Computer Communications Networks Course

PART 1
Overview and Introduction

PART 2
Communication Reference Models

PART 3
Emerging Network Technologies

PART 4
The Internet (TCP/IP) Protocol Suite

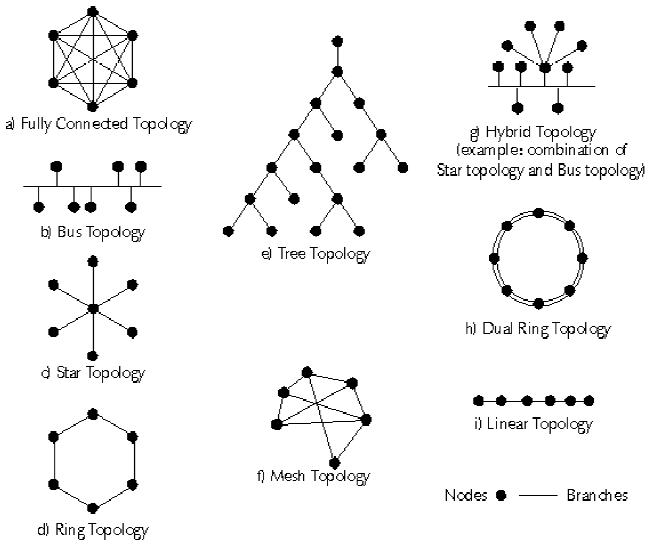
PART 5
Advanced Topics in Computer Communications Networks

Introduction

- In the real world, data/computer networks are implemented by following a predefined physical and logical layout.
- The physical layout (topology) of a network refers to how communication media, such as cables, computers, and other peripherals are physically connected and arranged.
- Logical topology is the method used to pass the information between workstations.

Network Topologies

Common network physical topologies may be summarized as shown in the Figure.



BUS Topology

- The bus topology is very common for local area networks.
- Network stations are attached to a transmission medium, called a bus.
- When a station transmits a frame on the bus all other stations attached to the bus receive the frame.
- Frames are said to be broadcast on the medium.
- A popular protocol used with this LAN topology is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.
- There is no controlling station on a broadcast bus topology LAN. Control functions are distributed to all LAN stations.
- Each station must also be capable of detecting faults.

STAR Topology

- In a network that has a star topology, each station is connected to a central controlling device (also called a hub/switch) via point-to-point lines. The central device acts as a high speed signal copier/multiplexer between connections.
- The structure of a star network is very simple and has many advantages over the single cable-bus topology such as .
- To overcome the disadvantage of having a single point of failure, the central switch must use very reliable components and usually provides some form of redundancy.

Mesh and Tree Topologies

- **Mesh Topology:** This topology involves some wiring overhead since every network station is directly connected to all the other stations.
- It also means that each station has to have (N-1) I/O ports, where N is the number of stations in the network.
- However, a mesh network topology has excellent fault tolerance, since, when a link fails, message traffic can be routed through an intermediate node.
- **Tree topology:** is a variation of the bus topology. A CSMA/CD protocol can be applied to both topologies, and in both cases transmitted frames are broadcast to all stations active on the shared medium. As with the bus topology, there is no controlling station on the LAN.

Ring Topologies

- In a network that has a ring topology, each station is attached to its adjacent station by point-to-point links thus forming a physical ring. Each station's adapter regenerates the signal as it retransmits a data packet that is circulating on the ring.
- A popular protocol used with ring topology is token passing, in which access to the medium is controlled by possession of a circulating token.
- Different token passing access protocols are defined for ring topology LANs.
- The major disadvantage of a physical ring topology is its sensitivity to single link failure. If one connection between two stations fails the ring traffic is down.

Communication Media and Network Access

- In a network, information (data) traverses a communications medium (typically a wire) as electrical signals that originate and terminate in computing devices like computers and printers.
- Three basic elements of a network:
  - **The communication medium**: (typically a cable, but radio frequency and infrared transmissions can also serve as a data communications medium);
  - **The data (information)**: its data (which flows in its most elementary binary form -essentially zeros and ones);
  - **The Access Points**: which contact between network wires and the computing devices to which they are connected. These latter are called network interface cards (**NICs**).

