# **Lesson 3: Network Management Responsibilities**

#### At a Glance



Network managers are responsible for not only planning, designing, and implementing networks, their job is also to keep the network running smoothly and efficiently, with little or no down time. Generally speaking, the functions of a manager include installing and configuring devices, diagnosing and troubleshooting problems, controlling access to service, etc.

These functions fall into five main categories as follows:

- Configuration management
- Performance management
- Fault management
- Security management
- Accounting management

This lesson discusses each of these network management functions.

#### What You Will Learn

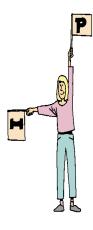
After completing this lesson, you will be able to do the following:

- Define, compare, and contrast OSI and TCP/IP management models
- Define and describe network configuration management
- Define and describe network performance management
- Define and describe network fault management
- Define and describe network security management
- Define and describe network accounting management



**Student Notes:** 

#### **Tech Talk**



- Accounting Management—The function of network management that includes capturing network usage data for the purpose of establishing charges and allocating costs to the appropriate users of the network.
- **Configuration Management**—The function of network management that involves monitoring the state of the network and modifying logical and physical configurations for more effective network operation.
- **Disk Duplexing**—Disk duplexing, just like disk mirroring, prevents the loss of data by duplicating the data to a second disk. The difference between them is that there is a separate controller for each disk.
- **Disk Mirroring**—Disk Mirroring, is a fault management technique that prevents the loss of data by duplicating, or mirroring, the data to a second disk.
- **Fault Management**—The function of network management that includes the detection, isolation, and correction of abnormal network behavior.
- **Performance Management**—The function of network management that keeps track of data traffic and overall network use. It also controls and analyzes the throughput and error rate of the network.
- Redundant Array of Inexpensive Disks (RAID)—RAID is a system whereby data that would traditionally be written to a single disk is written twice, once to the main disk and another time to a redundant disk.
- **Security Management**—The function of network management that controls who has access, the level of that access, and provides monitoring and analyzing network usage from an overall security perspective.



## **Network Management Responsibilities**

Network administrators must manage both software and hardware. To operate and maintain an efficient, secure, fully functional, cost-effective network does not require all of these standards; however, managers must know where can they find answers they need in a hurry, and what to do with the answers.

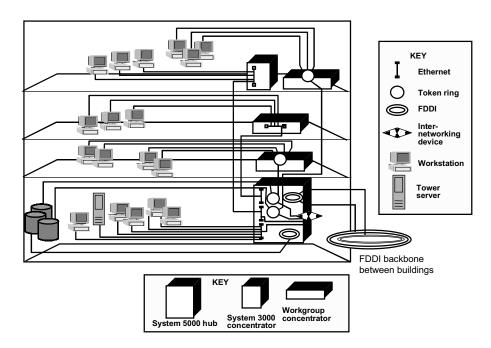
#### **Planning and Documentation**

In the 1970's and 1980's disk space at that time was extremely expensive and leaving two digits off the year did not seem to present a problem. Computer programmers did not have to foresight to consider the fact that the programs they were creating at the time would still be used in the year 2000. Today organizations worldwide are paying for this shortsightedness. The Year 2000 (Y2K) problem is the most public result of this lack of foresight. Programmers knew that the programs they were writing would only function correctly until 12/31/99. Unfortunately, the atmosphere of "get it done now, worry about that later," resulted in important pieces of the programming process to be left out.

In addition to programming limitations, many organizations did not take the time to document networking and programming data. Documentation is any information that you can refer to when you have a question about a process or program. If you need to change the design of a program that accepts a user id and password, you also need to know if other software and/or hardware might be affected. If you lengthen the user id field from 6 to 8 characters, will the next program that looks at that field still be expecting 6 characters? It might not accept the data in the new format. If that happens to you when you are using your bankcard and really need the cash, you will be legitimately upset.

When records and documentation are readily available, the person who makes the changes can quickly reference other programs and devices and make the necessary adjustments throughout the network. This is important since a network serves many people and processes, and cannot tolerate extensive down time while the problem is being researched.

What types of documentation should a network typically have? To start with, network documentation should include an up-to-date, accurate network architecture and design. These blueprints should provide complete descriptions and diagrams of the network and all of its components.



## **Map Showing Cabling Wiring Closets, and Devices**

A graphical representation of the network can assist when trying to diagnose networking problems. In addition to graphics, there needs to be text—words explaining the graphical representation, and information that cannot be expressed visually. For example, the first workstation in the series may require a static IP address rather than an address assigned dynamically from the DHCP server. If this information is not documented, a problem can arise within the network if a new NIC card is installed and configured to dynamically obtain IP data. It could take hours to determine what is wrong with the network.

Documentation is best kept in a place where it can be easily changed and updated. If hard copy is needed, a 3-ring binder will be more ideal than a bound volume. As changes are made to documentation, it is also important to maintain a revision history of the document. For example, the static IP address may have come about because of a requirement of the accounting software on that workstation.



Sample Documentation

Documentation should contain the branch of the network affected, the date, a notation of the work being done, relevant comments, and a signature (or initials) of the individual responsible for the change.

		-			
Network Branch	Date	Revision	Comments		
Accounting	5/3/9	Removed DHCP from	The accounting software		
· ·	9	workstation having	(version 89.7) requires a		
		Ethernet address:	fixed IP address. Later		
		02-A1-45-D3-74-E1	versions may not, but do		
			not install DHCP until		

Documentation is especially important in a large organization where the people who install and support application software may not be the same people as those who maintain and troubleshoot the network.

