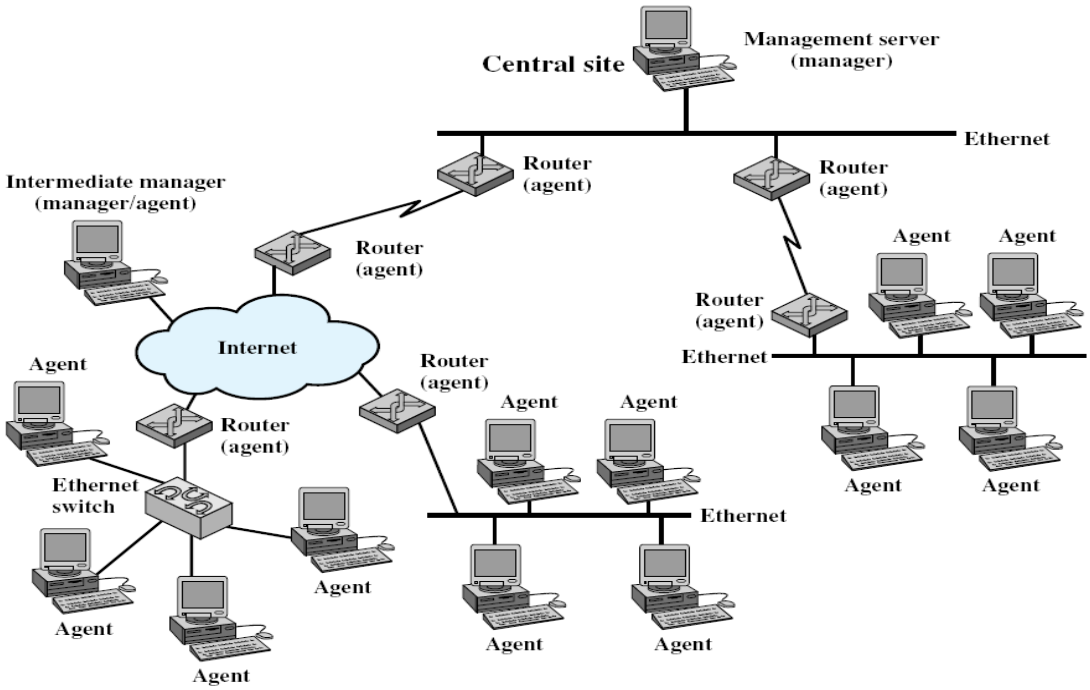

Figure 22.3 Example Distributed Network Management Configuration

In a decentralized network management scheme, there may be multiple top-level management stations, which might be referred to as management servers. Each such server might directly manage a portion of the total pool of agents. However, for many of the agents, the management server delegates responsibility to an intermediate manager. The intermediate manager plays the role of manager to monitor and control the agents under its responsibility. It also plays an agent role to provide information and accept control from a higher-level management server. This type of architecture spreads the processing burden and reduces total network traffic.

Network Management Protocol Architecture

SNMP is an applicationlevel protocol that is part of the TCP/IP protocol suite. It is intended to operate over the user datagram protocol (UDP). Figure 22.4 (Stallings) depicts the a classic configuration of protocols for SNMPv1.

