MODULE 5

OTHER WIRELESS NETWORKS

5.1 WiMAX

- WiMAX stands for Worldwide Interoperability for Microwave Access.
- WiMAX provides the "last mile" broadband wireless access.

Purpose of WiMAX:

- People want to have access to the Internet from home or office (fixed) where the wired
- access to the Internet is either not available or is expensive.
- People need to access the Internet when they are using their cellular phones (mobiles).

5.1.1 Services

WiMAX provides 2 types of services to subscribers:

- Fixed.
- Mobile.

1) Fixed WiMAX

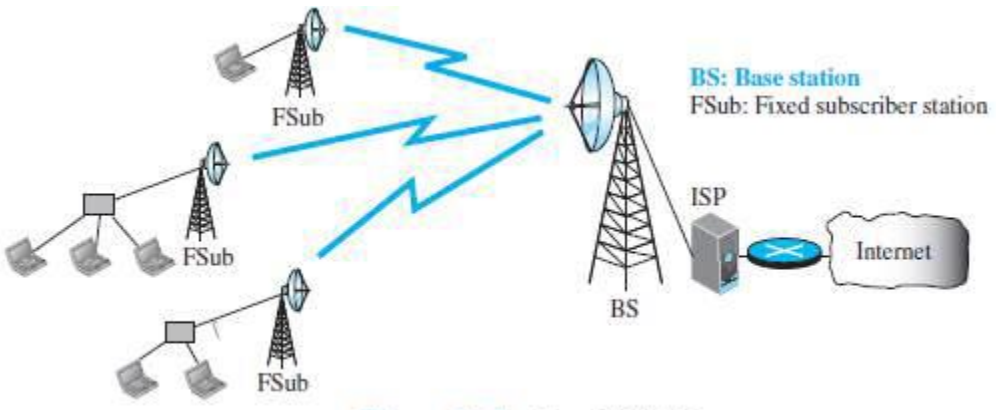


Figure 16.1 *Fixed WiMAX*

- A base-station can use 3 different types of antenna to optimize the performance:1) Omni-directional 2) Sector or 3) Panel.
- WiMAX uses a beam-steering AAS (Adaptive Antenna System).
- While transmitting, antenna can focus its energy in the direction of the subscriber-station.

- While receiving, antenna can focus in the direction of the subscriber-station to receive maximum energy sent by the subscriber.

2) Mobile WiMAX

- The subscribers are mobile-stations that move from one place to another

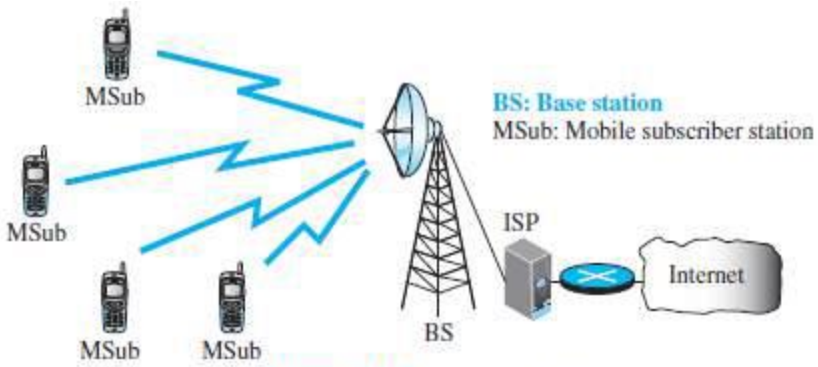


Figure 16.2 *Mobile WiMAX*

5.1.2 IEEE Project 802.16

- WiMAX is the result of the IEEE 802.16 project.
- The standard is also referred to as wireless local loop.

802.11 Projects 802.16 Projects	802.11 Projects 802.16 Projects
Standard for a wireless LAN Standard for a wireless WAN	Standard for a wireless LAN Standard for a wireless WAN
Defines a connectionless communication Defines a connection-oriented service	Defines a connectionless communication Defines a connection-oriented service
Distance b/w base-station & host is very limited Distance b/w base-station & host is above 10 km	Distance b/w base-station & host is very limited Distance b/w base-station & host is above 10 km

- IEEE 802.16 was revised into 2 new standards:
  - IEEE 802.16d which concentrates on the fixed WiMAX.
  - IEEE 802.16e which defines the mobile WiMAX.

5.1.3 Layers in Project 802.16

- The data-link layer is divided into 3 sublayers:
  - Service Specific Convergence Sublayer
  - Security Sublayer
  - MAC Sublayer.
- The physical layer is divided into 2 sublayers:
  - Transmission Convergence Sublayer

- Physical Medium Dependent Sublayer.

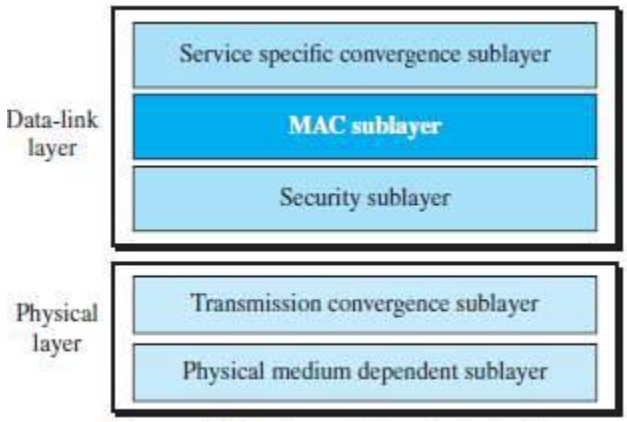


Figure 16.3 *Data-link and physical layers*

5.1.3.1 Data Link layer

1) Service Specific Convergence Sublayer

- This is actually the DLC sublayer revised for broadband wireless communication.
- It is devised for a connection-oriented service where each connection may benefit from a specific QoS

2) Security Sublayer

- This sublayer provides security for communication using WiMAX.
- The nature of wireless communication requires security.
- Security provided using encryption for information exchanged b/w subscriber-station & base-station.

3) MAC Sublayer

- The MAC sublayer defines the access method and the format of the frame.
- This sublayer is designed for connection-oriented service.
- The packets are routed from the base-station to the subscriber-station using a connection identifier.
- Connection identifier remains same during the duration of the communication.

5.1.3.2 Physical Layer

1) Transmission Convergence Sublayer

- This sublayer uses TDD.
- TDD a variation of TDM designed for duplex (bidirectional) communication.

- Each frame is made of 2 subframes: Downstream and Upstream subframes.
  - **Downstream Subframes:** carry data from the base-station to the subscribers.
  - **Upstream Subframes:** carry data from the subscribers to the base-station.
- Each subframe is divided into slots.

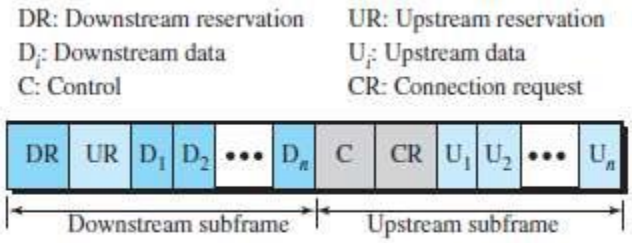


Figure 16.5 *WiMAX frame structure at the physical layer*

2) Physical Medium Dependent Sublayer

- This sublayer is in continuous revision.
- Originally, 802.16 defined the band 10-66 GHz.
- 802.16 defined following modulations:
  - QPSK used for long-distance communication.
  - QAM-16 used for medium-distance communication.
  - QAM-64 used for short-distance communication.
  - Later, IEEE defined 802.16d (fixed WiMAX), which added the band 2-11 GHz (compatible with wireless LANs) using the OFDM.
  - Sometime later, IEEE defined 802.16e (mobile WiMAX) and added SOFDM.
    (TDD:Time-Division Duplex, FEC-forward error correction)
    (OFDM: Orthogonal Frequency-Division Multiplexing)
    (SOFDM :scalable orthogonal frequency division multiplexing)

5.1.3.3 MAC Sublayer

- The MAC sublayer defines the access method and the format of the frame.
- This sublayer is designed for connection-oriented service.
- The packets are routed from the base-station to the subscriber-station using a connection identifier.
- Connection identifier remains same during the duration of the communication.

1) Access Method

- WiMAX uses the reservation (scheduling) access method.
- Base-station needs to make a slot-reservation before sending a data to a subscriber-station
- Each subscriber-station needs to make a reservation before sending a data to the base-station

2) Frame Format

- There are two types of frames:
  - Generic Frame is used to send and receive payload.
  - Control Frame is used only during the connection establishment.
- Both frame-types use a 6-byte generic header.
- However, some bytes have different interpretations in different frame types.

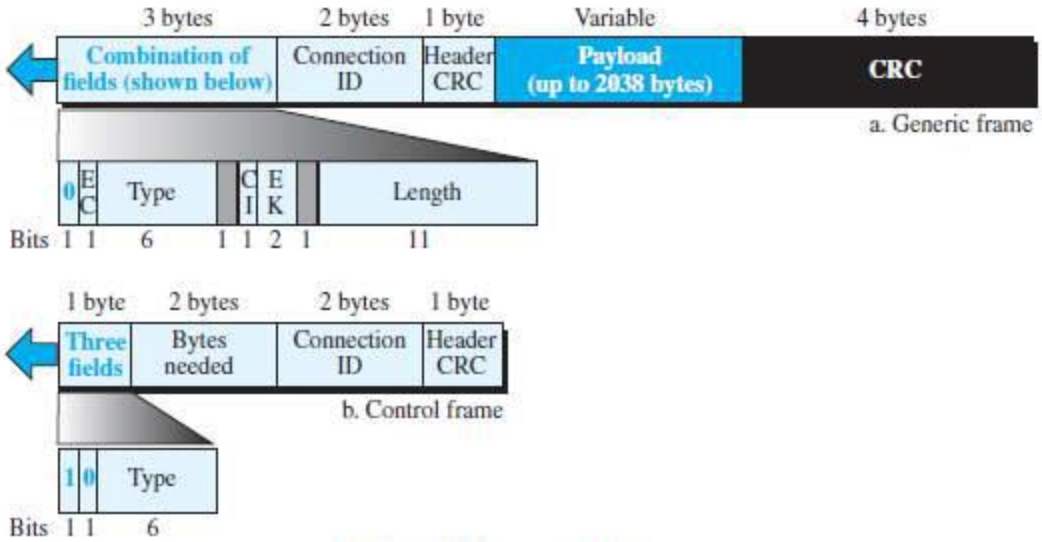


Figure 16.4 *WiMAX MAC frame format*

The frame contains following fields:

- **First bit**
  - The first bit in a frame is the frame identifier.
  - If first bit = 0, the frame is a generic frame.
  - If first bit = 1, the frame is a control frame.

- **EC (Encryption Control)**
  - This field uses one bit to define whether the frame should be encrypted for security purpose.
  - If EC = 0, it means no encryption.
  - If EC = 1, it means the frame needs to be encrypted at the security sublayer.
- **Type**
  - This field is used to define the type of the payload.
  - This field is only present in the generic frame.
  - The payload can be a packed-load or a fragmented-load.
- **CI (Checksum ID)**
  - This field defines whether the checksum field should be present or not.
  - If the payload is multimedia, FEC is applied to the frame and there is no need for checksum.
- **EK (Encryption Key)**
  - This field defines one of the 4 keys for encryption if encryption is required.
- **Length**
  - This field defines the total length of the frame.
  - This field is only present in the generic frame.
  - This field is replaced by the bytes needed field in the control frame.
- **Bytes Needed**
  - This field defines the number of bytes needed for allocated slots in the physical layer.
- **Connection ID**
  - This field defines the connection identifier for the current connection.
- **Header CRC**
  - Both types of frames need to have header CRC field.
  - Header CRC is used to check whether the header itself is corrupted.
  - This field uses the polynomial ($x^8 + x^2 + x + 1$) as the divisor.
- **Payload**
  - This field defines the payload.
  - Payload is encapsulated in the frame from the service specific convergence sublayer.
  - This field is not needed in the control frame.

- **CRC**
  - This field is used for error detection over the whole frame.

3) Addressing

- Each subscriber and base-station typically has a 48-bit MAC address.
- However, there is no source or destination address field.
- The reason is that the combination of source and destination addresses are mapped to a VCI during the connection-establishing phase.
- This protocol is a connection-oriented protocol that uses a VCI (Virtual Connection Identifier).
- Then, each frame uses the same connection identifier for the duration of data transfer.

5.2 CELLULAR TELEPHONY

- Cellular telephony is designed to provide communications between two moving units called mobile-stations (MSs) and between one mobile-station and one stationary unit called a land unit.
- 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.

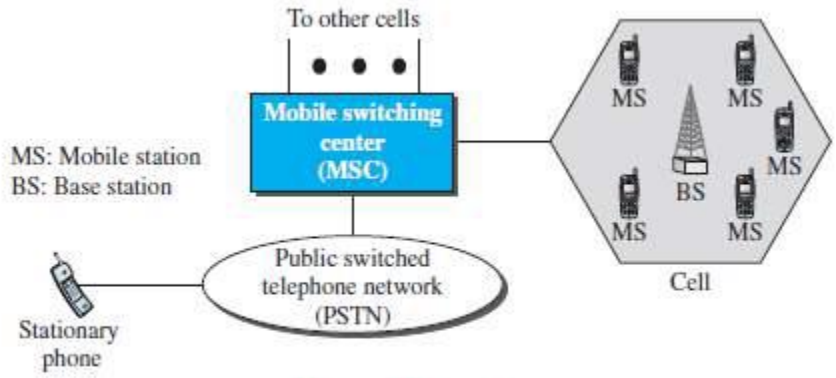


Figure 16.6 *Cellular system*

5.2.1 Operation

5.2.1.1 Frequency-Reuse Principle

- In general, neighbouring-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.

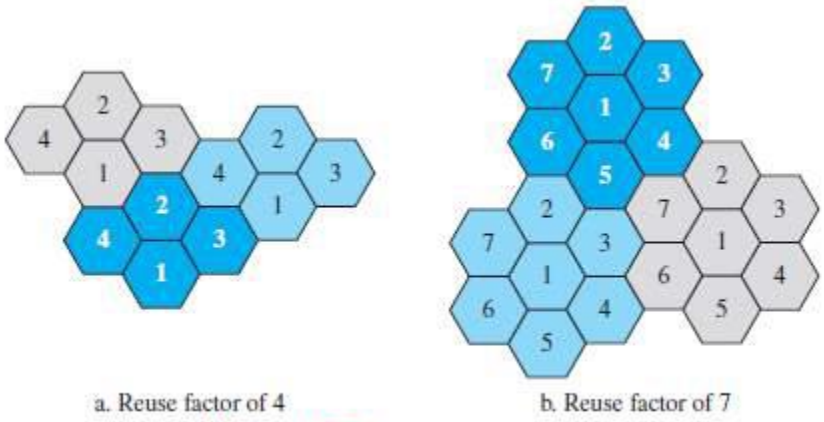


Figure 16.7 *Frequency reuse patterns*

5.2.1.2 Transmitting

Procedure to place a call from a mobile-station:

1) The caller

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

2) 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.

