Overview of Network Management

This chapter will:

- Describe responsibilities of a network manager
- Define network management vocabulary
- Discuss network management principles
- Provide an example of network management implementation
- Identify new network management approaches
- Document the evolution of network management

As the title of the chapter suggests, we intend to give the reader an initial perspective on network management, why the need for network management has increased and how the concepts and implementations evolved. The reader is introduced to the general network management recipe with a step-by-step example. The example provides a framework that is filled in by the details given in later chapters.
2.1 WHAT IS NETWORK MANAGEMENT?

2.1.1 The Early Days

The job of the network manager in the early days of network management was mostly a local one. This was possible because connectivity of interest was mostly local, networks were not large and there were not that many networks. The network manager was primarily concerned with attaching PCs, workstations and a server to a LAN using Network Interface Cards (NICs), installing and configuring operating systems on PCs, workstations and servers, installing protocol stacks, configuring NIC I/O addresses, Direct Memory Access (DMA) addresses and Interrupts so as not to conflict with other NIC selections and configuring protocol stacks. The Ping application was usually employed to ensure that all devices on the network could communicate with one another. Ping sends a message to a device identified by its IP address and waits for a reply from that device.

To control access to information on a network server, the manager might write a script for the server that would be executed when the user at the PC or workstation logged on. The script would provide a uniform view to all users and only provide access to drives, folders or files that the user or group of users needed. The manager would perform coordination activities for the PCs and workstations. He or she would also install a print server application on the server or a stand-alone print server PC to manage the print jobs from each of the PCs and workstations. After all, sharing a printer was one of the main purposes of networks in the first place.

If the network were to be divided into segments or subnets, say one for each department in the organization, a bridge or router, respectively, would be used to connect them. If a subnet, the manager would configure a router table to enable connectivity according to network address, subnet address and subnet mask. Connectivity to remote networks required more router configuration and installation and maintenance of Wide Area Network (WAN) interfaces but this was not often required.

Next, it was necessary to install user applications on PCs and workstations and to ensure that they were interfacing correctly with the operating system. Then, application support programs (APIs) appeared on the scene to support easy access to the protocol stack and thereby the server. Sometimes such support programs were an integral part of the protocol stack and sometimes not. Given all of these duties, it was still possible for the network manager to accomplish them in a timely manner because the number of devices to be managed was small by today’s standards.

2.1.2 Maintenance

All of the duties mentioned above configure the initial state of the network only. Network performance is not optimized, there will be software and hardware failures and network resources will change. Thus, maintaining the network will demand much of the manager’s time. In addition, the manager is usually required to
make estimates of the network capacity that will be necessary to meet the growing demands of the organization and to find ways of providing that capacity within budget. One can add to this list of duties the need to account for usage of the network so that charges can be assessed and applied to cost centers. Then there was need for some minimal security. Configuration of user IDs, passwords and file rights or permissions, at a minimum, was needed to control access to private and perhaps sensitive information. Given all of these responsibilities, it was just possible for the network manager to keep up with his duties on a small LAN, if he or she worked extra hours.

Note
The words in bold in the paragraph above are also the formal names of the management categories that were defined by the International Organization for Standards [Ref 1].

The above paragraphs imply that the network manager does everything. Given the size of today’s enterprise networks, even with the software tools available, network “management” has divided into specialties. For example, one specialty includes administrative functions, such as backing up servers, adding and deleting users, installing operating systems and applications and maintaining security. These tasks are typically done by people who, for example, have Novell’s Certified NetWare Administrator (CNA) training or perhaps Microsoft’s Certified Professional (MCP) training.

Then there are the network engineers who may have received Novell’s Certified NetWare Engineer (CNE) or the Microsoft Certified System Engineer (MCSE) certificates that provide training in network technologies, network support, network service and network management. These people are responsible for the health of the network and its availability to the user. When we use the term network manager, we are thinking of those in the latter group who use the tools of network management to monitor and control the network resources. It should be noted that there is no clear line of distinction between the roles of network professionals and that it is not necessary to have a certificate to perform the necessary functions.

2.1.3 Information Explosion
As the information age came upon us and the number of Internet users grew exponentially, the number of users on organizational networks (Intranets) also grew along with the number of such networks. In addition, as knowledge became an essential ingredient for a company’s success, the demand for networks to provide intra-organizational connectivity as well as global access using the Internet, grew dramatically. With such growth came the demand for applications that would enable all this information to be used effectively.

