CHAPTER 12
NETWORK MANAGEMENT

Chapter Summary
Network managers perform two key tasks: (1) designing new networks and network upgrades and (2) managing the day-to-day operation of existing networks. The prior chapters have examined network design, so this chapter focuses on day-to-day network management, discussing the things that must be done to ensure that the network functions properly, although we do discuss some special-purpose equipment designed to improve network performance. Our focus is on the network management organization and the basic functions that a network manager must perform to operate a successful network.

Learning Objectives
After reading this chapter, students should:

- Understand what is required to manage the day-to-day operation of networks
- Be familiar with the network management organization
- Understand configuration management
- Understand performance and fault management
- Be familiar with end user support
- Be familiar with cost management

Key Terms

alarm
alarm storm
application management software
application shaping
availability
bandwidth limiter
bandwidth shaper
capacity management
charge-back policy
configuration management
content caching
content delivery
content delivery provider
cost management
desktop management
device management software
downtime
end user support
fault management
firefighting
help desk
load balancer
managed device
managed network
management information base (MIB)
mean time between failures (MTBF)
mean time to diagnose (MTTD)
mean time to fix (MTTF)
mean time to repair (MTTR)
mean time to respond (MTTR)
monitor
network cost of ownership (NCO)
network documentation
network management
network management software
network monitoring
network operations center (NOC)
performance management
problem statistics
problem tracking
quality control chart
remote monitoring (RMON)
root cause analysis
server virtualization
service-level agreement (SLA)
Simple Network Management Protocol (SNMP)
system management software
total cost of ownership (TCO)
traffic shaper
trouble ticket
uptime
virtual server

Chapter Outline

1. Introduction
2. Designing for Network Performance
    a. Managed Networks
    b. Managing Network Traffic
    c. Reducing Network Traffic
3. Configuration Management
    a. Configuring the Network and Client Computers
    b. Documenting the Configuration
4. Performance and Fault Management
    a. Network Monitoring
    b. Failure Control Function
    c. Performance and Failure Statistics
    d. Improving Performance
5. End User Support
    a. Resolving Problems
    b. Providing End User Training
6. Cost Management
    a. Sources of Costs
    b. Reducing Costs
7. Implications for Management

8. Summary

Answers to Textbook Exercises

Answers to End-of-Chapter Questions

1. What skills does a network manager need?

   The books provides the following list:

   Strong technology skills in a variety of technologies
   LAN/WAN networking experience working with routers and switches
   Experience with Internet access solutions, including firewalls and VPN
   Network architecture design and implementation experience
   Information security experience
   Personnel management experience
   Project management experience
   Experience working in a team environment
   Ability to work well in an unstructured environment
   Excellent problem-solving and analytical skills
   Effective written and oral communication skills

2. What is "firefighting?"

   Many network managers spend most of their time firefighting -- dealing with breakdowns and immediate problems. If managers do not spend enough time on planning and organizing the network and networking staff, which are needed to predict and prevent problems, they are destined to be reactive rather than proactive in solving problems.

3. Why is combining voice and data a major organizational challenge?

   A major organizational challenge is the prospect of combining the voice communication function with the data and image communication functions. Traditionally, voice communications were handled by a manager in the facilities department who supervised the telephone switchboard systems and also coordinated the installation and maintenance of the organization's voice telephone networks. By contrast, data communications traditionally were handled by the IT department because the staff installed their own communication circuits as the need arose, rather than contacting and coordinating with the voice communications management staff.

   This separation of voice and data worked well over the years, but now changing communication technologies are causing enormous pressures to combine these functions. These pressures are magnified by the high cost of maintaining separate facilities, the low efficiency and productivity of the organization's employees because there are two separate network functions, and the potential political problems within an organization when neither manager wants to relinquish his or her functional duties or job position. A key factor in voice/data integration might turn out to be the elimination of one key management position and the merging of two staffs.

4. Describe what configuration management encompasses.

   Configuration management means managing the network's hardware and software configuration and documenting it (and ensuring it is updated as the configuration changes). Configuration management is concerned with knowing what hardware and software is where.