#### Reporting

One aspect of networking documentation often overlooked is report writing. The ability of a technical manager to report to a non-technical executive is a key ingredient in the success of that technical manager. What does an executive need to know about the network? He or she wants to know that it has been budgeted correctly, and that there have been few, if any, cost overruns. They don't want to know about specific technical details. When writing reports, always try to show the positive aspects of projects, etc. For example, instead of just stating that \$10,000 was spent on equipment to upgrade a segment of the network, take it a step further. Point out any positive aspects of newer more efficient and powerful network, such as the fact that the school can now have a web page, offer interactive courses, etc.

otherwise noted - SB

# **Check Your Understanding**

- Why should network managers plan for the future?
- Why should network managers document any/all network changes?
- Why should the name of the individual who makes changes to the network be included in the documentation?
- Who should know where network documentation is kept?



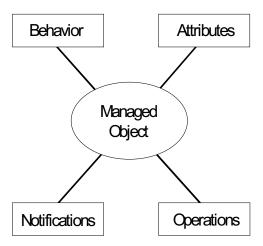
## **OSI and Network Management**

The OSI describes or defines managed objects according to the following:

- Behavior
- Attributes
- Notifications
- Operatives

A managed object might be a switch, NIC, routing algorithm, or printer queue.

### **OSI Definition of a Managed Object**



Behavior of managed objects refers to the type of notifications it can send and operations to which it can respond, such as whether it can set or replace values, or respond to such things as internal timers that trigger events.

Managed object attributes are its characteristics, current state, and operating conditions. Whether status is enabled or disabled is an example of an attribute.

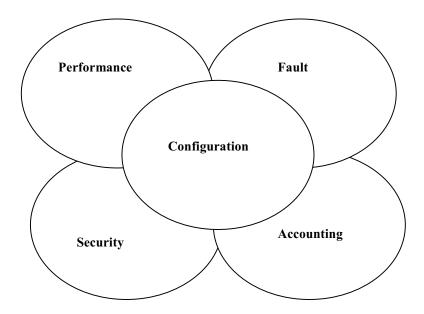
Notifications are the reports about events that occur. Operatives are the values that can be set, added, removed, or replaced.

The five network management functions as specified in the ISO's Specific Management Information Services Specifications include the following:

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

The OSI networking management standards used depend upon the network in question. If the network is small, with only a few devices but strict security needs, security may be the only management solution needed.

### **OSI Model for Network Management**





## **Check Your Understanding**

- ♦ How does the OSI describe managed objects?
- ♦ What are the five network management functions as specified by ISO's Specific Management Information Services Specifications?

## **Configuration Management**

Configuration management is basically the everyday work that helps prevent "fires." The primary tasks involved in configuration management include:

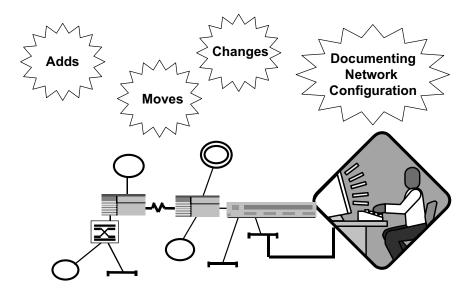
- Initial configuration of hardware and software.
- Developing a configuration map of the network topology along with an associated configuration map of the network software.
- Documenting and monitoring software configuration parameters. Note such things as which objects inter-operate with one another and issues that should be monitored.
- Ensuring that only one version of software is operating on the network and that users are notified of version changes.
- Noting changes in the operational characteristics of managed objects, such as enabled or disabled.
- Performing adds, moves, and changes for network segments and devices.

Often, initial configuration of network devices is considered part of installation, which is not an official part of the OSI definition of configuration management. However, since in many cases you use the same software tools and procedures for initial configuration that you use for performing adds, moves, and changes, it may be argued that initial configuration should become part of the standard. Configuration is equally important both initially and after the network has become operational.

Sometimes adding one device to a network and configuring it incorrectly can begin a chain reaction that can cause massive slowdowns, collisions, or in very rare circumstances, bring the network down completely. Therefore, this is one of the areas in which strict guidelines should be followed.

When adding a device to a small network, the installer can often use the default values configured by the vendor. Generally, default settings can also be used for software installed in small networks. As the users become more sophisticated and the network more complex, configurations generally need to be customized in order to accommodate connectivity and interoperability requirements.

#### **Configuration Management**



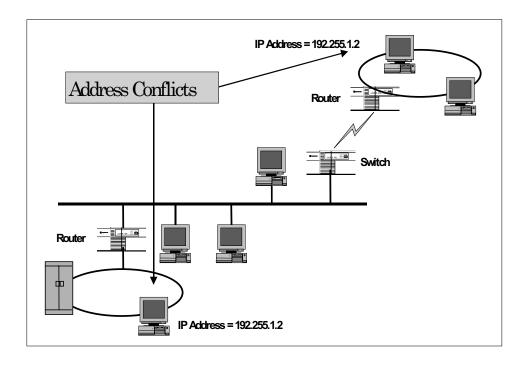
When devices and software work well together, configuration modifications are often unnecessary. However, the network manager needs to continuously monitor the state of the network. When needed, he or she can make changes in the logical and physical configurations of the network.



Making networking changes is one of the most difficult challenges a network manager can face and should be avoided whenever possible. When it becomes necessary to reconfigure, referring to prior network documentation is a must. In addition, documenting the changes being made is essential.

Network configurations might be modified for many reasons. If, for example, a company decides to move to Windows NT after many years as a UNIX site, it is pretty much guaranteed that there will be hours of configuration modifications involved.

### **Configuration Modifications Needed to Resolve IP Conflicts**

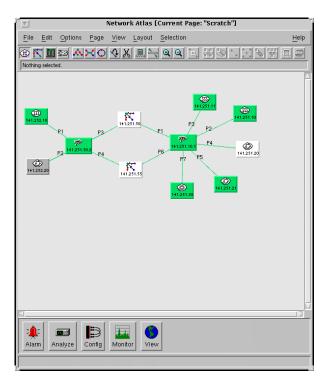


Another example might be when a network with an unregistered IP address needs to connect to the internetwork. The network manager must check the IP addresses of the network devices to be sure that they are unique to the internetwork. If not, changes will need to be made so that there are no duplications.