3) The base-station sends the data to the MSC.

4) The MSC sends the data on to the telephone central office.

5) If called party is available, a connection is made and the result is relayed back to the MSC.

6) The MSC assigns an unused voice channel to the call, and a connection is established.

7) The mobile-station automatically adjusts its tuning to the new channel.

8) Finally, voice communication can begin.

5.2.1.3 Receiving

Procedure to receive a call from a mobile-station:

1) When a mobile phone is called, the telephone central office sends phone number to the MSC.

2) MSC searches for the location of the mobile-station by sending query-signals to each cell in a process. This is called paging.

3) When the mobile-station is found, the MSC transmits a ringing signal.

4) When the mobile-station answers, the MSC assigns a voice channel to the call.

5) Finally, voice communication can begin.

5.2.1.4 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

Hard Handoff

- Early systems used a hard handoff.
- 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.

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.

5.2.1.5 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.
- Neighbouring service-providers can provide extended coverage through a roaming contract.

5.2.2 First Generation (1G)

- The first generation was designed for voice communication using analog signals.
- The main system evolved in the first generation: AMPS (Advanced Mobile Phone System).

5.2.2.1 AMPS

- This system is a 1G analog cellular system.
- The system uses FDMA to separate channels in a link.
- Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

- The system operates in the ISM 800-MHz band.
- The system uses 2 separate channels (Figure 16.8):
- First channel is used for forward communication (base-station to mobile-station)
- Band range: 869 to 894 MHz
- Second channel is used for reverse communication (mobile-station to base-station).

- Band range: 824 to 849 MHz.

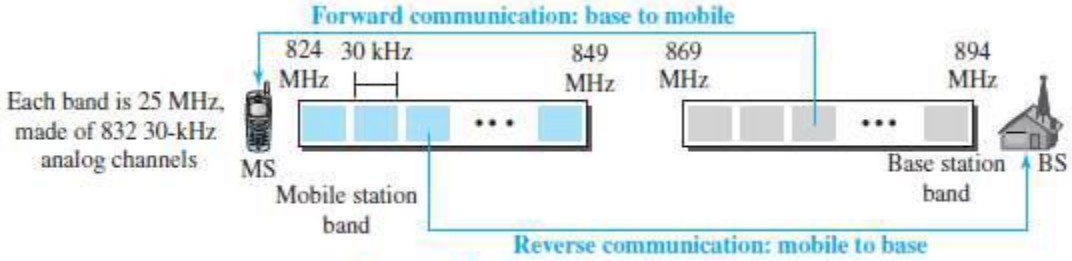


Figure 16.8 *Cellular bands for AMPS*

2) Transmission

- The system uses FM and FSK for modulation (Figure 16.9).
- Voice channels are modulated using FM.
- Control channels are modulated using FSK to create 30-kHz analog signals.
- The system uses FDMA to divide each 25-MHz band into 30-kHz channels.

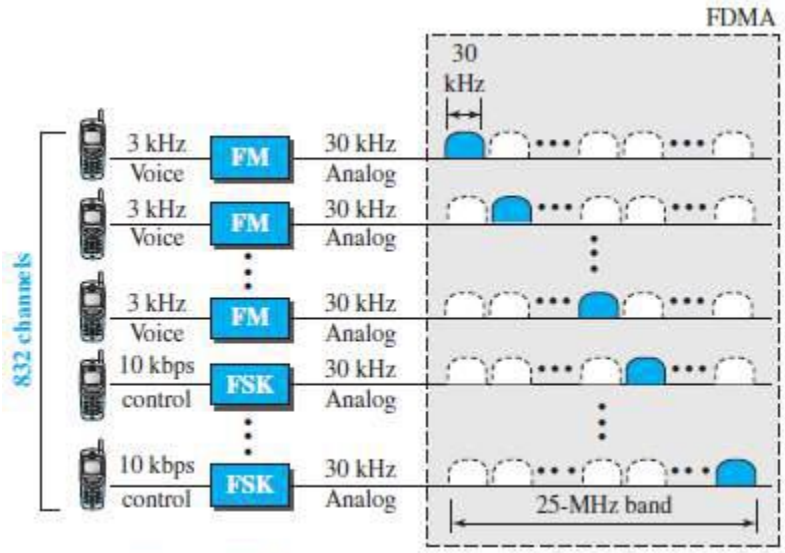


Figure 16.9 *AMPS reverse communication band*

5.2.3 Second Generation (2G)

- The second generation was designed for higher-quality voice communication using digital signals.
- 1G vs. 2G:
  - The first generation was designed for analog voice communication.
  - The second generation was mainly designed for digital voice communication.
- Three major systems evolved in the second generation: D-AMPS (digital AMPS) , GSM (Global System for Mobile communication) and IS-95 (Interim Standard).

5.2.3.1 D-AMPS

- D-AMPS (Digital AMPS) was improved version of analog AMPS.
- D-AMPS was backward-compatible with AMPS.
- Thus, in a cell, First telephone may use AMPS and Second telephone may use D-AMPS.
- Here we discuss, two issues: 1) Bands 2) Transmission

1) Band-The system uses the same bands and channels as AMPS (Figure 16.10).

2) Transmission- Each voice channel is digitized using a very complex PCM and compression technique.

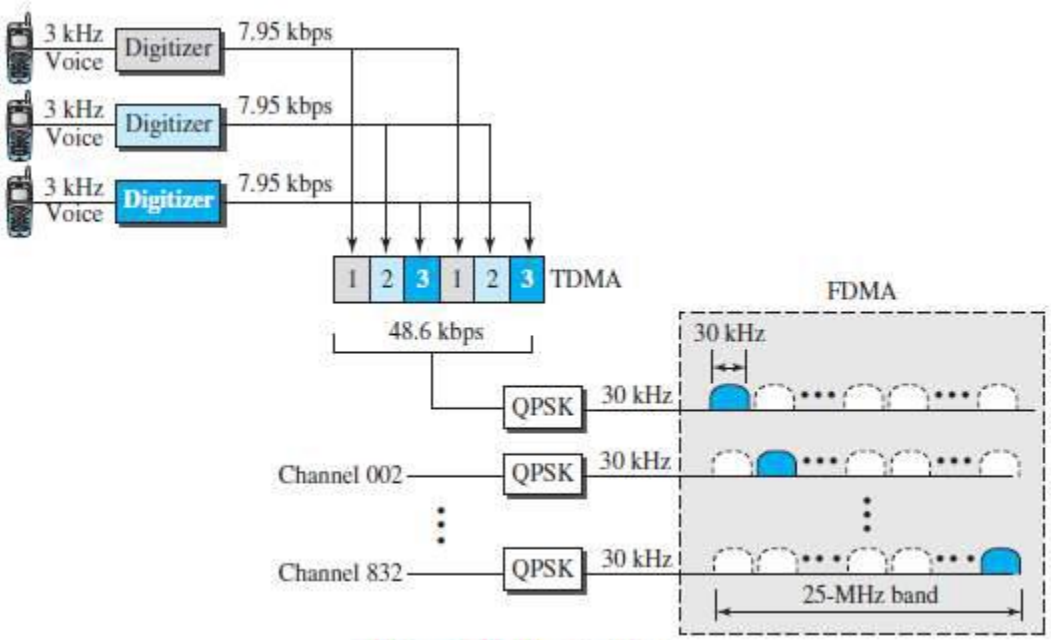


Figure 16.10 *D-AMPS*

5.2.3.2 GSM

- Aim of GSM: to replace a number of incompatible 1G technologies.
- Here we discuss, two issues: 1) Bands 2) Transmission

1) Bands

- The system uses two bands for duplex communication (Figure 16.11).
- Each band is 25 MHz in width.
- Each band is divided into 124 channels of 200 kHz.

2) Transmission

- Each voice channel is digitized and compressed to a 13-kbps digital signal (Figure 16.12).

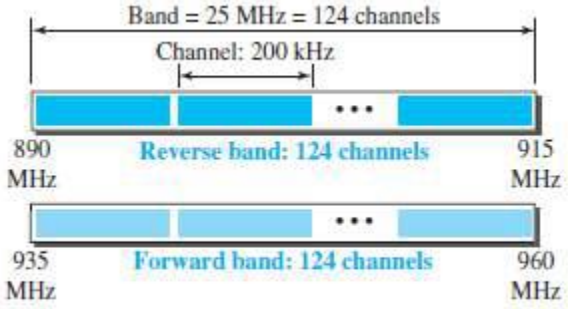


Figure 16.11 *GSM bands*

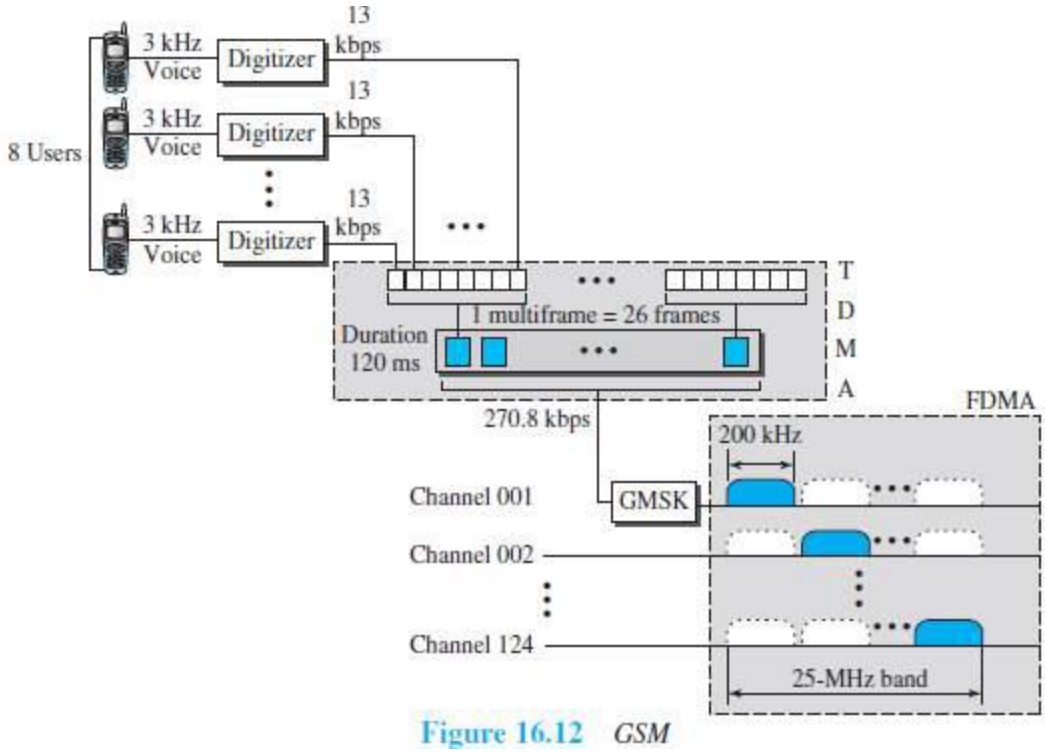


Figure 16.12 *GSM*

- Each slot carries 156.25 bits. Eight slots share a frame (TDMA) and 26 frames also share a multiframe (TDMA).
- Each 270.8-kbps digital channel modulates a carrier using GMSK (a form of FSK), the result is a 200-kHz analog signal.
- Finally, 124 analog channels of 200 kHz are combined using FDMA. The result is a 25-MHz band (Figure 16.13).

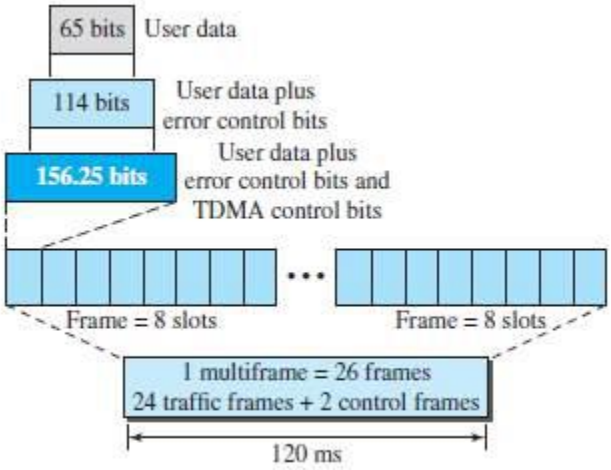


Figure 16.13 *Multiframe components*

5.2.3.3 IS-95

- The system is based on CDMA and DSSS.
- Here we discuss, following 6 issues: 1) Bands 2) Transmission 3) Synchronization
- Two Data-rate Sets 5) Frequency-Reuse Factor 6) Soft Handoff

1) Bands

- The system uses two bands for duplex communication.
- The bands can be ISM 800-MHz band or ISM 1900-MHz band.
- Each band is divided into 20 channels of 1.228 MHz.
- Each service-provider is allotted 10 channels.
- IS-95 can be used in parallel with AMPS.
- Each IS-95 channel is equivalent to 41 AMPS channels (41 × 30 kHz = 1.23 MHz).

2) Transmission

Two types of Transmission:

i) Forward Transmission (base to mobile)

- Communications between the base and all mobiles are synchronized.
- The base sends synchronized data to all mobiles (Figure 16.14).

ii) Reverse Transmission (mobile to base)

- The use of CDMA in the forward direction is possible because the pilot channel sends a continuous sequence of 1s to synchronize transmission.
- The synchronization is not used in the reverse direction because we need an entity to
- do that, which is not feasible.
- Instead of CDMA, the reverse channels use DSSS (Figure 16.15).

