Lesson 5-2: Network Maintenance and Management

At a Glance

This lesson presents an overview of network planning and management tasks. It also discusses hardware and software tools, and defines terms associated with network planning and management.

What you will learn

In this lesson, you will learn how to:

• List and define criteria involved with network planning and management
• Explain the benefits of network planning
• Identify the need for network management
• Identify hardware devices and software tools used to gather information for network management and planning
• Cite examples of software tools used for network management and planning
Tech Talk

- **Quality of Service Analysis (QoS)**—Quality of service analysis, which uses management logs, and a model of how objects should perform are important components of this function.

- **Propagation Delay**—Propagation delay measures the time between events: the transmission of a data unit and the arrival of a collision notification from the remotest device.

- **Resource Waiting Time**—Resource waiting time measures the performance of queue lengths, time waiting for a service, time it takes to complete the service.

- **Response Time**—Response time is the time between the sending of a request and the acknowledgment or confirmation of receipt.

- **Throughput**—Throughput measures the network data that is successfully transmitted without errors. The throughput is measured in both directions, to and from a device - traffic that enters the network through the physical medium as well as traffic that leaves the network through the medium.

- **Workload**—Workload specifies requirements for measuring overload conditions and notification of such conditions. Warnings are set to indicate that additional workload will be rejected. Conditions for clearing the rejection warning must also be defined.

Network Maintenance and Management

There are five major elements to the maintenance and management of a network. They include:

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

The table below summarizes the tasks and managing objects used for each of these five areas.

Fault Management

When networks run mission-critical applications, quick resolution of problems is imperative. When a factory that has an automated manufacturing process “goes down” it can impact other areas of the company. Orders might not be filled, payroll might be late, new products
may not get to the market ahead of the competition, and so on. If a hospital network goes down, the downtime can mean failure of a life-saving operation.

Resolving network problems, or faults, is the job of the network manager. Fault management involves several steps. The network administrator must:

• Identify the problem
• Find ways to isolate the cause
• Correct the problem
• Prevent it from occurring again

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

**Identifying Network Problems**

Network problems range from the network being down and completely unavailable to the slowing down of one device, such as a printer. Problems can include the following:

• Hardware errors:
  – Stopped working
  – Will not start
  – Has slowed down
  – Produces intermittent errors

• Software errors:
  – Quits unexpectedly
  – Does not load
  – Does not work as described in the documentation
  – Does not work with other applications
  – Produces unexpected errors

• Data transmission errors:
  – Connection failure
  – Collisions
  – Congestion
Transmission errors

The distinction between hardware, software, and transmission problems is often indistinguishable and requires that system tools be constantly updated to keep up with networking improvements.

Device Isolation

If a user’s workstation fails, troubleshooting is a relatively simple procedure. Among the procedures/tools that aid in isolating a fault when an operational device suddenly fails include the following:

- Checking for loose connections
- Using diagnostic procedures that have been built into the device
- Use loopback tests to determine whether the correct logical connections exist
- On a TCP/IP network, use the ping command and netstat utility for basic troubleshooting assistance:
  - The ping command determines whether a device is connected and operating over the network.
  - The netstat utility shows the active device drivers on the interface cards, the number of datagrams sent and received, the routers that a given workstation has “learned” about, and the connections that are established.

Software Fault Isolation

If the hardware works, then software can be checked for:

- Configuration errors
- Conflicts with other applications in use

General Failure

In the case of a general failure, tools that check or monitor network activity and provide reports on network errors help determine and isolate the problem. If a device has not failed completely, it may have sent a message reporting that it was shutting down, or that a number of transmission errors had occurred.

If a device has failed without sending out a message, each network device may need to be checked in turn. These devices can be any of the following:

- A hub through which user workstations connect to the network
- A server where user applications and/or files are stored
- An internetworking device that connects one network to another
Data Transmission

Data transmission errors can be reported by monitoring devices. Protocol analyzers capture and examine actual data, showing which devices have been communicating, what protocols are actively in use and which transmissions have been experiencing errors.

Fault Management Tools

Fault management tools provide the network manager with information that helps to isolate problems and can be used for troubleshooting purposes, such as:

- **Event reporting**—Systems can be configured to report events such as the shutting down of a device, activation, or deactivation of a connection.

- **Diagnostic testing**—Diagnostic tools can determine the integrity of a cable, locate overloaded network devices, or diagnose protocol problems.

- **Alarm reporting**—devices can send an “alarm alert” to a monitoring device when given events occur or when thresholds are reached (the network is operating at 60% capacity, the storage device is 80% full).

Configuration Management

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 networks more complex, configurations must be customized in order to accommodate connectivity and interoperability and issues.

When devices and software work together well, configurations of network resources require no modification. However, the network manager needs to continuously monitor the state of the network to ascertain that the network is operating as desired. When needed, the network manager can make changes in logical and physical configurations for more effective network operation.