   One of the most common configuration activities is adding and deleting user accounts. When new users are added to the network, they are usually categorized as being a member of some group of users (e.g., faculty, students, accounting department, personnel department). Each user group has its own access privileges, which define what file servers, directories, and files they can access and provide a standard login script.

   Another common activity is updating the software on the client computers attached the network. Every time a new application system is developed or updated (or, for that matter when a new version of networking software is released) each client computer in the organization must be updated.

   Configuration documentation includes information about network hardware, network software, user and application profiles, and network documentation. The most basic information about network hardware is a set of network configuration maps that document the number, type, and placement of network circuits (whether organization owned or leased from a common carrier), network servers, network devices (e.g., hubs, routers), and client computers. Documentation for network software includes the network operating system (NOS) and any special purpose network software.

   The third type of documentation is the user and application profiles, which should be automatically provided by the network operating system or additional vendor or third-party software agreements. These should enable the network manager to easily identify the files and directories to which each user has access and their access rights (e.g., read-only, edit, delete).

   In addition, other documentation must be routinely developed and updated pertaining to the network. This includes network hardware and software manuals, application software manuals, standards manuals, operations manuals for network staff, vendor contracts and agreements, and licenses for software. The documentation should include details about performance and fault management (e.g., preventive maintenance guidelines and schedules, disaster recovery plan, and diagnostic techniques), end user support (e.g., applications software manuals, vendor support telephone numbers), and cost management (e.g., annual budgets, repair costs for each device). The documentation should also include any legal requirements to comply with local or federal laws, control, or regulatory bodies.

5. People tend to think of software when documentation is mentioned. What is documentation in a network situation?

   Documentation in a network situation is mandatory and includes:

   - inventory of network hardware and equipment
   - network configuration and maps

- maintenance records
- software listings by hardware and network tasks
- software documentation manuals
- user names and telephone numbers
- vendor names and telephone numbers
- contracts
- legal requirements
- operating manuals
- disaster plan and recovery techniques
- troubleshooting techniques

6. What is desktop management and why is it important?

   Desktop management (DM), sometimes called Electronic Software Delivery (ESD) or automatic software distribution, is one solution to the configuration problem. DM enables network managers to install software on client computers over the network without needing individual access to each client computer. Most DM packages provide application layer software for the network server and all client computers. The server software communicates directly with the DM application software on the clients and can be instructed to download and install certain application packages on each client at some predefined time (e.g., at midnight on Saturday).

   DM software greatly reduces the cost of configuration management over the long term because it eliminates the need to manually update each and every client computer. It also automatically produces and maintains accurate documentation of all software installed on each client computer and enables network managers to produce a variety of useful reports. However, DM increases costs in the short term because it costs money (typically $50-100 per client computer) and requires network staff to manually install it on each client computer. The other problem with DM is that currently there are no standards. Standards are beginning to emerge (e.g., Desktop Management Interface (DMI)), but so far they have not been widely embraced.

7. What is performance and fault management?

   Performance management means ensuring the network is operating as efficiently as possible. Improving network performance is its essence. Several strategies for improving performance were discussed in previous chapters.

   Fault management means preventing, detecting, and correcting faults in the network circuits, hardware, and software (e.g., a broken hub or improperly installed software). Fault management and performance management are closely related, because any faults in the network reduce performance. Both require network monitoring, which means keeping track of the operation of network circuits and devices to ensure they are functioning properly and to determine how heavily they are used.

8. What does a help desk do?

   Failure control is handled by the network support group (often starting with a help desk) that is called when anything goes wrong in the network. This group has appropriate customer service representatives to record problems, report them to the testing and problem management group, follow up, and generally ensure that the network is back in operation as soon as possible. This group also might be responsible for change scheduling, coordination, and follow-up on any changes, whether they involve hardware, software, or circuits. In other words, this is the user's interface when there is a problem of any kind.