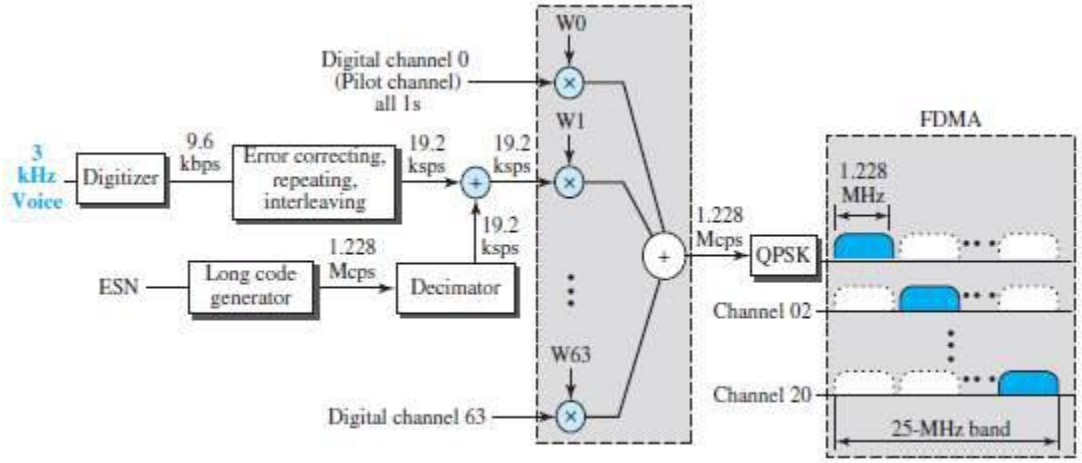


Figure 16.14 *IS-95 forward transmission*

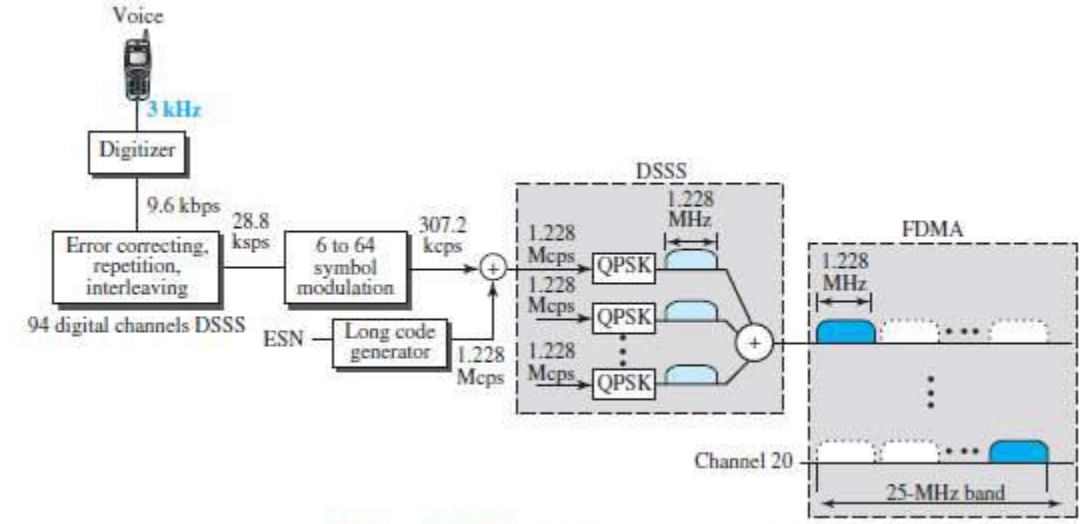


Figure 16.15 *IS-95 reverse transmission*

3) Synchronization

- All base channels need to be synchronized to use CDMA.
- To provide synchronization, bases use the services of a satellite system (GPS).

4) Two Data Rate Sets

IS-95 defines two data-rate sets:

i) The first set defines 9600, 4800, 2400, and 1200 bps.

ii) The second set defines 14,400, 7200, 3600, and 1800 bps.

5) Frequency-Reuse Factor

- The frequency-reuse factor is normally 1 because the interference from neighboring cells cannot affect CDMA or DSSS transmission.

6) Soft Handoff

- Every base-station continuously broadcasts signals using its pilot channel.
- Thus, a mobile-station can detect the pilot signal from its cell and neighboring cells. This enables a mobile-station to do a soft handoff.

5.2.4 Third Generation (3G)

- 3G cellular telephony provides both digital data and voice communication.
- For example: Using a Smartphone, A person can talk to anyone else in the world. A person can download a movie, surf the Internet or play games.
- Interesting characteristics: the Smartphone is always connected; we do not need to dial a number to connect to the Internet. (IMT Internet Mobile Communication)

Some objectives defined by the blueprint IMT-2000 (3G working group):

1) Voice quality comparable to that of the existing public telephone network.

2) Data-rate of

→ 144 kbps for access in a moving vehicle (car)

→ 384 kbps for access as the user walks (pedestrians) and

→ 2 Mbps for the stationary user (office or home).

3) Support for packet-switched and circuit-switched data services.

4) A band of 2 GHz.

5) Bandwidths of 2 MHz.

6) Interface to the Internet.

5.2.4.1 IMT-2000 Radio Interfaces

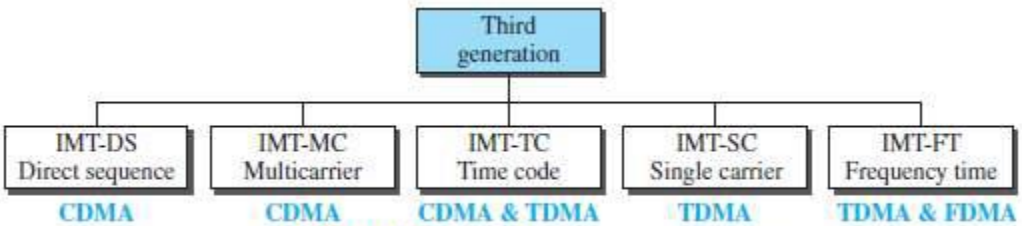


Figure 16.16 *IMT-2000 radio interfaces*

Radio interfaces (wireless standards) adopted by IMT-2000 (Figure 16.16):

1) IMT-DS

- This uses a version of CDMA called W-CDMA (wideband CDMA).

- W-CDMA uses a 5-MHz bandwidth and It is compatible with the CDMA used in IS-95.

2) IMT-MC

- This was known as CDMA 2000.
- It is an evolution of CDMA technology used in IS-95 channels.
- It combines new wideband (15-MHz) spread spectrum & narrowband (1.25-MHz) CDMA of IS-95.
- It is backward-compatible with IS-95.
- It allows communication on multiple 1.25-MHz channels up to 15 MHz.

3) IMT-TC

- This uses a combination of W-CDMA and TDMA.
- It tries to reach the IMT-2000 goals by adding TDMA multiplexing to W-CDMA.

4) IMT-SC

- This uses only TDMA.

5) IMT-FT

This uses a combination of FDMA and TDMA.

5.2.5 Fourth Generation (4G)

- 4G cellular telephony is expected to be a complete evolution in wireless communications.

Some objectives defined by the 4G working group:

1) A spectrally efficient system.

2) High network capacity.

3) 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.

4) Smooth handoff across heterogeneous networks.

5) Seamless connectivity and global roaming across multiple networks.

6) High quality of service for next generation multimedia support.

7) Interoperability with existing wireless standards.

8) All IP, packet-switched, networks.

- 4G is only packet-based networks and supports IPv6.
- 4G provides better multicast, security, and route optimization capabilities.
- Here we discuss, following issues: 1) Access Scheme 2) Modulation 3) Radio System Antenna 5) Applications

1) Access Scheme

- To increase efficiency, capacity, scalability new access techniques are being considered for 4G.
- For example: OFDMA and IFDMA are being considered for the downlink & uplink of the next generation UMTS. 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)

5.3 SATELLITE NETWORKS

- A satellite network is a combination of nodes that provides communication from one point on the Earth to another.
- A node can be Satellite,Earth station or End-user terminal/telephone
- Like cellular networks, satellite networks divide the planet into cells. Satellites can provide transmission capability to and from any location on Earth.
- Advantages:
    - Satellite makes high-quality communication available to undeveloped parts of the world.
    - Cost effective: A huge investment in ground-based infrastructure is not required.

5.3.1 General Issues for Operation of Satellites

Three issues related to the operation of satellites are Orbits, Footprint and Frequency Bands for Satellite Communication

1) Orbits

- An artificial satellite needs to have an orbit.
- An orbit is the path in which the satellite travels around the Earth.
- The orbit can be equatorial, inclined, or polar (Figure 16.17.)

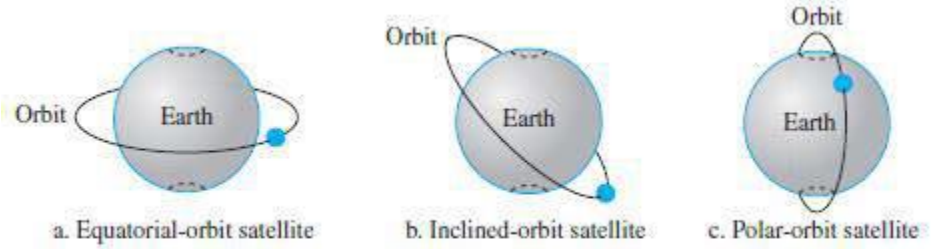


Figure 16.17 *Satellite orbits*

- The period means the time required for a satellite to make a complete trip around the Earth.
- The period of a satellite is determined by Kepler‟s law.
- Kepler‟s law defines period as a function of the distance of the satellite from the center of the Earth.

Example 5.1

What is the period of the moon, according to Kepler's law?

$$\text{Period} = C \times \text{distance}^{1.5}$$

Here C is a constant approximately equal to 1/100. The period is in seconds and the distance in kilometers.

Solution

The moon is located approximately 384,000 km above the Earth. The radius of the Earth is 6378 km. Applying the formula, we get the following.

$$\text{Period} = (1/100) \times (384{,}000 + 6378)^{1.5} = 2{,}439{,}090 \text{ s} = 1 \text{ month}$$

Example 5.2

According to Kepler's law, what is the period of a satellite that is located at an orbit approximately 35,786 km above the Earth?

Solution

Applying the formula, we get the following.

$$\text{Period} = (1/100) \times (35{,}786 + 6378)^{1.5} = 86{,}579 \text{ s} = 24 \text{ h}$$

This means that a satellite located at 35,786 km has a period of 24 h, which is the same as the rotation period of the Earth. A satellite like this is said to be *stationary* to the Earth. The orbit is called a *geostationary orbit*.

2) Footprint

- Satellites process microwaves with bidirectional antennas (line-of-sight).
- Normally, the signal from a satellite is aimed at a specific area called the footprint.
- The signal-power at the center of the footprint is maximum.
- The signal-power decreases, as we move out from the footprint-center.
- The boundary of the footprint is the location where the power-level is at a predefined threshold.

3) Frequency Bands for Satellite Communication

- For satellite communication, the frequencies reserved are in the GHz range.
- Each satellite sends and receives over 2 different bands (Table 16.1):

  1) Uplink: refers to the transmission from the Earth to the satellite.

  2) Downlink: refers to the transmission from the satellite to the Earth.

Table 16.1 *Satellite frequency bands*

Band	*Downlink, GHz*	*Uplink, GHz*	*Bandwidth, MHz*
L	1.5	1.6	15
S	1.9	2.2	70
C	4.0	6.0	500
Ku	11.0	14.0	500
Ka	20.0	30.0	3500

4) Three Categories of Satellites

Three categories of satellites based on the location of the orbit (Figure 16.18):

- **Geostationary Earth orbit (GEO):**There is only one orbit, at an altitude of 36000 km, for the GEO satellite.
- **Low-Earth-orbit (LEO) :** LEO satellites are below an altitude of 2000 km.
- **Medium-Earth-orbit (MEO):** MEO satellites are located at altitudes between 5000 and 15,000 km.

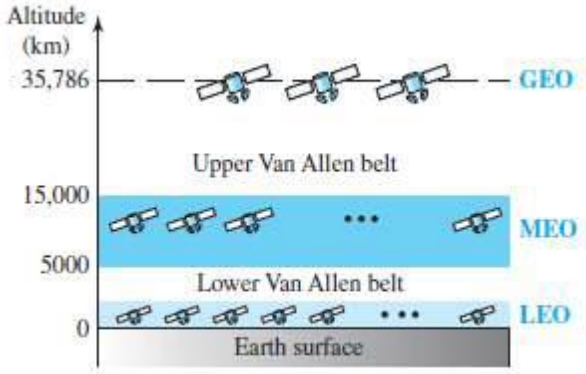


Figure 16.18 *Satellite orbit altitudes*

5.3.2 GEO Satellites

- There is only one orbit at an altitude of 36,000 km (Figure 16.19).
- Because orbital speed is based on the distance from the planet, only one orbit can be geostationary.
- The orbit occurs at the equatorial plane.
- Sending-antenna must have receiving-antenna in LOS (Line-of-sight).
- Problem: A satellite that moves faster/slower than Earth"s rotation is useful only for short periods.
- Solution: To ensure constant communication, the satellite must move at same speed as the Earth.Thus, the satellite seems to remain fixed above a certain spot.

Figure 16.19 *Satellites in geostationary orbit*

5.3.3 MEO Satellites

- MEO satellites are located at altitudes between 5000 and 15,000 km.
- Example: Global Positioning System (GPS)

5.3.3.1 Global Positioning System

- GPS consists of 24 satellites in 6 orbits (Figure 16.20).
- GPS is used for land, sea, and air navigation to provide time and location for vehicles and ships.
- The orbits and the locations of the satellites in each orbit are designed systematically.
- For example: At any time, 4 satellites are visible from any point on Earth.
- A GPS receiver has an almanac (or calendar) that tells the current position of each satellite.
- Here we discuss, 4 issues: Trilateration,Measuring the Distance, Synchronization & Application.

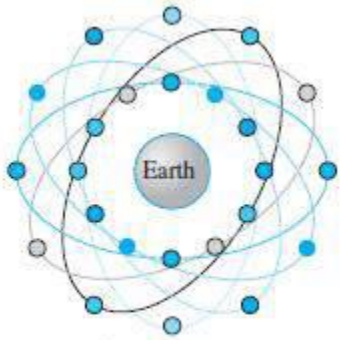


Figure 16.20 *Orbits for global positioning system (GPS) satellites*

1) Trilateration

GPS is based on a principle called trilateration.Trilateration means using three distances. **For example in Figure 16.21a**. On a plane, if we know our distance from three points, we know exactly where we are. Assume we are 10 miles away from point A, 12 miles away from point B, and 15 miles away from point C. If we draw three circles with the centers at A, B, and C, we must be somewhere on circle A, somewhere on circle B, and somewhere on circle C. These three circles meet at one single point; this is our position (Figure 16.21a).

a. Two-dimensional trilateration b. Three-dimensional trilateration

Figure 16.21 *Trilateration on a plane*

2) Measuring the Distance

- Trilateration principle can find our location on the Earth if we know our distance from 3 satellites and position of each satellite.
- The position of each satellite can be calculated by a GPS receiver. Then, the GPS receiver needs to find its distance from at least three GPS satellites.
- The distance is measured using a principle called one-way ranging.

