MODULE 3

Wireless LANs

INTRODUCTION

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.,

Architectural Comparison

1. ***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). In a very rare situation, we may be able to create a point-to-point communication between two wireless hosts by using a very limited bandwidth and two-directional antennas.

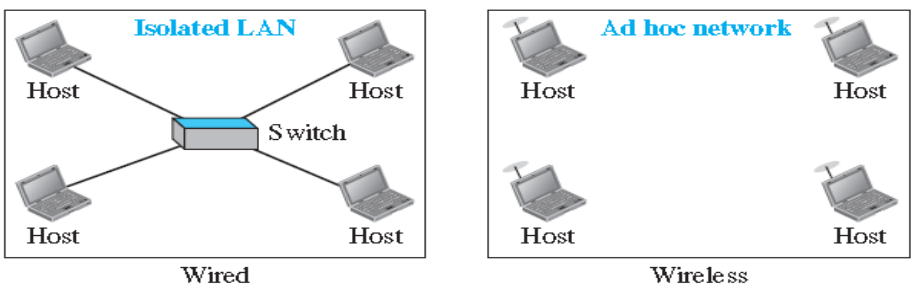
2. Hosts

In a wired LAN, a host is always connected to its network at a point with a fixed linklayer address related to its network interface card (NIC). Of course, a host can move from one point in the Internet to another point. In this case, its link-layer address remains the same, but its network-layer address will change. However, before the host can use the services of the Internet, it needs to be physically connected to the Internet. In a wireless LAN, a host is not physically connected to the network; it can move freely and can use the services provided by the network

3. Isolated LANs

A wired isolated LAN is a set of hosts connected via a link-layer switch. A wireless isolated LAN, called an ***ad hoc network in wireless*** LAN terminology, is a set of hosts that communicate freely with each other. The concept of a link-layer switch does not exist in wireless LANs.

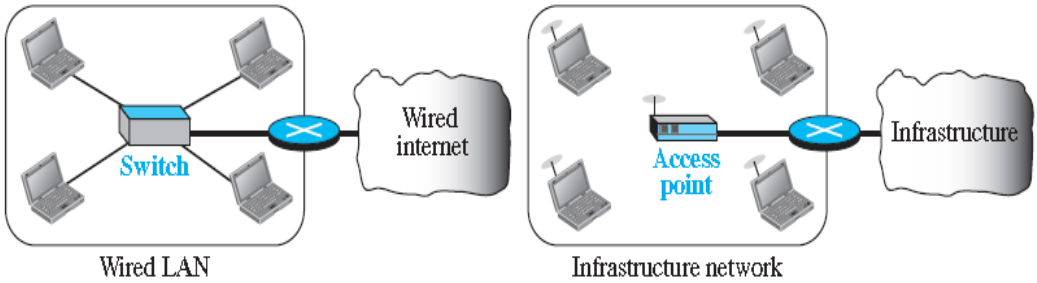
15.1 *Isolated LANs: wired versus wireless*



4. Connection to Other Networks

A wired LAN can be connected to another network or an internetwork such as the Internet using a router. A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN.

Figure 15.2 *Connection of a wired LAN and a wireless LAN to other networks*



5. Moving between Environments

In order to move from the wired environment to a wireless environment we need to change the network interface cards designed for wired environments to the ones designed for wireless environments. We replace the link-layer switch with an access point. In this change, the link-layer addresses will change but the network-layer addresses (IP addresses) will remain the same; we are moving from wired links to wireless links.

Access Control

The most important issue we need to discuss in a wireless LAN is access control. The CSMA/CD algorithm does not work in wireless LANs for three reasons:

1. To detect a collision, a host needs to send and receive at the same time (sending the frame and receiving the collision signal), which means the host needs to work in a duplex mode. Wireless hosts do not have enough power to do so (the power is supplied by batteries). They can only send or receive at one time.

2. **Hidden station problem,**

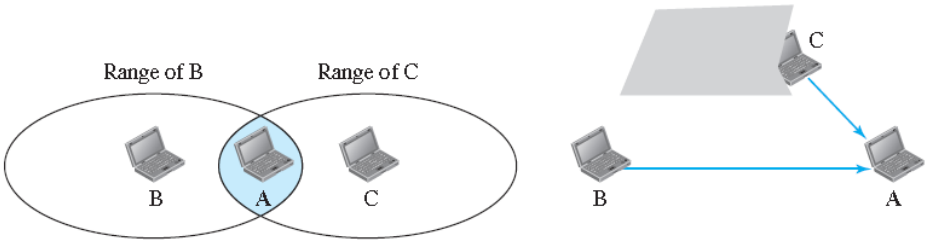
In this a station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected. Hidden stations can reduce the capacity of the network because of the possibility of collision.

3. Since the distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

To overcome the above three problems, Carrier Sense Multiple Access with Collision

Avoidance (CSMA/CA) was invented for wireless LANs

Figure 15.3 *Hidden station problem*



IEEE 802.11 PROJECT

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, It covers the physical and data-link layers. It is sometimes called *wireless Ethernet*.In some countries, including the United States, the public uses the term *WiFi (short for* wireless fidelity) as a synonym for *wireless LAN. However, WiFi is a wireless LAN* that is certified by the WiFi Alliance, a global, non-profit industry association

Architecture

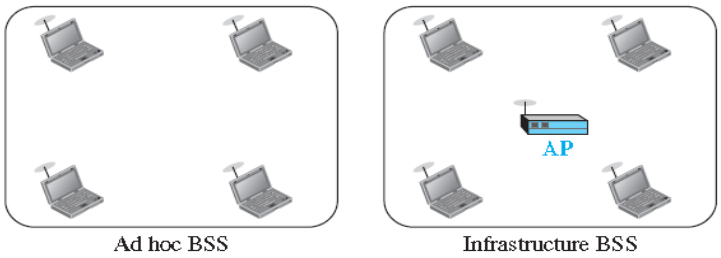
The standard defines two kinds of services:

- 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 blocks 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; A BSS with an AP is sometimes referred to as an *infrastructure BSS.*

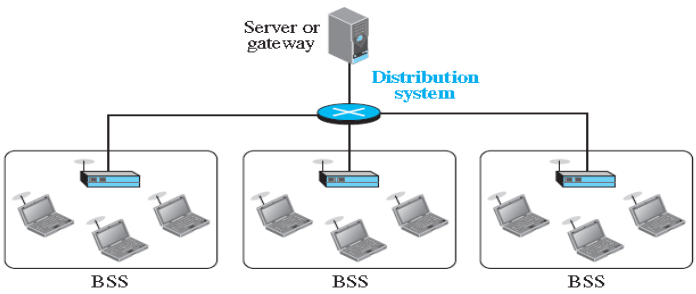
Figure 15.4 *Basic service sets (BSSs)*



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 a wired or a* wireless network. The distribution system connects the APs in the BSSs. 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.

Figure 15.5 *Extended service set (ESS)*



Here the stations within reach of one another can communicate without the use of an AP. However, communication between a station in a BSS and the outside BSS occurs via the AP. The idea is similar to communication in a cellular network .

Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

1. No-transition- is either stationary (not moving) or moving only inside a BSS.

2. BSS-transition- can move from one BSS to another, but the movement is confined inside one ESS.

3. ESS-transition mobility- can move from one ESS to another.

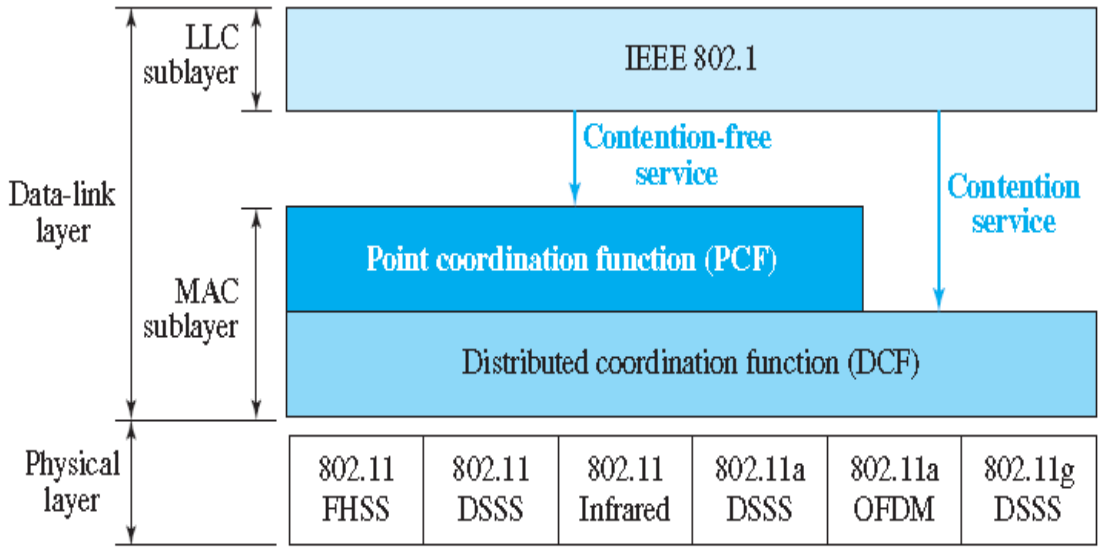
MAC Sublayer

IEEE 802.11 defines two MAC sublayers:

- Distributed Co-ordination Function(DCF)
- Point Co-ordination Function (PCF).

Figure 15.6 shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.

Figure 15.6 *MAC layers in IEEE 802.11 standard*



Distributed Coordination Function

DCF uses CSMA/CA as the access method.

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.

The stations 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.

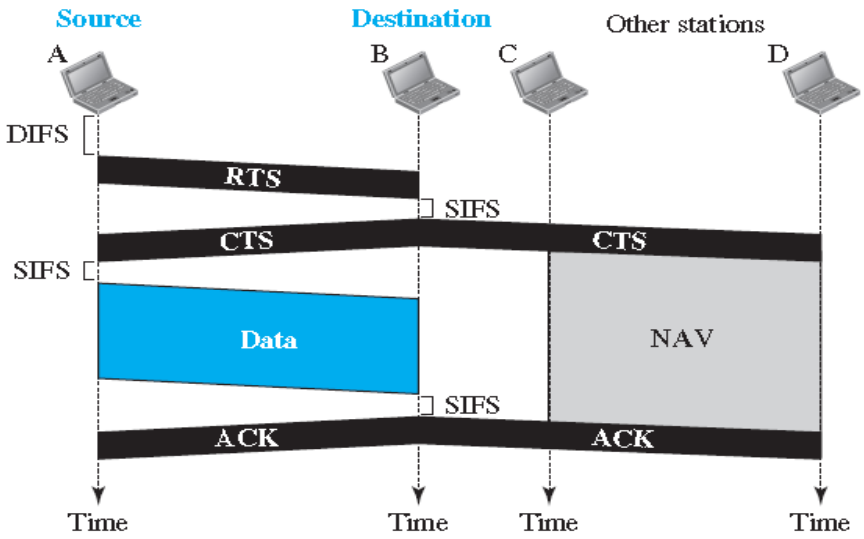
Network Allocation Vector

How is the collision avoidance aspect of this protocol accomplished?

The key is a feature called NAV.

The stations 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. Each time a station accesses the system and sends an CTS frame, other stations start their NAV.

Figure 15.7 *CSMA/CA and NAV*



Collision During Handshaking

What happens if there is a collision during the time when RTS or CTS control frames are in transition, often called the *handshaking period? i.E Two or more stations may try to* send RTS frames at the same time.

These control frames may collide.

However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver. The backoff strategy is employed, and the sender tries again.