Examples of Communication Media (1)

- Network cables are typically coaxial, twisted-pair, or fiber optic. Some are shielded while others are not. These different types of cable vary in cost and transmission capacity, and each typically serves a specific network role.
- Fiber optic cable has the added advantage of being non-conductive, which is advantageous for external cables.
- Coaxial cables is rapidly losing favor on modern networks because it is difficult to work with and integrates poorly with switched networks.

Examples of Communication Media (2)

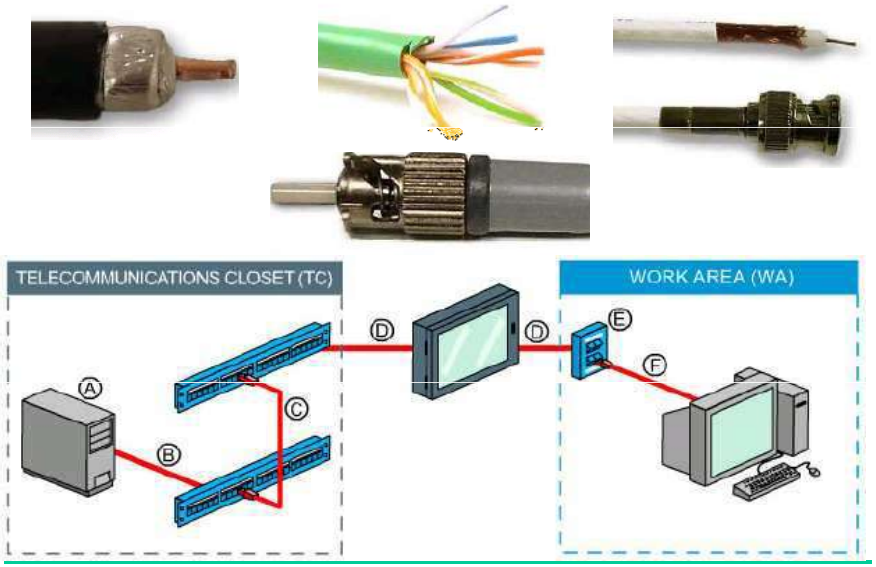
- In summary, we have
  - **Coax:** Two conductors share the same axis. Commonly used for thick Ethernet, thin Ethernet, cable TV and ARCnet, coaxial cabling that uses BNC connectors; heavy shielding protects data, but expensive and hard to make connectors. Bandwidth is between 2.5 Mbps and 10 Mbps.
  - **UTP**: Unshielded Twisted Pair uses RJ-45, RJ-11, RS-232, and RS-449 connectors. Max length is 100 meters, speed is up to 100Mps. Cheap, easy to install, length becomes a problem. It is most sensitive to electromagnetic interference. Can be CAT 2,3,4,5 or 6 quality grades.

Examples of Communication Media (3)

- **STP**: Shielded Twisted Pair. One or more twisted pairs of wire in foil or wire woven-copper shielding. Uses RJ-45, RJ-11, RS-232, and RS-449 connectors, max length is 100 meters, speed is up to 500Mps. Not as inexpensive as UTP, easy to install.

- **Fiber Optic**: (IEEE 802.8) Cable in which the center core, a glass cladding composed of varying layers of reflective glass, refracts light back into the core. Max length is 25 kilometers, speed is up to 2Gbps but very expensive. Best used for a backbone due to cost.

Examples of Communication Media (4)



Overview of Network Devices (1)

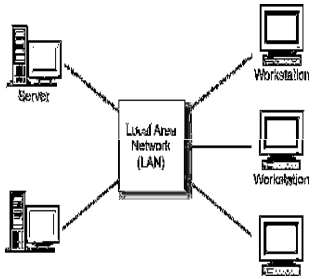
- LANs are the basic building blocks of a computer network.
- Large-scale networks join LANs together with cables (or other communications medium).
- Linking stations and LANs together introduces complexity, particularly if the network has a great many stations and LANs, or if they are separated geographically.
- Without network devices, large-scale networks would be impossible to build.

