CMR
INSTITUTE OF
TECHNOLOGY

USN | | | | | | | | | | |

Third Internal Test

Sub:	**Data Communications**							Code:	17CS46
Date:	15/ 05 / 2019	Duration:	90 mins	Max Marks:	50	Sem:	IV	Branch:	**ISE – A Section**

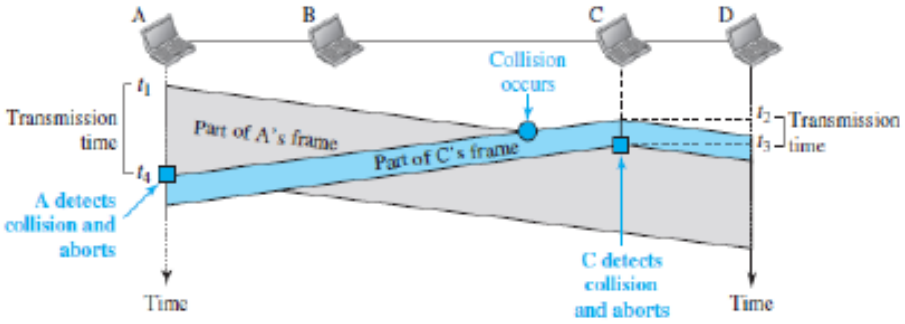
Answer Any **FIVE FULL** Questions

		Marks	OBE CO	OBE RBT
1 (a)	Illustrate CSMA/CD with suitable flow diagram.	[8]	CO3	L2
(b)	A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time is 25.6 μs, what is the minimum size of the frame?	[2]	CO3	L2
2 (a)	Illustrate CSMA/CA with suitable flow diagram.	[8]	CO3	L2
(b)	A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system produces 500 frames per second.	[2]	CO3	L3
3 (a)	What is channelization? List out the channelization protocols.	[2]	CO3	L1
(b)	Explain CDMA with an example.	[8]	CO3	L3
4 (a)	Explain Bluetooth architecture.	[4]	CO4	L2
(b)	Illustrate TDD-TDMA in Bluetooth with necessary diagrams.	[6]	CO4	L2
5 (a)	What is cellular telephony? Describe its principle of operation.	[5]	CO4	L2
(b)	Discuss the features of 4^{th} generation of cellular telephony.	[5]	CO4	L2
6	Explain the working of Mobile IP in detail.	[10]	CO5	L2
7	Analyze the IPv4 datagram frame format with neat diagram.	[10]	CO5	L2
8 (a)	Write a short note on IPv6 addressing.	[4]	CO5	L2
(b)	Compare the different methods of transition from IPv4 to IPv6.	[6]	CO5	L2

1(a). Illustrate CSMA/CD with suitable flow diagram. (8 marks)

CSMA/CD

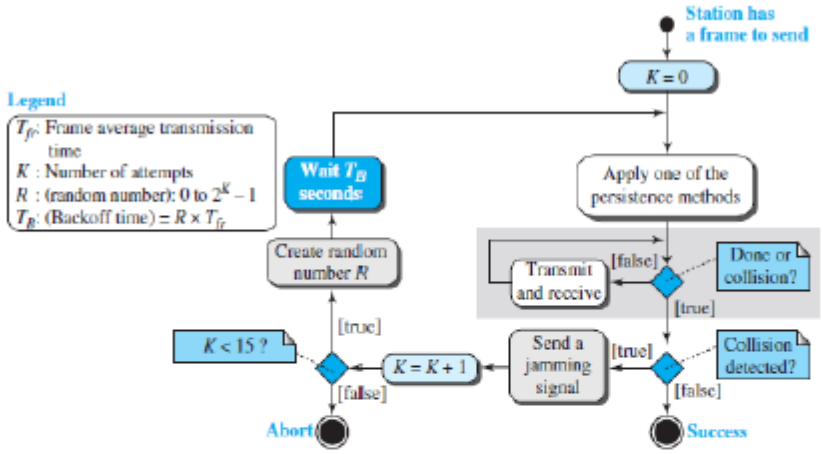
Disadvantage of CSMA: CSMA does not specify the procedure after a collision has occurred.
Solution: CSMA/CD enhances the CSMA to handle the collision.
Here is how it works (Figure 12.12):
A station
sends the frame &
then monitors the medium to see if the transmission was successful or not.
If the transmission was unsuccessful (i.e. there is a collision), the frame is sent again.



In the Figure,
At time t_1, station A has executed its procedure and starts sending the bits of its frame. At time t_2, station C has executed its procedure and starts sending the bits of its frame. The collision occurs sometime after time t_2.
Station C detects a collision at time t3 when it receives the first bit of A's frame.
Station C immediately aborts transmission.
Station A detects collision at time t_4 when it receives the first bit of C's frame.
Station A also immediately aborts transmission.
Station A transmits for the duration t4–t1. Station
C transmits for the duration t3-t2.
For the protocol to work:
The length of any frame divided by the bit rate must be more than either of these durations.

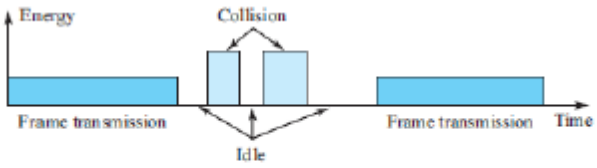
Minimum Frame Size

For CSMA/CD to work, we need to restrict the frame-size.
Before sending the last bit of the frame, the sender must
detect a collision and
abort the transmission.
This is so because the sender
does not keep a copy of the frame and
does not monitor the line for collision-detection.
Frame transmission time T_{fr} is given by
$T_{fr}=2T_p$ where T_p=maximum propagation time



Energy Level

- In a channel, the energy-level can have 3 values: 1) Zero 2) Normal and 3) Abnormal.
  1) At zero level, the channel is idle (Figure 12.14).
  2) At normal level, a station has successfully captured the channel and is sending its frame. 3) At abnormal level, there is a collision and the level of the energy is twice the normal level.
- A sender needs to monitor the energy-level to determine if the channel is
  → Idle
  → Busy or
  → Collision mode



Throughput

The throughput of CSMA/CD is greater than pure or slotted ALOHA.
The maximum throughput is based on
different value of G
persistence method used (non-persistent, 1-persistent, or p-persistent) and
"p" value in the p-persistent method.
For 1-persistent method, the maximum throughput is 50% when G =1.
For non-persistent method, the maximum throughput is 90% when G is between 3 and 8.

