St. Mary's University College

Faculty of Informatics

Study Guide

For

Computer Network

Department of Computer Science

Faculty of Informatics

Prepared by

Kalechristos Abebe

215

Degree Exit Exam Study Guides

January 2012

Module summary

The study guide of computer network is organized into seven units, with each unit having its own set of self test problems. The units are selected as, Introduction to data communication and networking, network models, transmission media, LAN technologies and Multiple access, WAN technologies and networks security.

For each of the chapters, self test problems are available as those having answer key and those without answer. All the questions are set to address main areas of the unit mentioned in the specifics objectives list. Students are advised to try to answer all the questions and check out answer for those questions with answer key

Questions listed as those without answer key are all subjective types which help the students to have better understanding of the subject

Unit I

Introduction to data communication and Network

Summary

Data communications are the transfer of data from one device to another via some form of transmission medium. A data communications system must transmit data to the correct destination in an accurate and timely manner. The five components that make up a data communications system are the message, sender, receiver, medium, and protocol. Text, numbers, images, audio, and video are different forms of information. Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.

A network is a set of communication devices connected by media links. In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link. Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology. A network can be categorized as a local area network or a wide area network. A LAN is a data communication system within a building, plant, or campus, or between nearby buildings. A WAN is a data communication system spanning states, countries, or the whole world. An internet is a network of networks. The Internet is a collection of many separate networks. There are local, regional, national, and international Internet service providers. A protocol is a set of rules that govern data communication; the key elements of a protocol are syntax, semantics, and timing. Standards are necessary to ensure that products from different manufacturers can work together as expected. The ISO, ITD-T, ANSI, IEEE, and EIA are some of the organizations involved in standards creation. Forums are special-interest groups that quickly evaluate and standardize new technologies. A Request for Comment is an idea or concept that is a precursor to an Internet standard.

General objective

The general objective of the unit is to help students understand the basic concepts of data communication and computer networks

Specific 0bjectives

Specific objectives of the unit include:

- Define data communication
    - Identify Components of data communication system
    - Identify Characteristics of data communication system
    - Describe direction of data flow
- Identify and describe computer networks
    - Describe Network criteria
    - Describe uses of computer network
    - Explain network physical structure
        - Identify Types of connection
        - Identify Physical topology
            - ✓ Explain the physical layout of topologies
            - ✓ Explain advantages and disadvantages of topologies
    - Identify categories of networks
        - Identify Local Area network(LAN)
        - Identify Wide Area network(WAN)
        - Identify Metropolitan Area Network(MAN)
- Identify the Internet
    - Explain the brief history of Internet
    - Describe Internet service providers
- Identify Protocol and Standards
    - Identify protocols
    - Identify standards
    - Identify standard organizations

Self test Problems without answer key

1. What are the advantages of a multipoint connection over a point-to-point connection?
2. Categorize the four basic topologies in terms of their line configuration
3. Suppose you add two new devices to an existing five device network. If you have a fully connected mesh topology, how many new cable lines are needed? If devices are arranged in a single ring, how many new cable lines are needed?
4. Draw a hybrid topology, with bus back bone connecting two ring back bones. Each ring backbone connects three star networks
5. What are some factors that determine whether a communication system is LAN, MAN or WAN.
6. What is an internet? What is an Internet?
7. Why are protocols and standards needed?

Self test Problems with answer key

Multiple choices

1. Frequency of failure and network recovery time after failure are measures of _____ of a network

   a. Performance b. Reliability c. Security d. Feasibility
2. Which topology requires a central controller or hub?

   a. Star b. Mesh d. Ring Bus
3. The_____ is a physical path over which a message travels

   a. Protocol b. Medium c. Signal d. Standard
4. Which topology requires multipoint connection?

   a. Mesh b. Star c. Bus d. Ring
5. Communication between computer and keyboard involves_____

   a. Simplex b. Duplex c. Half duplex d. Automatic
6. A _____ connection provides a dedicated link between two devices

a. Point-to-point b.Multi point c. Primary d. Secondary

7. A cable break in _____topology stops all transmission
   a. Mesh b. Bus c. Star d. Ring
8. In a network with 25 computers, which topology requires most extensive cabling?
   a. Mesh b. Star c. Bus d. Ring
9. A publishing company with head quarters in Addis Abeba and branch offices throughout Africa, Europe and Asia is probably connected by_____
   a. LAN b. WAN c. MAN d. None of the above
10. In_____ communication , the channel capacity is used by both communicating devices at all times
    a. Simplex b. Half-duplex c. Full-duplex d. Half-simplex

Answer the following questions

11. Identify the five components a data communication system
12. What are the advantages of a multipoint connection over a point-to-point connection
13. Name the four basic network topologies, and cite an advantage of each type
14. Assume six devices are arranged in a mesh topology, how many cables are needed? How many ports are needed for each device?
15. What are the three criteria needed for an efficient and effective network?

