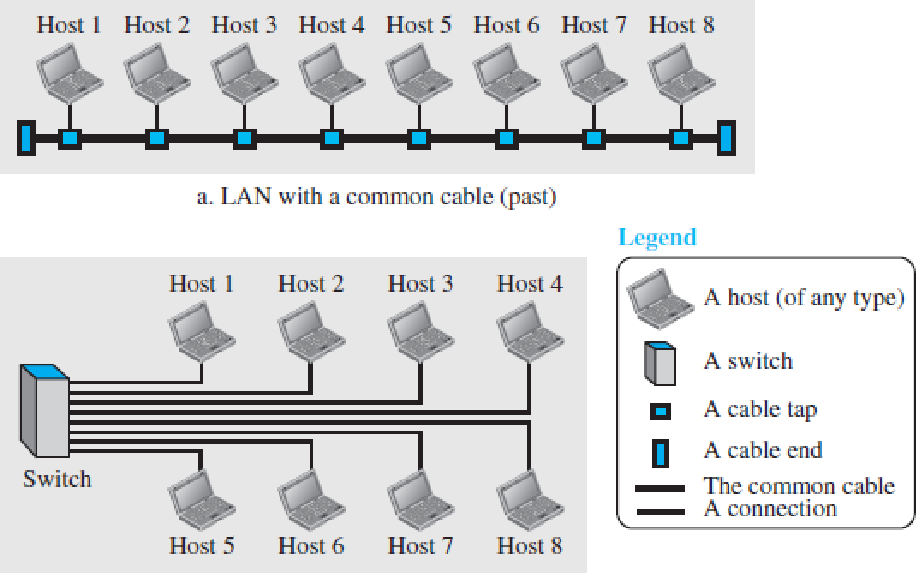
Computer Networking with TCP/IP

Module 2

Wired Local Area Network (LAN)

A local area network is a computer network that is designed for a limited geographic area such as building or campus.

Ethernet, token ring, token bus, FDDI, and ATM Lan are some examples of the LAN.



a. LAN with a common cable (past)

b. LAN with a switch (today)

The following characteristics differentiate one LAN from another:

- **Topology**: The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
- **Protocols**: The rules and encoding specifications for sending data. The protocols also determine whether the network uses peer-to-peer or client/server architecture.
- **Media**: Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks communicate via radio waves, hence, do not use any connecting media.

In 1980 and 1990s several different types of LANs were used. All these LAN used a media –access method to solve the problem of sharing the media. The Ethernet used the CSMA/CD approach. The token ring, Token BUS, and FDDi used token passing approach.

Wired LAN has six essential components.

1. **Network Adapter**: A network adapter is usually the only component within a computer for interfacing or connecting with a network. A network adapter for wired networks has an RJ-45 port that uses twisted or untwisted pair cable for network connectivity.
2. **Network Medium:** Wired networks need cable. The most common form of cable used in networks is called the "Unshielded Twisted Pair."

3. **Cable Connectors:** In wired networks, the most common form of connector is the RJ45. Every computer with networking capabilities has an RJ45 port. This is sometimes called a "network port" or an "Ethernet port."
4. **Power Supply:** Both wired and wireless networks need a power supply. A wireless network uses the current to generate radio waves. A cabled network sends data interpreted as an electronic pulse.
5. **Hub/Switch/Router:** connecting devices.
6. **Software:** is the intelligence that causes all the components to function together. The most popular network software today uses what is known as the TCP/IP protocol suite.

Network Topology

Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate with each other is determined by the network's topology. Topologies are either physical or logical.

Some of the most common network topologies are:

Bus topology, Star topology, Ring topology, Tree topology, Mesh topology, Cellular topology.

ETHERNET

Ethernet is most widely used LAN Technology, enabling devices to communicate with each other via a protocol -- a set of rules or common network language. which is defined under IEEE standards 802.3.

It usually transmits at 10 Mbps and relies on CSMA/CD to regulate traffic on the main cable segment.

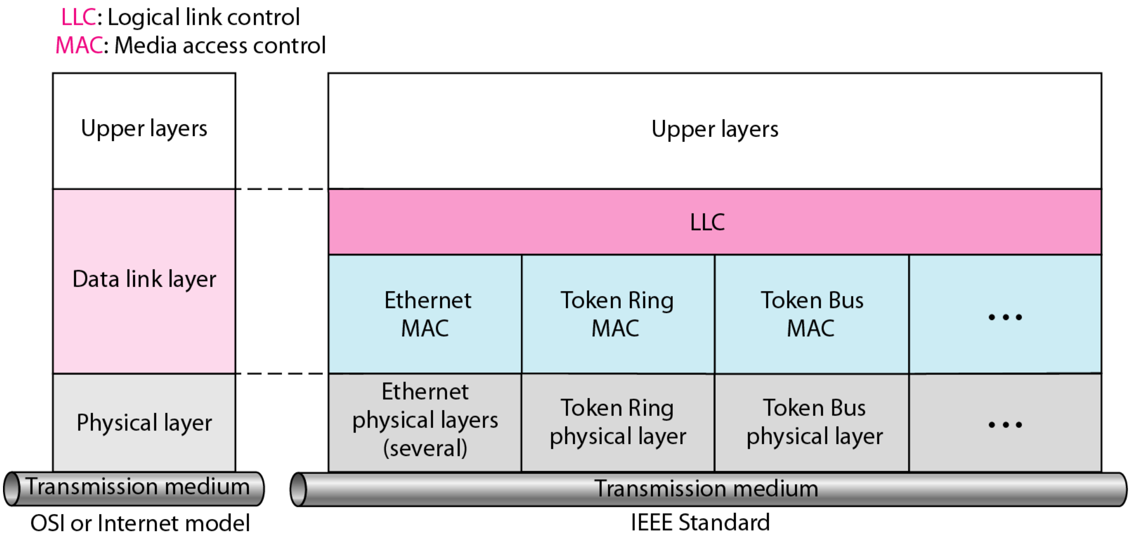
IEEE Standards

In 1985 the computer society of IEEE started a project 802 to set standards to enable inter communication among equipment from variety of manufactures.

The Data link layer is subdivided into the following:

Logical Link Control (LLC) & Media Access Control (MAC)

IEEE standard for LANs



Bottom part: MAC

- The frame is called **IEEE 802.3.**
- Handles framing, MAC addressing, Medium Access control
- **Specific implementation** for each LAN protocol
    - Defines CSMA/CD as the access method for Ethernet LANs and Token passing method for Token Ring.
- Implemented in **hardware**.

Top part: LLC (Logical Link Control)

- The subframe is called **IEEE 802.2**.
- Provides **error and flow control** if needed.
- It makes the MAC sublayer transparent.
    - Allows interconnectivity between different LANs data link layers.
- Used to multiplex multiple network layer protocols in the data link layer frame.
- Implemented in **software**.

Frame Format

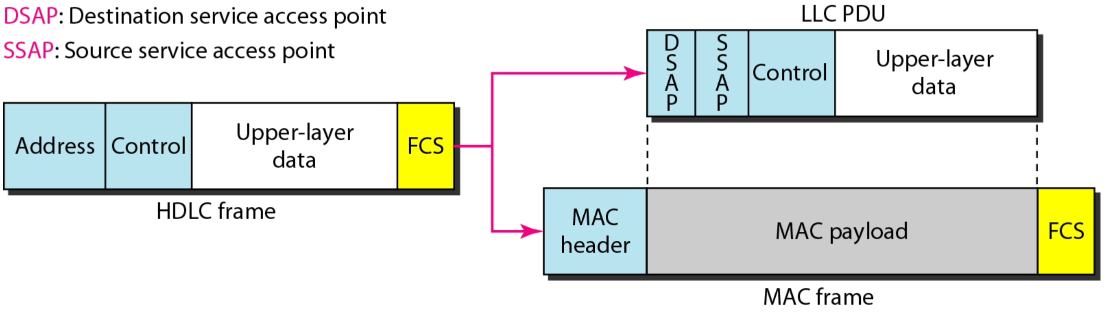
The protocol data unit sent in an ethernet LAN is called a frame.

- An Ethernet frame contains seven fields. Preamble, SFD, Destination Address, Source Address, length / type of data unit, upper layer data and Frame Check Sequence (FCS).
- Ethernet does not provide any mechanism for acknowledgement of received frames.
- Acknowledgement must be implemented at the higher layers.

HDLC frame compared with LLC and MAC frames

DSAP: Destination service access point

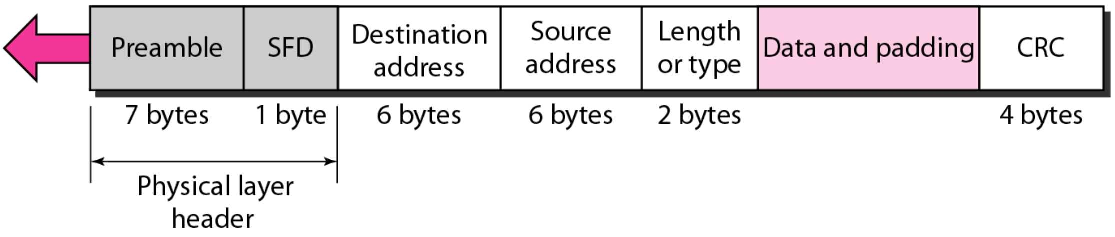
SSAP: Source service access point



802.3 MAC frame

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Preamble:

- The 802.3 frame contains 7 bytes.
- Added at physical layer.

- Enables it to synchronize its input timing.
- Alert and timing pulse.

Start frame delimiter (SFD)

- Signals the beginning of the frame.
- 1 byte length
- Added at the physical layer.

Destination Address DA: 6 bytes MAC address of the designation station.

Source Address SA: 6 Bytes MAC address of the source or the sender.

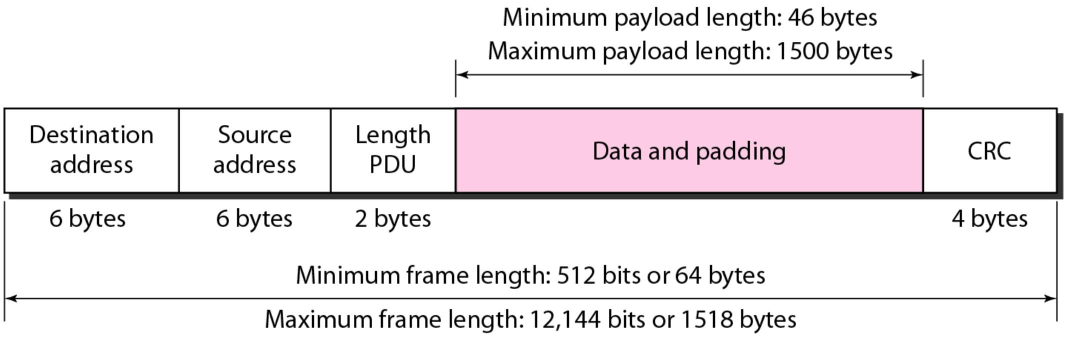
Length / type

- 2 bytes length.
- Ethernet used this field as the type of field to define upper layer protocol using the MAC frame.

Data: Field carries data encapsulated from the upper layer protocols.

CRC / FCS the last field contains error detection info.

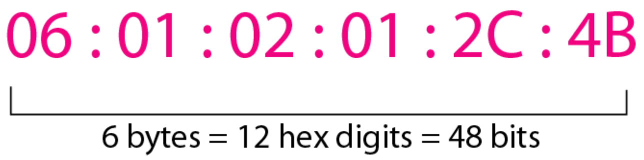
Minimum and maximum lengths of Frame


Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Addressing

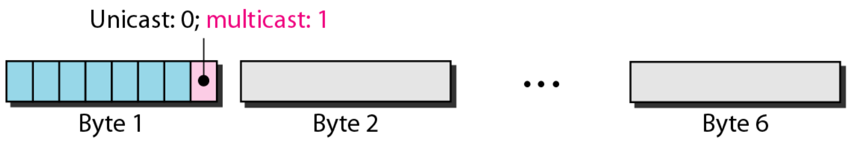
Each station on an ethernet network has its own network card (NIC) it is coming with 6-byte physical Address inbuilt called MAC address. A 48-bit address normally written hexadecimal notation with a colon. (:)

Example of an Ethernet address in hexadecimal notation

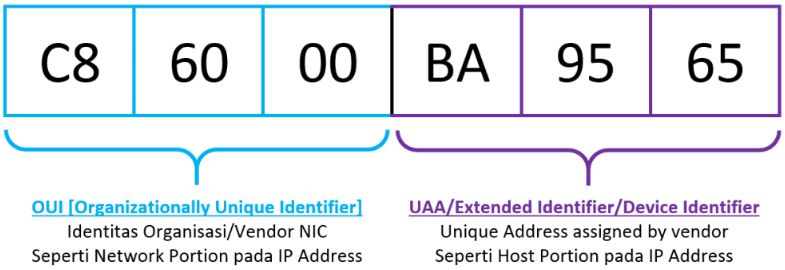

06 : 01 : 02 : 01 : 2C : 4B
6 bytes = 12 hex digits = 48 bits

There are three types of addresses.