9. What do trouble tickets report?

   Numerous software packages are available for recording fault information. The reports they produce are known as trouble tickets. The software packages assist the help desk personnel so they can type the trouble report immediately into a computerized failure analysis program. They also automatically produce various statistical reports to track how many failures have occurred for each piece of hardware, circuit, or software package. There are four main reasons for trouble tickets: problem tracking, problem statistics, problem-solving methodology, and management reports.

   Trouble tickets report on:

   - who reported the problem
   - the telephone number of the reporting the problem
   - time and date of the problem (not the time of reporting)
   - location and nature of the problem
   - when the problem was identified
   - why and how the problem happened
   - who is responsible for correcting any outstanding problems
   - what is the status of the problem
   - the priority of the problem

10. Several important statistics related to network uptime and downtime are discussed in this chapter. What are they and why are they important?

    The statistics related to network uptime and downtime are:

    - mean time to diagnose (MTTD)
      - measures the efficiency of the in-house testing and problem management personnel
      - can be used to evaluate the ability of network personnel to isolate and diagnose failure of hardware, software, or circuits and can often be improved by training
    - mean time to respond (MTTR)
      - indicates how quickly vendors and internal groups respond to emergencies
      - can lead to a change of vendors or internal management policies, or, at the minimum, can exert severe pressure on vendors who do not respond to problems promptly

    - can be influenced by showing vendors or internal groups how good or bad their response times have been in the past
- mean time to fix (MTTF)
    - measures how long it takes the vendor or internal support group to correct the problem once they arrive on the premises
    - can be affected by the use of redundant interface equipment, alternate circuit paths, adequate recovery or fallback procedures to earlier versions of software, and the technical expertise of internal or vendor staff
- mean time to repair
    - MTTRepair = MTTDiagnose + MTTRespond + MTTFix
- mean time between failures (MTBF)
    - indicates the reliability of a network component
    - developed by equipment vendors to tell customers how frequently their equipment fails (this is the number of hours or days of continuous operation before the component fails)
    - can be influenced by the original selection of vendor-supplied equipment

Because these mean times affect network availability, their collection is vital if network performance is to be improved. Availability is the percentage of time the network is available to users. It is calculated as the number of hours per month the network is available divided by the total number of hours per month (i.e., 24 hours per day x 30 days/month = 720 hours).

Another set of statistics that should be gathered are those collected daily by the network operations group who employ automated network management software (network monitors and analyzers). These statistics record the normal operation of the network, such as the number of errors (retransmissions) per communication circuit, per terminal, or whatever is appropriate. Statistics also should be collected on the daily volume of transmissions (characters per hour) for each communication link or circuit, each terminal, or whatever is appropriate for the network. It is important to closely monitor utilization rates, the percentage of the theoretical capacity that is being used. These data can identify computers/devices or communication circuits that have higher-than-average error rates, and may be used for predicting future growth patterns and failures. A device or circuit that is approaching maximum utilization obviously needs to be upgraded.

11. What is an SLA?

    More organizations are beginning to establish service level agreements (SLA) with their common carriers and Internet service providers. An SLA specifies the exact type of performance and fault conditions that the organization will accept. For example, the SLA might state that network availability must be 99 percent or higher and that the MTBF for T1 circuits must be 120 days or more. In many cases, SLA includes maximum allowable response times. Some organizations are also starting to use an SLA internally to clearly define relationships between the networking group and its organizational "customers." Specifically, it should include at least the following:

    Network availability

Average round-trip PVC delay
PVC throughput
MTTR
MTTF

12. How is network availability calculated?

    Network availability is the percentage of time the network is available to users. It is calculated, by using the various mean times, as the number of hours per month the network is available divided by the total number of hours per month (i.e., 24 hours per day x 30 days/month = 720 hours). Availability includes all components of the network that are required for the network to be up and operating (modems, circuits, and so forth).

13. What is problem escalation?

    Problem escalation is the increase in severity and scope of a problem caused when the initial problem or error situation is not resolved quickly and efficiently. Staff members who handle escalated problems have specialized skills in certain problem areas or with certain types of software and hardware.