Answer Key

1. B	**2. A**	**3. B**
4. C	**5. A**	**6. A**
7. D	**8. A**	**9. B**

10.C

11. The five components of a data communication system are:
    I. Message: information (data) to be communicated
    II. Sender: sender is a device that sends a data message

III. Receiver: Receiver is a device that receives the message

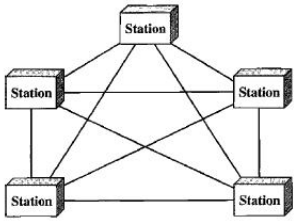
IV. Medium: Transmission medium is a physical path by which message travels for sender to receiver

V. Protocol: Protocol is a set of rules that governs data communication

12. The advantage of multi point connection over point to point connection is that multi point connection provides greater efficiency since more than two devices could share the link

13. The four basic topologies with their advantages and disadvantages

Mesh Toplogy: Each device has a dedicated point to point link to every other device in the network



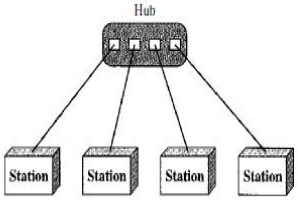
Advantage

- Eliminates traffic problem
- Robust
- Privacy or security

Disadvantages

- Extensive cabling and more number of ports are needed

Star Toplogy: Each device has a point to point link to a central controller device or hub



Advantage

- Less expensive
- Easy to install and configure
- Robust

Bus Topology: In but topology one cable acts as a back bone to link all other devices in the network

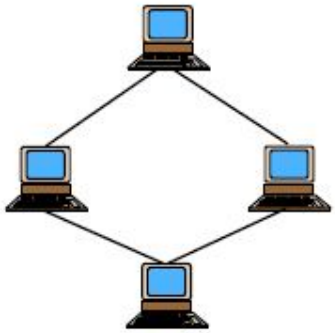
Advantage

- Ease of installation

Disadvantage

- Difficult re connection and fault isolation

Ring Topology: Each device has a dedicated point to point connection with only two devices on either side of it



Advantage

- Easy to install and configure
- Simple fault isolation

Disadvantage

- Unidirectional traffic
- Single point of failure

14. For six devices arranged in a fully connected mesh topology:

Number of cables needed = 6x(6-1)/2=15

Number of ports needed for each device=6-1=5

15. The three criteria's needed for efficient and effective network are@

I. Performance :Performance can be measured with transit time and response time of the network

II. Reliability: is a measure network frequency of failure, time it takes to recover from failure, and network's robustness in catastrophe

III. Security: Security issues include protecting data for un authorized access

Unit Two

Network Models

Summary

The International Standards Organization created a model called the Open Systems Interconnection, which allows diverse systems to communicate. The seven-layer OSI model provides guidelines for the development of universally compatible networking protocols. The physical, data link, and network layers are the network support layers. The session, presentation, and application layers are the user support layers

TCP/IP is a five-layer hierarchical protocol suite developed before the OSI model. The TCP/IP application layer is equivalent to the combined session, presentation, and application layers of the OSI model. Four levels of addresses are used in an internet following the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses. The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. The IP address uniquely defines a host on the Internet, The port address identifies a process on a host A specific address is a user-friendly address

General Objective

The general objective of the unit is to understand the network reference model

Specific Objectives

At the end of the unit students are expected to

- Understand the concepts of OSI reference model
    - Identify layered architecture
    - Identify peer-to-peer process
    - Indentify encapsulation
    - Identify layers in the OSI model
        - Explain the function of Physical layer
        - Explain the function of data link layer
        - Explain the function of network layer
        - Explain the function of transport layer
        - Explain the function of session layer
        - Explain the function of presentation layer
        - Explain the function of application layer
- Understand the concepts of TCP/IP reference model
    - Identify TCP/IP layers
        - Identify physical and data link layers
        - Identify network layer
        - Identify transport layer
        - Identify application layer
    - Identify TCP/IP protocols
        - Identify Internet protocol
        - Identify Transmission control protocol
        - Identity user datagram protocol
        - identify application layer protocols
    - identify IP addressing techniques
        - Explain IP address assignments
        - Explain IP address classes
    - Identify subnet addressing

- Explain subnetting
- Explain subnet masking

Self test problems without answer key

1. What are the advantages of using UDP over TCP?
2. Why is domain name reversed when searching for the IP address?
3. Write the functions of the following application layer protocols
   i. DHCP
   ii. DNS
   iii. FTP
   iv. RPC
4. Draw two Ethernet LANs connected by a gateway. Each LAN has three hosts. One LAN is class B and one is class C. Choose appropriate internet addresses. How many connections must the gateway have?
5. What is the difference between physical address and logical address?
6. Find the classes of the following IP addresses
   a. 121.56.3.67
   b. 193.23.56.23
   c. 231.23.67.123
   d. 142.23.56.23
7. Find the network addresses for IP addresses given in problem 6
8. Give some advantages and disadvantages of combining the session, presentation, and application layer in the OSI model into one single application layer as in the Internet model
9. For the given class B IP address give below, find

