Mount Kenya University

P.O BOX 13495-00100 GPO Nairobi.

Email: distance.learning@mku.ac.ke,

0700-912353, 0702-041042.

DEPARTMENT OF INFORMATION TECHNOLOGY

BBIT 3102:NETWORK MANAGEMENT

MBUGUA PHILIP

mbugua_mwenja@yahoo.com

BBIT 3102 NETWORK MANAGEMENT
Contact Hours 42
Pre-requisite BBIT 2203: Introduction to Business Data communication and computer networks
Purpose
To introduce basic techniques of managing a business information network operating systems.
Objectives
By the end of the course unit a learner shall be able to:

- Designing a physical computer network
- Selecting network devices and hardware for a business information network operating system.
- Managing day to day operations of a business information network.

Course Content:
Developing the physical network; preliminary groundwork, network foundations, planning networks strategies, policies and procedures of the organizations. Passing data across a network and choosing network gear. Planning server; strategies, application and administration. Server and network preparation; troubleshooting and optimization.
Configuring a network clients; hardware and connections software and configuration, training security and polices. Internet, intranet and extranets; terminology and technology, planning network strategies, preparations and hardware, security and polices, intranet and extranets running a web server. Outsourcing; types, choosing the hardware. Backing up the network, training users, troubleshooting. User and resource management, networking, monitoring and security issues. Case study: network operating systems projects.

Teaching Methodology
- Lectures
- Tutorials
- Computer Laboratory Exercises

Instructional materials/Equipment
- Audio visual aids in lecture rooms
- Network laboratory

Assessments; A learner is assessed through ;

Examination	- 60%
Continuous Assessment Test (CATS)	- 20%
Assignments	- 20%
Total	- 100%

Required text books

Plumley S.,Network Administration: Survival Guide, John Wiley (ISBN 0-471-29621-x)

Burges M., Principles of Network and System Administration, John Wiley and Sons

Text books for further reading

Winsnieski S., Advanced networking Administration, Prentice Hall

Stallings W., Network Security; Essential International Ed, Prentice Hall

Other support materials

Various application manuals and journals.

Variety of electronic resources as may be prescribed by the lecturer.

COURSE OUTLINE

WEEK 1 & 2
CHAPTER ONE: INTRODUCTION

- Definitions- Network, Node, Segment, Backbone, Topology;
- Network topologies; Bus, Star, Ring.
- Transmission Media.
- Network Protocols; OSI/TCPIP.

WEEK 3
CHAPTER TWO: NETWORK PLANNING

- Gathering user requirements
- Conducting site survey
- Network design principles.
- Assignment 1 : Develop a design for simple office network

WEEK 4
CHAPTER THREE: NETWORK H/W AND SOFTWARE

- Routers and Switches.
- Network Servers and Clients
- Network Operating Systems.

WEEK 5 & 6
CHAPTER FOUR : ACQUIRING NETWORK RESOURCES

- Procurement vs Outsourcing Options
- Request for proposals
- Acquisition process

WEEK 7 & 8
CHAPTER FIVE: CONFIGURING NETWORK DEVICES

- Server Configuration
- Client Configuration
- Connecting to the internet

WEEK 9

CHAPTER SIX: NETWORK SECURITY

- Firewalls.
- Intrusion detection systems(IDS).
- Security policies and procedures.
- Assignment 2 : Develop Network Security Policy for Medium Sized Company

WEEK 10

CHAPTER SEVEN: TROUBLESHOOTING NETWORK PROBLEMS

- Diagnostic tools
- Network management software

WEEK 11

CHAPTER EIGHT: DISASTER RECOVERY

- Risk assessment
- Risk mitigation Strategies
- Data backup and recovery techniques

WEEK 12 & 13

CHAPTER NINE: CASE STUDY

- Introduction to Linux Operating Systems
- Installation
- Configuration
- Security
- Diagnostic tools
- User management

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION 1
1.1 Definitions 1
1.2 Network Topologies 1
1.2.1 Physical Bus Topology 1
1.2.2 Physical Ring Topology 2
1.2.3 Physical Star Topology 3
1.2.4 Logical Topologies 4
1.2.5 Logical Bus Topology 4
1.3.2 Logical Ring Topology 6
1.2.6 Switching 7
1.3 Transmission Media 10
1.3.3 Wireless transmission 10
1.4 Network Protocols 11
1.4.1 TCP/IP Protocol 11
1.4.2 Open System Interconnection(OSI) Protocol 13
Review Questions 14
CHAPTER TWO: NETWORK PLANNING 15
2.1 Gathering Requirements 15
2.2 Selecting a topology 15
2.3 Conducting site Survey 16
2.4 Capacity Planning 16
2.5 Creating a Baseline 16
2.6 Designing the Network 17
2.7 Network Development Life Cycle(NDLC) 17
2.7.1 Analyze requirements 18
2.7.2 Develop the logical design 19
2.7.3 Develop the physical design 19
2.7.4 Factors That Affect a Network Design 20
2.8 IP Addresses and Address Classes 21
CHAPTERTHREE: NETWORK HARDWARE AND SOFTWARE COMPONENTS 25
3.1 Hardware and Software Components 25
3.1.1 Network Adapter(Network Interface Card) 25
3.1.2 Modem 26
3.1.3 Repeater 26
3.1.4 Hub 26
3.1.5 Switch 27
3.1.6 Wireless Access Point 27
3.1.7 Router 28
3.1.8 Residential Gateway 28
3.1.9 Gateway 29
3.2 Network Operating Systems 31
3.2.1 Choosing a NOS 32
3.2.2 Types 33

CHAPTER FOUR: PROCURING NETWORK RESOURCES 36
4.1 Introduction 36
4.2 Decision Making Strategy in Network Resource acquisition 36
4.3 IT Acquisition Process 37
Identifying the Business Objective 37
Implementing the Solution 41
CHAPTER FIVE: CONFIGURING NETWORK DEVICES 42
5.1 LAN network address 42
5.7 The LAN hardware 46
5.9 Configuring the LAN 47
5.10 Testing the LAN 52
5.11 Troubleshooting the LAN 54
5.12 Connecting to the Internet 55
Routing 56
Proxy servers 56
IP Masquerading (NAT) 58
Routing vs proxy servers vs IP Masquerading 59
CHAPTER SIX: NETWORK SECURITY 61
6.1 Security Issues 61
6.1.1 Common Attacks 62
6.1.2 Observing the Basics 63
6.2 Solutions to Security Issues 64
6.3 The Need for a Security Policy 68
6.3.1 Network Security Policy 69
6.3.2 Everything not specifically permitted is denied. 70
6.4 Incorporating Security into Your Network Design 71
6.4.1 Expecting the Worst, Planning for the Worst 71
CHAPTER SEVEN: TROUBLESHOOTING NETWORK PROBLEMS 74
7.1 Introduction 74
7.3 Network Management 75
7.4 Expectations 77
7.5 Functional Areas of Network Management 77
7.5.1 Fault Management 77
7.5.2 Configuration Management 78
7.5.5 Accounting Management 78
CHAPTER EIGHT: DISASTER RECOVERY 79
8.1 Introduction 79
8.2 What Is Risk With Respect To Network Systems? 80
8.3 Why Is It Important to Manage Risk? 82
8.4 Risk Assessment 82
8.4.1 Quantitative Risk Assessment 82
8.4.2 Qualitative Risk Assessment 83
8.4.3 Identifying Threats 84
8.4.4 Identifying Vulnerabilities 84
8.4.5 Relating Threats to Vulnerabilities 85
8.4.6 Defining Likelihood 86

8.4.7 Sample Likelihood Definitions 86
8.4.8 Defining Impact 87
8.4.9 How Is Risk Managed? 87
8.4.10 Communicating Risks and Risk Management Strategies 88

CHAPTER ONE: INTRODUCTION

1.1 Definitions

Network - A group of computers connected together in a way that allows information to be exchanged between the computers.

Node - Anything that is connected to the network. While a node is typically a computer, it can also be devices such as:

- Mainframes, minicomputers, supercomputers
- Workstations
- Printers, disk servers, robots
- X-terminals
- Gateways, switches, routers, bridges
- Cellular phone, Pager.
- Refrigerator, Television, Video Tape Recorder

Segment - Any portion of a network that is separated, by a switch, bridge or router, from other parts of the network.

Backbone - The main cabling of a network that all of the segments connect to. Typically, the backbone is capable of carrying more information than the individual segments. For example, each segment may have a transfer rate of 10 Mbps (megabits per second: 1 million bits a second), while the backbone may operate at 100 Mbps.

Topology - The way that each node is physically connected to the network.

1.2 Network Topologies

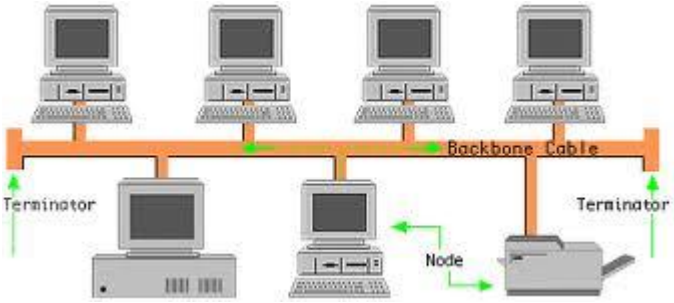
A network topology can be physical or logical.

Physical Topology is the actual layout of a network and its connections. Logical Topology is the way in which data accesses the medium and transmits packets. There are several network topologies:

1.2.1 Physical Bus Topology

Each node is daisy-chained (connected one right after the other) along the same backbone. Information sent from a node travels along the backbone until it reaches

its destination node. Each end of a bus network must be terminated with a resistor to keep the packets from getting lost.



Physical Bus Topology

Advantages

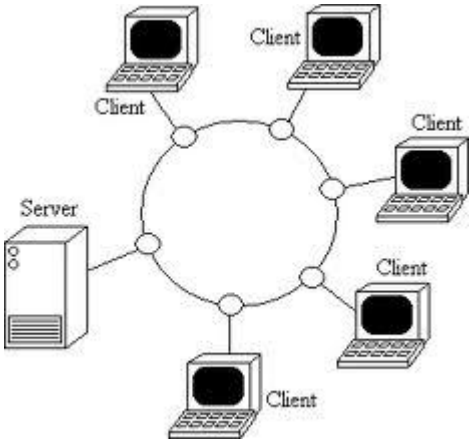
- Inexpensive to install.
- Easy to add stations.
- Use less cable compared to other topologies.
- Works well for small networks.

Disadvantages

- No longer recommended, due to frequent collisions of packets
- If backbone breaks, whole network down
- Limited no of devices can be attached
- Difficult to isolate problems.
- Sharing same cable slows response rates

1.2.2 Physical Ring Topology

Similar to a bus network, rings have nodes daisy chained, but the end of the network in a ring topology comes back around to the first node, creating a complete circuit. Each node takes a turn sending and receiving information through the use of a token. The token along with any data is sent from the first node to the second node which extracts the data addressed to it and adds any data it wishes to send. Then second node passes the token and data to the third node, etc. until it comes back around to the first node again. Only the node with the token is allowed to send data . All other nodes must wait for the token to come to them.



Physical Token Ring

Advantages

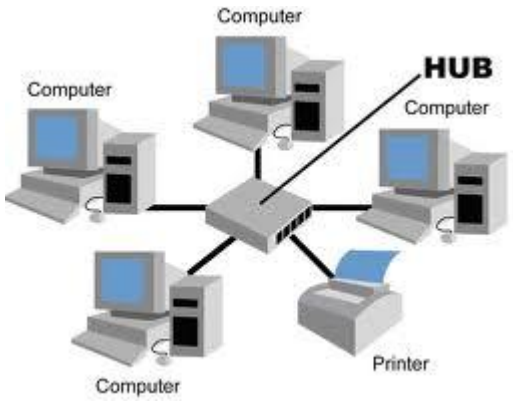
- Data packets travel at great speed
- No collisions
- Easier to fault find
- No terminators required

Disadvantages

- Requires more cable than a bus
- A break in the ring will bring it down
- Not as common as the bus – less devices available

1.2.3 Physical Star Topology

In a star network, each node is connected to a central device called a hub. The hub takes a signal that comes from any node and passes it along to all the other nodes in the network. A hub does not perform any type of filtering or routing of the data. A hub is a junction that joins all the different nodes together.



Advantages

- Easy to add devices as the network expands
- One cable failure does not bring down the entire network (resilience)
- Hub provides centralised management
- Easy to find device and cable problems
- Can be upgraded to faster speeds
- Lots of support as it is the most used

Disadvantages

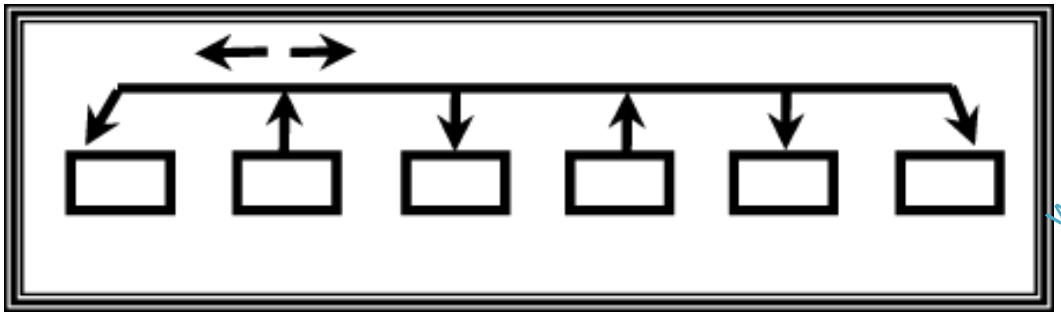
- A star network requires more cable than a ring or bus network
- Failure of the central hub can bring down the entire network
- Costs are higher (installation and equipment) than for most bus networks

Star networks can be extended by interconnecting several hubs to form segments.

