

WIRED-LAN, WIRELESS-LAN & VIRTUAL LAN

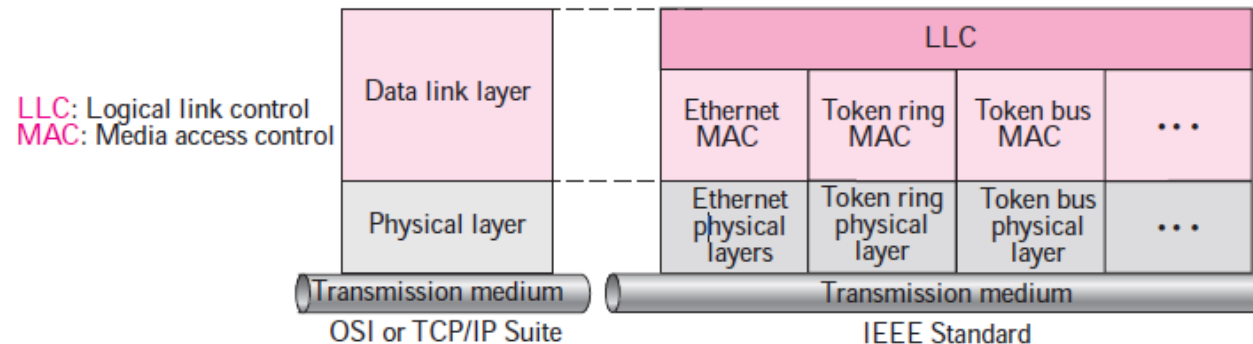
Note: This is chapter 3 (Underlying Technologies) from Text book 2
Behrouz_Forouzan

WIRED LOCAL AREA NETWORKS

- A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. 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.
- In this section, we first briefly discuss the IEEE Standard Project 802, designed to regulate the manufacturing and interconnectivity between different LANs. We then concentrate on the Ethernet LANs.

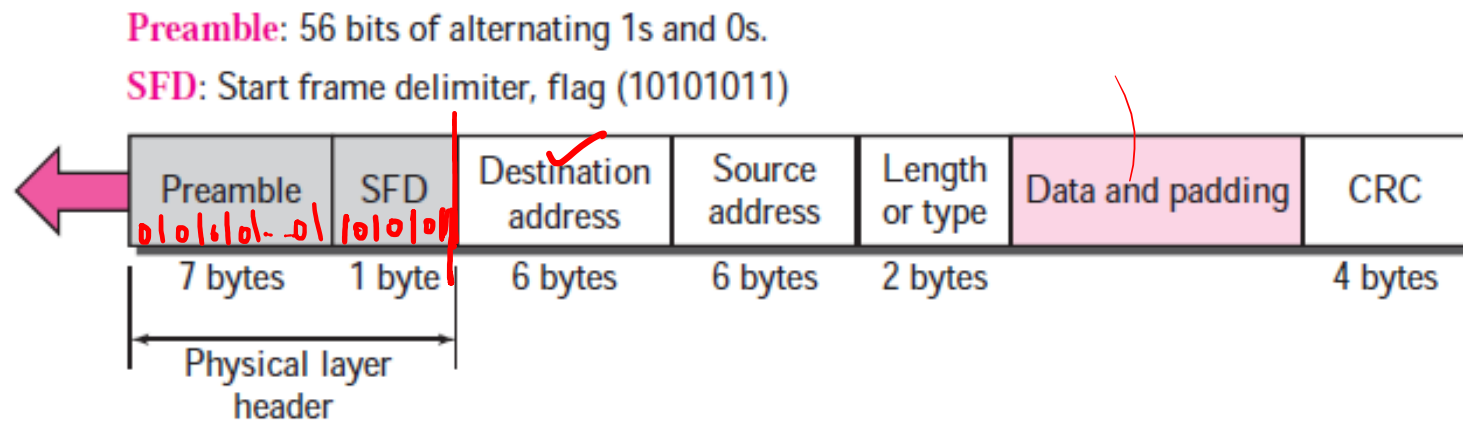
IEEE Standards

- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model.
- Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols. The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Standards Organization (ISO) also approved it as an international standard under the designation ISO 8802. IEEE 802.
- The relationship of the 802 Standard to the traditional OSI model is shown in Figure. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.



Frame Format

- The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of data unit, upper-layer data, and the CRC.
- Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.
- Acknowledgments must be implemented at the higher layers.

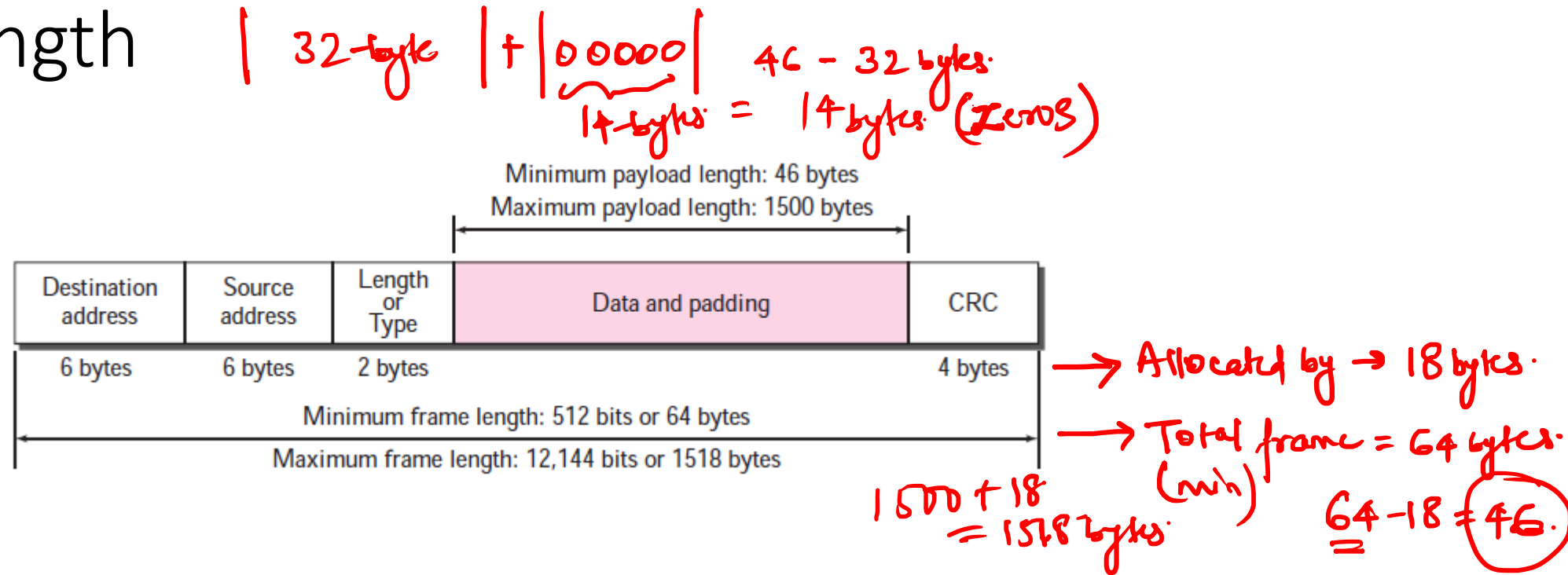


Frame Format

- ❑ **Preamble.** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- ❑ **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits are 11 and alert the receiver that the next field is the destination address. The SFD is also added at the physical layer.
- ❑ **Destination address (DA).** The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet. We will discuss addressing shortly.
- ❑ **Source address (SA).** The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- ❑ **Length or type.** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.
- ❑ **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes, as we will see later.
- ❑ **CRC.** The last field contains error detection information, in this case a CRC-32

(010101... (8-bits) - 0110101011)

