A TEAM BY VU SQUAD

CS-601 FINAL TERM NOTCE BY MOHSIN CHINIOTI

03137248280

VUSQUAD134@GMAIL.COM

Chptr(9 to 16)

Note: M means MCQs & Q means Question

Chapter 09

Data-Link Layer

The Internet is a combination of networks joined together by connecting devices (routers or switches). M

If a packet is to travel from a host to another host, it needs to pass through these networks. M

Data Link layer controls node-to-node communication. M

Nodes and Links

Communication at the data-link layer is node-to-node. M

A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point.

We refer to the two routers as a node and the networks in between as a links. M

Services provided by Data-Link Layer

Data Link Layers Located between the physical and the network layers. M

Data Link Layers Provides services to Network Layer and receives services from Physical layer. M

- Framing
- Flow Control
- Error Control
- Blocking Control

Two Categories of Links

We can have the following two types of links: M &Q

- ✓ Point-to-point link or a
- ✓ Broadcast link

Two nodes are physically connected by a transmission medium such as cable or air. M

Data-link layer controls how the medium is used

- ✓ Data-link layer can use whole capacity
- ✓ Data-link layer can use only part of the capacity

Two Sub layers of Data-Link Layer M

- Data Link Control (DLC)
- Media Access Control (MAC)

DLC is both Broadcast and point to point links. M

MAC is Only Broadcast link. M

Why LINK-LAYER ADDRESSING?

IP addresses are the identifiers at the network layer. M

In Internet we cannot make a packet reach its destination using only IP addresses.

Source end and destination end, IP addresses define the both ends but cannot define which links the packet will take.

Three Types of addresses

Some link-layer defines three types of addresses: M

- Unicast
- Multicast
- Broadcast

Even numbers show the multicast Address. M

Address Resolution Protocol (ARP)

Anytime a node has an IP packet to send to another node in a link, it has the IP address of the receiving node.

IP address of the next node is not helpful in moving a frame through a link; we need the link-layer address of the next node then for this purpose we need Address Resolution Protocol (ARP).

Chapter 10

Types of Errors

Data transmission suffers unpredictable changes because of interference. M

The interference can change the shape of the signal. M

- ✓ Single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1 M
- ✓ Burst Error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1 M

Redundancy

Central concept in detecting or correcting errors is Redundancy. M

Redundancy is able to detect or correct errors, we send some extra bits with our data. The presence of these redundant bits allows the receiver to detect or correct corrupted bits. M

Detection versus Correction

Correction is more difficult than the detection. M

In error detection, we are only looking to see if any error has occurred (Yes or No). We are not interested in the number of corrupted bits in Detection. M

Single-bit error is same as a Burst error In Error Correction, we need to know: M

- ✓ The exact number of bits that are corrupted and,
- ✓ Their location in the message

Coding

Redundancy is achieved through various coding schemes.

Sender adds redundant bits through a process that creates a relationship between redundant bits and the actual data bits.

The receiver checks the relationships between the two sets of bits to detect errors

The ratio of redundant bits to data bits and the strength of the process are important factors in any coding scheme. M

Types of Coding Schemes

Coding schemes can be divided into 2 broad categories: M

- ✓ Block Coding
- ✓ Difficulty Coding

Block Coding

We divide our message into blocks, each of 'k' bits, called data words. M

We add 'r' redundant bits to each block to make the length

'n = k + r' M

The resulting 'n-bit' blocks are called code words. M

BLOCK CODING in Error Detection

If the following two conditions are met, the receiver can detect a change in the original code word:

- ✓ The receiver has (or can find) a list of valid code words
- ✓ The original code word has changed to an invalid one

Hamming Distance

Hamming Distance is Distance between two words with the same size and differences number of corresponding bits. M

Hamming Distance between two words x and y is $d(x, y)$. M

Hamming distance between received code word and sent code word.

Minimum Hamming Distance

Minimum Hamming Distance is smallest hamming distance between all possible pairs of code words.

$D_{min} = s+1$

Where,

S →no. of detectable errors

D_{min} → minimum hamming distance

For Example,

A code scheme has a Hamming distance $D_{min} = 4$. This code guarantees the detection of up to how many errors?

$D_{min} = 4$

$D_{min} = s+1$

To find the number of detectable error,

S?