1(b). A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time is 25.6 µs, what is the minimum size of the frame? (2 marks)

The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ µs. This means, in the worst case, a station needs to transmit for a period of 51.2 µs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 µs = 512 bits or 64 bytes. This is actually the minimum size of the frame

2(a). Illustrate CSMA/CA with suitable flow diagram. (8 marks)

CSMA/CA

Here is how it works:

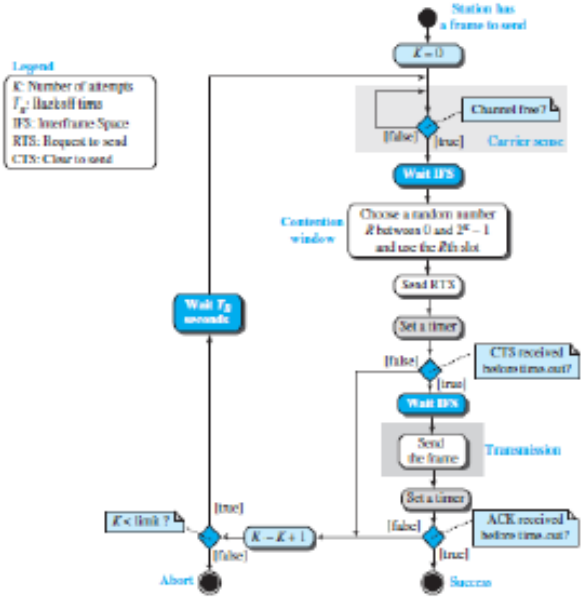
A station needs to be able to receive while transmitting to detect a collision.

When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives 2 signals:

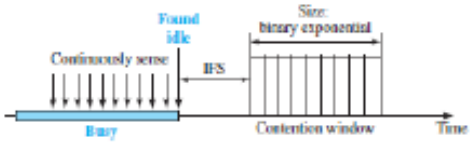
Its own signal and

Signal transmitted by a second station.

To distinguish b/w these 2 cases, the received signals in these 2 cases must be different.



Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments.



1) Interframe Space (IFS)

Collisions are avoided by deferring transmission even if the channel is found idle. When the channel is idle, the station does not send immediately.

Rather, the station waits for a period of time called the inter-frame space or IFS.

- After the IFS time,
  if the channel is still idle,
  then, the station waits for the contention-time &
  finally, the station sends the frame.
- IFS variable can also be used to prioritize stations or frame types.
  For example, a station that is assigned a shorter IFS has a higher priority.

2) Contention Window

The contention-window is an amount of time divided into time-slots. A ready-station chooses a random-number of slots as its wait time.

In the window, the number of slots changes according to the binary exponential back-off strategy. For example:

At first time, number of slots is set to one slot and
Then, number of slots is doubled each time if the station cannot detect an idle channel.

3) Acknowledgment

There may be a collision resulting in destroyed-data.
In addition, the data may be corrupted during the transmission.
To help guarantee that the receiver has received the frame, we can use
Positive acknowledgment and
Time-out timer

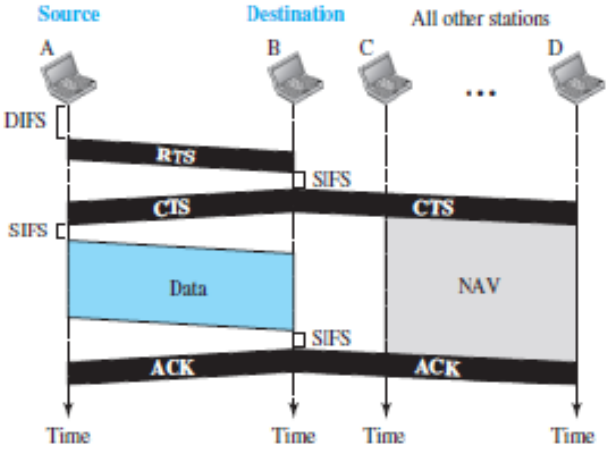
Frame Exchange Time Line

- Two control frames are used: 1)
  Request to send (RTS) 2)
  Clear to send (CTS)
- The procedure for exchange of data and control frames in time (Figure 12.17):
  1) The source senses the medium by checking the energy level at the carrier frequency. If
     the medium is idle,
     then the source waits for a period of time called the DCF interframe space (DIFS); finally, the source sends a RTS.

  The destination
  receives the RTS
  waits a period of time called the short interframe space (SIFS) sends a control frame CTS to the source.
  CTS indicates that the destination station is ready to receive data.

  The source
  receives the CTS
  waits a period of time SIFS
  sends a data to the destination

  The destination
  receives the data
  waits a period of time SIFS
  sends a acknowledgment ACK to the source.
  ACK indicates that the destination has been received the frame.



Network Allocation Vector

- When a source-station sends an RTS, it includes the duration of time that it needs to occupy the channel.
- The remaining stations create a timer called a network allocation vector (NAV).
- NAV indicates waiting time to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

Collision During Handshaking

- Two or more stations may try to send RTS at the same time.
- These RTS may collide.
- The source assumes there has been a collision if it has not received CTS from the destination.
- The backoff strategy is employed, and the source tries again.

Hidden-Station Problem

- Figure 12.17 also shows that the RTS from B reaches A, but not C.
- However, because both B and C are within the range of A, the CTS reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

2(b). A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system produces 500 frames per second. (2 marks)

The average number of successful transmissions is given by

$$S = G \times e^{-G}.$$

Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

3(a). What is channelization? List out the channelization protocols. (2 marks)

Channelization (or *channel partition*, as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.

FDMA (Frequency Division Multiple Access)
TDMA (Time Division Multiple Access) and
CDMA (Code Division Multiple Access)

3(b). Explain CDMA with an example. (8 marks)

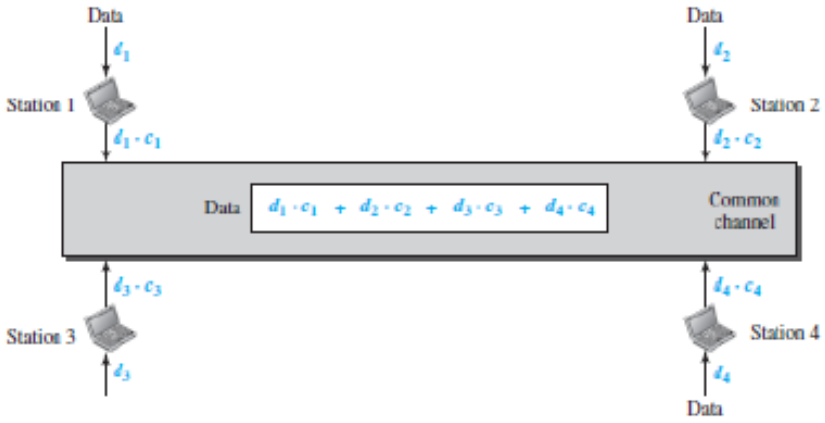
CDMA

CDMA simply means communication with different codes.
CDMA differs from FDMA because
only one channel occupies the entire bandwidth of the link.
CDMA differs from TDMA because
all stations can send data simultaneously; there is no timesharing.