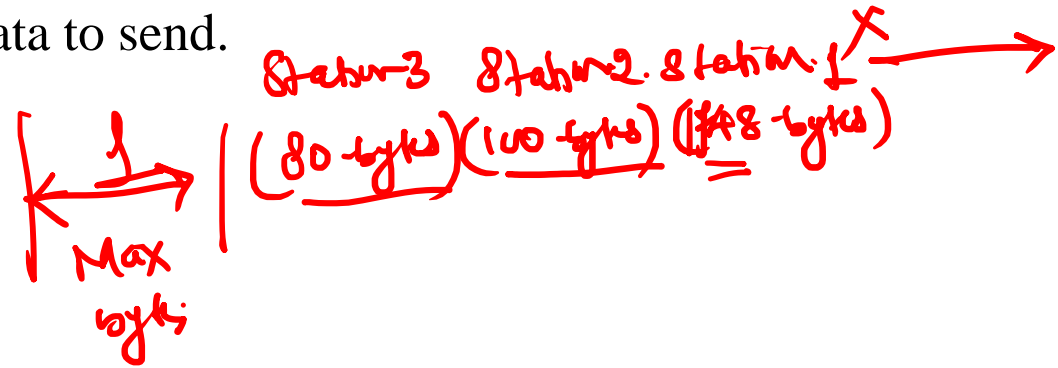
Frame Length



- The minimum length restriction is required for the correct operation of CSMA/CD, as we will see shortly. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer.
- If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of CRC), then the minimum length of data from the upper layer is $64 - 18 = 46$ bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

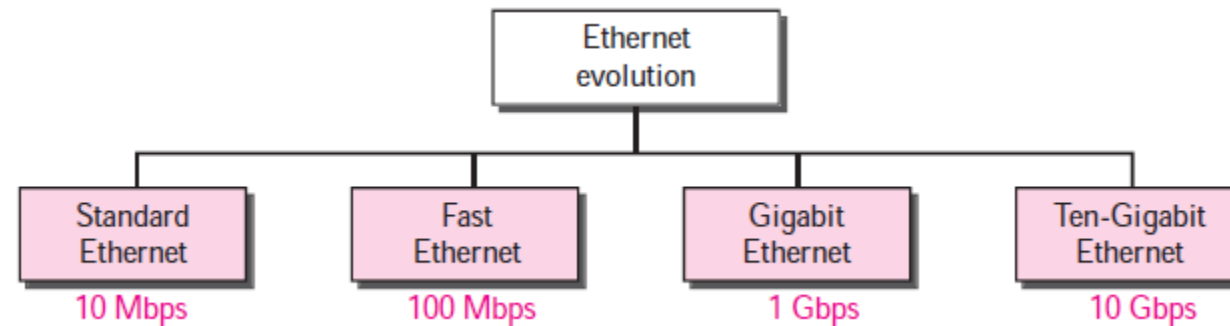
Frame Length

- The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.
- The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.



Ethernet Evolution

Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: **Standard Ethernet** (10 Mbps), **Fast Ethernet** (100 Mbps), **Gigabit Ethernet** (1 Gbps), and **Ten-Gigabit Ethernet** (10 Gbps), as shown in Figure 3.6. We briefly discuss all these generations starting with the first, Standard (or traditional) Ethernet.



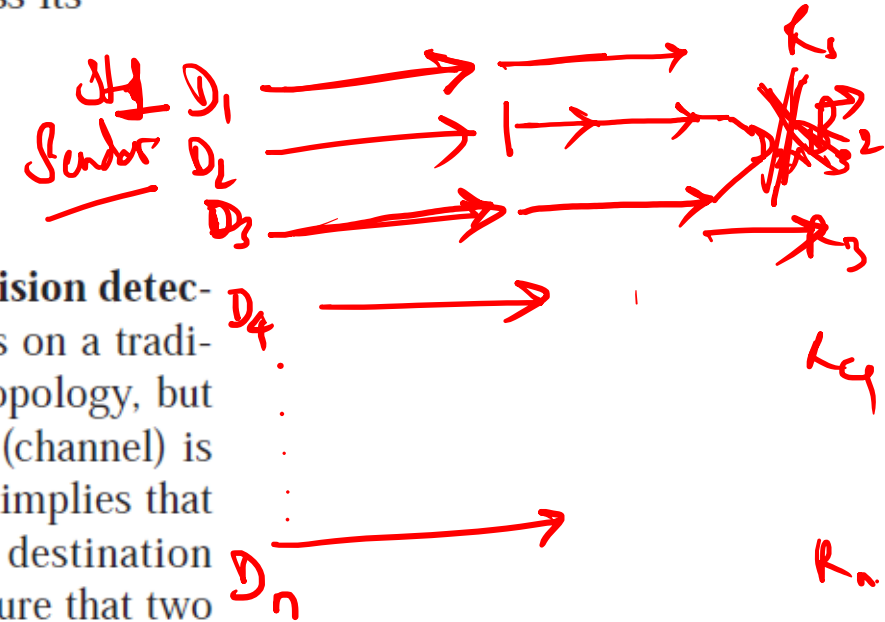
Ethernet Evolution

Standard Ethernet

The original Ethernet with 10-Mbps data rate is now history, but we briefly discuss its characteristics to pave the way for understanding other Ethernet versions.

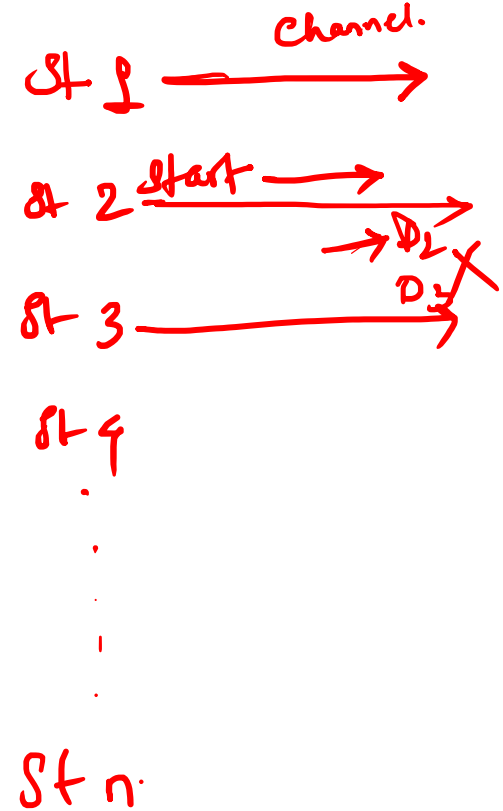
Access Method: CSMA/CD

The IEEE 802.3 standard defines carrier sense multiple access with collision detection (CSMA/CD) as the access method for traditional Ethernet. Stations on a traditional Ethernet can be connected together using a physical bus or star topology, but the logical topology is always a bus. By this, we mean that the medium (channel) is shared between stations and only one station at a time can use it. It also implies that all stations receive a frame sent by a station (broadcasting). The real destination keeps the frame while the rest drop it. In this situation, how can we be sure that two stations are not using the medium at the same time? If they do, their frames will collide with each other.



Ethernet Evolution

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. **Carrier sense multiple access (CSMA)** requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle “sense before transmit” or “listen before talk.” CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure 3.7, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).



Ethernet Evolution

Standard Ethernet

The original Ethernet with 10-Mbps data rate is now history, but we briefly discuss its characteristics to pave the way for understanding other Ethernet versions.

Implementation

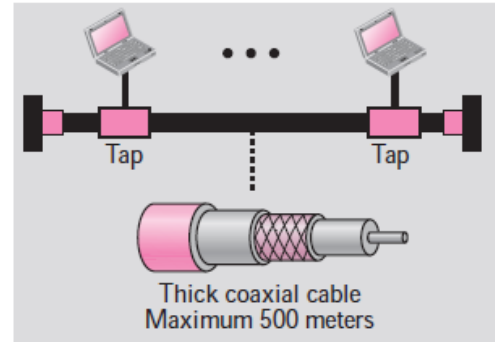
The Standard Ethernet defined several implementations, but only four of them became popular during '80s. Table 3.1 shows a summary of Standard Ethernet implementations. In the nomenclature 10Base-X, the number defines the data rate (10 Mbps), the term Base means baseband (digital) signal, and X approximately defines either the maximum size of the cable in 100 meters (for example 5 for 500 or 2 for 185 meters) or the type of the cable, T for unshielded twisted pair cable (UTP) and F for fiber-optic.