1.2.4 Logical Topologies

There are three logical topologies (bus, ring, and switching) which are usually implemented as a physical star.

1.2.5 Logical Bus Topology



HUB

Modern Ethernet networks are Star Topologies (physically) but logically they are bus topologies. The Hub is at the centre, and defines a Star Topology.

In any network, computers communicate by sending information across the media as a series of signals. In a logical bus topology, the signals travel along the length of the cable in all directions until they weaken enough so as not to be detectable or until they encounter a device that absorbs them. This traveling across the medium is called **signal propagation**

When a computer has data to send, it addresses that data, breaks it into manageable chunks, and sends it across the network as electronic signals

- All computers on a logical bus receive them
- Only the destination computer accepts the data
- All users must share the available amount of transmission time, implying network performance is reduced
- Collisions are bound to occur since all nodes are sharing same bus.

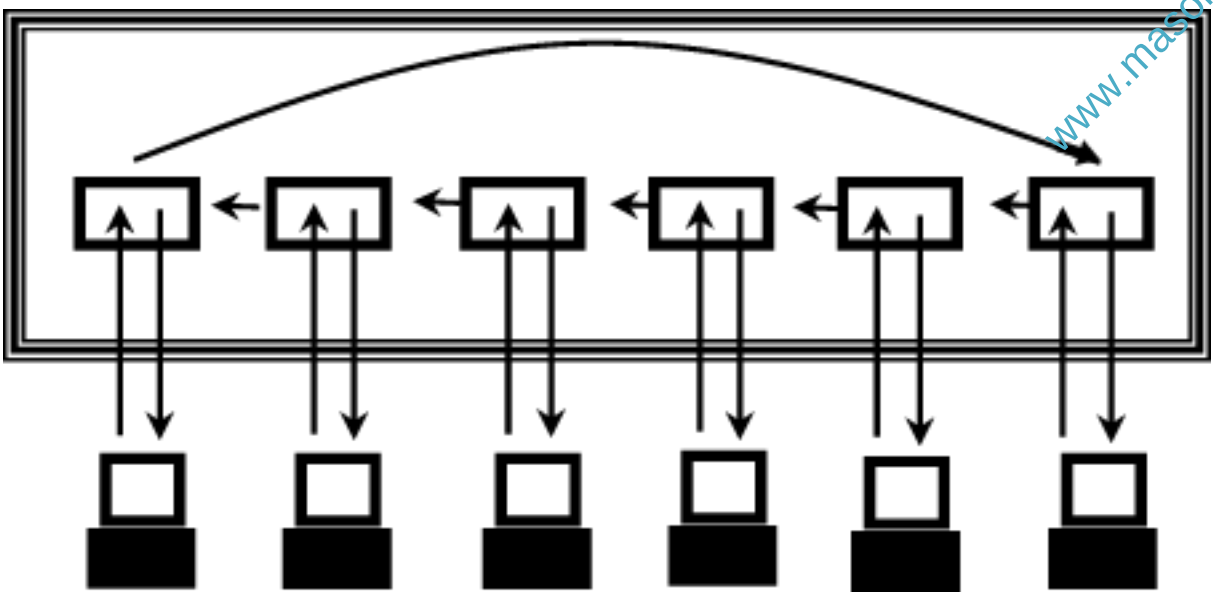
Advantages

- A single node failure does not bring the network down
- Most widely implemented topology
- Network can be added to or changed without affecting other stations

Disadvantages

- Collisions can occur easily
- Only one device can access the network media at a time

1.3.2 Logical Ring Topology



Multiple Access Unit(MAU)

Data in a logical ring topology travels from one computer to the next computer until the data reaches its destination. Token passing is one method for sending data around a ring

Token is a small packet which passes around the ring to each computer in turn.

If a computer (sender) has packets to send, it modifies the token, adds address and data, and sends it around the ring. The receiver returns an acknowledgement packet to the sender.

Upon receiving the acknowledgement packet, the sender releases the tokens and sends it around the ring for another sender to use.

Logical ring can be implemented on a physical star. Modern logical ring topologies use “smart hubs” that recognize a computer’s failure and remove the computer from the ring automatically. One advantage of the ring topology lies in its capability to share network resources fairly.

Advantages

- The amount of data that can be carried in a single message is greater than on a logical bus.
- There are no collisions.

Disadvantages

- A broken ring will stop all transmissions.
- A device must wait for an empty token to be able to transmit.

1.2.6 Switching

A switch takes a signal coming from a device connected and builds a circuit on the fly to forward the signal to the intended destination computer

Superior to other logical topologies because unlike bus and ring, multiple computers can communicate simultaneously without affecting each other. Switching is the dominant logical topology in LAN design.

1.3 Transmission Media

This refers to the mode in which messages are delivered from one node to another over the network. There are several types of media:

1.3.1 Guided Transmission Media - uses a conductor cable to transmit data e.g. twisted pair(shielded/unshielded), coaxial cable.

Twisted pair Cable

Twisted pair is two insulated copper wires that are twisted around each other to minimize interference and noise from other wires. Based on the presence of individual shield and overall (outer) shield, there are three types of twisted pair, i.e. UTP, STP, and ScTP. Individual shield encloses a single twisted pair, while outer shield encloses all twisted pairs in a cable. A shield is a protective sheath that is made from conductive material (metal) and functions to protect the twisted

pair from external interference. An insulator is made from non-conductive material, such as plastic.

UTP (Unshielded Twisted Pair) is a cable containing several twisted pairs that is only insulated but not shielded. UTP is the most widely used cable in telephone and computer networks because it is relatively cheaper than other cables and performs well in normal electrical environment such as inside an office or a house.
Coaxial cable contains a solid or stranded wire in the core that is insulated with a dielectric layer, then protected with a solid or braided metallic shield, and covered with an outer insulator. Electromagnetic wave propagation in a coaxial cable is confined within the space between the core and the outer conductors. The structure of a coaxial cable makes it less susceptible to interference, noise, and crosstalk than the twisted pair cable.

Coaxial Cable

1.3.2 Glass or plastic - Uses optical technology to transmit data using light waves e.g. fiber optics

Fibre Optic Cable

Fiber-optic cable or optical fiber provides a medium for signals using light rather than electricity. Light waves are immune to electromagnetic interference and crosstalk. Optical fiber can be used for much longer distances before the signal must be amplified. Data transmission using optical fiber is many times faster than with electrical methods.

1.3.3 Wireless transmission - Uses air interface to transmit e.g. microwave, satellite. Microwave links are widely used to provide communication links when it is

impractical or too expensive to install physical transmission media. Two properties of microwave transmission place restrictions on its use. First, microwaves travel in a straight line and will not follow the earth's curvature. Second, atmospheric conditions and solid objects interfere with microwaves. For example, they cannot travel through buildings.

Satellite transmission is microwave transmission in which one of the stations is a satellite orbiting the earth. A microwave beam is transmitted to the satellite from the ground. This beam is received and retransmitted (relayed) to the predetermined destination. Receiver and transmitter in satellites is known as transponder.
The optimum frequency range for satellite transmission is in the range 1 to 10 GHz. Below 1 GHz, there is significant noise from natural sources,

atmospheric noise, and noise from electronic devices. Above 10 GHz, the signal is attenuated by atmospheric absorption.

1.4 Network Protocols

Communication between devices on a network is governed by a set of rules called protocols. There are two types of network protocols, TCP/IP and OSI.

1.4.1 TCP/IP Protocol

TCP/IP is responsible for a wide range of activity: it interfaces with hardware, route data to appropriate nodes, provides error control, and much more.

The developers of TCP/IP designed a modular protocol stack- meaning that the TCP/IP system was divided into separate components or layers. But why use a modular design? Not only does it aid in the education process, but it also lets manufacturers easily adapt to specific hardware and operating system needs.

For example- if we had a token ring network and an extended star network, we surely wouldn't want to create entirely different network software builds for each one. Instead, we can just edit the network layer, called the Network Access Layer, to allow compatibility. Not only does this benefit manufacturers, but it greatly aids networking students in education. The TCP/IP suite is divided into four layers.

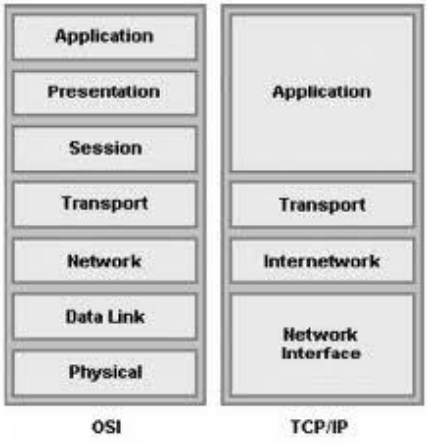
Network Access Layer – The Network Access Layer is fairly self explanatory- it interfaces with the physical network. It formats data and addresses data for subnets, based on physical hardware addresses. More importantly, it provides error control for data delivered on the physical network.

Internet Layer – The Internet Layer provides logical addressing. More specifically, the internet layer relates physical addresses from the network access layer to logical addresses. This can be an IP address, for instance. This is vital for passing along information to subnets that aren't on the same network as other parts of the network. This layer also provides routing that may reduce traffic, and supports delivery across an internetwork. (An internetwork is simply a greater network of LANs, perhaps a large company or organization.)

Transport Layer – The Transport Layer provides flow control, error control, and serves as an interface for network applications. An example of the transport layer

would be Transmission Control Protocol (TCP) - a protocol suite that is connection-oriented. We may also use UDP- a connectionless means of transporting data.

Application Layer – Lastly, we have the Application Layer. We use this layer for troubleshooting, file transfer, internet activities, and a slew of other activities. This layer interacts with many types of applications, such as a database manager, email program, or Telnet.



1.4.2 Open System Interconnection(OSI) Protocol

The International Organization of Standardization (ISO) defined procedures for computer communications which was called Open System Interconnection (OSI) Reference Model or OSI Model for short. The OSI Model describes how data flows from one computer to another computer in a network.

The OSI Model

The Open System Interconnection Model, more commonly known as simply OSI, is another model that can help break the TCP/IP suite into modules. Technically speaking, it is exactly the same as the TCP/IP model, except that it has more layers. This is currently being pushed by Cisco since it aids in learning the TCP/IP stack in an easier manner.

Physical Layer – They Physical Layer converts data into streams of electric or analog pulses- commonly referred to as "1's and 0's." Data is broke down into simple electric pulses, and rebuilt at the receiving end.

Data Link Layer – The Data Link layer provides an interface with the network adapter, and can also perform basic error checking. It also maintains logical links for subnets, so that subnets can communicate with other parts of the network without problem.

Network Layer – Much like the Transport Layer of the TCP/IP model, the Network Layer simply supports logical addressing and routing. The IP protocol operates on the Network Layer.

Transport Layer – Since we left out the error and flow control in the Network Layer, we introduce it into the Transport Layer. The Transport Layer is responsible for keeping a reliable end-to-end connection for the network.

Session Layer – The Session Layer establishes sessions between applications on a network. This may be useful for network monitoring, using a login system, and reporting. The Session Layer is actually not used a great deal over networks, although it does still serve good use in streaming video and audio, or web conferencing.

Presentation Layer – The Presentation Layer translates data into a standard format, while also being able to provide encryption and data compression. Encryption or data compression does not have to be done at the Presentation Layer, although it is commonly performed in this layer.

Application Layer – The Application Layer provides a network interface for applications and supports network applications. This is where many protocols such as FTP, SMTP, POP3, and many others operate. Telnet can be used at this layer to send a ping request- if it is successful, it means that each layer of the OSI model should be functioning properly.

Review Questions

i) Define a the following terms:
   a) Protocol
   b) Network
   c) Physical Topology
   d) Logical Topology

ii) Differentiate between TCP/IP and OSI protocols and give the benefits of each.

iii) Describe the biggest limitation of bus topology.

CHAPTER TWO: NETWORK PLANNING

2.1 Gathering Requirements

Every organization has unique needs for which they would require a network. There are several factors to consider when gathering requirements:

- Identify the nature and volume of data and how it is used within and outside the organization.
- Determine how the network will be used and by whom which often dictates the topology you use. Location of data with respect to users is also critical here.
- Decide the types of devices for interconnecting computers and sites
- The type and usage level of network resources dictates how many servers you need and where to place servers.

2.2 Selecting a topology

Most new network designs come down to only one choice: How fast should the network be?

This will be guided by the needs identified earlier, in particular the location of sites, volume of data and nature of existing equipment and consideration for future expansion.

In most cases the physical topology will almost certainly be a star, and the logical topology is almost always switching. Ethernet switches are typically used on a LAN, but you might consider other logical topologies for reasons such as:

- Use of legacy equipment – such as token ring
- Network size – using hub-based bus topology
- Cost restrictions – using hub instead of switch
- Difficulty to run cables – consider wireless ?

2.3 Conducting site Survey

The purpose of a site survey is to understand the nature of the business premises in terms of how the building, office space and electrical wiring are set up. It helps answer whether or not the type of network requested can be supported by the organization of the building. It also helps estimate how much material will be required to layout the network.

2.4 Capacity Planning

Capacity planning involves trying to determine the amount of network bandwidth necessary to support an application or a set of applications.

A number of techniques exist for performing capacity planning, including linear projection, computer simulation, benchmarking, and analytical modeling.

Linear projection involves predicting one or more network capacities based on the current network parameters and multiplying by some constant.

A computer simulation involves modeling an existing system or proposed system using a computer-based simulation tool.

Benchmarking involves generating system statistics under a controlled environment and then comparing those statistics against known measurements.