Overview of Network Devices (2)

- The technology of central connection points, such as hubs, bridges, routers, and switches allow networks to be segmented, and they also add "address-intelligence" at the level of the physical wire.
- They solve the problem of line-length constraints by acting as repeaters.
- The main used network devices are:
  - **Hub:** it is the point of central connection for all of the LAN's shared devices. a hub serves the same function as the shared cable in the bus model -it connects devices on the LAN.

Overview of Network Devices (3)

- On a hubbed LAN, devices exchange data by first sending it to the hub. The hub, in turn, repeats the "message" back out to all of its connected devices.



- As with the bus LAN, only the device to which the message is addressed will copy the message, while the others ignore it.
- When a LAN reaches its maximum effective size, it is necessary to install another LAN and then connect the two.

Overview of Network Devices (4)

- **Router:** is a device that, like a hub, has ports through which data passes.
  - With a router, data passes only from one LAN to another.
  - Unlike hubs, routers do not blindly repeat the data they receive. Instead, routers are "intelligent" devices.
  - As data packets flow into a router, it inspects the packet's header (which contains the packet's destination address) and based on this information it makes a routing decision.
  - Because routers understand communications protocols (like IP, which governs Internet addressing), routers can make configurable routing decisions.
  - Routers are typically more expensive than other inter-network connection devices, and they are also more complicated to set up.

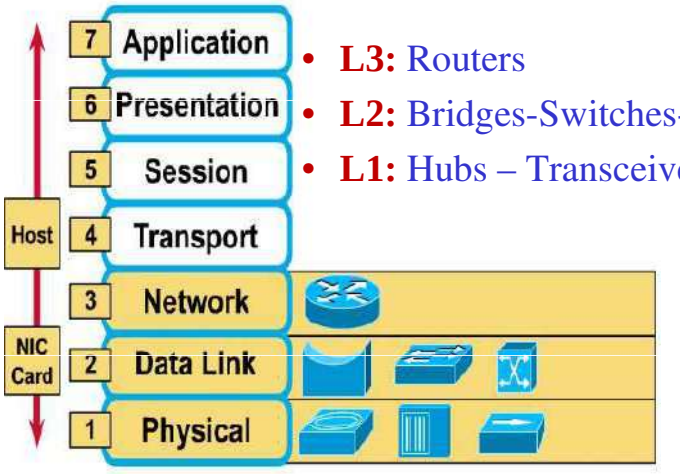
Overview of Network Devices (5)

- **Bridge:**
  - Bridges are simpler and less expensive than routers, but offer similar inter-network capability.
  - Typically, bridges have ports connected to two or more separate LAN segments.
  - Rather than complicated routing decisions, bridges make straightforward yes/no decisions about forwarding the data packets they receive.
  - Bridges base their decisions on the packet's destination address (H/W), which it compares to a stored table of known network addresses.
  - Although, bridges are not sophisticated as routers, they do possess some filtering capabilities.

Overview of Network Devices (6)

- **Switches:** are the most recent and most sophisticated of inter-networking devices.
  - Like routers and bridges, switches also link LANs.
  - Their strength comes in their ability to link many LANs.
  - They are like multi-port bridges, so they can manage complex switching among multiple LANs. This makes them useful tools for segmenting network traffic.
  - Switches provide the same kind of address-intelligence (filtering and forwarding) that routers provide.
  - But rather than working with the IP address, as routers do, a switch uses H/W address that works at a low level, where the network devices interface with the medium.