Table 3.1 *Summary of Standard Ethernet implementations*

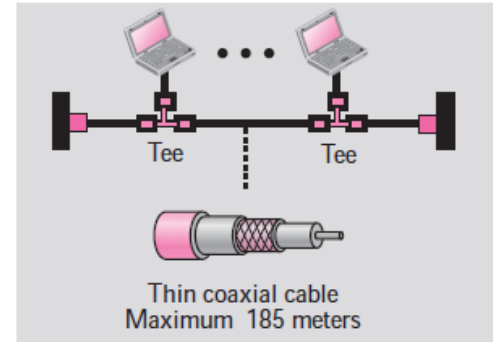
<i>Characteristics</i>	<i>10Base5</i>	<i>10Base2</i>	<i>10Base-T</i>	<i>10Base-F</i>
Medium	Thick coax	Thin coax	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m

Ethernet Evolution

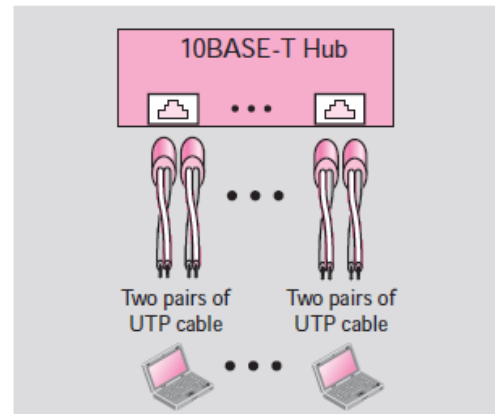
Standard Ethernet: Implementation



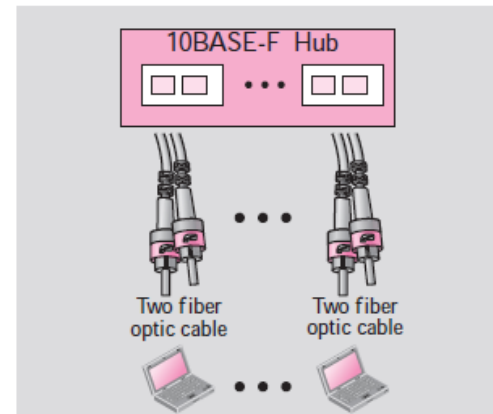
a. 10BASE5



b. 10BASE2



c. 10BASE-T




d. 10BASE-F

Ethernet Evolution

Fast Ethernet

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

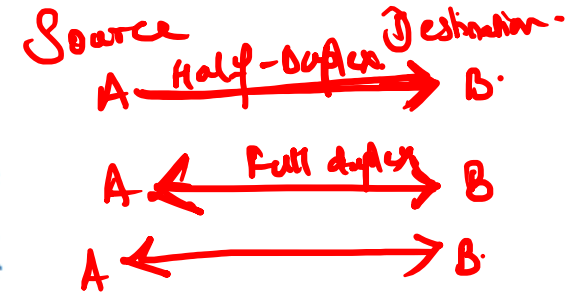
1. Upgrade the data rate to 100 Mbps.
 2. Make it compatible with Standard Ethernet.
 3. Keep the same 48-bit address.
 4. Keep the same frame format.
 5. Keep the same minimum and maximum frame lengths.
- 

Ethernet Evolution

MAC Sublayer

A main consideration in the evolution of Ethernet from 10 to 100 Mbps was to keep the MAC sublayer untouched. However, a decision was made to drop the bus topologies and keep only the star topology. For the star topology, there are two choices: half duplex and full duplex. In the half-duplex approach, the stations are connected via a hub; in the full-duplex approach, the connection is made via a switch with buffers at each port (see Section 3.5, Connecting Devices, at the end of the chapter).

The access method is the same (CSMA/CD) for the half-duplex approach; for full-duplex Fast Ethernet, there is no need for CSMA/CD. However, the implementations keep CSMA/CD for backward compatibility with Standard Ethernet.



Autonegotiation

A new feature added to ~~Fast Ethernet~~ is called **autonegotiation**. It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:

- ❑ To allow incompatible devices to connect to one another. For example, a device with a maximum capacity of 10 Mbps can communicate with a device with a 100 Mbps capacity (but can work at a lower rate).
- ❑ To allow one device to have multiple capabilities.
- ❑ To allow a station to check a hub's capabilities.

Ethernet Evolution

Fast Ethernet

Implementation

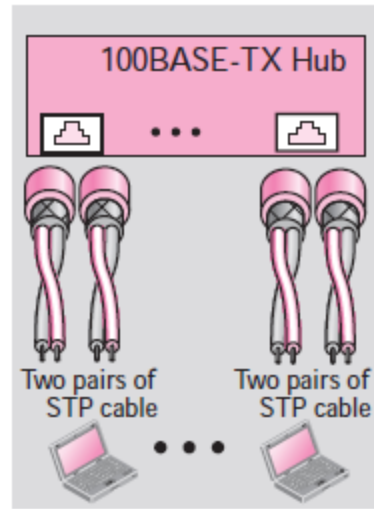
Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either shielded twisted pair, STP (**100Base-TX**) or fiber-optic cable (**100Base-FX**). The four-wire implementation is designed only for unshielded twist pair, UTP (**100Base-T4**). Table 3.2 is a summary of the Fast Ethernet implementations.

Table 3.2 *Summary of Fast Ethernet implementations*

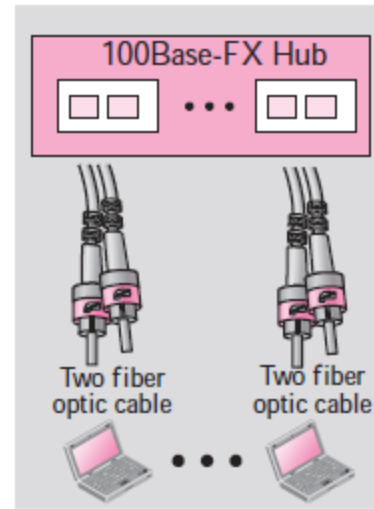
<i>Characteristics</i>	<i>100Base-TX</i>	<i>100Base-FX</i>	<i>100Base-T4</i>
Media	STP	Fiber	UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m

Ethernet Evolution

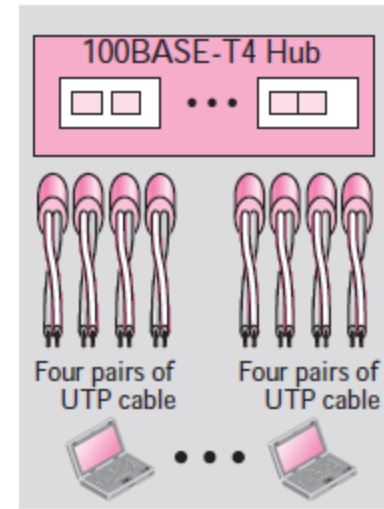
Fast Ethernet : Implementation



a. 100BASE-TX



b. 100BASE-FX



c. 100BASE-T4

Ethernet Evolution

Gigabit Ethernet

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

Ethernet Evolution

Gigabit Ethernet

Implementation

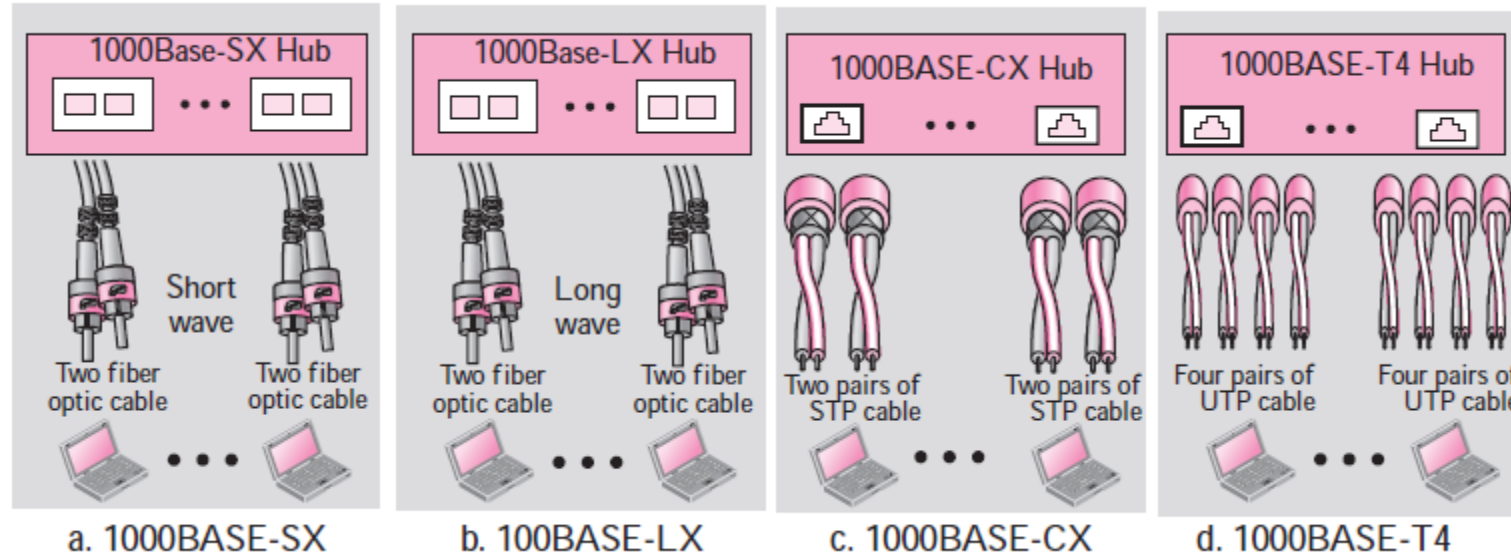
Table 3.3 is a summary of the Gigabit Ethernet implementations.