Analytical modeling involves the creation of mathematical equations to calculate various network values.

2.5 Creating a Baseline

Involves the measurement and recording of a network's state of operation over a given period of time.

A baseline can be used to determine current network performance and to help determine future network needs.

Baseline studies should be ongoing projects, and not something started and stopped every so many years.

To perform a baseline study, you should:

- Collect information on number and type of system nodes, including workstations, routers, bridges, switches, hubs, and servers.
- Create an up-to-date roadmap of all nodes along with model numbers, serial numbers and any address information such as IP or Ethernet addresses.
- Collect information on operational protocols used throughout the system.
- List all network applications, including the number, type and utilization level.
- Create a fairly extensive list of statistics to help meet your goals. These statistics can include average network utilization, peak network utilization, average frame size, peak frame size, average frames per second, peak frames per second, total network collisions, network collisions per second, total runts, total jabbers, total CRC errors, and nodes with highest percentage of utilization.

2.6 Designing the Network

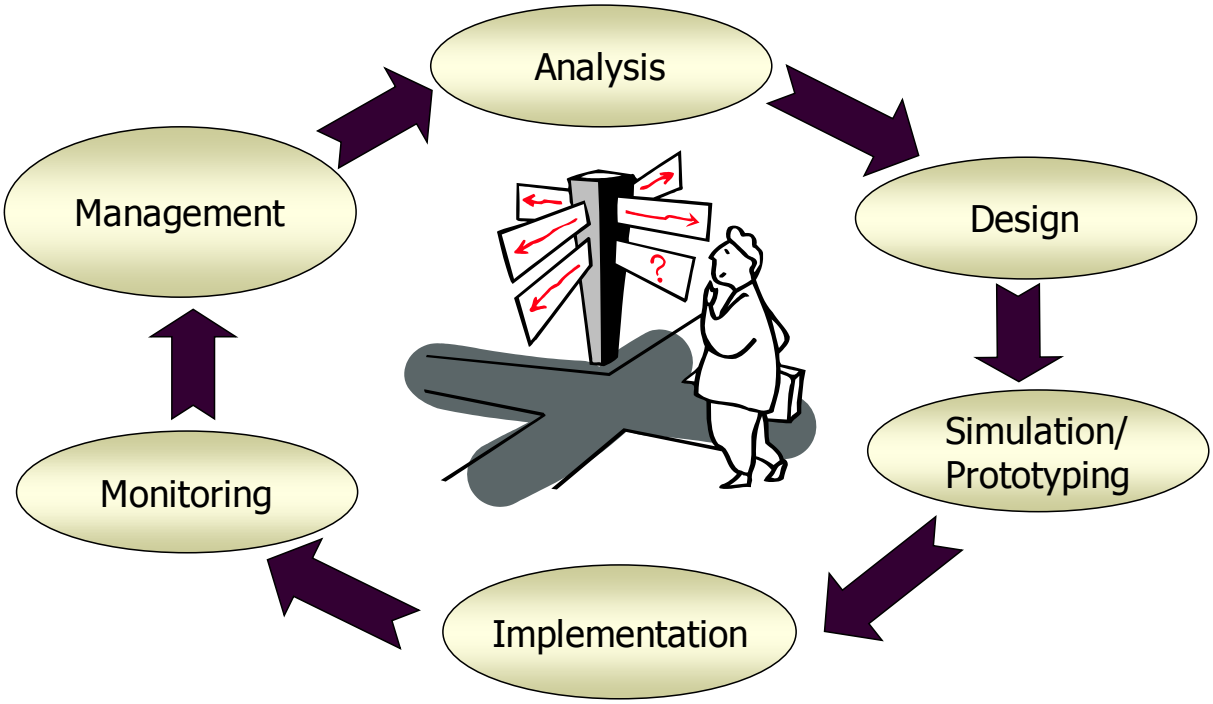
A network design must be documented, and network diagram must be kept up to date.

Some useful questions to be answered before drawing the diagram:

- How many client computers will be attached?
- How many servers will be attached?
- Will there be a connection to the Internet?
- How will the building's physical architecture influence decisions, such as whether to use a wired or wireless topology, or both?
- Which topology or topologies will you use?

2.7 Network Development Life Cycle(NDLC)

The NDLC is a model that summarizes the network design process, from initial problem/needs assessment to implementation.



2.7.1 Analyze requirements

A network cannot very well provide effective solutions to problems that have not been clearly defined in objective terms. To attempt to implement networks before everyone agrees to (buy-in) the exact nature of the problem to be solved is somewhat akin to hitting a moving target. The network will never satisfy all constituencies' needs because no one agreed what those needs were in the first place. All network development efforts start with a problem as perceived by someone, be they management or end-users. At some point, management agrees that a problem exists that is worth expending resources to at least investigate. The responsibility for conducting the investigation may be given to in-house personnel or to an outside consultant or facilitator.

- Interviews with users and technical personnel
- Understand business and technical goals for a new or enhanced system

- Characterize the existing network: logical and physical topology, and network performance
- Analyze current and future network traffic, including traffic flow and load, protocol behavior, and QoS requirements

2.7.2 Develop the logical design

An IP network has two very important resources, its IP addresses and the corresponding naming structure within the network. To provide effective communication between hosts or stations in a network, each station must maintain a unique identity. In an IP network this is achieved by the IP address. The distribution and management of these addresses is an important consideration in an IP network design. IP addresses are inherently not easy to remember. People find it much easier to remember names and have these names related to individual machines connected to a network. Even applications rarely refer to hosts by their binary identifiers, in general they use ASCII strings such as polo@mku.ke. These names must be translated to IP addresses because the network does not utilize identifiers based on ASCII strings. The management of these names and the translation mechanism used must also be considered by the IP network designer.

2.7.3 Develop the physical design

Specific technologies and products to realize the logical design are selected. The investigation into service providers must be completed during this phase.

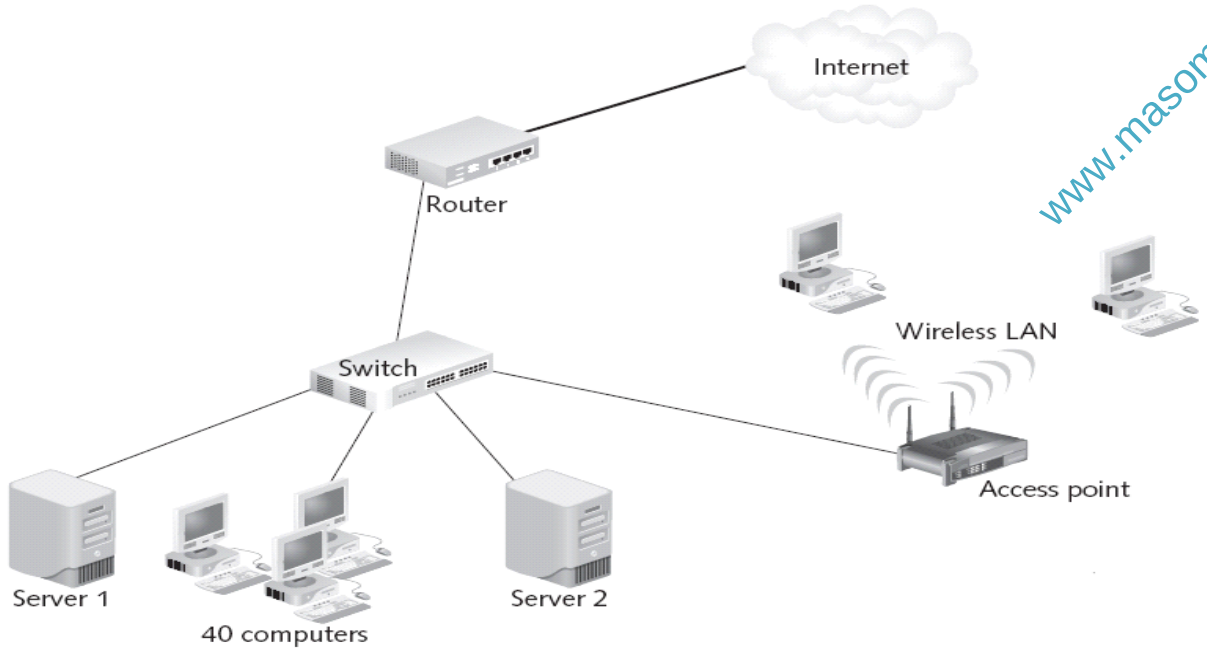


Figure 2-13 A simple network layout diagram

Network Layout Diagram

2.7.4 Factors That Affect a Network Design

Designing a network is more than merely planning to use the latest gadget in the market. A good network design takes into consideration many factors:

Size Matters

At the end of the day, size does matter. Designing a LAN for a small office with a few users is different from building one for a large company with two thousand users. In building a small LAN, a flat design is usually used, where all connecting devices may be connected to each other. For a large company, a hierachical approach should be used.

Geographies

The geographical locations of the sites that need to be connected are important in a network design. The decision making process for selecting the right technology and equipment for remote connections, especially those of cross-country nature, is different from that for a LAN. The tariffs, local expertise, quality of service from service providers, are some of the important criteria.

Politics

Politics in the office ultimately decides how a network should be partitioned.

Department A may not want to share data with department B, while department C allows only department D to access its data. At the network level, requirements such as these are usually done through filtering at the router so as to direct traffic flow in the correct manner. Business and security needs determine how information flows in a network and the right tool has to be chosen to carry this out.

Types of Application

The types of application deployed determines the bandwidth required. While a text-based transaction may require a few kbps of bandwidth, a multimedia help

2.8 IP Addresses and Address Classes

An IP address is defined in RFC 1166 - Internet Numbers as a 32-bit number having two parts:

IP address = <network number><host number>

The first part of the address, the network number, is assigned by a regional authority and will vary in its length depending on the class of addresses to which it belongs. The network number part of the IP address is used by the IP protocol to route IP datagrams throughout TCP/IP networks. These networks may be within your enterprise and under your control, in which case, to some extent, you are free to allocate this part of the address yourself without prior reference to the Internet authority, but if you do so, you are encouraged to use the private IP addresses that have been reserved by the Internet Assigned Number Authority (IANA) for that purpose.

However if your routing may take you into networks outside of your control, using for example, the worldwide services, it is imperative that you obtain a unique IP address from your regional Internet address authority.

The second part of the IP address, the host number, is used to identify the individual host within a network. This portion of the address is assigned locally within a network by the authority that controls that network. The length of this number is, as mentioned before, dependent on the class of the IP address being used and also on whether subnetting is in use. (subnetting is beyond the scope of this course).

The 32 bits that make up the IP address are usually written as four 8-bit decimal

values concatenated with dots (periods). This representation is commonly referred to as a dotted decimal notation. An example of this is the IP address 172.16.3.14. In this example the 172.16 is the network number and the 3.14 is the host number. The split into network number and host number is determined by the class of the IP address.

Class A addresses have the first bit set to 0. The next 7 bits are used for the network number. This gives a possibility of 128 networks (2^7). However, it should be noted that there are two cases, the all bits 0 number and the all bits 1 number, which have special significance in classes A, B and C.

The remaining 24 bits of a Class A address are used for the host number. Once again, the two special cases apply to the host number part of an IP address. Each Class A network can therefore have a total of 16,777,214 hosts (224 -2). Class A addresses are assigned only to networks with very large numbers of hosts (historically, large corporations). An example is the 9.0.0.0 network, which is assigned to IBM.

The Class B address is more suited to medium-sized networks. The first two bits of the address are predefined as 10. The next 14 bits are used for the network number and the remaining 16 bits identify the host number. This gives a possibility of 16,382 networks each containing up to 65,534 hosts.

The Class C address offers a maximum of 254 hosts per network and is therefore suited to smaller networks. However, with the first three bits of the address predefined to 110, the next 21 bits provide for a maximum of 2,097,150 such networks.

The remaining classes of address, D and E, are reserved classes and have a special meaning. Class E addresses are reserved for future use while Class D addresses are used to address groups of hosts in a limited area. This function is known as multicasting.

Review Questions

i) Describe the process of gathering user requirements for a small network.

ii) Why is it important to consider future expansion when planning for a

	network?
iii)	Briefly describe the five network classes.
iv)	Differentiate between a public and a private IP address
v)	How many hosts can the following network have : 172.16.0.0

CHAPTERTHREE: NETWORK HARDWARE AND SOFTWARE COMPONENTS

3.1 Hardware and Software Components

A network component's functions are not necessarily handled by a specific device. Many devices combine several networking functions. For example: a router could have a built-in switch, a residential gateway that includes a broadband modem, etc. So, be sure to check the product specification before buying to avoid duplication. You must also check interfaces that are supported by a product. They must be compatible with the ports available in your computers or other devices.

A network component's functions may also be performed by a software application. For example, Windows XP provides built-in support for Network Bridging that handle a bridge's functions in a home network with mixed media. There are also built-in or add-on software applications that handle modem, router, or gateway functions. However, the software-only alternative is mostly suitable for small networks. Some of the hardware components are:

3.1.1 Network Adapter(Network Interface Card)

Network adapter works as an interface between a computer or device and a network. You may need Ethernet, Wi-Fi, HomePNA, or HomePlug network adapter depending on the type of network your computer is connecting to. Network adapter converts a computer message into electrical or optical signals for transmission across the network. A network adapter is identified in a network through a MAC address that is hard-coded onto the hardware by its manufacturer.

Network Adapter Cards

Built-in network adapter is integrated with a computer motherboard. Internal network adapter is installed inside a computer on an expansion slot. It is often called NIC (network interface card) usually inserted into a PCI slot in a PC or a mini PCI slot in a notebook.