14. What are the primary functions of end user support?

    Providing end user support means solving whatever problems users encounter while using the network. There are three main functions within end user support: resolving network faults, resolving software problems, and training.

15. What is total cost of ownership?

    The total cost of ownership (TCO) is a measure of how much it costs per year to keep one computer operating. TCO includes the cost of support staff to attach it to the network, install software, administer the network (e.g., create user ids, backup user data), provide training and technical support, and upgrade hardware and software. It also includes the cost of time "wasted" by the user when problems occur or when the user is attempting to learn new software.

16. Why is the total cost of ownership so high?

    While TCO has been accepted by many organizations, other firms argue against the practice of including "wasted" time in the calculation. Some organizations therefore prefer to focus on costing methods that examine only the direct costs of operating the computers, omitting softer costs such as "wasted" time. The most expensive item is personnel (network managers and technicians), which typically accounts for 50 to 70 percent of total costs. The second most expensive cost item is WAN circuits, followed by hardware upgrades and replacement parts. The largest time cost (where staff spend most of their time) is systems management, which includes configuration, fault, and performance management tasks that focus on the network as a whole. The second largest item is end user support.

    There is one very important message from this pattern of costs. Since the largest cost item is personnel time, the primary focus of cost management lies in designing networks and

developing policies to reduce personnel time, not to reduce hardware cost. Over the long term, it makes more sense to buy more expensive equipment if it can reduce the cost of network management.

17. How can network costs be reduced?

    Network costs can be reduced by taking these steps:

    - Develop standard hardware and software configurations for client computers and servers
    - Automate as much of the network management function as possible by deploying a solid set of network management tools
    - Reduce the costs of installing new hardware and software by working with vendors
    - Centralize help desks
    - Move to thin client architectures

18. What do network management software systems do and why are they important?

    Network management software is designed to provide automated support for some or all of the network management functions. Network management software systems are used to perform some of the functions of monitors and analyzers, identify errors, run diagnostic tests, monitor entire an network, compile statistics, and prepare real-time management reports. Network management software systems are important because they signify improved or deteriorating conditions.

    There are dozens of network management tools available. Some software tools support configuration management, some support performance and fault management, while some attempt to do both. Some tools have modules to support the help desk providing end user support.

19. What is SNMP and RMON?

    The most commonly used network management protocol is Simple Network Management Protocol (SNMP). Each SNMP device (e.g., router, switch, server) has an agent that collects information about itself and the messages it processes and stores that information in a database called the management information base (MIB).The network manager's management station that runs the network management software has access to the MIB. Using this software, the network manager can send control messages to individual devices or groups of devices asking them to report the information stored in their MIB.

    RMON allows for remote monitoring of equipment. RMON SNMP software enables MIB information to be stored on the device itself or on distributed RMON probes that store MIB information closer to the devices that generate it. The data are not transmitted to the central server until the network manager requests, thus reducing network traffic.

20. Compare and contrast device management software, system management software, and application management software.

    Device management software provides information about the specific devices on a network. It enables the network manager to monitor important devices such as servers, routers, and switches, and switches and to report configuration information, traffic volumes, and error conditions for each device.

    System management software provides the same configuration, traffic, and error information as device management systems but can analyze the device information to diagnose patterns, not just display individual device problems.

    Application management software also builds on the device management software, but instead of monitoring systems, it monitors applications.

21. How does a load balancer work?

    A load balancer acts as a traffic manager at the front of the server farm. All requests are directed to the load balancer at its IP address. When a request hits the load balancer, it forwards it to one specific server using the server's IP address. Sometimes a simple round-robin formula is used, while in other cases, more complex formulas track how busy each server actually is.

22. What is server virtualization?

    Server virtualization is the process of utilizing one physical server and using special software, creating multiple virtual computers that each run their own separate operating system.

23. What is policy-based management?

    Policy-based management allows the network manager to use special software to set priority policies for network traffic that take effect when the network becomes busy. It is usually implemented as a combination of hardware and software.

24. What is capacity management?

    Capacity management is used to monitor traffic and can slow down traffic from users who consume a lot of network capacity. Capacity management is related to policy-based management but is simpler in that it only looks at the source of the traffic rather than the nature of the traffic.