Table 3.3 *Summary of Gigabit Ethernet implementations*

<i>Characteristics</i>	<i>1000Base-SX</i>	<i>1000Base-LX</i>	<i>1000Base-CX</i>	<i>1000Base-T4</i>
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m

Ethernet Evolution

Gigabit Ethernet : Implementation



Ethernet Evolution

Ten-Gigabit Ethernet

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae. The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address. ✓
4. Use the same frame format. ✓
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM.

Ethernet Evolution

Ten-Gigabit Ethernet

Implementation

Ten-Gigabit Ethernet operates only in full duplex mode, which means there is no need for contention; CSMA/CD is not used in Ten-Gigabit Ethernet. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E. Table 3.4 shows a summary of the Ten-Gigabit Ethernet implementation.

Table 3.4 *Ten-Gigabit Ethernet Implementation*

<i>Characteristics</i>	<i>10GBase-S</i>	<i>10GBase-L</i>	<i>10GBase-E</i>
Media	multi-mode fiber	single-mode fiber	single-mode fiber
Number of wires	2	2	2
Maximum length	300 m	10,000 m	40,000 m

WIRELESS LANS

Introduction

IEEE 802.
↓

- Wireless communication is one of the fastest-growing technologies. 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.
- In this section, we concentrate on two wireless technologies for LANs: IEEE 802.11 wireless LANs, sometimes called wireless Ethernet, and Bluetooth, a technology for small wireless LANs.

IEEE 802.11



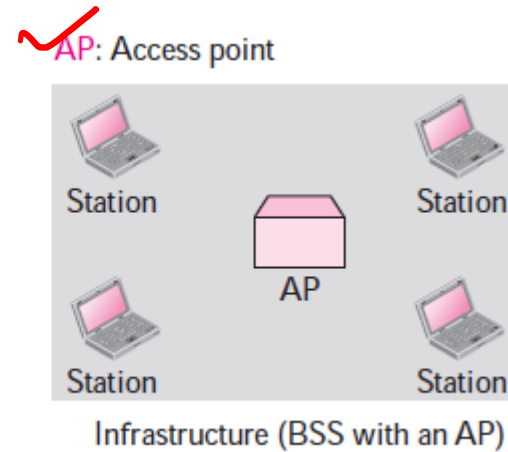
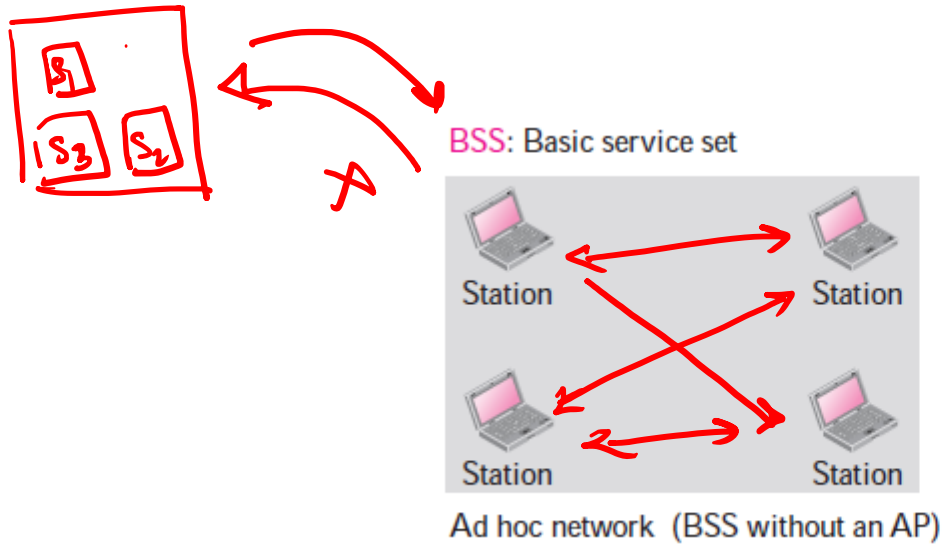
- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Architecture: The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

- **Basic Service Set:** IEEE 802.11 defines the **basic service set (BSS)** as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

IEEE 802.11

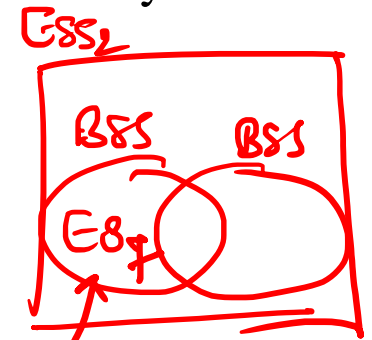
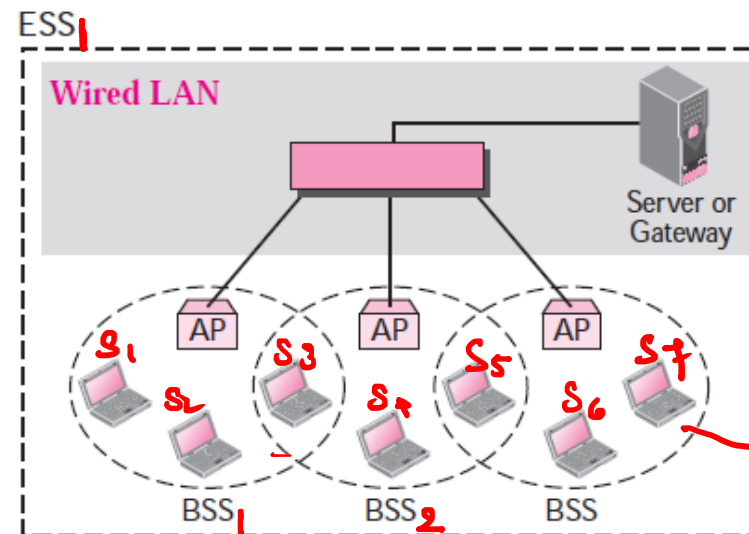
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture.
- In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.



IEEE 802.11

- Extended Service Set: An extended service set (ESS) is made up of two or more BSSs with Aps.
- In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.
- The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- Note that the extended service set uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs.

ESS: Extended service set
BSS: Basic service set
AP: Access point



IEEE 802.11

- **Station Types:**

- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS-transition, and ESS-transition mobility. (Stationary).
- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another.