## **Configuration Tools**

Configuration management relies on documentation of network IP addresses, MAC addresses, serial numbers, locations, and changes made to default settings. Managers of large networks cannot enter all changes manually and still keep up with other responsibilities. A network manager needs a tool that can keep track of the information and that has the capability of generating reports. These configuration tools range from databases to sophisticated management tools. Databases are built from data gathered from internal reports generated by network devices. The more sophisticated management tools modify configurations according to the criteria set by the network manager.

### **Configuration Management Tool**





# **Check Your Understanding.**

- ♦ What are the main tasks of configuration management?
- What are some configuration tools a network manager might use?
- Give an example not mentioned in the text, of when a network manager might have to modify network configurations.

## **Fault Management**

Fault tolerance is nothing more than building and maintaining systems that can handle minor interruptions without bringing down the network. There are many things that can be done to provide fault tolerance. As with all networking options, the greater tolerance required the more expensive the solution. The more monitoring you do, the fewer faults you will have.

The main network management responsibilities involved in fault management are:

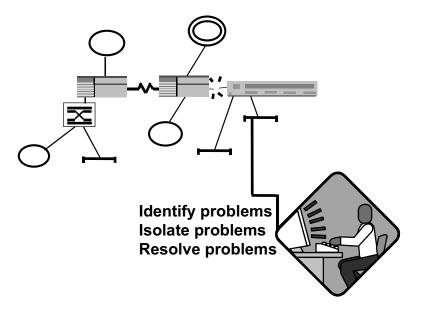
- Identifying the problem
- Isolating or locating the problem/cause
- Correcting the problem
- Preventative measures

Fault management includes determining that a problem exists, locating the device causing the problem in the network, and correcting the fault, preferably before users notice it and begin to complain. One way fault management is accomplished by identifying problems through the use of software tools, which monitor network activity and detect noteworthy variations. The use of the ping command can determine whether a device is operational.

The focus of fault management is on the network devices and on physical and virtual connections, all of which operate at the lower three layers of the OSI reference model.



### **Fault Management**



Fault management involves identifying whether there is a hardware, software, or data transmission error. Isolating the cause can be difficult. The trouble might be with the user, a single device, or it may be a general failure.

### Redundant Array of Inexpensive Disks (RAID)

Fault management includes identifying, isolating, and fixing problems; it also involves prevention measures that prevent troubles from occurring in the first place. This aspect of fault management is closely related to performance management.

Redundant Array of Inexpensive Disks (RAID) is an example of a way in which a network manager can prevent a problem. The loss of data is a major liability to any organization. RAID is a system whereby data that would traditionally be written to a single disk is written twice, once to the main disk and another time to a redundant disk. The array of disks can be anywhere from 1 to 10 disks large, and the data is written using one of a number of methods. RAID is used to improve network performance and prevent data loss. It does this through a process called data striping. With data striping, data is written across a number of disks, usually two or more. However, RAID 0 uses one disk that is partitioned. RAID improves performance since data written on one disk may take 3 microseconds, but written over three separate disks might take only 1 microsecond. Reading of disks is also faster with the use of RAID.

RAID 0 offers little protection, since the loss of the disk will result in a loss of all of the data. The primary reason for using RAID 0 is to speed up the read/write processing between data and disks.

RAID 1 writes the same data to more than one disk. If one disk fails, it is unlikely that the second disk will also fail, so the data is not lost.

RAID 5 employs both data striping and parity striping (parity is the information that tells where the end of a packet is, and how to read it). Additionally, it employs error correction capabilities. In addition, it distributes the error correction and parity data over all the disks. As a result, a single point of failure does not exist.



#### **Disk Mirroring and Duplexing**

Disk Mirroring, is a fault management technique that prevents the loss of data by duplicating, or mirroring, the data to a second disk. With disk mirroring, there is only one disk controller for both disks. Controllers are Mean Time Between Failures (MTBF) rated. Your device's controller may be rated at 10,000 hours. This is important information that should become part of the network documentation.

Disk duplexing does the same thing as disk mirroring, the difference is that there is a separate controller for each disk. In the event of a failure, the second disk can be used with its own controller and cable. Some systems can switch to the backup disk without interrupting service to network users. Others require the network administrator to reboot the system. This is something to take into account when planning or expanding a network.

#### **Backups**

Backing up your system frequently and fully is a good, cost-effective defense against lost work, and can even make you a hero when someone is looking for a file that they have been working on all day and have deleted by mistake! Tape drives can be set up either inside or outside of a server. Network administrators should always back up data. It is important to purchase reliable back up systems because once data is lost, the time and effort spent reconstructing the data can be insurmountable.

Backups can be either full or incremental. Just as it sounds, a full backup is of the entire system. An incremental backup is a backup of only the data that changed since the last backup. It makes sense to do incremental backups since program files do not change. To back up all program files each and every time takes unnecessary time, effort, media, and expense. What a network administrator is concerned with is the new data that has been entered since the last backup.

There are daily backups, weekly backups, and monthly backups. Generally speaking it is best to schedule full backups at night or over weekends when the network is more likely to be quite. Backing up data is usually done on a rotating basis. One of the most popular methods of backing up data is known as the "child-parentgrandparent" method, and requires 10 tapes. This rotation method uses 4 daily tapes, labeled with 4 successive days: Monday, Tuesday, Wednesday, and Thursday. Three tapes labeled Friday 1, Friday 2, and Friday 3; and 3 tapes labeled Month 1, Month 2, and Month 3. Over the course of 12 weeks, all of these tapes will be used. Each Monday the changes made that day are backed up. Friday 1 backs up the data from week one, Friday 2, from week 2 and so on. Month 1 for the entire first month, etc.