1. Unicast – the least significant bit of the first byte = 0
2. Multicast – the least significant bit of the first byte = 1
3. Broadcast Address – All digits are F (All 1’s)



A MAC Address


C8
60
00
BA
95
65
OUI [Organizationally Unique Identifier]
Identitas Organisasi/Vendor NIC
Seperti Network Portion pada IP Address
UAA/Extended Identifier/Device Identifier
Unique Address assigned by vendor
Seperti Host Portion pada IP Address

Example 3.1

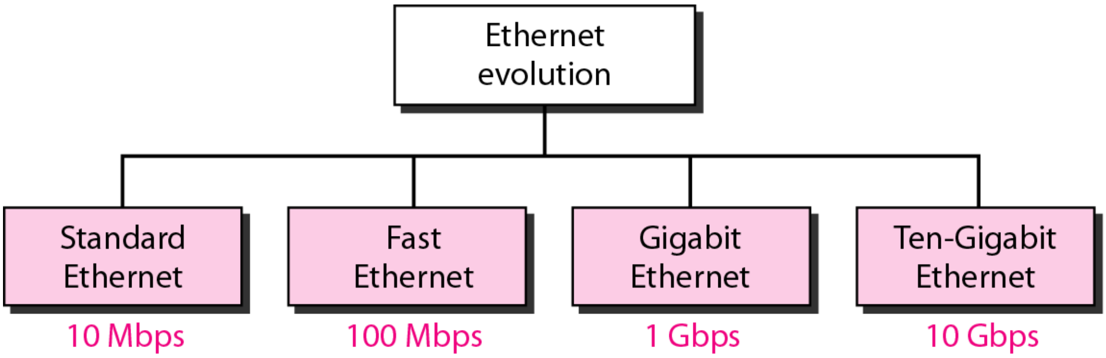
Define the type of the following destination addresses:
a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are F's.

Ethernet Evolution

The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Since then, it has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps),



CSMA/CD Carrier Sense Multiple Access with Collision Detection.

Collision Domain

A Collision Domain is a scenario in which when a device sends out a message to the network, all other devices which are included in its collision domain must pay attention to it, no matter if it was destined for them or not. This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time. Remember, it happens only in case of a half-duplex mode.

Broadcast Domain

A Broadcast Domain is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain must pay attention to it. This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

CSMA/CD

Is a media access control method that was widely used in early ethernet technology / LANS.

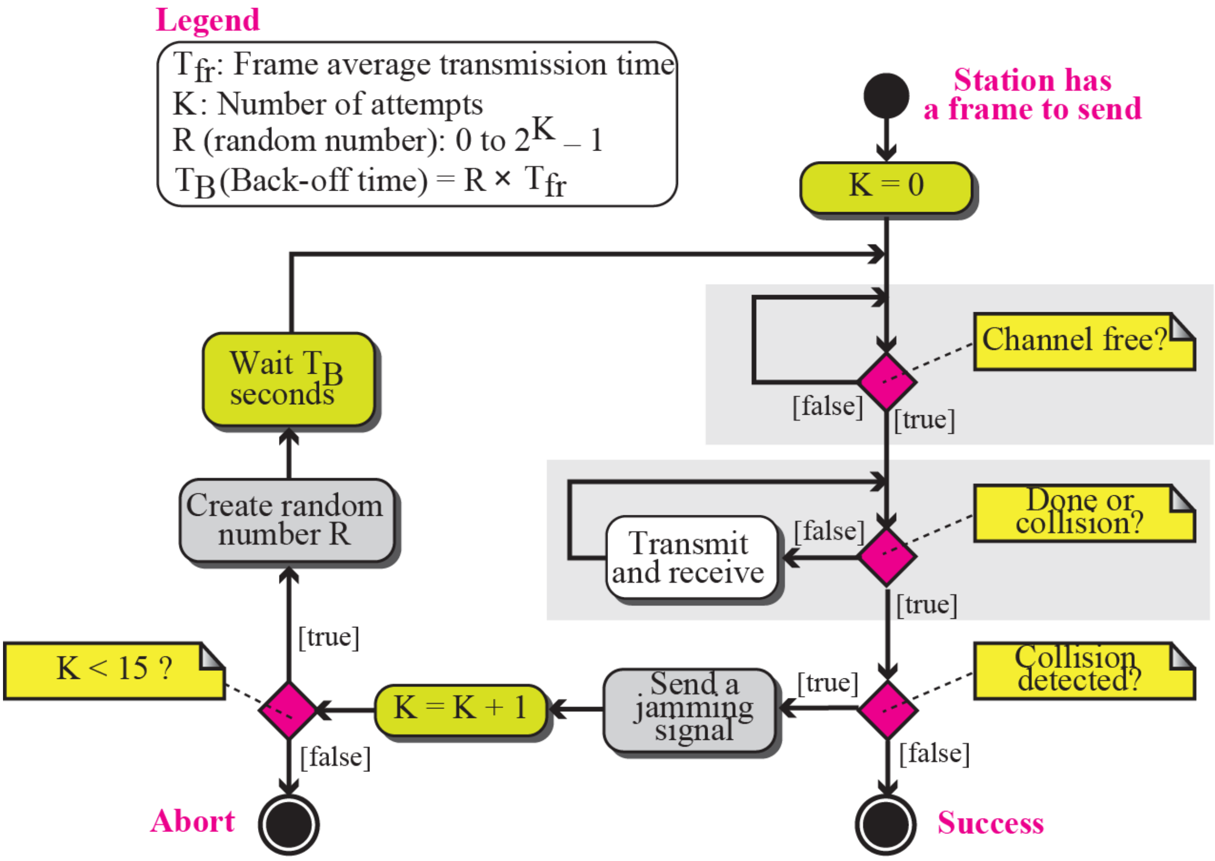
CSMA/CD follow the protocol to agree on some terms and collision detection measures for effective transmission. This protocol divides with station will transmit and when, so that data reaches destination without corruption.

- Collision detected with in short time.
- Colliding transmission aborted, reducing channel wastage.
- Persistent or non-persistent retransmission

Collision Detection

- Easy in wired LANS, measure signal strengths compare transmitted, received signals.
- Difficult in wireless LANS receiver shut off while transmitting.

CSMA/CD Flow Diagram



Carrier Sensing

- A node is listens to the channel before transmitting.
- If a frame from another node currently being transmitted into the channel, a node then waits a random amount of time and then again senses the channel.
- If the channel is sensed to idle, then begins frame transmission.
- Otherwise, the node waits another random amount of time and repeats their process.

Collision Detection

- A Transmitting node listens to the channel while it is transmitting.
- If it detects that another node is transmitting an interfering frame, it stops transmitting and and uses some protocol to determine when it should next attempt to transmit.

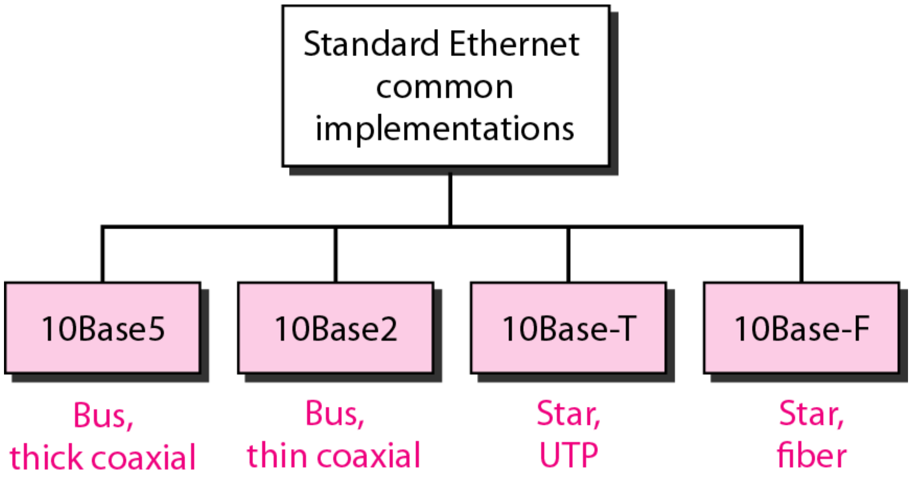
CSMA/CD Algorithm

- **Step 1**. A device with a frame to send listens until the Ethernet is not busy.
- **Step 2**. When the Ethernet is not busy, the sender begins sending the frame.
- **Step 3.** The sender listens while sending to discover whether a collision occurs; collisions might be caused by many reasons, including unfortunate timing. If a collision occurs, all currently sending nodes do the following:
    - A. They send a jamming signal that tells all nodes that a collision happened.
    - B. They independently choose a random time to wait before trying again, to avoid unfortunate timing.
    - C. The next attempt starts again at Step 1.

Standard Ethernet (10 Mbps)

All Ethernet connections are limited by the slowest component, be that the hub, the Ethernet card, or the Ethernet cable. The 10-Mbps Standard Ethernet has gone through several changes before moving to the higher data rates. These changes opened the road to the evolution of the Ethernet to become compatible with other high-data-rate LANs. Used “Manchester encoding”.

Categories of Standard Ethernet

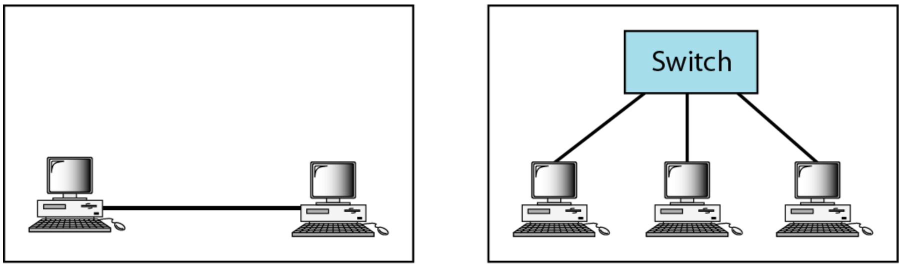


Summary of Standard Ethernet implementations

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

Fast Ethernet (100 Mbps)

This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure.



a. Point-to-point

b. Star

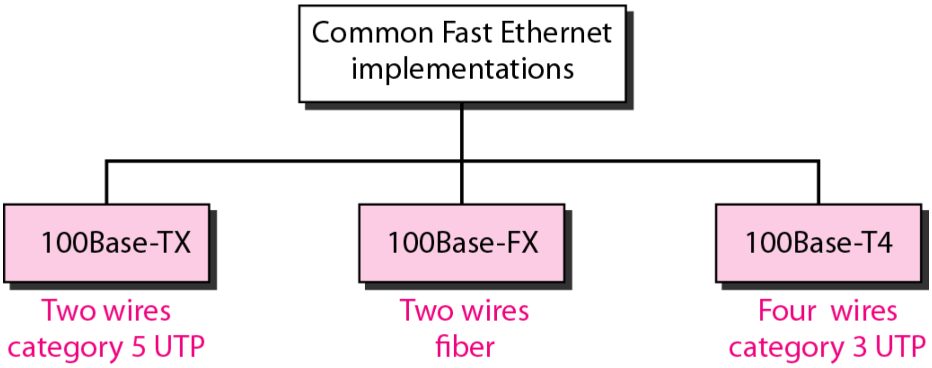
The access method is the same (CSMA/CD) for the half-duplex approach; for fullduplex Fast Ethernet, there is no need for CSMA/CD.