3.1.2 Modem

Modem means modulator-demodulator. At the sending end, a modem modulates a carrier with the data (baseband signal) to prepare it for transmission. At the receiving end, the modulated carrier is demodulated (i.e. converted back to the original shape) and the data is extracted. A modem also performs other functions, such as digital-to-analog/analog-to-digital conversion, compression/decompression, error correction, and encryption/decryption.

Modem in Internet access

3.1.3 Repeater

Repeater receives signal from a transmitter, amplifies it, and retransmits it to a receiver. A repeater is put in a network to extend the network to a longer distance or a greater area. There can be more than one repeater between a transmitter and a receiver, however the number of repeaters is not unlimited, because additional repeaters may introduce more interference or noise.

Repeater

3.1.4 Hub

Hub is the central connection point in a network. Hub is used in a network that uses star topology. A sending computer transmits its signal to a hub, the hub then retransmits the signal to all other computers. A passive hub functions as a relay station that receives and retransmits signal. An active hub functions as a repeater that regenerates signal before retransmitting.

Hub

Using a hub, the network bandwidth (capacity) is shared by all available computers, therefore each computer only uses a portion of bandwidth. That's why hub is mostly used in small networks where there are only a few connected devices or computers. However, hub is not required if there are only two computers in a network. In that case, a direct connection using cable or wireless link can be used to connect both computers.

3.1.5 Switch

Like hub, switch works as the central connection point in a network. However when a switch receives a packet from a sending computer, it examines the destination address (i.e. MAC address of the destination computer) from the packet header and retransmits the packet to the destination computer only. That's possible because a switch maintains a table that maps all its ports with all connected devices' MAC addresses.

Switch

3.1.6 Wireless Access Point

Access point in a wireless LAN (Wi-Fi) functions like a hub or a switch in wired network. It connects computers or devices together to create a wireless network. Most wireless access points also function as a network bridge that connects the Wi-Fi network to a wired network such as Ethernet. An access point has an interface to a broadband modem or a router that is used when the Wi-Fi network connects to the Internet. Some access points come as a multi-function device that incorporates the functions of switch, bridge, router, or broadband modem. An access point is also known as base station.

Wireless (Wi-Fi) Access Point.

Data transfer rate decreases as the distance from a computer or a device to the access point increases. A Wi-Fi access point provides wireless network coverage

within an area of up to about 100 meters outdoor. In typical indoor application, an access point can cover an area of up to about 50 meters. The exact coverage depends on the access point transceiver and antenna design. Physical obstacles and interference from other wireless networks can reduce the wireless signal range.
An area that is within a Wi-Fi network coverage is popularly known as hotspot. Many public places such as airports, hotels, and cafs provide public Wi-Fi hotspots that have broadband connection to the Internet. Such hotspots can be accessed by the public for free or with a fee. To connect to a Wi-Fi hotspot, your wireless network adapter must be compatible with the hotspot's access point.

3.1.7 Router

Router functions to forward packets across different networks. Router maintains a routing table. The routing table contains IP addresses of other networks routers. In a static router the routing table is configured manually, while a dynamic router can communicate with other routers and configure the routing table according to information it receives from other routers.

Router in OSI Model protocol stack

3.1.8 Residential Gateway

Residential gateway is basically a router that is configured to enable the sharing of a single Internet connection (subscription) by multiple users in a home network. However when you buy a residential gateway, it most likely incorporates other functions such as hub, switch, wireless access point, or bridge. Some residential gateways also already include broadband (cable/DSL) modem.

Residential Gateway

By using a residential gateway to connect your home network to the Internet, you don't need to always turn on a computer as an ICS host.
With a residential gateway, you don't have to manually set an IP address for each computer in your network because a residential gateway usually has DHCP server. Using DHCP, IP address for each computer is assigned dynamically by the residential gateway.

A residential gateway also keeps your computers anonymous on the Internet because it translates the IP address of each computer to an IP address assigned by the ISP. This function is called Network Address Translation (NAT).
Besides, a residential gateway protects your home network from intruders that try to gain access through certain applications in your computers because it has built-in firewall.
Residential gateway is also known as broadband router or Internet gateway device (IGD).

3.1.9 Gateway

Gateway functions to connect two completely different networks. It performs protocol translation. Although gateway is considered a Layer 7 device in many publications, it actually works across the seven layers of the OSI Model. In Internet Telephony, a gateway connects the VoIP network to the PSTN.

Gateway

The following table summarizes network components along with their functions and the corresponding layers in the OSI Model:

Network Component	Functions	OSI Model
Network Adapter	converts a computer message into electrical/optical signals for transmission across a network.	Physical (Layer 1)
M o d e m	puts a message (baseband signal) on a carrier for efficient transmission; takes the baseband signal from the carrier.	Physical (Layer 1)
Repeater (Regenerator)	receives signal, amplifies it, then retransmits it.	Physical (Layer 1)

Bridge	connects networks with different Layer 2 protocols; divides a network into several segments to filter traffic.	Data Link (Layer 2)
Hub	connects computers in a network; receives a packet from a sending computer and transmits it to all other computers.	Physical (Layer 1)
Switch	connects computers in a network; receives a packet from a sending computer and transmits it only to its destination.	Data Link (Layer 2)
Access Point	Connects computers in a wireless network; connects the wireless network to wired networks; connects it to the Internet.	Data Link (Layer 2)
Router	Forwards a packet to its destination by examining the packet destination network address.	Network (Layer 3)
Residential Gateway	Connects a home network to the Internet; hides all computers in the home network from the Internet.	Network (Layer 3)
Gateway	Connects two totally different networks; translates one signaling/protocol into another.	All layers

3.2 Network Operating Systems

Any modern Operating System contains built-in software designed to simplify networking of a computer. Typical O/S software includes an implementation of TCP/IP protocol stack and related utility programs like ping and traceroute. This includes the necessary device drivers and other software to automatically enable a

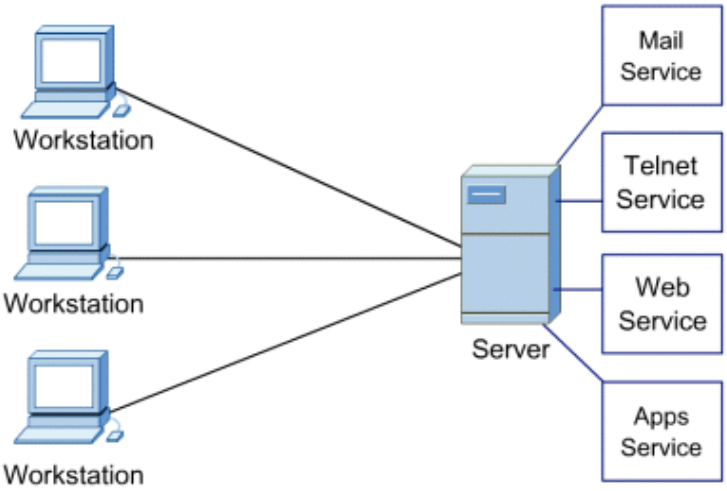
device's Ethernet interface. Mobile devices also normally provide the programs needed to enable Wi-Fi, Bluetooth, or other wireless connectivity.

The early versions of Microsoft Windows did not provide any computer networking support. Microsoft added basic networking capability into its operating system starting with Windows 95 and Windows for Workgroups. Microsoft also introduced its Internet Connection Sharing (ICS) feature in Windows 98 Second Edition (Win98 SE). Contrast that with Unix, which was designed from the beginning with networking capability. Nearly any consumer O/S today qualifies as a network operating system due to the popularity of the Internet.

Network operating systems (NOSs) distribute their functions over a number of networked computers they add functions that allow access to shared resources by a number of users concurrently.

Client systems contain specialized software that allows them to request shared resources that are controlled by server systems responding to a client request. The NOS enhances the reach of the client PC by making remote services available as extensions of the local native operating system.

NOSs also support multiple user accounts at the same time and enables concurrent access to shared resources by multiple clients. A NOS server is a multitasking system.



Several clients in a network

3.2.1 Choosing a NOS

The main features to consider when selecting a NOS include:

- Performance
- Management and monitoring tools
- Security
- Scalability
- Robustness/fault tolerance

3.2.2 Types

There are two popular competing NOS families. Windows based and Unix based. The former is proprietary whereas the latter is open source.

Windows NOS

Windows server-based networks that run Windows NT Server or Windows 2000 Server are based on the concept of the domain. A domain is a group of computers and users that serves a boundary of administrative authority.

Windows NT domains and Windows 2000 domains, although similar in function, interact with one another differently. In Windows NT 4.0, the Domain Structure of Windows NT was entirely different from the Domain Structure in Windows 2000.

Instead of Active Directory, Windows NT provides an administrative tool called the User Manager for Domains. It is accessed from the domain controller and is used to create, manage, and remove domain user accounts. Each NT domain requires one Primary Domain Controller (PDC). A domain can also have one or more Backup Domain Controllers (BDCs).

Windows 2000 and 2003 Family of Operating Systems includes:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server

Unix/Linux

Linux is an operating system similar to UNIX. It runs on many different computers and was first released in 1991. Linux is portable, which means versions can be found running on name brand or clone PCs. It offers many features adopted from other versions of UNIX.

The UNIX NOS was developed in 1969, and it has evolved into many varieties.

The source code is opened, that is, available at no cost to anyone who wants to modify it. It is written in C programming language so businesses, academic institutions, and even individuals can develop their own versions. There are hundreds of different versions of UNIX. Linux is sometimes referred to as "UNIX Lite", and it is designed to run on Intel-compatible PCs. Linux brings the advantages of UNIX to home and small business computers.

The following are a few of the most popular types:

- Red Hat Linux
- Linux Mandrake
- Caldera eDesktop and eServer

- Debian GNU/Linux
- Corel Linux
- Turbo Linux
- Ubuntu

Other Software and Programs

A popular use of a Linux system is a web server. Web server software uses Hypertext Transfer Protocol (HTTP) to deliver files to users that request them, using a web browser from their workstation.

A Mail Server is a system that is configured with the proper programs and services that enable handling the exchange of e-mail sent from one client to another.

Review Questions

i) Describe the following network devices and what they do:
   - Switch
   - Gateway
   - Repeater

ii) Network Operating systems are said to be multi-user and multi-tasking. Differentiate these two terms.

iii) How does a network operating system differ from a standalone operating system?

iv) What factors will you consider before choosing a network operating system?

v) Describe the role of software in supporting a computer network.

CHAPTER FOUR: PROCURING NETWORK RESOURCES

4.1 Introduction

The dependency on computer networks has increased progressively for organizations as a strategically important competitive advantage. If planned, developed, and managed properly, a network can bring about greater efficiency in organizational operations, better working environments, and effective decision-making processes. Therefore, many organizations are trying to catch up the development gap with the industry by means of technology acquisition. Technology acquisition process is essential in developing a good management information system for an organization. Many IT projects have failed because of poor design planning, false selection of the development, and a lack of follow up on key milestones addressed in the acquisition process.

4.2 Decision Making Strategy in Network Resource acquisition

The term 'acquisition' refers to all the stages from buying, introducing, applying, adopting, adapting, localizing, and developing through to diffusion. The set of processes for the build, lease, or buy decision must be identical for every instance or business opportunity that arises. The processes determine the strategic value and potential savings of the proposed acquisition, as well as factors like business transformation versus drive for competitive advantage.

Prior to the acquisition process, the detail requirements of the process should have already been identified clearly. More importantly, the business objectives should be identified for the solution being sought and the management decision whether building, leasing, or buying the resources should consider a value-versus-risk matrix to determine which options can be applied. Both IT auditors and corporate

management should evaluate offerings over the long term and compare the "trickling" investment over time to the one-time cost of buying and implementing a network. Moreover, this technology acquisition process requires an extensive evaluation considering the system requirements, feasibility analysis, and risk management assessment.]

4.3 IT Acquisition Process

The acquisition process should involve the identification and analysis of alternative solutions that are each compared with the established business requirements. The decision making to acquire a device primarily consists of the following stages:

Identifying the Business Objective

One of the most essential assessments in decision making process is identifying the business objective after first knowing the problems being solved. The management should primarily identify the business processes involved in the organization. The first phase of the acquisition process should align the business process with the company objectives and the business plan. Note that specific process may need to be prioritized to fully obtain the benefits of the implementation. Moreover, each process should be carefully analyzed to ensure that it will have the certain functionality to meet the requirements of the business process and the users, as well as the benefits which can be justified with its cost.

Analyzing alternatives

There are several options in procuring networking solutions. Some available alternatives are: (1)Buying all equipment from a vendor and installing on your own (2) Leasing equipment from a service provider (ISP) or lease through utility computing (contracted development), (3) Outsourcing network services from another company etc.

While an organization is in the phase of deciding which alternative being selected, the management should carefully examine not only the advantages and

disadvantages of each procuring option, but more importantly, the option must be best-fit with the organization business plan.

Conducting a feasibility analysis

As a part of the assessment in acquiring the solutions, a feasibility analysis is important to identify the constraints for each alternative from both technical and business perspective. Feasibility analysis incorporates the following categories:

- Economic feasibility analysis provides cost-benefit justification with being regard to the expenses of a system, which include procurement, project-specific, start-up, and operational costs. Some cost examples are one-time and recurring cost, consultants, support staff, infrastructure, maintenance and training costs. This examination ensures that the solution won't exceed the budget limit as well as it increase the efficiency and better resource utilization.
- Technical feasibility assessment analyzes the technical reasonableness of the proposed solution. Technical feasibility evaluates whether the company has the infrastructure and resources including hardware, software capability to support the new network. Meanwhile, it also assesses the consistency of the proposed system in terms of the technical requirements with the company technical resource. Therefore, this assessment guarantees the reliability and capacity for the future growth.
- Operational feasibility evaluation reviews the extent of organizational changes required to accommodate the proposed system. The proposed system should solve the business problems and provide better opportunity for the business since the business process might be changed. Some alignments that may occur include business process, human resource management, and products or service offered.
- Legal and contractual feasibility. The proposed solution must pass any related legal or contractual obligations associated with. Corporate legal counsel should ensure that there are no illegal practices corresponding to the new system related with any preexisting regulations. Organization

also may work with some experts from Computer Law Association to make sure this analysis strictly enforced. Thus, the underlying theme will protect the company and the establishment of the remedy process should the vendor or contractor fail to perform as promised.