(Analogy: CDMA simply means communication with different codes.
For example, in a large room with many people, 2 people can talk privately in English if nobody else understands English. Another 2 people can talk in Chinese if they are the only ones who understand Chinese, and so on).

Implementation

Let us assume we have four stations 1, 2, 3, and 4 connected to the same channel. The data from station-1 are d_1, from station-2 are d_2, and so on.
The code assigned to the first station is c_1, to the second is c_2, and so on. We assume that the assigned codes have 2 properties.
If we multiply each code by another, we get 0.
If we multiply each code by itself, we get 4 (the number of stations).



Here is how it works:

Station-1 multiplies the data by the code to get $d_1.c_1$.
Station-2 multiplies the data by the code to get $d_2.c_2$.
And so on. The data that go on the channel are the sum of all these terms.

The receiver multiplies the data on the channel by the code of the sender.
For example, suppose stations 1 and 2 are talking to each other. Station-2 wants to hear what station-1 is saying.
Station-2 multiplies the data on the channel by c_1 the code of station-1. $(c_1.c_1)=4$, $(c_2.c_1)=0$, $(c_3.c_1)=0$, and $(c_4.c_1)=0$,
Therefore, station-2 divides the result by 4 to get the data from station-1.

$$\begin{aligned}\text{data} &= (d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4) \cdot c_1 \\ &= d_1 \cdot c_1 \cdot c_1 + d_2 \cdot c_2 \cdot c_1 + d_3 \cdot c_3 \cdot c_1 + d_4 \cdot c_4 \cdot c_1 = 4 \times d_1\end{aligned}$$

Chips

CDMA is based on coding theory.

Each station is assigned a code, which is a sequence of numbers called chips (Figure 12.24).

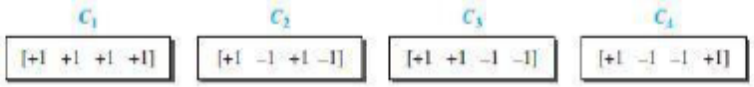


Figure 12.24 *Chip sequences*

These sequences were carefully selected & are called orthogonal sequences These sequences have the following properties:

Each sequence is made of N elements, where N is the number of stations.

Multiplication of a sequence by a scalar:

If we multiply a sequence by a number i.e. every element in the sequence is multiplied by that element.

For example,

3) Inner product of 2 equal sequences:

If we multiply 2 equal sequences, element by element, and add the results, we get N, where N is the number of elements in the each sequence.

For example,

4) Inner product of 2 different sequences:

If we multiply 2 different sequences, element by element, and add the results, we get 0. For example,

5) Adding 2 sequences means adding the corresponding elements. The result is another sequence.

For example,

Data Representation

We follow the following rules for encoding:

To send a 0 bit, a station encodes the bit as -1

To send a 1 bit, a station encodes the bit as +1

When a station is idle, it sends no signal, which is interpreted as a 0.

Encoding and Decoding

We assume that

Stations 1 and 2 are sending a 0 bit. Station-4 is sending a 1 bit.

Station-3 is silent.

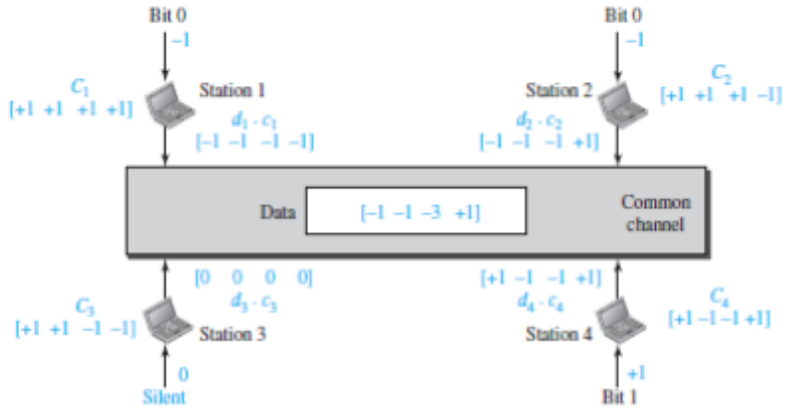
Here is how it works (Figure 12.26):

At the sender-site, the data are translated to -1, -1, 0, and +1.

Each station multiplies the corresponding number by its chip (its orthogonal sequence). The result is a new sequence which is sent to the channel.

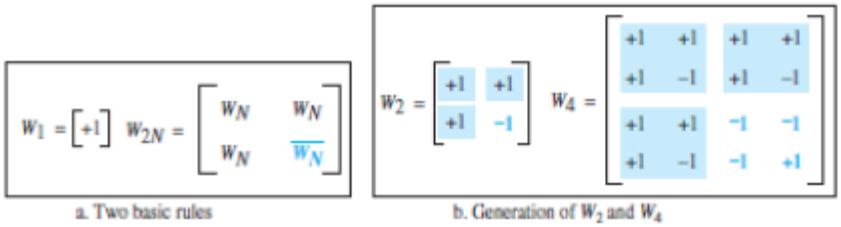
The sequence on the channel is the sum of all 4 sequences. Now imagine station-3, which is silent, is listening to station-2.

Station-3 multiplies the total data on the channel by the code for station-2, which is [+1 -1 +1- 1], to get



Sequence Generation

To generate chip sequences, we use a Walsh table (Figure 12.29).
Walsh table is a 2-dimensional table with an equal number of rows and columns.



a. Two basic rules b. Generation of W_2 and W_4

In the Walsh table, each row is a sequence of chips.

W1 for a one-chip sequence has one row and one column. We can choose –1 or +1 for the chip for this trivial table (we chose +1).

According to Walsh, if we know the table for N sequences W_N, we can create the table for 2N sequences W_{2N} (Figure 12.29).

The W_N with the overbar $\overline{W_N}$ stands for the complement of W_N where each +1 is changed to -1 and vice versa.

After we select W1, W2 can be made from four W1's, with the last one the complement of W1 After W2 is generated, W4 can be made of four W2's, with the last one the complement of W2. The number of sequences in a Walsh table needs to be $N = 2^m$.

4(a). Explain Bluetooth architecture. (4 marks)

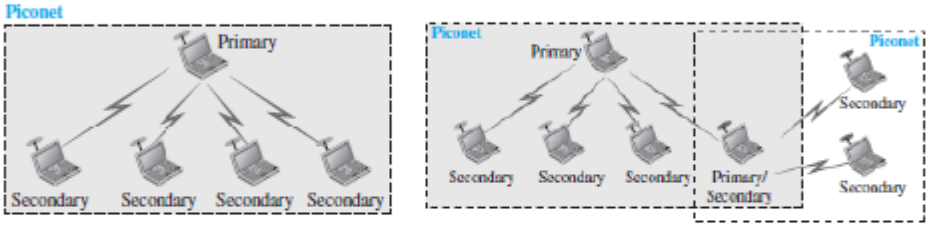
Bluetooth defines 2 types of networks: 1) Piconet and 2) Scatternet.