   IP:255.255.254.0

   i. Network address
   ii. Subnet Mask
   iii. Broad cast address

Self test problem with answer key

Choose the best answer for the following

1. The _____ layer of OSI model decides the location of synchronization points
   a. Transport b. Session c. Presentation d. Application
2. Which of the following layers of OSI model is responsible for end to end delivery of entire message?
   a. Network b. Transport c. Session d. Presentation
3. In the _____layer of OSI model , data unit is called a frame
   a. Physical b. Data link c. Network d. Transport
4. Which layer of the OSI model uses the trailer of the frame for error detection?
   a. Physical b. Data link c. Transport d. Presentation
5. On which layer of the OSI model both header and trailer information are added?
   a. Physical b. Network c. Data link d. Transport
6. Which of the following applies of UDP?
   a. Un reliable and connectionless
   b. Contains destination and source port addresses
   c. Reports certain errors
   d. All of the above
7. Which of the following is a class A network address?
   a. 128.4.5.6
   b. 127.4.5.0
   c. 127.0.0.0
   d. 127.8.0.0
8. Which of the following is a class B host address
   a. 230.0.0.0
   b. 130.4.5.6
   c. 230.4.5.9
   d. 30.4.5.6
9. Which IP address class has few hosts per network?

a. A b. B c. C d. D

10. The data unit in TCP/IP data link layer is called_____

a. Message b. Segment c. Datagram d. Frame

Answer the following questions

11. Describe the fields available in IPV6 header format
12. Physical, port, and IP addresses are used in data communication. In TCP/IP environment, what layers are they associated with?
13. What does subnetting and subnet masking refers to?
14. For the given class B IP address give below, find

    IP:255.255.192.0

    i. Network address

    ii. Subnet Mask

    iii. Broad cast address

Answer Key

1. B	2. B	3. B	
4. B	5. C	6. D	
7. C	8. B	9. C	10. D

11. IPV6 Header format is as follows

Traffic Class: This 8-bit value specifies what, if any, form of differentiated service is to be provided for the packet. Use of this field is defined separately from IPv6; see RFC 2474 for more about differentiated services. The default value for this field is all zeros.

Flow label: This 20-bit value identifies packets that belong to the same flow. A node can be the source for more than one simultaneous flow. The flow label and the address of the source node uniquely identify flows.

Payload length: This 16-bit field contains an integer value equal to the length of the packet payload in octets; that is, the number of octets contained in the packet after the end of the IPv6 header. IPv6 extensions are included as part of the payload for the purposes of calculating this field.

Next header: This field indicates what protocol is in use in the header immediately following the IPv6 packet. Similar to the IPv4 protocol field, the next header field may refer to a higher layer protocol like TCP or UDP, but it may also indicate an IPv6 extension header.

Hop limit: Every time a node forwards a packet, it decrements this eight-bit field by one. If the hop limit reaches zero, the packet is discarded. Unlike in IPv4, where the time-to-live field fulfills a similar purpose, sentiment is currently against putting a protocol-defined upper limit on packet lifetime for IPv6. This means that the function of timing-out old data should be accomplished in upper layer protocols.

Destination address: This is the 128-bit address of the intended recipient of the IPv6 packet. This address may be a unicast, multicast, or anycast address. If a routing extension is being used (which specifies a particular route that the packet must traverse), the destination address may be one of those intermediate nodes instead of the ultimate destination node.

12. The physical address is associated with the data link layer. The logical address is associated with the network layer. A port address is associated with application layer

13. Subnetting refers to the partitioning of a network address space into separate autonomous sub networks.

14. IP address: **255.255.192.0**

172.16.0.0=Network address

255.255.192.0=Subnet mask

1. 2^2–2=2.

2. 2^{14}–2=16,382.

3. 256–192=64. 64+64=128.

4. First find the broadcast addresses in step 5, then come back and perform step 4 by filling in the host addresses.

5. Find the broadcast address of each subnet, which is always the number right before the next subnet.

The following table shows the two subnets available, the valid host range, and the broadcast address of each.

Subnet	64.0	128.0
First Host	64.1	128.1
Last Host	127.254	191.254
Broadcast	127.255	191.255

Notice we just added the fourth octet's lowest and highest values and came up with the answers. Again, it is the same answer as for a Class C subnet, but we just added the fourth octet.