IEEE 802.11

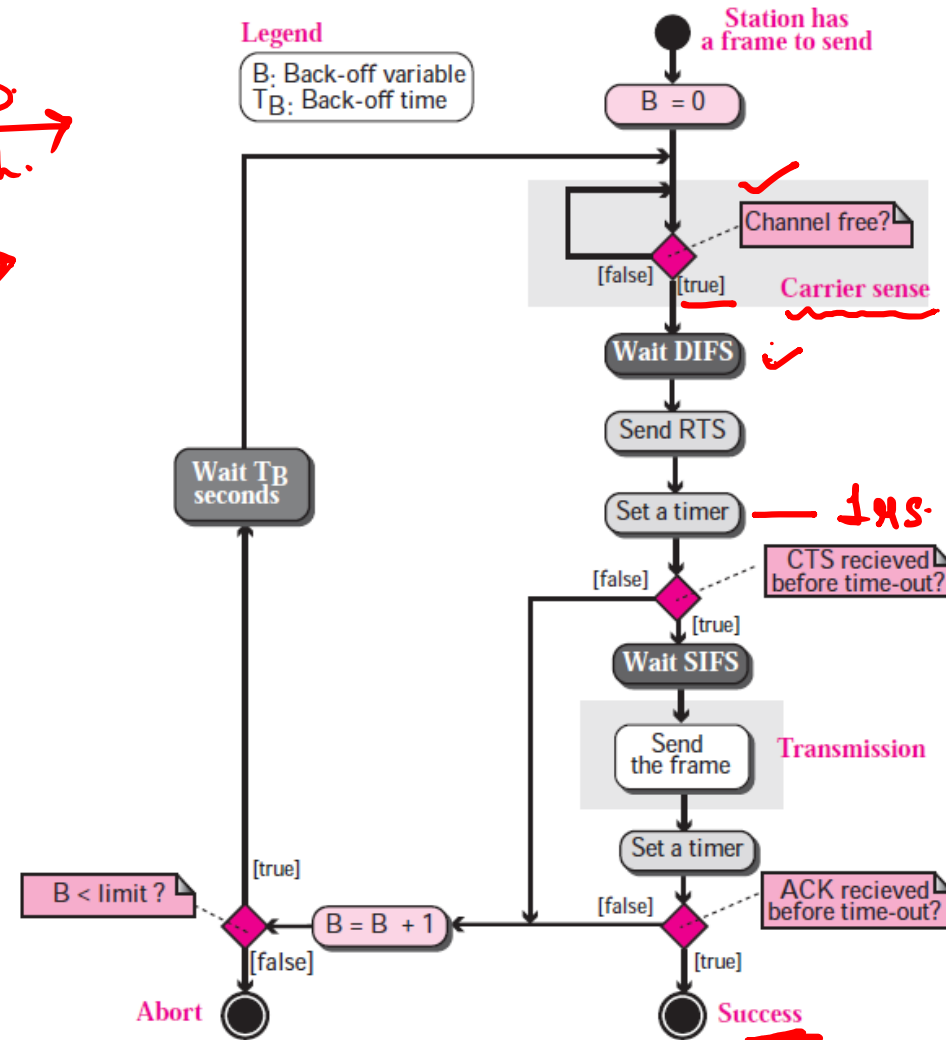
Datalink layer



- **MAC Sublayer:**
- There are two different MAC sublayers in this protocol, however; the one that is used most of the time is based on CSMA/CA (carrier sense multiple access with collision avoidance).

① CSMA/CD $\xrightarrow{\text{Loss: DxD path.}}$

② CSMA $\xrightarrow{\text{Station empty.}}$

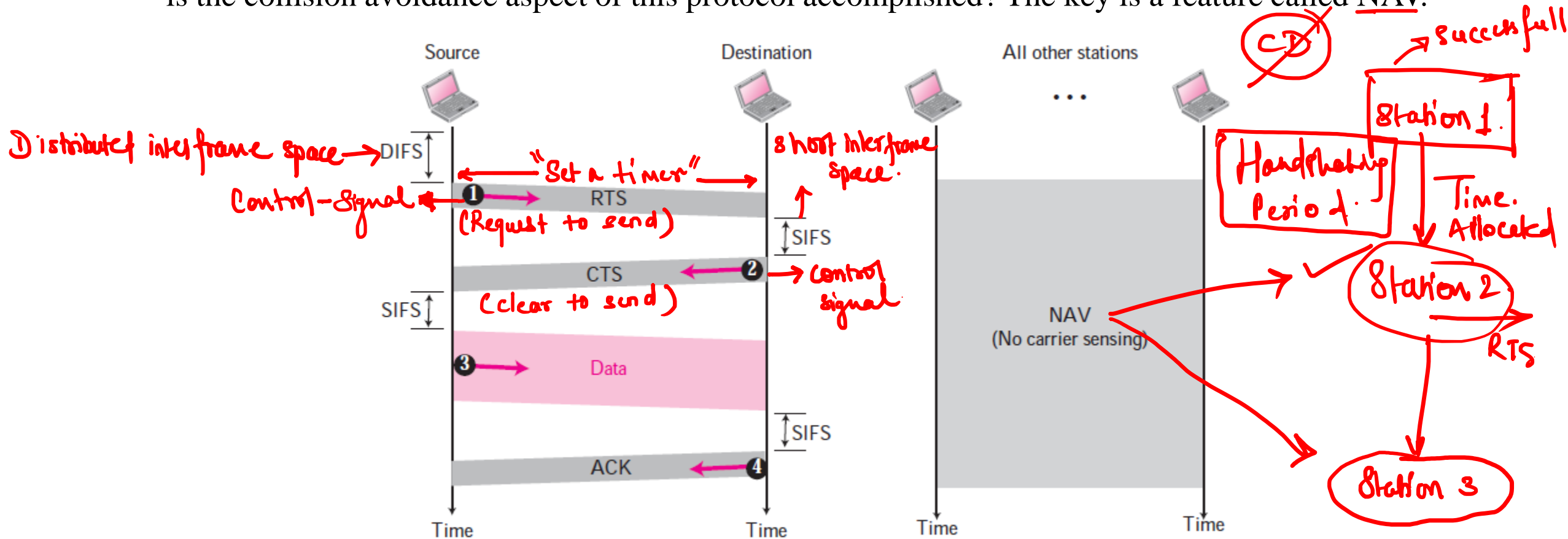


* Reasons for not implementing CSMA/CD \rightarrow (Detection).

- ① Collision detection station can send & receive collision signals. This requires higher B.W.
- ② Collision may not be detected because of hidden station problem.
- ③ Due to large distance betⁿ stations (sending & receiving) there can be fading of signals (collision signals).

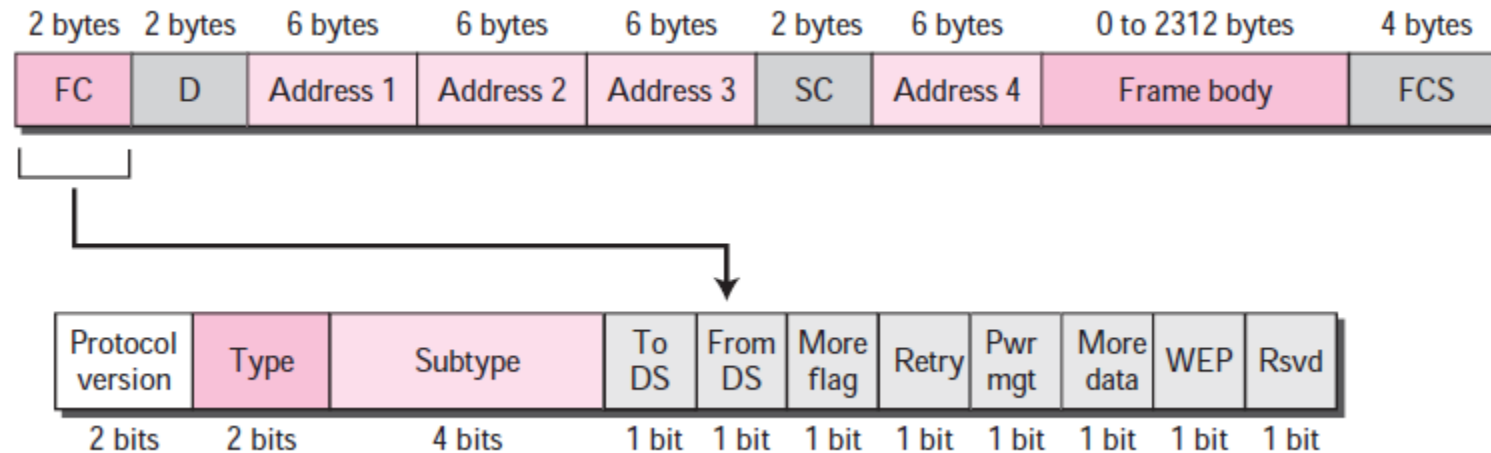
IEEE 802.11

- **Frame Exchange Time Line:**
- Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
- **Network Allocation Vector: (NAV)**
- How do other stations defer sending their data if one station acquires access? In other words, how is the collision avoidance aspect of this protocol accomplished? The key is a feature called NAV.