Piconets

A Bluetooth network is called a piconet, or a small net.
(Figure 15.17). A piconet can have up to 8 stations. Out of which

One of station is called the primary.
The remaining stations are called secondaries.

All the secondary-stations synchronize their clocks and hopping sequence with the primary station. A piconet can have only one primary station.
The communication between the primary and the secondary can be one-to-one or one-to-many.



Although a piconet can have a maximum of 7 secondaries, an additional 8 secondaries can be in the parked state.

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

Because only 8 stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scatternet

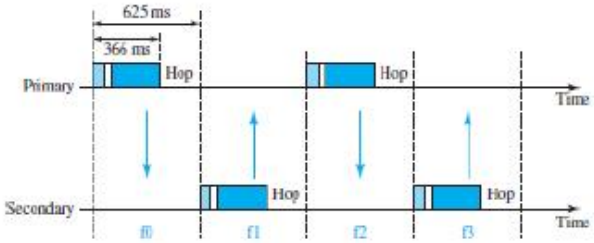
Piconets can be combined to form a scatternet. A station can be a member of 2 piconets.
A secondary station in one piconet can be the primary in another piconet. This is called mediator station.

Acting as a secondary, mediator station can receive messages from the primary in the first piconet.
Acting as a primary, mediator station can deliver the message to secondaries in the second piconet.

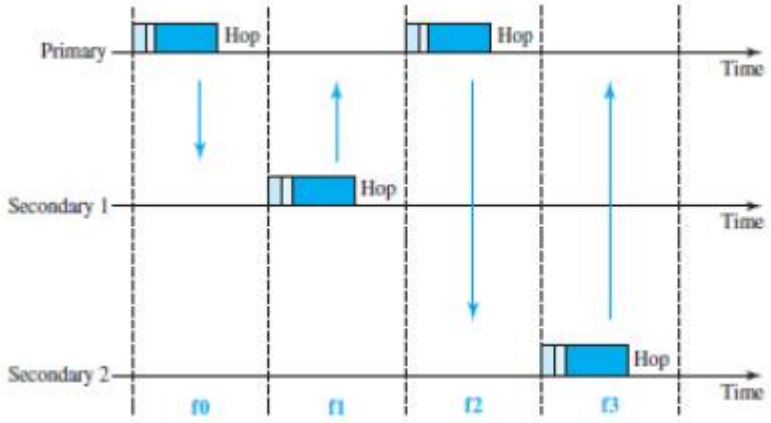
4(b). Illustrate TDD-TDMA in Bluetooth with necessary diagrams. (6 marks)

Bluetooth uses a form of TDMA that is called ***TDD-TDMA (time-division duplexTDMA)***. 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.

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.



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 shows a scenario.



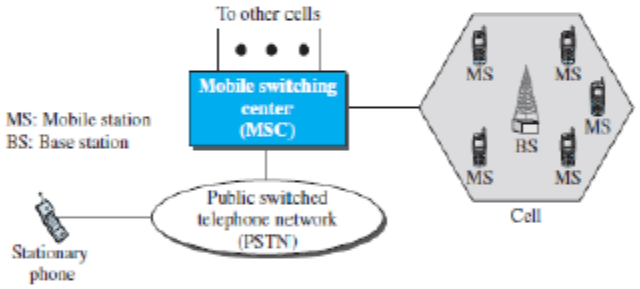
Let us elaborate on the figure.

1. In slot 0, the primary sends a frame to secondary 1.
2. In slot 1, only secondary 1 sends a frame to the primary because the previous frame was addressed to secondary 1; other secondaries are silent.
3. In slot 2, the primary sends a frame to secondary 2.
4. In slot 3, only secondary 2 sends a frame to the primary because the previous frame was addressed to secondary 2; other secondaries are silent.
5. The cycle continues.

We can say that this access method is similar to a poll/select operation with reservations. When the primary selects a secondary, it also polls it. The next time slot is reserved for the polled station to send its frame. If the polled secondary has no frame to send, the channel is silent.

5(a). What is cellular telephony? Describe its principle of operation. (5 marks)

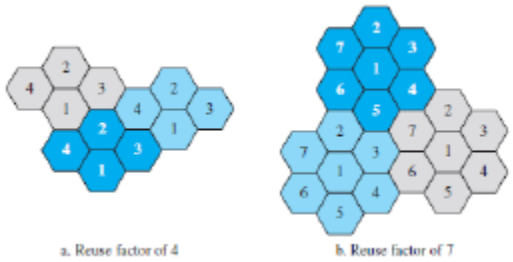
Cellular telephony is designed to provide communications
between two moving units called mobile-stations (MSs) or
between one mobile-station and one stationary unit called a land unit (Figure 16.6).
A service-provider is responsible for
locating & tracking a caller
assigning a channel to the call and
transferring the channel from base-station to base-station as the caller moves out-of-range.
Each cellular service-area is divided into small regions called cells.
Each cell contains an antenna.
Each cell is controlled by AC powered network-station called the base-station (BS).
Each base-station is controlled by a switching office called a mobile-switching-center (MSC).
MSC coordinates communication between all the base-stations and the telephone central office.
MSC is a computerized center that is responsible for
connecting calls
recording call information and
billing.
Cell-size is not fixed; Cell-size can be increased or decreased depending on population of the area.
Cell-radius = 1 to 12 mi.
Compared to low-density areas, high-density areas require many smaller cells to meet traffic demands.
Cell-size is optimized to prevent the interference of adjacent cell-signals.



Operation

Frequency-Reuse Principle

In general, neighboring-cells cannot use the same set of frequencies for communication.
Using same set of frequencies may create interference for the users located near the cell-boundaries.
However,
set of frequencies available is limited and
frequencies need to be reused.
A frequency reuse pattern is a configuration of N cells. Where N = reuse factor
Each cell uses a unique set of frequencies.
When the pattern is repeated, the frequencies can be reused.
There are several different patterns (Figure 16.7).
The numbers in the cells define the pattern.
The cells with the same number in a pattern can use the same set of frequencies. These cells are called the reusing cells.



a. Reuse factor of 4 b. Reuse factor of 7

Transmitting

Procedure to place a call from a mobile-station:

The caller
- enters a phone number and
- presses the send button.

The mobile-station
- scans the band to determine setup channel with a strong signal and
- sends the data (phone number) to the closest base-station.

The base-station sends the data to the MSC.
The MSC sends the data on to the telephone central office.
If called party is available, a connection is made and the result is relayed back to the MSC.
The MSC assigns an unused voice channel to the call, and a connection is established.
The mobile-station automatically adjusts its tuning to the new channel.
Finally, voice communication can begin.