Hidden-Station Problem

The solution to the hidden station problem is the use of the handshake frames (RTS and CTS)

Figure 15.7 also shows that the RTS message from A reaches B, 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 A to B, reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

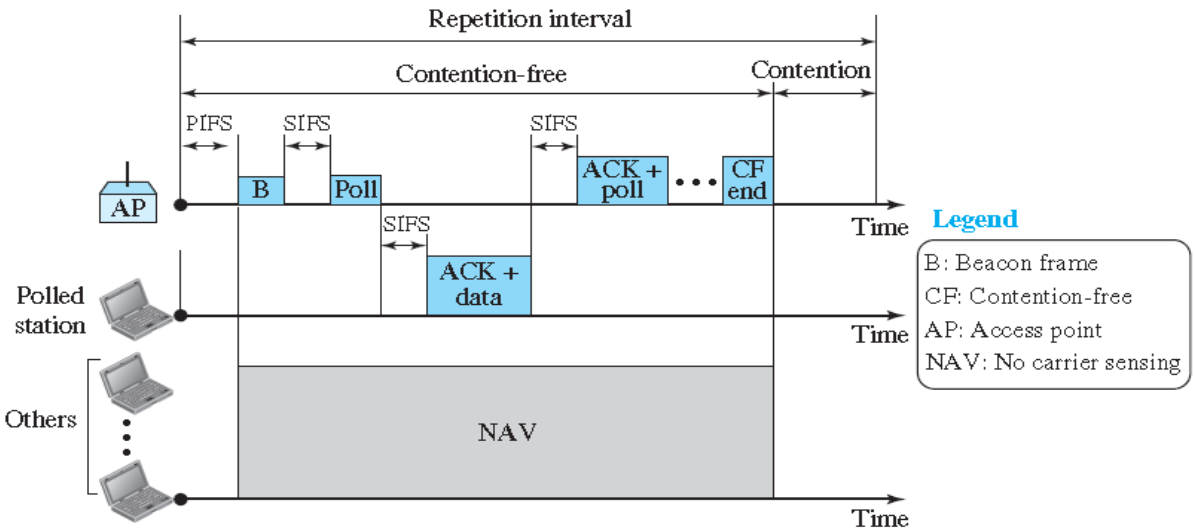
Point Coordination Function (PCF)

The **point coordination function (PCF) is an optional access method that can be** implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission. 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.

To give priority to PCF over DCF, another interframe space, PIFS, has been defined. PIFS (PCF IFS) is shorter than DIFS. This means that if, at the same time, a station wants to use only DCF and an AP wants to use PCF, the AP has priority. 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.

Figure 15.8 *Example of repetition interval*



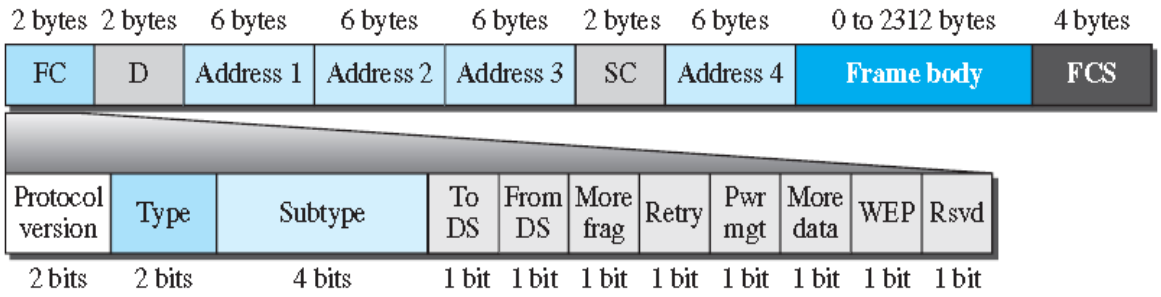
The *repetition interval,* which is repeated continuously, starts with a special control frame, called a ***beacon frame. When the stations hear the beacon frame, they start their NAV for the duration*** of the contention-free period of the repetition interval.During the repetition interval, the PC (point controller) can send a poll frame, receive data, send an ACK, receive an ACK, or do any combination of these (802.11 uses piggybacking). At the end of the contention-free period, the PC sends a CF end (contention-free end) frame to allow the contention-based stations to use the medium.

Fragmentation

The wireless environment is very noisy, so frames are often corrupted. 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

Figure 15.9 *Frame format*



Frame control (FC). The FC field is 2 bytes long and defines the type of frame and some control information.

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

- ***D****. This field defines the duration of the transmission that is used to set the value* of NAV.
- ***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, 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.

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames:

1. Management Frames

Management frames are used for the initial communication between stations and access points.

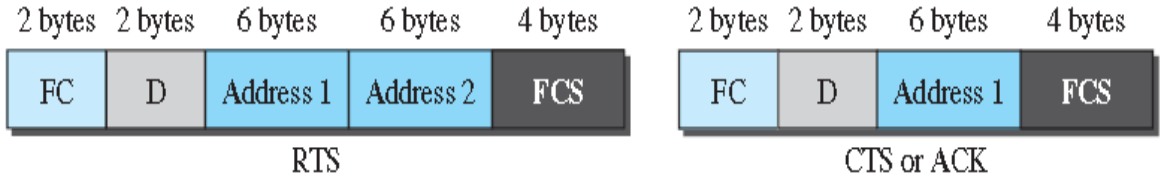
2. Control Frames

Control frames are used for accessing the channel and acknowledging frames.

3. Data Frames

Data frames are used for carrying data and control information.

Figure 15.10 *Control frames*



For control frames the value of the type field is 01; the values of the subtype fields for frames we have discussed are shown in Table 15.2.

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,.

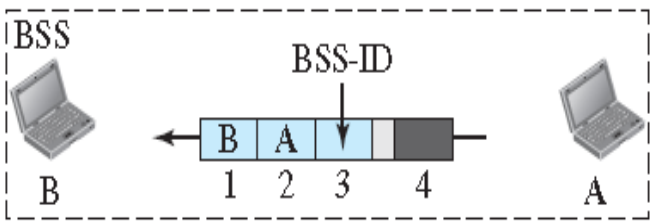
- Address 1 is always the address of the next device that the frame will visit.
- Address 2 is always the address of the previous device that the frame has left.
- Address 3 is the address of the final destination station
- Address 4 is the original source when the distribution system is also wireless.

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

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.



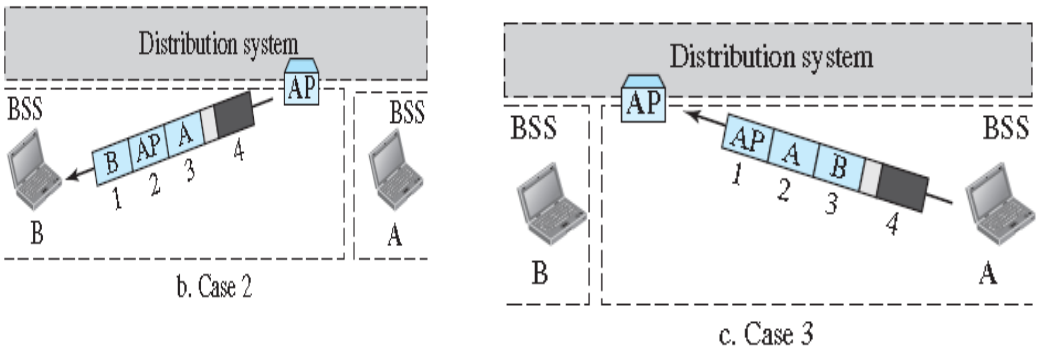
a. Case 1

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.

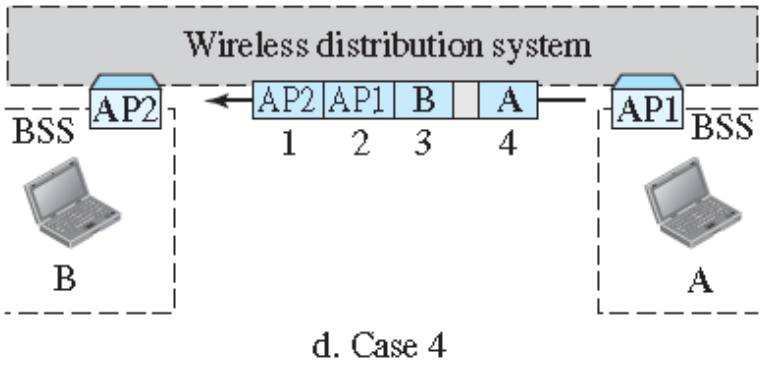
Case 3: 10

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.



Case 4: 11

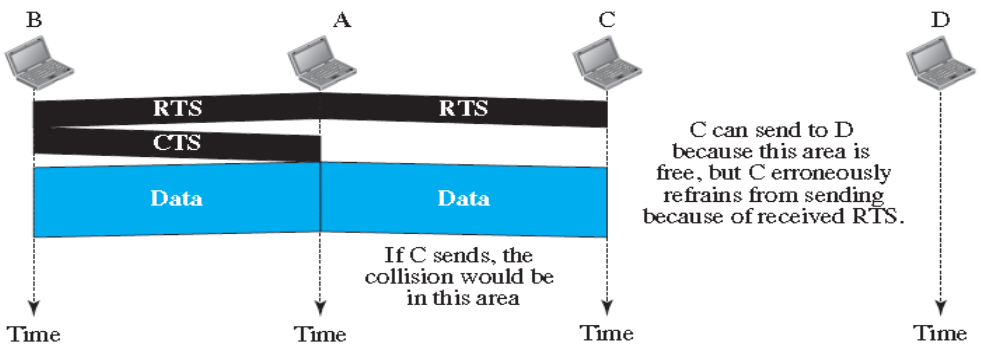
In this case, *To DS = 1 and From DS = 1. This is the case in which the* distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system.



Exposed Station Problem

In this problem a station refrains from using a channel when it is, in fact, available.

Figure 15.12 *Exposed station problem*



Physical Layer

All implementations, except the infrared, operate in the *industrial, scientific, and medical (ISM) band, which defines* three unlicensed bands in the three ranges 902–928 MHz, 2.400–4.835 GHz, and 5.725–5.850 GHz.

Table 15.4 *Specifications*

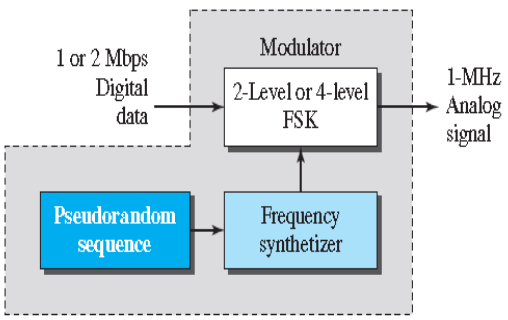
IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

IEEE 802.11 FHSS

IEEE 802.11 FHSS uses the **frequency-hopping spread spectrum (FHSS) method**. FHSS uses the 2.400–4.835 GHz ISM band. The band is divided into 79 subbands of 1 MHz (and some guard bands).

A pseudorandom number generator selects the hopping sequence. The modulation technique in this specification is either two-level FSK or four-level FSK with 1 or 2 bits/baud, which results in a data rate of 1 or 2 Mbps .

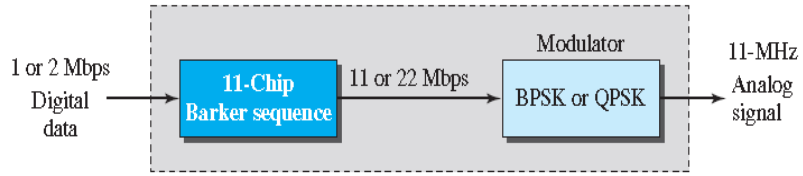
Figure 15.13 *Physical layer of IEEE 802.11 FHSS*



IEEE 802.11 DSSS

IEEE 802.11 DSSS uses the **direct-sequence spread spectrum (DSSS) method.** DSSS uses the 2.400–4.835 GHz ISM band. The modulation technique in this specification is PSK at 1 Mbaud/s. The system allows 1 or 2 bits/baud (BPSK or QPSK), which results in a data rate of 1 or 2 Mbps.