Unit 3

Transmission Media

Summary

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. Transmission media lie below the physical layer. Guided medium provides a physical conduit from one device to another. Twisted pair cable, coaxial cable, and optical fiber are the most popular types of guided media. Twisted-pair cable consists of two insulated copper wires twisted together. Twisted pair cable is used for voice and data communications. Coaxial cable consists of a central conductor and a shield. Coaxial cable can carry signals of higher frequency ranges than twisted-pair cable. Coaxial cable is used in cable TV networks and traditional Ethernet LANs. Fiber-optic cables are composed of a glass or plastic inner core surrounded by cladding, all encased in an outside jacket. Fiber-optic cables carry data signals in the form of light. The signal is propagated along the inner core by reflection. Fiberoptic transmission is becoming increasingly popular due to its noise resistance, low attenuation, and high-bandwidth capabilities. Fiber-optic cable is used in backbone networks, cable TV networks, and Fast Ethernet networks. Unguided media (free space) transport electromagnetic waves without the use of a physical conductor.

Wireless data are transmitted through ground propagation, sky propagation, and line of-sight propagation. Wireless waves can be classified as radio waves, microwaves, or infrared waves. Radio waves are Omni-directional; microwaves are unidirectional. Microwaves are used for cellular phone, satellite wireless LAN communications. Infrared waves are used for short-range communications such as those between a PC and a peripheral device. It can also be used for indoor LANs.

General Objective

The general objective of the unit is to understand use of transmission media at the physical layer

Specific Objectives

At the end of the unit, students are expected to:

- Understand use of guide media

- Explain the working mechanism of twisted pair cable
- Explain the working mechanism of coaxial cable
- Explain the working mechanism of Fiber optic cable

- Understand the use of Un guided transmission media
  - Explain the working mechanism of Radio waves
  - Explain the working mechanism of microwaves
  - Explain the working mechanism of infrared

Self test problems without answer key

1. How do guided media differ from unguided media?
2. How does sky propagation differ from line of sight propagation?
3. Differentiate straight through and cable cross over connections in twisted pair
4. Name the advantages of fiber optic over twisted pair cable
5. Differentiae among the following coaxial cable standards
   i. RG-8
   ii. RG-9
   iii RG-11
   iv RG-58

Self test problems with answer key

Choose the best answer for the following

1. Transmission media are usually categorized as _____
   a. Fixed or unfixed
   b. Guided or unguided
   c. Determined or undetermined
   d. Metallic or non metallic
2. In fiber optics , the signal source is _____ waves
   a. Light
   b. Radio

c. Infrared
d. Very low frequency

3. In an environment with many high voltage devices , the best transmission medium is___
    a. Twisted pair cable
    b. Coaxial cable
    c. Optical fiber cable
    d. Atmospheres
4. What is the reason that makes coaxial cable less susceptible to noise than twisted pair cable?
    a. Inner conductor
    b. Diameter of cable
    c. Outer conductor
    d. Insulating material
5. The inner core of an optical fiber is _____ in composition
    a. Glass or plastic
    b. Copper
    c. Bimetallic
    d. Liquid

Answer the following questions

6. Explain what cross talk is and what is needed to reduce it
7. Why should the light ray be reflective rather than refractive in fiber optics?
8. Why is there a distance limit of terrestrial microwaves? What factors do you need to calculate this limit?
9. Discuss the different categories of twisted pair cable

Answer Key

1. B 2. A 3. C
4 C 5. A

6. Cross talk is the undesired effect of one circuit (channel) on another circuit. Cross talk can be reduced by shielding each pair of twisted pair cable
7. In fiber optics cable the light ray needs to travel along a long narrow channel, the core; it does this by successive reflections against the cladding. On the other hand , a refractive ray goes into the cladding and leaves the core area; the information thus does not get propagated; it is lost
8. Terrestrial microwave transmission is limited by the curvature of the earth and the height of the antenna. Both of these factors are needed to calculate the distance a signal can travel
9. The different categories of twisted pair cable are shown in the table below

Category	*Specification*	*Data Rate (Mbps)*	*Use*
I	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

Unit 4

Local Area Networks and multiple Access

Summary

We can consider the data link layer as two sub layers. The upper sublayer is responsible for data link control, and the lower sub layer is responsible for resolving access to the shared media. Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups: random access protocols, controlled access protocols, and channelization protocols.

Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet .Ethernet is the most widely used local area network protocol. The IEEE 802.3 Standard defines I-persistent *CSMA/CD* as the access method for first-generation 10-Mbps Ethernet. In this unit, the focus is on IEEE Standard Project 802, designed to regulate the manufacturing and interconnectivity between different LANs

General objective

The general objective of the unit is to understand different LAN technologies and multiple access schemes

Specific objectives

At the end of the unit students are expected to:

- Define multiple access
    - Explain random access techniques
        - Explain how carrier sense multiple access (CSMA) works
        - Explain how carrier sense multiple access with collision detection (CSMA/CD)works
        - Explain how carrier sense multiple access with collision avoidance(CSMA/CA) works
    - Explain controlled access techniques
        - Explain how reservation technique works
        - Explain how polling technique works
        - Explain how token passing technique works