#### Sample Backup Schedule

Week	Monday	Tuesday	Wednesday	Thursday	Friday
1	Monday	Tuesday	Wednesday	Thursday	Friday 1
2	Monday	Tuesday	Wednesday	Thursday	Friday 2
3	Monday	Tuesday	Wednesday	Thursday	Friday 3
4	Monday	Tuesday	Wednesday	Thursday	Month 1
5	Monday	Tuesday	Wednesday	Thursday	Friday 1
6	Monday	Tuesday	Wednesday	Thursday	Friday 2
7	Monday	Tuesday	Wednesday	Thursday	Friday 3
8	Monday	Tuesday	Wednesday	Thursday	Month 2
9	Monday	Tuesday	Wednesday	Thursday	Friday 1
10	Monday	Tuesday	Wednesday	Thursday	Friday 2
11	Monday	Tuesday	Wednesday	Thursday	Friday 3
12	Monday	Tuesday	Wednesday	Thursday	Month 3
13	Monday	Tuesday	Wednesday	Thursday	Friday 1

Whether the backups are full or incremental depends on the needs of the network. The network administrator sets the parameters for what will be backed up. S/he also determines when this will take place. If the above schedule were for full backups, it would not be unusual to have incremental backups periodically each day.



## **Fault Management Tools**

Fault management tools provide the network manager with the information necessary to identify, isolate, and correct networking faults. Three categories of fault management tools are:

- **Event reporting tools**—Can be configured to report events such as the shutting down of a device or the activation/deactivation of a link.
- **Diagnostic testing tools**—Can determine the integrity of a line, locate overloaded network devices, or diagnose protocol problems.
- **Alarm reporting**—Can send an "alarm alert" to a monitoring device when a given event occurs, when thresholds are reached, or when a storage device is full.

One of the simplest tools used for fault management is an uninterruptible power supply.

# **Check Your Understanding**

- What are some fault management tools used by network managers?
- What is disk mirroring?
- Why do you think having only one controller for disk mirroring might be a problem?
- Describe RAID levels 0, 3, and 5.
- What do event reporting tools do for a network manager?
- What do diagnostic testing tools do for a network manager?
- What do alarm reporting tools to for a network manager?



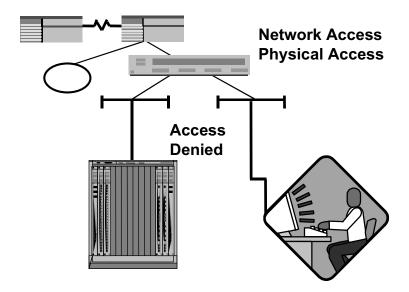
## **Security Management**

Security management involves controlling access to information on the network and identifying attempts to access that information. Security measures implemented depend upon the sensitivity of the data and the levels of access required by the network users. There are a number of ways to limit access to network information:

- Physical security
- Operating system security
- Network access security

Access points are areas where information can be obtained by unauthorized users. An unlocked communications closet, eavesdropping with electronic equipment, remote file transfer, passwords left out carelessly, are all ways an intruder can access a network. In addition to controlling unauthorized access, security management also includes the process of monitoring attempts at unauthorized access.

### **Security Management**



#### **Passwords**

A basic security measure is the use of passwords. Passwords limit access to network resources as follows:

- Users have passwords which only they can use
- Software, hardware, and directories can have passwords
- Passwords can be encrypted
- Audit trails and alarm systems can be implemented

#### **Alarm Login**



- Access Rights
  - Read only
  - Read/Write
  - None

When establishing the user id's and passwords for your network, administrators have to consider the community of your workplace from the perspective of their "need to know." Does the manager of finance need to know the status of the software development project to the point where they can view it online? Do the manufacturing managers need to know the status of ordered parts? Does the Executive Vice President's assistant need to know the salaries of every employee? These are the kinds of questions that can arise while establishing security.



In general, it is better to give users fewer rights than you think they might need and expand them later on. In addition to password security, rights to network resources can be assigned so that some users can have selective levels of access.

- Read Files
- Write to Files
- Create Files
- Delete Files
- List Files
- Change File Attributes
- Change Permissions

Network administrators cannot only implement individual passwords, they can create group passwords. With group rights, individuals can easily be added or removed.

For example, web page designers are part of the group called "Software Developers." This group has the rights to perform all file-related tasks listed above, but cannot change file attributes nor change permissions. The supervisor of this group might also be a member of an additional group, "Technical Managers." This group has the rights to change file attributes, and change permissions for those in the software developer group.

The security of the network can be compromised in two different ways: either from within the company and from outside infiltration. There are different tactics for dealing with each of these, and we will discuss them very briefly.

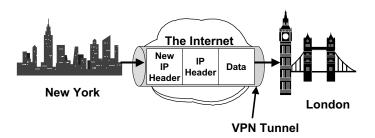
An irate or maladjusted employee usually causes internal threats. There may be someone on the staff who has just received a very poor performance evaluation. This person may realize they have little future with this company and try to cause harm by deleting files wherever possible.

#### **Firewalls**

Another security measure a network administrator can implement is a firewall. A firewall functions like a border guard at the security checkpoint at the border between two countries. When you enter/leave a country, the border guard asks for identification and possibly a passport and visa. The guard asks questions about your intentions (vacation, business trip, etc.), what you are bringing with you, etc. The firewall in a network performs the same security function as the border guard. A firewall can be either software or hardware. It prevents unwanted data from entering or leaving a network. It is the responsibility of the network manager to determine the levels of security needed.

Routers, gateways, and software are commonly used as firewalls to provide security through the use of passwords, encryption, and client authentication services. Industry encryption protocol examples include Secure Electronic Translation (SET), which is used for credit card transactions over the Internet; and, Pretty Good Privacy (PGP), which is a digital signature utility used for email. Client authentication services include such things as dial-back systems where a remote user dials in to the network, hangs up and the network dials-back to a pre-determined number. Or, global positioning systems that can actually tell where around the globe the remote user is physically located.