$S = D_{min} - 1$

$S = 4 - 1$

$S = 3$

Linear Block Codes

Subset of Block Codes in which the exclusive OR of two valid code words creates another valid code word,

Linear block code (n=k+1)

Parity-Check Code

Most common error-detecting code, M

The extra parity bit is selected to make total number of 1s in code word even.

CYCLIC CODES

Special linear block codes with one extra property,

If a code word is cyclically shifted (rotated), the result is another code word

If 1011000 is a code word and we cyclically left-shift, then 0110001 is also a code word.

Cyclic Redundancy Check (CRC)

Cyclic redundancy check (CRC) is used in networks such as LANs and WANs. M

Advantages of Cyclic Codes

1. Good performance in detection:

Single-bit errors

Double errors

Odd number of errors

Burst errors

2. Easy Implementation

3. Fast Implementation

CHECKSUM

Error-detection technique that can be applied to a message of any length, M

Checksum mostly used at the network and transport layer rather than the data-link layer. M

Forward Error Correction

Retransmission of corrupted and lost packets is not useful for real-time multimedia transmission. We need to correct the error or reproduce the packet immediately. Several techniques developed and are commonly called Forward Error Correction techniques.

Using Hamming Distance

For error detection, we definitely need more distance.

It can be shown that to correct' errors, we need to have:

$$D_{min} = 2t + 1$$

If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits. A lot of redundant bits need to be sent with the data.

If we want to correct 10 bits in a packet, we need to make the minimum hamming distance 21 bits.

$D_{min} = 2t + 1$

$= 2(10) + 1$

$= 21$ bits

Using XOR

Another recommendation is to use the property of the exclusive OR operation as shown below.

$$R = P_1 \oplus P_2 \oplus .. \oplus P_i \oplus ... \oplus P_N$$

This means:

$$P_i = P_1 \oplus P_2 \oplus .. \oplus R \oplus . . \oplus P_N$$

Combining Hamming Distance & Interleaving

Hamming distance and interleaving can be combined. M

We can first create n-bit packets that can correct t-bit errors.

Then we interleave m rows and send the bits column by column.

Possible to correct burst errors up to m × t bits of errors.

Compounding High & Low Resolution Packets

Creation of a duplicate of each packet with a low-resolution redundancy and combine the redundant version with the next

packet, For example, we can create four low-resolution packets out of five high-resolution packets and send them.

Chapter 11

Data Link Control (DLC) Services

The data link control (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast. M & Q

Data link control functions include framing, flow control and error control. M & Q

Framing

Data-Link layer needs to pack bits into frames, so that each frame is different from another.

Our postal system practices a type of framing. M

Framing separates a message by adding a sender address and a destination address. M

Frame Size

Why not one BIG Frame?

Frames can be of: M & Q

- ✓ Fixed Size

✓ Variable Size

How to define Beginning and End of a Frame?

Connection Oriented Framing

Data to be carried are 8-bit characters

Byte Stuffing in Connection-Oriented Framing

Connection-oriented Framing used text characters as flags. M

Nowadays any character used for flag can also be a part of the data. M

In order to avoid confusing the receiver, we use Byte Stuffing. M & Q

Bit-Oriented Framing

Data section of frame is a sequence of bits. M

We need a delimiter to separate one frame from the other. M

A special 8-bit pattern (01111110) to define beginning and end of a frame, M

Bit-Oriented Framing has the same issue as Connection-oriented Framing. M

Flow and Error Control

One of the responsibilities of the data-link control sub layer is flow and error control at the data-link layer. Q & M

Flow Control

Balance between production and consumption rates. M

If frames are produced faster than they are consumed at the receiving data link layer, the frames will be discarded. M

Use of buffers; one at sending end and other at receiving end,

Q & M

Example

Consumers need to communicate with the producers on two occasions:

- ✓ When the buffer is full; &
- ✓ When there are vacancies

If the two parties use a buffer with only one slot, the communication can be easier.