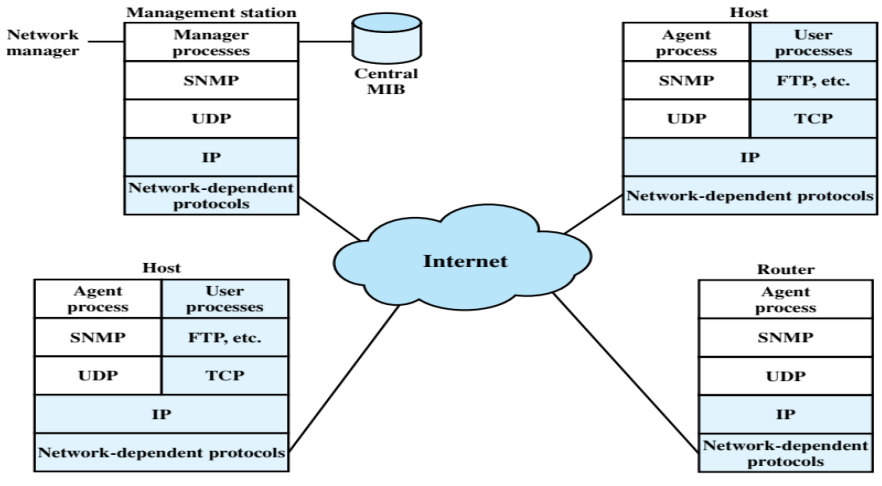

Figure 22.4 SNMPv1 Configuration

For a standalone management station, a manager process controls access to a central MIB at the management station and provides an interface to the network manager. The manager process achieves network management by using SNMP, which is deployed on top of UDP, IP, and the relevant networkdependent protocols for instance Ethernet, ATM, frame relay.

Each agent must equally implement SNMP, UDP, and IP. Furthermore, there is an agent process that interprets the SNMP messages and controls the agent's MIB. Thus, an agent device that supports other applications, such as FTP,TCP as well as UDP is required. In Figure 22.4, the shaded portions represent the operational environment: that is the environment which is to be managed.The unshaded portions provide support to the network management function.

On the other hand, Figure 22.5 (Stallings) provides an indepth representation of the protocol context of SNMP.

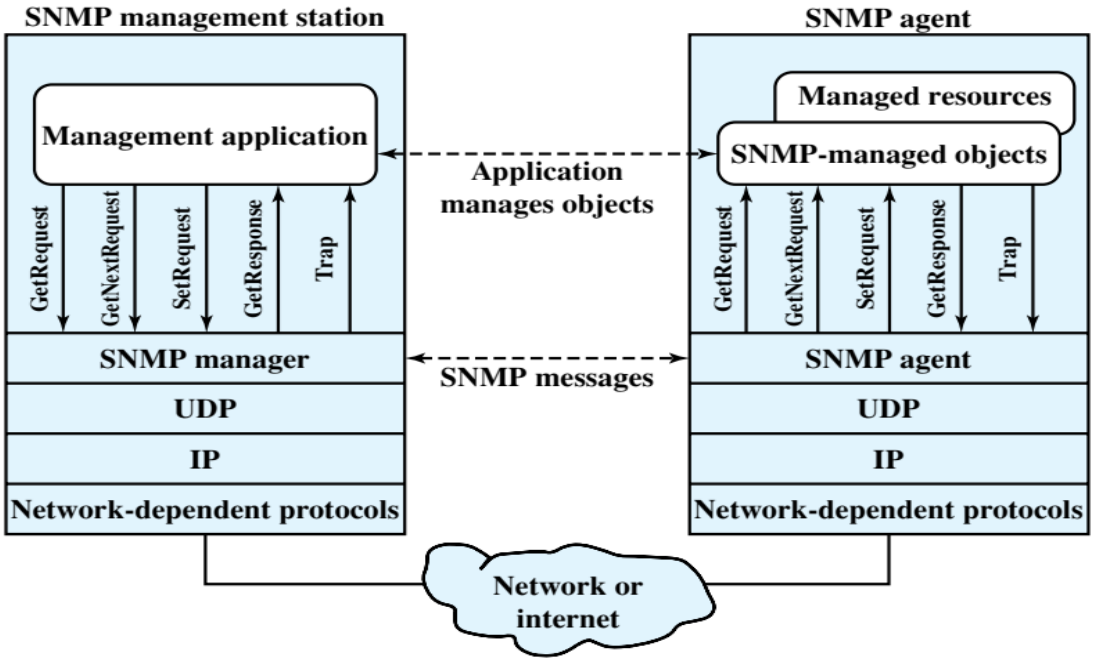

Figure 22.5 The Role of SNMPv1

From a management station, three types of SNMP messages are issued on behalf of a management applications: GetRequest, GetNextRequest, and SetRequest. The first two are two variations of the get function. All three messages are acknowledged by the agent in the form of a GetResponse message, which is passed up to the management application. Additionally, an agent may issue a trap message in response to an event that affects the MIB and the underlying managed resources. Management requests are sent to UDP port 161, while the agent sends traps to UDP port 162.