Autonegotiation

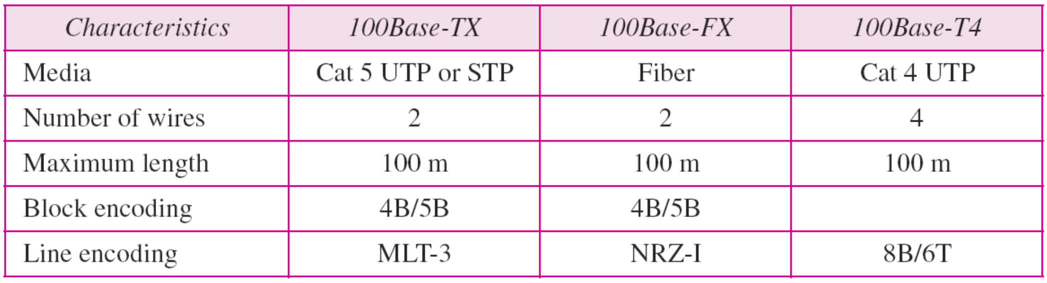
A new feature added to Fast Ethernet is called autonegotiation. It allows a station or a hub a range of capabilities. Autonegotiation allows two devices to negotiate the mode or data rate of operation. It was designed particularly for the following purposes:

- To allow incompatible devices to connect to one another.
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

Fast Ethernet implementations



Summary of Fast Ethernet implementations

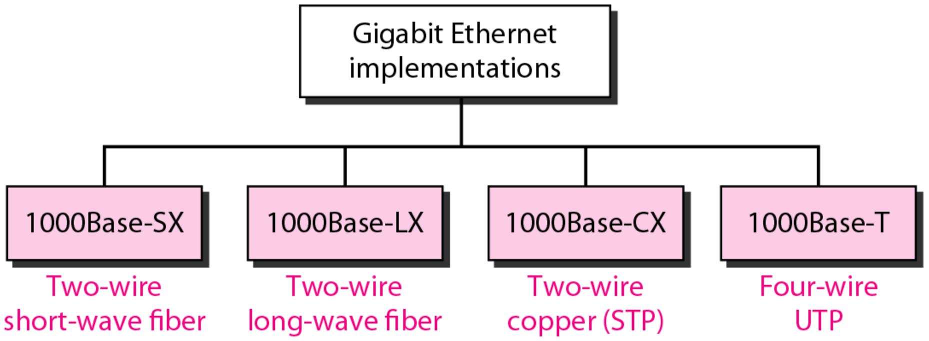


Characteristics	*100Base-TX*	*100Base-FX*	*100Base-T4*
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Gigabit Ethernet (1 Gbps)

Also known as “gigabit-Ethernet over copper” or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Operates in both full duplex and half duplex

Gigabit Ethernet implementations



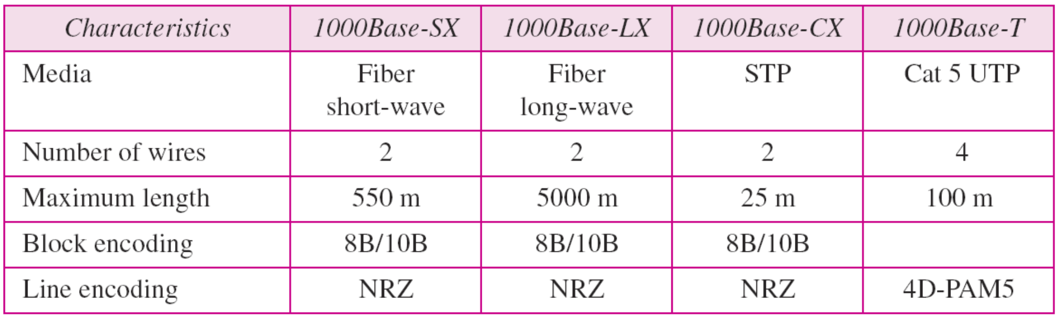
Carrier Extension:

To allow for a longer network, we increase the minimum frame length. The carrier extension approach defines the minimum length of a frame as 512 bytes (4096 bits). This means that the minimum length is 8 times longer.

Frame Bursting

Carrier extension is very inefficient if we have a series of short frames to send; each frame carries redundant data. To improve efficiency, frame bursting was proposed. Instead of adding an extension to each frame, multiple frames are sent.

Summary of Gigabit Ethernet implementations



Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
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
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

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:

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

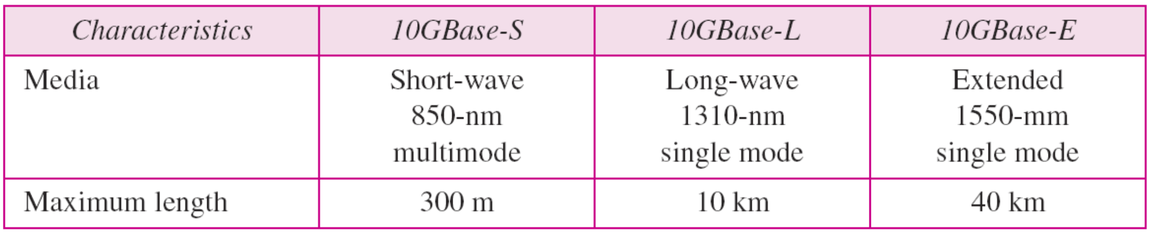
10 Gbps Implementation

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:

1. 10GBase-S,
2. 10GBase-L, and
3. 10GBase-E.

Summary of Ten-Gigabit Ethernet implementations



Characteristics	*10GBase-S*	*10GBase-L*	*10GBase-E*
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-mm single mode
Maximum length	300 m	10 km	40 km

Wireless LAN IEEE 802.11

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

Two Wireless technologies for LANs:

1. IEEE 802.11 wireless LANs, sometimes called wireless Ethernet.
2. Bluetooth, a technology for small wireless LANs.

Medium

The first difference we can see between a wired and a wireless LAN is the medium. In a wireless LAN, the medium is air, the signal is generally broadcast. When hosts in a wireless LAN communicate with each other, they are sharing the same medium (multiple access).

Hosts

In a wireless LAN, a host is not physically connected to the network; it can move freely (as we'll see) and can use the services provided by the network.

Isolated LANs ad hoc or independent basic service set

The 802.11 standard allows two or more wireless clients to communicate directly with each other, with no other means of network connectivity. This is known as an ad hoc wireless network, or an independent basic service set (IBSS).

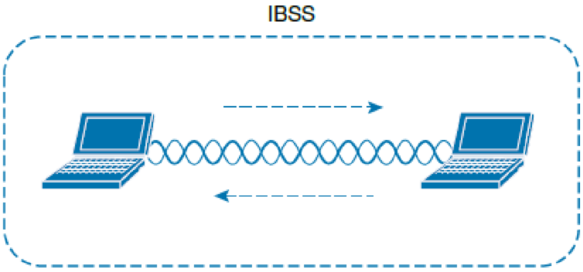


Figure 26-9 *802.11 Independent Basic Service Set*

Characteristics

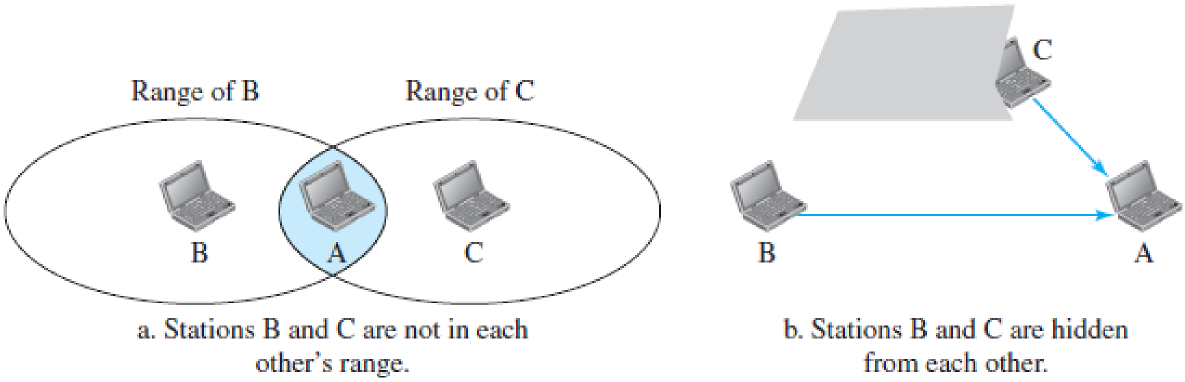
1. **Attenuation:** The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.
2. **Interference:** Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.
3. **Multipath Propagation:** A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected from obstacles such as walls, the ground, or objects. The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.
4. **Error** With the above characteristics of a wireless network, we can expect that errors and error detection are more serious issues in a wireless network than in a wired network. If we think about the error level as the measurement of signal-to-noise ratio (SNR), we can better understand why error detection and error correction and retransmission are more important in a wireless network.

Access Control

Maybe the most important issue we need to discuss in a wireless LAN is access control—how a wireless host can get access to the shared medium (air).

Hidden station problem

In which a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.



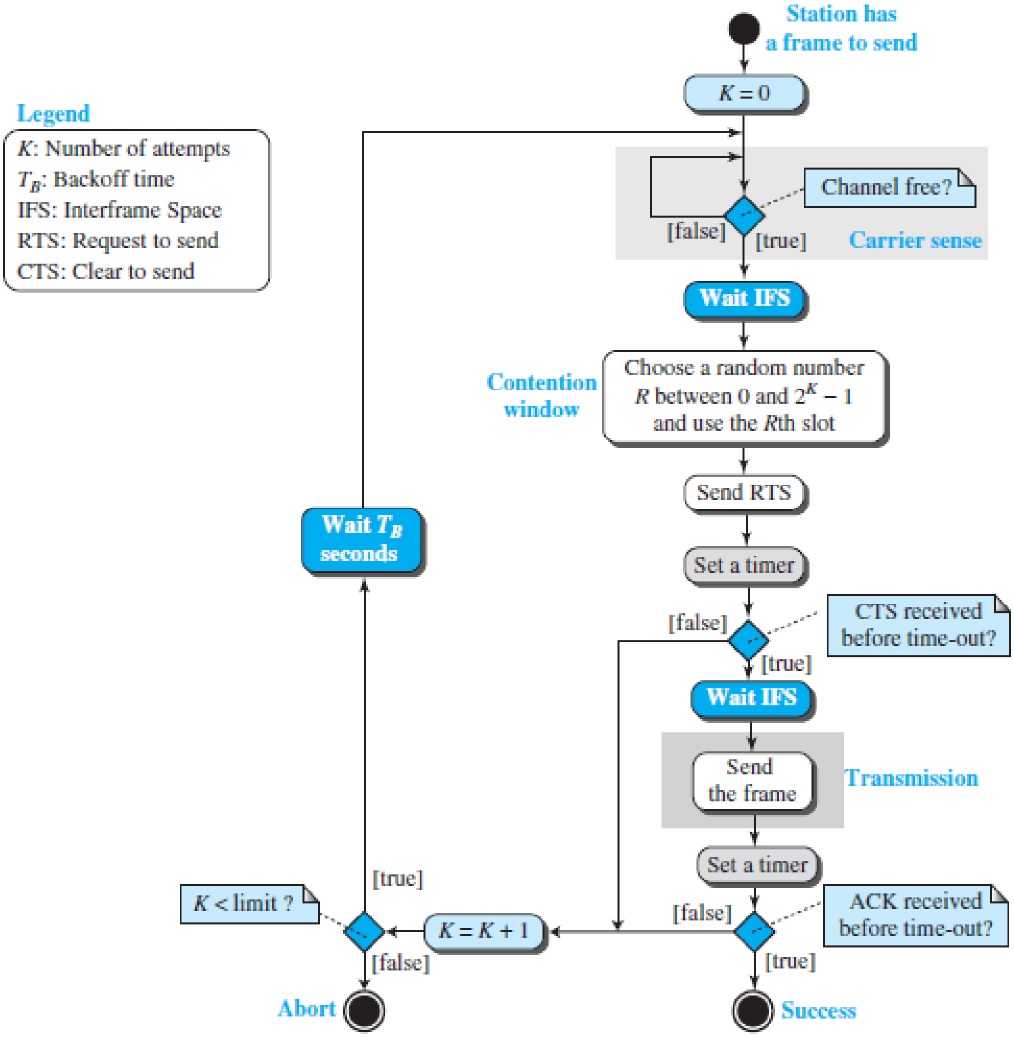
a. Stations B and C are not in each other's range.

b. Stations B and C are hidden from each other.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided using CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments.

Flow diagram of CSMA / CA



1. **Interframe Space (IFS).** First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period called the interframe space or IFS.
2. **Contention Window.** The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy.
3. **Acknowledgment**. With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

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**.