25. How does content caching differ from content delivery?

    Content caching is used to store other people's Web data closer to your users. Content delivery is the opposite. Rather than storing other people's web files closer to their own internal users, a content delivery provider stores web files for its clients closer to their potential users.

26. How does network cost of ownership (aka real TCO) differ from total cost of ownership? Which is the most useful measure of network costs from the point of view of the network manager? Why?

    The total cost of ownership (TCO) for typical networked PCs is about $7,000 per year per computer, far more than the initial purchase price. The network management cost (omitting "wasted" time) is between $1500 and $3500 per year per computer. The largest single cost item is staff salaries.

27. Many organizations do not have a formal trouble reporting system. Why do you think this is the case?

    Typically size, application diversity and volume of traffic determine whether or not a formal trouble reporting system is required. All large organizations with heterogeneous type networks require a formal trouble reporting system because the annual cost of maintenance demands it.

Mini-Cases

I. City School District, Part 1

City School District is a large, urban school district that operates 27 schools serving 22,000 students from kindergarten through grade 12. All schools are networked into a regional WAN that connects the schools to the district central office and each other. The district has a total of 5,300 client computers. The table below shows the annual costs. Calculate the real TCO (without wasted time).

Budget Item	**Annual Cost**
IT staff salaries	$7,038,400
Consultants	1,340,900
Software	657,200
Staff training	545,900
Client computers	2,236,600
Servers	355,100
Network	63,600
Supplies and parts	2,114,700

Total Costs = $14,352,400
Client Computers = 5,300
TCO = $2,708

II. City School District, Part 2

Read and complete Minicase I. Examine the TCO by category. Do you think that this TCO indicates a well-run network? What suggestions would you have?

This TCO total indicates a well-run network. Research has estimated that the TCO of a Windows-based client computer averages $7,000/year. The School District TCO of $2,708 is well below that figure.

III. Central Textiles

Central Textiles is a clothing manufacturer that operates 16 plants throughout the southern United States and in Latin America. The Information Systems Department, which reports to the vice president of finance, operates the central mainframe and LAN at the headquarters building in Spartanburg, South Carolina, and the WAN that connects all the plants. The LANs in each plant are managed by a separate IT group at each plant that reports to the plant manager (the plant managers report to the vice president of manufacturing).The telephone communications system and long-distance agreements are managed by a telecommunications department in the headquarters that reports to the vice president of finance. The CEO of Central Textiles has come to you asking about whether this is the best arrangement, or whether it would make more sense to integrate the three functions under one new department. Outline the pros and cons of both alternatives.

Integrating the three systems under one department would consolidate some of the management issues, and likely would allow for some headcount (cost) reduction. Centralization would also ensure that decisions taken about system upgrades and/or expansions will consider the systems in place in the other areas.

On the other hand, consolidating each system in one department might result in poorer services at the local level. For example, it may take longer for a centralized unit to respond to a trouble ticket on a local LAN than would a decentralized office on site where the problem is occurring.

IV. Indiana University

Take another look at Figure 12-1. If this is a typical traffic pattern, how would you suggest that they improve performance?

They could increase performance by adding circuit capacity between devices that have higher circuit utilization.

Next Day Air Service Case Study

The NDAS network system is finally in place and operating. President Coone has assigned operational control of the network to the Information Services Department. He believes this is reasonable and justified because of the Information Services Department's data processing responsibilities and experience in operating data communications equipment. In addition, his nephew, Les Coone, is running that department and has expressed considerable interest in data communications.

The Human Resources Department originally set up the telephone system, because--at the time--no one else was interested in doing it. As a result, Human Resources, headed by Karen Lott, controls the voice and facsimile communication system for the company.

One recurring problem is that two department heads disagree on which department should be responsible for dealing with the common carriers. Each department believes it should be the contact for dealing with the common carriers, and each thinks the other is stopping it from assuming its rightful place within the organization.