Error Control

Error Control at Data Link layer uses CRC in one of the two ways: Q

- ✓ If a frame is corrupted, it is silently discarded and if it is good, it is delivered to network layer
- ✓ If frame is corrupted, it is silently discarded and if it is good, an acknowledgement is sent to sender

Connectionless and Connection-Oriented

A DLC protocol can be either connectionless or connection-oriented. M

Connectionless: No relationship between the frames M

Connection-Oriented: Frames are numbered and sent in order M

DATA-LINK LAYER PROTOCOLS

Traditionally four protocols have been defined for the data-link layer to deal with flow and error control:

- ✓ Simple Protocol
- ✓ Stop-and-Wait Protocol
- ✓ Go-Back-N Protocol
- ✓ Selective-Repeat Protocol

Finite State Machine (FSM)

A machine with a finite number of states, M

Machines stay in one of the states until an event occurs. M

Each event is associated with 2 reactions:

- ✓ List of actions to be performed
- ✓ Determining the next state

Simple Protocol

Simple protocol has neither flow nor error control.

Stop-and-Wait Protocol

Stop-and-Wait protocol uses both flow and error control. M

The sender sends one frame at a time and waits for a response before sending the next one.

To detect corrupted frames, we add a CRC code. M

Piggybacking

Both Simple and Stop-and-wait protocols are designed for unidirectional communication. Q & M

Data flows in one direction and ACK travels in the other. M

To make the system efficient, the data in one direction is piggybacked with the response in the other direction. Q & M

High-level Data Link Control (HDLC)

Bit -oriented protocol for communication over point-to-point and multipoint links.

It implements Stop-and-Wait protocol.

Most of the concepts defined in this protocol are the basis for other protocols such as PPP, Ethernet, or wireless LANs.

Configurations & Transfer Modes in HDLC

HDLC provides two common transfer modes that can be used in different configurations:

- ✓ Normal Response Mode (NRM) &
- ✓ Asynchronous Balanced Mode (ABM)

Framing

HDLC defines three types of frames: M

- ✓ information frames (I-frames)
- ✓ Supervisory frames (S-frames)
- ✓ Unnumbered frames (U-frames

Point-to-Point Protocol (PPP)

Most common protocol for point-to-point access, M

Millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. M & Q

To control and manage the transfer of data, there is a need for a PPP at the data-link layer. M & Q

Services provided by PPP

The designers of PPP have included several services to make it suitable for a point-to-point protocol, but have ignored some traditional services to make it simple.

Services Included	Services Not Included
Framing	Flow Control
Link Establishment and Data Exchange	Error Correction (PPP has CRC detection only)

Authentication	No Sequence Numbering
Multilink PPP Address configuration	Absence of sophisticated Addressing Mechanism
Network Address configuration	

Multiplexing in PPP

Three sets of protocols are:

- Link Control Protocol (LCP)
- Two Authentication Protocols (APs)
- Several Network Control Protocols (NCPs)

Chapter 12

Media Access Control (MAC) Sub-Layer Q

When nodes use a multipoint or broadcast link, we need a multiple-access protocol for direct access to the link.

There are many protocols created for this access all of these protocols belong to Media Access Control (MAC) sub-layer.

Random Access

In random-access no station is superior to the other. M

ALOHA Q

ALOHA, the earliest random access method was developed in early 1970s. M

Designed for a radio (wireless) LAN, but it can be used on any shared medium.

Carrier Sense Multiple Access (CSMA) Q

To minimize the chance of collision and, therefore, increase the performance, CSMA was developed.

Carrier Sense Multiple Access/Collision Detection

CSMA method does not specify the procedure following a collision. M

CSMA/CD boosts the algorithm to handle the collision. M

Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA was invented for Wireless Networks. M

Collisions are avoided through the use of three strategies: Q&M

- ✓ The Interfame Space
- ✓ The Contention Window
- ✓ Acknowledgements

Interfame Space (IFS): Collisions are avoided by submitting transmission even if the channel is lazy.

Contention Window: Amount of time divided into slots.

Acknowledgement: Positive acknowledgement can help guarantee that the receiver has received the frame. M

CONTROLLED ACCESS Q

The stations consult one another to find which station has the right to send. A station cannot send unless authorized by other stations.

We discuss three controlled-access methods: Q&M

- ✓ Reservation
- ✓ Polling
- ✓ Token Passing

Polling Q

Polling works with topologies in which one device is design as a primary station and the other devices are secondary stations.

All data exchanges, the primary device controls the link; the secondary devices follow its instructions.

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring.