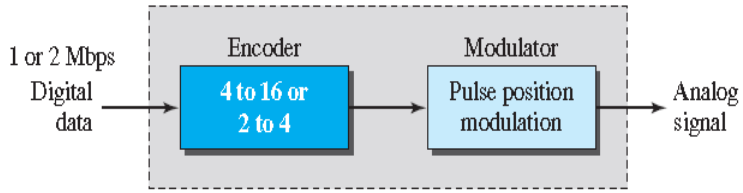
Figure 15.14 *Physical layer of IEEE 802.11 DSSS*



IEEE 802.11 Infrared

IEEE 802.11 infrared uses infrared light in the range of 800 to 950 nm. The modulation technique is called ***pulse position modulation (PPM). For a 1-Mbps data rate, a 4-bit*** sequence is first mapped into a 16-bit sequence. For a 2-Mbps data rate, a 2-bit sequence is first mapped into a 4-bit sequence .The mapped sequences are then converted to optical signals; the presence of light specifies 1, the absence of light specifies 0.

Figure 15.15 *Physical layer of IEEE 802.11 infrared*



IEEE 802.11a OFDM

IEEE 802.11a OFDM describes the **orthogonal frequency-division multiplexing (OFDM) method for signal generation in a 5.725–5.850 GHz ISM band. OFDM** is similar to FDM, with one major difference: All the subbands are used by one source at a given time. Sources contend with one another at the data-link layer for access.

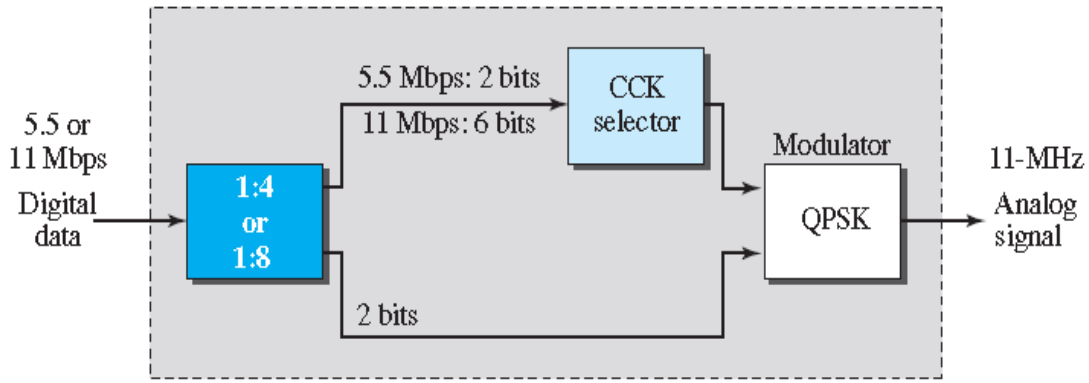
The band is divided into 52 subbands, with 48 subbands for sending 48 groups of bits at a time and 4 subbands for control information. Dividing the band into subbands diminishes the effects of interference. If the subbands are used randomly, security can also be increased. OFDM uses PSK and QAM for modulation. The common data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

IEEE 802.11b DSSS

IEEE 802.11b DSSS describes the **high-rate direct-sequence spread spectrum (HRDSSS)** method for signal generation in the 2.400–4.835 GHz ISM band. HR-DSSS is similar to DSSS except for the encoding method, which is called ***complementary code keying (CCK).***

CCK encodes 4 or 8 bits to one CCK symbol. To be backward compatible with DSSS, HR-DSSS defines four data rates: 1, 2, 5.5, and 11 Mbps. The first two use the same modulation techniques as DSSS. The 5.5-Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding. The 11-Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

Figure 15.16 *Physical layer of IEEE 802.11b*



IEEE 802.11g

This new specification defines forward error correction and OFDM using the 2.400–4.835 GHz ISM band. The modulation technique achieves a 22- or 54-Mbps data rate. It is backward-compatible with 802.11b, but the modulation technique is OFDM.

IEEE 802.11n

An upgrade to the 802.11 project is called 802.11n (the next generation of wireless LAN). The goal is to increase the throughput of 802.11 wireless LANs. The new standard emphasizes not only the higher bit rate but also eliminating some unnecessary overhead.

The standard uses what is called ***MIMO (multiple-input multiple-output antenna) to overcome the noise problem in wireless LANs. The idea is that if we can*** send multiple output signals and receive multiple input signals, we are in a better position to eliminate noise. Some implementations of this project have reached up to 600 Mbps data rate.

BLUETOOTH

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. A Bluetooth LAN can even be connected to the Internet

History

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. *Blaatand translates to Bluetooth in English.*

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.

Applications.

- Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.
- Monitoring devices can communicate with sensor devices in a small health care center.
- Home security devices can use this technology to connect different sensors to the main security controller.
- Conference attendees can synchronize their laptop computers at a conference.

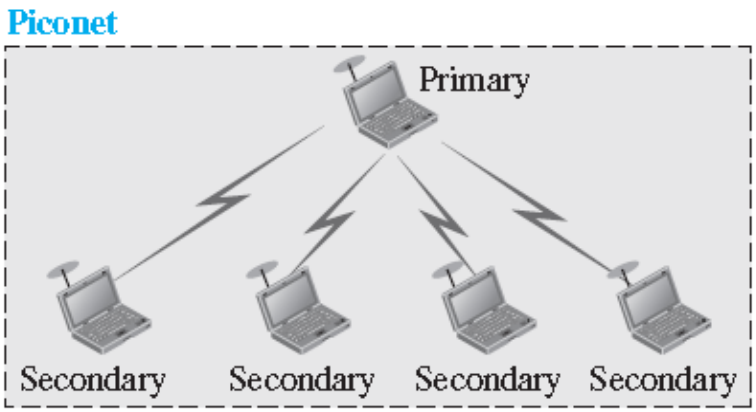
Architecture

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. The communication between the primary and secondary stations can be one-to -one or one-to-many. Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the *parked state.*

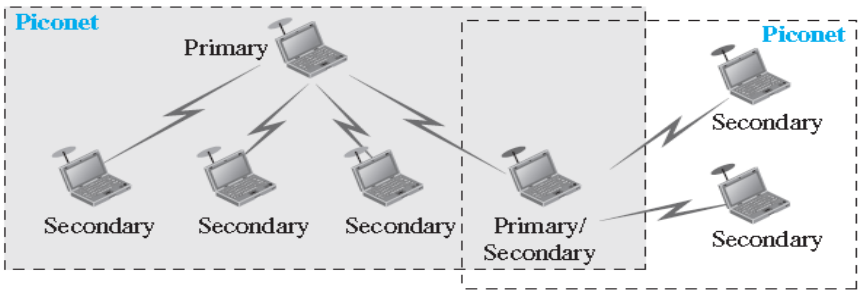
A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state.



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.

Figure 15.18 *Scatternet*

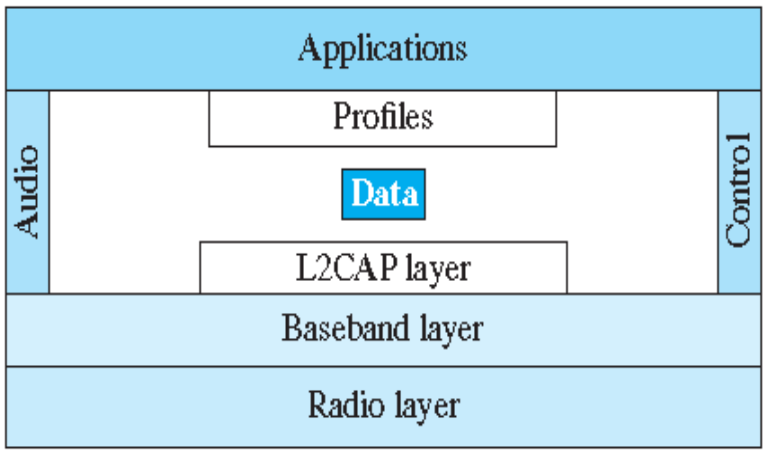


Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth Layers

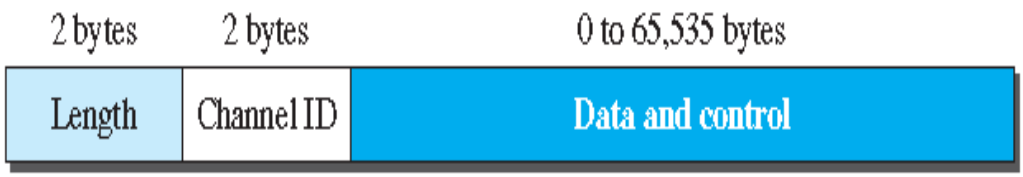
Figure 15.19 *Bluetooth layers*



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 *L2CAP data packet format*



The 16-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level

The L2CAP has specific duties: multiplexing, segmentation and reassembly, Quality of service (QoS), and group management.

Baseband Layer

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

Note : communication is only between the primary and a secondary; Secondaries cannot communicate directly with one another.

TDMA

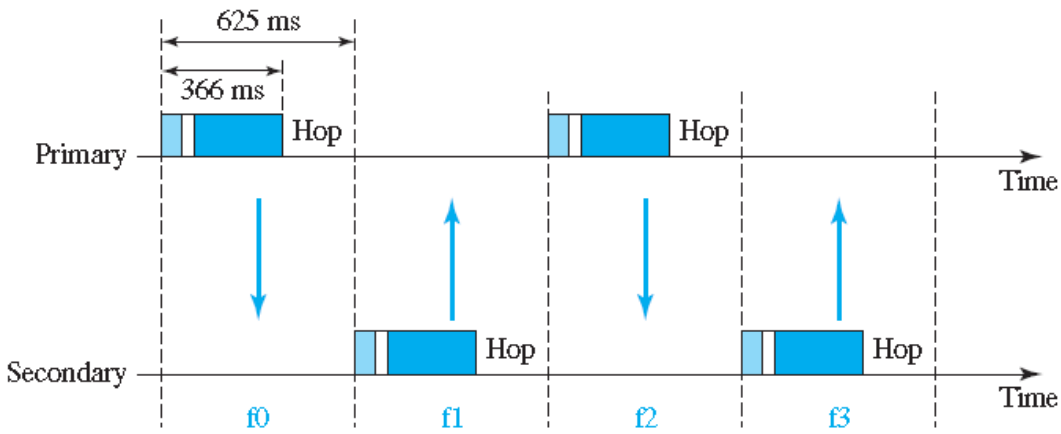
Bluetooth uses a form of TDMA that is called ***TDD-TDMA (time-division duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the sender and*** receiver send and receive data, but not at the same time (half-duplex);

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, . . .).

TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode. In slot 0, the primary sends and the secondary receives; in slot 1, the secondary sends and the primary receives. The cycle is repeated.

Figure 15.21 *Single-secondary communication*

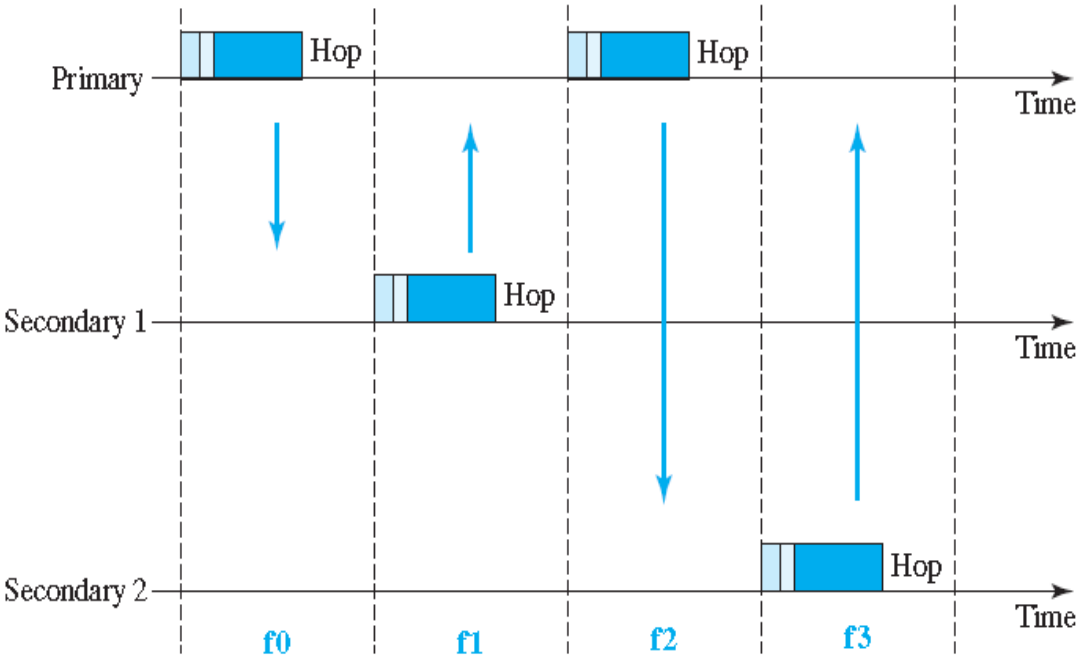


Multiple-Secondary Communication

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. All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

Figure 15.22 *Multiple-secondary communication*



Links

Two types of links can be created between a primary and a secondary:

- SCO(synchronous connection-oriented) Links

  A SCO link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery). In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals. The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted. SCO is used for real-time audio where avoiding delay is all-important. A secondary can create up to three SCO links with the primary, sending digitized audio (PCM) at 64 kbps in each link.