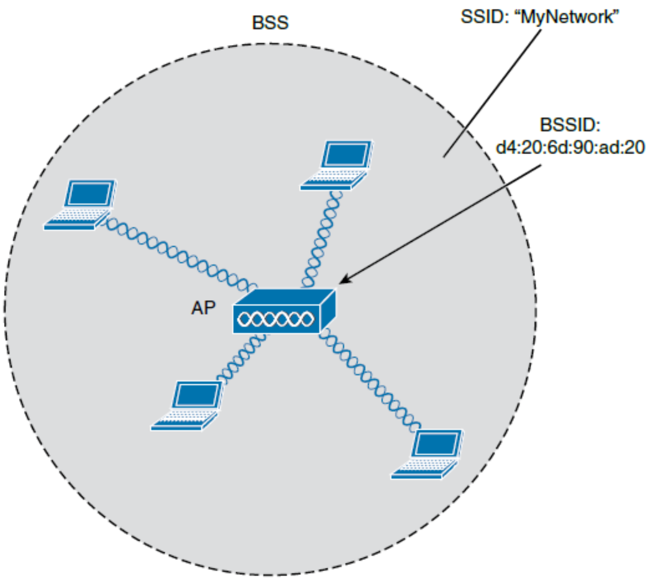


Figure 26-4 *802.11 Basic Service Set*

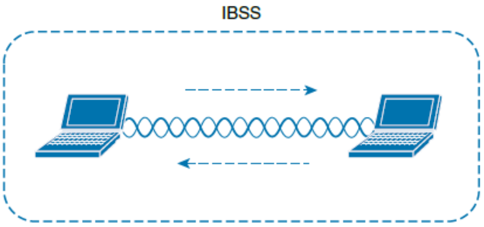


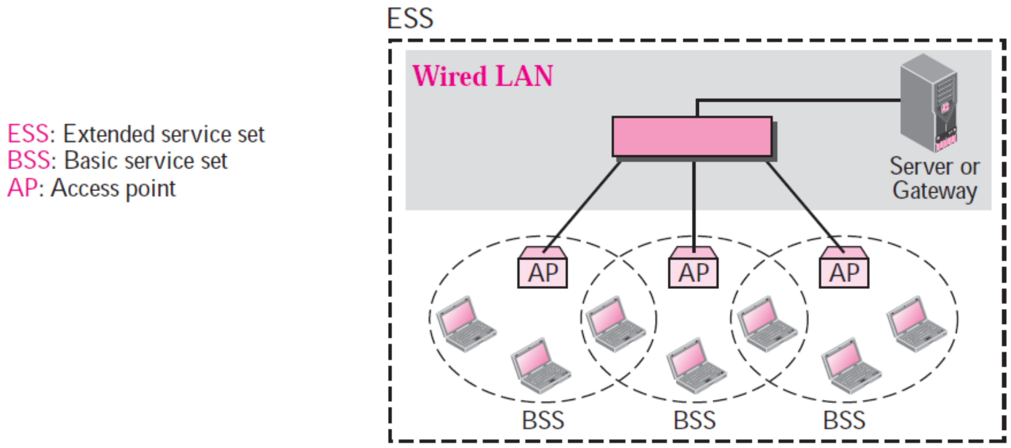
Figure 26-9 *802.11 Independent Basic Service Set*

A BSS without an AP is called an ad hoc network; a BSS with an AP is called an infrastructure network.

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:

1. **mobile**. The mobile stations are normal stations inside a BSS.
2. **stationary** The stationary stations are AP stations that are part of a wired LAN.



Station Types

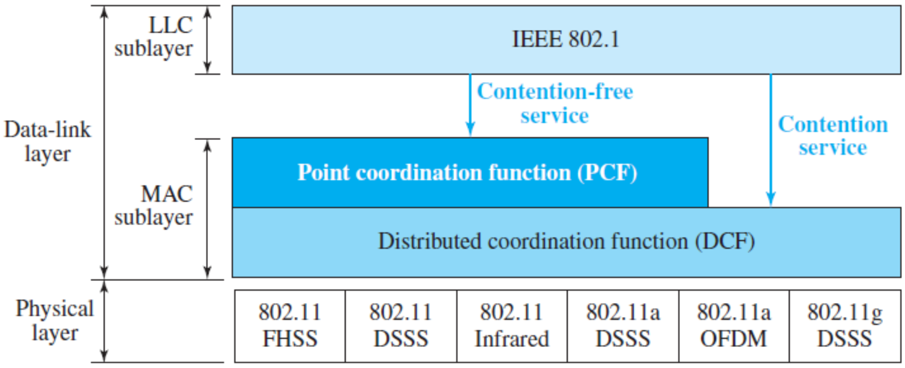
IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: **no-transition, BSS-transition, and ESS-transition mobility.**

1. A station with no-transition mobility is either stationary or moving only inside a BSS.
2. A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
3. A station with ESS-transition mobility can move from one ESS to another.

MAC Sublayer

There are two different MAC sublayers in this protocol,

MAC layers in IEEE 802.11 standard

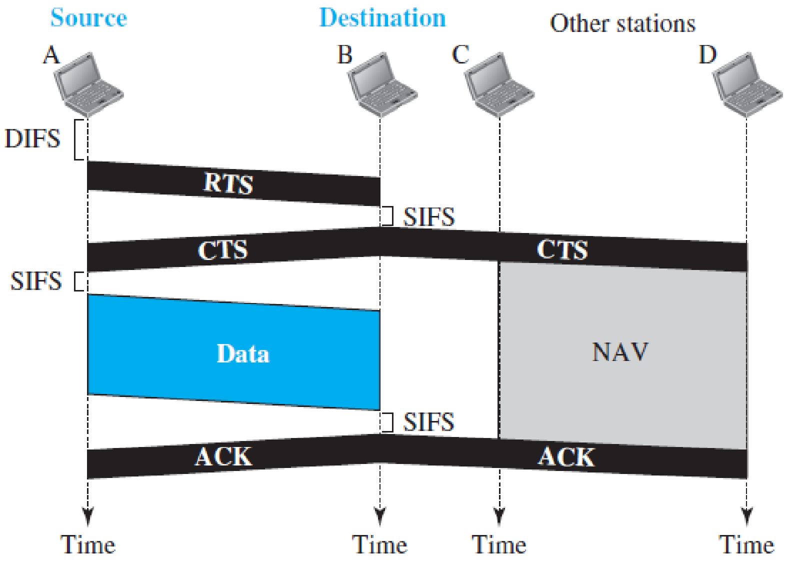


1. **Distributed Coordination Function**

   One of the two protocols defined by IEEE at the MAC sublayer is called the distribute coordination function (DCF). DCF uses CSMA/CA as the access method

   Frame Exchange Time Line.

   station waits for a period called **the distributed interframe space (DIFS)**; then the station sends a control frame called **the request to send** (RTS). After receiving the RTS and waiting a period called the **short interframe space (SIFS)**, the destination station sends a control frame, called the **clear to send (CTS)** to the source station.



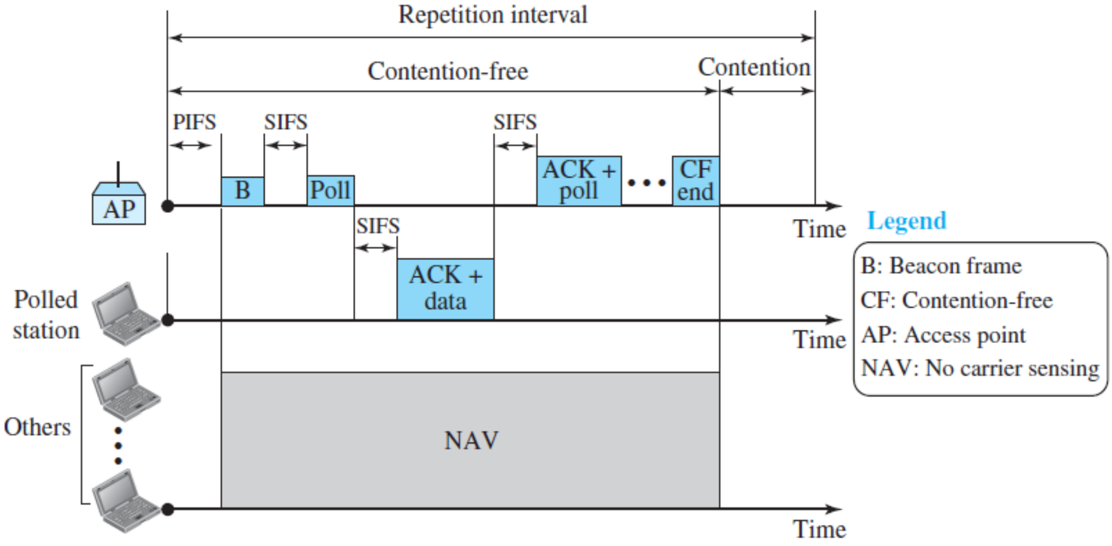
Network Allocation Vector

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a *network allocation vector* (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.

2. **Point Coordination Function (PCF)**

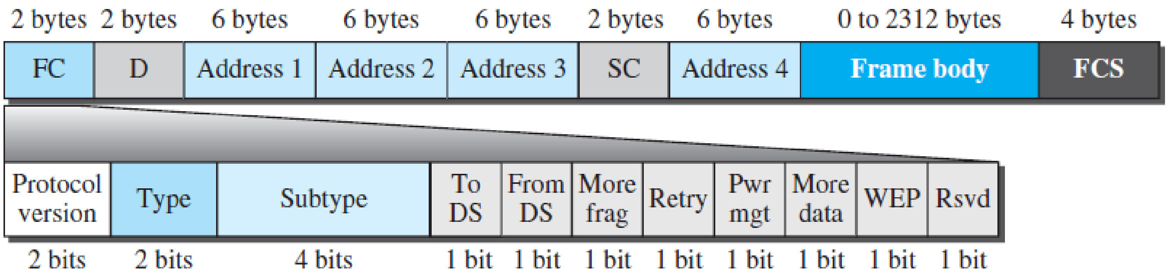
The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium. To prevent this, a repetition interval has been designed to cover both contention-free PCF and contention-based DCF traffic. **The repetition interval**, which is repeated continuously, starts with a special control frame, called a **beacon frame**. When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval. Figure 15.8 shows an example of a repetition interval.



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.

D. This field defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

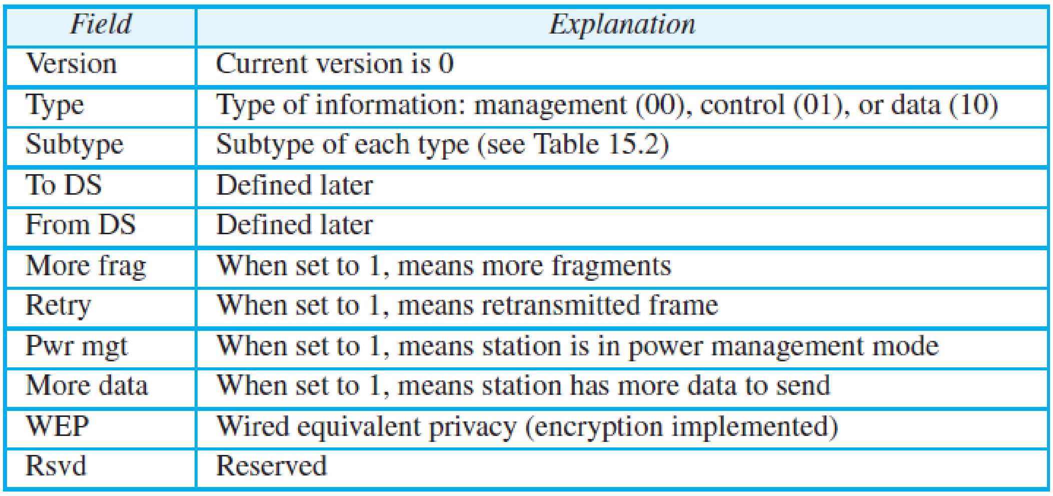
Addresses. There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields.

Sequence control. This field, often called the SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

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.

Table 15.1 *Subfields in FC field*



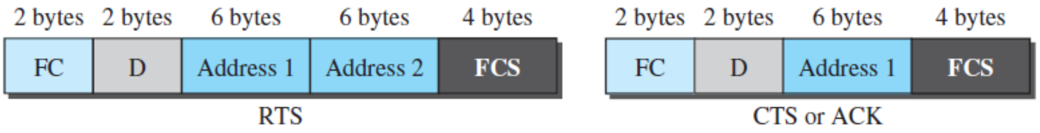
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 15.2)
To DS	Defined later
From DS	Defined later
More frag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr 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

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data 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.

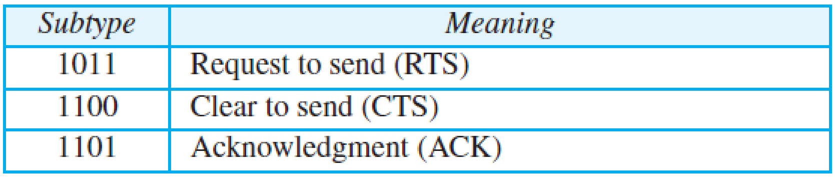


RTS

CTS or ACK

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

Table 15.2 *Values of subtype fields in control frames*

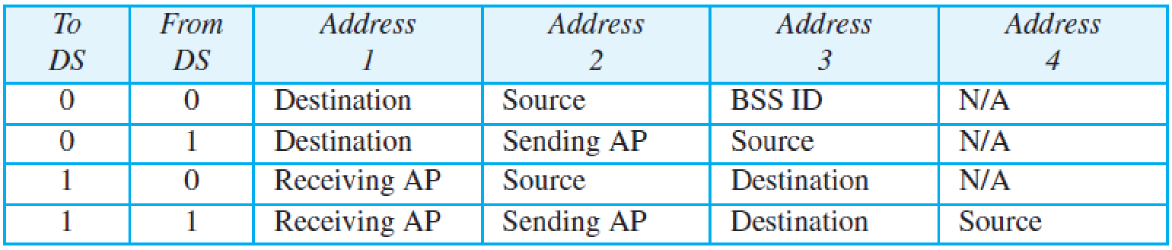


Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Addressing Mechanism

The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and from DS. Each flag can be either 0 or 1, resulting in four different situations. The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags.