Software that enabled applications to communicate with applications on other machines was now more in demand. (Enter client/server systems) [Ref 2].
Such software provided interfaces to protocol stacks and the network. These interfaces are analogous to the Application Program Interfaces (APIs) on the local computer that simplify access to the operating system and other local programs. You will often hear the term middleware used for programs that provide these interfaces.

2.1.4 Network-Based Management

The reader can easily see that the workload for the network manager had gotten so great that all of it could not be handled locally or be effective and timely. Also, as networks have grown larger and more complicated, many other demands on the network manager have arisen. The network manager needed to find more efficient ways to determine and control the state of network. The Simple Network Management Protocol (SNMP) [Ref 3-8], the Management Information Base (MIBs) [Ref 9-11] and network management systems (NMS) were developed that could be used by the network manager to remotely control values of device parameters. For remote network traffic monitoring, the Remote Monitor (RMON1) standard [Ref 12-14] was later added. This standard allowed the manager to access the agent on a “probe” that captured traffic on the segment to which it was attached and analyze the statistics of that traffic. The long-term goal of network management is automatic detection of potential network problems and correction of these problems before they become network failure points. A modern example of this approach is discussed in Appendix E.

Some of the references listed above are called Requests for Comments (RFCs). If the reader is not familiar with RFCs, it is important to know that these are the “Proposed Standards” for the Internet community in the United States. All RFCs are available on the Internet. Yahoo provides a number of ways to access them. Our preference from Yahoo is [Ref 15]. [Ref 16] is equivalent and provides other information about the Internet Engineering Task Force (IETF) that oversees Internet standards development. In both of these references, the RFCs are hyperlinked for rapid access. The primary body of non-proprietary networking knowledge consists of the IETF RFCs and the IEEE and ISO standards.

2.2 SOME NETWORK MANAGEMENT VOCABULARY

Network management today is mostly a combination of local and remote configuration and management with software. Remote network management is accomplished when one computer is used to monitor, access and control the configuration of other devices on the network. Figure 2.1 shows a simple network management environment.

The managing device is called a Management Station and the managed device is called a Management Agent. In this example, the station and agent are using the Public Switched Telephone Network (PSTN) to communicate. A management agent hosts software that provides access to information about the device that is hosting it. A management station hosts management software called the Network
Management System (NMS). The NMS consists of applications that enable the station to access, display and analyze the information provided by the agent. The management agent can be a computer, as shown in Figure 2.1, or another device, such as a hub, router or switch. Figure 2.2 depicts management terminology and functionality in more detail.

Figure 2.2 Protocol Stacks on the Management Station and the Management Agent
If the terminology is not clear at this time, don’t worry, we will come back to it often. The terminology we use is that defined in the Open Systems Interconnection (OSI) Reference Model specified by the International Organization for Standards (ISO) [Ref 1]. ISO Standards can be obtained from the Website of the American National Standards Institute (ANSI) given in [Ref 17] by clicking on the “Standards Information” button. Also, there are many standards that are published by the International Telecommunications Union (ITU) that are relevant. For example, the standard that we refer to as [Ref 1] was originally an ITU standard with the title X.200. It was initiated by the ITU-T technical committee that was originally the International Consultative Committee for Telegraphy and Telephony (CCITT), a French standards organization. To access the ITU-T Standards (called Recommendations) go to [Ref 18].

Figure 2.2 shows flow of network management information between a Management Station and a Management Agent. To make this happen, two or more software modules are added to both the Management Station and the Management Agent. One of these is the program that enables transport of management information between two devices. This program implements the network management protocol. SNMP is an example of a network management protocol.

### Note

There are distinctions between modules, programs and processes that are not important to us in the context of this book. A program is executable code. A process is a program that is active. A module is code that may not be executable by itself.

Another program added is called a **management process** on the Management Station and an **agent process** on the Management Agent. The management process services management application programs and provides an interface to the network management protocol, e.g., SNMP. The agent process is an integrator of processes (called subagents) that access information requested by a network management application and also serves as an interface to the network management protocol. An overview of what agent code embodies and its role as integrator can be found in [Ref 9].