- ACL(**asynchronous connectionless link**) links.

  An ACL link is used when data integrity is more important than avoiding latency. An **asynchronous connectionless link (ACL) is used when data integrity is** more important than avoiding latency.

In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted.

A secondary returns an ACL frame in the available odd-numbered slot if the previous slot has been addressed to it. ACL can use one, three, or more slots and can achieve a maximum data rate of 721 kbps.

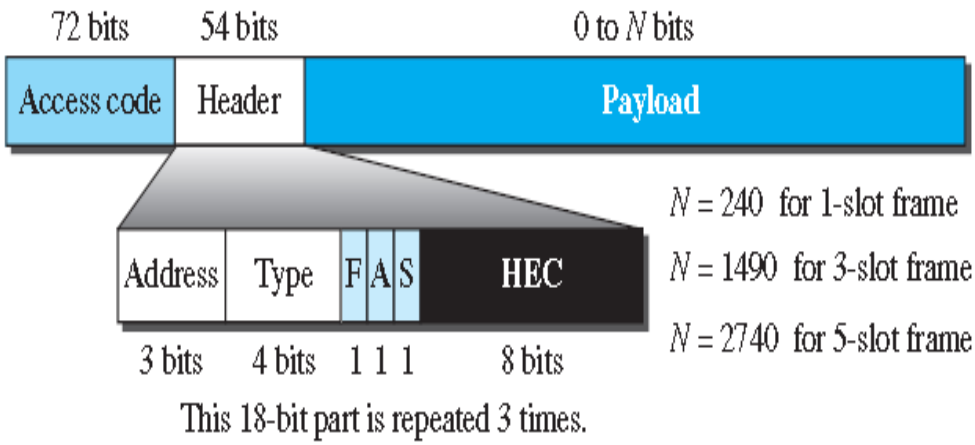
Frame Format

A frame in the baseband layer can be one of three types: one-slot, three-slot, or fiveslot. A slot is 625 μs in length. However, in 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. With a 1-MHz bandwidth and 1 bit/Hz, the size of a one slot frame is 366 bits.

A 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 device that uses a three-slot frame remains at the same hop (at the same carrier frequency) for three slots. A five -slot frame also uses 259 bits for hopping, which means that the length of the frame is 5 × 625 – 259 = 2866 bits.

Frame format types

Figure 15.23 *Frame format types*



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

  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.

F. This 1-bit subfield is for flow control. When set (1), it indicates that that 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.

- ***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.

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering;) GFSK has a carrier frequency.

- Bit 1 is represented by a frequency deviation above the carrier;
- bit 0 is represented by a frequency deviation below the carrier.

The frequencies, are defined according to the following formula for each channel.

$$Fc = 2402 + n \ MHz \qquad n = 0, 1, 2, 3, \ldots, 78$$

Frequency-Hopping Spread Spectrum (FHSS) method

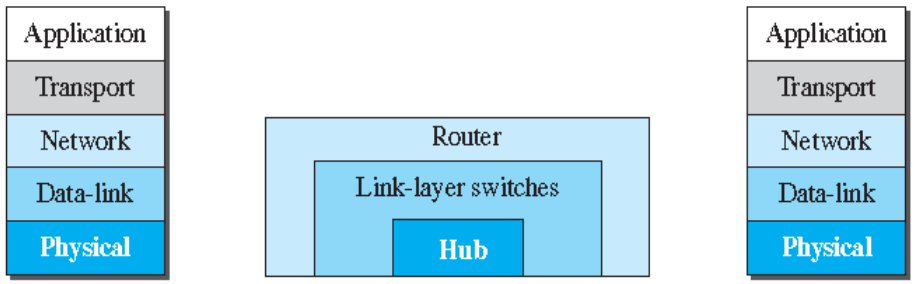
Bluetooth uses the **frequency-hopping spread spectrum (FHSS) method in the physical** layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second. A device uses a frequency for only 625 μs (1/1600 s) before it hops to another frequency; the dwell time is 625 μs.

CONNECTING DEVICES

We use **connecting devices to** connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model.

There are 3 kinds of *connecting devices: 1. Hubs, 2. Link-layer switches, and 3.Routers.*

Figure 17.1 *Three categories of connecting devices*



Hubs

A hub is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation. A **repeater receives a signal and, before it becomes too weak or corrupted,** *regenerates and retimes the original bit pattern and then sends the refreshed* signal.

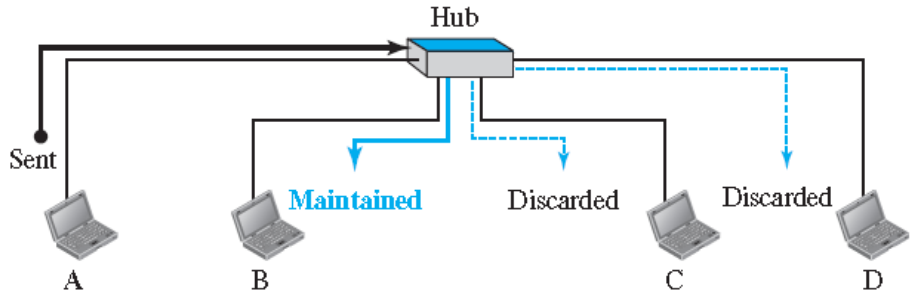
In the past, Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable. Today, Ethernet LANs use star topology. In a star topology, a repeater is a multiport device, often called a *hub.*

Hub can be used to serve as the connecting point and at the same time function as a repeater. When a packet from station A to station B arrives at the hub, the hub forwards the packet to all outgoing ports except the one from which the signal was received.

The figure definitely shows that a hub does not have a filtering capability;

It does not have the intelligence to find from which port the frame should be sent out. A hub or a repeater is a physical-layer device. They do not have a link-layer address and they do not check the link-layer address of the received frame. They just regenerate the corrupted bits and send them out from every port.

Figure 17.2 *A hub*



Link-Layer Switches

A link-layer switch (or *switch) operates in both the physical and the data-link layers.* As a physical-layer device, it regenerates the signal it receives. As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

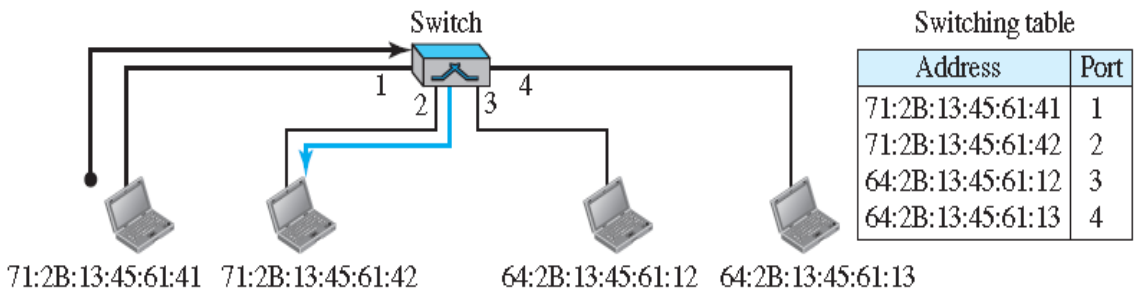
What is the difference in functionality is between a link-layer switch and a hub.?

Answer: A link-layer switch has **filtering capability.**

A Link layer switch can check the destination address of a frame and can decide from which outgoing port the frame should be sent.

Filtering

Figure 17.3 *Link-layer switch*



Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

- *If a frame destined for station 71:2B:13:45:61:42 arrives at port 1,*
- *The link-layer switch consults its table to find the departing port.*
- *According to its table, frames for 71:2B:13:45:61:42 should be sent out only through port 2;*
- *Therefore, there is no need for forwarding the frame through other* ***ports.***

Transparent Switches

A transparent switch is a switch in which the stations are completely unaware of the switch's existence. If a switch is added or deleted from the system, reconfiguration of the stations is unnecessary.

According to the IEEE 802.1d specification, a system equipped with transparent switches must meet three criteria:

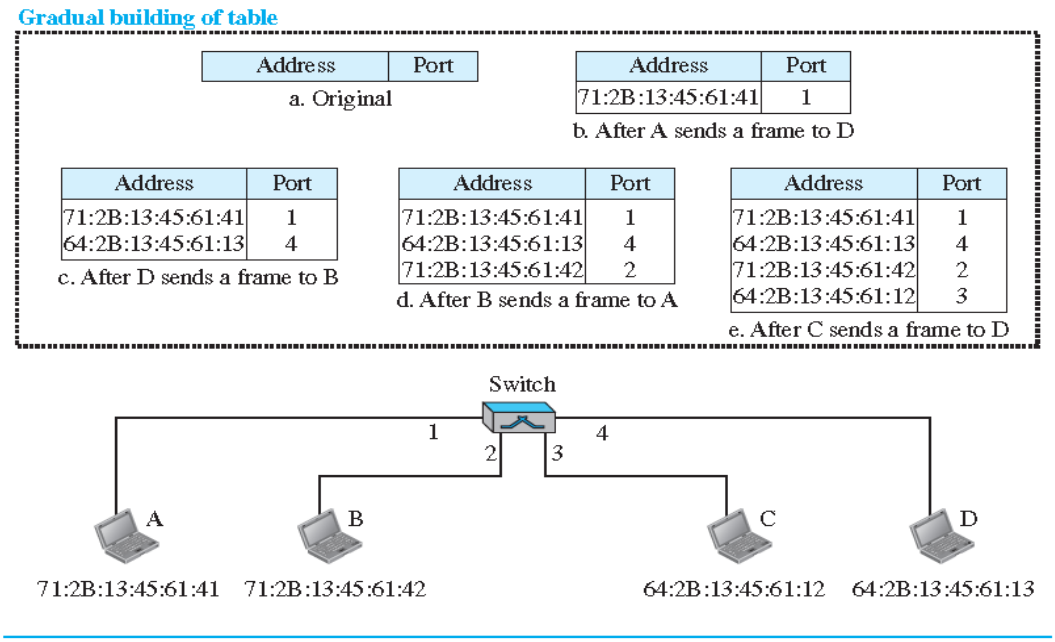
- ❑ Frames must be forwarded from one station to another.
- ❑ The forwarding table is automatically made by learning frame movements in the network.
- ❑ Loops in the system must be prevented.

Learning

The earliest switches had switching tables that were static. The system administrator would manually enter each table entry during switch setup. Although the process was simple, it was not practical. If a station was added or deleted, the table had to be modified manually. The same was true if a station's MAC address changed, which is not a rare event. For example, putting in a new network card means a new MAC address.

A better solution to the static table is a dynamic table that maps addresses to ports (interfaces) automatically. To make a table dynamic, we need a switch that gradually learns from the frames movements. To do this, the switch inspects both the destination and the source addresses in each frame that passes through the switch. The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes.

