CHAPTER 4

Network Management Basics

Background

The early 1980s saw tremendous expansion in the area of network deployment. As companies realized the cost benefits and productivity gains created by network technology, they began adding networks and expanding existing networks almost as rapidly as new network technologies and products were introduced. By the mid-1980s, growing pains from this expansion were being felt, especially by those companies that had deployed many different (and incompatible) network technologies.

The primary problems associated with network expansion are day-to-day network operation management and strategic network growth planning. Specifically, each new network technology requires its own set of experts to operate and maintain. In the early 1980s, strategic planning for the growth of these networks became a nightmare. The staffing requirements alone for managing large, heterogeneous networks created a crisis for many organizations. Automated network management (including what is typically called *network capacity planning*), integrated across diverse environments, became an urgent need.

This chapter describes technical features common to most network management architectures and protocols. It also presents the five functional areas of management as defined by the International Organization for Standardization (ISO).

Network Management Architecture

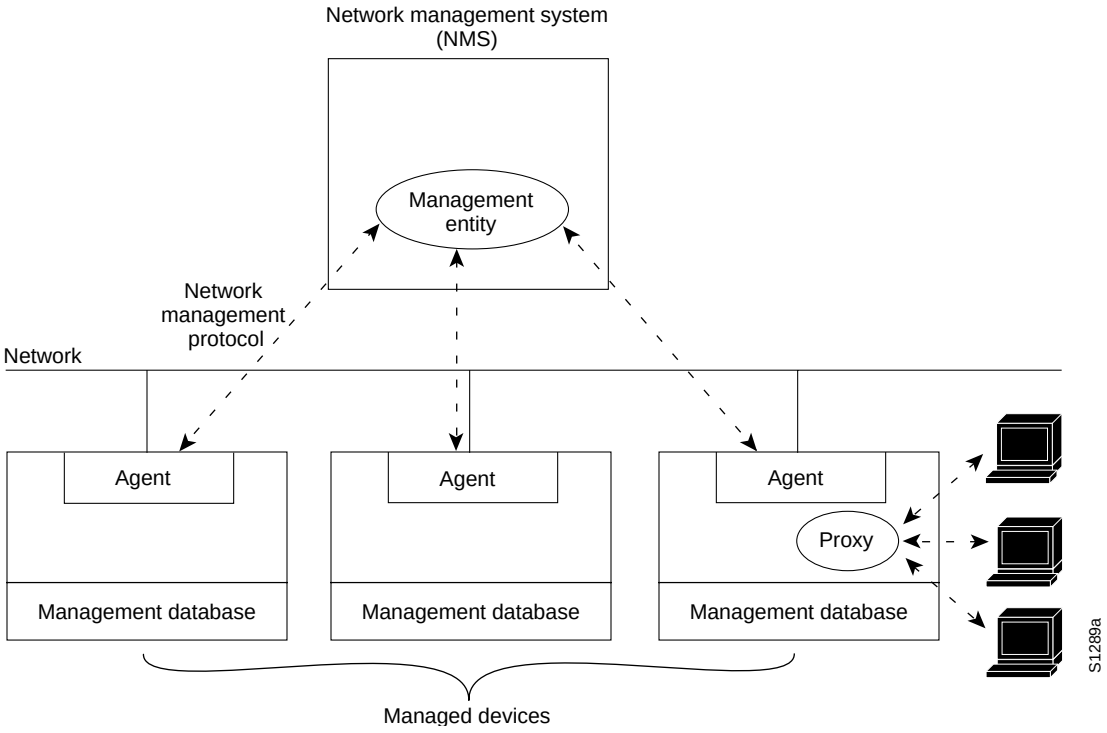
Most network management architectures use the same basic structure and set of relationships. End stations (*managed devices*) such as computer systems and other network devices run software allowing them to send alerts when they recognize problems. Problems are recognized when one or more user-determined thresholds are exceeded. Upon receiving these alerts, *management entities* are programmed to react by executing one, several, or all of a group of actions, including:

- Operator notification
- Event logging
- System shutdown
- Automatic attempts at system repair

Management entities can also poll end stations to check the values of certain variables. Polling can be automatic or user initiated. *Agents* in the managed devices respond to these polls. Agents are software modules that compile information about the managed devices in which they reside, store this information in a *management database*, and provide it (proactively or reactively) to management entities within *network management systems* (NMSs) via a *network management protocol*. Well-known network management protocols include the Simple Network Management Protocol

(SNMP) and Common Management Information Protocol (CMIP). *Management proxies* are entities that provide management information on behalf of other entities. A typical network management architecture is shown in Figure 4-1.

Figure 4-1 Typical Network Management Architecture



ISO Network Management Model

The ISO has contributed a great deal to network standardization. Their network management model is the primary means for understanding the major functions of network management systems. This model consists of five conceptual areas:

- Performance Management
- Configuration Management
- Accounting Management
- Fault Management
- Security Management

Performance Management

The goal of performance management is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Performance management involves several steps:

1. Gather performance data on those variables of interest to network administrators.
2. Analyze the data to determine normal (baseline) levels.
3. Determine appropriate performance thresholds for each important variable such that exceeding of these thresholds indicates a network problem worthy of attention.

Management entities continually monitor performance variables. When a performance threshold is exceeded, an alert is generated and sent to the network management system.

Each of the steps just described is part of the process to set up a reactive system. When performance becomes unacceptable by virtue of an exceeded user-defined threshold, the system reacts by sending a message. Performance management also permits proactive methods. For example, network simulation can be used to project how network growth will affect performance metrics. Such simulation can effectively alert administrators to impending problems, so that counteractive measures can be taken.

Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed. Because all hardware and software elements have operational quirks, flaws, or both that might affect network operation, such information is important to maintaining a smooth-running network.

Each network device has a variety of version information associated with it. For example, an engineering workstation might be configured as follows:

- Operating system, Version 3.2
- Ethernet interface, Version 5.4
- TCP/IP software, Version 2.0
- NetWare software, Version 4.1
- NFS software, Version 5.1
- Serial communications controller, Version 1.1
- X.25 software, Version 1.0
- SNMP software, Version 3.1

Configuration management subsystems store this information in a database for easy access. When a problem occurs, this database can be searched for clues that might help solve the problem.

Accounting Management

The goal of accounting management is to measure network utilization parameters so that individual or group uses of the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned out based on resource capacities) and maximizes the fairness of network access across all users.

As with performance management, the first step toward appropriate accounting management is to measure utilization of all important network resources. Analysis of the results provides insight into current usage patterns. Usage quotas can be set at this point. Some correction will be required to

reach optimal access practices. From that point on, ongoing measurement of resource use can yield billing information as well as information used to assess continued fair and optimal resource utilization.

Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems in order to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

Fault management involves several steps:

1. Determine problem symptoms.
2. Isolate the problem.
3. Fix the problem.
4. Test the fix on all important subsystems.
5. Record the problem's detection and resolution.

Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. For example, a security management subsystem can monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes.

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to any network resources is inappropriate. Such users are usually company outsiders. For other (internal) network users, access to information originating from a particular department is inappropriate. For example, access to human resource files is inappropriate for most users outside the human resource department.

Security management subsystems perform several functions:

- Identify sensitive network resources (including systems, files, and other entities).
- Determine mappings between sensitive network resources and user sets.
- Monitor access points to sensitive network resources.
- Log inappropriate access to sensitive network resources.