#### **Tunneling Security**





Virtual Private Networks (VPNs) use tunneling protocols such as Internet Protocol Security (IPSec) for security purposes. Tunneling and VPNs are discussed in the *Unified Networks/Emerging Technologies* course.

#### **Additional Services**

Additional services identified by OSI documents on security management include:

- Data integrity
  - Confirm that the source of data is as stated.
  - Confirm that the data has not been changed in transit.
  - Protect data from modification, deletion, or analysis. Services can ensure that data recovery procedures are executed or allow the network manager to specify that no recovery procedure can be attempted.
- Delivery of information
  - Guarantee accuracy, origin, timing, and delivery of information.
  - Select data paths that bypass certain networks for purposes of security through routing controls.
  - Control who can block the sending or receipt of information.

# **Check Your Understanding**

- Who can have passwords?
- What are some levels of password access?
- What is the function of a firewall?
- What is security management?
- ♦ List three ways of limiting access to network security.
- Name some areas where unauthorized users can gain access to the network.

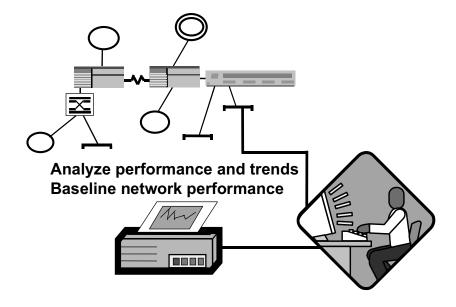


# **Performance Management**

Performance management involves gathering statistics that describe the various activities that occur in a network, usually for individual segments or subnets. By recording measurements periodically, you can identify changes or trends in network performance. These periodic measurements are referred to as benchmarks or baseline data. The primary network management tasks involved in performance management are:

- Planning for future needs
- Measuring system performance and trends through baselining network performance characteristics such as:
  - Activity
  - Errors
  - User response time
  - File transfer time
  - Network delay
  - Network traces
  - Setting thresholds

#### **Performance Analysis**



The only way a network manager can determine if there is a problem with the network is to know how it normally performs at all times. On a Monday morning, the network will probably slow down. Does that mean there is a problem? Not necessarily. First thing Monday morning is when most people access their email to get messages. There's nothing wrong with the network this is "normal" Monday morning traffic. Baselining allows a manager to become familiar with normal network activity. Problems are noted when the network veers from the established baseline.

There are several tools a network manager can use to monitor network performance.

# OmniView Ethernet 141.251.10.25 Display Pane Configuration File Help Last Poll: Use "Display" pulldown menu t RMON tools: Manager Console Version 7.2 File Config Tools 141.251.10.25 Global Statist 早里 Segm Statist WANsummary File Configure Configure View WAN Links Number of Entries: 1 Number of Entries: 2 LAN Nam 141.251.10.100\_seg 1123

## **OmniView and RMON Performance Management Tools**

Examples of tools network managers use for baselining include; Windows NT performance monitor, Sniffer Basic®, and Optivity.



To establish a baseline to determine the current network performance:

- Record any physical changes made to the network on the configuration map previously prepared (discussed under configuration management).
- Determine the baseline (normal, operational) performance of the network: track daily use, variation over time, and occurrence of different types of low-level errors.
- Keep a record of actual network use, which is the number of bits transmitted over the network.
- Examine link-level errors, such as frames that are too long. Collisions and runt frames (frames shorter than the minimum allowable).
- Record the types of protocols used on the network.
- Eliminate bottlenecks to improve resource availability.

Once a baseline is established, monitor the network for deviations.

#### **Performance Measurements**

The OSI management standard defines the following types of performance measurements:

- Workload—A measure of overload conditions.
- Throughput—A measure of successfully transmitted, error-free data.
- **Resource waiting time**—A measure of the amount of time data spends in queues.
- **Response time**—A measure of the amount of time between requests and acknowledgements.
- **Propagation delay**—A measure of the time between events such as the time between the transmission of data and a collision.
- Any quality of service (QoS) change—A measure of how objects should perform.

# **Check Your Understanding**

- List and describe the OSI performance management standards.
- What are some tools network managers use for baselining networks?
- What is performance management?
- ♦ What are the baselining performance characteristics used to measure system performance?
- What are the steps a network manager should take to establish a baseline for the purpose of determining current network performance?



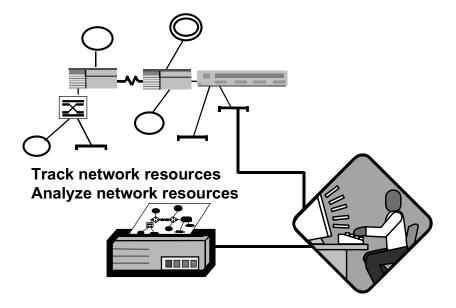
## **Accounting Management**

Accounting management involves tracking the use of network resources, analyzing the level of network resources available to specific groups or users, and assigning the cost for network use. Another aspect of accounting management involves managing corporate network assets and maintaining an accurate inventory of network devices and equipment.

The goal of accounting management is to ensure that users in an organization have the kinds of network resources they need to meet their objectives and that the cost of the network is accurately assigned.

In small networks, the manager may want to monitor the use of network disk storage space or network activity. Statistics about network use provide valuable data for performance, configuration, and fault management. In addition the data can be used for tracking and billing access time.

### **Accounting Management**



# **Check Your Understanding**

- What does network accounting management involve?
- ♦ What is the goal of network accounting management?

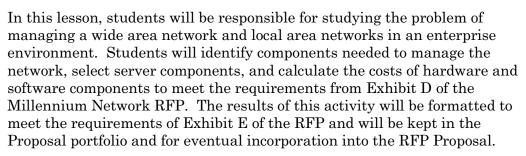


## Try It Out

#### **Materials Needed:**

- RFP
- Internet connection
- Word processing software
- Spreadsheet software (optional)
- Calculator (optional)





This activity is similar to the network management and control design activities undertaken by network designers as they plan and specify their networks.