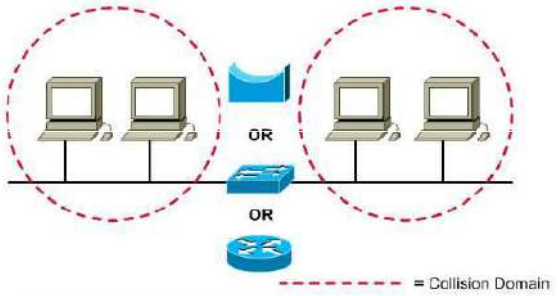
Network devices Function at Layers



- **L3:** Routers
- **L2:** Bridges-Switches- Concentrators
- **L1:** Hubs – Transceivers - Repeaters

Limiting Collisions in LANs

- **Reducing traffic in networks makes it more efficient**
- **This can be done using Bridges, Switches and/or Routers.**
- **Each shared link is called collision domain.**
- **We can improve the performance of a Large network by dividing it into multiple collision domains (subnets).**



Overview of Public Network Technologies (1)

- Data needs an engine to drive it. Different technologies handle the task of moving the data over the communication media and regulating the characteristics of the signals that carry it.
- The most common of these is Ethernet/Fast Ethernet, in place in a reported 80% of LANs.
- Other technologies include Token Ring, FDDI (fiber distributed data interface), LocalTalk (for Apple Macintoshes), Asynchronous Transfer Mode (ATM) and some others.
- Each of these standards governs several key features of how data moves around a network.

Overview of Public Network Technologies (2)

- Two important key features of a network technology:
  - the physical characteristics of the signals
  - the manner in which the data is packaged.
- Other issues involve:
  - the speed at which data can flow
  - the physical length of wire it can support
  - the network's topology (that is, the physical layout of the network, as in a star, ring, or straight-line bus).
- Finally, there is the very important issue of how it deals with the shared access to the network communication medium to avoid data "collisions."

Overview of Public Network Technologies (3)

- Typically, Ethernet is the most widely popular technology for local area networks (LANs). It provides transmission speed at 10Mbps (Ethernet), 100Mbps (Fast Ethernet), 1000Gbps (Gigabit Ethernet), and 10Gbps (10 Gigabit Ethernet).
- By introducing ATM network technology, high-level classes of services as well as higher bandwidths are offered to the network users. However, ATM is expensive as a complete integrated solution.

Overview of Public Network Technologies (4)

- Fiber Distributed Data Interface (FDDI) is a token-passing technology, operating at 100 Mbps. But since it requires different wiring (fiber), FDDI is losing ground to Fast Ethernet and other high-speed technologies.
- In next, the basics of Ethernet network technology, as an example of the connectionless-oriented networks, and ATM network technology –as an example of the connection-oriented networks are discussed.

Ethernet Network Technology (1)

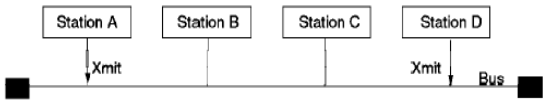
- Ethernet (IEEE 802.3) is currently the most widely used LAN protocol in the world.
- It is introduced to the marketplace in the 1970's it.
- A consortium of DEC, Intel and Xerox brought out a new version of Ethernet in 1980 called Ethernet (DIX) V2.
- Institute of Electrical and Electronics Engineers (IEEE) confirms the Ethernet DIX V2 standards with some slight modifications as IEEE 802.3. Today both Ethernet and 802.3 LANs are widely implemented across all areas of the marketplace.

Ethernet Network Technology (2)

- While Ethernet and 802.3 are not identical, the term Ethernet is widely used to describe LANs that use either protocol.
- Both Ethernet V2 and 802.3 can be used on the same physical Ethernet simultaneously. However, stations using one type cannot interoperate with stations using the other frame type unless they have both frame types configured.
- In practice, applications tend to use Ethernet V2 frame types while management programs tend to use 802.3 frame types.

Ethernet Operation Concepts (1)

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is the name of the protocol used on the Ethernet bus to control the operation of the network.
- The operation of CSMA/CD bus is summarized as the following:
  - when a station wants to transmit data on the network bus, it first listens to see if the bus is free (that is, no other station is transmitting).