CHANNELIZATION (Channel Partition) Q&M

The available bandwidth of a link is shared in time, frequency, or through code, among different stations,

We discuss three protocols:

- ✓ Frequency Division Multiple Access (FDMA)
- ✓ Time Division multiple Access (TDMA)
- ✓ Code Division Multiple Access (CDMA)

Frequency-Division Multiple Access (FDMA)

In FDMA, the available bandwidth is divided into frequency bands. M

Time Division multiple Access (TDMA)

Stations share the bandwidth of the channel in time. M

Code Division Multiple Access (CDMA)

CDMA differs from FDMA in which only one channel occupies the entire bandwidth of the link.

CDMA differs from TDMA in which all stations can send data simultaneously; there is no timesharing. M

CHAPTER 13

Ethernet Protocol Q

Data-link layer and the physical layer is the zone of local and wide area networks. We can have wired or wireless networks.

IEEE Project 802

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable inter-communication. M

Project 802 did not seek to replace any part of the OSI model or TCP/IP protocol suite.

Project 802 is a way of specifying functions of the physical layer and the data-link layer. M

Ethernet Evolution Q

The Ethernet LAN was developed in the 1970s. M

Since then, it has gone through four generations: Q&M

- ✓ Standard Ethernet (10 Mbps)
- ✓ Fast Ethernet (100 Mbps)
- ✓ Gigabit Ethernet (1 Gbps)

✓ 10 Gigabit Ethernet (10 Gbps)

Standard Ethernet Q

The original Ethernet technology with the data rate of 10 Mbps is called Standard Ethernet. M

Connectionless & Unreliable Service Q

Ethernet is unreliable like IP and UDP M

Each frame is independent of other

No connection establishment or tear down process

If frame drops, sender will not know about it unless we are using TCP (Transport)

If a frame is corrupted, receiver silently drops it

The original Ethernet technology with the data rate of 10 Mbps is called Standard Ethernet.

Addressing in Standard Ethernet Q

Each station on Ethernet has its own network interface card (NIC).

The NIC fits inside the station and provides the station with a link-layer/physical address.

The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes M

For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

Transmission of Address Bits

How the address 47:20:1B:2E:08: EE is sent out online. Q

The address is sent left to right, byte by byte; it is sent right to left, bit by bit,

Access Method in Standard Ethernet Q

Since the network that uses the standard Ethernet protocol is a broadcast network, we need to use an access method to control access to the sharing medium. The standard Ethernet chose CSMA/CD with 1-Persistent Method.

Efficiency of Standard Ethernet Q

The practical efficiency of standard Ethernet has been measured to be:

$$\text{Efficiency} = 1/ (1+ 6.4 \times a)$$

Where a = number of frames that can fit on a medium

Implementation of Standard Ethernet Q&M

The Standard Ethernet defined several implementations, but only four of them became popular during the 1980s M

Changes in the Standard

Development of the Ethernet to become compatible with other high-data-rate LANs

- ✓ Bridged Ethernet
- ✓ Switched Ethernet
- ✓ Full-Duplex Ethernet

Fast Ethernet Q&M

In the 1990s, Ethernet increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet.

To make it compatible with the Standard Ethernet, the MAC sub layer was left unchanged.

Goals of Fast Ethernet: Q

- Upgrade data rate to 100Mbps
- Make it compatible with Standard Ethernet
- Keep same 48-bit address
- Keep same frame format

To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer. M

Gigabit Ethernet Q&M

Need for higher data rate IEEE Standard design Gigabit Ethernet Protocol (1000 Mbps).

The goals of the Gigabit Ethernet were: Q

- Upgrade the data rate to 1 Gbps
- Make it compatible with standard or Fast Ethernet
- Use same 48 bit address
- Use the same frame format

MAC Sub-layer Q&M

A main thought in the evolution of Ethernet was to keep the MAC sub layer untouched. To achieve a data rate of 1 Gbps, this was no longer possible.

Gigabit Ethernet has two unique approaches for medium access: Q

- ✓ Half-duplex
- ✓ Full-duplex

The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet

10-gigabit Ethernet Q&M

The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used in LANs and MANs (metropolitan area network)

The IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae M

Implementation Q

10 Gigabit Ethernet operates only in full-duplex mode; CSMA/CD is not used in 10 Gigabit Ethernet

CHAPTER 14 (Part 1)

Other Wired Networks

Access Networks M

- ✓ Networks that connect a small LAN to an ISP

Wide Area Networks M

- ✓ Wired networks used to transfer data over long distances

Telephone Network

The telephone network had its beginnings in the late 1800s M

Plain Old Telephone System (POTS) was originally an analog system using analog signals to transmit voice M

Major Components

The telephone network is made of three major components: Q&M

- ✓ Local Loops
- ✓ Trunks
- ✓ Switching offices

The telephone network has several levels of switching offices: Q

- ✓ End offices
- ✓ Cycle offices
- ✓ Local offices

Local-Access Transport Areas (LATAs) Q

A LATA can be a small or large metropolitan area. M

A small state may have a single LATA; a large state may have several LATAs.