Review RFP Exhibits D and E.

Your task is to design a Network Management and Control Center, the "Best Network Control Center." The Control Center's role is to assure nonstop operation of the campus network, which is capable of diagnosing and troubleshooting problems in the network at the six other sites.

- ◆ From your knowledge of Network Troubleshooting, the Optivity and Sniffer Software, and other tools, what is needed to manage this network?
- Make a draft list of the things (hardware and software) you think you will need.

#### Part 2: Identify and Estimate Management and Control Components

Determine network control and management tools to be used in the network. Create an estimate for the cost of the selected tools.



Get together with a small group of your classmates and compare your notes on the equipment needed.

When you come up with a list of necessary components to which you all agree, break the list down so each person has one or two items

- 1. Use the Internet to research competitive market prices for the management and control hardware and software. Two good Web sites to use are <a href="https://www.shopper.com">www.shopper.com</a> and <a href="https://www.shopper.com">www.cdwg.com</a>.
- 2. Put your list of items together in a word processing document for inclusion in your RFP portfolio.

### Part 3: Identify and Estimate Network Server Hardware and Software

Specify Server Hardware and Operating Software to manage and operate the Millennium Network.

The Network RFP specifies that the following are needed:

- Network operating systems licenses
- Network File Server Compaq 7000 or equivalent 1 GB RAM with 750 GB of RAID Storage

- Network Firewall and Proxy Server Compaq 3000 or equivalent 512 MB RAM – 50 GB Storage
- Network Management Control Server Compaq 1850 or equivalent 256 MB RAM – 36 GB Storage
- Racks, cables, and miscellaneous equipment
- Network management tools and software

For each of these items, get competitive market prices. Make sure the prices you get are for systems configured with the correct amount of memory and storage space.

When you calculate the number of workstations planned for the Network Operating System licenses, use the total of all users at all sites, with the growth factor included.

Select the operating system that gives you the best deal. Note that this price does not require you to include any application software for the network (word processing, spreadsheet, presentation, etc.) If you want to include an optional price for this you can.



#### Part 4: Prepare Cost Proposal for RFP

Consolidate the results of your calculations into a concise set of costs. Prepare documentation for submission in your Network RFP Proposal.

- 1. Put your price proposals for the Network Management and Control Center, and the Network Servers into a combined format similar to the prices you prepared for the telecommunications and hardware in an earlier activity.
- 2. Make a list of any items that you think will be required for the network, but were not requested. Discuss this list with your class.
- 3. You have now completed the last section of the RFP Proposal. Your teacher will give you instructions on presenting it to the class and the final paperwork required to submit the proposal.

## Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Read and understand a set of networking requirements in the RFP	25	
Determine network control and management tools to be used in network. You will create an estimate for the cost of the selected tools	25	
Specify Server Hardware and Operating Software to manage and operate the Millennium Network	25	
Consolidate the results of your calculations into a concise set of costs. Prepare documentation for submission in your Network RFP Proposal	25	
Other		
TOTAL	100	

#### Stretch Yourself

#### **Materials Needed:**

- Classroom Network
- Optivity software

## **Troubleshooting**

In this lab, you practice the skills required to identify and locate problems in Ethernet and token ring networks. You will use Optivity applications and options to monitor network and device faults. You will use SNMP notifications and Optivity tools to identify and locate problems.

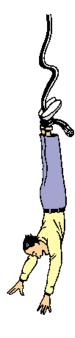
In this lab, your instructor creates problems on different devices, such as turning off the fan on a hub or disconnecting one interface on a router. You will use Optivity tools to view the status of the affected devices in different ways.

- 1. Monitor network faults at hub level using the Alarm panel and the Alarm Manager.
  - a. In the CCC Folders panel, click on the Hubs folder.
  - b. In the Contents panel, double-click any hub that has changed color.
  - c. In the Attributes panel, click the Alarm tab.
  - d. Click the Bell icon on the Alarm panel to view the alarms.
  - e. Read the details about the notification provided by the Alarm Manager.
- 2. Monitor network faults for a segment or ring using Flat Network View.
  - a. From the HP OpenView Internetwork View, choose Flatnet View from the Applications menu.
  - b. Click the right mouse button on a ring or segment icon, and choose Diagnostics from the Fault menu.

For token ring networks, you can also view isolating and non-isolating errors.

The Diagnostics window opens for the selected ring or segment.

- List the types of errors present in the space provided below:
- c. Close the Diagnostics window.
- d. Close the Flat Network View.





- 3. Monitor network faults for individual hubs using Segment View.
  - a. In the CCC Folders panel, click on the LANs folder.
  - b. Select your team's segment or ring and click the Map button.
    - The Segment View for the selected LAN appears.
  - c. Select Diagnostics from the Fault menu.
    - The Diagnostics window opens for the selected ring or segment.
  - d. Click the right mouse button on a hub and choose Status from the Fault menu.
    - The Status window is displayed for the selected hub. This window shows the current status of the hub.
  - e. Close the Status and Diagnostics windows.
  - f. Close the **Segment** View.
- 4. Monitor network faults for network nodes using NodalView.
  - a. In the CCC Folders panel, click on the LANs folder.
  - b. Select your team's segment or ring and click the Monitor button.
    - The NodalView for the selected LAN appears.
  - c. Double-click on one of the Errors columns.
    - The NodalView is displayed sorted by nodes with the highest selected error rate at the top of the window.
  - d. Click the right mouse button on the second pop—up menu in the NodalView portion of the window. Select each of the available options to view different MIB groups.
  - e. Click the right mouse button on Properties and choose Net Address to display device IP addresses.
  - f. Pull down the Configuration menu from the menu bar and choose Validate now to obtain current device information.