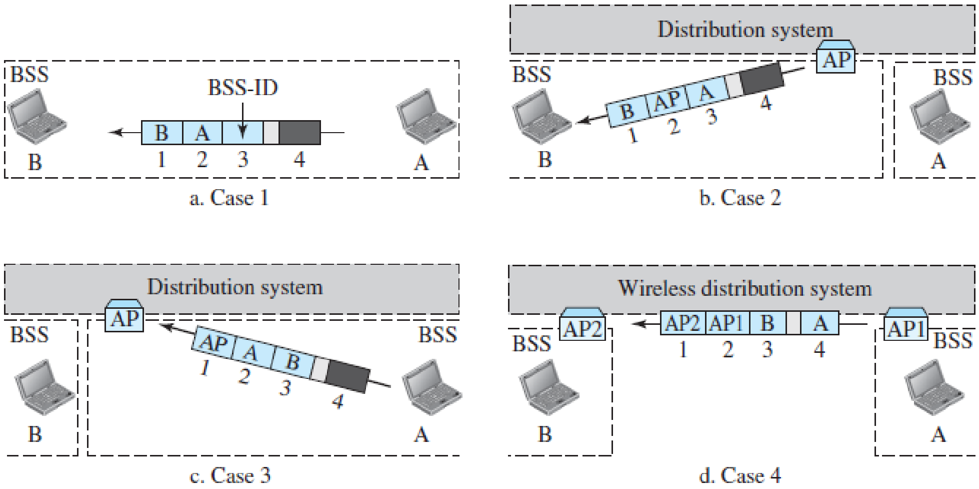
Table 15.3 *Addresses*



To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

1. **Address 1** is always the address of the next device that the frame will visit.
2. **Address 2** is always the address of the previous device that the frame has left.
3. **Address 3** is the address of the final destination station if it is not defined by address 1 or the original source station if it is not defined by address 2.
4. **Address 4** is the original source when the distribution system is also wireless.

- **Case 1: 00** In this case, To DS = 0 and From DS = 0. This means that the frame is not going to a distribution system (To DS = 0) and is not coming from a distribution system (From DS = 0). The frame is going from one station in a BSS to another without passing through the distribution system.
- **Case 2: 01** In this case, To DS = 0 and From DS = 1. This means that the frame is coming from a distribution system (From DS = 1). The frame is coming from an AP and going to a station. Note that address 3 contains the original sender of the frame (in another BSS).
- Case 3: 10 In this case, To DS = 1 and From DS = 0. This means that the frame is going to a distribution system (To DS = 1). The frame is going from a station to an AP. The ACK is sent to the original station. Note that address 3 contains the final destination of the frame in the distribution system.



a. Case 1

b. Case 2

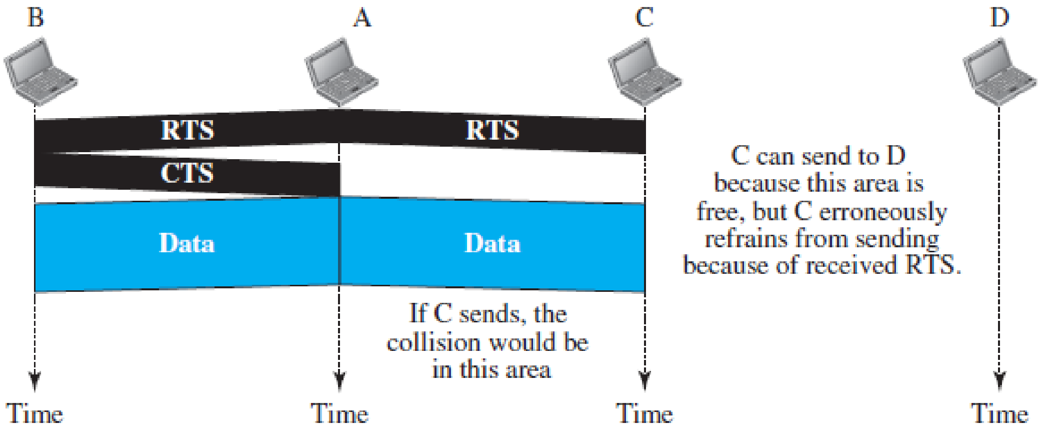
c. Case 3

d. Case 4

- **Case 4: 11** In this case, To DS = 1 and From DS = 1. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system. Here, we need four addresses to define the original sender, the final destination, and two intermediate APs. Figure 15.11 shows the situation.

Exposed Station Problem

In this problem a station refrains from using a channel when it is, in fact, available. In Figure 15.12, 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. The handshaking messages RTS and CTS cannot help in this case. Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.


B
A
C
D
RTS
RTS
CTS
Data
Data
C can send to D because this area is free, but C erroneously refrains from sending because of received RTS.
If C sends, the collision would be in this area
Time
Time
Time
Time

BLUETOOTH - IEEE 802.15.1

Bluetooth is a short-range and low power wireless technology originally developed for exchanging data over short distances from fixed and mobile devices creating personal area network.

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a short distance from each other. 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.

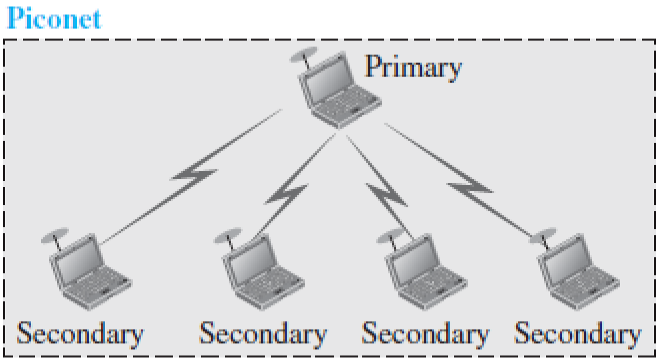
Architecture

Bluetooth defines two types of networks: piconet and scatternet.

Piconets

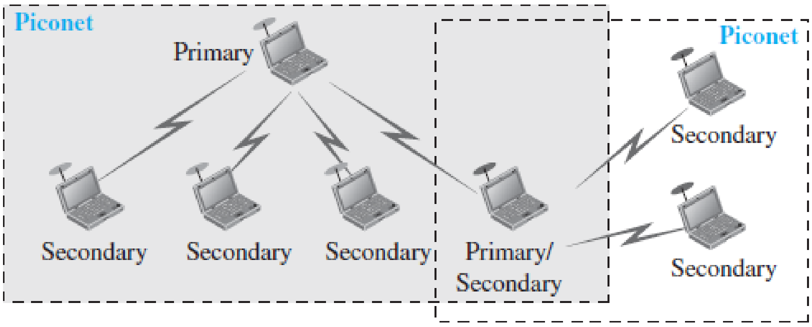
A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the *primary*; the rest are called *secondaries*. All the secondary stations synchronize their clocks and hopping sequence with the primary.

Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state*.



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.



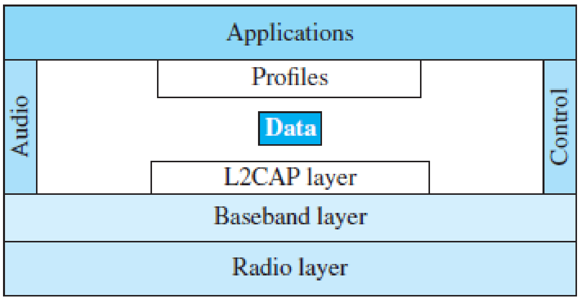
Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth.

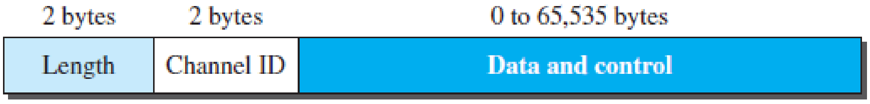
Bluetooth Layers

L2CAP

The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCO channels do not use L2CAP. Figure 15.20 shows the format of the data packet at this level.



L2CAP data packet format



Multiplexing

The L2CAP can do multiplexing. At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer. At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.

Segmentation and Reassembly

The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes. This includes 4 bytes to define the packet and packet length. Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes. The L2CAP segments the packets at the source and reassembles them at the destination.

QoS

Bluetooth allows the stations to define a quality-of-service level.

Group Management

Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves. This is similar to multicasting.

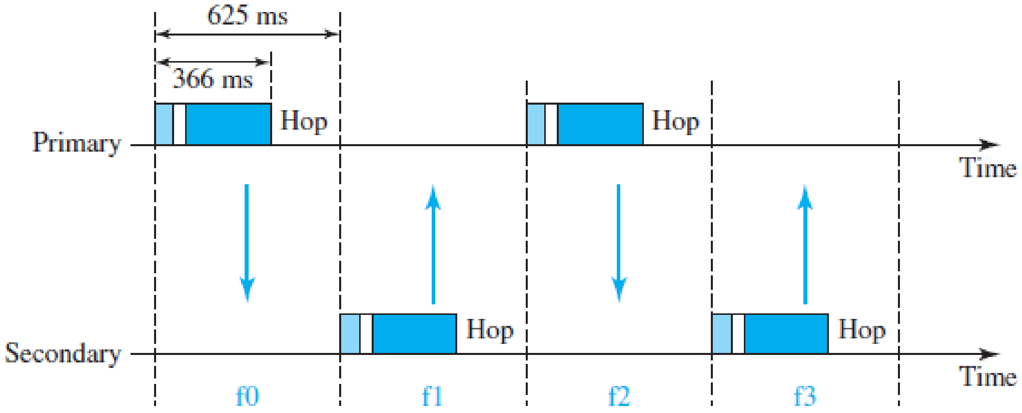
Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA (discussed later). The primary and secondary stations communicate with each other using time slots.

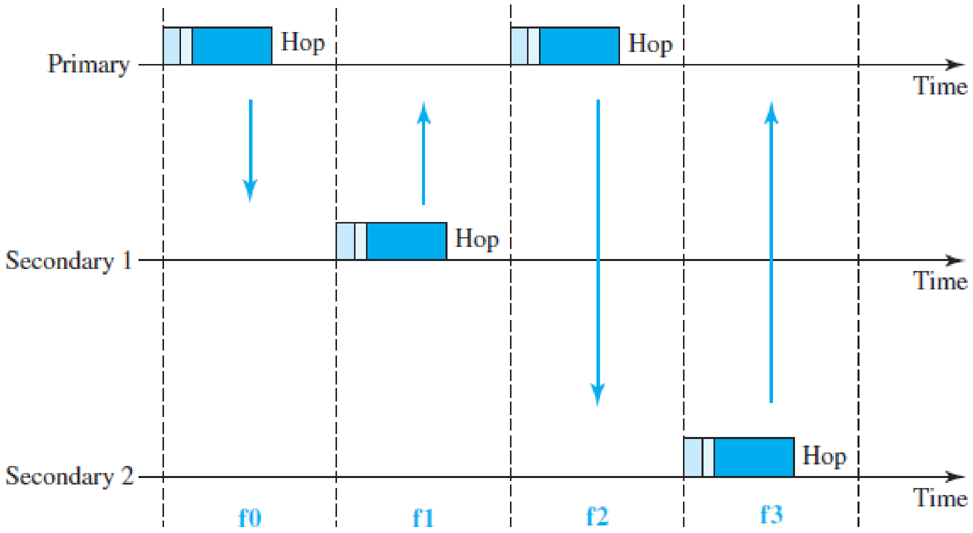
TDMA

Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the sender and receiver send and receive data, but not at the same time (half-duplex); however, the communication for each direction uses different hops. This is like walkie-talkies using different carrier frequencies.

- **Single-Secondary Communication** If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 µs. The primary uses even-numbered slots (0, 2, 4, . . .); the secondary uses odd-numbered slots (1, 3, 5, . . .).



- **Multiple-Secondary Communication** The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.



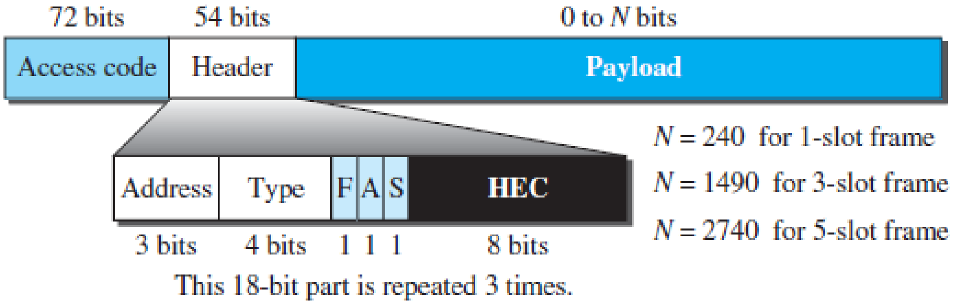
Frame Format

A frame in the baseband layer can be one of three types: **one-slot, three-slot, or five-slot**. A slot, as we said before, is 625 µs.

a one-slot frame exchange, 259 µs is needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 µs.

three-slot frame occupies three slots. However, since 259 µs is used for hopping, the length of the frame is 3 × 625 − 259 = 1616 µs or 1616 bits.