Modifying Configurations

The configuration of devices may need modification for the following reasons:

- Network changes
- Availability
Changes in the network may suddenly cause problems, making some vital aspect of the network malfunction. For example, a network with an unregistered IP address may now want to connect to the internetwork. Unless already configured, all IP addresses for devices on a network must be unique. The following graphic illustrates an address conflict that has occurred after a network has connected to an internetwork.

**IP Address Conflicts**

When a second file server is installed on a small network, the configuration of the first server may need to be changed so both servers can be used efficiently.

A device initially available to one group only may now need to be more generally accessible on the network. Access to files in a sales office database or on a mainframe computer in the main office may be limited to one site or even one group in the organization. As the organization grows, people in the new site might request access to these resources.
Lack of Use

Often the addition of a faster connection between two sites, or more efficient devices might cause a decrease in the use of the slower connection. It may be more cost-effective to eliminate the connection or move it to another workgroup. It may need to be discarded completely.

Objectives/Polices

Organizational objectives, such as the adoption of devices using the latest technology, can result in frequent configuration changes as these devices are introduced to the network.

Configuration Management

Responsibilities associated with managing configurations include the following:

- Developing a configuration map of the devices on the network. Having this map will help the network manager anticipate modifications needed when a new connection is added. If devices have been reconfigured from their default settings, that should be noted.

- Developing a configuration map of the software on the network. The configuration information should include memory requirements, memory buffers, driver settings and interoperability issues. A map will also help track and isolate problems.

- Adding devices to the configuration map so that it is current. Note which devices it is connected to and indicate any issues or concerns that should be monitored.

- Ensure that only one version of software is operating on the network and that all users are notified of version changes.

- Change the operational characteristics of managed objects and record any changes in the state of the objects.
  - Enabled: Not in use, but operational and available
  - Disabled: Not available, or dependent on another source that is not available
  - Active: Available and can accept services
  - Busy: Available, but cannot accept additional services
Performance Management

Performance management is a continuous monitoring and tuning process designed to:

- Measure system performance
- Determine if performance is satisfactory
- Adjust measurement criteria
- Plan for future needs

Establishing a Benchmark

Performance management starts with establishing a benchmark, or baseline, to determine the current network performance. For example, to collect baseline data, and keep track of data traffic and overall network use:

- 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 transmission 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
- Throughput
- Resource waiting time
- Response time
- Propagation delay
• Any quality of service (QoS) change

Workload specifies requirements for measuring overload conditions and notification of such conditions. Warnings are set to indicate that additional workload will be rejected. Conditions for clearing the rejection warning must also be defined.

Throughput measures the network data that is successfully transmitted without errors. The throughput is measured in both directions, to and from a device - traffic that enters the network through the physical medium as well as traffic that leaves the network through the medium.

Resource waiting time measures the performance of queue lengths, time waiting for a service, time it takes to complete the service.

Response time is the time between the sending of a request and the acknowledgment or confirmation of receipt.

Propagation delay measures the time between events: the transmission of a data unit and the arrival of a collision notification from the remotest device.

Quality of service analysis, which uses management logs, and a model of how objects should perform are important components of this function.

Security Management

The security measures required by a network depend upon:

• Sensitivity of the information

• Levels of access that are needed

A basic security measure is password assignment. Passwords limit access to network resources as follows:

• Users have passwords so that only authorized users can log on to the network.

• Passwords can also be assigned to software, hardware devices, and to directories on the network.

Passwords can be encrypted so that they cannot be easily decoded as they pass through the network system.

Audit trails and alarm systems (notification of unauthorized attempt to access a resource) add to these password security measures.

In addition to password security, rights to network resources can be assigned so that some users can have selective levels of access. For example, the network administrator and the person who maintains a database might have read-write rights, so that they can add, modify, or copy data. Other users can be granted rights to copy information from the
database, but not to modify the data. Still others might be able to add to the database, but not copy or modify the data. Finally, other users might be completely excluded from the use of the database.

Additional services identified by OSI documents on security management, but not yet defined, include those related to:

- **Data integrity**
  - Confirm that the source of the 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.

**Accounting Management**

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

Accounting specifications have not been completed by OSI. Rules under consideration include the use of accounting meters, which are triggers for updating data and for reporting usage.

**Network Management Tools**

A variety of hardware and software tools are available to support network management. SNMP compliant devices like routers and switches can transmit information to be collected by SNMP software applications. These applications can report configuration information, status or faults for a wide array of measurements. SNMP applications can also be used to control network devices and to change general network configuration. Many network devices include simple diagnostic displays on their front panels. Even network interface cards usually have some sort of diagnostic readout that can help diagnose status and fault information. Packet sniffing is useful for detecting problems in network transmission, which
may be either hardware or software related faults. Packet sniffer software applications like Sniffer Basic must be executed on a computer that is physically connected to the network. Some hardware sniffers are basically hand-held computers with network interface cards that must be connected to the network to capture packets. Others use inductive interfaces to capture packets without being directly connected to the network cable.

Check Your Understanding

♦ What are the five major areas of network management?