3) Synchronization

- Satellites use atomic clocks, which are precise and can function synchronously with each other.
- The receiver‟s clock is a normal quartz clock. However, there is no way to synchronize receiver‟s clock with the satellite‟s clock.
- There is an unknown offset between the satellite-clocks and the receiver-clock. The unknown offset introduces a corresponding offset in the distance calculation. Because of the offset, the measured distance is called a pseudo-range.

4) Applications

- GPS is used by military forces. For example: Thousands of portable GPS receivers were used during the WW2 by foot soldiers, vehicles, and helicopters.
- GPS is used in navigation. For example: The driver of a car can find the location of the car.
- GPS is used for clock synchronization.

5.3.4 LEO Satellites

- LEO satellites have polar orbits. Usually, a LEO system has a cellular type of access (similar to the cellular telephone system).
- Specifications:
  - Altitude = 500 to 2000 km
  - Rotation Period = 90 to 120 min
  - Satellite Speed =20,000 to 25,000 km/h
  - Footprint Diameter = 8000 km
  - Round-Trip Time < 20 ms
- Because LEO satellites are close to Earth, 20 ms RTT is normally acceptable for audio communication.
- A LEO system is made of a group of satellites that work together as a network. Each satellite acts as a switch.

Different types of links (Figure 16.22):

1) ISLs (Inter-Satellite Links): Satellites that are close to each other are connected through ISLs.

2) UML (User Mobile Link): A mobile system communicates with the satellite through a UML.

3) GWL (Gate Way Link): A satellite communicates with the Earth station (gateway) through a GWL.

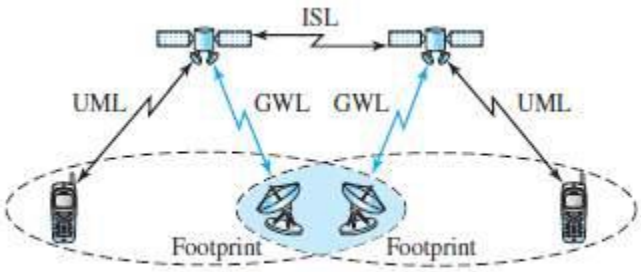


Figure 16.22 *LEO satellite system*

LEO satellites can be divided into three categories:

1) Little LEO

- Operating frequency < 1 GHz.
- They are mostly used for low data-rate messaging.

2) Big LEO

- Operating frequency = 1 to 3 GHz.
- Examples: Globalstar & Iridium

	Globalstar	Globalstar Iridium
Orbit-Altitude	1400 km	750 km
No. of Satellites	48	66
No. of Orbits	6	6
Satellites per Orbit	8 11	11

3) Broadband LEO

- Broadband LEO provides communication similar to fiber-optic networks.
- Example: Teledesic. This satellite provides fiber-optic-like communication (broadband channels, low error rate, and low delay).
- Main purpose: To provide broadband Internet access for users all over the world.

Network Layer Protocols

The network layer contains following 4 protocols (Figure 19.1):

1) Internet Protocol (IP)

- IP is the main protocol responsible for packetizing, forwarding, and delivery of a packet at the network layer.

2) Internet Control Message Protocol (ICMP)

- ICMP helps IP to handle some errors that may occur in the network-layer delivery.

3) Internet Group Management Protocol (IGMP)

- IGMP is used to help IPv4 in multicasting.

4) Address Resolution Protocol (ARP)

- ARP is used to glue the network and data-link layers in mapping network-layer addresses to link-layer addresses.

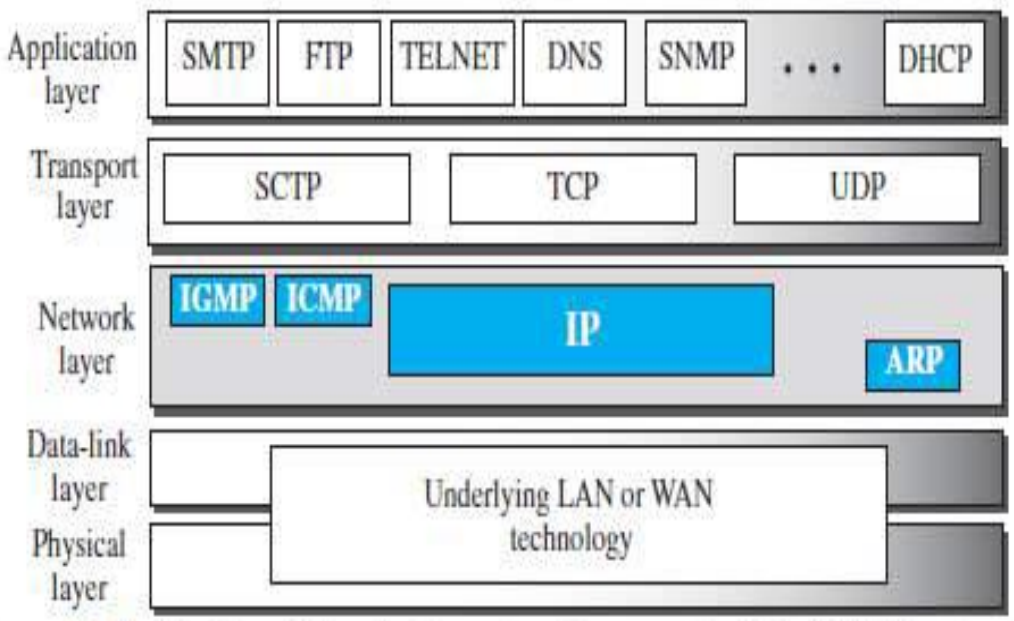


Figure 19.1 *Position of IP and other network-layer protocols in TCP/IP protocol suite*

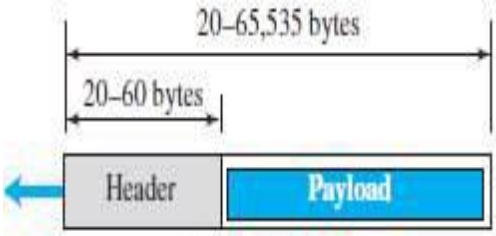
5.5 INTERNET PROTOCOL (IP)

5.5.1 Internet Protocol (IP)

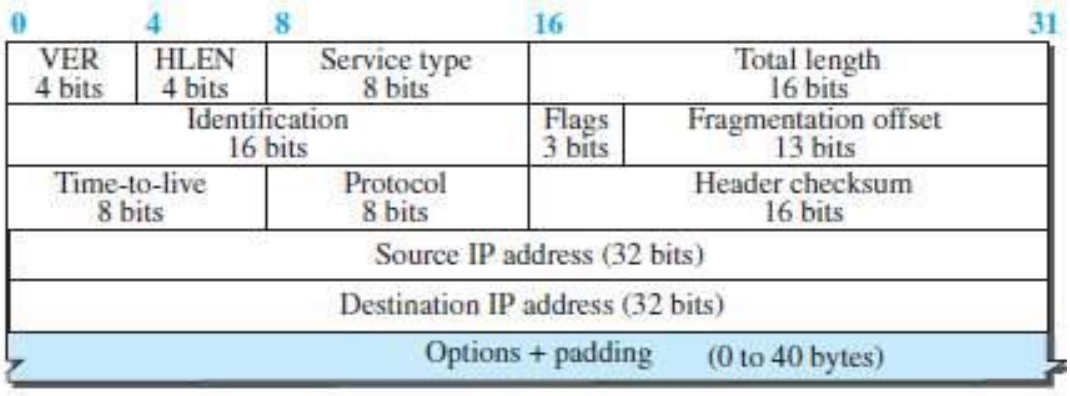
- IP is main protocol responsible for packetizing, forwarding & delivery of a packet at network layer.
- IP is an unreliable datagram protocol.
- IP provides a best-effort delivery service.
- The term best-effort means that the packets can be corrupted, be lost or arrive out-of-order.
- If reliability is important, IP must be paired with a TCP which is reliable transport-layer protocol.
- IP is a connectionless protocol.
- IP uses the datagram approach.
  1) Each datagram is handled independently.
  2) Each datagram can follow a different route to the destination.
  3) Datagrams may arrive out-of-order at the destination.

5.5.2 Datagram Format

- IP uses the packets called datagrams.
- A datagram consist of 2 parts (Figure below): 1) Payload 2) Header.



a. IP datagram



b. Header

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 : 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, route to be taken by packet and 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.

Example 5.3

An IPv4 packet has arrived with the first 8 bits as $(01000010)_2$. The receiver discards the packet. Why?

Solution

There is an error in this packet. The 4 leftmost bits $(0100)_2$ show the version, which is correct. The next 4 bits $(0010)_2$ show an invalid header length $(2 \times 4 = 8)$. The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Example 5.4

In an IPv4 packet, the value of HLEN is $(1000)_2$. How many bytes of options are being carried by this packet?

Solution

The HLEN value is 8, which means the total number of bytes in the header is 8×4, or 32 bytes. The first 20 bytes are the base header, the next 12 bytes are the options.

Example 5.5

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is $(0028)_{16}$. How many bytes of data are being carried by this packet?

Solution

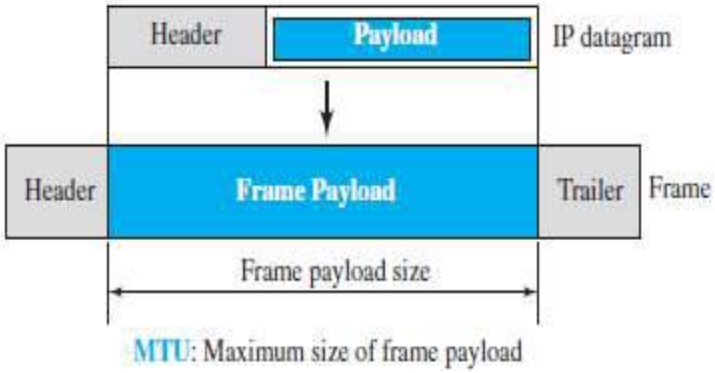
The HLEN value is 5, which means the total number of bytes in the header is 5×4, or 20 bytes (no options). The total length is $(0028)_{16}$ or 40 bytes, which means the packet is carrying 20 bytes of data $(40 - 20)$.

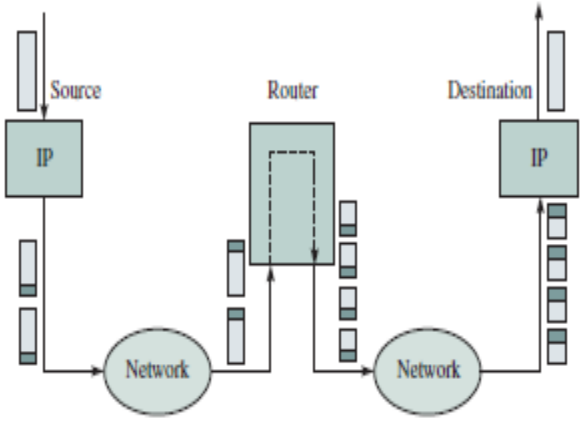
5.5.3 Fragmentation

5.5.3.1 Maximum Transfer Unit (MTU)

- Each network imposes a restriction on maximum size of packet that can be carried. This is called the MTU (maximum transmission unit).
- For example: For Ethernet, MTU = 1500 bytes and For FDDI, MTU = 4464 bytes
- When IP wants send a packet that is larger than MTU of physical-network, IP breaks packet into smaller fragments. This is called fragmentation (Figure 19.5).
- Designers have decided to make the maximum length of IP datagram = 65,535 bytes. This ensures that the IP protocol is independent of the physical network,
- When a datagram is fragmented, each fragment has its own header.

- A fragmented-datagram may itself be fragmented if it encounters a network with an even smaller MTU.
- Source host or router is responsible for fragmentation of original datagram into the fragments. Destination host is responsible for reassembling the fragments into the original datagram.





5.5.3.2 Fields Related to Fragmentation & Reassembly

Three fields in the IP header are used to manage fragmentation and reassembly:

1) Identification 2) Flags 3) Fragmentation offset.

1) Identification

- This field is used to identify to which datagram a particular fragment belongs to (so that fragments for different packets do not get mixed up).
- To guarantee uniqueness, the IP protocol uses an up-counter to label the datagrams.
- When the IP protocol sends a datagram, IP protocol copies the current value of the counter to the identification field and increments the up-counter by 1.
- When a datagram is fragmented, the value in the identification field is copied into all fragments.
- The identification number helps the destination in reassembling the datagram.

2) Flags

This field has 3 bits.

1) The leftmost bit is not used.

2) DF bit (Don't Fragment):

i) If DF=1, the router should not fragment the datagram. Then, the router discards the datagram and sends an error-message to the source host.

ii) If DF=0, the router can fragment the datagram if necessary.

3) MF bit (More Fragment):

i) If MF=1, there are some more fragments to come.

ii) If MF=0, this is last fragment.

3) Fragmentation Offset

This field identifies location of a fragment in a packet. This field is the offset of the data in the original datagram.

Example 5.6

A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 0, it means that there are no more fragments; the fragment is the last one. However, we cannot say if the original packet was fragmented or not. A nonfragmented packet is considered the last fragment.

Example 5.7

A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or a middle one, but not the last one. We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset).

Example 5.8

A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

Solution

Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the first fragment.

Example 5.9

A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Solution

To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data.

Example 5.10

A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

Solution

The first byte number is $100 \times 8 = 800$. The total length is 100 bytes, and the header length is 20 bytes (5×4), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879.

5.5.4 Options

- This field allows the packet to request special features such as security level, route to be taken by packet and timestamp at each router.
- This field can also be used for network testing and debugging.
- As the name implies, options are not required for a datagram.
- The header is made of two parts: 1) Fixed part and 2) Variable part.
- Maximum size of Fixed part = 20 bytes.
- Maximum size of Variable part = 40 bytes
- Options are divided into two broad categories: 1) Single-byte options and 2) Multiple-byte options.

1) Single Byte Options

i) No Operation

This option is used as filler between options.

ii) End of Option

This option is used for padding at the end of the option field.

2) Multiple Byte Options

i) Record Route

- This option is used to record the routers that handle the datagram.
- This option can list up to 9 router-addresses.

ii) Strict Source Route

- This option is used by the source to pre-determine a route for the datagram.
- Useful purposes: The sender can choose a route with a specific type of service, such as minimum delay, maximum throughput or more secure/reliable.
- All the defined-routers must be visited by the datagram.
- If the datagram visits a router that is not on the list, the datagram is discarded.

iii) Loose Source Route

- This option is similar to the strict source route, but it is less rigid.
- Each router in the list must be visited, but the datagram can visit other routers as well.

iv) Timestamp

- This option is used to record the time of datagram processing by a router.
- The time is expressed in milliseconds from midnight GMT (Greenwich Mean Time).
- The recorded-time can help the managers to track the behavior of the routers in the Internet.