Receiving

Procedure to receive a call from a mobile-station:

When a mobile phone is called, the telephone central office sends phone number to the MSC.
MSC searches for the location of the mobile-station by sending query-signals to each cell in a process. This is called paging.
When the mobile-station is found, the MSC transmits a ringing signal.
When the mobile-station answers, the MSC assigns a voice channel to the call.
Finally, voice communication can begin.

Handoff

During a conversation, the mobile-station may move from one cell to another.
Problem: When the mobile-station goes to cell-boundary, the signal becomes weak.
To solve this problem, the MSC monitors the level of the signal every few seconds.
If signal-strength decreases, MSC determines a new cell to accommodate the communication.
Then, MSC changes the channel carrying the call (hands signal off from old channel to a new one).

- Two types of Handoff: 1) Hard Handoff 2) Soft Handoff

1) Hard Handoff

Early systems used a hard handoff.
A mobile-station only communicates with one base-station.
When the MS moves from one cell to another cell,
- Firstly, communication must be broken with the old base-station.
- Then, communication can be established with the new base-station.

This may create a rough transition.

2) Soft Handoff

New systems use a soft handoff.
A mobile-station can communicate with two base-stations at the same time.
When the MS moves from one cell to another cell,
- Firstly, communication must be broken with the old base-station.
- Then, the same communication may continue with the new base-station.

Roaming

Roaming means that the user
- can have access to communication or
- can be reached where there is coverage.

Usually, a service-provider has limited coverage.
Neighboring service-providers can provide extended coverage through a roaming contract.

5(b). Discuss the features of 4th generation of cellular telephony. (5 marks)

4G cellular telephony is expected to be a complete evolution in wireless communications.
Some objectives defined by the 4G working group:

- A spectrally efficient system.
- High network capacity.
- Data-rate of
  - 100 Mbps for access in a moving vehicle
  - 1 Gbps for stationary users and
  - 100 Mbps between any two points in the world.
- Smooth handoff across heterogeneous networks.
- Seamless connectivity and global roaming across multiple networks.
- High quality of service for next generation multimedia support.
- Interoperability with existing wireless standards.
- All IP, packet-switched, networks.

4G is only packet-based networks.
4G supports IPv6.
4G provides better multicast, security, and route optimization capabilities.

- Here we discuss, following issues: 1) Access Scheme 2) Modulation 3) Radio System 4) Antenna 5) Applications

1) Access Scheme

- To increase efficiency,
  i) capacity, ii) scalability & iii) new access techniques are being considered for 4G.
- For example:
  i) OFDMA and IFDMA are being considered for the downlink & uplink of the next generation UMTS. ii) MC-CDMA is proposed for the IEEE 802.20 standard.

2) Modulation

More efficient 64-QAM is being proposed for use with the LTE standards.

3) Radio System

The 4G uses a SDR system.
The components of an SDR are pieces of software and thus flexible.
The SDR can change its program to shift its frequencies to mitigate frequency interference.

4) Antenna

The MIMO and MU-MIMO antenna system is proposed for 4G.
Using this antenna, 4G allows independent streams to be transmitted simultaneously from all the antennas to increase the data-rate.
MIMO also allows the transmitter and receiver coordinates to move to an open frequency when interference occurs.

5) Applications

At the present rates of 15-30 Mbps, 4G is capable of providing users with streaming high-definition television.
At 100 Mbps, the content of a DVD-5 can be downloaded within about 5 minutes for offline access.

(OFDMA → Orthogonal FDMA IFDMA → interleaved FDMA)
(LTE → Long Term Evolution SDR → Software Defined Radio)
(MIMO → multiple-input multiple-output MU-MIMO → multiuser MIMO)
(UMTS → Universal Mobile Telecommunications System)
(MC-CDMA → multicarrier code division multiple access)

6. Explain the working of Mobile IP in detail. (10 marks)

Mobile IP is the extension of IP protocol.
Mobile IP allows mobile computers to be connected to the Internet.

Addressing

In Mobile IP, the main problem that must be solved is addressing.

Stationary Hosts

The original IP addressing assumed that a host is stationary.
A router uses an IP address to route an IP datagram.
An IP address has two parts: a prefix and a suffix.
The prefix associates a host with a network.
For example, the IP address 10.3.4.24/8 defines a host attached to the network 10.0.0.0/8.

- The address is valid only when the host is attached to the network.

If the network changes, the address is no longer valid.

Mobile Hosts

When a host moves from one network to another, the IP addressing structure needs to be modified.
The host has two addresses (Figure 19.12):

Home address &
Care-of address

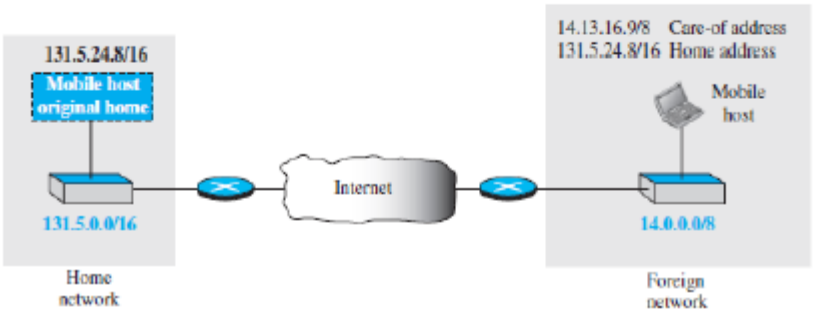
Home Address

Original address of host called the home address.
The home address is permanent.
The home address associates the host with its home network.
Home network is a network that is the permanent home of the host.

2) Care-of-Address

The care-of address is temporary.
The care-of address changes as the mobile-host moves from one network to another.
Care-of address is associated with the foreign network.
Foreign network is a network to which the host moves.
When a mobile-host visits a foreign network, it receives its care-of address during the agent discovery and registration phase.

Figure 19.12 *Home address and care-of address*

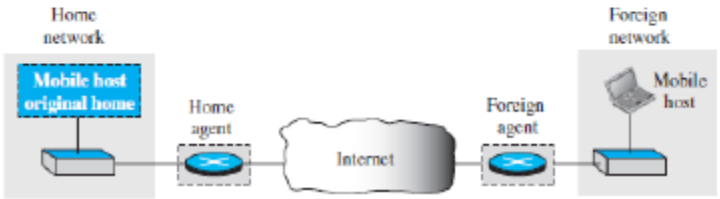


Agents

Two agents are required to make change of address transparent to rest of the Internet (Fig 19.13):

Home-agent and
Foreign-agent.

Figure 19.13 *Home agent and foreign agent*



1) Home Agent

- The home-agent is a router attached to the home network.
- The home-agent acts on behalf of mobile-host when a remote-host sends a packet to mobile-host.
- The home-agent receives and delivers packets sent by the remote-host to the foreign-agent.