IEEE 802.11

- **Fragmentation:**
- The wireless environment is very noisy; a corrupt frame has to be retransmitted. The protocol, therefore, recommends fragmentation—the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.
- **Frame Format:**
- The MAC layer frame consists of nine fields:



IEEE 802.11

- **Frame Format:** The MAC layer frame consists of nine fields:
- **Frame control (FC):** The FC field is 2 bytes long and defines the type of frame and some control information. Table describes the subfields.

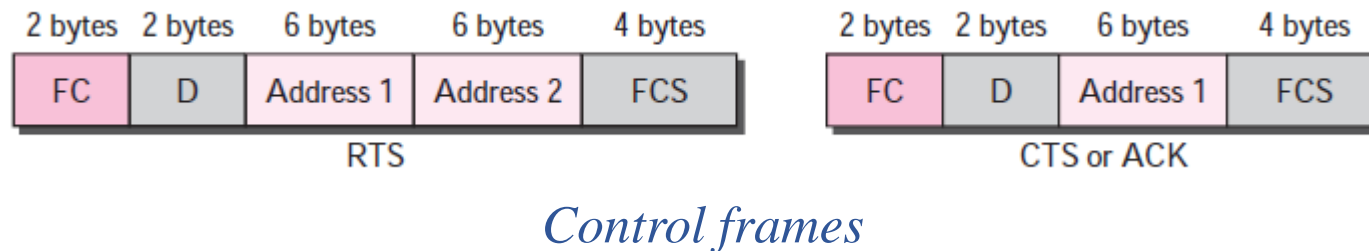
<i>Field</i>	<i>Explanation</i>
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 3.6)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

IEEE 802.11

- **D:** In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV. In one control frame, this field defines the ID of the frame.
- **Addresses:** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the *To DS* and *From DS* subfields and will be discussed later.
- **Sequence control:** This field defines the sequence number of the frame to be used in flow control.
- **Frame body:** This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.
- **FCS:** The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

IEEE 802.11

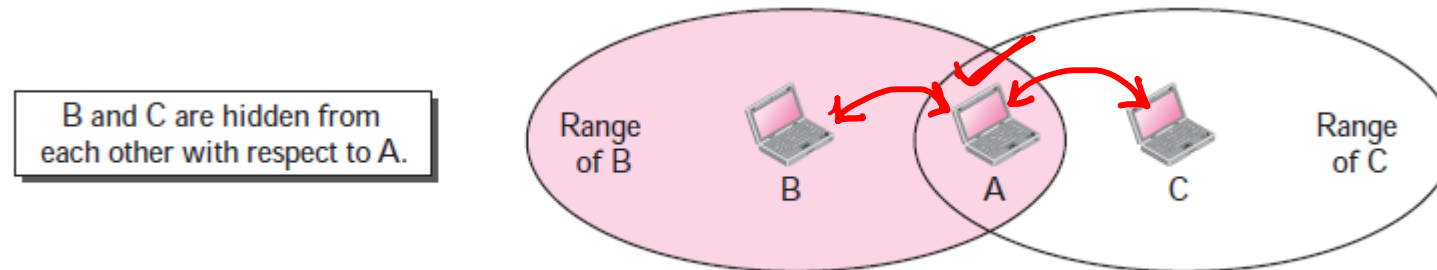
- **Frame Types:** A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.
- **Management Frames:** Management frames are used for the initial communication between stations and access points.
- **Control Frames:** Control frames are used for accessing the channel and acknowledging frames.



- **Data Frames:** Data frames are used for carrying data and control information.

IEEE 802.11

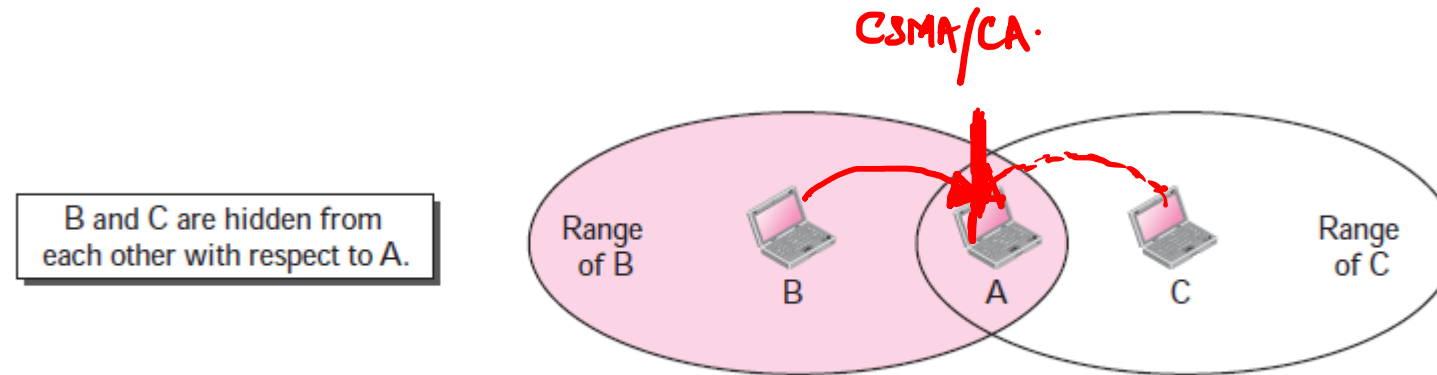
- **Hidden and Exposed Station Problems:** We will refer to hidden and exposed station problems and their effects.
- **Hidden Station Problem:** Fig below shows an example of the hidden station problem.
- Station B has a transmission range shown by the left oval (sphere in space); every station in this range can hear any signal transmitted by station B. Station C has a transmission range shown by the right oval (sphere in space); every station located in this range can hear any signal transmitted by C.
- Station C is outside the transmission range of B; likewise, station B is outside the transmission range of C. Station A, however, is in the area covered by both B and C; it can hear any signal transmitted by B or C.



Hidden station problem

IEEE 802.11

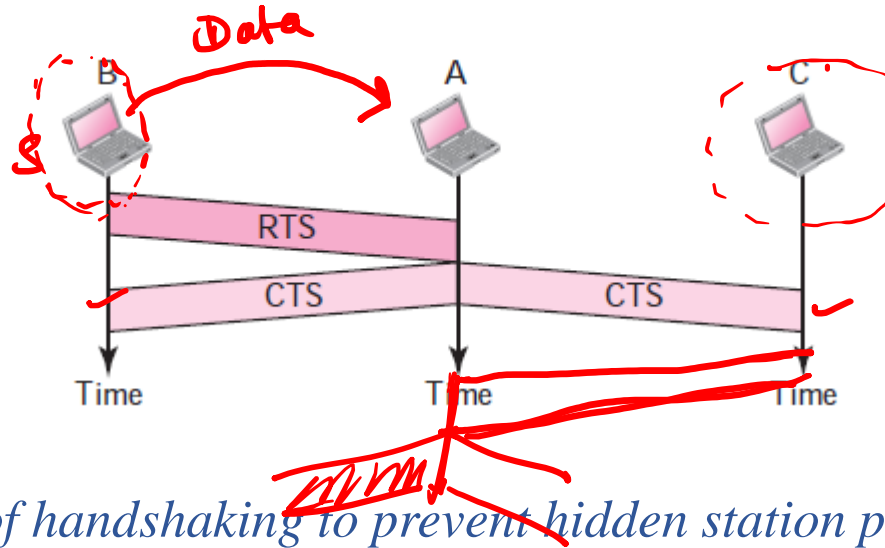
- Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free.
- Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations B and C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because of the possibility of collision.