Upon completion of the series of feasibility analyses, the risk analysis review most likely will be conducted. Risk analysis evaluate the security of proposed system, potential threats, vulnerabilities, impacts, as well as the feasibility of other controls can be used to minimize the identified threats.

Selection Procedure

Selection procedure is the process of identifying the best match between the available options and the identified requirements. In this process, the company requests for a proposal from prospective providers, evaluates the proposal, and selects the best available alternative. There are various ways to solicit responses from providers. Some of the common methods comprise request for information (RFI), request for bid (RFB), and request for proposal (RFP). An RFI is used to seek information from vendors for a specific intention. RFI should act as a tool for determining the alternatives or associated alternatives for meeting the organization's needs. An RFB is designed to procure specific items or services and used where either multiple vendors are equally competent of meeting all of the technical and functional specifications or only one provider can meet them. Furthermore, an RFP specifies the minimal acceptable requirements, including functional, technical, and contractual aspects. This document offers flexibility to respondents to further define the requested requirements. RFPs can be a lead to a purchase or continued negotiation.

All of these processes should be structurally proceeded to ensure the process would be completed neatly in a timely fashion. If done properly, this process turns out to be a purchasing decision for the selected application. Note that the entire process must be documented in a written letter before moving to the next step. This is an important issue to avoid a bid protest that may be filled from any other potential

vendors. Management, IT auditor and also legal counsel must review every point in detail before the proposal evaluation process begins.

Proposal Evaluation Process

Proposal evaluation is a crucial process in the acquisition since one of more key stakeholders reviews submitted proposals using a list of objective selection criteria and decide the best match between the product features and functionality with the identified requirements.

Negotiating a contract

Once the vendor is selected, then the company can move to the contract negotiation, in which the company can specify the price of the job and the type of the support to be provided by the vendor. The contract must describe the detailed specifications, all the included services provided by the vendor, and other detail terms of the system. Contract is a legal document so the company should involve the experienced staff in IT and legal matters. Since the contract can be very tricky so these legal counsel should be involved from the beginning of selection process.

Establishing a service level agreement (SLA) SLA is formal agreement regarding the distribution of work between the organization and its vendor. Such agreement is created according to a set of agreed-upon objective, quality tests, and some what-if situations. Overall, SLA defines: (1) company and vendor responsibilities, (2) framework for designing support services, (3) company privilege to have most of the control over their system.

Implementing the Solution

Upon completion of the contract negotiation, an acceptance plan should be agreed by both the company and the vendor so that the network can be ready to be installed. During this process, the level of performance is also tested and user reactions are evaluated. After implementation the company management may deal

with organizational issues such as conversion strategies, training, and resistant to change.

Review Questions

i) Why is it important to do a needs assessment before setting up a computer network.
ii) There are various ways to solicit responses from providers, describe any three.
iii) Describe the following techniques of procuring network resources:
   - Outsourcing network services
   - Leasing network equipment
   - Buying from a vendor and installing on your own
iv) Explain why it is important for organizations to sign service level agreements(SLAs) wit vendors
v) You have been appointed to negotiate a contract with a vendor to install a network in your company. Describe three things you will consider when arriving at your price.

Learning Objectives

CHAPTER FIVE: CONFIGURING NETWORK DEVICES

5.1 LAN network address

The first three octets of an IP address should be the same for all computers in the LAN. For example, if a total of 128 hosts exist in a single LAN, the IP addresses could be assigned starting with 192.168.1.*x*, where *x* represents a number in the range of 1 to 128. You could create consecutive LANs within the same company in a similar manner consisting of up to another 128 computers. Of course, you are not limited to 128 computers, as there are other ranges of IP addresses that allow you to build even larger networks.

There are different classes of networks that determine the size and total possible unique IP addresses of any given LAN. For example, a class A LAN can have over 16 million unique IP addresses. A class B LAN can have over 65,000 unique IP addresses. The size of your LAN depends on which reserved address range you use and the subnet mask(explained later) associated with that range. (see Table below.).

Table 1. Address ranges and LAN sizes

Address range	Subnet mask	Provides	Addresses per LAN
10.0.0.0 - 10.255.255.255.255	255.0.0.0	1 class A LAN	16,777,216
172.16.0.0 - 172.31.255.255	255.255.0.0	16 class B LANs	65,536
192.168.0.0 - 192.168.255.255	25.255.255.0	256 class C LANs	256

5.2 Network and broadcast addresses

Another important aspect of building a LAN is that the addresses at the two extreme ends of the address range are reserved for use as the LAN's network address and broadcast address. The *network address* is used by an application to represent the overall network. The *broadcast address* is used by an application to send the same message to all other hosts in the network simultaneously.

For example, if you use addresses in the range of 192.168.1.0 to 192.168.1.128, the first address (192.168.1.0) is reserved as the network address, and the last address (192.168.1.128) is reserved as the broadcast address. Therefore, you only assign individual computers on the LAN IP addresses in the range of 192.168.1.1 to 192.168.1.127:

Network address: 192.168.1.0

Individual hosts: 192.168.1.1 to 192.168.1.127

Broadcast address: 192.168.1.128

5.3 Subnet masks

Each host in a LAN has a subnet mask. The *subnet mask* is an octet that uses the number 255 to represent the network address portion of the IP address and a zero to identify the host portion of the address. For example, the subnet mask 255.255.255.0 is used by each host to determine which LAN or class it belongs to. The zero at the end of the subnet mask represents a unique host within that network.

5.4 Domain name

The *domain name*, or *network name*, is a unique name followed by a standard Internet suffixes such as .com, .org, .mil, .net, etc. You can pretty much name your LAN anything if it has a simple dial-up connection and your LAN is not a server providing some type of service to other hosts directly. In addition, our sample network is considered private since it uses IP addresses in the range of 192.168.1.x. Most importantly, the domain name of choice should not be accessible from the Internet if the above constraints are strictly enforced. Lastly, to obtain an "official" domain name you could register through InterNIC, Network Solutions or Register.com.

5.5 Hostnames

Another important step in setting up a LAN is assigning a unique hostname to each computer in the LAN. A hostname is simply a unique name that can be made up and is used to identify a unique computer in the LAN. Also, the name should not contain any blank spaces or punctuation. For example, the following are valid hostnames that could be assigned to each computer in a LAN consisting of 5 hosts: hostname 1 - Simba; hostname 2 - Chui; hostname 3 - Duma; hostname 4 - Nyati; and hostname 5 - Ndume. Each of these hostnames conforms to the requirement that no blank spaces or punctuation marks are present. Use short hostnames to eliminate excessive typing, and choose a name that is easy to remember.

Table 2 summarizes what we have covered so far in this article. Every host in the LAN will have the same network address, broadcast address, subnet mask, and domain name because those addresses identify the network in its entirety. Each computer in the LAN will have a hostname and IP address that uniquely identifies that particular host. The network address is 192.168.1.0, and the broadcast address is 192.168.1.128. Therefore, each host in the LAN must have an IP address between 192.168.1.1 to 192.168.127.

Table 2. Sample IP addresses for a LAN with 127 or fewer interconnected computers

IP address	Example	Same/unique

Network address	192.168.1.0	Same for all hosts
Domain name	www.yourcompanyname.com	Same for all hosts
Broadcast address	192.168.1.128	Same for all hosts
Subnet mask	255.255.255.0	Same for all hosts
Hostname	Any valid name	Unique to each host
Host addresses	192.168.1.*x*	*X* must be unique to each host

5.6 Assigning IP addresses in a LAN

There are two ways to assign IP addresses in a LAN. You can manually assign a *static* IP address to each computer in the LAN, or you can use a special type of server that automatically assigns a *dynamic* IP address to each computer as it logs into the network.

5.6.1 Static IP addressing

Static IP addressing means manually assigning a unique IP address to each computer in the LAN. The first three octets must be the same for each host, and the last digit must be a unique number for each host. In addition, a unique hostname will need to be assigned to each computer. Each host in the LAN will have the same network address (192.168.1.0), broadcast address (192.168.1.128), subnet mask (255.255.255.0), and domain name (yourcompanyname.com). It's a good idea to start by visiting each computer in the LAN and jotting down the hostname and IP address for future reference.

5.6.2 Dynamic IP addressing

Dynamic IP addressing is accomplished via a server or host called DHCP (Dynamic Host Configuration Program) that automatically assigns a unique IP address to each computer as it connects to the LAN. A similar service called BootP can also automatically assign unique IP addresses to each host in the network. The DHCP/ BootP service is a program or device that will act as a host with a unique IP address. An example of a DHCP device is a router that acts as an Ethernet hub on

one end and allows a connection to the Internet on the opposite end. Furthermore, the DHCP server will also assign the network and broadcast addresses. You will not be required to manually assign hostnames and domain names in a dynamic IP addressing scheme.

5.7 The LAN hardware

Assigning hostname and IP addresses will be useless if there is no hardware available to connect all the computers together. There are several different types of hardware schemes such as Ethernet, Token Ring, FDDI, Token Bus, etc. Since Ethernet is the most widely used hardware scheme, we will focus our attention on it. Ethernet is available from several different computer vendors, and it is relatively inexpensive. Ethernet is a 10-Mbps baseband LAN specification developed by Xerox, Intel, and Digital Equipment. In order to build an Ethernet hub you need the following: an Ethernet Network Interface Card (NIC) for each computer, an Ethernet compatible hub with at least the same number of ports as there will be computers in the LAN, and Ethernet cables (or 10BaseT cables) to connect each computer's NIC to the Ethernet hub.

Also make sure that the hardware of choice is compatible with the operating system. This hardware/software compatibility information is usually found in the Requirements section on the back of the box of each product. Alternatively, you could ask a computer sales person about hardware/software requirements. You can usually save money by purchasing LAN cards as a package vs. purchasing them individually.

When choosing an Ethernet hub ensure that it contains at least as many ports as there are computers that will participate in the LAN. It is always best to choose a hub with additional ports to allow for expansion.

If you plan to use all of the computers in the LAN to access the Internet via a local Internet Service Provider (ISP), the router/Ethernet combo is an ideal choice. The router/Ethernet unit is normally configured using any computer that is connected to the LAN. Assuming that all computers in the LAN will be running the Red Hat

Linux operating system, a router will be required that can be configured using a Linux configuration program such as LinuxConf.

Finally, choose network cables to allow for expansion. Typically, most Ethernet networks use 10BaseT cables with RJ45 jacks at each end. It's always a good idea to purchase cables that are 1 or 2 times longer than the required length in case the structure (topology) of the LAN changes in the future.

5.8 Installing the hardware

Assuming that all LAN hardware is available, the next step is to install it. First turn off all the computers that will participate in the LAN. Next, open the case on each computer and install each NIC in the appropriate slot on the motherboard, being careful to follow the manufacturer's instructions.

Find a convenient but safe location for the Ethernet hub, preferably a centralized location in the same building or room along with the computers. Next, run the cable from the NIC in each computer to the Ethernet hub ensuring all cables are out of the way of users who will need physical access to each computer in the LAN. Moreover, make sure you follow all instructions provided with the LAN hardware before starting up any of the computers that will participate in the LAN.

If you are using a router to connect the LAN to the Internet or using a DHCP server, you will need to do some configuration as required by the user's manual. Lastly, assuming all computers are attached to the Ethernet hub via the NIC and a specific port on the hub, you can now begin the software configuration process using the Red Hat operating system.

5.9 Configuring the LAN

How you configure the computers on the LAN will depend on whether the Red Hat OS was installed before or after the LAN hardware. If you installed the LAN hardware before installing Red Hat you will be prompted for network configuration during the Red Hat installation process. However, if you installed the Red Hat OS after the LAN hardware, a program called "Kudzu" will detect the newly installed

Ethernet card and initiate the configuration process automatically. Follow these steps when configuring each Ethernet card using the "Kudzu" program:

1. During the bootup process look for a dialog box titled "Welcome to Kudzu." Press Enter to begin the configuration process.
2. Next, you should see another dialog box that displays the brand name for the installed Ethernet card. Press Enter again to continue.
3. After a brief delay you should see "Would You Like to Set up Networking".
4. Select the NO option using the Tab key and then press Enter. I will describe setting up networking using a utility called LinuxConf later in this article.

At this point, the bootup process should continue normally and you will be required to log on to the computer as the root user. You should have been given the opportunity to create a root account during the initial installation of Red Hat.

5.9.2 Using LinuxConf to configure your Ethernet card

You can use an application program called LinuxConf to configure or reconfigure the NIC of each computer in the LAN. You can launch the LinuxConf utility by typing linuxconf at the command prompt of any terminal window in the KDE or GNOME desktop environment. Another way to start the LinuxConf utility is to click the Main menu button, select System, then LinuxConf. When the LinuxConf application is displayed, follow the steps below to configure the Ethernet card:

1. From the LinuxConf tree structure, select Config, Networking, Client Tasks, Basic Host Information.
2. Type the fully qualified hostname that you assigned to this computer on the Host name tab.
3. Next, click the Adaptor 1 tab, which displays your Ethernet card settings.
4. Verify that the Enabled button is selected to ensure that the Ethernet card will be accessible.
5. Choose the Manual option if you will not be using a DHCP or BootP server on your LAN and continue to step 6. Otherwise, if you will be using a DHCP or BootP server, choose either DHCP or BootP accordingly and continue to step 12.