2) Foreign Agent

The foreign-agent is a router attached to the foreign network.
The foreign-agent receives and delivers packets sent by the home-agent to the mobile-host.
The mobile-host can also act as a foreign-agent i.e. mobile-host and foreign-agent can be the same.
However, to do this, a mobile-host must be able to receive a care-of address by itself.
In addition, the mobile-host needs the necessary software to allow it to communicate with the home-agent and to have two addresses: i) its home address and ii) its care-of address.
This dual addressing must be transparent to the application programs.

Collocated Care-of-Address

When the mobile-host and the foreign-agent are the same, the care-of-address is called a collocated care-of-address.

Advantage:
mobile-host can move to any network w/o worrying about availability of a foreign-agent.

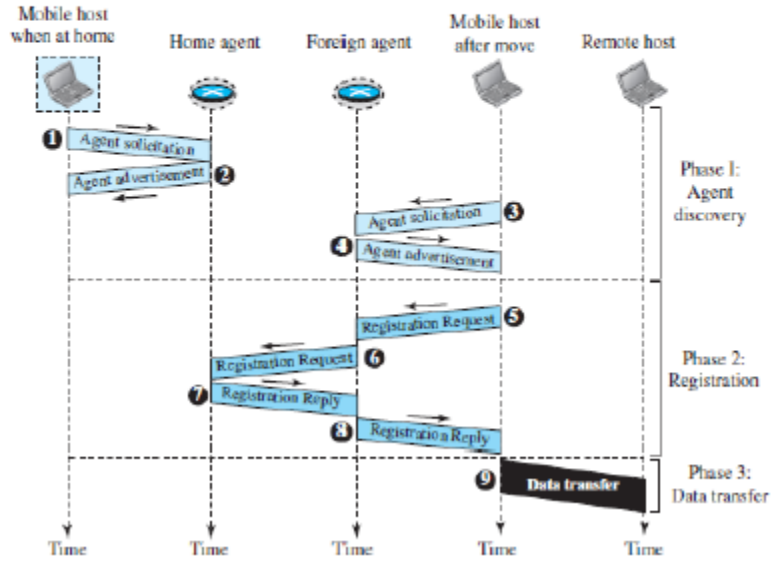
Disadvantage:
The mobile-host needs extra software to act as its own foreign-agent.

Three Phases

To communicate with a remote-host, a mobile-host goes through 3 phases (Figure 19.14):

Agent Discovery: involves the mobile-host, the foreign-agent, and the home-agent.
Registration: involves the mobile-host, the foreign-agent, and the home-agent.
Data Transfer: Here, the remote-host is also involved.

Figure 19.14 *Remote host and mobile host communication*



Agent Discovery

Agent discovery consists of two subphases:

A mobile-host must discover (learn the address of) a home-agent before it leaves its home network.

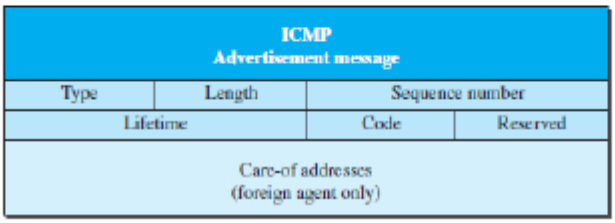
A mobile-host must also discover a foreign-agent after it has moved to a foreign network.

This discovery consists of learning the care-of address as well as the foreign-agent"s address.
Two types of messages are used: i) advertisement and ii) solicitation.

1) Agent Advertisement

• When a router advertises its presence on a network using an ICMP router advertisement, it can append an agent advertisement to the packet if it acts as an agent.

Figure 19.15 *Agent advertisement*



Various fields are (Figure 19.15):

Type

This field is set to 16.

Length

This field defines the total length of the extension message.

Sequence Number

This field holds the message number.
The recipient can use the sequence number to determine if a message is lost.

Lifetime

This field defines the number of seconds that the agent will accept requests. If the value is a string of 1s, the lifetime is infinite.

Code

This field is a flag in which each bit is set (1) or unset (0) (Table 19.1).

2) Agent Solicitation

When a mobile-host has moved to a new network and has not received agent advertisements, it can initiate an agent solicitation.

It can use the ICMP solicitation message to inform an agent that it needs assistance

Registration

After a mobile-host has moved to a foreign network and discovered the foreign-agent, it must register.

Four aspects of registration:

The mobile-host must register itself with the foreign-agent.

The mobile-host must register itself with its home-agent. This is normally done by the foreign-agent on behalf of the mobile-host.

The mobile-host must renew registration if it has expired.

The mobile-host must cancel its registration (deregistration) when it returns home.

Request & Reply

To register with the foreign-agent and the home-agent, the mobile-host uses a registration request and a registration reply.

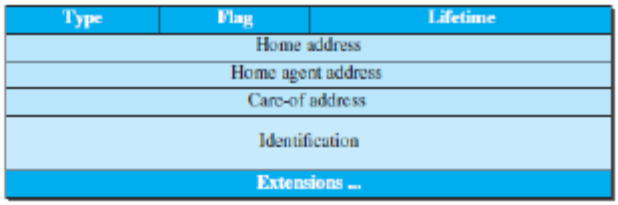
1) Registration Request

A registration request is sent from the mobile-host to the foreign-agent
to register its care-of address and
to announce its home address and home-agent address.

Foreign-agent, after receiving and registering the request, relays the message to the home-agent.

The home-agent now knows the address of the foreign-agent because the IP packet that is used for relaying has the IP address of the foreign-agent as the source address.

Figure 19.16 *Registration request format*



Various fields are (Figure 19.16):

Type
This field defines the type of message.
For a request message the value of this field is 1.

2) Flag
This field defines forwarding information.
The value of each bit can be set or unset (Table 19.2).

3) Lifetime
- This field defines the number of seconds the registration is valid.
  - i) If the field is a string of 0s, the request message is asking for deregistration.
  - ii) This field If the field is a string of 1s, the lifetime is infinite.

4) Home Address
- This field contains the permanent (first) address of the mobile-host.

5) Home Agent Address
- This field contains the address of the home-agent.

6) Care-of-Address
This field is the temporary (second) address of the mobile-host.

7) Identification
This field contains a 64-bit number that is inserted into the request by the mobile-host.
This field matches a request with a reply.

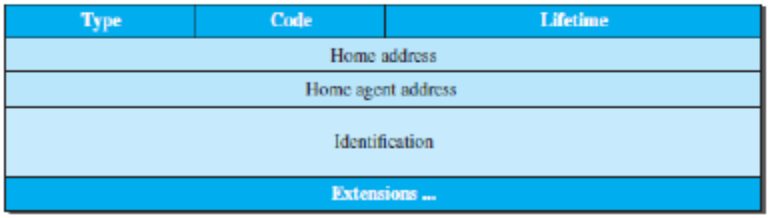
8) Extensions
This field is used for authentication.
This field allows a home-agent to authenticate the mobile agent.