A management application is a readily available application that you buy from a vendor. A collection of management applications is typically called a Network Management System (NMS). The agent process can run on any device such as a PC, workstation, server, router, hub, and switch. The agent process collects the values of a specified set of variables when a request is made by the Management Station. The virtual store of such values is called the Management Information Base (MIB). The MIB is called a virtual store because the values are actually maintained by the managed sub-systems of the device [Ref 9]. The management application program queries the agent’s MIB, obtains the results and displays them in readable form on the management station.
The following are the basic steps that take place when a management application wishes to obtain the value of a MIB variable on a Management Agent. Figure 2.2 is the software architecture that implements these steps.

1. A management application belonging to the NMS calls for the service of the management process.
2. The management process calls the program that implements the network management protocol, e.g., SNMP.
3. The network management protocol implementation constructs a request packet. This packet is embedded in a frame constructed using the protocol stack. The frame is sent to the program on the Management Agent that implements the network management protocol, e.g. SNMP. In SNMP, a typical request packet is called a Get-Request packet.
4. The implementation of the network management protocol on the Management Agent causes the request packet to be passed to the agent process.
5. The agent process accesses the value of the requested variable (perhaps with the help of a subagent) and passes it to the program that implements the network management protocol.
6. The network management protocol constructs the response packet that is embedded in the frame constructed by the protocol stack and the frame is sent to the Management Station. In SNMP, the response packet is called a Get-Response packet.
7. At the management station, the program that implements the network management protocol receives the response packet. Implementation of this protocol causes the response packet to be passed to the management process.
8. The management process either passes the requested value to the application program that displays it, perhaps using a Graphical User Interface (GUI), or stores it in memory for later retrieval.

Implementation of these steps constitutes the overhead that is incurred when network management over a network is implemented. This overhead includes, for example, the number of CPU cycles used by the management application program and the network management protocol in constructing a request packet and the number of control bytes supplied by the protocol stack layers that are necessary to ensure that the packet gets to the port of the processing module. In addition, storage used on management stations and management agents may be significant for large networks. It is convenient to have a dedicated Management Station on the network so that management processing does not interfere with other processing. Beyond these overhead considerations, the network manager has to be concerned about the amount of traffic being generated by network management packets. Too much network management traffic creates a new problem. There is always a trade-off to be defined.
The diagram in Figure 2.2 shows OSI Reference Model protocol stacks on the Management Station and the Management Agent. As we discussed in Chapter 1, there are seven layers in the OSI Reference Model protocol stack. The top layer is the Application layer. It contains the network management protocol, e.g., SNMP, and the agent or management processes. The Application layer will also contain other protocols and service processes, e.g., FTP, HTTP, SMTP. They are not relevant for this discussion and thus have not been shown for clarity. We are also not concerned at this time with the necessary functions that are performed by lower layers of the protocol stack that were discussed in Chapter 1.

2.4 ADDITIONAL NETWORK MANAGEMENT PROTOCOL CAPABILITIES

Network management protocols can construct requests for multiple values in a single message. The agent process retrieves each value and puts them in the Get-Response packet in the order in which they were requested. Accessing multiple values in one Get-Request packet speeds up the access process. In addition, there are commands that make it possible to traverse the management information data structure (MIB) on the Management Agent in logical order. For SNMP, this is accomplished with the Get-Next-Request command. These commands and their implementation will be examined in detail in Chapter 6: SNMP.

Network management protocols also enable the Management Agent to send unsolicited messages to the Management Station. These messages, called traps, are sent, for example, if a device goes from the powered-up to the powered-down state and when there is a Get-Request that does not contain the correct community name, the SNMP password. There are many other trap messages that are used, as we will see.

In addition to accessing information from standard network devices such as computers, routers and switches, information can also be accessed from other network devices called probes or remote monitors (RMON). The use of the words remote monitor may seem redundant since most network monitoring is of a remote device. However, remote monitoring and the RMON standard refer to monitoring activity (traffic) on a network segment, not a particular device. Thus, the Management Agent is remote from (not a part of) the devices it is monitoring. A remote monitor can be configured to capture and store all or selected groups of frames that it receives on the network segment to which it is attached. Thus, remote monitors provide information about traffic between devices on a network segment. Such information includes, among other things, hardware and network addresses of source and destination devices, the protocols that are being used and statistics about usage of the segment by specific devices.