- 5. Monitor network faults for slots and ports using Expanded View.
  - a. In the CCC Folders panel, click on the Hubs folder.
  - b. In the Contents panel, click the right mouse button on a hub and choose Expanded View.

The Expanded View for the selected hub appears.

c. Click the right mouse button on a port and choose Diagnostics from the Fault menu.

The Diagnostics window opens for the selected port.

- d. Close the Diagnostics window.
- e. Click the right mouse button on a port or module and choose Status from the Fault menu.

The Status window is displayed for the selected port or module. This window shows the current status of the port.

- f. Close the Status window.
- g. Close the Expanded View.
- 6. Monitor router faults using RouterMan.
  - a. In the CCC Folders panel, click on the Routers folder.
  - b. In the Contents panel, click on a router.
  - c. On the toolbar, click the Monitor button.

The RouterMan window opens.

You can also click the right mouse button on the router icon and choose RouterMan from the menu that is displayed.

d. Click the right mouse button on the Fault icon in the Router section and select Fault Log.

The Fault Log window opens.

• What information is listed at the top of the display?



- Close the **Fault Log** window.
- e. Click the right mouse button on the IP Fault button in the Protocols section and select Statistics.
  - The Fault Statistics window opens for each protocol selected.
- f. Note the number of output packets with no routes. A large number of discards for this reason may indicate network configuration problems.
- ♦ How many header errors are shown?
- g. Click the right mouse button on the Ethernet Performance button in the Interface section and select History.
  - The Performance History window opens.
- h. Select the Options button on the toolbar of IP-Performance History.
- ♦ What are the seven headings for history data?
- i. Select the Threshold button on the toolbar of RouterMan.
- j. Change a threshold by moving the slide in the Router section.
- k. Select Apply from the toolbar.
- l. Select the Defaults button on the toolbar. Note all the settings reset to default.
- ♦ What percentage of errors are CRC?
- m. Close RouterMan.

- 7. Use BayStack 28xxx switch Fault Management options.
  - a. In the CCC Folders panel, click on the Switches folder.
  - b. In the Contents panel, click the right mouse button on a BayStack 28xxx switch and choose **Expanded View**.
  - c. In the Expanded View window, click the right mouse button on the port to reset.
  - d. Choose Reset from the Fault menu.
  - e. To display an error log for all ports, choose Error Log from the Expanded View Fault menu.
  - f. Select View and LANarchitect.

To display an error log for a particular port, click on the port in LANarchitect and choose the Diag button from the toolbar.

- ♦ What percentage of errors are CRC?
- g. Close the Diagnostic window for LANarchitect.
- h. Close the LANarchitect window.
- i. In Expanded View for the BayStack 28xxx switch, select the same port as viewed in LANarchitect. Use the right mouse button to select Fault and Diagnostics.
- ♦ How many CRC errors are shown?
- j. Close the Expanded View window.



# **Rubric: Suggested Evaluation Criteria and Weightings:**

Criteria	%	Your Score
Successful completion of activity	15	
Complete, accurate responses to lab activity questions	15	
Complete summary of experiences and an insightful analysis of how a network manager might use this software to help improve network performance.	20	
Summary included in portfolio	15	
Participation and cooperative teamwork during activity	20	
TOTAL	100	

#### **Network Wizards**

#### **Materials Needed:**

- Research materials on issues that face network managers/designers
- Internet connection



#### **Hot Topics for Network Designers and Managers**

Students will break into teams to explore a wide set of issues, which affect Network Management and Network Managers. They will report to the group on the impact, and solutions for each issue.

Issues may include, but not be limited to:

Network Management of Large Complex Systems

- Help Desks and Customer Support
- Maintaining Network Performance (Reliability & Availability)
- Viruses
- The Y2K Problem and beyond
- Keeping the Network Current
- The Impact of VoIP and Multimedia on the Network
- How to Stay Current on New Technologies

#### Part 1: Find Hot Topics in Networking

Research a wide range of issues that face Network Designers and Managers

How do network designers and managers stay current on all of the Hot Topics that face them? Through attendance at conferences, education, and reading networking publications, increasingly on-line. Network Magazine is one excellent example.

#### http://www.networkmagazine.com/

- 1. Explore the Internet to see if you can find other sources that will keep YOU informed on the issues of interest to network professionals. Find at least 5 online periodicals.
- 2. Use these periodicals to create a list of the top 10 Hot Topics that you think face networking professionals today.
- 3. Share and compare your lists with others in the class.
- 4. Put together a class list of the top Hot Topics.



## Part 2: Select One Hot Topic and Research it in Depth

Select a specific issue and study it in depth.

- 1. From the class list of Hot Topics in Networking each student will select a topic of interest to them
- 2. You will spend at least two hours researching the Hot Topic of your choice to understand the issue fully.
- 3. You will prepare a presentation on your Hot Topic which answers these questions:
  - What are the technologies involved?
  - What are the choices, options, or competing technologies?
  - Why is this a Hot Topic?
  - What is the impact on Networking Organizations?
  - What if Network Professionals ignore this Topic?
  - How does this affect the general public, if at all?

## Part 3: Present and Explain Your Hot Topic

Present and explain the issues to your classmates and discuss their implications.

- 1. Each student will make a 15 minute presentation to the class. Class members will be expected to ask thought provoking and probing questions of the presenter.
- 2. At the end of the presentations the class will vote on the three Hot Topics they feel will most affect the short term future of Networking and the two Hot Topics which will affect the long term future of Networking.

## Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Understand the wide range of issues which face Network Designers and Managers	25	
Identify specific issues and study them in depth	35	
Present and explain the issues to your classmates and discuss their implications	40	
Other		
TOTAL	100	



# **Summary**

# **Lesson 3: Network Management Responsibilities**

In this lesson, you learned to do the following:

- Define, compare and contrast OSI and TCP/IP management models
- Define and describe network configuration management
- Define and describe network performance management
- Define and describe network fault management
- Define and describe network security management
- Define and describe network accounting management

Unit 4 Review Questions

# **Review Questions**

## **Lesson 3: Network Management Responsibilities**

Multiple Choice: Select the best answer.