Ethernet Operation Concepts (2)

- If the bus is available, the station starts transmitting data immediately. If the bus is not available (that is, another station is transmitting), the station waits until the activity on the bus stops and a predetermined period of inactivity follows before it starts transmitting.
- If there is a collision after transmission (that is another station starts to transmit at the same time), the stations will stop transmitting data immediately after the collision is detected, but they continue to transmit a jamming signal to inform all active stations about the collision.

Ethernet Operation Concepts (3)

* In response to this signal, each transmitting station stops transmitting and uses a binary exponential backoff algorithm to wait before attempting to transmit again.
* This causes each station to wait for a random amount time of before starting the whole process again beginning with the process of carrier sensing.
* If a station's subsequent attempt results in another collision, its wait time will be doubled.
* This process may be repeated up to 16 times, after which the station, if still unsuccessful, reports a transmission error to the higher layer protocols.

Ethernet Operation Concepts (4)

- The probability of a collision occurring is proportional to
  * the number of stations
  * the frequency of transmissions
  * size of frames
  * length of the LAN.
- According to Ethernet and the 802.3 standards, to be able to detect collisions, a transmitting station should monitor the network for a period of time called a slot time.

Ethernet Operation Concepts (4)

- Slot time is the time during which a collision may occur and is the maximum delay for a transmission to reach the far end of the network and for a collision to propagate back.
- Slot time is defined to be 51.2 microseconds (512 bit times in a 10 Mbps LAN).
- This time imposes a maximum length on the size of the network.
- It also imposes a minimum (64 bytes, excluding preamble and SYN) on the size of the frames transmitted by each station.

Ethernet and IEEE 802.3 Frame Formats (1)

- The frame formats of Ethernet and IEEE 802.3 are not the same. However, both protocols use the same medium and access method.
- LAN stations running these protocols could share a common bus, but they could not communicate with each other.

Ethernet frame format

PREAMBLE	SYNC	DA	SA	TYPE	DATA	FCS
1010....1010	11					
62 Bits	2 Bits	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

IEEE 802.3 frame format

PREAMBLE	SFD	DA	SA	LENGTH	DATA	FCS
1010....1010	10101011					
56 Bits	8 Bits	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

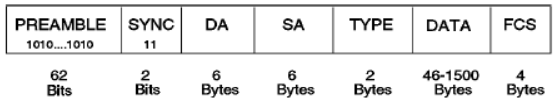
Ethernet Frame Format (1)

Ethernet frame format

- **PREAMBLE:** 62 bits, allows the Physical Layer Signaling (PLS) circuitry to synchronize with the receive frame timing circuitry.
- **SYNC (Synchronize):** 2 bits, indicates that the data portion of the frame will follow.
- **DA (Destination Address) and SA (Source Address):** 48 bits, Media Access Control (MAC) address. Three types of destination addressing are supported:
  - **Individual (unicast):** unique address of one node on the network.
  - **Multicast:** first bit of the DA is set ➔ a group address is being used.
  - **Broadcast:** if the DA field is set to all 1's, it indicates a broadcast. All nodes on the network must be capable of receiving a broadcast.

Ethernet Frame Format (2)

Ethernet frame format



- **TYPE (Type Field):** 16 bits, this field identifies the higher layer protocol, which is used. Each registered protocol is given a unique 2-byte type identifier. The value assigned to the type field in Ethernet is always higher than the maximum value in the length field for the IEEE 802.3. This is to ensure that both protocols can coexist on the same net.
- **DATA (Data field):** This contains the actual data being transmitted and is 46-1500 bytes in length. Ethernet assumes that the upper layers will ensure that the minimum data field size (46 bytes) is met prior to passing the data to the MAC layer. The existence of any padding character is unknown to the MAC layer.
- **FCS**: 32 bits, the result of a cyclic redundancy check algorithm. The receiving station uses the same algorithm to ensure that transmission was error free.