The Management Station accesses information captured by the remote monitor using the procedures described above in steps 1–8. It also may, automatically poll the monitors on a regular basis for updates of information.
2.5 NETWORK MANAGEMENT ENHANCEMENTS

The capabilities of network management applications continue to expand as the need arises and technology advances. Included in these expansions are fault, capacity, resource and trending management. New categories of management such as Service Level Agreements (SLA) [Ref 19-20] and Management by Policy [Ref 21] and their metrics have become important. In addition, the number of network management approaches has increased. Included in these new approaches are Web-based Management [Ref 22] and Desktop Management [Ref 23]. We talk about these approaches in Chapters 10 and 11.

There are also more management application programs available. They provide a wide range of data analysis and decision-making capabilities. However, it is important to emphasize at this point that all management application programs depend on the protocols and databases that are the focus of this book. Furthermore, no matter how comprehensive the management application, what is important is that the application provide information important to the network manager and display it in a manner that is easy to comprehend.

As promised, let’s now look at the evolution of network management. It is useful to do so because the resulting perspective will provide the reader with an appreciation of how we got to where we are and the rationale for today’s and future approaches to network management. This understanding will also enable the reader to evaluate evolving approaches to network management. As you will see, a lot happened in the short time period between when network management was first thought to be necessary and today.

2.6 EVOLUTION OF NETWORK MANAGEMENT

2.6.1 OSI Reference Model

About 10 years before people working in the field of data networks began to see a need for remote and/or automated network management, those associated with data networks and the International Organization for Standards (ISO) recognized that growth in the use of communication over distributed networks required a formal protocol architecture specification that would promote uniformity in standards development. In 1977, the ISO established a subcommittee to develop such an architecture. The result was the Open Systems Interconnection (OSI) Reference Model, ISO Standard 7498-1 [Ref 1], which was published in 1984. The stated purpose of this Reference Model was to “provide a common basis for the coordination of standards developments for the purpose of system interconnection, while allowing existing standards to be placed in perspective within the overall Reference Model.” This Reference Model is usually used to explain the functionality of protocol stacks as was done in Chapter 1.
2.6.2 SGMP

In March of 1987, a few network engineers in the United States began an effort to develop a network management protocol for gateways [Ref 8]. (This reference provides an interesting look at the controversy surrounding network management developments at the time.) By November of 1987, this effort led to RFC 1028, the Simple Gateway Monitoring Protocol (SGMP) [Ref 24]. The goal of the SGMP developers was to minimize the complexity of software needed for gateway management and the number of commands to which gateway agents would have to respond. Thus only two types of commands were viewed essential: "get" the value of a variable and "set" (change) the value of a variable.

During the time frame in which SGMP was developed, those continuing to enhance the Open Systems Interconnection (OSI) Reference Model began to develop a network management protocol to add to the OSI suite of protocols. A group in the United States therefore thought that the long-term solution would be to add the OSI network management protocol to the existing Internet TCP/IP architecture rather than pursue SGMP. This approach was called CMOT (CMIP over TCP) where CMIP is Common Management Information Protocol. CMIP is contained in the Application layer of the OSI protocol stack. CMIP is defined in ISO standard 7498-4 [Ref 25]. See [Ref 5] for a good description of it.

2.6.3 CMIP

As was mentioned in Chapter 1, in the OSI Reference Model protocol stack, CMIP plays a role similar to that of SNMP in the TCP/IP protocol stack. Upon request from the management application, CMIP creates the protocol data unit and maps it to a Remote Operations Service Element (ROSE) protocol that supports communications between all distributed applications in the OSI environment. Referring back to Figure 2.2, in the OSI environment, CMIP and ROSE are part of a Management Process that is very comprehensive. For all applications, including management, the OSI application layer provides more application services than does the TCP/IP application layer.

Included among the additional capabilities of the CMIP are eleven management operations (commands) rather than the five supported by SNMP and the ability to operate over a variety of protocol stacks including TCP/IP. By making extensive use of object-oriented modeling concepts, CMIP provides more detailed representation of MIB objects, the ability to create objects, and objects that inherit the properties of other objects. In addition, the ability to define the scope of object filtering according to attributes leads to much greater control of its Get operation. These capabilities also lead naturally to a larger MIB with objects that have many attributes not present in MIB definitions used by SNMP.

There has been a price to pay for these capabilities at the Application and other layers of the OSI Reference Model. Long development times and complexity have kept the industry from adopting it pervasively. In short, the difference be-
between CMIP and SNMP can be best stated by the SNMP motto: "Keep it Simple." A thorough discussion of OSI System Management Concepts, including CMIP, is given in [Ref 5].