Since SNMP relies on UDP, which is a connectionless protocol, SNMP is itself connectionless. This implies that no dedicated connections are maintained between a management station and its agents. Rather, each exchange is a separate transaction between a management station and an agent.

Simple Network Management Protocol Version 2 (SNMPv2)

In August of 1988, the specification for SNMP was issued and quickly became the predominant network management standard. A couple of vendors offered standalone network management

workstations based on SNMP, and most vendors of bridges, routers, workstations, and PCs offer SNMP agent packages that allow their products to be managed by an SNMP management station.

As the name signifies, SNMP is a simple tool for network management. It defines a limited, easily implemented MIB of scalar variables and two dimensional tables, and it defines a streamlined protocol to enable a manager to get and set MIB variables and to enable an agent to issue unsolicited notifications, called *traps.* This simplicity is the strength of SNMP. SNMP is easily implemented and consumes modest processor and network resources. Besides, the structure of the protocol and the MIB are quite straightforward such that it is not difficult to accomplish interoperability among management stations and agent software from diverse vendors.

With its widespread use, the deficiencies of SNMP became increasingly apparent; these include both functional deficiencies and a lack of a security facility. As a result, an enhanced version, known as SNMPv2, was issued (RFCs 1901, 1905 through 1909, and 2578 through 2580). SNMPv2 has quickly gained support, and a number of vendors created products within months of the issuance of the standard.

The Elements of SNMPv2

As with SNMPv1, SNMPv2 provides a framework on which network management applications can be built.Those applications, such as fault management, performance monitoring, accounting, and so on, are outside the scope of the standard.

SNMPv2 provides the infrastructure for network management. Figure 22.6 is an example of a configuration that illustrates that infrastructure.

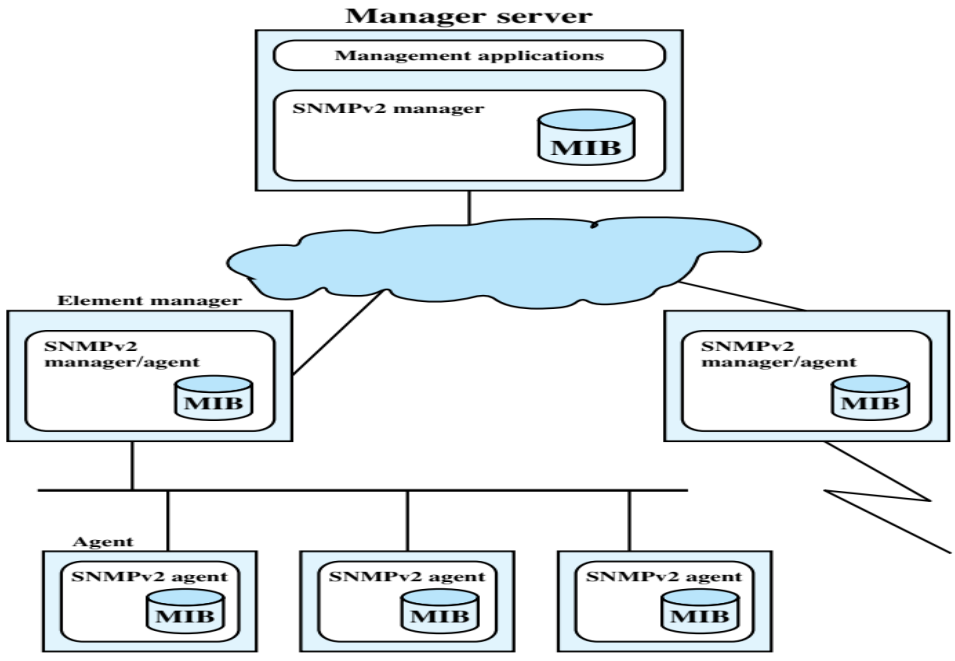

Figure 22.6 SNMPv2-Managed Configuration

The fundamental nature of SNMPv2 is a protocol that is used to exchange management information. Each "player" in the network management system maintains a local database of information relevant to network management, referred to as the MIB. The SNMPv2 standard defines the structure of this information and the permissible data types; this definition is known as

the structure of management information (SMI).We can think of this as the language for defining management information.The standard also provides a number of MIBs that are generally useful for network management. In addition, new MIBs may be defined by vendors and user groups.