Hidden station problem

IEEE 802.11

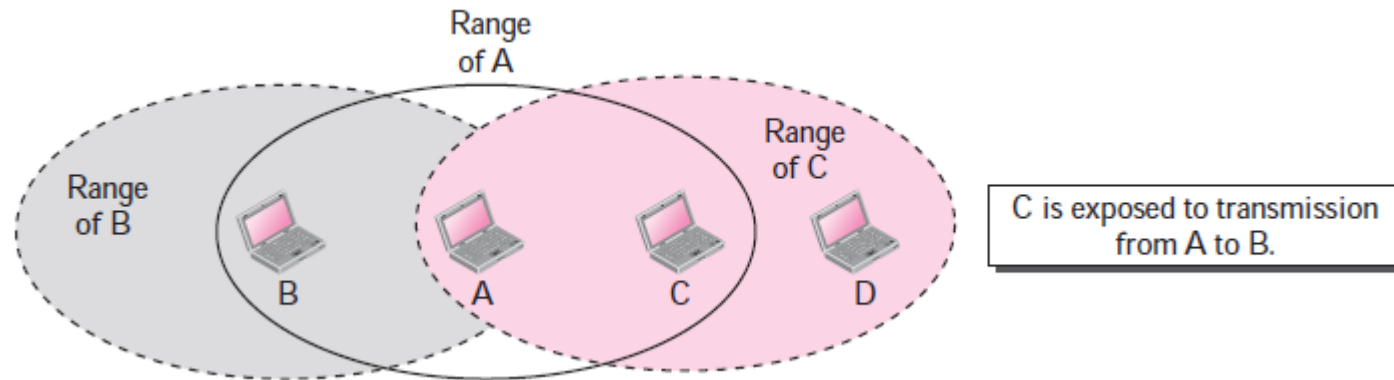
- **Hidden Station Solution:** The solution to the hidden station problem is the use of the handshake frames (RTS and CTS) that we discussed earlier. Fig below shows that the RTS message from B reaches A, but not C.
- However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.



Note: The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

IEEE 802.11

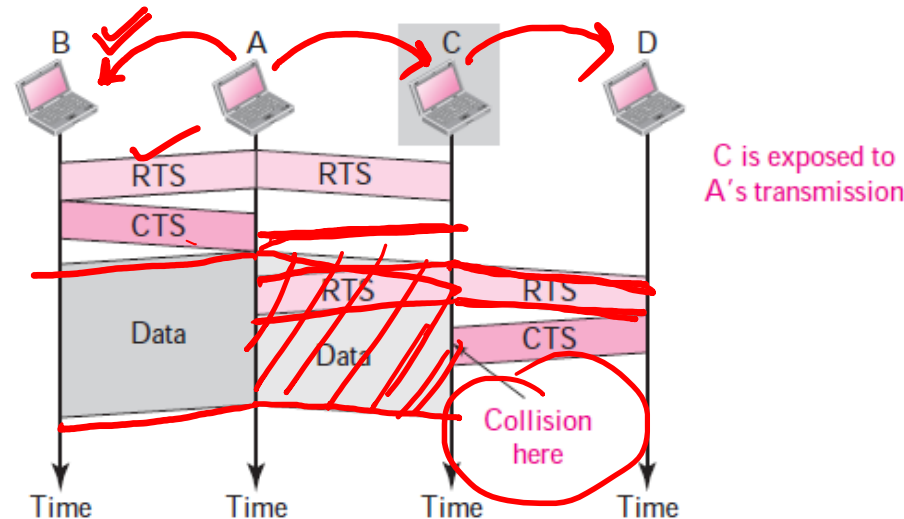
- **Exposed Station Problem:** Fig below shows an example of the exposed station problem.
- In this problem a station refrains from using a channel when it is, in fact, available. In Fig, station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending.
- In other words, C is too conservative and wastes the capacity of the channel.



Exposed station problem

IEEE 802.11

- **Exposed Station Problem:** The handshaking messages RTS and CTS cannot help in exposed station problem.
- Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that the CTS from B reaches A; it then sends an RTS to D to show that it needs to communicate with D.
- Both stations D and A may hear this RTS, but station A is in the sending state, not the receiving state. Station D, however, responds with a CTS. The problem is here.
- If station A has started sending its data, station C cannot hear the CTS from station D because of the collision; it cannot send its data to D. It remains exposed until A finishes sending its data.



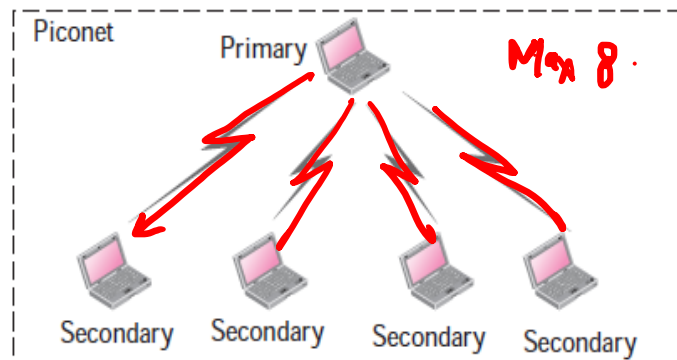
Use of handshaking in exposed station problem

Bluetooth

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.
- A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.
- Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal area network (PAN) operable in an area the size of a room or a hall.

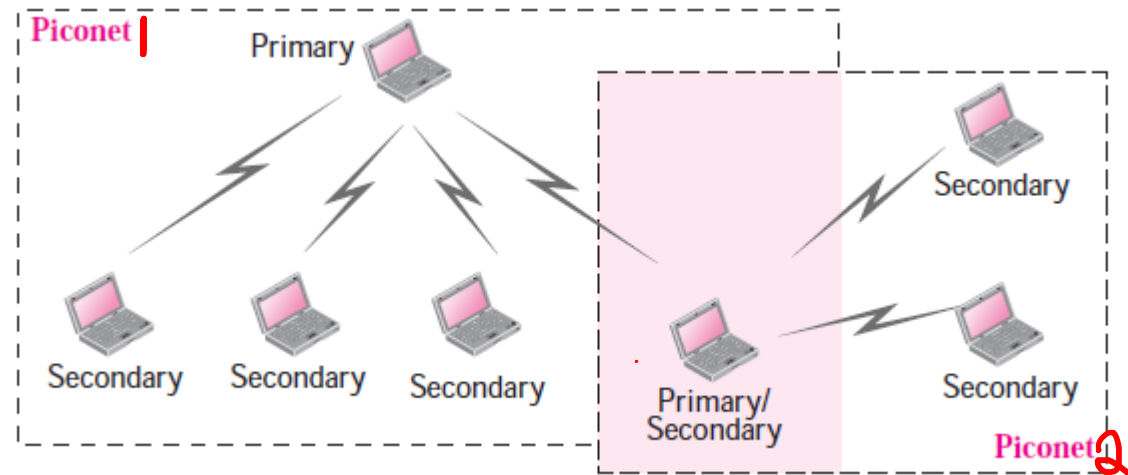
Bluetooth

- **Architecture:** Bluetooth defines two types of networks: piconet and scatternet.
- **Piconets:**
 - A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
 - All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many. Figure shows a piconet.
 - Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state.
 - A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.



Bluetooth

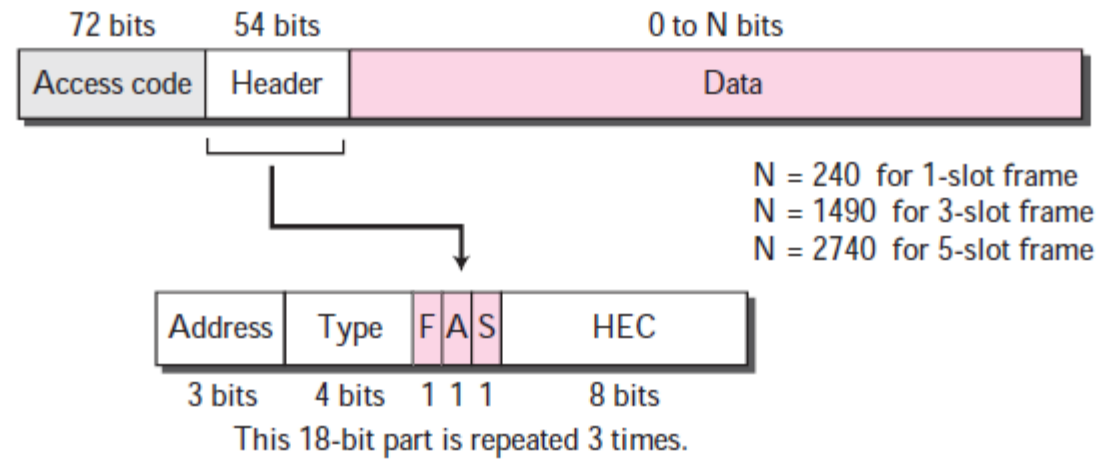
- **Architecture:** Bluetooth defines two types of networks: piconet and scatternet.
- **Scatternet:**
- Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure illustrates a scatternet.



Bluetooth

Frame Format:

- **Access code.** This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.