5.5.5 Security of IPv4 Datagrams

Three security issues applicable to the IP protocol:

1) Packet sniffing

2) Packet modification and

3) IP spoofing.

1) Packet Sniffing

- Attackers may capture certain packets, intercept the packets and make a copy of the packets.
- Packet sniffing is a passive attack. Passive attack means the attacker does not modify the contents of the packet.
- The attack is difficult to detect " sender & receiver may never know that the packet has been copied.
- Solution: Although the attack cannot be stopped, encryption of packet may make the attacker"s job difficult.The attacker may still sniff the packet, but the content is not detectable (or understandable).

2) Packet Modification

- Attackers may succeed in accessing the content of a packet.Then, the attacker can change the address of the packet or change the data of the packet
- Solution: The attack can be prevented by data integrity mechanism. Data integrity guarantees that the packet is not modified during the transmission.

3) IP Spoofing

- The attacker pretends as a trusted entity and obtains all the secret information.
- For example: An attacker sends an IP packet to a bank pretending as legitimate customers.
- Solution:The attack can be prevented using an origin-authentication mechanism.

5.5.5.1 IPSec (IP Security)

- IP packets can be protected from the various network-attacks using a protocol called IPSec.

- IPSec protocol & IP protocol can be used to create a connection-oriented service between 2 entities.

Four services of IPSec:

1) Defining Algorithms & Keys

To create a secure channel b/w two entities, the two entities can agree on some available algorithms and keys.

2) Packet Encryption

To provide privacy, the packets exchanged b/w two parties can be encrypted using the encryption-algorithms and a shared key. This prevents the packet sniffing attack.

3) Data Integrity

Data integrity guarantees that the packet is not modified during the transmission. If the received packet does not pass the data integrity test, the packet is discarded. This prevents the packet modification attack.

4) Origin Authentication

Origin Authentication guarantees that the packet is not created by a pretender. This prevents the IP Spoofing attack.

5.6 ICMP (Internet Control Message Protocol)

ICMP is a network-layer protocol. This is used to handle error and other control messages.

5.6.1 MESSAGES

ICMP messages are divided into 2 broad categories:

1) Error-Reporting Messages

These messages report problems that a router or a host may encounter during the processing of datagram.

2) Query Messages

- These messages help a host or a network manager get specific information from a router or another host.
- For example: Nodes can discover their neighbors. Hosts can discover and learn about routers on their network. Routers can help a node redirect the messages.

Fields of ICMP messages (Figure 19.8):

1) Type: This field identifies the type of message.

2) Code: This field specifies the reason for the particular message type.

For example,

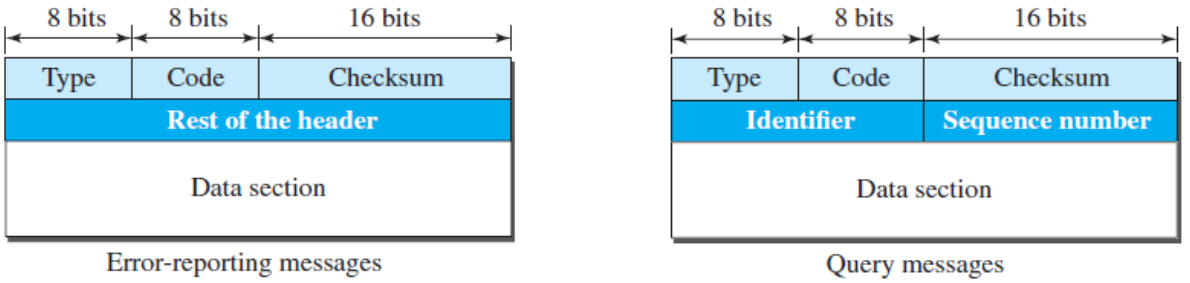
Type 03 = problem reaching the destinations

Type 11 = problem related to time exceeded.

3) Checksum: This field is used to detect errors in the ICMP message.

4) Data section: This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP packet.

Figure 19.8 *General format of ICMP messages*



Type and code values

Error-reporting messages	Query messages
03: Destination unreachable (codes 0 to 15)	08 and 00: Echo request and reply (only code 0)
04: Source quench (only code 0)	13 and 14: Timestamp request and reply (only code 0)
05: Redirection (codes 0 to 3)	
11: Time exceeded (codes 0 and 1)	
12: Parameter problem (codes 0 and 1)	

5.6.1.1 Error Reporting Messages

- Main responsibility of ICMP: To report some errors that may occur during the processing of the datagram (Figure 19.9).
- These messages report problems that a router or a host may encounter during the processing of datagram.
- ICMP does not correct errors; ICMP simply reports the errors to the source.
- Error correction is left to the higher-level protocols (such as TCP or UDP).

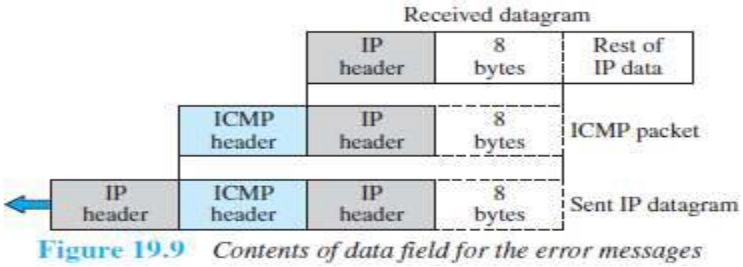


Figure 19.9 *Contents of data field for the error messages*

Rules for reporting messages:

- No error-message will be generated for a datagram having a multicast address (or special address).
- No error-message will be generated in response to a datagram carrying an ICMP error message.
- No error-message will be generated for a fragmented datagram that is not the first fragment.

1) Destination Unreachable (Type=3)

- This message is related to problem reaching the destinations.
- This message uses different codes (0 to 15) to define type of error-message.
- Possible values for code field:

  Code 0 = network unreachable

  Code 1 = host unreachable

  Code 2 = protocol unreachable

  Code 3 = port unreachable

2) Source Quench (Type=4)

- This message informs the sender that network has encountered congestion and datagram has been dropped.
- The source needs to slow down sending more datagrams.
- In other words, ICMP adds a kind of congestion control mechanism to the IP protocol.

3) Redirection Message (Type=5)

- This is used when the source uses a wrong router to send out its message.
- The router redirects the message to the appropriate router & informs the source to change its default router in the future.
- The IP address of the default router is sent in the message.
- TTL prevents a datagram from being aimlessly circulated in the Internet.
- When TTL becomes 0, the datagram is dropped by the visiting router and a time exceeded message (type 11) is sent to the source.

4) Parameter Problem (Type=12)

This message can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

5.6.1.2 Query Messages

These messages help a network manager to get specific information from a router or host.

Two types of query messages: request (type 8) and reply (type 0).

1) Echo Request & Echo Reply

- These messages are used to determine whether a remote-host is alive.
- A source-host sends an echo request message to destination-host. If the destination-host is alive, it responds with an echo reply message.
- Type=8 is used for echo request
- Type=0 is used for echo reply.
- These messages can be used in two debugging tools: ping and traceroute.

2) Timestamp Request & Timestamp Reply

- These messages are used to find the round-trip time between two devices or check whether the clocks in two devices are synchronized.
- The timestamp request sends a number, which defines the time the message is sent.
- The timestamp reply resends another number, which defines the time the message is sent.
- The timestamp reply also includes 2 new numbers representing i) the time the request was received and ii) the time the response was sent.
- Type=13 is used for timestamp request.
- Type=14 is used for timestamp reply.

5.6.2 Debugging Tools

- There are several tools that can be used in the Internet for debugging.
- We can determine the viability of a host or router.
- We can trace the route of a packet.
- Two tools used for debugging: 1) Ping and 2) Traceroute.

5.6.2.1 Ping

- The ping program can be used to find if a host is alive and responding
- Here, ping is used to see how it uses ICMP packets
- The source host sends ICMP echo-request messages;
- The destination, if alive, responds with ICMP echo-reply messages.
- The ping program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0; this number is incremented by 1 each time a new message is sent.

- Ping can calculate the round-trip time. It inserts the sending time in the data section of the message. When the packet arrives, it subtracts the arrival time from the departure time to get the round-trip time (RTT).

5.6.2.2 Traceroute

- The traceroute program can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- The traceroute program is different from the ping program.
- The ping program gets help from 2 query messages;
- The traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable.
- The traceroute is an application layer program, but only the client program is needed.
- In other words, there is no traceroute server program.
- The traceroute application program is encapsulated in a UDP user datagram, but traceroute intentionally uses a port number that is not available at the destination.

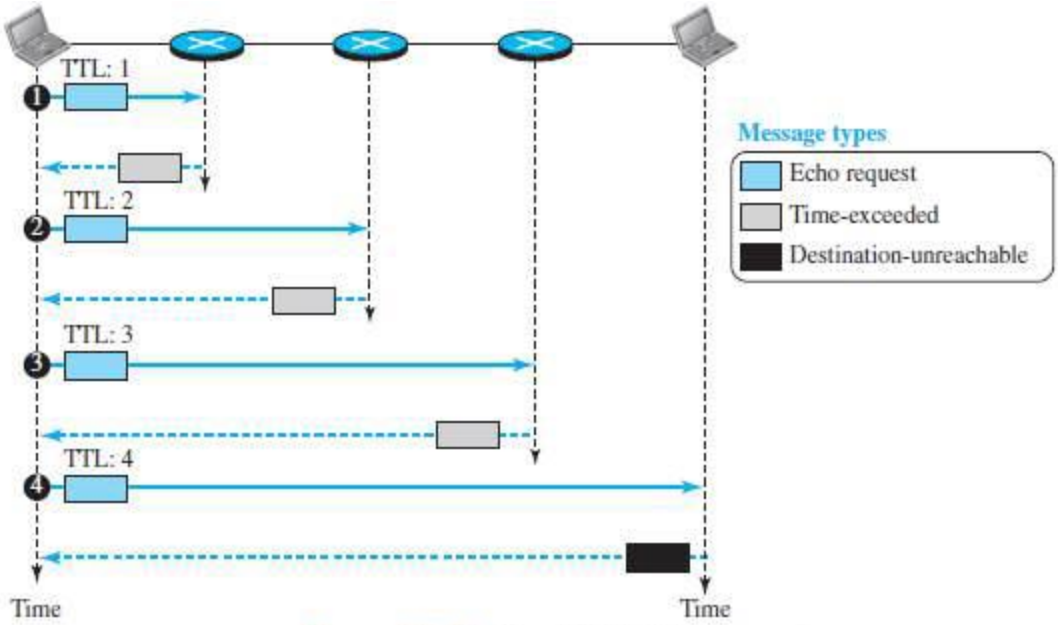


Figure 19.10 *Use of ICMPv4 in traceroute*

5.7 MOBILE IP

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

5.7.1 Addressing

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

5.7.1.1 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.

5.7.1.2 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):
  1) Home address &
  2) Care-of address

1) 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.

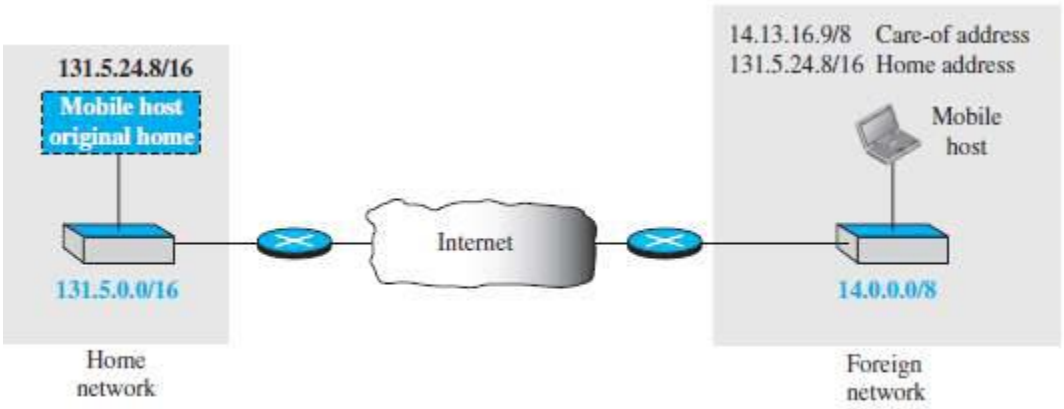


Figure 19.12 *Home address and care-of address*

5.7.2 Agents

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

1) Home-agent.

2) Foreign-agent.

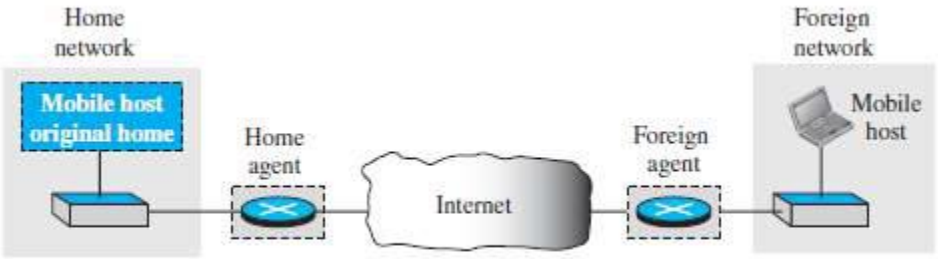


Figure 19.13 *Home agent and foreign agent*

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 homeagent 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.

5.7.3 Three Phases

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

1) Agent Discovery: involves the mobile-host, the foreign-agent, and the home-agent.

2) Registration: involves the mobile-host, the foreign-agent, and the home-agent.

3) Data Transfer: Here, the remote-host is also involved.