Figure 17.4 *Learning switch*



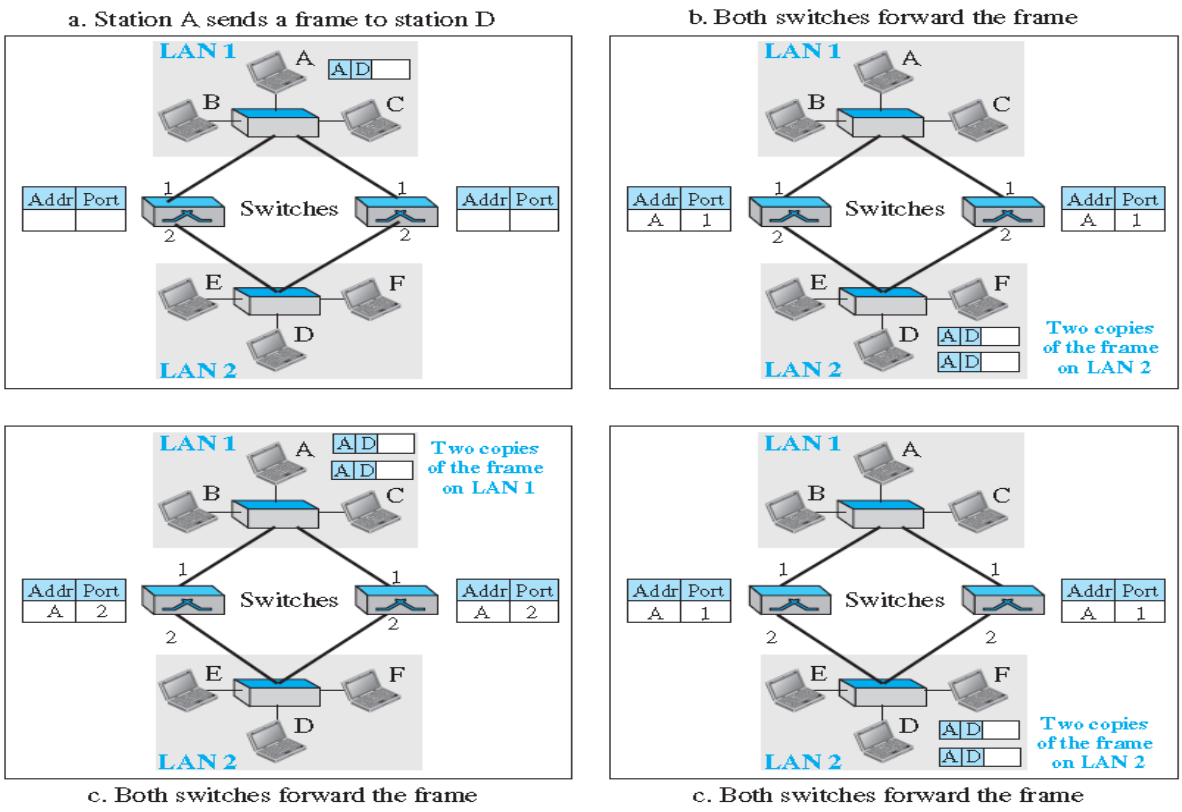
- When station A sends a frame to station D, the frame goes out from all three ports; the frame floods the network.
- However, by looking at the source address, the switch learns that station A must be connected to port 1.
- This means that frames destined for A, in the future, must be sent out through port 1.
- The switch adds this entry to its table.
- When station D sends a frame to station B, the switch has no entry for B, it adds one more entry to the table related to station D.

The learning process continues until the table has information about every port. However, the learning process may take a long time. For example, if a station does not send out a frame (a rare situation), the station will never have an entry in the table

Loop Problem

Transparent switches work fine as long as there are no redundant switches in the system. Systems administrators, however, like to have redundant switches (more than one switch between a pair of LANs) to make the system more reliable. Redundancy can create loops in the system, which is very undesirable. Loops can be created only when two or more broadcasting LANs (those using hubs, for example) are connected by more than one switch.

Figure 17.5 *Loop problem in a learning switch*



1. Station A sends a frame to station D. The tables of both switches are empty. Both forward the frame and update their tables based on the source address A.

2. Now there are two copies of the frame on LAN 2. The copy sent out by the left switch is received by the right switch, which does not have any information about the destination address D; it forwards the frame.

The copy sent out by the right switch is received by the left switch and is sent out for lack of information about D.

Note:- Each frame is handled separately because switches, as two nodes on a broadcast network sharing the medium, use an access method such as CSMA/CD.

3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies are sent to LAN2.

4. The process continues on and on. This is called Loop problem

Spanning Tree Algorithm

To solve the looping problem, the IEEE specification requires that switches use the spanning tree algorithm to create a loopless topology. In graph theory, a **spanning tree is a graph in which there is no loop.**

In a switched LAN, this means creating a topology in which each LAN can be reached from any other LAN through one path only (no loop).

To find the spanning tree, we need to assign a cost (metric) to each arc. The interpretation of the cost is left up to the systems administrator. We have chosen the minimum hops. However, the hop count is normally 1 from a switch to the LAN and 0 in the reverse direction.

Steps to find Spanning tree

1. *Every switch has a built-in ID (normally the serial number, which is unique). Each switch broadcasts this ID so that all switches know which one has the smallest ID. The switch with the smallest ID is selected as the root switch (root of the tree). We assume that switch S1 has the smallest ID. It is, therefore, selected as the root switch.*

2. *The algorithm tries to find the shortest path (a path with the shortest cost) from the root switch to every other switch or LAN. The shortest path can be found by examining the total cost from the root switch to the destination.*

3. *The combination of the shortest paths creates the shortest tree, which is also shown in Figure 17.7.*

4. *Based on the spanning tree, we mark the ports that are part of it, the **forwarding ports, which forward a frame that the switch receives. We also mark those ports** that are not part of the spanning tree, the **blocking ports, which block the frames** received by the switch*

Figure 17.6 *A system of connected LANs and its graph representation*

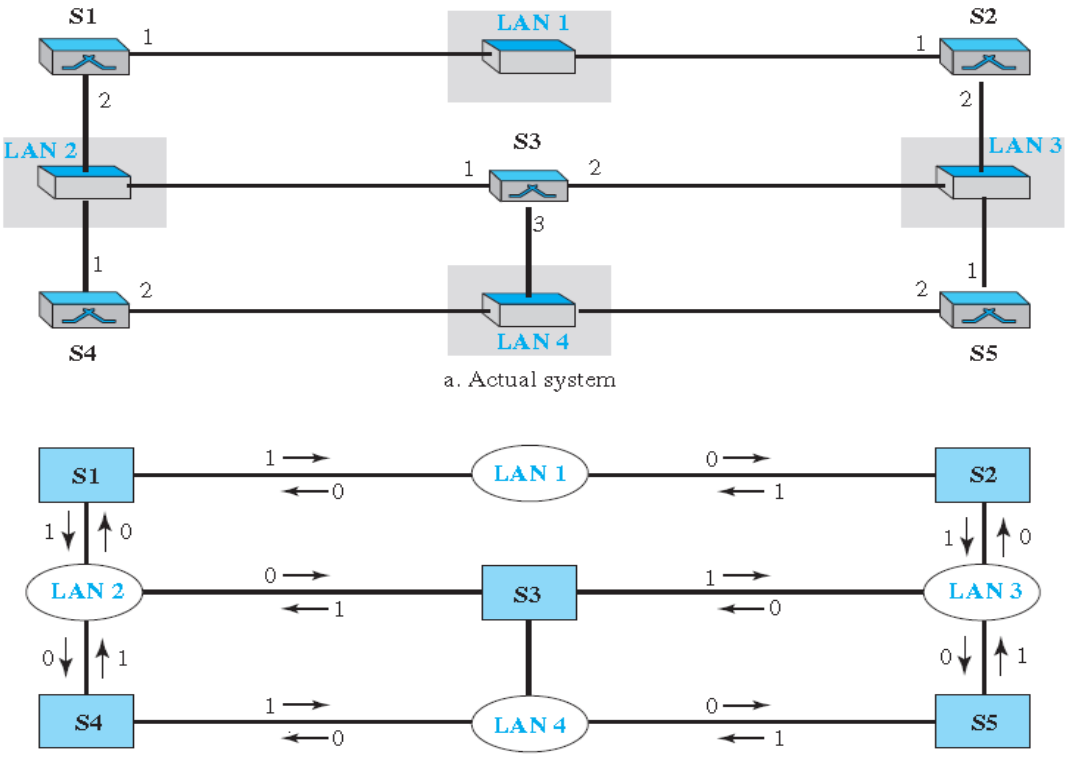


Figure 17.7 *Finding the shortest paths and the spanning tree in a system of switches*

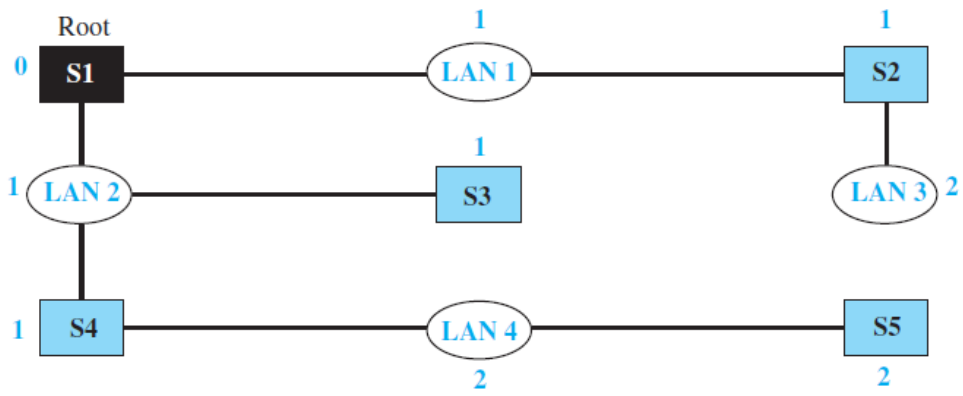
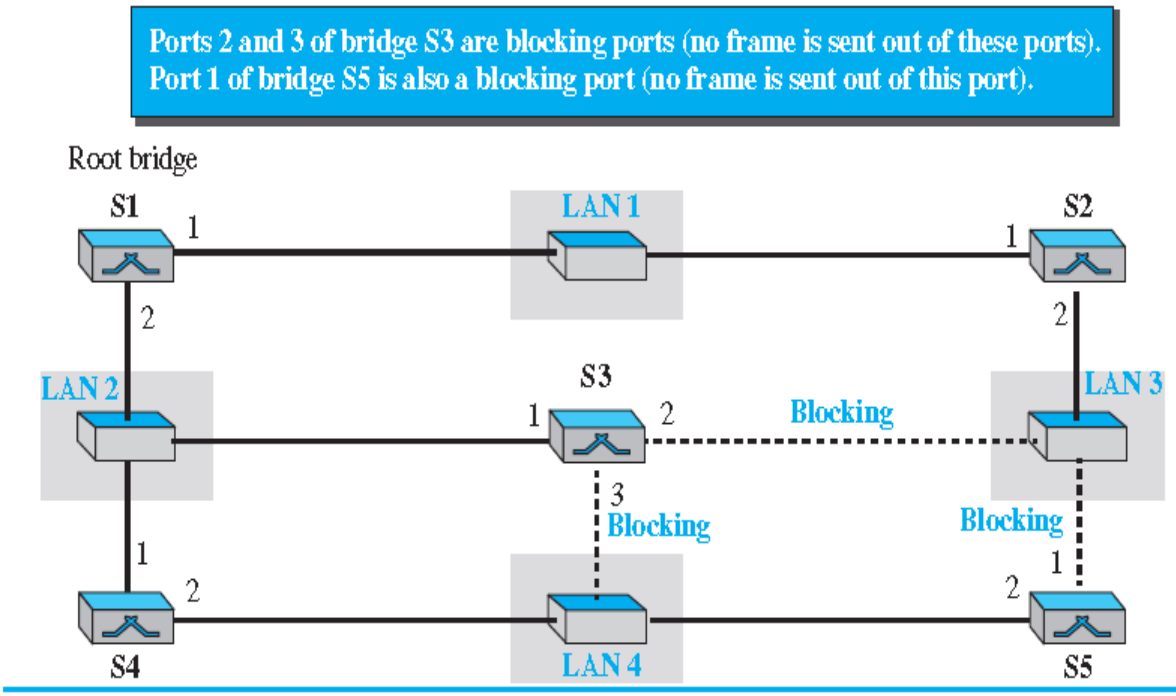


Figure 17.8 *Forwarding and blocking ports after using spanning tree algorithm*



Note that there is only one path from any LAN to any other LAN in the spanning tree system. This means there is only one path from one LAN to any other LAN. No loops are created. We have described the spanning tree algorithm as though it required manual entries. This is not true. Each switch is equipped with a software package that carries out this process dynamically.