2) Registration Reply

A registration reply is sent from home-agent to foreign-agent and then relayed to the mobile-host.
The reply confirms or denies the registration request. (Figure 19.17)
The fields are similar to registration request with the 3 exceptions:

The value of the type field is 3.
The code field replaces the flag field and shows the result of the registration request (acceptance or denial).
The care-of address field is not needed.

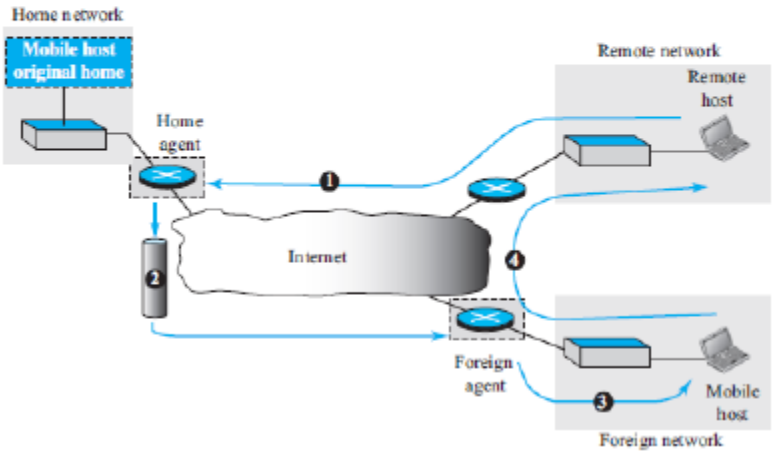
Figure 19.17 *Registration reply format*



Data Transfer

- After agent discovery & registration, a mobile-host can communicate with a remote-host (Fig 19.17).

Figure 19.18 *Data transfer*



Here we have 4 cases (Figure 19.18):

1) From Remote-host to Home Agent

When a remote-host wants to send a packet to the mobile-host, the remote-host uses
address of itself as the source address and
home address of the mobile-host as the destination address.

In other words, the remote-host sends a packet as though the mobile-host is at its home network.

The packet is intercepted by the home-agent, which pretends it is the mobile-host.

This is done using the proxy ARP technique (Path 1 of Figure 19.18).

2) From Home Agent to Foreign Agent

After receiving the packet, the home-agent sends the packet to the foreign-agent, using the tunneling concept.

The home-agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign-agent"s address as the destination. (Path 2 of Figure 19.18).

3) From Foreign Agent to Mobile Host

When the foreign-agent receives the packet, it removes the original packet.

However, since the destination address is the home address of the mobile-host, the foreign-agent consults a registry table to find the care-of address of the mobile-host. (Otherwise, the would just be sent back to the home network.)

The packet is then sent to the care-of address (Path 3 of Figure 19.18).

4) From Mobile Host to Remote Host

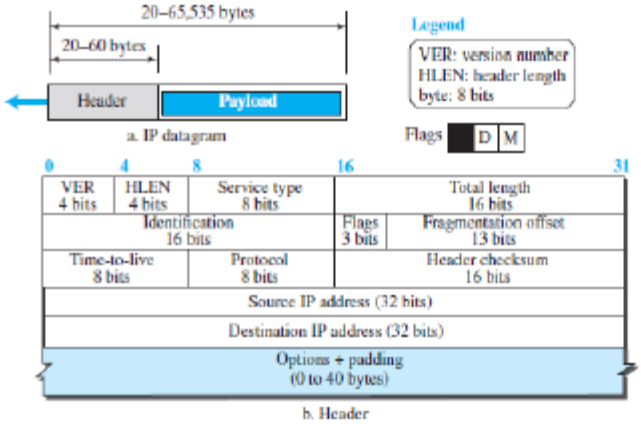
When a mobile-host wants to send a packet to a remote-host (for example, a response to the packet it has received), it sends as it does normally.

The mobile-host prepares a packet with its home address as the source, and the address of the remote-host as the destination.

Although the packet comes from the foreign network, it has the home address of the mobile-host (Path 4 of Figure 19.18).

7. Analyze the IPv4 datagram frame format with neat diagram. (10 marks)

Figure 19.2 *IP datagram*



1) Payload

Payload (or Data) is the main reason for creating a datagram.

Payload is the packet coming from other protocols that use the service of IP.

2) Header

Header contains information essential to routing and delivery.

IP header contains following fields:

1) Version Number (VER)

This field indicates version number used by the packet. Current version=4

2) Header Length (HLEN)

This field specifies length of header.

When a device receives a datagram, the device needs to know

when the header stops and

when the data starts.

3) Service Type

This field specifies priority of packet based on delay, throughput, reliability & cost requirements.

4) Total Length

This field specifies the total length of the datagram (header plus data).

Maximum length=65535 bytes.

5) Identification, Flags, and Fragmentation Offset

These 3 fields are used for fragmentation and reassembly of the datagram.

Fragmentation occurs when the size of the datagram is larger than the MTU of the network.

6) Time-to-Live (TTL)

This field is indicates amount of time, the packet is allowed to remain in the network.

If TTL becomes 0 before packet reaches destination, the router

discards packet and

sends an error-message back to the source.

7) Protocol

This field specifies upper-layer protocol that is to receive the packet at the destination-host.

For example (Figure 19.3):

For TCP, protocol = 6 For UDP, protocol = 17

8) Header Checksum

This field is used to verify integrity of header only.

If the verification process fails, packet is discarded.

9) Source and Destination Addresses

These 2 fields contain the IP addresses of source and destination hosts.

10) Options

This field allows the packet to request special features such as

security level

timestamp at each router.

This field can also be used for network testing and debugging.

11) Padding

This field is used to make the header a multiple of 32-bit words.

8(a). Write a short note on IPv6 addressing. (4 marks)

IPv6 ADDRESSING

The main reason for migration from IPv4 to IPv6 is the small size of the address-space in IPv4.
Size of IPv6 address =128 bits (four times the address length in IPv4, which is 32 bits).

Representation

- Two notations can be used to represent IPv6 addresses: 1) binary and 2) colon hexadecimal.

Binary (128 bits)	1111111011110110	...	1111111100000000
Colon Hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00		

Address Space

The address-space of IPv6 contains 2^{128} addresses.

Three Address Types

Three types of destination address: 1) Unicast 2) Anycast and 3) Multicast.

1) Unicast Address

- A unicast address defines a single interface (computer or router).
  The packet with a unicast address will be delivered to the intended recipient.

2) Anycast Address

An anycast address defines a group of computers that all share a single address.
A packet with an anycast address is delivered to only one member of the group.
The member is the one who is first reachable.

3) Multicast Address

A multicast address also defines a group of computers.
Difference between anycasting and multicasting.