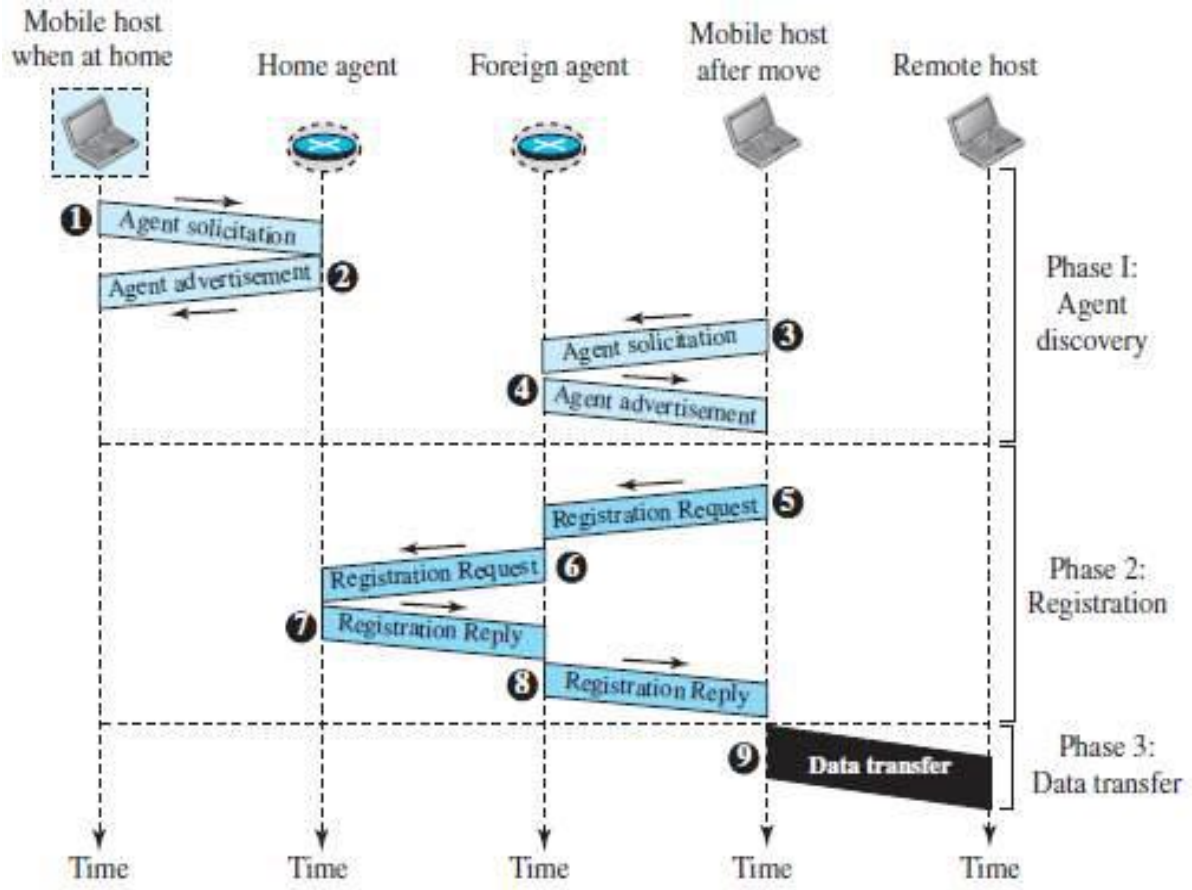


Figure 19.14 *Remote host and mobile host communication*

5.7.3.1 Agent Discovery

Agent discovery consists of two sub-phases:

1. A mobile-host must discover (learn the address of) a home-agent before it leaves its home network.
2. 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*

- **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).

Table 19.1 *Code Bits*

Bit	*Meaning*
0	Registration required. No collocated care-of address.
1	Agent is busy and does not accept registration at this moment.
2	Agent acts as a home agent.
3	Agent acts as a foreign agent.
4	Agent uses minimal encapsulation.
5	Agent uses generic routing encapsulation (GRE).
6	Agent supports header compression.
7	Unused (0).

- **Care-of Addresses:** This field contains a list of addresses available for use as care-of addresses. The mobile-host can choose one of these addresses. The selection of this care-of address is announced in the registration request.

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.

5.7.3.2 Registration

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

Four aspects of registration:

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

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

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

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

5.7.3.2.1 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.

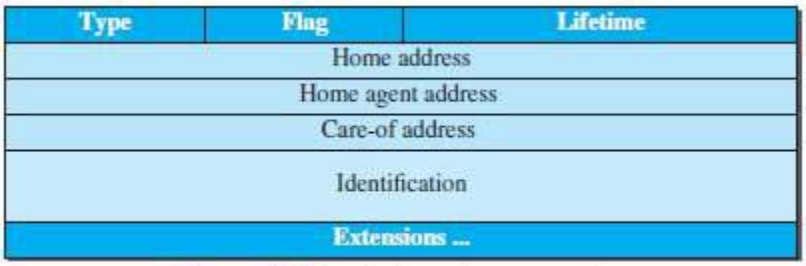


Figure 19.16 *Registration request format*

Various fields are (Figure 19.16):

1) 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).

Table 19.2 *Registration request flag field bits*

Bit	*Meaning*
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using collocated care-of address.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests generic routing encapsulation (GRE).
5	Mobile host requests header compression.
6–7	Reserved bits.

3) Lifetime: This field defines the number of seconds the registration is valid. If the field is a string of 0s, the request message is asking for deregistration. 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:

  1) The value of the type field is 3.

  2) The code field replaces the flag field and shows the result of the registration request.

  3) The care-of address field is not needed.

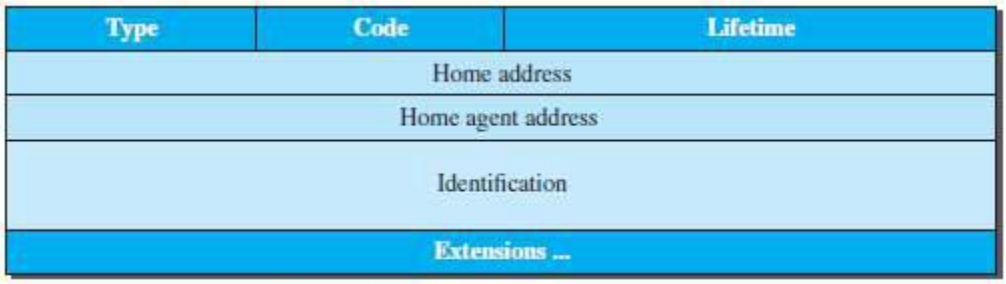


Figure 19.17 *Registration reply format*

5.7.3.3 Data Transfer

- After agent discovery & registration, a mobile-host can communicate with a remote-host.

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).

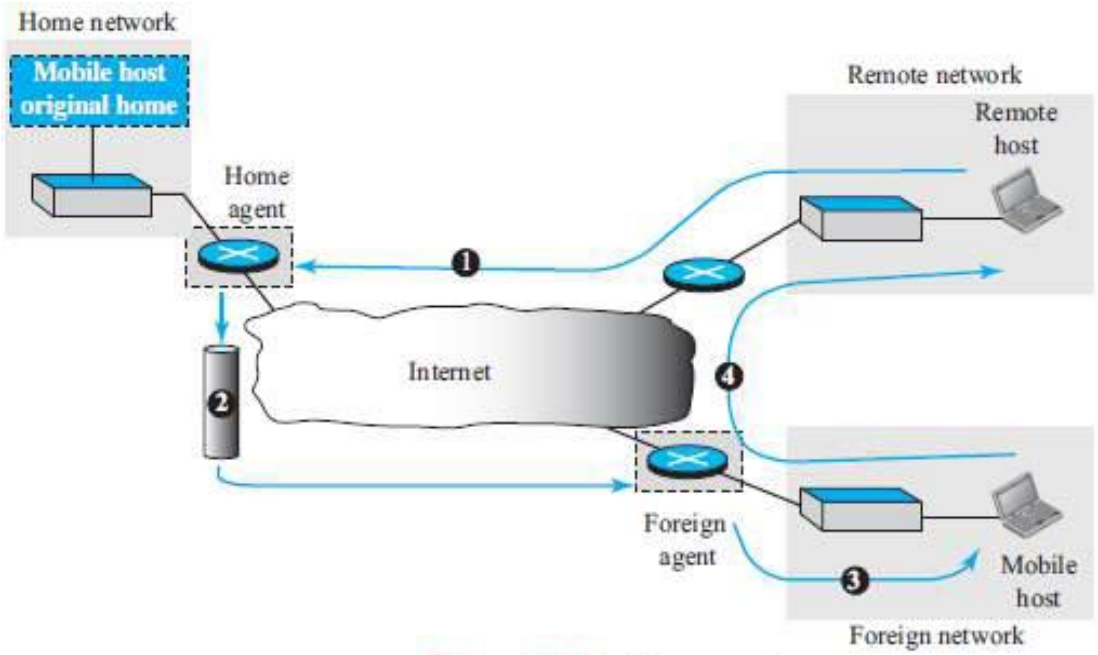


Figure 19.18 *Data transfer*

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).

5.7.4 Inefficiency in Mobile IP

- Communication involving mobile IP can be inefficient.
- The inefficiency can be severe or moderate.
- The severe case is called double crossing or 2X.
- The moderate case is called triangle routing or dog-leg routing.

5.7.4.1 Double Crossing

- Double crossing occurs when a remote-host communicates with a mobile-host that has moved to the same network (or site) as the remote-host (Figure 19.19).
- When the mobile-host sends a packet to the remote-host, there is no inefficiency; the communication is local.
- However, when remote-host sends a packet to mobile-host, the packet crosses the Internet twice. Since a computer usually communicates with other local computers (principle of locality), the inefficiency from double crossing is significant.

5.7.4.2 Triangle Routing

- Triangle routing occurs when the remote-host communicates with a mobile-host that is not attached to the same network (or site) as the mobile-host.
- When the mobile-host sends a packet to the remote-host, there is no inefficiency.

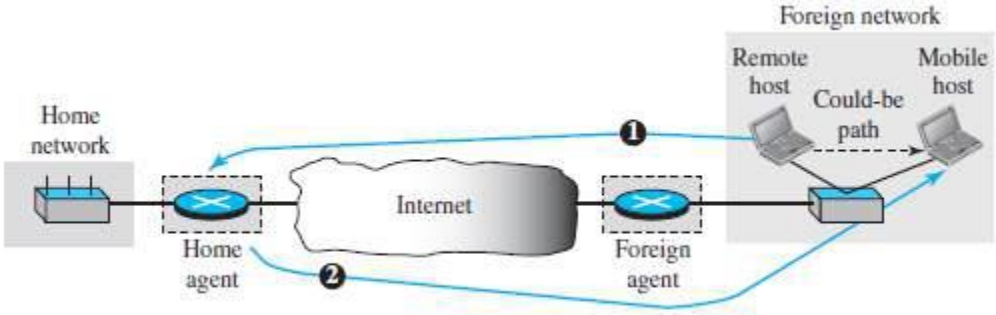


Figure 19.19 *Double crossing*

- However, when the remote-host sends a packet to the mobile-host, the packet goes from the remote-host to the home-agent and then to the mobile-host.
- The packet travels the two sides of a triangle, instead of just one side (Figure 19.20).

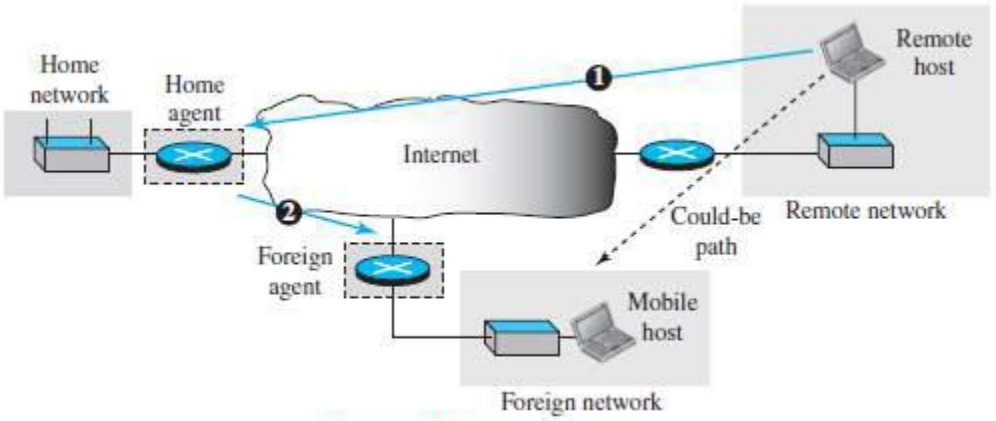


Figure 19.20 *Triangle routing*

Solution

- One solution to inefficiency is for the remote-host to bind the care-of address to the home address of a mobile-host.
- For example, when a home-agent receives the first packet for a mobile-host, it forwards the packet to the foreign-agent; it could also send an update binding packet to the remote-host so that future packets to this host could be sent to the care-of address.
- The remote-host can keep this information in a cache.
- The problem with this strategy is that the cache entry becomes outdated once the mobile-host moves. In this case, the home-agent needs to send a warning packet to the remote-host to inform it of the change.

Next Generation IP

5.8 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).

5.8.1 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

5.8.2 Address Space

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

5.8.2.1 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.

5.8.3 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

5.8.3.1 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 2125 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):
    1. Global routing prefix (n bits)
    2. Subnet identifier (m bits) and
    3. Interface identifier (q bits).

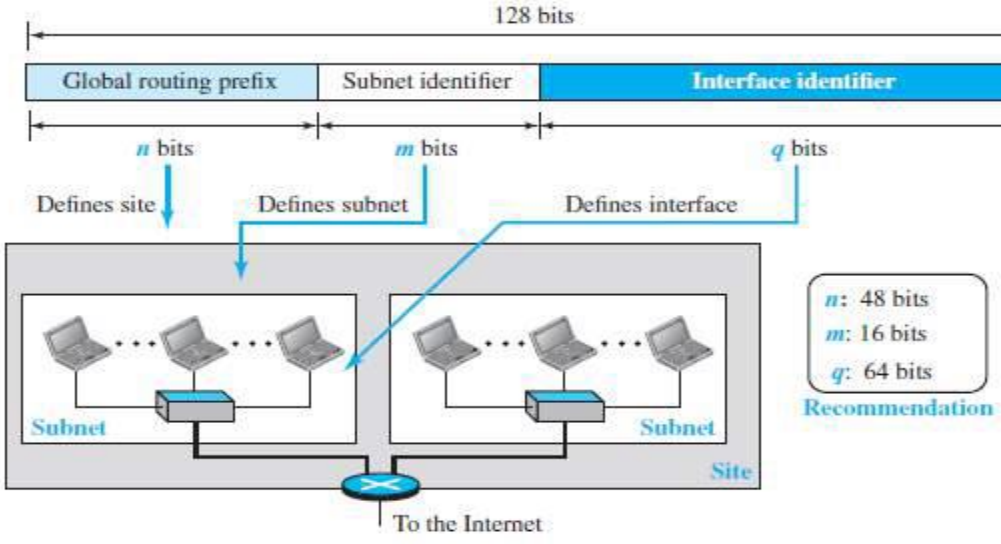


Figure 22.1 *Global unicast address*

- 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 245 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:
    1. 64-bit extended unique identifier (EUI-64) defined by IEEE.
    2. 48-bit link-layer address defined by Ethernet.