2.6.4 SNMP

As a result of controversy over the SGMP and CMOT approaches, the Internet Activities Board (IAB), the body that was responsible for all Internet research and development in the United States at the time, convened a subcommittee in February 1988 to identify the best approach to follow. The decision was that both approaches would be pursued. Eventually the CMOT approach was found too difficult to implement and was abandoned. However, an enhanced version of SGMP, called the Simple Network Management Protocol (SNMP) was developed [Ref 3]. Several groups worked on this management system definition. Work on the Internet-standard Network Management Framework was also initiated (see below). This framework encompasses SNMP. By 1989, SNMP had become the de facto operational standard for network management of TCP/IP-based networks.

2.6.5 More History

A little more history is appropriate at this point. At about the same time that development of the OSI Reference Model protocol architecture was initiated, universities in the United States were developing protocols that would enable communication between a small number of their computers for collaborative research. This effort was supported by the DOD Advanced Research Projects Agency (ARPA) and led to the non-proprietary set of protocols known as TCP/IP. [Ref 26] The TCP/IP protocols were an intrinsic part of the Unix operating system developed at UC Berkeley. Eventually corporations took notice of the TCP/IP protocols and use began to grow. However, as mentioned, it was expected that the TCP/IP protocols, and thus SNMP, would be a temporary measure until completion of the OSI protocols.

This was not to be the case. SNMP became so widespread and the OSI protocols were so slow in developing that SNMP became the dominant network management protocol. Even so, a study of the details of the OSI Reference Model Standard 7498-1 and its protocols is very worthwhile. The standard describes the protocols and their interactions in great detail. Such detail is difficult to find elsewhere. Although TCP/IP and SNMP are today the dominant protocol stack and network management protocol, respectively, the OSI Reference Model and CMIP are in use.

2.6.6 Network Management Framework

In August 1988, the Internet Activities Board (IAB) assigned a working group the task of creating an Internet Standard Network Management Framework to define the components required for network management of TCP/IP networks. This re-
sulted in three RFCs. RFC 1155 [Ref 27] defined the Structure of Management Information (SMI). SMI makes use of Abstract Syntax Notation One (ASN.1). ASN.1 was developed to enable specification of the OSI Reference Model and is the language used to define SMI managed objects. For discussion of ASN.1, see [Ref 9, 28, 29] and Appendix B of this book. As explained above, the agent process accesses the value of an object requested in an SNMP Get-Request packet. Object values are stored in a data structure on the Management Agent. RFC 1156 defines this data structure and calls it the Management Information Base (MIB)[Ref 9-11]. The requested object is referenced using the language of SMI (a subset of ASN.1). Finally, RFC 1157 defines the Simple Network Management Protocol, SNMP [Ref 3].

2.6.7 History Table

Table 2.1 provides a summary of the evolution of the computerized network management developments described above and lists other relevant events. We have not discussed all of these developments in this chapter but they will be addressed in other parts of this book. As you can see, 1988 and 2002 were busy years for network management development. There are many informative articles available in Network World, Data Communications, and Network Computing magazines about network management and related topics during this time. In addition, the magazines refer to vendor products that are improving the state-of-the-art in network management applications. We refer to these in the appropriate chapters.

2.7 HISTORY GRAPH

Figure 2.3 is a graph of the data in the Table 2.1. While being less accurate than the History Table, the graph gives us a birds-eye-view of the technology and protocols that have made possible or impacted the development of network management. What is not included in the table or shown on the graph are the tools being developed that, using the current protocols, are providing added value that make network management more powerful for the enterprise. We discuss such tools in Appendix E.

The only axis on the graph that has meaning is the ordinate where years are shown. However, we have attempted to show the dependence of one development on others by placing it directly over ones on which it depended. For example, RMONI depended on RMONII. The height of the boxes is intended to give an indication of the time frame over which major development indicated in the box took place. The width of the box has no meaning and is chosen only to accommodate the included text.
### Table 2.1  Evolution of Network Management (References are those at end of chapter)