Intra-LATA and Inter-LATA Services Q

Services offered by Telephone companies inside a LATA are called Intra-LATA services and between LATAs are called Inter-LATA services.

Carrier that handles Intra-LATA are called a Local Exchange Carrier (LEC) and the ones that handle Inter-LATA are called Interexchange Carriers (IXCs). M

Signaling Q

The telephone network in the beginning used a circuit-switched network with dedicated links to transfer voice communication. M

The operator connected the two parties by using a wire with two plugs inserted into the corresponding two jacks.

Later, the signaling system became automatic.

Services

Telephone companies provide two types of services: Q&M

- ✓ Analog Services
  - ➢ Analog Switched Services
  - ➢ Analog Leased Services
- ✓ Digital Services
  - ➢ Switched /56 Service
  - ➢ Digital Data Service

Digital Subscriber Line (DSL) Q

Telephone companies developed another technology, DSL, to provide higher-speed access to the Internet. DSL supports high-speed digital communication over the existing telephone

DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL)

Cable Network

The Cable TV networks were initially created to provide remote subscribers access to TV programs. M

Cable networks enabled access to remote broadcasting stations via microwave connections M

Traditional Cable Networks Q

It was called community antenna television (CATV) because an antenna at the top of a tall hill or building received the signals from the TV stations.

Hybrid Fiber Coaxial (HFC) Network Q

Second generation of cable network is called a Hybrid Fiber-Coaxial (HFC) network. M

The network uses a combination of fiber-optic and coaxial cable. M

Cable TV for Data Transfer Q

DSL technology provides high-data-rate connections for residential subscribers over the local loop but UTP is subject to Interface. A solution is the use of the cable TV network.

CHAPTER 14 (Part 2)

Synchronous Optical Network (SONET) Q

A wide area network (WAN) that is used as a transport network to carry loads from other WANs,

ITU–T standard called Synchronous Digital Hierarchy (SDH) M

Architecture of a SONET system consists of signals, devices, and connections. Q&M

SONET Architecture Q

Signals

- ✓ Synchronous Transport Signals (STS)
- ✓ Optical Carriers (OCs)
- ✓ Synchronous Transport Module (STM)

Devices

- ✓ STS Mux/De mux
- ✓ Regenerators
- ✓ Add-Drop Multiplexer and Terminals

Connections

- ✓ Section
- ✓ Line
- ✓ Path

SONET Layers

The SONET standard includes four functional layers: Q&M

- ✓ The Path Layer
- ✓ The Line Layer
- ✓ The Section Layer
- ✓ The Photonic Layer

The layers correspond to both the physical and the data-link layers.

SONET Frames

Each synchronous transport signal STS-n is composed of 8000 frame. M

STS-1 frame is 9 rows by 90 columns (810 bytes), and an STS-3 is 9 rows by 270 columns (2430 bytes) M

STS Multiplexing

In SONET, frames of lower rate can be synchronously time-division multiplexed into a higher-rate frame.

For example, three STS-1 signals (channels) can be combined into one STS-3 signal (channel),

SONET Networks Q

SONET network can be used as a high-speed backbone carrying loads from other networks such as ATM or IP.

We can roughly divide SONET networks into three categories: Q&M

- ✓ Linear Networks
- ✓ Ring Networks
- ✓ Mesh networks

ATM Q&M

Asynchronous Transfer Mode (ATM) is a wide area network. M

The combination of ATM and SONET will allow high-speed interconnection of networks. M

Problems

Some of the problems associated with existing systems are:

- ✓ Frame Networks
- ✓ Mixed Network Traffic

Solution

- ✓ Cell Networks
- ✓ Asynchronous TDM

Architecture Q

ATM is a cell-switched network M

The switches are connected through network-to-network interfaces (NNIs).

CHAPTER 15

Introduction

Wireless communication is one of the fastest-growing technologies M

The demand for connecting devices without the use of cables is increasing everywhere.