  - Explain channelization techniques
    - Explain how Frequency –Division multiple access(FDMA) works
    - Explain how Time-Division Multiple access(TDMA) works
    - Explain how Code-Division Multiple access (CDMA) works
- Define LAN technologies
  - Explain the IEEE standards
    - Explain functions of data link layer
    - Explain functions of physical layer
  - Explain the standard Ethernet
    - Explain Ethernet topologies
    - Explain the functions of MAC sub layer
    - Explain bridged Ethernet
    - Explain switched Ethernet
    - Explain full-duplex Ethernet
    - Explain fast Ethernet
    - Explain gigabit Ethernet

Self test problems without answer key

1. Define random access and list protocols in this category
2. Explain why collision is an issue in a random access protocol but not in controlled access or channelizing protocols
3. Compare and contrast a controlled access protocol with a channelizing protocol.
4. Write the functions of the following data link sub layers
   a. LLC
   b. MAC
5. Differentiate among the following types of Ethernet
   a. Bridged Ethernet
   b. Switched Ethernet
   c. Giga bit Ethernet

6. Compare the following LAN technologies in terms of their topology, alternate topology, access method and transmission media used
    a. Ethernet
    b. Token ring

Self test problems with answer key

Choose the best answer for the following

1. In CSMA/CD, the number of collision is _____ than MA
    a. Greater than
    b. Less than
    c. Equal to
    d. twice
2. In Ethernet , the source address field in the MAC frame is _____ address
    a. The original senders physical
    b. The previous stations physical
    c. The next destinations physical
    d. The original senders service port
3. Which of the following use star topology?
    a. 10BASE5
    b. 10BASE2
    c. 10BASE-T
    d. None of the above
4. 10BASE2 uses _____ cable while 10BASE5 uses _____
    a. Thick coaxial , thin coaxial
    b. Twisted pair , thick coaxial
    c. Thin coaxial , thick coaxial
    d. Fiber optic, thin coaxial
5. _____ specifies a star topology featuring central hub and daisy chaining
    a. 10BASE5
    b. 10BASE2
    c. 10BASE-T
    d. 1BASE5
6. What can happen at a token ring station?
    a. Examination of destination address
    b. Regeneration of the frame

c. Passing of the frame to the next station

d. All of the above

7. In token ring , where is the token when a data frame is in circulation?
   a. At the receiving station
   b. At the sending station
   c. Circulating the ring
   d. None of the above
8. Which LAN has the highest data rate?
   a. 10BASE5
   b. 10BASE-T
   c. Twisted –pair token ring
   d. FDDI
9. In which OSI layer does the FDDI protocol operate?
   a. Physical
   b. Data link
   c. Network
   d. A and b
10. Which project of 802 standard provides for collision-free protocols?
    a. 802.2
    b. 802.3
    c. 802.5
    d. 802.6

Answer the following questions

11. Explain how CSMA/CD works
12. Explain how token passing works
13. Explain the how the FDMA channel access method works

Answer Key

1. B
2. B
3. C
4. C
5. D
6. D
7. B
8. D
9. D
10. C

11. The basic idea behind *CSMA/CD* is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

12. In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor* and a *successor*. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send

13. In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a band pass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small *guard bands*. FDMA specifies a predetermined frequency band for the entire

period of communication. This means that stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA

Unit 5

Connecting LAN's, Backbone networks, virtual LAN's

Summary

LANs do not normally operate **in** isolation. They are connected to one another or to the Internet. To connect LANs, or segments of LANs, we use connecting devices. Connecting devices can operate **in** different layers of the Internet model.

A repeater is a connecting device that operates in the physical layer of the Internet model. A repeater regenerates a signal, connects segments of a LAN, and has no filtering capability. A bridge is a connecting device that operates in the physical and data link layers of the Internet model. A transparent bridge can forward and filter frames and automatically build its forwarding table. A bridge can use the spanning tree algorithm to create a loop less topology. A backbone LAN allows several LANs to be connected. A backbone is usually a bus or a star. A virtual local area network (VLAN) is configured by software, not by physical wiring. Membership in a VLAN can be based on port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of these features. VLANs are cost- and time-efficient, can reduce network traffic, and provide an extra measure of security.

General Objective

To understand the different ways of connecting LAN's, backbone network and VLAN's

Specific Objectives

At end of the unit students are expected to:

- Understand LAN connecting devices
    - Explain the operations of Hubs

        - Describe Hub operation
        - Describe Hub features
        - Describe Peer versus stand alone hubs
        - Describe intelligent Hubs
        - Describe multi architecture Hubs
    - Explain operations of Switches
        - Describe operations of switches
        - Describe two layer switches
        - Describe three layer switches
    - Explain the operations of repeaters
        - Describe repeaters and network architecture
        - Describe repeater to repeater connection
    - Explain the operations of routers
        - Describe Route Discovery
        - Describe Router Operation
        - Describe Router Groupings
        - Describe Router Protocols
    - Explain operations of bridges
        - Bridges versus Routers, Brouters, and Repeaters
        - Protocol Independence of Bridges
        - Packet Transmission
        - Types of Bridges
    - Explain the operations of gateways
        - Gateways in Networks
        - Gateway Operation
        - Gateway Categories
- Understand backbone networks