Advantages of Switches

1. ***Collision Elimination***

   A link-layer switch eliminates the collision. This means increasing the average bandwidth available to a host in the network. In a switched LAN, there is no need for carrier sensing and collision detection; each host can transmit at any time.

2. Connecting Heterogenous Devices

A link-layer switch can connect devices that use different protocols at the physical layer (data rates) and different transmission media.

As long as the format of the frame at the data-link layer does not change, a switch can receive a frame from a device that uses twisted-pair cable and sends data at 10 Mbps and deliver the frame to another device that uses fiber-optic cable and can receive data at 100 Mbps.

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 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. A router can connect networks. In other words, a router is an internetworking device; It connects independent networks to form an internetwork.

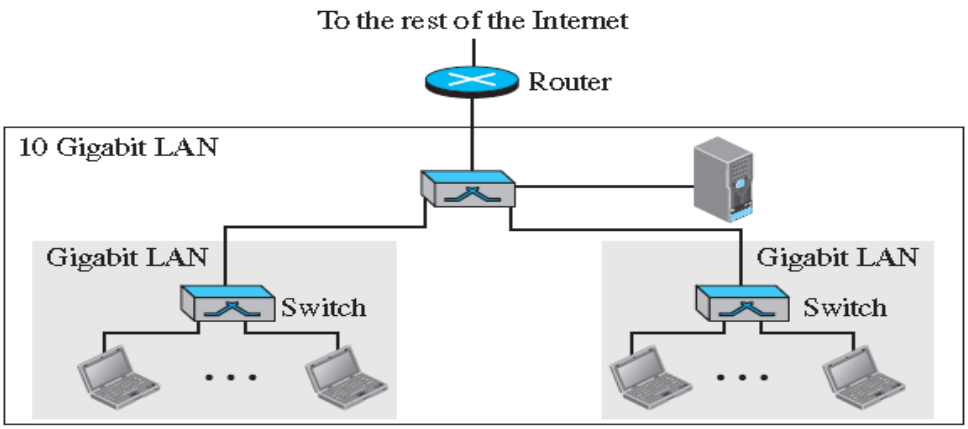
Differences between a router and a switch

1. A router has a physical and logical (IP) address for each of its interfaces.

2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.

3. A router changes the link-layer address of the packet (both source and destination) when it forwards the packet.

Figure 17.9 *Routing example*



A router, will change the MAC addresses it receives because the MAC addresses have only local jurisdictions.

VIRTUAL LANs

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic.

What happens if we need a virtual connection between two stations belonging to two different physical LANs? We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

Figure 17.10 *A switch connecting three LANs*

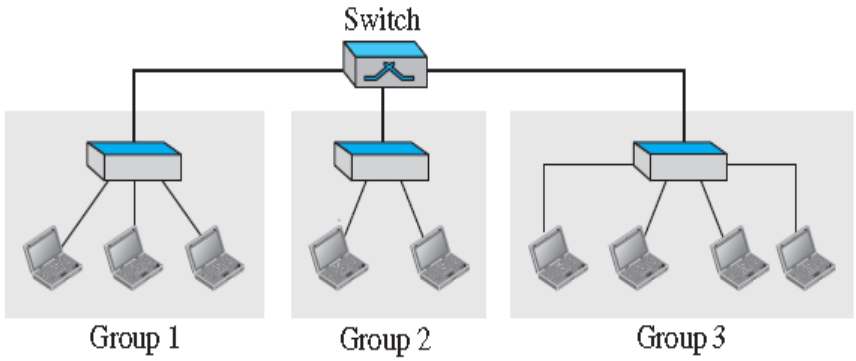
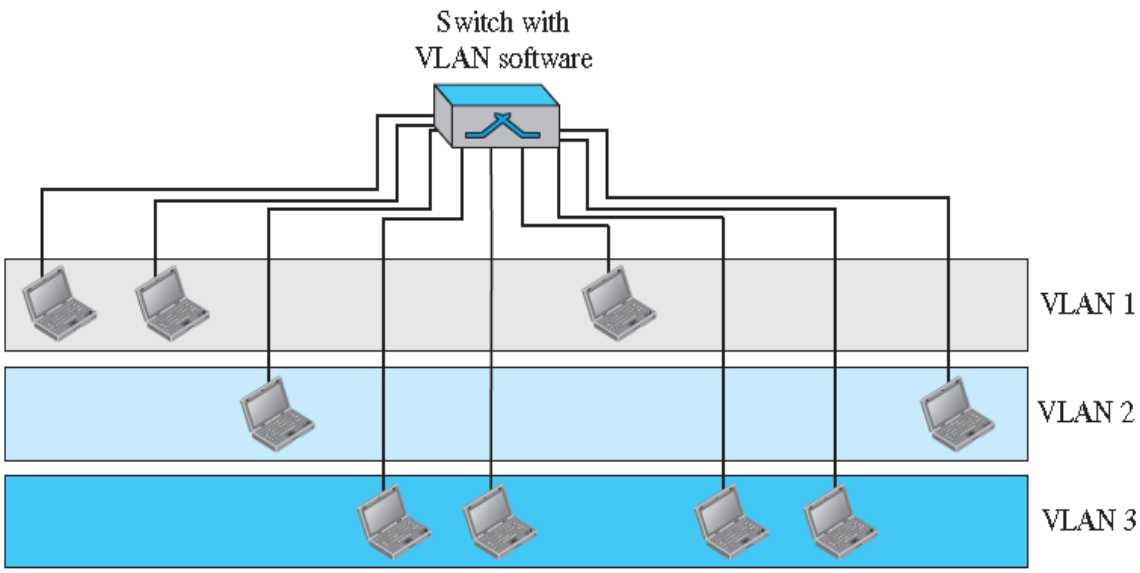


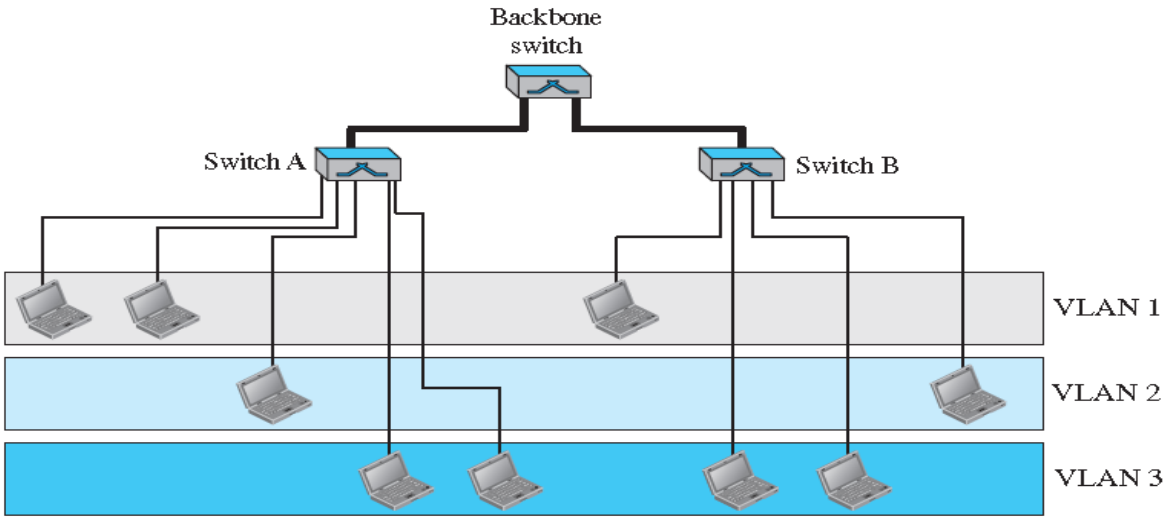
Figure 17.11 *A switch using VLAN software*



The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments. A LAN can be divided into several logical LANs, called *VLANs. Each VLAN* is a work group in the organization. If a person moves from one group to another, there is no need to change the physical configuration. Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN.

This means that if a station moves from VLAN 1 to VLAN 2, it receives broadcast messages sent to VLAN 2, but no longer receives broadcast messages sent to VLAN 1.

Figure 17.12 *Two switches in a backbone using VLAN software*



VLAN technology even allows the grouping of stations connected to different switches in a VLAN. Stations from switches A and B belong to each VLAN. This is a good configuration for a company with two separate buildings. Each building can have its own switched LAN connected by a backbone. People in the first building and people in the second building can be in the same work group even though they are connected to different physical LANs.

Membership

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

Vendors use different characteristics such as interface numbers, port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these.

Interface Numbers

Some VLAN vendors use switch interface numbers as a membership characteristic. For example, the administrator can define that stations connecting to ports 1, 2, 3, and 7 belongto VLAN 1, stations connecting to ports 4, 10, and 12 belong to VLAN 2, and so on.

MAC Addresses

Some VLAN vendors use the 48-bit MAC address as a membership characteristic. For example, the administrator can stipulate that stations having MAC addresses E2:13:42:A1:23:34 and F2:A1:23:BC:D3:41 belong to VLAN 1.

IP Addresses

Some VLAN vendors use the 32-bit IP address as a membership characteristic. For example, the administrator can stipulate that stations having IP addresses 181.34.23.67, 181.34.23.72, 181.34.23.98, and 181.34.23.112 belong to VLAN 1.

Multicast IP Addresses

Some VLAN vendors use the multicast IP address as a membership characteristic.

Combination

Recently, the software available from some vendors allows all these characteristics to be combined. The administrator can choose one or more characteristics when installing the software.

Configuration

How are the stations grouped into different VLANs? Stations are configured in one of three ways:

1. ***Manual Configuration:*** In a manual configuration, the network administrator uses the VLAN software to manually assign the stations into different VLANs at setup. Later migration from one VLAN to another is also done manually. Note that this is not a physical configuration; it is a logical configuration. The term *manually here means that the administrator types* the port numbers, the IP addresses, or other characteristics, using the VLAN software.
2. ***Automatic Configuration***: In an automatic configuration, the stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator. For example, the administrator can define the project number as the criterion for being a member of a group.
   When a user changes projects, he or she automatically migrates to a new VLAN.
3. ***Semiautomatic Configuration:*** *A semiautomatic configuration is somewhere between a manual configuration and an automatic configuration. Usually, the initializing is done manually, with migrations done automatically.*

Communication between Switches

In a multi-switched backbone, each switch must know not only which station belongs to which VLAN, but also the membership status of stations connected to other switches.

For example, in Figure 17.12, switch A must know the membership status of stations connected to switch B, and switch B must know the same about switch A.

Three methods have been devised for this purpose: they are

1. ***Table Maintenance***

   In this method, when a station sends a broadcast frame to its group members, the switch creates an a table and records station membership. The switches send their tables to one another periodically for updating.

2. ***Frame Tagging***

   In this method, when a frame is traveling between switches, an extra header is added to the MAC frame to define the destination VLAN. The frame tag is used by the receiving switches to determine the VLANs to be receiving the broadcast message.