6. Enter this computer's hostname followed by a period and the domain name of the LAN for the Primary name + domain option.
7. Enter the computer's hostname in addition to any aliases separated by a blank space under the Aliases option.
8. Enter the IP address assigned to this computer next to IP Address (such as 192.168.1.1).
9. Type in 255.255.255.0 for the Netmask.
10. For net device, type eth0, which represents the first Ethernet card located inside the computer.
11. The driver or Kernel Module option for the Ethernet card should automatically be filled in upon exiting LinuxConf.
12. Click the Accept button to activate all changes.
13. Repeat steps 1-12 for each computer in the LAN, verifying that you've entered the correct hostname and the corresponding IP address.

5.9.3 Nameserver specification

Another important step in setting up LAN is to configure the Nameserver specification, which is used by Linux to look up IP addresses when only the computer's hostname is given. There are two methods that are used by Red Hat Linux to resolve hostnames into IP addresses. One method is via Domain Name Services (DNS), and the other is by means of a local file at /etc/hosts. Locate the hosts file by typing cd /etc to change to the /etc directory. The /etc directory is where most system configuration files are found for each computer. Next, follow the steps below to resolve hostnames into IP address using the /etc/hosts file:

1. In the left column of LinuxConf, open the Nameserver specification (DNS) category.
2. Left-click the DNS Usage option. (The button should be pushed in.)
3. Enter localdomain next to the Search Domain 1 category.
4. If you know the primary and secondary IP addresses for the nameserver, which should be available for this Ethernet card, enter those in the IP of nameserver 1 and IP of nameserver 2 categories. Otherwise, you can leave those categories blank.

5. Left-click the Accept button to activate all changes.

5.9.4 Hostname search path

The hostname search path is used by Red Hat Linux to search for IP addresses assigned to hostnames. To configure the hostname search path so that the local host (/etc/hosts) file is used to resolve local hostnames, and the ISP domain services to resolve Internet domain services, follow these steps:

1. In the left column of LinuxConf, open the Routing and Gateways category.
2. Select the Host Name Search path option.
3. In the right column of LinuxConf, select the Multiple IPs for One Host option.
4. Select the hosts, dns option in the right portion of LinuxConf.
5. Left-click the Accept button to activate all changes.

5.9.5 Setting up /etc/hosts

The Red Hat Linux OS needs some way to find IP addresses within the LAN based on the each computer's hostname. I described earlier in the article that the Domain Name Service (DNS) is one method of resolving hostnames into IP addresses. In a DNS configuration the hostnames and IP addresses should already be listed in a pre-existing nameserver. Consult your local ISP to obtain those IP addresses. On the other hand, if there is a centralized nameserver, as with small LANs, a host file will need to be configured on each computer that was assigned a hostname, IP address, and any aliases. This configuration process involves editing a text file located at /etc/host. You will need to go to one of the computers in the LAN and follow the below steps in order to create and configure the /etc/hosts file:

1. In the left column of LinuxConf, open the Misc category.
2. Open the Information about hosts category. You should see an entry for this computer that includes the IP address, hostname, and any aliases.
3. Left-click the Add button once to add an entry for another host in the LAN.
4. Type the Primary + Domain Name for another host in the LAN in the dialog box that appears (such as trinity.yourcompanyname.com).
5. Type one or more aliases for this computer next to the Alias option (such as tank).

6. Enter the IP address for the hostname that you've assigned for this computer next to IP number.
7. Left-click the Accept button to activate all changes.
8. Repeat steps 1-7 for each computer in your LAN.

After you have done steps 1-7 for all computers, the /etc/hosts tab of LinuxConf should list one entry for every computer in your LAN, in addition to the local host's loopback interface. The local host name should appear as localhost. Finally, you can save all changes and exit the LinuxConf application by following the steps below:

1. Left-click the Quit button in the /etc/host screen after all hostnames and IP addresses have been entered.
2. To exit the LinuxConf application, left-click the Quit button at the bottom-left corner.
3. Left-click the Activate the Changes button to activate all changes and exit LinuxConf.

Now that you have configured one computer in your LAN, you will need to go back and repeat all the above steps for each computer starting with the section "Configuring the LAN". If you would prefer a less time-consuming procedure of configuring each computer, you can modify the /etc/hosts file on each computer manually using a copy method.

You can copy the /etc/hosts file that you have just created to a flash disk or CD-ROM (if you have a writeable CD-ROM drive) and copy that file to the /etc directory of each computer in your LAN.

Next, take the flash to each computer in the LAN and type the command cp /flash/ hosts /etc/host in a terminal window. This will copy the hosts file to the /etc directory on each host. The /etc/hosts file, as you probably noticed, is just a text file with a list of hostnames and IP addresses separated into three columns. Lastly, make sure that the local computer and its associated IP address are listed twice and all the other computers in the LAN are listed only once.

5.10 Testing the LAN

To test the completely configured LAN, make sure that the computers are able to communicate with each other after the bootup process. You can start by typing reboot at the command prompt at a command terminal on each computer. This allows you to monitor the testing information that scrolls down the screen as a standard procedure during the Linux boot process. Look for the following information:

Setting hostname:	<hostname you assigned to this computer>
Bringing up Interface lo:	<OK> or <FAILED>
Bringing up interface eth0	<OK> or <FAILED>

The Setting hostname field should display the hostname that you assigned for this computer. The lo and eth0 interfaces should display [OK] to indicate that both tests were successful.

To determine whether each computer can communicate with every other computer in the LAN, use the ping command. Open any terminal window on the current host and type the command ping <IP address> or <hostname>, where <IP address> or <hostname> is the IP address and/or the hostname that you assigned to this computer. Note that you must type either the IP address or the hostname in order for the ping command to work properly.

If you have configured the DNS nameserver specification properly, the ping <hostname> command should resolve the hostname into a corresponding IP address. Otherwise, you will need to use the IP address that you should currently already have listed for all computers in the LAN. The ping command will send messages across the LAN to the designated IP address or computer. You should see several messages or packets (consisting of bytes of information) if the computers are "talking" or communicating with each other. These packets look similar to the following:

64 bytes from 192.168.1.x : icmp_seq=0 ttl=255 time=0.8ms

64 bytes from 192.168.1.x : icmp_seq=0 ttl=255 time=0.8ms
64 bytes from 192.168.1.x : icmp_seq=0 ttl=255 time=0.8ms

Note that the "192.168.1" represents the LAN that this particular host is a member of and the x indicates the specific host number that you are attempting to ping (e.g. such as Oracle) which jointly makes up the IP address. You can press the Ctrl+C to terminate the test and you should see the following basic information about the entire ping test:

--- hostname.yourcompanyname.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.8 ms

Verify that the packet loss is 0%, which is an immediate indication that the test was successful. However, there is a problem if the ping command results in the following message:

From hostname.comanyname.com (192.168.1.1): Destination Host Unreachable

This is an immediate indication that the two computers are not communicating at all. If the computers are not communicating, see the next section, "Troubleshooting the LAN". Otherwise, when you can successfully ping all other computers in the LAN from one designated computer, the overall basic communications functionality is indeed a success. At this point, you can consider this LAN to be a fully functional network that you can install and on which you can configure various network services as desired.

5.11 Troubleshooting the LAN

If you are unable to ping another computer in the LAN, here's how to get to the source of the problem. First of all, it's a good idea to shut down every computer in the LAN using the shutdown command. At the command prompt on each computer,

type shutdown. The main reason for shutting down all computers is to monitor feedback from the boot process when each computer is started up again.

Check all cable connections between every computer, making sure that all RJ45 jacks are connected properly. After verifying that all the cables are secured properly, start each computer one at a time and look for the following response during the boot process:

Setting hostname: hostname.networkname [OK]

You can turn on the interactive mode by typing I at the LILO boot prompt during the initial bootup process of Red Hat to get a closer view of the feedback. Ensure that the hostname and network name that was assigned to this computer is spelled correctly. If this is not the case, you will need to return to the Basic Host Information section of LinuxConf. In interactive mode you will be prompted to start several services. Respond to each question with Yes and pay close attention to results of various tests. If the Kudzu program detects an Ethernet card, then this an indication that the card was not properly configured the first time around. Proceed to let Kudzu configure the card. When you are prompted to configure the network, choose "Yes" and type the correct IP address and other related information for this particular computer.

Another important response to examine carefully is the following:

Bringing up interface eth0 [OK]

This line indicates whether the Ethernet card is working properly. If this test fails you should check all network settings using LinuxConf to ensure that the card was configured properly. If the network settings are correct, there is probably a defect in the Ethernet card itself. In order to verify this, consult the manufacturer of the Ethernet card or a computer technician to determine whether or not the card is

defective. Repeat the preceding troubleshooting procedures on each new Ethernet card installed.

5.12 Connecting to the Internet

There are several ways to do connect your computers to the internet. According to this manual, there are at least 3 :

- **Modem sharing** - similar to sharing a hard disk, a folder or a printer over a network, you can also share a modem, but this requires additional software.
- **Routing** - i.e. using a separate machine (a router, or an old computer set up to function as a router by running routing software) that transfers network packets from and to the internet, based on their address. This usually involves some Network Address Translation (NAT) as well.

- **Proxy server** : software that handles your communication with the internet for you (and other computers on your network). Proxy servers are "application gateways" : they serve certain applications, such as your web browser. Using a proxy server to browse the web is therefore easy to set up, but other applications (e-mail, games, ...) might require additional software to be 'proxy-enabled'.

Routing

This is what most businesses use. They get a block of static IP addresses from their ISP and give each of their machines an IP address. In most cases, what I call the "gateway computer" is in fact a router, a special hardware device which forwards the packets. Many operatings systems (e.g. Unix, Windows NT/2K, OS/2 etc.) can route IP packets too.) The disadvantage of routing that it is more expensive because you will have to 'buy' static IP addresses from your ISP. Not only that, the ISP will have to define a "route" to your own little subnet on their systems. That means they'll have to do

some work and thus they want to be paid for it. It also means that intervention by your ISP is required, i.e. you can't do it all on your own. This is in contrast with the next two strategies.

Proxy servers

Routing works great for businesses which are connected to the Internet 24 hours a day. But what if you're not, and you still want to hook up a whole LAN to the Internet once in a while? One solution would be if somehow a workstation computer could ask the gateway computer to send and receive data on it's behalf. The software which does the trick is called a proxy server. A well known example is WinGate. As far as the operating system is concerned, the proxy server is a normal TCP/IP application. A workstation computer sends a request to the gateway asking it to send data to the Internet. The data is sent using the gateway's IP address, and any response comes back the same way. Any number of computers on your LAN can use the connection in this way at the same time, as long as the data for separate requests is kept separate. The gateway computer can be a 'normal' PC with a standard Internet connection. There are several different way to do proxying: using the SOCKS protocol, socket relays and application proxies.

The SOCKS protocol is defined by an official standard. TCP/IP applications have got to support SOCKS (in other words: must be SOCKSified) in order to connect to a SOCKS proxy server. Some do, but many of them do not. Some operatings systems, such as Warp 4, have special support in their TCP/IP stack so that non-SOCKS aware programs can be used with SOCKS servers.

With socket relay (also known as "port mapping"), the proxy server mirrors ports from the remote machine on the Internet and makes them available as though it was providing the services. In this case, when a workstation on the internal network connects to for instance the SMTP port on the proxy server, the proxy server opens a matching socket on the connection to the Internet and then just ferries data between the two connections. Unlike SOCKS, a socket relay does not require any special support on behalf of the client

program, so it can be used with most applications. The disadvantage of socket relays is that not all protocols can be handled. For instance, using the FTP protocol in non-passive mode is very problematical, and is not normally possible with a socket relay system.

An application proxy is a special TCP/IP program that knows about a particular application protocol, and will accept requests using this protocol. A common example of this is the HTTP proxy provided by many internet server providers. This program accepts HTTP requests from clients using the HTTP protocol and converts them to requests to other HTTP servers.

IP Masquerading (NAT)

Some operating systems, most notably Linux, have the capability to perform IP routing with the addition of changing the IP address in the packets on the fly, i.e. as the data is passed through from the LAN to the Internet. When there is a mapping of multiple addresses on an internal LAN to one particular IP address of the gateway, this is called IP Masquerading. When the mapping is a bit broader (any IP address to any other IP address) the feature is called Network Address Translation (NAT). NAT is a superset of IP Masquerading and is often used in firewalls for security reasons. Note that ISPA also has a feature called NAT (used for a different purpose).

Let's say in the following example that you use IPRoute for NAT. IPRoute changes the addresses in the packets it receives from the workstation machines into the address it is using itself. For example, 2 workstation machines can each run a webbrowser. IPRoute changes the addresses so the ISP thinks both webbrowsers are running on one and the same machine! There's nothing strange with that, it has always been possible to run multiple webbrowsers on one machine.

Running servers (say, webservers) on multiple workstation machines is a bit less transparent. Most servers listen to a "well-known" port number. For a webserver this is port 80. But only 1 server can listen to a port at the same

time. That means that the gateway machine can remap a port to only one workstation machine. So, if you want to run more than one webserver on your internal network which must all be reachable from the outside, there is a problem. Fortunately, there is also a solution. Let's say you have webservers on each port 80 of the workstation machines 192.168.0.2, 192.168.0.3 and 192.168.0.4. You can remap port 80 on the gateway machine to port 80 on 192.168.0.2, port 81 to port 80 on 192.168.0.3 and port 82 to port 80 on 192.168.0.4. People on the outside will have to specify URLs with "non-standard" ports for the last two workstation machines, say http://www.example.com:81/ and http://www.example.com:82/
It works but it isn't very elegant...