Bluetooth

- **Header.** This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
 - **Address:** The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
 - **Type:** The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.
 - **F:** This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).
 - **A:** This 1-bit subfield is for acknowledgment. Bluetooth uses stop-and-wait ARQ; 1 bit is sufficient for acknowledgment.
 - **S:** This 1-bit subfield holds a sequence number. Bluetooth uses stop-and-wait ARQ; 1 bit is sufficient for sequence numbering.
 - **HEC:** The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.
- **Data:** This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

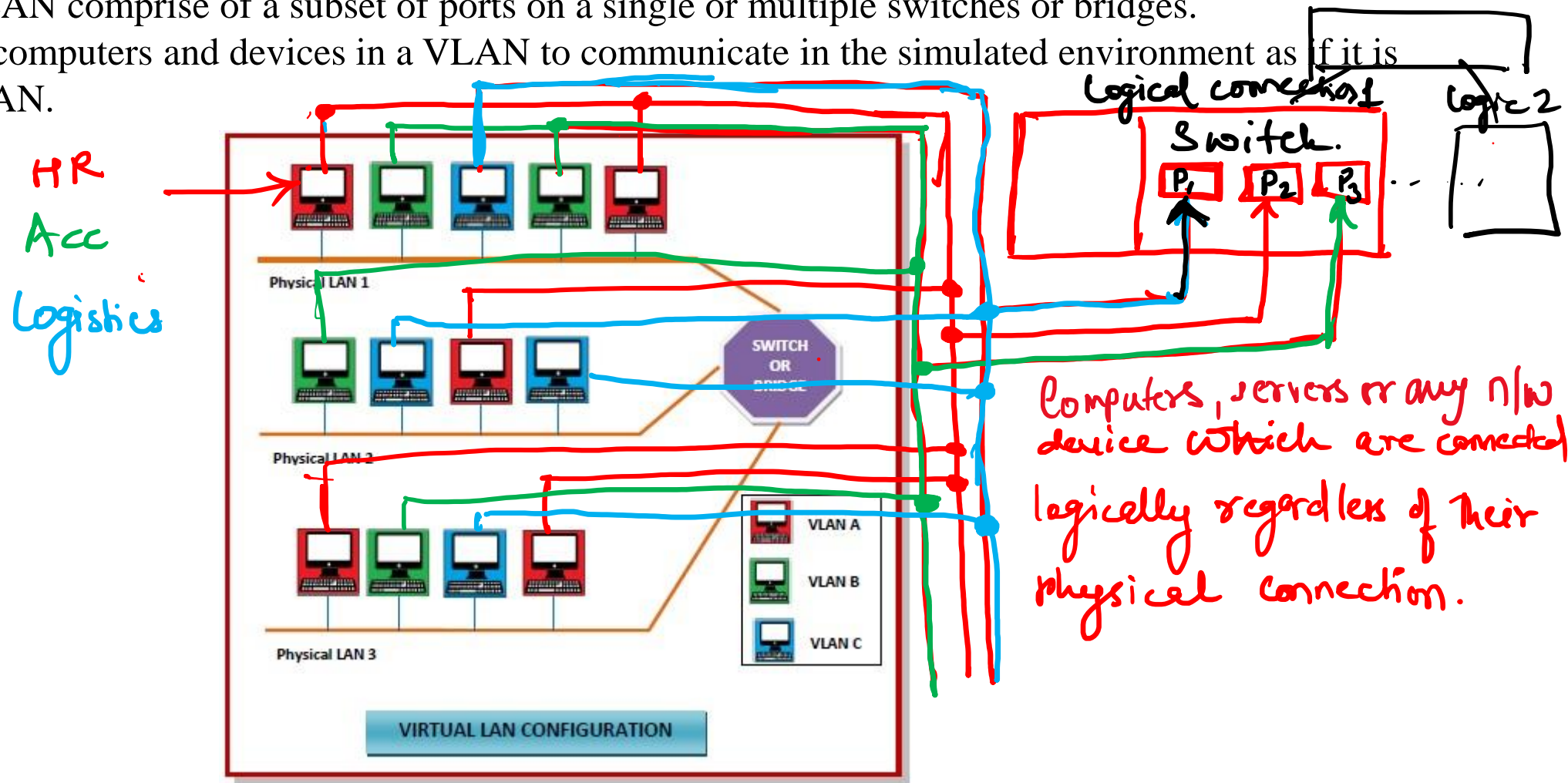
Bluetooth

- **Data:** This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.
 - a. The sending station, after sensing that the medium is idle, sends a special small frame called request to send (RTS). In this message, the sender defines the total time it needs the medium.
 - b. The receiver acknowledges the request (broadcast to all stations) by sending a small packet called clear to send (CTS).
 - c. The sender sends the data frame.
 - d. The receiver acknowledges the receipt of data.

Virtual LANS

Introduction

- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.
- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges.
- This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.



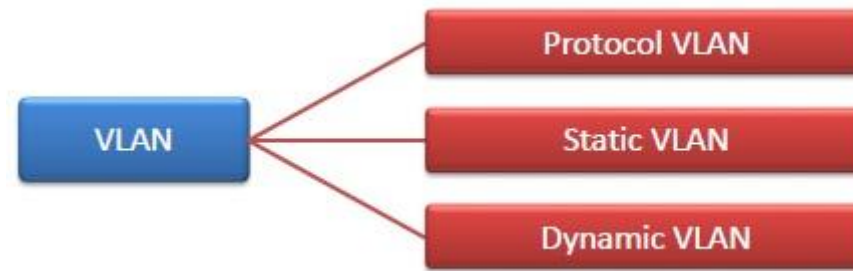
Features of VLANs



- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids in quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

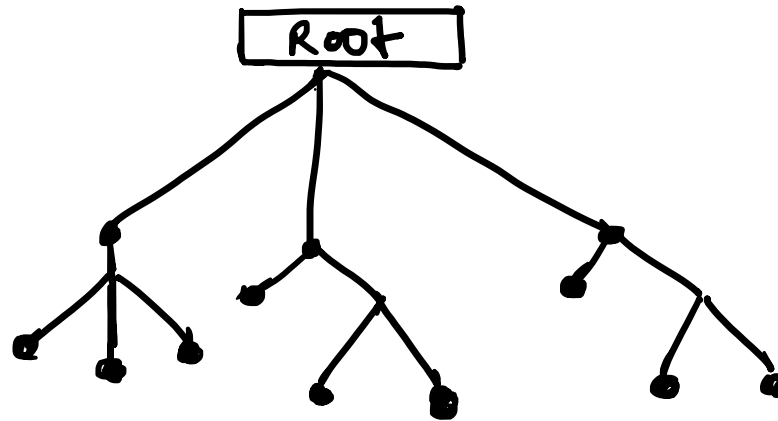
Types of VLANs

- Protocol VLAN – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames that come to it based upon the traffic's protocol.
- Port-based VLAN – This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- Dynamic VLAN – Here, the network administrator simply defines network membership according to device characteristics.



Virtual LAN Protocol and Design

- The VLAN protocol and design are based on IEEE 802.1Q, where IEEE 802.1 format is a group of multiplexed VLAN that supports VLAN multivendor. Other protocols like ISC (Cisco Inter-switch link) and VLT (Virtual LAN trunk) are also implemented on VLANs to carry the data of VLAN in a frame header of IEEE 802.1Q.
- Spanning tree protocol (STP) creates loop-free network topology on each data link layer (layer 2) of the OSI model among the switch links. This type of virtual LAN protocol and design is used to minimize the total STP of similar network topologies or multi-instance STP (MISTP) and blocks the connections of loop propagations of data. It is mainly used when the breakdown occurs in another part of the network during the transmission of data packets through a selected switch or route.



Advantages

- The use of VLAN reduces the traffic of broadcast and multicasting domains in computer networks. So, that data packets easily reach the destinations.
- Enhances performance.
- It forms the workgroups and logical groups virtually to increase the communication between the users within the workgroups
- Easy to control and manage the VLAN's because there is no need to reconfigure the routers reduces the use of devices on the network topology and cabling.
- Reduces the installation and maintenance cost
- It increases the security during the broadcasting of sensitive data on the computer network by controlling firewalls, intrusions, and restrict access to the network.
- Easy to resolve all the broadcasting issues and reduce the size of the domains of broadcast on the network.

Thankyou