♦ Name three types of network problems:

♦ List areas for which the OSI has defined standards.

♦ What might a network administrator do to increase security management?

♦ Why is it important for a network administrator to establish benchmarks?
Try It Out

Mapping Network Topology

Materials Needed

- None

A visual map of network topology is a valuable tool for network management. The map can be generated as part of network planning, or used to document the current state of a network.

1. Draw a physical topology map of a simple network. Include a router, at least one switch, and several workstations and network printers. A physical map of network topology illustrates where devices actually connect, and actual cable locations and network speeds.

2. Now, for the same imaginary network, draw a logical topology map. A logical map will look similar to the physical map, but shows how traffic is segmented by subnetting, switching and addressing. It can also show workgroups or domain information. The logical map is useful for planning and trouble shooting network traffic management.

3. Talk with your school’s network system administrator and draw partial or full maps of your school network’s physical and logical network topology.

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maps legible, complete and detailed</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Demonstrated understanding of distinction between physical and logical topology</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Clear communication and independent interaction with system administrator to learn about school network</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
Stretch Yourself

Network Management

(This lab should not be done prior to Course 3 which teaches Network Management more specifically, additionally, this lab will have to be updated to use Optivity NMS 9.0 Campus version)

If you have access to Optivity Campus software:

Materials Needed

- Optivity Campus Software
- Optivity Campus documentation
- Internet connection (optional)

1. Run Optivity Campus on a computer that is connected to your classroom test network.

2. Study the software user’s guide and on-line help to learn how to produce network topology maps. Can the software produce both physical and logical maps? How does the software determine the topology?

3. Write an analysis of features provided by Optivity Campus. For each feature or tool in Optivity Campus, explain how a network administrator would use the feature in real network management.

4. Use the software to create graphical documentation of your network’s configuration. Which software features will you need to use? What sort of information will you need to provide manually, and what information can the software detect on its own?

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent exploration of features using printed and on-screen documentation</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Clear and concise report of features with associated relevance</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Successful use of Optivity Campus to document test network</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
Network Wizards

Developing a Network Plan

Work in teams to create a comprehensive network plan for a business.

Imagine that you are responsible for creating a network. Go through the following steps to create a plan for building a network that will meet your customers’ immediate needs, and can also be expanded for the future.

Materials Needed

- Internet connection (optional)

1. Defining the customer and their needs: Who is your (imaginary) customer? What are their computing and networking needs? Document details about your customer’s business objectives. What will they use their network for? What kinds of software do they use? Do they need to connect to the Internet?

2. Based on your analysis of your customer’s needs, design a network structure that will support the correct number of workstations, servers and printers. What type of transmission systems will they need? How fast do they need to communicate? Will they be using high-bandwidth applications like videoconferencing? Draw a detailed map of both the logical and physical topology of the new network.

3. Decide how to manage network traffic within the new network, and between the local network and the Internet or WAN. How will you organize the users into domains or workgroups to help predict and control network traffic? Will you deploy faster transmission systems between hubs and slower transmissions to the actual workstations? Will some workstations require higher-speed connection? How will you detect and fix traffic bottlenecks?

4. What security issues will your customers have? How will you provide security within the LAN environment, and how will you provide security against intrusions from the Internet or dial-up connections? What operating systems do your customers use, and how does that effect security?

5. EXTRA: Once you have planned the network, try to estimate the cost of setting it up. How much will the actual hardware, cabling and software cost? (Check on the Internet for prices) How many people and hours of labor will it take to get the network installed and operating? How much will you have to pay per hour for the labor?
Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thoughtful brainstorming and attention to detail</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Well formatted, readable planning documents</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Collaborative process and information sharing</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>

Summary

In this unit, you learned the following:

- Criteria involved with network planning and management
- The benefits of network planning
- How to identify the need for network management
- Identify hardware devices and software tools used to gather information for network management and planning
Review Questions

Lesson 5-2: Network Maintenance and Management

Part A

1. What are the four steps in the fault management process?

2. Name several hardware, software, and data transmission errors.

3. What are the five major elements to the maintenance and management of a network?

4. Network planning is driven by
   a. The fastest hardware
   b. Complete fault prevention
   c. The cheapest solution
   d. The requirements of the users
   e. Absolute security

Part B

1. Network planning allows you to
   a. Create a perfect network
   b. Create the largest possible network
   c. Meet current needs and anticipate maintenance and change
   d. Guarantee error-free service

2. Describe how network planning can ensure smoother operation later.
Part C

1. What are dangers of running a network without management?

Part D

Name five hardware devices or software tools that are used to gather information for network management and planning

1. ____________________
2. ____________________
3. ____________________
4. ____________________
5. ____________________

Scoring

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part A: List and define criteria involved with network planning and management</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Part B: Explain the benefits of network planning</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Part C: Identify the need for network management</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Part D: Identify hardware devices and software tools used to gather information for network management and planning</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Try It Out</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Stretch Yourself</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>For Network Wizards</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>FINAL TOTAL</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>
Resources