- Explain bus backbone network
- Explain star backbone network
- Explain connecting remote LANs

- Understand virtual LAN
  - Describe VLAN membership
  - Describe VLAN configuration

Self test problems without answer key

1. Differentiate among the following types of LAN switches
   i. Store and forward
   ii. Cut through
2. Describe the working mechanism of ISL protocol for VLAN
3. How does VLAN reduce network traffic?
4. What do we mean when we say that a bridge can filter traffic? Why is filtering important?
5. Write the operations of distance vector and link state routing algorithms
6. How is a repeater different from amplifier
7. Describe operations of bus and star backbone networks

Self test problems with answer key

Choose the best answer for the following

1. Which of the following uses greater number of layers in OSI model?
   a. Bridge
   b. Repeater
   c. Router
   d. Gateway

2. A bridge forwards or filters a packet comparing the information in its address table to the packet's_____
   a. Layer 2 source address
   b. Source node's physical address
   c. Layer 2 destination address
   d. Layer 3 destination address
3. A simple bridge does which of the following?
   a. Filters a data packet
   b. Forwards a data picket
   c. Extends LAN's
   d. All of the above
4. Which of the following are bridge types?
   a. Simple,complex,learning
   b. Simple, learning, multiport
   c. Simple , complex, multiport
   d. Spanning ,contract, suspension
5. The shortest path in routing refers to _____
   a. The least expensive path
   b. The least distant path
   c. The path with smallest number of hops
   d. Any or combination of then above
6. Gateways function in which OSI layers?
   a. The lower three
   b. The upper four
   c. All seven
   d. All but the physical layer
7. A repeater takes a weakened signal and _____ it

a. Amplifies
b. Regenerates
c. Resamples
d. Reroutes

8. In distance vector routing each router receives vectors from_____
   a. Every router in the network
   b. Every router less than two units away
   c. A table stored by the software
   d. It's neighbours only
9. In link state routing , flooding allows changes to be recorded by _____
   a. All routers
   b. Neighbour routers only
   c. Some routers
   d. All networks
10. For which of the following would you not need to provide a crossover cable?
    a. Connecting uplinks between switches
    b. Connecting routers to switches
    c. Connecting hub to hub
    d. Connecting hub to hub

Answer the following questions

11. Write the three distinct functions of layer2 switching
12. Describe the difference between static and dynamic VLAN
13. Describe the active and passive hubs

Answer key

1. D	3. D	5. D
2. C	4. B	6. C

7. B
8. D
9. A
10. B

11. There are three distinct functions of layer-2 switching:

    Address learning:

    Layer-2 switches and bridges remember the source hardware address of each frame received on an interface and enter this information into a MAC database.

    Forward/filter decisions: When a frame is received on an interface, the switch looks at the destination hardware address and finds the exit interface in the MAC database.

    Loop avoidance: If multiple connections between switches are created for redundancy, network loops can occur. The Spanning-Tree Protocol (STP) is used to stop network loops and allow redundancy.

12. *Static VLANs* are the typical way of creating VLANs and the most secure. The switch port that you assign a VLAN association always maintains that association until an administrator changes the port assignment. This type of VLAN configuration is easy to set up and monitor, working well in a network where the movement of users within the network is controlled. Using network management software to configure the ports can be helpful but is not mandatory.

    Dynamic VLANs determine a node's VLAN assignment automatically. Using intelligent management software, you can enable hardware (MAC) addresses, protocols, or even applications to create dynamic VLANs. For example, suppose MAC addresses have been entered into a centralized VLAN management application. If a node is then attached to an unassigned switch port, the VLAN management database can look up the hardware address and assign and configure the switch port to the correct VLAN. This can make management and configuration easier for the

administrator. If a user moves, the switch will automatically assign them to the correct VLAN. However, more administration is needed initially to set up the database.

13. Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Active Hubs

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. We have seen examples of hubs in some Ethernet implementations (10Base-T, for example). However, hubs can also be used to create multiple levels of hierarchy

Unit 6

Wide Area Networks

Summary

To understand WAN technologies, you need to understand the different WAN terms and connection types that can be used to connect your networks together. This unit focuses the different WAN terms and connection types typically used by service providers. Leased line, circuit switching and packet switching are types of connections to be used. The unit also focuses on different WAN technologies like , Distributed Queue Dual Bus (DQDB) ,Synchronous Digital Hierarchy (SDH),Synchronous Optical Network (SONET) Asynchronous Transfer Mode (ATM)

General Objective:

To understand different WAN connections and technologies

Specific Objectives:

At the end of the unit students are expected to

- Understand the concept of WAN
    - Describe WAN connection types
        - Describe leased line connection
        - Describe circuit switching
        - Describe packet switching

    Describe WAN technologies
        - Describe Synchronous Digital Hierarchy (SDH)
        - Describe Synchronous Optical Network (SONET)
        - Describe Asynchronous Transfer Mode (ATM)
        - Frame relay
        - Describe integrated services digital network(ISDN)

Self test problems without answer key

1. What is the relationship between SONET and SDH?
2. There are no sequence numbers in Frame Relay. Why?
3. How is an ATM virtual connection identified?
4. Briefly describe the issues involved in using ATM technology in LANs.
5. Discuss the Frame Relay physical layer.