IEEE 802.3 Frame Format (1)

IEEE 802.3 frame format

- **PREAMBLE:** 56 bits, allows the Physical Layer Signaling (PLS) circuitry to synchronize with the receive frame timing circuitry.
- **SFD** (Start Frame Delimiter): 8 bits, indicates that the data portion of the frame will follow.
- **DA** (Destination Address), **SA** (Source Address): 48 bits, Media Access Control (MAC) address: As in Ethernet frame format.
- **LF** (Length Field) - 16 bits, indicates the number of data bytes (excluding the PAD) that are in the data field.
- **DATA (+ PAD)** field - IEEE 802.3 specify a minimum packet size (header plus data) of 64 bytes. However, it permits the data field to be less than the 46 bytes required. The MAC layer may add pad characters to data field before sending the data over the network.

Ethernet and IEEE 802.3 Network Model (1)

- As Ethernet is a Data Link layer protocol, its network model allows a DTE to use the network to exchange information with the other DTEs attached to the same network.
- The model's main part is the Media Access Control (MAC) Sublayer that controls the routing of information between the physical layer and higher layers.
- The MAC sublayer is responsible for:
  - **Constructing Frames**: a frame containing the data passed to it from the upper layers. The transmitted frame will contain four bytes of FCS.
  - **Collision Detection and Recovery**: To transmit the frame, the status of the medium is sensed by the Physical Layer Signaling (PLS) sublayer and is passed to the MAC sublayer. If the medium is busy, the transmission will defer until the medium becomes idle and a period of time known as Inter Packet Gap expires. After this period, the MAC sublayer will start transmitting the frame. IGP is 9.6 microseconds and its purpose is to allow all the stations in the network to detect the idle carrier.

Ethernet and IEEE 802.3 Network Model (2)

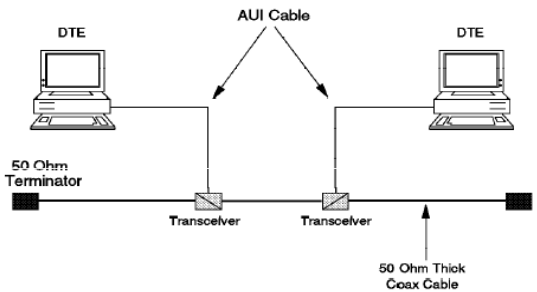
- **Frame Recognition and Copying**: When receiving a frame, the MAC sublayer identifies the Destination Address within the received frame and compares it with the address of the DTE (including Group and Broadcast addresses supported by that DTE). If a match is found, it will copy the frame, compute the FCS, and compare the result with the FCS contained in the received frame. If the frame is received error free, it will be passed to the higher layers; otherwise, a CRC Error will be reported.

Ethernet (802.3) Topologies (1)

- In an Ethernet (802.3) network, various types of cables can be used to provide the physical link between the DTEs. The media used can be:
  - thick or thin coax
  - twisted pair
  - fiber optic cable.

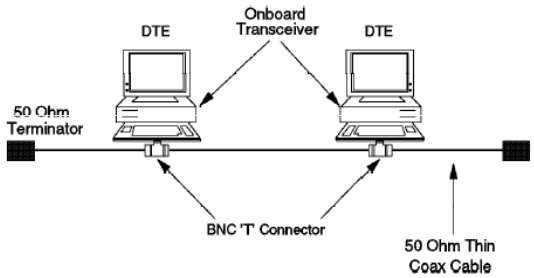
Ethernet (802.3) Topologies (2)

- **10Base5 (Thicknet)**
  - 10 indicates the data rate (10 Mbps)
  - Base indicates the transmission type (Baseband)
  - 5 indicates the maximum cable length (500 meters)



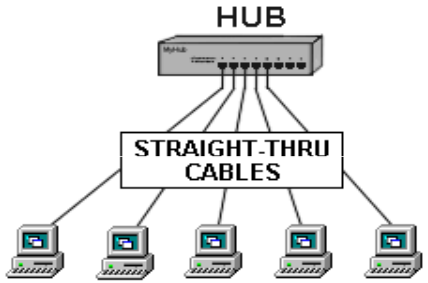
Ethernet (802.3) Topologies (3)

- **10Base2 (Thinnet/Cheapernet)**
  - 10 indicates the data rate (10 Mbps)
  - Base indicates the transmission type (Baseband)
  - 2 indicates the maximum cable length (200 meters: actual length permitted on a 10Base2 segment is 185 meters).