Mapping EUI-64

To map a 64-bit physical address, the global/local bit of this format needs to be changed from 0 to 1 (local to global) to define an interface address (Figure 22.2).

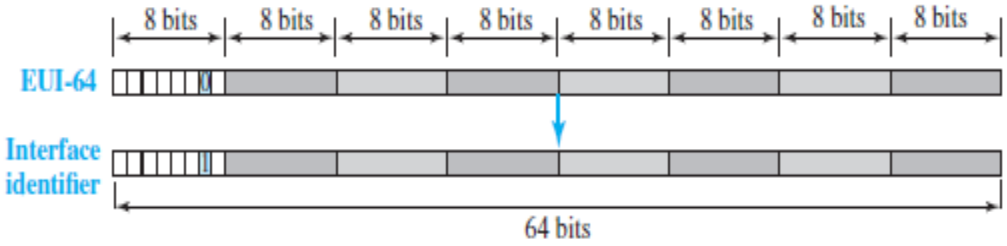
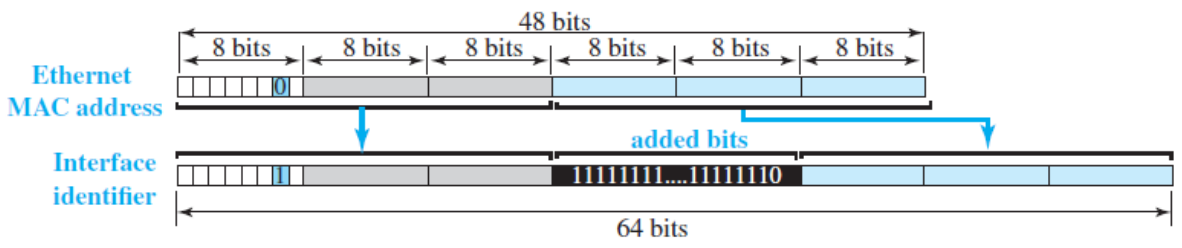


Figure 22.2 *Mapping for EUI-64*

Mapping Ethernet MAC Address

Mapping a 48-bit Ethernet address into a 64-bit interface identifier is more involved. We need to change the local/global bit to 1 and insert an additional 16 bits. The additional 16 bits are defined as 15 ones followed by one zero, or FFFE16.

Figure 22.3 *Mapping for Ethernet MAC*



Example 22.1

An organization is assigned the block 2000:1456:2474/48. What is the CIDR notation for the blocks in the first and second subnets in this organization?

Solution

Theoretically, the first and second subnets should use the blocks with subnet identifier 0001_{16} and 0002_{16}. This means that the blocks are 2000:1456:2474:0000/64 and 2000:1456:2474:0001/64.

Example 22.2

Using the format we defined for Ethernet addresses, find the interface identifier if the physical address in the EUI is $(\mathbf{F5\text{-}A9\text{-}23\text{-}EF\text{-}07\text{-}14\text{-}7A\text{-}D2})_{16}$.

Solution

We only need to change the seventh bit of the first octet from 0 to 1 and change the format to colon hex notation. The result is **F7A9:23EF:0714:7AD2.**

Example 22.3

Using the format we defined for Ethernet addresses, find the interface identifier if the Ethernet physical address is $(\mathbf{F5\text{-}A9\text{-}23\text{-}14\text{-}7A\text{-}D2})_{16}$.

Solution

We only need to change the seventh bit of the first octet from 0 to 1, insert two octets $FFFE_{16}$ and change the format to colon hex notation. The result is **F7A9:23FF:FE14:7AD2** in colon hex.

Example 22.4

An organization is assigned the block 2000:1456:2474/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is $(\mathbf{F5\text{-}A9\text{-}23\text{-}14\text{-}7A\text{-}D2})_{16}$?

Solution

The interface identifier for this interface is **F7A9:23FF:FE14:7AD2** (see Example 22.3). If we append this identifier to the global prefix and the subnet identifier, we get:

2000:1456:2474:0003:F7A9:23FF:FE14:7AD2/128

5.8.3.2 Special Addresses

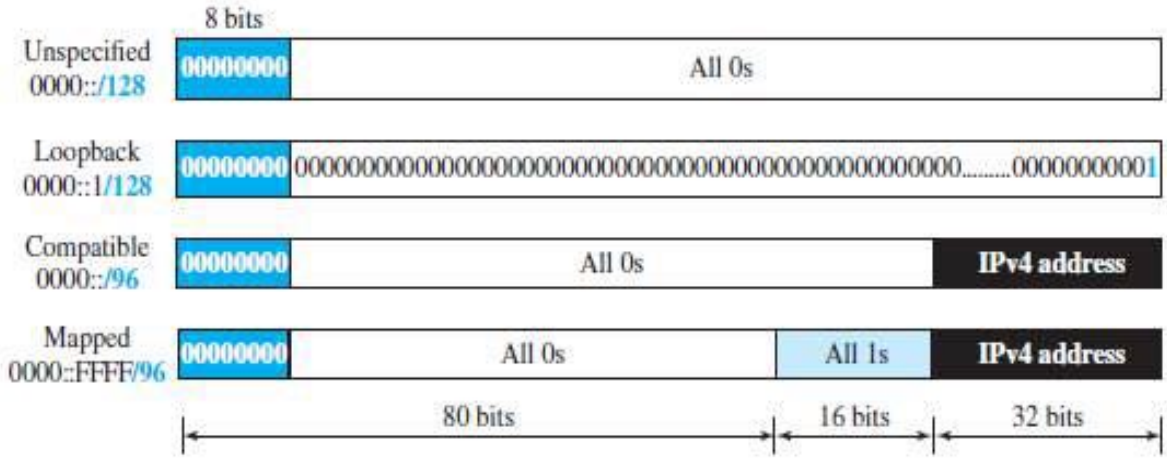


Figure 22.4 *Special addresses*

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.

5.8.3.3 Other Assigned Blocks

IPv6 uses 2 large blocks for private addressing and one large block for multicasting (Figure 22.5).

1) Unique Local Unicast Block

- A subblock in a unique local unicast block can be privately created and used by a site.
- The packet carrying this type of address as the destination address is not expected to be routed.
- This type of address has the identifier 1111 110.
- The next bit can be 0 or 1 to define how the address is selected (locally or by an authority).

2) Link Local Block

- A subblock in link local block can be used as a private address in a network.
- This type of address has the block identifier 1111111010.
- The next 54 bits are set to zero.
- The last 64 bits can be changed to define the interface for each computer.

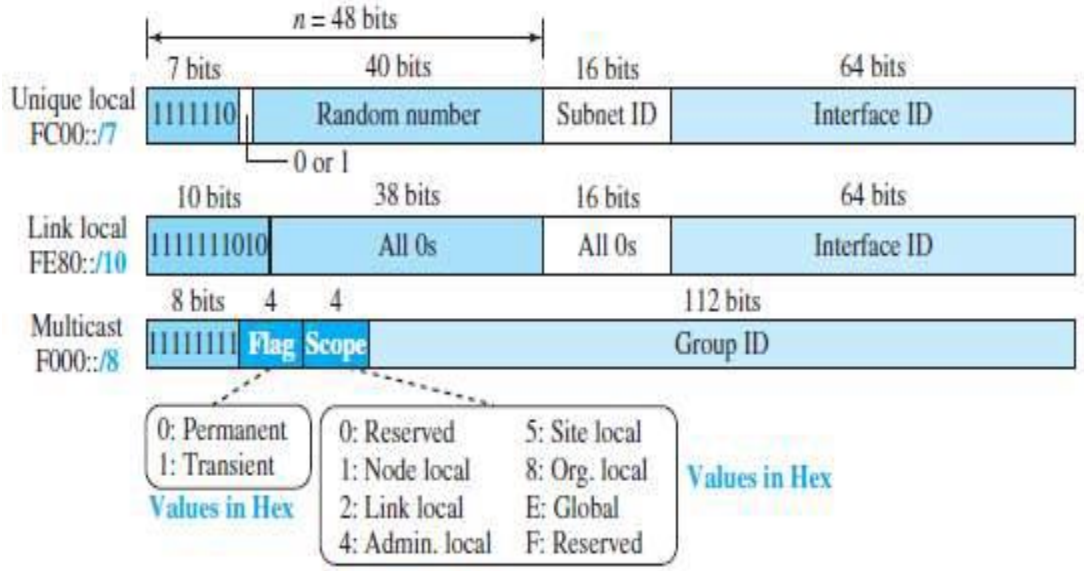


Figure 22.5 *Unique local unicast block*

5.8.4 Autoconfiguration

• When a host in IPv6 joins a network, it can configure itself using the following process:

1) The host first creates a link local address for itself.

<u>This is done by</u>

- taking the 10-bit link local prefix (1111 1110 10)
- adding 54 zeros and
- adding the 64-bit interface identifier.
- The result is a 128-bit link local address.

2) The host then tests to see if this link local address is unique and not used by other hosts. Since the 64-bit interface identifier is supposed to be unique, the link local address generated is unique with a high probability. To check uniqueness, the host sends a neighbour solicitation message and waits for a neighbour advertisement message. If any host in the subnet is using this link local address, the process fails and the host cannot auto-configure itself.

3) If the uniqueness of the link local address is passed, the host stores this address as its link local address (for private communication), but it still needs a global unicast address. The host then sends a router solicitation message to a local router. If there is a router running on the network, the host receives a router advertisement message that includes global unicast prefix and subnet prefix that the host needs to add to its interface identifier to generate its global unicast address. If the router cannot help the host with the configuration, it informs the host in the router advertisement message (by setting a flag).

5.9 THE IPv6 PROTOCOL

5.9.1 Changes from IPv4 to IPv6 (Advantages of IPv6)

1) Header Format

- IPv6 uses a new header format.
- Options are separated from the base-header and inserted between the base-header and the data.
- This speeds up the routing process (because most of the options do not need to be checked by routers).

2) New Options

IPv6 has new options to allow for additional functionalities.

3) Extension

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

4) Resource Allocation

In IPv6, type-of-service (TOS) field has been removed and two new fields: traffic class and flow label, are added to enable the source to request special handling of the packet. This mechanism can be used to support real-time audio and video.

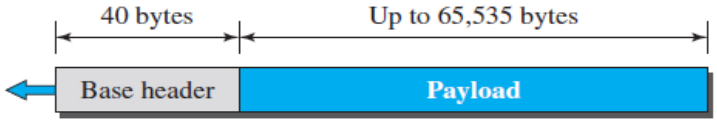
5) Security

- The encryption option provides confidentiality of the packet.

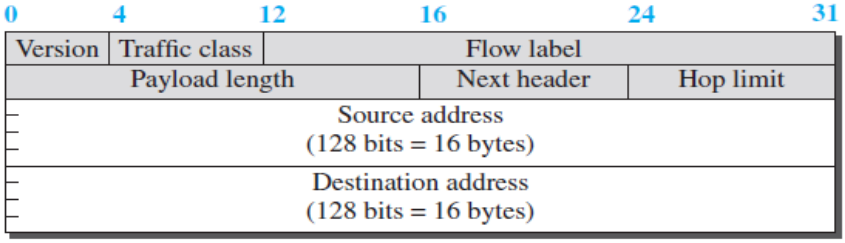
- The authentication option provides integrity of the packet.

5.9.2 Packet Format

Figure 22.6 *IPv6 datagram*



a. IPv6 packet



b. Base header

IP header contains following fields (Figure 22.6):

1) Version

This specifies version number of protocol. For IPv6, version=6.

2) Traffic Class

This field is used to distinguish different payloads with different delivery requirements.

(Traffic class replaces the type-of-service field in IPv4).

3) Flow Label

This field is designed to provide special handling for a particular flow of data.

4) Payload Length

- This indicates length of data (excluding header). Maximum length=65535 bytes.
- The length of the base-header is fixed (40 bytes); only the length of the payload needs to be defined.

5) Next Header

This identifies type of extension header that follows the basic header.

6) Hop Limit

This specifies number of hops the packet can travel before being dropped by a router. (Hop limit serves the same purpose as the TTL field in IPv4).

7) Source and Destination Addresses

These identify source host and destination host respectively.

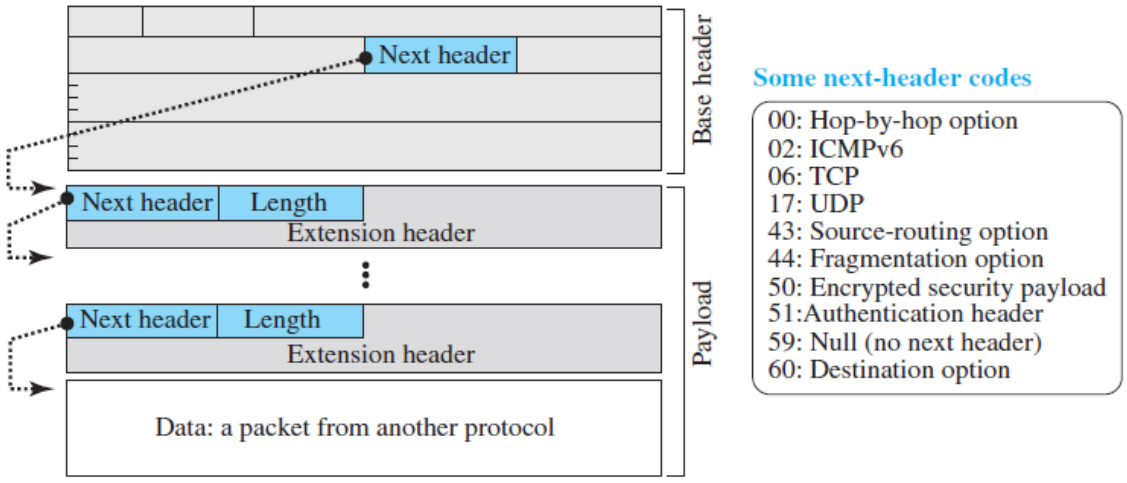
8) Payload

- The payload contains zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).
- The payload can have many extension headers as required by the situation.
- Each extension header has 2 mandatory fields (Figure 22.7):

  1) Next header and

  2) Length
- Two mandatory fields are followed by information related to the particular option.

Figure 22.7 *Payload in an IPv6 datagram*



5.9.2.1 Concept of Flow & Priority in IPv6

- To a router, a flow is a sequence of packets that share the same characteristics such as
  - Traveling the same path
  - Using the same resources or
  - Having the same kind of security
- A router that supports the handling of flow labels has a flow label table.
- The table has an entry for each active flow label.
- Each entry defines the services required by the corresponding flow label.
- When a router receives a packet, the router consults its flow label table.
- Then, the router provides the packet with the services mentioned in the entry.
- A flow label can be used to support the transmission of real-time audio/video.
- Real-time audio/video requires resources such as
  - high bandwidth
  - large buffers or

- long processing time

- Resource reservation guarantees that real-time data will not be delayed due to a lack of resources.