Self test problems with answer key

Choose the best answer

1. ATM can use_____ as transmission medium
    a. Twisted pair cable
    b. Coaxial cable
    c. Fiber optic cable

d. All of the above

2. Which layer in ATM protocol reformats the data received from other networks?
   a. Physical
   b. ATM
   c. Application adaptation
   d. Data adaptation
3. Which AAL type can best process a data stream having a non constant bit rate?
   a. AAL1
   b. AAL2
   c. AAL3/4
   d. AAL5
4. SONET is a standard for _____ networks
   a. Twisted pair cable
   b. Coaxial cable
   c. Ethernet
   d. Fiber optic cable
5. SONET's _____layer correspond to the OSI model's physical layer
   a. Path
   b. Line
   c. Section
   d. Photonic
6. The optical link between two SONET devices is called_____
   a. Section
   b. Line
   c. Path
   d. None of the above
7. What does the ISDN Basic Rate Interface (BRI) provide?

b. 23 B channels and one 64Kbps D channel
c. Total bit rate of up to 1.544Mbps
d. Two 56Kbps B channels and one 64Kbps D channel
e. Two 64Kbps B channels and one 16Kbps D channel

Answer the following questions

8. Describe the leased line, circuit switching and packet switching WAN connection types
9. Discuss the functions of each SONET layer
10. Name the ATM layers

Answer Key

1. D
2. C
3. B
4. D
5. C
6. A
7. B

8. The following are WAN connection types:

Leased lines Typically referred to as a point-to-point or dedicated connection. It is a pre-established WAN communications path from the CPE, through the DCE switch, to the CPE of the remote site, allowing DTE networks to communicate at any time with no setup procedures before transmitting data. It uses synchronous serial lines up to 45Mbps.

Circuit switching

Sets up line like a phone call. No data can transfer before the end-to-end connection is established. Uses dial-up modems and ISDN. It is used for low-bandwidth data transfers.

Packet switching

WAN switching method that allows you to share bandwidth with other companies to save money. Think of packet switching networks as a party line. As long as you are not constantly transmitting data and are instead using bursty data transfers, packet switching

can save you a lot of money. However, if you have constant data transfers, then you will need to get a leased line. Frame Relay and X.25 are packetswitching technologies. Speeds can range from 56Kbps to 2.048Mbps

9. The following are SONET layers and their functions

Path Layer

The path layer is responsible for the movement of a signal from its optical source to its optical destination. At the optical source, the signal is changed from an electronic form into an optical form, multiplexed with other signals, and encapsulated in a frame. At the optical destination, the received frame is demultiplexed, and the individual optical signals are changed back into their electronic forms. Path layer overhead is added at this layer. STS multiplexers provide path layer functions.

Line Layer

The **line layer** is responsible for the movement of a signal across a physical line. Line layer overhead is added to the frame at this layer. STS multiplexers and add/drop multiplexers provide line layer functions.

Section Layer

The **section layer** is responsible for the movement of a signal across a physical section. It handles framing, scrambling, and error control. Section layer overhead is added to the frame at this layer.

Photonic Layer

The **photonic layer** corresponds to the physical layer of the OSI model. It includes physical specifications for the optical fiber channel, the sensitivity of the receiver, multiplexing functions, and so on. SONET uses NRZ encoding with the presence of light representing 1 and the absence of light representing 0

10. The following are ATM layers and their function

    A. Application adaptation layer (AAL)

    B. ATM Layer

C. Physical Layer

Unit 7

Network Security

Summary

The increase in attacks of message during transmission coincides with an increased use of the Internet and with increases in the complexity of protocols, applications, and the Internet itself. Critical infrastructures increasingly rely on the Internet for operations. Individual users rely on the security of the Internet, email, the Web, and Web-based applications to a greater extent than ever. Thus, a wide range of technologies and tools are needed to counter the growing threat. At a basic level, cryptographic algorithms for confidentiality and authentication assume greater importance. As well, designers need to focus on Internet-based protocols and the vulnerabilities of attached operating systems and applications.