A five-slot frame also uses 259 bits for hopping. The length of the frame is 5 × 625 − 259 = 2866 bits.



- **Access code.** This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.
- **Header**. This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
    a. 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.
    b. Type. The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.
    c. 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).
    d. A. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ;
    e. S. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ;
    f. HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.
- **Payload.** This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.

Modulation To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering.

POINT-TO-POINT WANS

A second type of network we encounter in the Internet is the point-to-point wide area network. A point-to-point WAN connects two remote devices using a line available from a public network such as a telephone network. We discuss traditional modem technology, DSL line, cable modem, T-lines, and SONET.

65K Modems, DSL Technology, Cable Modem

T Lines, SONET, PPP

Switched WANS

The backbone networks on the Internet can be switched WANs. A switched WAN is a wide area network that covers a large area (a state or a country) and provides access at several points to the users. Inside the network, there is a *mesh of point-to-point networks that connects switches.*

The switches, multiple port connectors, allow the connection of several inputs and outputs.

Comparison of LAN and WAN

- First, instead of a star topology, switches are used to create multiple paths.
- Second, LAN technology is considered a **connectionless technology**; there is no relationship between packets sent by a sender to a receiver.
- Switched WAN technology, on the other hand, is a **connection-oriented technology**. Before a sender can send a packet, a connection must be established between the sender and the receiver.
- After the connection is established, it is assigned an identifier (sometimes called a label) used during the transmission. The connection is formally terminated when the transmission is over.
- The connection identifier is used instead of the source and destination addresses in LAN technology.

X.25

The X.25 protocol, introduced in the 1970s. It was mostly used as a public network to connect individual computers or LANs. It provides an end-to-end service. X.25, which was designed before the Internet, is a three-layer protocol; it has its own network layer. IP packets had to be encapsulated in an X.25 network-layer packet to be carried from one side of the network to another.

X.25 performs extensive error control. This makes transmission very slow and is not popular given the ever-increasing demand for speed.

The functionality of X.25 is specified on three levels:

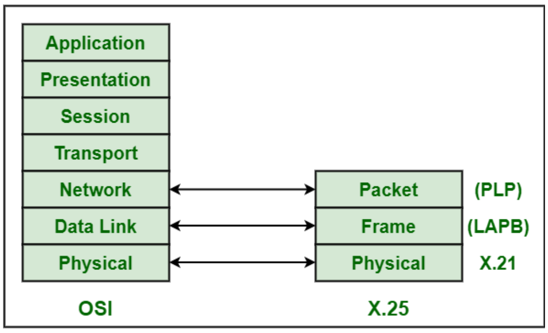
- Physical level
- Link level
- Packet level

The physical level deals with the physical interface between an attached station (computer, terminal) and the link that attaches that station to the packet-switching node.

The link level provides for the reliable transfer of data across the physical link, by transmitting the data as a sequence of frames.

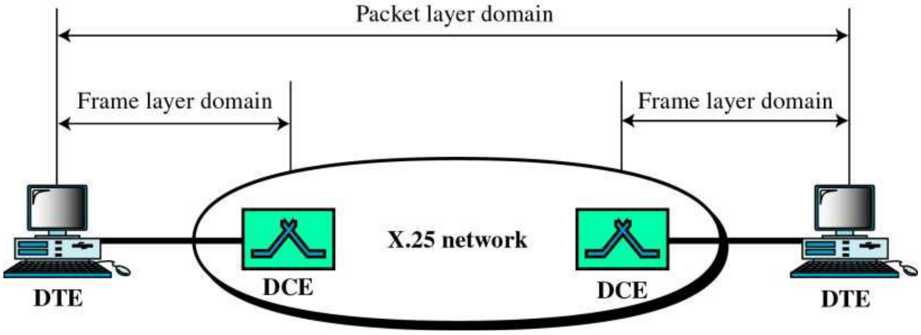
The packet level provides a virtual circuit service. This service enables any subscriber to the network to set up logical connections, called virtual circuits, to other subscribers.

The term **virtual circuit** refers to the logical connection between two stations through the network; this is perhaps best termed an external virtual circuit. Earlier, we used the term virtual circuit to refer to a specific preplanned route through the network between two stations; this could be called an internal virtual circuit.



X.25 Layer Mapping with OSI Model

- X.25 defines how a node terminal could be interfaced to the network for communication in Packet Mode.
- Key terms used here are: **DTE** and **DCE** node
- It defines how DTE's communicates with network and how packets are sent over that network using DCEs.
- It is also known as SUBSCRIBER NETWORK INTERFACE(SNI) PROTOCOL.



Limitation to X.25 protocol

It does not explicitly define what type of addressing should be used during call set-up to access a remote DTE.

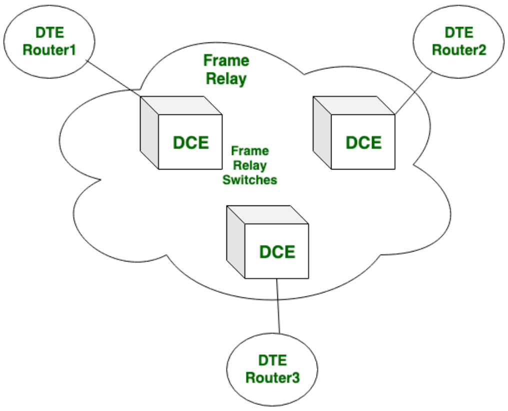
- It operates at low data rate of 64kbps.
- Links used for data and control exchange were highly erroneous.
- To transfer a single packet, many F&E control packets were needed.
- It does not support burst nature of data.

Frame Relay

The Frame Relay protocol, a switched technology that provides low-level (physical and data link layers) service, was designed to replace X.25. Frame Relay has some advantages over X.25:

It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends.

- High Data Rate.
- Burst Data.
- Less Overhead Due to Improved Transmission Media.



Frame relay layers

Frame relay has only two layers i.e. physical layer and data link layer.

Physical layer

- Frame relay supports ANSI standards.
- No specific protocol is defined for the physical layer. The user can use any protocol which is recognized by ANSI.

Data link layer

- A simplified version of HDLC is employed by the frame relay at the data link layer.
- A simpler version is used because flow control and error correction is not needed in frame relay.

ATM

Asynchronous Transfer Mode (ATM) is the cell relay protocol designed by the ATM Forum and adopted by the ITU-T.

Design Goals

Among the challenges faced by the designers of ATM, six stand out.

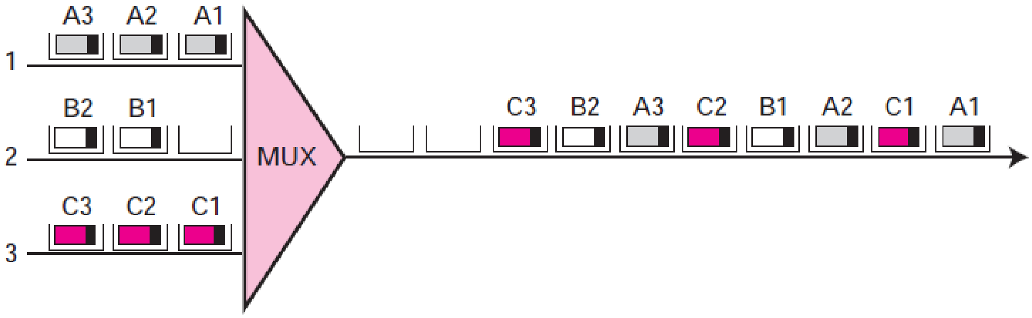
- First and foremost is the need for a transmission system to optimize the use of high-data-rate transmission media, in particular optical fiber.
- Second is the need for a system that can interface with existing systems, such as the various packet networks, and provide wide area interconnectivity between them without lowering their effectiveness or requiring their replacement.
- Third is the need for a design that can be implemented inexpensively so that cost would not be a barrier to adoption.
- Fourth, the new system must be able to work with and support the existing telecommunications hierarchies.
- Fifth, the new system must be connection-oriented to ensure accurate and predictable delivery.
- And last but not least, one objective is to move as many of the functions to hardware as possible (for speed) and eliminate as many software functions as possible (again for speed).

Cell Networks

ATM is a cell network. A cell network uses the cell as the basic unit of data exchange. A cell is defined as a small, fixed-size block of information.

Asynchronous TDM

ATM uses asynchronous time-division multiplexing—that is why it is called Asynchronous Transfer Mode—to multiplex cells coming from different channels.

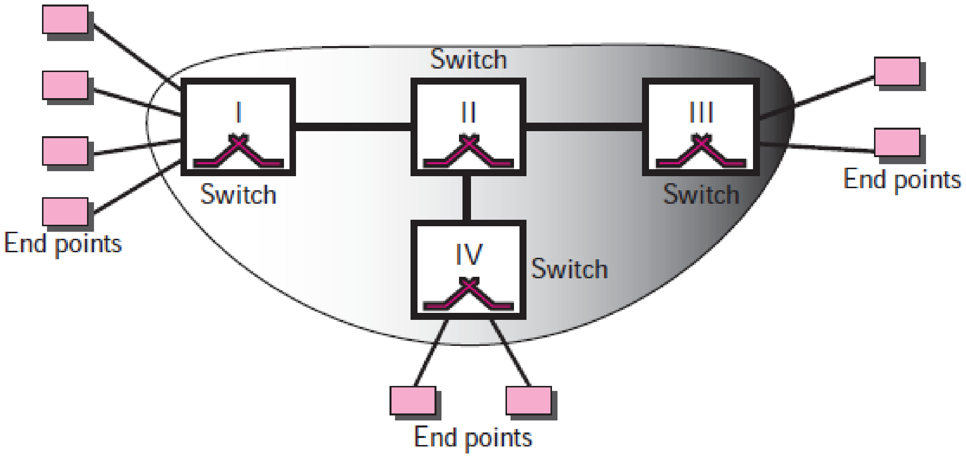


ATM Architecture

ATM is a switched network. The user access devices, called the end points, are connected to the switches inside the network. The switches are connected to each other using high-speed communication channels.

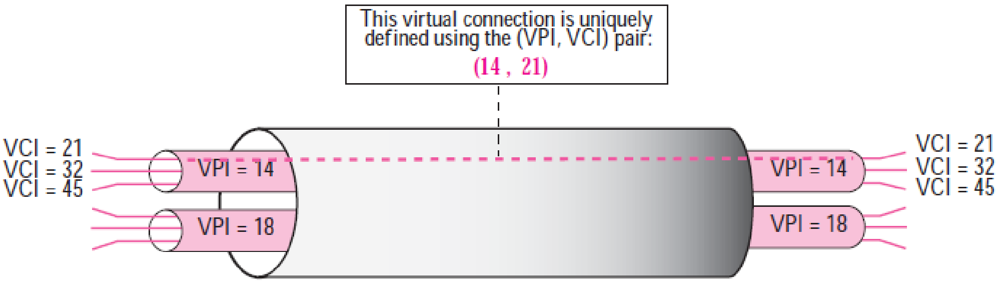
Virtual Connection: Connection between two end points is accomplished through transmission paths (TPs), virtual paths (VPs), and virtual circuits (VCs). A transmission path (TP) is the physical connection (wire, cable, satellite, and so on) between an end point and a switch or between two switches.

Architecture of an ATM network



A virtual path (VP) A transmission path is divided into several virtual paths. A virtual path (VP) provides a connection or a set of connections between two switches.

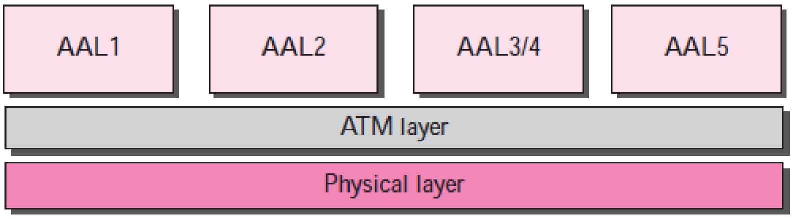
Virtual circuits (VCs) Cell networks are based on virtual circuits (VCs). All cells belonging to a single message follow the same virtual circuit and remain in their original order until they reach their destination.