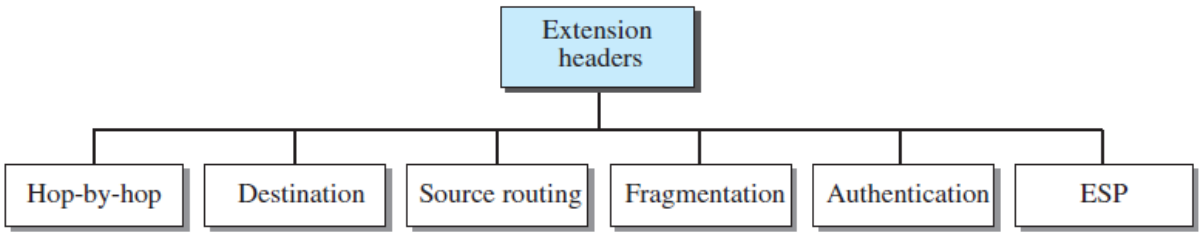
5.9.2.2 Fragmentation & Reassembly

- Fragmentation of the packet is done only by the source, but not by the routers. The reassembling is done by the destination.
- At routers, the fragmentation is not allowed to speed up the processing in the router.
- Normally, the fragmentation of a packet in a router needs a lot of processing. This is because The packets need to be fragmented and all fields related to the fragmentation need to be recalculated.
- The source will check the size of the packet and make the decision to fragment the packet or not. If packet-size is greater than the MTU of the network, the router will drop the packet. Then, the router sends an error message to inform the source.

5.9.3 Extension Header

- An IP packet is made of base-header & some extension headers.
- Length of base header = 40 bytes. To support extra functionalities, extension headers can be placed b/w base header and payload. Extension headers act like options in IPv4.
- **Six types of extension headers**: Hop-by-hop option , Source routing , Fragmentation, Authentication ,Encrypted security payload and Destination option.

Figure 22.8 *Extension header types*



1) Hop-by-Hop Option

- This option is used when the source needs to pass information to all routers visited by the datagram.
- Three options are defined: i) Pad1, ii) PadN, and iii) Jumbo payload.

  i) Pad1

  - This option is designed for alignment purposes.

- Some options need to start at a specific bit of the 32-bit word.
- Pad1 is added, if one byte is needed for alignment.

ii) PadN

- PadN is similar in concept to Pad1.
- The difference is that PadN is used when 2 or more bytes are needed for alignment.

iii) Jumbo Payload

- This option is used when larger packet has to be sent. (> 65,535 bytes)
- Large packets are referred to as jumbo packets.
- Maximum length of payload = 65,535 bytes.

2) Destination Option

- This option is used when the source needs to pass information to the destination only.
- Intermediate routers are not allowed to access this information.
- Two options are defined: i) Pad1 & ii) PadN

3) Source Routing

- This option combines the concepts of strict source routing and loose source routing.

4) Fragmentation

- In IPv6, only the original source can fragment.
- A source must use a "Path MTU Discovery technique" to find the smallest MTU along the path from the source to the destination.
- Minimum size of MTU = 1280 bytes. This value is required for each network connected to the Internet.
- If a source does not use a Path MTU Discovery technique, the source fragments the datagram to a size of 1280 bytes.

5) Authentication

- This option has a dual purpose:
- Validates the message sender: This is needed so the receiver can be sure that a message is from the genuine sender and not from an attacker.
- Ensures the integrity of data: This is needed to check that the data is not altered in transition by some attacker.

6) Encrypted Security Payload (ESP)

- This option provides confidentiality and guards against attacker.

5.9.3.1 Comparison of Options between IPv4 and IPv6

- The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
- The record route option is not implemented in IPv6 because it was not used.
- The timestamp option is not implemented because it was not used.
- The source route option is called the source route extension header in IPv6.
- The fragmentation fields in the base-header section of IPv4 have moved to the fragmentation extension header in IPv6.
- The authentication extension header is new in IPv6.
- The encrypted security payload extension header is new in IPv6.

5.10 THE ICMPv6 PROTOCOL

ICMP, ARP & IGMP protocols in IPv4 are combined into one single protocol called ICMPv6 (Fig 22.9).

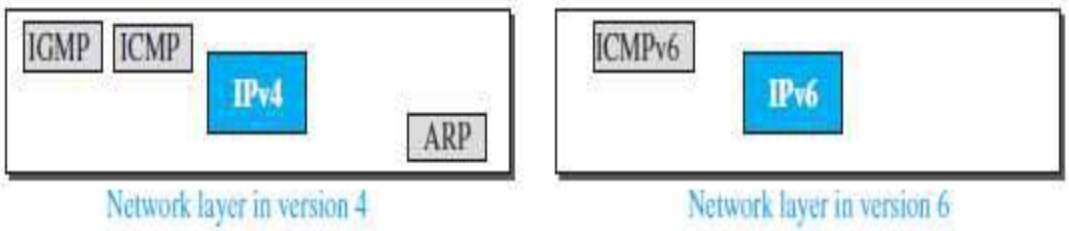


Figure 22.9 *Comparison of network layer in version 4 and version 6*

Four groups of messages (Figure 22.10):

1) Error-reporting messages

2) Informational messages

3) Neighbor-discovery messages and

4) Group-membership messages.

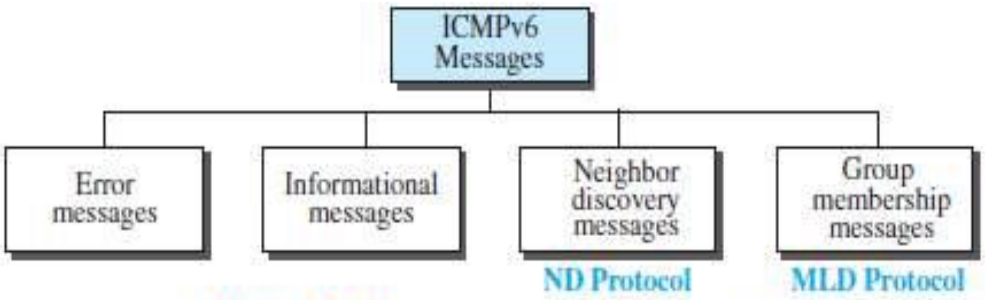


Figure 22.10 *Categories of ICMPv6 messages*

5.10.1 Error-Reporting Messages

Main responsibility of ICMP: Report errors.

ICMP forms an error packet, which is then encapsulated in the datagram.

The encapsulated datagram is delivered to the original source.

Four types of errors:

1) Destination unreachable

2) Packet too big

3) Time exceeded and

4) Parameter problems.

1) Destination-Unreachable Message

- Here, a router cannot forward a datagram or a host cannot deliver the datagram to the upper layer protocol.
- So, the router/host discards the datagram and sends a destination-unreachable message to the source.

2) Packet-Too-Big Message

- Fragmentation of the packet is done only by the source, but not by the routers.
- If a router receives a datagram larger than MTU size of the network, the router discards the datagram and sends a packet-too-big message to the source.

3) Time-Exceeded Message

- A time-exceeded error message is generated in 2 cases:
    - When the TTL value becomes zero and

- When not all fragments of a datagram have arrived in the time-limit.

4) Parameter-Problem Message

- Any missing value in the datagram-header can create serious problems.
- If a router discovers any missing value in any field, the router discards the datagram and sends a parameter-problem message to the source.

5.10.2 Informational Messages

- Two types of messages: i) echo request and ii) echo reply.
- These 2 messages are used to check whether 2 devices can communicate with each other.
- A source-host can send an echo-request message to another host.
- The destination-host can respond with the echo-reply message to the source-host.

5.10.3 Neighbor-Discovery Messages

- Two new protocols are used:
  1) Neighbor-Discovery (ND) protocol and
  2) Inverse-Neighbor-Discovery (IND) protocol.
- These 2 protocols are used by nodes on the same link for 3 main purposes:
  1) Hosts use the ND protocol to find routers in the neighborhood that will forward packets for them.
  2) Nodes use the ND protocol to find the link-layer addresses of neighbors.
  3) Nodes use the IND protocol to find the IPv6 addresses of neighbors.

Seven types of errors:

1) Router-Solicitation Message

- A host/router uses router-solicitation message to find a router in n/w that can forward a datagram.
- Physical address of the host/router is included to make the response easier for the router.

2) Router-Advertisement Message

- A host/router sends the router-advertisement message in response to a router solicitation message.

3) Neighbor-Solicitation Message

- The neighbor solicitation message has the same duty as the ARP request message.

- A host uses the neighbor solicitation message when the host has a message to send to a neighbor.
- The sender knows the IP address of the receiver, but needs the physical address of the receiver.
- The physical address is needed for the datagram to be encapsulated in a frame.

4) Neighbor-Advertisement Message

- A host sends the neighbor-advertisement message in response to a neighbor solicitation
  message.

5) Redirection Message

- The purpose of the redirection message is the same as for version 4.
- However, the format of the packet now accommodates the size of the IP address in version 6. Also, an option is added to let the host know the physical address of the target router.

6) Inverse-Neighbor-Solicitation Message

- A host uses inverse-neighbor-solicitation message to know the physical address of a
- neighbor, but not the neighbor‟s IP address.
- The message is encapsulated in a datagram using a multicast address.
- The node must send the following 2 information in the option field:
  i) Physical address of the sender and
  ii) Physical address of the target node.
- The sender can also include its IP address and the MTU value for the link.

7) Inverse-Neighbor-Advertisement Message

- A host sends the inverse-neighbor-advertisement message in response to a inverse-neighbordiscovery message.

5.10.4 Group Membership Messages

- The management of multicast delivery handling in IPv4 is given to the IGMPv3 protocol.
- In IPv6, this responsibility is given to the Multicast Listener Delivery protocol.
- MLDv2 has 2 types of messages:
  1) Membership-query message and 2) Membership-report message.
- The first type can be divided into 3 subtypes: i) General, ii) Group-specific, and iii) Group-and-source specific.

1) Membership-Query Message

- A router sends a membership-query message to find active group-members in the network.
- The format of the membership-query in MLDv2 is exactly the same as the one in IGMPv3 three exceptions:

  i) Size of the multicast address & source address has been changed from 32 bits to 128 bits.

  ii) The field size is in the maximum response code field, in which the size has been changed from 8 bits to 16 bits.

  iii) The format of the first 8 bytes matches the format for other ICMPv6 packets because MLDv2 is considered to be part of ICMPv6.

2) Membership-Report Message

- The format of the membership-report in MLDv2 is exactly the same as the one in IGMPv3 one exception: Size of the multicast address & source address has been changed from 32 bits to 128 bits.
- In particular, the record type is the same as the one defined for IGMPv3 (types 1 to 6).

5.11 TRANSITION FROM IPv4 TO IPv6

5.11.1 Strategies

- Three strategies have been devised for transition:
  1) Dual stack
  2) Tunneling and
  3) 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).

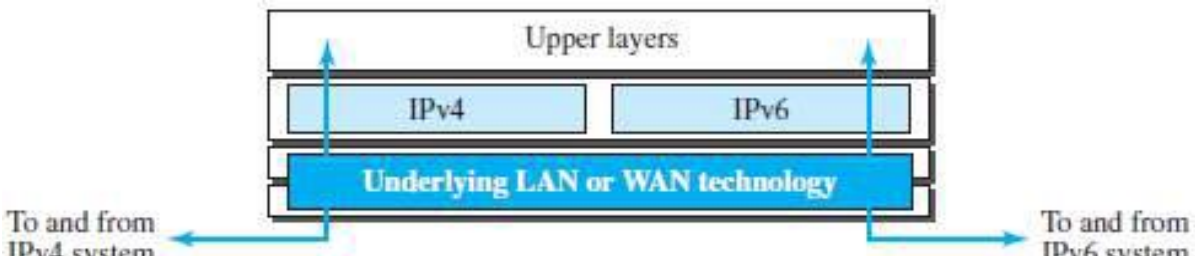


Figure 22.11 *Dual stack*

- 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.

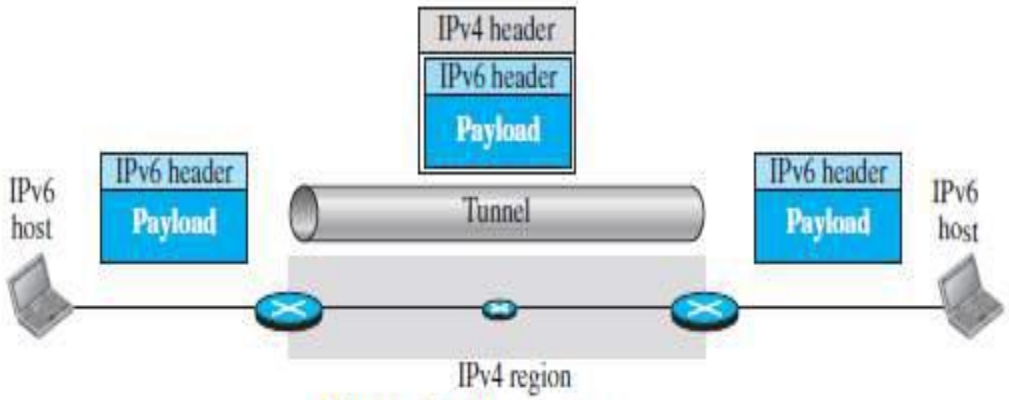


Figure 22.12 *Tunneling strategy*

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

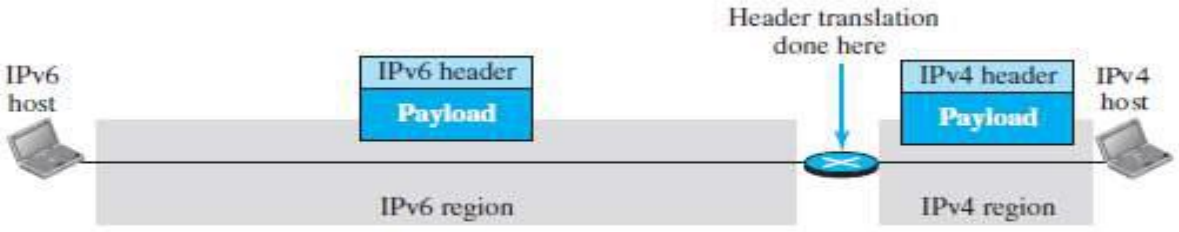


Figure 22.13 *Header translation strategy*