Ethernet (802.3) Topologies (4)

- **10Base-T**
  - 10 indicates the data rate (10 Mbps)
  - BASE indicates the transmission type (Baseband)
  - T indicates the medium (Twisted Pair)



Ethernet (802.3) Topologies (5)

- **FOIRL and 10Base-FL**
  - Fiber Optic Inter Repeater Link (FOIRL) was the first standard to be defined for the use of fiber optic cables in an Ethernet LAN.
  - Originally intended as a repeater-to-repeater link only, providing a long-distance connection of up to 1 km between two repeaters.
  - FOIRL is similar to the 10Base-T standard
  - It also requires the use of repeaters in a central hub acting as the concentration point for a group of nodes. 10Base-FL extends the allowable distance between two stations to 2 km.

Ethernet Design Rules (1)

- There are considerations for designing Ethernet networks used to ensure that data transmitted by the source will be received by the destination error free and any collisions that occur can be reliably detected. These Includes:
  - Maximum segment lengths for each medium type must not exceed the stated limits for that medium:
    - » 10Base5: 500 m
    - » 10Base-T: 100 m
    - · 10Base2: 185 m
    - · 10Base-FL: 2000 m
  - The maximum number of stations allowed on a segment varies according to the type of medium used:
    - » 10Base5: 100 stations
    - » 10Base-T: 2 stations
    - · 10Base2: 30 stations
    - · 10Base-FL: 2 stations

Ethernet Design Rules (2)

- The maximum number of stations in a collision domain is 1024.
- Repeaters can be attached at any position on the coax segments but should be at the ends of a link segment.
- Each repeater takes one attachment position on the segment and should be counted towards the maximum number of stations allowed on that medium.
- You can have many segments and repeaters within a single collision domain as long as no two DTEs in the same collision domain are separated by more than four repeaters.
- No two DTEs in the same collision domain can be separated by more than three coax segments.

Ethernet Design Rules (3)

* Link segments can be 10Base-T, FOIRL and 10Base-FL.
* 10Base2 and 10Base5 segments cannot be used as link segments.
* 10Base5 and 10Base2, 10Base-T and fiber segments can be mixed in a single collision domain allowing you to take advantage of the facilities offered by the most appropriate medium for different parts of your network.

Fast Ethernet and Gigabit Ethernet (1)

- Fast Ethernet (100BASE-T), which could transmit at 100Mb/s, has been introduced as a second generation of Ethernet.
- Fast Ethernet technology provides a smooth, non-disruptive evolution to 100 Mbps performance while using UTP cables cat 5 which may be used also by 10BaseT Ethernet.
- Gigabit Ethernet is an extension of the highly successful 10Mbps (10BASE-T) Ethernet and 100Mbps (100BASE-T) Fast Ethernet standards for network connectivity.
- Gigabit Ethernet is fully compatible with the huge installed base of Ethernet and Fast Ethernet nodes.

Fast Ethernet and Gigabit Ethernet (2)

- Gigabit Ethernet employs all of the original Ethernet specification such as frame format and support for CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol, full duplex, flow control, and management objects as defined by the IEEE 802.3 standard.
- The next generation version of Gigabit Ethernet is 10 Gigabit Ethernet. It supports a data rate of 10Gbps. It offers similar benefits of the Ethernet and Gigabit Ethernet standards (Ethernet address, Ethernet Frame Format) but it does not support the half-duplex operation mode.

Fast Ethernet and Gigabit Ethernet (3)

- 10 Gigabit Ethernet offers a low cost solution to solve the demands for bandwidth and offers straightforward scalability (10/100/1000/10000Mb/s).
- Upgrading to 10 gigabit Ethernet is simple since the upgrade paths are similar to those of gigabit Ethernet.
- Since it is a full-duplex only technology, it does not need the carrier-sensing, multiple-access with collision detection