Routing vs proxy servers vs IP Masquerading

One of the major problems with using the SOCKS protocol is that it requires that clients be able to perform name lookups for external addresses, usually via DNS. This means that as well as implementing a SOCKs server, the proxy server must also provide a full DNS service to it's clients. Additionally, some protocols do not lend themselves to transport via SOCKs. The FTP protocol, in non-passive mode, can be particularly difficult. It is also possible to use a socket relay server without access to a DNS server, but this is not always the case.

If you have several workstation machines who all hit the same webpage at the same time, a caching proxy server may be provide better performance than a system with IP Masquerading. That is because the webpages can be

served from the cache (local harddisk) instead of getting each of them over the modem/ ISDN link. On the other hand, a caching proxy may require a more powerful machine with a big harddisk.

Review Questions

i) Describe the structure of an IP- address.
ii) You have been given an IP address 172.16.1.1 determine
    i. Network address
    ii. The range of addresses you can assign to individual hosts
    iii. Broadcast address
    iv. Network address
    v. Subnet mask

iii) Differentiate between static IP-addressing and dynamic IP-addressing.
iv) What is the function of /etc/hosts file in linux machine?
v) Contrast between routing, proxy server and IP- Masquerading with respect to routing.

CHAPTER SIX: NETWORK SECURITY

Introduction

This chapter discusses security issues regarding TCP/IP networks and provides an overview of solutions to resolve security problems before they can occur. The field of network security in general and of TCP/IP security in particular is too wide to be dealt with in an all encompassing way in this manual, so the focus of this chapter is on the most common security exposures and measures to counteract them. Because many, if not all, security solutions are based on cryptographic algorithms, we also provide a brief overview of this topic for the better understanding of concepts presented throughout this chapter.

6.1 Security Issues

This section gives an overview of some of the most common attacks on computer security, and it presents viable solutions to those exposures and lists actual implementations.

6.1.1 Common Attacks

For thousands of years, people have been guarding the gates to where they store their treasures and assets. Failure to do so usually resulted in being robbed, neglected by society or even killed. Though things are usually not as dramatic anymore, they can still become very bad. Modern day I/T managers have realized that it is equally important to protect their communications networks against intruders and saboteurs from both inside and outside. We do not have to be overly paranoid to find some good reasons why this is the case:

- **Wire tapping**: listening a link to get access to cleartext data and passwords
- **Impersonation**: to get unauthorized access to data or to create unauthorized e-mails, orders, etc.

- **Denial-of-service:** to render network resources non-functional
- **Replay of messages:** to get access to and change information in transit
- **Guessing of passwords:** to get access to information and services that would normally be denied (dictionary attack)
- **Guessing of keys:** to get access to encrypted data and passwords (brute-force attack, chosen ciphertext attack, chosen plaintext attack)
- **Viruses, trojan horses and logic bombs:** to destroy data

Though these attacks are not exclusively specific to TCP/IP networks, they should be considered potential threats to anyone who is going to base his/her network on TCP/IP, which is what the majority of enterprises, organizations and small businesses around the world are doing today. Hackers (more precisely, crackers) do likewise and hence find easy prey.

6.1.2 Observing the Basics

Before even thinking about implementing advanced security techniques, you should make sure that basic security rules are in place:

Passwords: Make sure that passwords are enforced to be of a minimum length (typically six to eight characters), to contain at least one numeric character, to be different from the user ID to which they belong, and to be changed at least once every two months.

User IDs: Make sure that every user has a password and that users are locked out after several logon attempts with wrong passwords (typically five attempts). Keep the passwords to superuser accounts (root, supervisor,administrator, maint, etc.) among a very limited circle of trusted system,network and security administrators.

System defaults: Make sure that default user IDs are either disabled or have passwords that adhere to the minimum requirements stated above. Likewise, make sure that only those services are enabled that are required for a system to fulfill its designated role.

Physical access: Make sure that access to the locations where your systems and users physically reside is controlled appropriately. Information security begins at the receptionist, not at the corporate firewall.

Help desk: Make sure that callers are properly identified by help desk representatives or system administrators before they give out "forgotten" passwords or user IDs. Social engineering is often the first step to attack a computer network.

6.2 Solutions to Security Issues

With the same zealousness that intruders search for a way to get into someone's computer network, the owners of such networks should, and most likely will, try to protect themselves. Taking on the exposures mentioned earlier, here are some solutions to effectively defend yourself against an attack. It has to be noted that any of those solutions solve only a single or just a very limited number of security problems. Therefore, a combination of several such solutions should be considered in order to guarantee a certain level of safety and security.

Encryption: to protect data and passwords

Authentication and authorization: to prevent improper access

Integrity checking and message authentication codes (MACs): to protect against the improper alteration of messages

Non-repudiation: to make sure that an action cannot be denied by the person who performed it

Digital signatures and certificates: to ascertain a party's identity

Frequent key refresh, strong keys and prevention of deriving future keys: to protect against breaking of keys (crypto-analysis)

Address concealment: to protect against denial-of-service attacks

Content inspection: to check application-level data for malicious content before delivering it into the secure network

Summary Security Exposures and Protections

Problem / Exposure	Remedy	Available Technologies
How to make break-ins into my network as difficult as possible?	Install a combination of security technologies for networks aswell as for applications.	Firewalls (IP filtering + proxy servers + SOCKS + IPSec, etc.). Antivirus + content inspection + intrusion

		detection software. No system defaults + enforced password policies. Passwords for every user and every service/application + ACLs. Extensive logging + alerting + frequent log audits/analysis. No unauthorized dial-in + callback
How to protect against viruses, trojan horses, logic bombs, etc.?	Restrict access to outside sources. Run antivirus software on every server and workstation. Run content-screening software on your gateways for application data (mail, files, Web pages, etc.) and mobile code (Java, ActiveX, etc.). Update that software frequently.	IBM/Norton AntiVirus, etc. Content Technologies' MIMESweeper and WebSweeper, etc. Finjan Surfingate, etc.

How to prevent the improper use of services by otherwise properly authenticated users? Server file systems (UNIX, NTFS, NetWare, HPFS-386, etc.). System security services (RACF, DCE, UNIX, NT, etc.).	Use a multi-layer access control model based on ACLs.	Application security (DBMS, Web servers, Lotus Notes, etc.).
How to obtain information on possible security exposures?	Observe security directives by organizations such as CERT and your hardware and software vendors	http://www.cert.org
How to make sure that only those people, that you want dial into your network?	Use access control at link establishment by virtue of central authentication services, two-factor authentication, etc.	RADIUS (optionally using Kerberos, RACF, etc.), TACACS. Security Dynamics' SecureID ACE/Server, etc.
How do you know that your system has been broken into?	Use extensive logging and examine logs frequently. Use intrusion detection programs.	Application/Service access logs (Lotus Notes, DB2/UDB, Web servers, etc.). System logs (UNIX, Windows NT, AS/400, etc.). Firewall logs and alerting (IBM firewalls, etc.).

		Systems management and alerting (Tivoli, etc.)
How to prevent wire tappers from reading messages?	Encrypt messages, typically using a shared secret key. Secret keys offer a tremendous performance advantage over public/private keys.)	SET, SSL, IPSec, Kerberos, PPP

6.3 The Need for a Security Policy

It is important to point out that you cannot implement security if you have not decided what needs to be protected and from whom. You need a security policy, a list of what you consider allowable and what you do not consider allowable, upon which to base any decisions regarding security. The policy should also determine your response to security violations.

An organization's overall security policy must be determined according to security analysis and business requirements analysis. Since a firewall, for instance, relates to network security only, a firewall has little value unless the overall security policy is properly defined. The following questions should provide some general guidelines:

- Exactly who do you want to guard against?
- Do remote users need access to your networks and systems?
- How do you classify confidential or sensitive information?
- Do the systems contain confidential or sensitive information?

- What will the consequences be if this information is leaked to your competitors or other outsiders?
- Will passwords or encryption provide enough protection?
- How much access do you want to allow to your systems from the Internet and/or users outside your network (business partners, suppliers, corporate affiliates, etc.)?
- What action will you take if you discover a breach in your security?
- Who in your organization will enforce and supervise this policy?

This list is short, and your policy will probably encompass a lot more before it is complete. Perhaps the very first thing you need to assess is the depth of your paranoia. Any security policy is based on how much you trust people, both inside and outside your organization. The policy must, however, provide a balance between allowing your users reasonable access to the information they require to do their jobs, and totally disallowing access to your information. The point where this line is drawn will determine your policy.

6.3.1 Network Security Policy

If you connect your system to the Internet then you can safely assume that your network is potentially at risk of being attacked. Your gateway or firewall is your greatest exposure, so the following is recommended:

- The gateway should not run any more applications than is absolutely necessary; for example, proxy servers and logging because applications have defects that can be exploited.
- The gateway should strictly limit the type and number of protocols allowed to flow through it or terminate connections at the gateway from either side, because protocols potentially provide security holes.
- Any system containing confidential or sensitive information should not be directly accessible from the outside.
- Generally, anonymous access should at best be granted to servers in a demilitarized zone.
- All services within a corporate intranet should require at least password

authentication and appropriate access control.

- Direct access from the outside should always be authenticated and accounted.
- The network security policy defines those services that will be explicitly allowed or denied, how these services will be used and the exceptions to these rules.
- Every rule in the network security policy should be implemented on a firewall and/or Remote Access Server (RAS). Generally, a firewall uses one of the following methods.

6.3.2 Everything not specifically permitted is denied.

This approach blocks all traffic between two networks except for those services and applications that are permitted. Therefore, each desired service and application should be implemented one by one. No service or application that might be a potential hole on the firewall should be permitted. This is the most secure method, denying services and applications unless explicitly allowed by the administrator. On the other hand, from the point of users, it might be more restrictive and less convenient.

6.3.3 Everything not specifically denied is permitted.

This approach allows all traffic between two networks except for those services and applications that are denied. Therefore, each untrusted or potentially harmful service or application should be denied one by one. Although this is a flexible and convenient method for the users, it could potentially cause some serious security problems.

Remote access servers should provide authentication of users and should ideally also provide for limiting certain users to certain systems and/or networks within the corporate intranet (authorization). Remote access servers must also determine if a user is considered roaming (can connect from multiple remote locations) or stationary (can connect only from a single remote location), and if the server should use callback for particular users once they are properly authenticated.

6.4 Incorporating Security into Your Network Design

You have seen throughout previous chapters that the design of an IP network is sometimes exposed to environmental and circumstantial influences that dictate certain topologies or strongly favor one design approach over another. One such influential topic is IP security.

6.4.1 Expecting the Worst, Planning for the Worst

In general, network administrators tend to either overemphasize or neglect security aspects when designing their networks. It is very important that you do not follow either of those cases but take great care that the security measures you need to implement in your network match those specified in your overall security policy. Once a security policy is in place, adequate technologies and their impact on the network design can be discussed.

However, if in doubt, expect the worst and add one more layer of security. You can remove it later if a thorough investigation reveals that it is not required. Do not trade in security for availability or performance unless you can really justify it.

It helps to divide your network into three major zones in order to define a more detailed security policy and the designs required to implement them at the right points within the network. Those zones are described below:

Core Network: This is the network where your business-critical applications and their supporting systems are located. This part of the network requires maximum protection from the outside and is usually also kept apart from internal users as an additional layer of protection.

Perimeter Network: This is the network where your public resources are located. These include Web and FTP servers but also application gateways and systems that provide specialized security functions, such as content inspection, virus protection and intrusion detection. This part of the network is typically secured from the outside as well as the inside to provide maximum isolation of the traffic in this network. This part of the network may also contain internal users.

Access Network: This is the network, whether private, public or virtual, leased or dial-up, that is used by the outside to access your network and its services and applications. This network is typically secured to the outside only.

Review Questions

i) What is network security?

ii) Describe three security compromises that can be performed on data.

iii) Explain why it is necessary for an organization to have a network security policy.

iv) Explain how a firewall works to enforce a security policy.

v) You are network administrator in an organization. How will you know that the network has been broken into? What will you do?

vi) How does a security plan differ from a security policy?

vii) Why is it important to achieve buy-in from users, managers, and technical staff for the security policy?

viii) What are some methods for keeping hackers from viewing and changing router and switch configuration information?

ix) How can a network manager secure a wireless network?

CHAPTER SEVEN: TROUBLESHOOTING NETWORK PROBLEMS

7.1 Introduction

Troubleshooting is a process of identifying common network problems. If a computer is unable to connect to a network or see other computers on a network for instance, it may be necessary to troubleshoot the network. A network may not work because of any of the below reasons.

1. Network card not connected properly.
2. Bad network card drivers or software settings.
3. Firewall preventing computers from seeing each other.
4. Connection related issues.
5. Bad network hardware.

Because of the large variety of network configurations, operating systems, setup, etc... not all of the above information may apply to your network or operating system. If your computer is connected to a company or large network, or you are not the administrator of the network, it is recommended that if you are unable to resolve your issues after following the below recommendations that you contact the network administrator or company representative.

7.2 Basic Troubleshooting

- Verify connections / LEDs
- Verify that the network cable is properly connected to the back of the computer. In addition, when checking the connection of the network cable, ensure that the LEDs on the network are properly illuminated. For example, a network card with a **solid** green LED or light usually indicates that the card is either connected or receiving a signal. Note: generally, when the green light is flashing, this is an indication of data being sent or received.

If, however, the card does not have any lights or has orange or red lights, it is possible that either the card is bad, the card is not connected properly, or that the card is not receiving a signal from the network.