IEEE Standard

In 1996, the IEEE 802.1 subcommittee passed a standard called 802.1Q that defines the format for frame tagging. The standard also defines the format to be used in multiswitched backbones and enables the use of multivendor equipment in VLANs

3. Time-Division Multiplexing (TDM)

In this method, the connection (trunk) between switches is divided into time-shared channels. For example, if the total number of VLANs in a backbone is five, each trunk is divided into five channels. The traffic destined for VLAN 1 travels in channel 1, the traffic destined for VLAN 2 travels in channel 2, and so on. The receiving switch determines the destination VLAN by checking the channel from which the frame arrived.

Advantages

1. Cost and Time Reduction

VLANs can reduce the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software.

2. Creating Virtual Work Groups

VLANs can be used to create virtual work groups. For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department. This can reduce traffic if the multicasting capability of IP was previously used.

3. Security

VLANs provide an extra measure of security. People belonging to the same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.

Network Layer

Introduction

The network layer in the TCP/IP protocol suite is responsible for the host-to-host delivery of datagrams. It provides services to the transport layer and receives services from the data-link layer. In this chapter, we introduce the general concepts and issues in the network layer.

NETWORK-LAYER SERVICES

- **Packetizing**
- **Routing and Forwarding**
- **Other Services**

  i) ***Error Control***

  ii) Flow Control

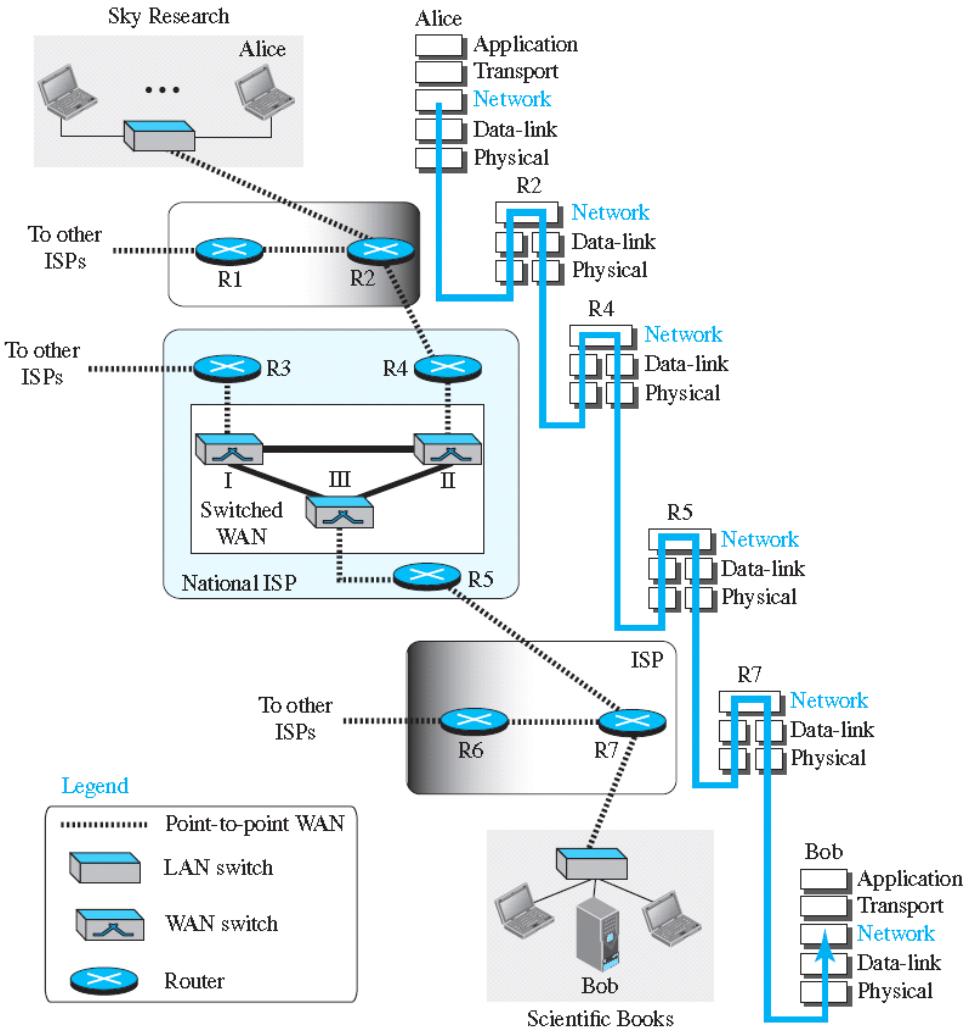
  iii) Congestion Control

  iv) Quality of Service

  v) Security

As the figure shows, the network layer is involved at the source host, destination host, and all routers in the path (R2, R4, R5, and R7). At the source host (Alice), the network layer accepts a packet from a transport layer, encapsulates the packet in a datagram, and delivers the packet to the data-link layer. At the destination host (Bob), the datagram is decapsulated, and the packet is extracted and delivered to the corresponding transport layer. Although the source and destination hosts are involved in all five layers of the TCP/IP suite, the routers use three layers if they are routing packets only;

Figure 18.1 *Communication at the network layer*



Packetizing

The first duty of the network layer is definitely **packetizing: encapsulating the payload** in a packet at the source and decapsulating the payload from the packet at the destination. In other words network layer is to carry a payload from the source to the destination without changing it or using it.

The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented. If the packet is fragmented at the source or at routers along the path, the network layer is responsible for waiting until all fragments arrive, reassembling them, and delivering them to the upper-layer protocol. The routers are not allowed to change source and destination addresses either.

Routing and Forwarding

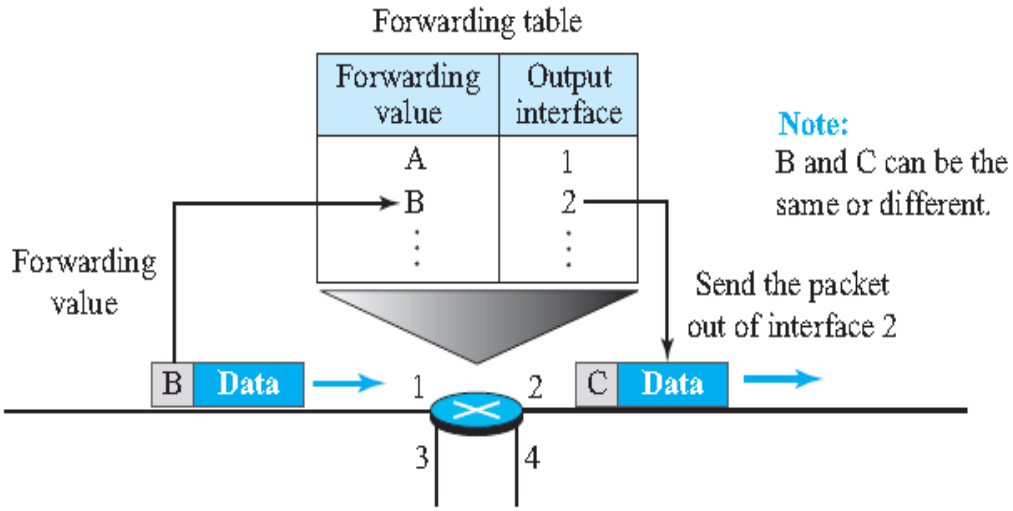
Routing

The network layer is responsible for routing the packet from its source to the destination. Generally there is more than one route from the source to the destination. The network layer is responsible for finding the best one among these possible routes. The network layer needs to have some specific strategies for defining the best route. The routing protocols, should be run before any communication occurs.

Forwarding

Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces. A router normally uses *forwarding table* for applying this action is sometimes called the the *routing table.* To make decision, the router uses a piece of information in the packet header, which can be the destination address or a label, to find the corresponding output interface number in the forwarding table .

Figure 18.2 *Forwarding process*



Other Services

Error Control

Although error control also can be implemented in the network layer, the designers of the network layer ignore this issue. One reason is the fact that the packet in the network layer may be fragmented at each router, which makes error checking at this layer inefficient. Although the network layer in the Internet does not directly provide error control, the Internet uses an auxiliary protocol, ICMP, that provides some kind of error control .

Flow Control

Flow control regulates the amount of data a source can send without overwhelming the receiver. To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data. The network layer, however, does not directly provide any flow control. The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

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 is beyond the capacity of the network or routers. In this situation, some routers may drop some of the datagrams.

However, as more datagrams are dropped, the situation may become worse because, due to the error control mechanism at the upper layers, the sender may send duplicates of the lost packets. If the congestion continues, sometimes a situation may reach a point where the system collapses and no datagrams are delivered.

Quality of Service

As the Internet has allowed new applications such as multimedia communication the quality of service (QoS) of the communication has become more and more important. However, to keep the network layer untouched, these provisions are mostly implemented in the upper layer.

Security

Security was not a concern when the Internet was originally designed because it was used by a small number of users at universities for research activities; other people had no access to the Internet. The network layer was designed with no security provision. Today, however, security is a big concern. To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service.

PACKET SWITCHING

A router, in fact, is a switch that creates a connection between an input port and an output port (or a set of output ports), Just as an electrical switch connects the input to the output to let electricity flow. Switching techniques are divided into two broad categories, circuit switching and packet switching,

Only packet switching is used at the network layer because the unit of data at this layer is a packet. Circuit switching is mostly used at the physical layer;

A packet-switched network can use two different approaches to route the packets:

1. ***Datagram Approach: Connectionless Service***

When the network layer provides a connectionless service, each packet traveling in 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. A packet* belonging to a message may be followed by a packet belonging to the same message or to a different message. Each packet is routed based on the information contained in its header: source and destination addresses. The destination address defines where it should go; the source address defines where it comes from.

Figure 18.3 *A connectionless packet-switched network*

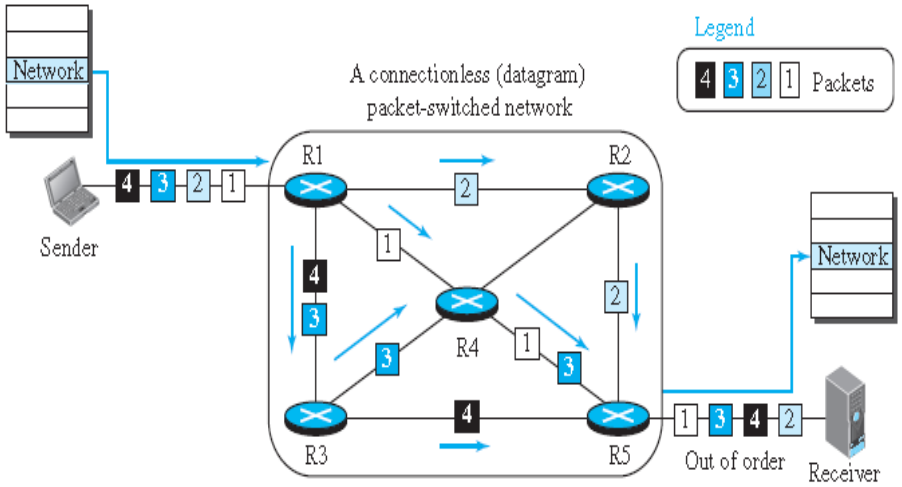
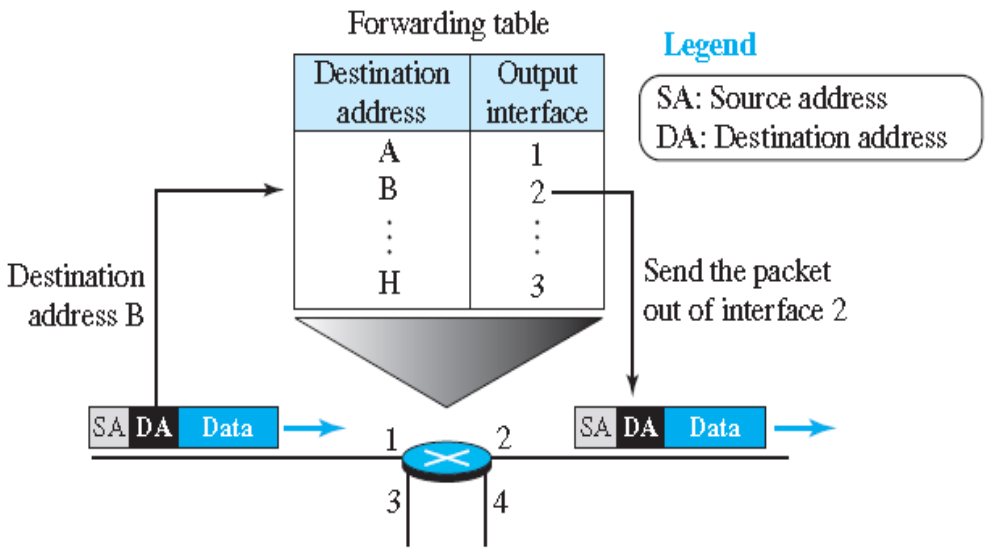


Figure 18.4 *Forwarding process in a router when used in a connectionless network*



2. *Virtual-Circuit Approach: Connection-Oriented Service*

In a connection-oriented service (also called *virtual-circuit approach), there is a relationship* 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 all 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 flow label is a virtual circuit identifier that defines the virtual path the packet should follow.