- 1. Which of the following is important in network management?
  - a. An up-to-date, accurate documentation on network architecture and design.
  - b. Graphical representation of the network
  - c. Revision history
  - d. Notation about kinds and locations of problems
  - e. All of the above
- 2. Which statement about report writing is false?
  - a. The ability of a technical manager to report effectively to a non-technical executive is very important.
  - b. Reports should include incorrect budgeting.
  - c. Reports should include any costs exceeding budget.
  - d. Reports should not include positive aspects of projects.
- 3. Connect the OSI managed object description with the corresponding example/definition on the right.

Behavior	a) Reports about events that occur, such as an error report
Attributes	b) Actions a managed object can perform such as replacing values or responding to certain events
Notifications	c) Values that an be set, added, removed or replaced, such as user permissions
Operatives	d) Object characteristics, such as a program that is active



- 4. Which of the following is not one of the network management functions specified in the ISO's Specific Management Information Services Specifications?
  - a. Configuration Management
  - b. Redundancy Management
  - c. Fault Management
  - d. Security Management
  - e. Performance Management
- 5. Which one of the following does not belong in configuration management?
  - a. Adding a new network segment
  - b. Developing a configuration map of the network software
  - c. Monitoring attempts of unauthorized access
  - d. Making sure only one version of software is operating
- 5. Which of the following statements about network backups is false?
  - a. Incremental backups only include data that has changed since the last full backup.
  - b. To do full backups every day takes unnecessary time, effort, and tape space.
  - c. Full backups are usually done during the day when more workers are available to help when problems occur.
  - d. Whether backups are full or incremental depends on the needs of the network.
- 6. Which one of the following statements about firewalls is false?
  - a. Firewalls can be either hardware or software.
  - b. Firewalls can provide security through passwords, encryption, and client authentication services.
  - c. Routers, gateways, and switches are commonly used as firewalls.
  - d. Client authentication includes dial-back systems.
- 6. Match the network management function with the appropriate activity.

Configuration Management	a) Set user passwords
Fault Management	b) Add a new device to the
	network

Unit 4 Review Questions

Security Management	<ul> <li>c) Use diagnostic tool to locate ar overloaded network device</li> </ul>
Performance Management	d) Track and bill access time
Accounting Management	e) Monitor file transfer time

- 7. Which one of the following examples of performance measurements is not correct?
  - a. Use of segment b has doubled Workload
  - b. 20% of packets are in error Throughput
  - c. Printing is very slow today Resource waiting time
  - d. Microsoft Word takes 3 minutes to load Resource waiting time
- 8. Which one of the following functions is not included in Accounting Management?
  - a. Protect data from modification or deletion
  - b. Analyze the level of network resources available to groups or individual users
  - c. Track use of network resources
  - d. Monitor network use and disk storage space



<b>Tr</b>	ue/False: Indicate whether each of the following statements is true or se.
1.	Making networking changes is one of the most difficult challenges a network manager can face.
2.	The focus of fault management is on the network devices and on physical and virtual connections, all of which operate in the upper four levels of the OSI reference model.
3.	Configuration tools often involve databases.
4.	To back up all program files all the time is expensive.
5.	The "child-parent-grandparent" method is not used often because it requires so many tapes.
6.	Disk duplexing is safer than disk mirroring, but more costly.
7.	When assigning permissions to users, it is better to give users extra rights so you will not need to modify them later.
8.	The more frequently data on a network changes, the more important a good backup system becomes.
9.	One of the most important aspects of being a good network manager is keeping clear, up-to-date documentation.
10.	Fault management involves identifying, isolating, and fixing problems, but not prevention measures.

Unit 4 Review Questions

## **Short Answer**

1. Briefly explain why, when using disk mirroring, it is important to document your controller's MTBF rating and total hours the controller has been used.

- 2. Briefly explain the similarities between Fault Management and Performance Management.
- 3. With Performance Management, briefly explain why it is so important to establish a network baseline.



# **Scoring**

Criteria	%	Your Score
Check Your Understanding		
Define, compare and contrast OSI and TCP/IP management models	20	
Define and describe network configuration management	20	
Define and describe network performance management		
Define and describe network fault management	20	
Define and describe network security management	20	
Define and describe network accounting management	20	
TOTAL	100	
Try It Out:	100	
Stretch Yourself:	100	
Network Wizards:	100	
Review	100	
FINAL TOTAL	500	

Unit 4 Resources

## Resources

Bay Networks, Inc. (1995). *Introduction to Network Management*. Bay Networks, Inc., Billerica, Massachusetts.

Bay Networks, Inc. (1998). Network Management with Optivity for Windows. Bay Networks, Inc., Billerica, Massachusetts.

Berg, Glenn (199). MCSE Networking Essentials: Next Generation Training. New Riders Publishing, Indianapolis, Indiana.

Craft, Melissa, Poplar, Mark A., Watts, David V., Willis, Will. (1999). *Network* +. The Coriolis Group, LLC, Scottsdale, Arizona.

Groth, David. Bergersen, Ben. Catura-Houser, Tim. (1999). *Network+Study Guide*. Sybex Inc., Alameda, California.

NortelNetworks<sup>TM</sup>. (June, 1999). *Network Design Essentials for Routers and Switches*, NortelNetworks<sup>TM</sup>, Billerica, Massachusetts.

Palmer, Michael J. Ph.D. (1998). *Hands-On Networking Essentials with Projects*. Course Technology, Cambridge, Massachusetts.

Parnell & Null. (1999). *Network Administrator's Reference*. Osborne/McGraw-Hill, Berkeley, California.

Sheldon, Tom. (1998). LANTIMES Encyclopedia of Networking, Elecetronic Edition. Osborne/McGraw-Hill, Berkeley, California.