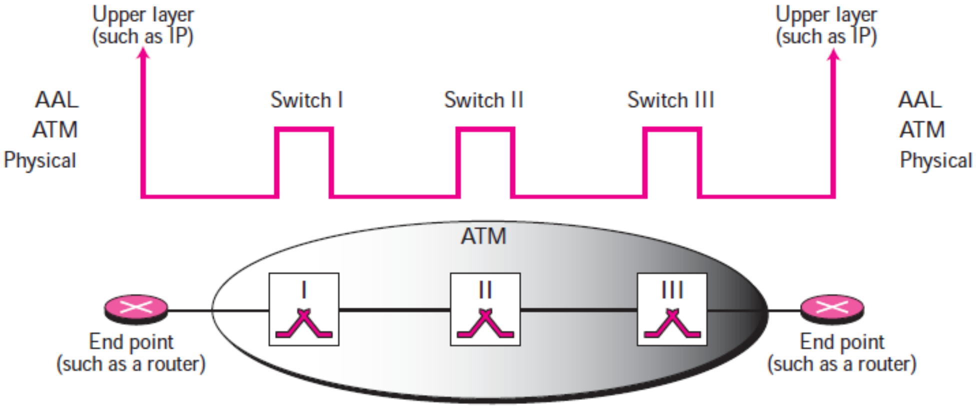
A virtual connection is defined by a pair of numbers: the VPI and the VCI. a virtual path identifier (VPI) and a virtual circuit identifier (VCI). The VPI defines the specific VP and the VCI defines a particular VC inside the VP.

ATM Layers

The ATM standard defines three layers. They are, from top to bottom, the application adaptation layer, the ATM layer, and the physical layer.



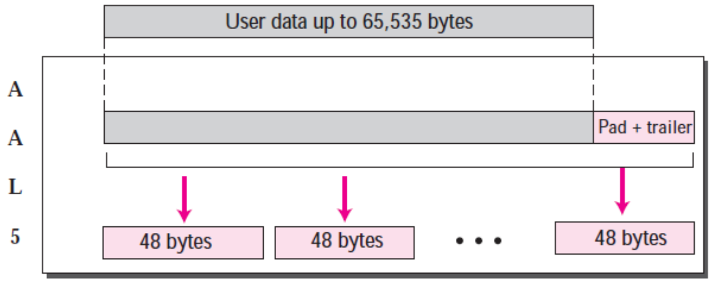
Use of the layers



AAL Layer

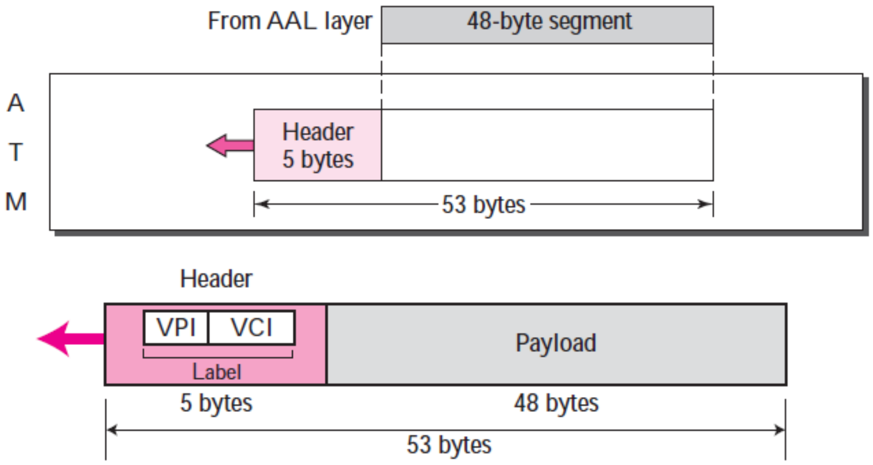
The application adaptation layer (AAL) allows existing networks (such as packet networks) to connect to ATM facilities. AAL protocols accept transmissions from upper-layer services (e.g., packet data) and map them into fixed-sized ATM cells.

AAL5, which is sometimes called the **simple and efficient adaptation layer (SEAL),** assumes that all cells belonging to a single message travel sequentially and that control functions are included in the upper layers of the sending application. The IP protocol uses the AAL5 sublayer.



ATM Layer

The ATM layer provides routing, traffic management, switching, and multiplexing services. It processes outgoing traffic by accepting 48-byte segments from the AAL
sublayer.

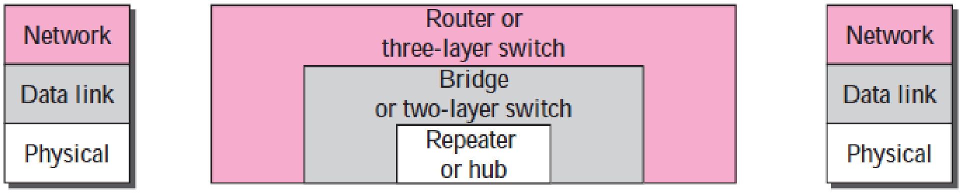


Physical Layer

The physical layer defines the transmission medium, bit transmission, encoding, and electrical to optical transformation.

CONNECTING DEVICES

LANs or WANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect LANs and WANs together we use connecting devices. Connecting devices can operate in different layers of the Internet model. We discuss three kinds of connecting devices: repeaters (or hubs), bridges (or two-layer switches), and routers (or three-layer switches).



Repeaters

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern. The repeater then sends the refreshed signal. A repeater forwards every bit; it has no filtering capability.

Bridges

A bridge operates in both the physical and the data link layers. As a physical-layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the MAC addresses (source and destination) contained in the frame. A bridge has a table used in filtering decisions.

Two-Layer Switch

When we use the term switch, we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates.

Routers

A router is a three-layer device; it operates in the physical, data link, and network layers. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the router checks the physical addresses (source and destination) contained in the packet. As a network layer device, a router checks the network layer addresses (addresses in the IP layer). Note that bridges change collision domains, but routers limit broadcast domains.

A repeater or a bridge connects segments of a LAN. A router connects independent LANs or WANs to create an internetwork (internet).

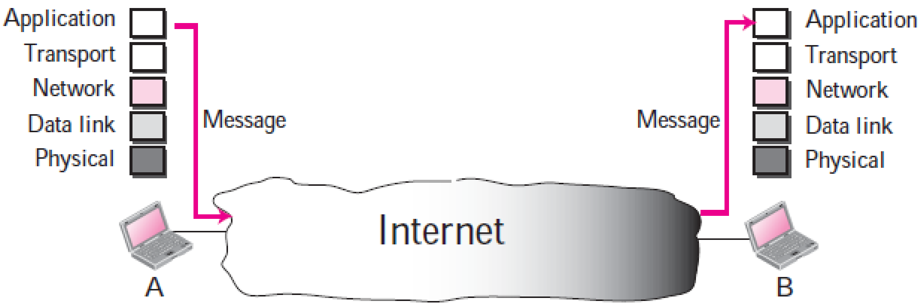
Three-Layer Switch

A three-layer switch is a router; a router with an improved design to allow better performance.

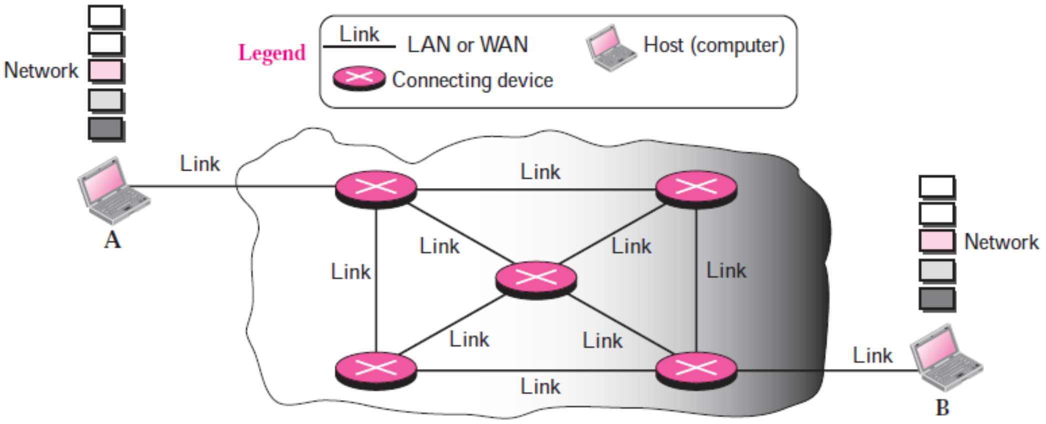
The network Layer

The network layer is responsible for host-to-host delivery and for routing the packets through the routers.

At the conceptual level, we can think of the global Internet as a black box network that connects millions (if not billions) of computers in the world together. At this level, we are only concerned that a message from the application layer in one computer reaches the application layer in another computer.



The Internet, however, is not one single network; it is made of many networks (or links) connected through the connecting devices. In other words, the Internet is an internetwork, a combination of LANs and WANs.



An internet as a combination of links and connecting devices

Packetizing

The first duty of the network layer is packetizing: encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

- The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and some other information that is required by the network-layer protocol (as discussed later) and delivers the packet to the data-link layer.
- The destination host receives the network-layer packet from its data-link layer, decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.

Routing and Forwarding

Other duties of the network layer, which are as important as the first, are routing and forwarding, which are directly related to each other.

Routing

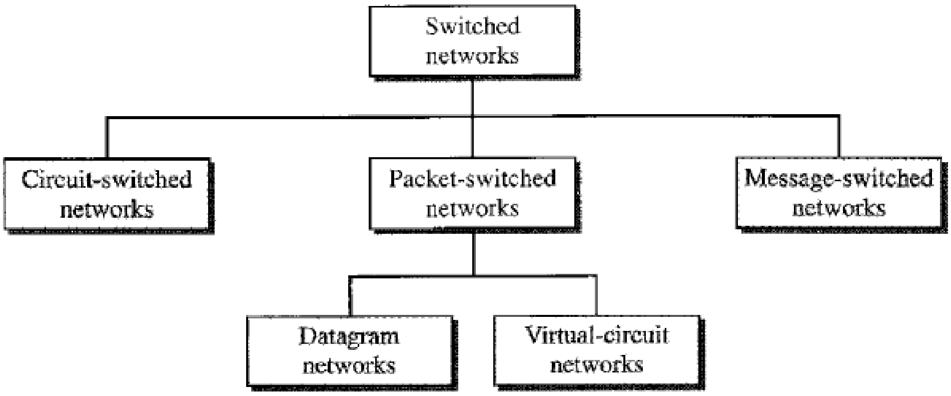
The network layer is responsible for routing the packet from its source to the destination. A physical network is a combination of networks (LANs and WANs) and routers that connect them. The network layer needs to have some specific strategies for defining the best route.

Forwarding

If routing is applying strategies and running some routing protocols to create the decision-making tables for each router, forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces. The decision-making table a router normally uses for applying this action is sometimes called the forwarding table and sometimes the routing table.

SWITCHING

When a message reaches a connecting device, a decision needs to be made to select one of the output ports through which the packet needs to be send out. In other words, the connecting device acts as a switch that connects one port to another port.



Message Switching

Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced. In message switching, end-users communicate by sending and receiving messages that included the entire data to be shared. Messages are the smallest individual unit.

Also, the sender and receiver are not directly connected. There are a number of intermediate nodes that transfer data and ensure that the message reaches its destination.

Circuit Switching

One solution to the switching is referred to as circuit switching, in which a physical circuit (or channel) is established between the source and destination of the message before the delivery of the message. [After the circuit is established, the entire message, is transformed from the source to the destination. The source can then inform the network that the transmission is complete, which allows the network to open all switches and use the links and connecting devices for another connection. The circuit switching was never implemented at the network layer; it is mostly used at the physical layer.]

Packet Switching

The second solution to switching is called packet switching. The network layer in the Internet today is a packet-switched network. In this type of network, a message from the upper layer is divided into manageable packets and each packet is sent through the network. The source of the message sends the packets one by one; the destination of the message receives the packets one by one. Today, a packet-switched network can use two different approaches to route the packets:

- the datagram approach (Connectionless Service) and
- the virtual circuit approach (Connection Oriented).

PACKET SWITCHING AT NETWORK LAYER

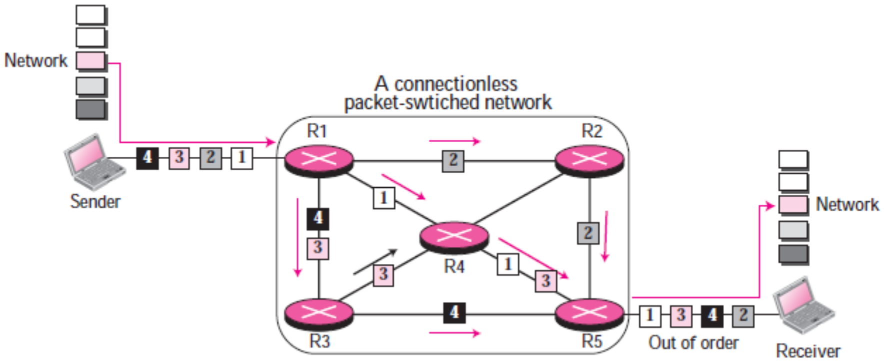
The network layer is designed as a packet-switched network. This means that the packet at the source is divided into manageable packets, normally called datagrams. Individual datagrams are then transferred from the source to the destination. The received datagrams are assembled at the destination before recreating the original message.