At least one system in the configuration must be responsible for network management. It is here that any network management applications are hosted. There may be more than one of these management stations, to provide redundancy or simply to split up the duties in a large network. Most other systems act in the role of agent. An agent collects information locally and stores it for later access by a manager. The information includes data about the system itself and may also include traffic information for the network or networks to which the agent attaches.

SNMPv2 supports either a highly centralized network management strategy or a distributed one. In the latter case, some systems operate both in the role of manager and of agent. In its agent role, such a system will accept commands from a superior management system. Some of those commands relate to the local MIB at the agent. Other commands require the agent to act as a proxy for remote devices. In this case, the proxy agent assumes the role of manager to access information at a remote agent, and then assumes the role of an agent to pass that information on to a superior manager.

All of these exchanges take place using the SNMPv2 protocol, which is a simple request/response type of protocol. Normally, SNMPv2 is implemented on top of the user datagram protocol (UDP), which is part of the TCP/IP suite. Since SNMPv2 exchanges are in the nature of discrete request-response pairs, an ongoing reliable connection is not required.

Simple Network Management Protocol Version 3 (SNMPv3)

Many of the functional deficiencies of SNMP were addressed in SNMPv2. To correct the security deficiencies of SNMPv1/v2, SNMPv3 was issued as a set of Proposed Standards in January 1998 (currently RFCs 2570 through 2575). This set of documents does not provide a complete SNMP capability but rather defines an overall SNMP architecture and a set of security capabilities. These are intended to be used with the existing SNMPv2. SNMPv3 provides three important services: ***authentication, privacy, and access control***. The first two are part of the User-Based Security model (USM), and the last is defined in the View-Based Access Control Model (VACM). Security services are governed by the identity of the user requesting the service; this identity is expressed as a principal, which may be an individual or an application or a group of individuals or applications.

The authentication mechanism in USM assures that a received message was transmitted by the principal whose identifier appears as the source in the message header. This mechanism also assures that the message has not been altered in transit and has not been artificially delayed or replayed. The sending principal provides authentication by including a message authentication code with the SNMP message it is sending.This code is a function of the contents of the message, the identity of the sending and receiving parties, the time of transmission, and a secret key that should be known only to sender and receiver. The secret key must be set up outside of USM as a configuration function. That is, the configuration manager or network manager is responsible for distributing secret keys to be loaded into the databases of the various SNMP managers and agents. This can be done manually or using some form of secure data transfer outside of USM. When the receiving principal gets the message, it uses the same secret key to calculate the message authentication code once again. If the receiver's version of the code matches the value appended to the incoming

message, then the receiver knows that the message can only have originated from the authorized manager and that the message was not altered in transit. The shared secret key between sending and receiving parties must be preconfigured. The actual authentication code used is known as HMAC (*hash message autentication code*) , which is an Internet-standard authentication mechanism.

The privacy facility of USM enables managers and agents to encrypt messages. Again, manager principal and agent principal must share a secret key. In this case, if the two are configured to use the privacy facility, all traffic between them is encrypted using the Data Encryption Standard (DES). The sending principal encrypts the message using the DES algorithm and its secret key and sends the message to the receiving principal, which decrypts it using the DES algorithm and the same secret key.

The access control facility makes it possible to configure agents to provide different levels of access to the agent's MIB to different managers. An agent principal can restrict access to its MIB for a particular manager principal in two ways. First, it can restrict access to a certain portion of its MIB. For instance, an agent may restrict most manager parties to viewing performance-related statistics and only allow a single designated manager principal to view and update configuration parameters. Second, the agent can limit the operations that a manager can use on that portion of the MIB. For example, a particular manager principal could be limited to read-only access to a portion of an agent's MIB. The access control policy to be used by an agent for each manager must be preconfigured and basically consists of a table that detail the access privileges of the various authorized managers.