Figure 18.5 *A virtual-circuit packet-switched network*

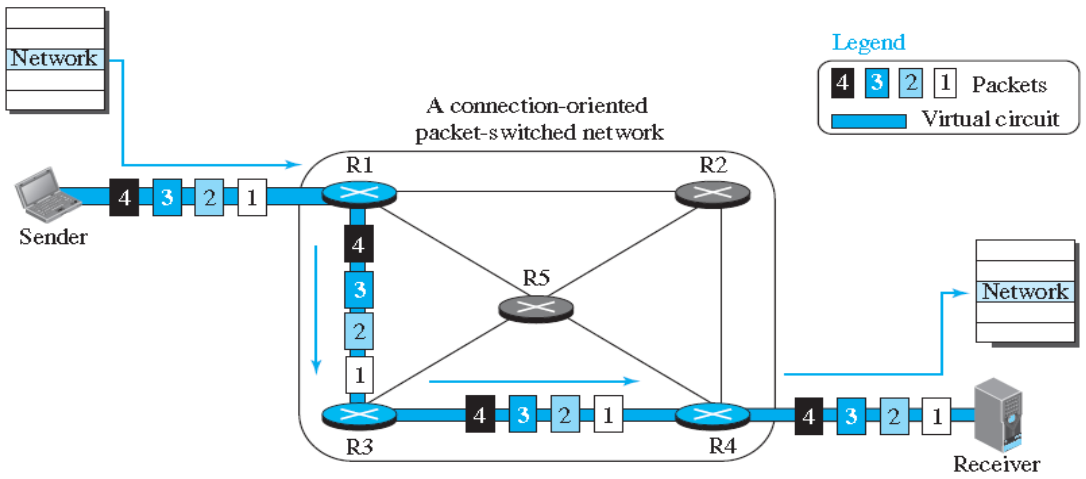
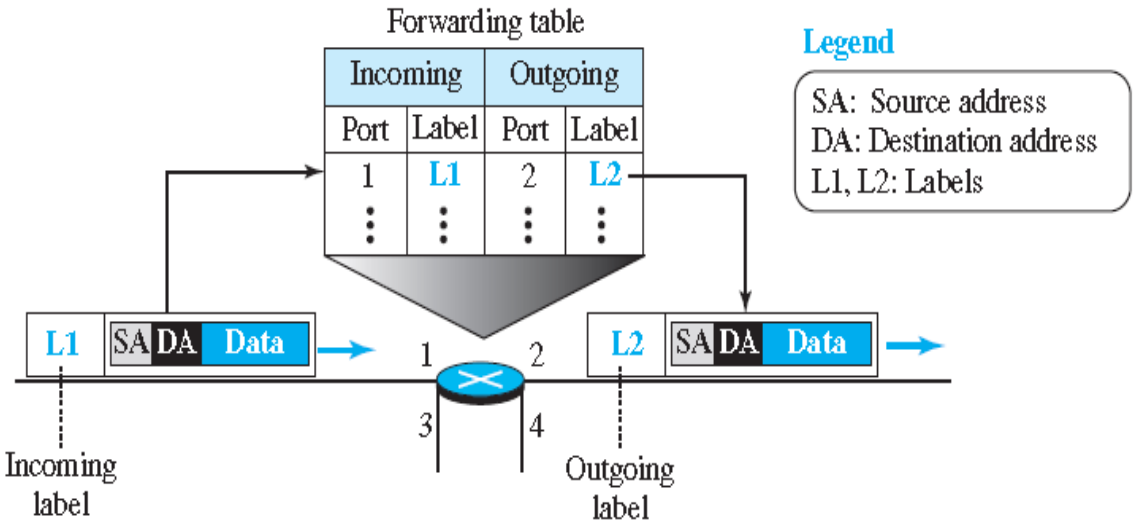


Figure 18.6 *Forwarding process in a router when used in a virtual-circuit network*



IPV4 ADDRESSES

The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed. IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet.

Address Space

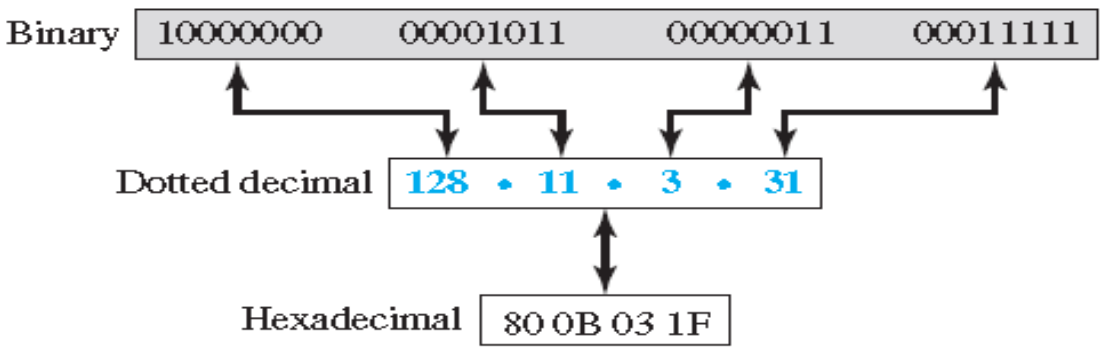
An **address space is** the total number of addresses used by the protocol. If a protocol uses *b bits to define an* address, the address space is 2^b *because each bit can have two different values (0 or 1).* IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion). If there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notation

There are three common notations to show an IPv4 address:

- binary notation (base 2),
- dotted-decimal notation (base 256), and
- hexadecimal notation (base 16).

Three different notations in IPv4 addressing



Hierarchy in Addressing

In any communication network that involves delivery, such as a telephone network or a postal network, the addressing system is hierarchical. In a postal network, the postal address (mailing address) includes the country, state, city, street, house number, and the name of the mail recipient.

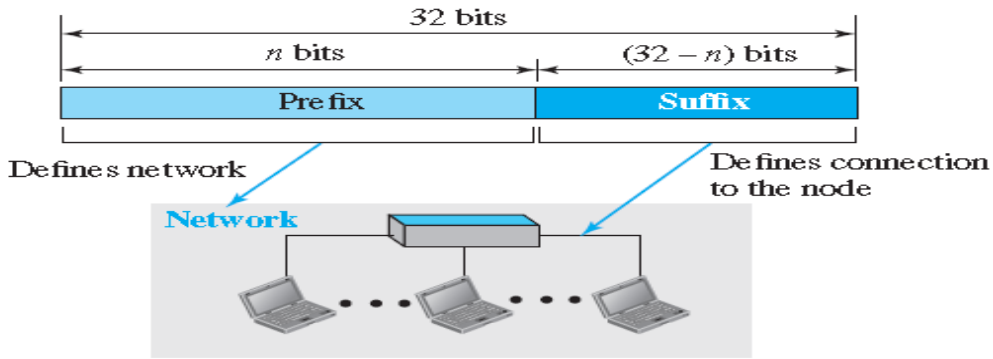
Similarly, a telephone number is divided into the country code, area code, local exchange, and the connection.

A 32-bit IPv4 address is also hierarchical, but divided only into two parts. The first part of the address, called the *prefix, defines the network; the second part of the* address, called the *suffix, defines the node* (connection of a device to the Internet).

The prefix length is *n bits and the suffix length is (32 − n) bits.*

A prefix can be fixed length or variable length. The network identifier in the IPv4 was first designed as a fixed-length prefix. This scheme, which is now obsolete, is referred to as classful addressing. The new scheme, which is referred to as classless addressing, uses a variable-length network prefix .

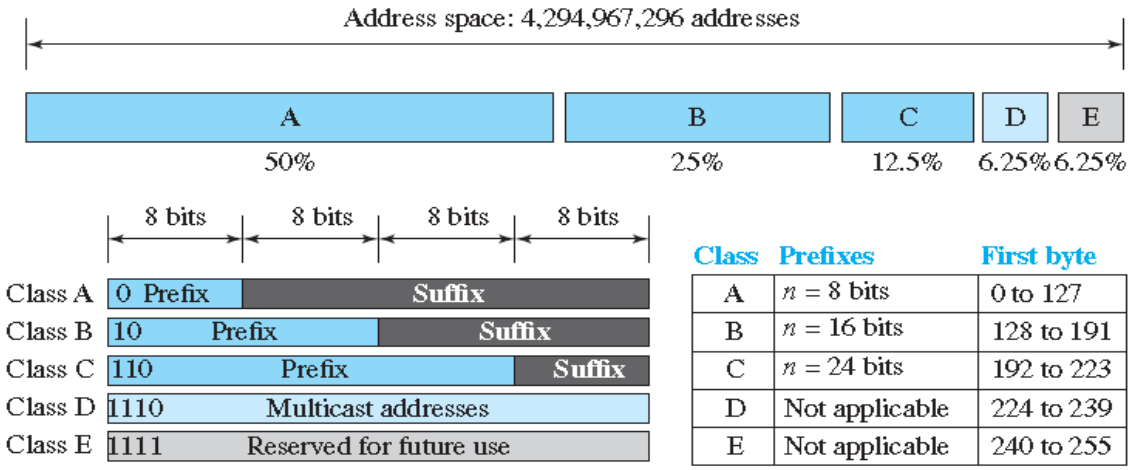
Hierarchy in addressing



Classful Addressing

When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (*n = 8, n = 16, and n = 24).* The whole address space was divided into five classes (class A, B, C, D, and E), as shown in Figure 18.18. This scheme is referred to as **classful addressing.**

Figure 18.18 *Occupation of the address space in classful addressing*



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Address Depletion

The reason that classful addressing has become obsolete is address depletion. Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up. This resulted in no more addresses available for organizations and individuals that needed to be connected to the Internet.

To understand the problem, let us think about class A. This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network). Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).

Class B addresses were designed for midsize organizations, but many of the addresses in this class also remained unused.

Class C addresses have a completely different flaw in design. The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address class. Class E addresses were almost never used, wasting the whole class.

In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier. This means there are only 27 = 128 networks in the world that can have a class A address.

Subnetting and Supernetting

To alleviate address depletion, two strategies were proposed and, to some extent, implemented: subnetting and supernetting.

In subnetting, a class A or class B block is divided into several subnets. Each subnet has a larger prefix length than the original network. For example, if a network in class A is divided into four subnets, each subnet has a prefix of nsub = 10.

At the same time, if all of the addresses in a network are not used, subnetting allows the addresses to be divided among several organizations. This idea did not work because most large organizations were not happy about dividing the block and giving some of the unused addresses to smaller organizations.

While subnetting was devised to divide a large block into smaller ones, supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block. This idea did not work either because it makes the routing of packets more difficult.

Advantage of Classful Addressing

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately. In other words, the prefix length in classful addressing is inherent in the address; no extra information is needed to extract the prefix and the suffix.