- If you are on a small or local network and have the capability of checking a hub or switch, verify that the cables are properly connected and that the hub or switch has power.
- Verify that the network card is capable of pinging or seeing itself by using the ping command. Windows / MS-DOS users ping the computer from a MS-DOS prompt. Unix / Linux variant users ping the computer from the shell. To ping the card or the localhost, type either ping 127.0.0.1 or ping localhost
- If your computer network utilizes a firewall, ensure that all ports required are open. If possible, close the firewall software program or disconnect the computer from the firewall to ensure it is not causing the problem.

7.3 Network Management

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- **Security:** Ensuring that the network is protected from unauthorized users.
- **Performance:** Eliminating bottlenecks in the network.
- **Reliability:** Making sure the network is available to users and responding to hardware and software malfunctions.

Network management involves keeping an eye on the following:

Network Operations: keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
Administration: deals with keeping track of resources in the network and how they are assigned.
Maintenance: concerned with performing repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run "better".
Provisioning: is concerned with configuring resources in the network to support a given service.
We Monitor

- System & Services
    - Available, reachable
- Resources
    - Expansion planning, maintain availability
- Performance
    - Round-trip-time, throughput
- Changes and configurations
    - Documentation, revision control, logging

We Keep Track of

- Statistics
    - For purposes of accounting and metering
- Faults (Intrusion Detection)
    - Detection of issues,
    - Troubleshooting issues and tracking their history

- Ticketing systems are good at this
- Help Desks are a useful to critical component

7.4 Expectations

A network in operation needs to be monitored in order to:

- Deliver projected SLAs (Service Level Agreements)
- SLAs depend on policy
  - ➔ What does your management expect?
  - ➔ What do your users expect?
  - ➔ What do your customers expect?
  - ➔ What does the rest of the Internet expect?

7.5 Functional Areas of Network Management

The International Organization for Standardization (ISO) Network Management forum divided network management into five functional areas:

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

7.5.1 Fault Management

Is the process of locating problems, or faults, on the data network

It involves the following steps:

- Discover the problem
- Isolate the problem
- Fix the problem (if possible)

7.5.2 Configuration Management

The configuration of certain network devices controls the behavior of the data network. Configuration management is the process of finding and setting up (configuring) these critical devices

7.5.3 Security Management

Is the process of controlling access to information on the data network

Provides a way to monitor access points and records information on a periodic basis.

Provides audit trails and sounds alarms for security breaches

7.5.4 Performance Management

Involves measuring the performance of the network hardware, software, and media.

Examples of measured activities are:

- Overall throughput
- Percentage utilization
- Error rates
- Response time

7.5.5 Accounting Management

Involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources

Involves granting or removing permission for access to the network

Review Questions

i) what is the first thing you will do if you discover your computer is not connecting?

ii) What is network management? Why do networks need to be managed?

iii) Describe the five functional areas of network management.

CHAPTER EIGHT: DISASTER RECOVERY

8.1 Introduction

The fundamental precept of information security is to support the mission of the organization. All organizations are exposed to uncertainties, some of which impact the organization in a negative manner. In order to support the organization, IT security professionals must be able to help their organizations' management understand and manage these uncertainties.

Managing uncertainties is not an easy task. Limited resources and an ever-changing landscape of threats and vulnerabilities make completely mitigating all risks impossible. Therefore, network security professionals must have a toolset to assist them in sharing a commonly understood view with IT and business managers concerning the potential impact of various network security related threats to the mission. This toolset needs to be consistent, repeatable, cost-effective and reduce risks to a reasonable level.

Risk management is nothing new. There are many tools and techniques available for managing organizational risks. There are even a number of tools and techniques that focus on managing risks to information systems. This chapter explores the issue of risk management with respect to information systems and seeks to answer the following questions:

- What is risk with respect to information systems?
- Why is it important to understand risk?
- How is risk assessed?
- How is risk managed?
- What are some common risk assessment/management methodologies and tools?

8.2 What Is Risk With Respect To Network Systems?

Risk is the potential harm that may arise from some current process or from some future event.

Risk is present in every aspect of our lives and many different disciplines focus on risk as it applies to them. From the network security perspective, risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. Network security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information.

Risk is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization.

Threat: The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat-Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability. The threat is merely the potential for the exercise of a particular vulnerability. Threats in themselves are not actions. Threats must be coupled with threat-sources to become dangerous.

This is an important distinction when assessing and managing risks, since each threat-source may be associated with a different likelihood, which, as will be demonstrated, affects risk assessment and risk management. It is often expedient to incorporate threat sources into threats. The list below shows some (but not all) of the possible threats to information systems.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.Notice that the vulnerability can be a flaw or weakness in any aspect of the system.

Vulnerabilities are not merely flaws in the technical protections provided by the system.

Significant vulnerabilities are often contained in the standard operating procedures that systems administrators perform, the process that the help desk uses to reset passwords or inadequate log review. Another area where vulnerabilities may be identified is at the policy level. For instance, a lack of a clearly defined security testing policy may be directly responsible for the lack of vulnerability scanning. Here are a few examples of vulnerabilities related to contingency planning/ disaster recovery:

- Not having clearly defined contingency directives and procedures
- Lack of a clearly defined, tested contingency plan
- The absence of adequate formal contingency training
- Lack of information (data and operating system) backups
- Inadequate information system recovery procedures, for all processing areas (including networks)
- Not having alternate processing or storage sites
- Not having alternate communication services

8.3 Why Is It Important to Manage Risk?

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Therefore, risk management must be a management function rather than a technical function.

It is vital to manage risks to systems. Understanding risk, and in particular, understanding the specific risks to a system allow the system owner to protect the information system commensurate with its value to the organization. The fact is that all organizations have limited resources and risk can never be reduced to zero. So, understanding risk, especially the magnitude of the risk, allows organizations to prioritize scarce resources.

8.4 Risk Assessment

Risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk. It’s easy, right? Unfortunately, risk assessment is a complex undertaking,usually based on imperfect information. There are many

methodologies aimed at allowing risk assessment to be repeatable and give consistent results.

8.4.1 Quantitative Risk Assessment

Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs.

Mathematically, quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period.

ALE = SLE * ARO

Where:

• SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss.

• ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood.

Mathematically, this gets complicated very quickly, involving statistical techniques that are beyond the scope of this discussion.

While utilizing quantitative risk assessment seems straightforward and logical, there are issues with using this approach with information systems. While the cost of a system may be easy to define, the indirect costs, such as value of the information, lost production activity and the cost to recover is imperfectly known at best. Moreover, the other major element of risk, likelihood, is often even less perfectly known. For example, what is the likelihood that someone will use social engineering to gain access to a user account on the accounting system?

Therefore, a large margin of error is typically inherent in quantitative risk assessments for information systems. This might not always be the case in the future. As the body of statistical evidence becomes available, trends can be extrapolated on past experience. Insurance companies and financial institutions make excellent use of such statistics to ensure that their quantitative risk assessments are meaningful, repeatable and consistent.

Typically, it is not cost-effective to perform a quantitative risk assessment for an IT system, due to the relative difficulty of obtaining accurate and complete information. However, if the information is deemed reliable, a qualitative risk assessment is an extremely powerful tool to communicate risk to all level of management.

8.4.2 Qualitative Risk Assessment

Qualitative risk assessments assume that there is already a great degree of uncertainty in the likelihood and impact values and defines them, and thus risk, in somewhat subjective or qualitative terms. Similar to the issues in quantitative risk assessment, the great difficulty in qualitative risk assessment is defining the likelihood and impact values. Moreover, these values need to be defined in a manner that allows the same scales to be consistently used across multiple risk assessments.

The results of qualitative risk assessments are inherently more difficult to concisely communicate to management. Qualitative risk assessments typically give risk results of “High”,

“Moderate” and “Low”. However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization’s management.

8.4.3 Identifying Threats

As was alluded to in the section on threats, both threat-sources and threats must be identified.

Threats should include the threat-source to ensure accurate assessment.

Some common threat-sources include:

- Natural Threats—floods, earthquakes, hurricanes
- Human Threats—threats caused by human beings, including both unintentional (Inadvertent data entry) and deliberate actions (network based attacks, virus infection, unauthorized access)
- Environmental Threats—power failure, pollution, chemicals, water damage

It is valuable to compile a list of threats that are present across the organization and use this list as the basis for all risk management activities. As a major consideration of risk management is to ensure consistency and repeatability, an organizational threat list is invaluable.

8.4.4 Identifying Vulnerabilities

Vulnerabilities can be identified by numerous means. Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, start with commonly available vulnerability lists or control areas. Then, working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system. Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org) or the National Vulnerability Database (NVD - http://nvd.nist.gov). If they exist, previous risk assessments and audit reports are the best place to start.

Additionally, while the following tools and techniques are typically used to evaluate the effectiveness of controls, they can also be used to identify vulnerabilities:

- Vulnerability Scanners – Software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – An attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering
- Audit of Operational and Management Controls – A thorough review of operational and management controls by comparing the current documentation to best practices (such as ISO 17799) and by comparing actual practices against current documented processes.

It is invaluable to have a base list of vulnerabilities that are always considered during every risk assessment in the organization. This practice ensures at least a minimum level of consistency between risk assessments. Moreover, vulnerabilities

discovered during past assessments of the system should be included in all future assessments. Doing this allows management to understand that past risk management activities have been effective.

8.4.5 Relating Threats to Vulnerabilities

One of the more difficult activities in the risk management process is to relate a threat to a vulnerability. Nonetheless, establishing these relationships is a mandatory activity, since risk is defined as the exercise of a threat against a vulnerability. This is often called threat-vulnerability (T-V) pairing. Once again, there are many techniques to perform this task.

Not every threat-action/threat can be exercised against every vulnerability. For instance, a threat of “flood” obviously applies to a vulnerability of “lack of contingency planning”, but not to a vulnerability of “failure to change default authenticators.” While logically it seems that a standard set of T-V pairs would be widely available and used; there currently is not one readily available. This may be due to the fact that threats and especially vulnerabilities are constantly being discovered and that the T-V pairs would change fairly often.

Nonetheless, an organizational standard list of T-V pairs should be established and used as a baseline. Developing the T-V pair list is accomplished by reviewing the vulnerability list and pairing a vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that that threat-action/threat can act against have been identified. For each system, the standard T-V pair list should then be tailored.

8.4.6 Defining Likelihood

Determining likelihood is fairly straightforward. It is the probability that a threat caused by a threat-source will occur against a vulnerability. In order to ensure that risk assessments are consistent, it is an excellent idea to utilize a standard definition of likelihood on all risk assessments.

8.4.7 Sample Likelihood Definitions

Low 0-25% chance of successful exercise of threat during a one-year period

Moderate 26-75% chance of successful exercise of threat during a one-year period

High 76-100% chance of successful exercise of threat during a one-year period

The most important thing is to make sure that the definitions are consistently used, clearly communicated, agreed upon and understood by the team performing the assessment and by organizational management.

8.4.8 Defining Impact

In order to ensure repeatability, impact is best defined in terms of impact upon availability,impact upon integrity and impact upon confidentiality.Sample Impact Definitions illustrates a workable approach to evaluating impact by focusing attention on the three aspects of information security. However, in order to be meaningful, reusable and easily communicated, specific ratings should be produced for the entire organization.

8.4.9 How Is Risk Managed?

Recall that the purpose of assessing risk is to assist management in determining where to direct resources. There are four basic strategies for managing risk: mitigation, transference, acceptance and avoidance. Each will be discussed below. For each risk in the risk assessment report, a risk management strategy must be devised that reduces the risk to an acceptable level for an acceptable cost. For each risk management strategy, the cost associated with the strategy and the basic steps for achieving the strategy (known as the Plan Of Action & Milestones or POAM) must also be determined.

Mitigation is the most commonly considered risk management strategy. Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw. A common mitigation for a technical security flaw is to install a patch provided by the vendor. Sometimes the process of determining mitigation strategies is called control analysis.

Transference

Transference is the process of allowing another party to accept the risk on your behalf. This is not widely done for IT systems, but everyone does it all the time in

their personal lives. Car, health and life insurance are all ways to transfer risk. In these cases, risk is transferred from the individual to a pool of insurance holders, including the insurance company. Note that this does not decrease the likelihood or fix any flaws, but it does reduce the overall impact (primarily financial) on the organization.

Acceptance

Acceptance is the practice of simply allowing the system to operate with a known risk. Many low risks are simply accepted. Risks that have an extremely high cost to mitigate are also often accepted. Beware of high risks being accepted by management. Ensure that this strategy is in writing and accepted by the manager(s) making the decision. Often risks are accepted that should not have been accepted, and then when the penetration occurs, the IT security personnel are held responsible. Typically, business managers, not IT security personnel, are the ones authorized to accept risk on behalf of an organization.

Avoidance

Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself. For instance, during a risk assessment, a website was uncovered that let vendors view their invoices, using a vendor ID embedded in the HTML file name as the identification and no authentication or authorization per vendor. When notified about the web pages and the risk to the organization, management decided to remove the web pages and provide vendor invoices via another mechanism. In this case, the risk was avoided by removing the vulnerable web pages.

8.4.10 Communicating Risks and Risk Management Strategies

Risk must also be communicated. Once risk is understood, risks and risk management strategies must be clearly communicated to organizational management in terms easily understandable to organizational management. Managers are used to managing risk, they do it every day. So presenting risk in a

way that they will understand is key. Ensure you do not try to use “fear, uncertainty and doubt.” Instead, present risk in terms of likelihood and impact. The more concrete the terms are, the more likely organizational management will understand and accept the findings and recommendations.

With a quantitative risk assessment methodology, risk management decisions are typically based on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action. Managers are very familiar with using ROI to make decisions.

Review Questions

i) Explain three ways of mitigating against risk.

ii) Describe the relationship between attack ,threat and vulnerability.

iii) Why is it important to quantify risk before developing mitigating mechanisms ?

iv) How can a network manager secure a wireless network?