Wireless LANs can be found on college campuses, in office buildings, and in many public areas. Q

Architectural Comparison Q

Architecture comparison of wired and wireless LANs

- ✓ Medium
- ✓ Hosts
- ✓ Remote LANs

- ✓ Connection to other Networks
- ✓ Moving between Environments

Characteristics of a Wireless LAN Q

Several characteristics of wireless LANs either do not apply to wire LANs.

- ✓ Interference
- ✓ Multipath Broadcast
- ✓ Error

Access Control

CSMA/CD does not work in wireless LANs for three reasons: Q

1. Wireless hosts don't have power to send and receive at the same time
2. The hidden station problem stops crash detection
3. The distance between stations can be large

IEEE 802.11 PROJECTS Q&M

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers M

IEEE 802.11is sometimes called Wireless Ethernet. M

Architecture Q

The standard defines two kinds of services:

- ✓ The basic service set (BSS); and
- ✓ The Extended service set (ESS)

Types of Stations

No-Transition Mobility

BSS-Transition Mobility

ESS-Transition Mobility

MAC Sub-layer

IEEE 802.11 defines two MAC sub-layers: Q

- ✓ The Distributed Coordination Function (DCF) ; and
- ✓ The Point Coordination Function (PCF

Frame Types Q

- Management Frames
- Control Frames
- Data Frames

Values of Subfields in Control Frames M

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

BLUETOOTH Q

Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other.

A Bluetooth LAN is an ad hoc network. M

The devices, sometimes called gadgets, find each other and make a network called a Pico net. **Q&M**

Architecture

Bluetooth defines two types of networks: Q

- ✓ Pico net
- ✓ Scatter net

Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter M

The current data rate is 1 Mbps with a 2.4-GHz bandwidth M

CHAPTER 16

Connecting Devices

Hosts and networks do not normally operate in isolation. M

Connecting devices connect hosts together to make a network or connect networks together to make an internet. M

Three kinds of connecting devices: **Q&M**

- Hubs
- Link-layer switches
- Routers

Hubs Q&M

Hub is a device that operates only in the physical layer. M

A hub (repeater) receives a signal and, before it becomes too weak or corrupted, regenerates it.

Link-Layer Switches Q&M

A link-layer switch (or switch) operates in both the physical and the data-link layers. M

As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

Switch versus Hub Q

Switch has the 'Filtering' capability. M

Unlike hub, a switch can check the destination address of a frame.

Switches connect mixed devices.

Loop Problem in a Switch Q

Switches create Loops in the system.

Spanning Tree Algorithm Q&M

In graph theory, Spanning Tree is a graph in which there is no loop.

Routers Q&M

A router is a three-layer device two switch and a hub; it operates in the physical, data-link, and network layers.

Router vs. Switch Q

Three differences between a router and a switch:

1. A router has a physical and logical (IP) address.
2. A router acts only on those packets in which the link-layer address matches the address of the interface at which the packet arrives.
3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.

VIRTUAL LANS (VLAN) Q&M

A VLAN is a LAN organized by software, not by physical wiring.

Provides a virtual connection between two stations belonging to two different physical LANs,

Membership of a VLAN

What characteristic can be used to group stations in a VLAN? Q

Dealers use different characteristics such as interface numbers, port numbers, MAC addresses, IP addresses, IP multicast addresses,

Configuration of a VLAN

How are the stations grouped into different VLANs? Q

Stations are configured in one of three ways:

- ✓ Manually
- ✓ Semi-Automatically
- ✓ Automatically

Communication between Switches

In a multi-switched backbone, each switch must know:

- ✓ Which station belongs to which VLAN;
- ✓ The membership of stations connected to other switches

Advantages of using VLANs Q

- Cost and Time Reduction
- Creating virtual Workgroups
- Security

Fiber to the Curb (FTTC) Q

An access network in which fiber is used for part, but not the entire link from the provider to the end-user,

The terminal network part of a FTTC network is usually twisted pair or coaxial cable.

Fiber to the Home (FTTH) Q

Need: High-speed data, reliable voice and high-quality video

Problems:

How to get high speed lines out to each customer?

How to future-proof the architecture?

Solution: FTTH

Fiber-to-the-home (FTTH) is the installation of optical fiber from a telephone switch into the subscriber's home. M

It is one of the latest access technologies. M

FTTH is also referred to as Fiber-to-the-Building (FTTB) M