Connection Oriented and Connectionless Services

Connection oriented and Connectionless services are the two data transmission services provided by the network layer protocols and transport layer protocols. The Connection oriented services establish a connection prior to sending the packets belonging to the same message from source to the destination. On the other hand, the connectionless service considers each packet belonging to the same message as a different & independent entity and route them with a different path.

Connectionless Service – Datagram Approach

In Connectionless service the network layer protocol treats each packet independently, with each packet having no relationship to any other packet. The packets in a message may or may not travel the same path to their destination.

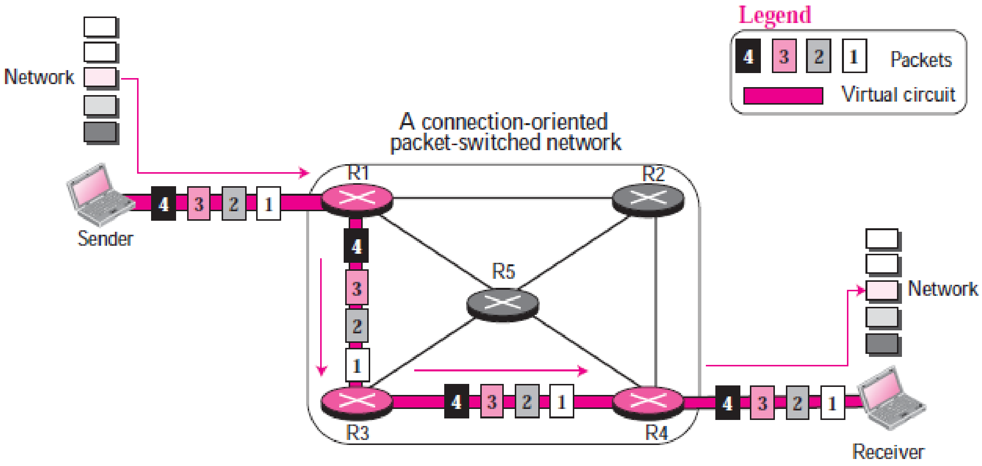


When the network layer provides a connectionless service, each packet traveling on the Internet is an **independent entity**; there is **no relationship** between packets belonging to the same message. *The switches in this type of network are called routers.*

In a connectionless packet-switched network, the forwarding decision is based on the destination address of the packet.

Connection-Oriented Service – Virtual Circuit Approach

In a connection-oriented service, there is a relation between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can follow the same path. In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.



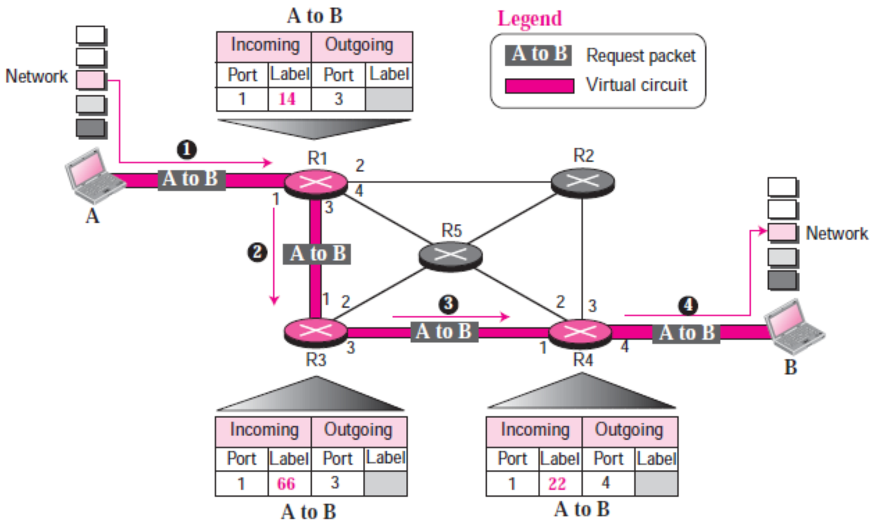
To create a connection-oriented service, a three-phase process is used: **setup, data transfer, and teardown.** In the setup phase, the source and destination address of the sender and receiver is used to make table entries for the connection-oriented service. In the teardown phase, the source and destination inform the router to delete the corresponding entries. Data transfer occurs between these two phases.

In a connection-oriented packet switched network, the forwarding decision is based on the label of the packet.

Setup Phase

In the setup phase, a router creates an entry for a virtual circuit.

Request packet A request packet is sent from the source to the destination. This auxiliary packet carries the source and destination addresses.



A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	

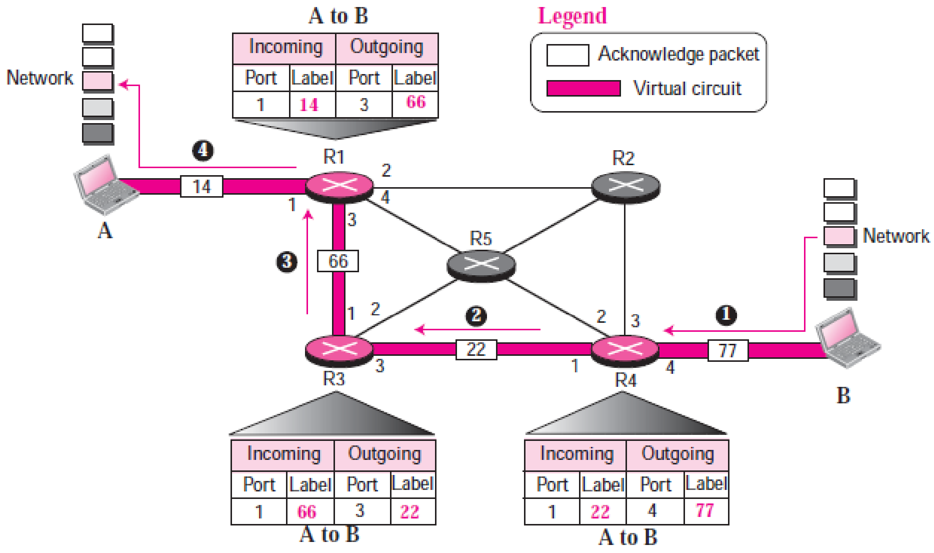
Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	

A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	

A to B

Acknowledgment Packet A special packet, called the acknowledgment packet, completes the entries in the switching tables. Figure 4.9 shows the process.



A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	14	3	66

Incoming		Outgoing	
Port	Label	Port	Label
1	66	3	22

A to B

Incoming		Outgoing	
Port	Label	Port	Label
1	22	4	77

A to B

Data Transfer Phase

The second phase is called the data transfer phase. After all routers have created their routing table for a specific virtual circuit, then the network-layer packets belonging to one message can be sent one after another.

Teardown Phase

In the teardown phase, source A, after sending all packets to B, sends a special packet called a teardown packet. Destination B responds with a confirmation packet. All routers delete the corresponding entry from their tables.

NETWORK LAYER SERVICES

Logical Addressing

Since the network layer provides end-to-end communication, the two computers that need to communicate with each other each need a universal identification system, referred to as network-layer address or logical address.

Services Provided at the Source Computer

The network layer at the source computer provides four services: packetizing, finding the logical address of the next hop, finding the physical (MAC) address of the next hop, and fragmenting the datagram if necessary.

Packetizing

The first duty of the network layer is to encapsulate the data coming from the upper layer in a datagram. This is done by adding a header to the data that contains the logical source and destination address of the packet, information about fragmentation, the protocol ID of the protocol that has requested the service, the data length, and possibly some options.

Finding Logical Address of Next Hop

The network layer at the source computer needs to consult a routing table to find the logical address of the next hop.

Finding MAC Address of Next Hop

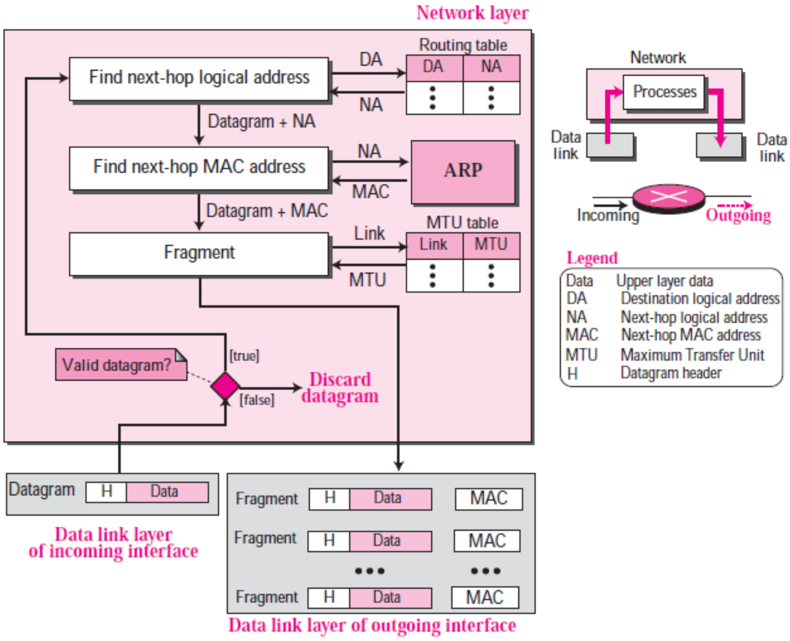
The network layer does not actually deliver the datagram to the next hop; it is the duty of the data link layer to do the delivery. this task has been assigned to another auxiliary protocol called Address Resolution Protocol (ARP) that finds the MAC address of the next hop given the logical address.

Fragmentation

The datagram prepared at the network layer, may be larger than that limit. The datagram needs to be fragmented to smaller units before being passed to the data link layer. Fragmentation needs to preserve the information at the header of the datagram.

Services Provided at Each Router

As we have mentioned before, a router is involved with two interfaces with respect to a single datagram: the incoming interface and the outgoing interface. The network layer at the router, therefore, needs to interact with two data link layers: the data link of the incoming interface and the data link layer of the outgoing interface. The network layer is responsible to receive a datagram from the data link layer of the incoming interface, fragment it if necessary, and deliver the fragments to the data link of the outgoing interface.



Services Provided at the Destination Computer

The network layer at the destination computer is simpler. No forwarding is needed. However, the destination computer needs to assemble the fragments before delivering the data to the destination. After validating each datagram, the data is extracted from each fragment and stored. When all fragments have arrived, the data are reassembled and delivered to the upper layer. The network layer also sets a reassembly timer. If the timer is expired, all data fragments are destroyed, and an error message is sent that all the fragmented datagrams need to be resent.

OTHER NETWORK LAYER ISSUES

Error Control

Error control means including a mechanism for detecting corrupted, lost, or duplicate datagrams. Error control also includes a mechanism for correcting errors after they have been detected. The network layer in the Internet does not provide a real error control mechanism

Flow Control

Flow control regulates the amount of data a source can send without overwhelming the receiver. No flow control is provided for the current version of Internet network layer.

Congestion Control

Another issue in a network layer protocol is congestion control. Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet. Congestion may occur if the number of datagrams sent by source computers are beyond the capacity of the network or routers.

Congestion Control in a Connectionless Network

There are several ways to control congestion in a connectionless network. One solution is referred to as signaling. In backward signaling a bit can set in the datagram moving in the direction opposite to the congested direction to inform the sender that congestion has occurred and the sender needs to slow down the sending of packets.

Congestion in a connectionless network can also be implemented using a choke packet, a special packet that can be sent from a router to the sender when it encounters congestion. This mechanism, in fact, is implemented in the Internet network layer. The network layer uses an auxiliary protocol, ICMP, which we discuss in Chapter 9. When a router is congested, it can send an ICMP packet to the source to slow down.

Congestion Control in a Connection-Oriented Network

It is sometimes easier to control congestion in a connection-oriented network than in a connectionless network. One method simply creates an extra virtual circuit when there is a congestion in an area. This, however, may create more problems for some routers. A better solution is advanced negotiation during the setup phase. The sender and the receiver may agree to a level of traffic when they setup the virtual circuit.

Quality of Service

As the Internet has allowed new applications such as multimedia communication (real-time communication of audio and video), the quality of service (QoS) of the communication has become more and more important.

Routing

A very important issue in the network layer is routing; how a router creates its routing table to help in forwarding a datagram in a connectionless service or helps in creating a virtual circuit, during setup phase, in a connection-oriented service. This can be done by routing protocols, that help hosts, and routers make their routing table, maintain them, and update them.

Security

Another issue related to the communication at the network layer is security.