Because of your excellent past performance, President Coone has asked you to study certain organizational issues pertaining to the control and operation of both voice and data communications. He wants you to analyze the operations of both departments and propose a method for streamlining the organization and fixing the problem. This analysis should address the possibility of combining the voice and data communication responsibilities under a single manager. You may propose any reorganization that seems appropriate. Be sure to consider economies of scale when submitting any recommendations. President Coone reminds you that

you were a staunch advocate of video conferencing. He wants you to include video and image transmission considerations in your analysis.

You should also consider the type of individual that should manage this reorganization. Some of the factors to evaluate are the traits and characteristics needed for successful leadership, the ability to understand current systems, the ability to handle both data and voice networks, and the ability to analyze and manage future growth. The results of this evaluation will help determine whether such an individual exists within Next Day Air Service or whether the firm needs to hire someone from outside the organization.

Another little problem occurred last week when NDAS experienced its first network line failure. President Coone had to ask Karen Lott to determine what failed on the circuit. After fiddling with the problem for an hour and a half, she finally called the modem vendor, who then took three hours to get to the Tampa headquarters building. The good news is that the vendor's maintenance employee swapped a new circuit card into the failed modem and had it fixed in 15 minutes. Needless to say, President Coone was not happy!

Additional Content

Teaching Notes

Plan to spend about 4 hours on this chapter. It is suggested that the course include a network simulation exercise. See this book's Web Site.

My goals in this chapter are to outline the primary tasks that a network manager must do, as well as to introduce the idea of a managed network. I spend only a little time on the different cultures between LANs and WANs, but I think it is an issue that students entering the work force need to be sensitive to.

Most of the material is fairly straightforward. I use the LAN outage war story below as a lead-in to the need for managed networks. I pose the problem and help the students trace the cause and mentally walk through what they would do without SNMP.

Cost management (total cost of ownership (TCO)) has emerged as a crucial issue over the past few years. I spend some time making sure the students understand the TCO measure and trade-offs in using it. Cost management will continue to be a hot topic that will need to be watched over the next few years. We are likely to see several new technologies emerge that attempt to reduce TCO.

War Stories

LAN Outage

(Objective: illustrate the need for managed networks)
During the summer of 1995, I hosted a meeting of 20 senior consultants from CSC that were using our GSS software to perform a major reengineering project for the U.S. Department of Defense. Suddenly, the network crashed, making it impossible for us to work.

The network technicians went to work and tried to find the problem. Unfortunately, we had an unmanaged network, meaning the techs had to do their own trouble shooting. After several hours it became clear that something was jamming the entire Ethernet LAN -- there was a constant stream of traffic being generated. This suggested that a network card was "jabbering," that is, transmitting constantly. The techs went around turning off all computers one by one until the problem stopped. Once they had identified the computer, it was simple to replace the failed network card and the network was restarted. However, it took 18 hours to find the failed computer. Needless to say, the CSC folks were not impressed.

ESD in the University

(Objective: illustrate the practical uses of ESD)
One of the constant problems we have had (and I suspect your university has as well), is ensuring that the computers in our labs do not get changed by students. Our students were often changing the Windows configurations, adding software and putting wallpaper on the computers that we did not want. We developed our own home-grown solution to reset the computers. We have since switched to a commercial ESD tool which simplifies upgrades as well as resetting software and configuration files when they are first booted in the morning.

Network Growth Versus Staff Growth

(Objective: illustrate the crisis in staffing)
In 1995, the College of Business at the University of Georgia had five servers, 250 client computers, 200 network connections, and four electronic classrooms. Today in mid 1998, we have 30 servers, 600 client computers, 2200 network connections (most are designed for use by portable computers) and 25 electronic classrooms.

In 1995, we had 9 full-time staff members, while today, we have ten. Annual turnover has averaged 30% per year. Simply put, we are having a difficult time keeping up with the network growth. While faculty and staff have lobbied hard for increased network staff, our administration has not committed the needed resources to add staff. As we look around campus here at Georgia, the story is similar to what is occurring in other colleges, although we tend to be a bit more advanced than most.