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1968</td>
<td>ARPA funds development of packet switching networks</td>
<td>• RFC 1120 Internet Activities Board. V. Cerf. Sep-01-1989. (Obsoleted by RFC1160)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RFC 1160 Internet Activities Board. V. Cerf. May-01-1990. (Obsoletes RFC1120)</td>
</tr>
<tr>
<td>1978</td>
<td>OSI Reference Model development initiated</td>
<td>ISO/IEC 7498 (CCITT X.200) [Ref 1]</td>
</tr>
<tr>
<td>1983</td>
<td>OSI Reference Model becomes international standard</td>
<td>[Ref 24]</td>
</tr>
<tr>
<td>1987</td>
<td>SGMP development started</td>
<td>ISO 8824, Parts 1–4</td>
</tr>
<tr>
<td>1988</td>
<td>IAB initiates study of SGMP and CMIP</td>
<td>Interim RFC 1028 (SNMPv1)</td>
</tr>
<tr>
<td></td>
<td>SNMPv1 becomes Interim Draft Standard</td>
<td>Draft RFC 1098 (SNMPv1)</td>
</tr>
<tr>
<td></td>
<td>SNMPv1 becomes Draft Standard</td>
<td>Draft RFC 1065 (SMI)</td>
</tr>
<tr>
<td></td>
<td>IAB initiates development of Internet Standard</td>
<td>Draft RFC 1066 (MIB I) [Ref 10]</td>
</tr>
<tr>
<td></td>
<td>Network Management Framework MIB I developed</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>CMOT approach abandoned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP becomes the defacto standard for TCP/IP management</td>
<td></td>
</tr>
<tr>
<td>1990</td>
<td>SMI becomes Recommended Standard</td>
<td>RFC 1165 (SMI)</td>
</tr>
<tr>
<td></td>
<td>SNMPv1 becomes Recommended Standard</td>
<td>RFC 1157 (SNMP) [Ref 3]</td>
</tr>
<tr>
<td></td>
<td>MIB I becomes Recommended Standard</td>
<td>RFC 1156 (MIB I) [Ref 11]</td>
</tr>
<tr>
<td>1991</td>
<td>MIB II</td>
<td>RFC 1213 (MIB II)</td>
</tr>
<tr>
<td></td>
<td>RMONI</td>
<td>RFC1271 (RMONI) [Ref 12]</td>
</tr>
<tr>
<td>1993</td>
<td>SNMPv2 Proposed</td>
<td>RFC 1441 (SNMPv2 Management Framework)</td>
</tr>
<tr>
<td></td>
<td>SNMPv2 Security</td>
<td>RFC 1446 (SNMPv2 Security Protocols)</td>
</tr>
<tr>
<td></td>
<td>SNMPv2 MIB</td>
<td>RFC 1450 (SNMPv2 MIB)</td>
</tr>
<tr>
<td></td>
<td>SNMPv2 SMI</td>
<td>RFC 1442 (SNMPv2 Structure of Management Information)</td>
</tr>
<tr>
<td>1995</td>
<td>RMONI</td>
<td>RFC1757 [Ref 13]</td>
</tr>
<tr>
<td>1997</td>
<td>RMONII</td>
<td>RFC2021</td>
</tr>
<tr>
<td>1998</td>
<td>Desktop Management Interface (DMI) Specification v2.0s</td>
<td>• <a href="http://www.dmtf.org/sped/dmis">http://www.dmtf.org/sped/dmis</a></td>
</tr>
<tr>
<td></td>
<td>Web-based Management Initiative</td>
<td>• Network Computing, Feb 2001, p. 57</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="http://www.dmtf.org/standards/standard-wbem.php">http://www.dmtf.org/standards/standard-wbem.php</a></td>
</tr>
<tr>
<td>1999</td>
<td>SNMPv2 Management Frameworks</td>
<td>RFC 2571</td>
</tr>
<tr>
<td></td>
<td>SNMPv3 Security</td>
<td>RFC 2574 (User-based Security Model)</td>
</tr>
<tr>
<td>2002</td>
<td>SNMP Management Frameworks</td>
<td>RFC 3411 std 62</td>
</tr>
<tr>
<td></td>
<td>SNMPv3 Security</td>
<td>RFC 3414 (User-based Security Model), std 62</td>
</tr>
<tr>
<td></td>
<td>SNMP VACM</td>
<td>RFC 3415 (View-based Access Control Model), std 62</td>
</tr>
<tr>
<td></td>
<td>SNMP MIB</td>
<td>RFC 3418, std 62</td>
</tr>
</tbody>
</table>
Figure 2.3  Evolution of Network Management Technologies
REFERENCES