Thus network security typically deals applying different cryptographic techniques in order secure a message selecting different protocols and algorithms to counter measure attacks

General objective

To understand the different network security techniques

Specific Objectives

At the end of this unit students are expected to :

- Describe Security Trends
- Explain The OSI Security Architecture
- Explain Security Attacks

- Explain Passive Attacks and Active Attacks

- Describe Security Services
  - Authentication
  - Access Control
  - Data Confidentiality
  - Data Integrity
  - Nonrepudiation
  - Availability Service
  - Security Mechanisms

- Describe Confidentiality with Symmetric Encryption
  - Explain Symmetric Encryption
  - Explain Encryption Algorithms
  - Explain Location of Encryption Devices

- Describe Message Authentication and Hash Functions

- Describe Public-Key Encryption and Digital Signature
  - Explain Public Key Encryption
  - Explain Digital Signature
  - Explain The RSA Public-Key Encryption Algorithm
  - Explain Key Management

- Describe Secure Socket Layer and Transport Layer Security
    - Explain SSL Architecture
- Describe IP security and email security
    - Explain IPV4 and IPV6 securities
    - Explain the scope of IPSec

Self test problems without answer key

1. Differentiate between security services and mechanisms
2. Define the following terms
    a. Cryptography
    b. Cryptanalysis
3. What are important features of symmetric encryption
4. Describe the hash function properties and procedures
5. Differentiate between public and private keys
6. Explain the key management techniques used in public crypto system
7. Write the digital signature algorithm and its properties
8. Explain the SSL architecture

Self test problems with answer key

1. Differentiate between active and passive attacks
2. Describe the meaning of the following security services
    a. Access control
    b. Non repudiation
    c. Authentication
3. Define the following basic terminologies
    a. Plain text
    b. Cipher text
    c. Cipher
    d. Key
    e. Encryption
    f. Decryption
4. Explain how cryptographic systems are characterized
5. Describe the message authentication code (MAC) procedures
6. Write essential differences of symmetric(conventional) and asymmetric(public key) encryption
7. Write the RSA public key encryption/decryption algorithm

8. What are IPSec services?
9. Write the PGP operations used for email security

Answer key

1. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service

2. **Access Control** - prevention of the unauthorized use of a resource

Non-Repudiation - protection against denial by one of the parties in a in

Communication

Authentication - assurance that the communicating entity is the one claimed

3. Basic terminologies definition
    a. plaintext - original message
    b. cipher text - coded message
    c. cipher - algorithm for transforming plaintext to cipher text
    d. key - info used in cipher known only to sender/receiver
    e. Encryption - converting plaintext to cipher text
    f. Decryption - recovering cipher text from plaintext

4. Cryptographic systems are characterized by

a. type of encryption operations used

i. substitution / transposition / product

b. number of keys used

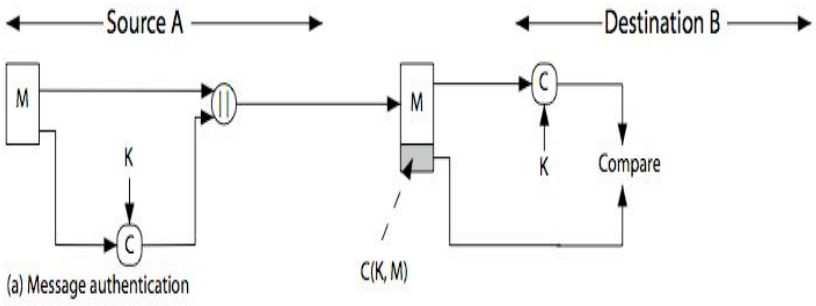
i. single-key or private / two-key or public

c. way in which plaintext is processed

i. block / stream

5. Message authentication code MAC works as follows

- ✓ Generated by an algorithm that creates a small fixed-sized block
- ✓ depending on both message and some key
- ✓ like encryption though need not be reversible
- ✓ appended to message as a signature
- ✓ receiver performs same computation on message and checks it matches the MAC
- ✓ provides assurance that message is unaltered and comes from sender



des

Where

M= input message

C = MAC function

K = shared secret key

MAC = message authentication code

6.

Conventional encryption	Public key encryption
• The same algorithm with the same key is used for encryption and decryption. • The sender and receiver must share the algorithm and the key • One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. • The sender and receiver must each have one of the matched pair of keys (not the same one).	• One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. • The sender and receiver must each have one of the matched pair of keys (not the same one) • One of the two keys must be kept secret.

St. Mary's University College

Faculty of Informatics

7. RSA encryption and decryption algorithms are stated as follows

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

8. The following describes

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

IPSec services

- ✓ Access control
- ✓ Connectionless integrity
- ✓ Data origin authentication
- ✓ Rejection of replayed packets
- ✓ a form of partial sequence integrity
- ✓ Confidentiality (encryption)
- ✓ Limited traffic flow confidentiality

9. PGP operations for email authentication are

a. sender creates message

b. use SHA-1 to generate 160-bit hash of message

c. signed hash with RSA using sender's private key, and is attached to message

d. receiver uses RSA with sender's public key to decrypt and recover hash code

receiver verifies received message using hash of it and compares with decrypted hash code