In anycasting, only one copy of the packet is sent to one of the members of the group.
in multicasting each member of the group receives a copy.

Address Space Allocation

The address-space is divided into several blocks of varying size.
Each block is allocated for a special purpose.

Table 22.1 *Prefixes for assigned IPv6 addresses*

Block prefix	*CIDR*	*Block assignment*	*Fraction*
0000 0000	0000::/8	Special addresses	1/256
001	2000::/3	Global unicast	1/8
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

Global Unicast Addresses

The block in the address-space used for unicast communication b/w 2 hosts in the Internet is called global unicast address block.

CIDR for the block is 2000::/3. This means that the three leftmost bits are the same for all addresses in this block (001).

The size of this block is 2^{125} bits, which is more than enough for Internet expansion for many years to come.

An address in the block is divided into 3 parts (Figure 22.1):

Global routing prefix (n bits)
Subnet identifier (m bits) and
Interface identifier (q bits).

The global routing prefix is used to route the packet through the Internet to the organization site, such as the ISP that owns the block.

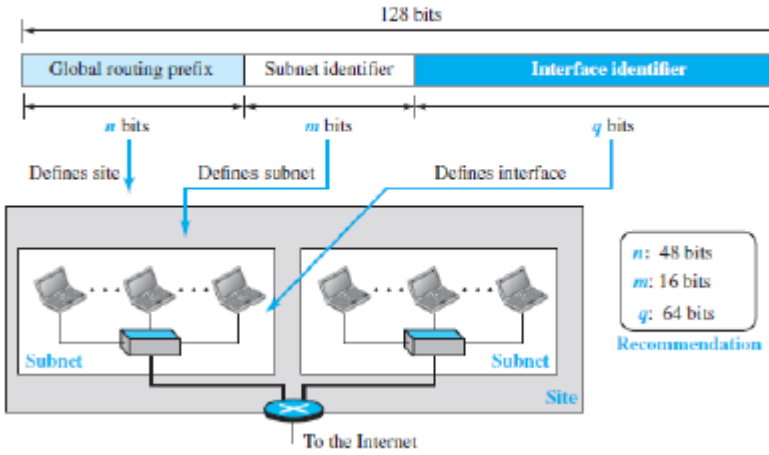
Since the first 3 bits in this part are fixed (001), the rest of the 45 bits can be defined for up to 2^{45} sites (a private organization or an ISP).

The global routers in Internet route a packet to its destination site based on the value of n.
The next m bits define a subnet in an organization.
The last q bits define the interface identifier.

Two link layer addressing schemes:

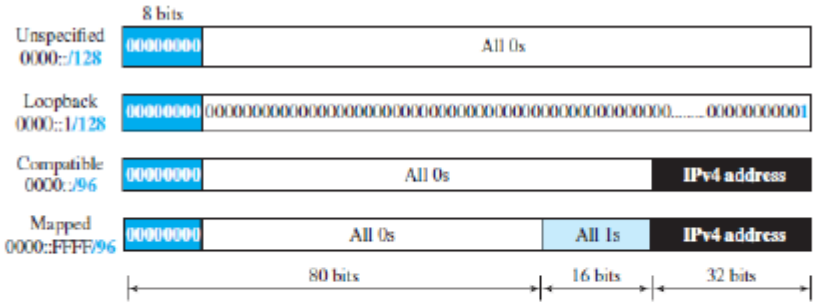
64-bit extended unique identifier (EUI-64) defined by IEEE and
48-bit link-layer address defined by Ethernet.

Figure 22.1 *Global unicast address*



Special Addresses

Figure 22.4 *Special addresses*



Following are different special addresses (Figure 22.4):

1) Unspecified Address

The unspecified address is a subblock containing only one address.

This address is used during bootstrap when a host does not know its own address and wants to send an inquiry to find it.

2) Loopback Address

The loopback address also consists of one address.

3) Transition Address

- During the transition from IPv4 to IPv6, hosts can use their IPv4 addresses embedded in IPv6 addresses.
- Two formats have been designed for this purpose: compatible and mapped.

1) Compatible Address

A compatible address is an address of 96 bits of zero followed by 32 bits of IPv4 address.

It is used when a computer using IPv6 wants to send a message to another computer using IPv6.

2) Mapped Address

A mapped address is used when a computer already migrated to version 6 wants to send an address to a computer still using version 4.

8(b). Compare the different methods of transition from IPv4 to IPv6. (6 marks)

TRANSITION FROM IPv4 TO IPv6

Strategies

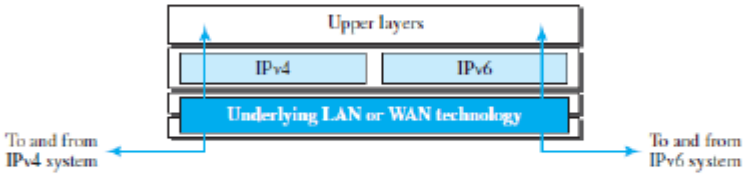
Three strategies have been devised for transition:

Dual stack
Tunneling and
Header translation.

1) Dual Stack

• Recommended: All hosts must run IPv4 and IPv6 (dual stack) simultaneously until all the Internet uses IPv6 (Figure 22.11).

Figure 22.11 *Dual stack*

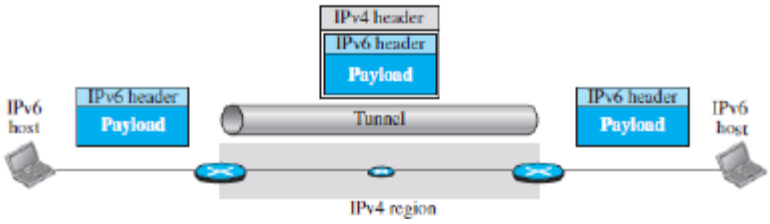


To determine which version to use, the source queries the DNS.
If the DNS returns an IPv4 address, the source sends an IPv4 packet.
If the DNS returns an IPv6 address, the source sends an IPv6 packet.

2) Tunneling

Tunneling is a strategy used when
two computers using IPv6 want to communicate with each other and
the packet must pass through an IPv4 network.
To pass through IPv4 network, the packet must have an IPv4 address (Figure 22.12).
So,
IPv6 packet is encapsulated in an IPv4 packet when the packet enters the IPv4 network.
IPv6 packet is decapsulated from an IPv4 packet when the packet exits the IPv4 network.

Figure 22.12 *Tunneling strategy*



3) Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4 (Figure 22.13).
The sender wants to use IPv6, but the receiver does not understand IPv6.
Tunneling does not work in this situation because
the packet must be in the IPv4 format to be understood by the receiver.
In this case, the header format must be totally changed through header translation.
The header of the IPv6 packet is converted to an IPv4 header.

Figure 22.13 *Header translation strategy*