Unit II: Mobile Computing through Telephony: Evolution of Telephony – Multiple Access Procedures – Satellite Communication Systems – Mobile Computing through Telephone – Voice XML – Telephony Application Programming Interface. Emerging Technologies: Bluetooth - Radio Frequency Identification (RFID) – Wireless Broadband (WIMAX) – Mobile IP – Internet Protocol Version 6 (IPV6).

CHAPTER 3

Mobile Computing through Telephony

3.1 Evolution of Telephony

Mobile telephone system is used for wide area voice and data communication. Cell phones have gone through three different generations, called 1G, 2G and 3G. The generations are as following:

1. Analog voice

2. Digital voice

3. Digital voice and data

These are explained as following below.

First generation (1G) Mobile Phones : Analog Voice 1G system used a single large transmitter and had a single channel, used for both receiving and sending. If a user wants to talk then he has to push the button that enabled the transmitter and disabled the receiver. Such systems were called push-to-talk systems, and they were installed in the late 1950's. In 1960's IMTS (Improved Mobile Telephone System) was installed. It also used a high-powered (20-watt) transmitter on top of a hill but it had two frequencies, one for sending and one for receiving, so push to talk button was no longer needed.

Second generation (2G) Mobile phones : Digital voice The first generation mobile phones was analog though second generation is digital. It enables new services such as text messaging. There was no worldwide standardization during second generation. Several different systems were developed and three have been deployed. GSM (Global System for Mobile Communications). It is the dominant 2G system.

Third generation (3G) Mobile Phones : Digital Voice and Data The first generation was analog voice and second generation was digital voice but 3rd generation is about digital voice and data. 3G mobile telephony is all about providing enough wireless bandwidth to keep future users happy. Apple's iPhone is the kind of 3G device but actually it is not using exactly 3G , they used enhanced 2G network i.e. 2.5G and there is not enough data capacity to keep users happy.

Fourth generation (4G) Mobile Phones : Broadband Internet Access with Digital Voice and Data The fourth generation mobile phone is to access internet along with digital voice and digital data. It is more faster than 3G phones. 4G phones are capable to work like a computer. 4G phones made cloud services usable. Even after decades still there are remote areas where 4G network is not available.

Fifth generation (5G) Mobile Phones :Super Fast Connectivity and More Than 4G The fifth generation mobile phones are to provide super fast connectivity. It provides superior performance with low latency. You will be able to connect more devices than 4G. As 4G network is not available all places so 5G network will take time to make a perfect level of coverage.

Evolution of Telephone
InformationQ.com
1880s
1940s
1960s
1980s
1990-2000s
2010s
2020s
info

3.2 Satellite Communication – Introduction

A satellite is a smaller object that revolves around a larger object in space. For example, moon is a natural satellite of earth.

We know that Communication refers to the exchange (sharing) of information between two or more entities, through any medium or channel. In other words, it is nothing but sending, receiving and processing of information.

If the communication takes place between any two earth stations through a satellite, then it is called as satellite communication. In this communication, electromagnetic waves are used as carrier signals. These signals carry the information such as voice, audio, video or any other data between ground and space and vice-versa.

Soviet Union had launched the world's first artificial satellite named, Sputnik 1 in 1957. Nearly after 18 years, India also launched the artificial satellite named, Aryabhata in 1975.

Need of Satellite Communication

The following two kinds of propagation are used earlier for communication up to some distance.

- Ground wave propagation − Ground wave propagation is suitable for frequencies up to 30MHz. This method of communication makes use of the troposphere conditions of the earth.
- Sky wave propagation − The suitable bandwidth for this type of communication is broadly between 30–40 MHz and it makes use of the ionosphere properties of the earth.

The maximum hop or the station distance is limited to 1500KM only in both ground wave propagation and sky wave propagation. Satellite communication overcomes this limitation. In this method, satellites provide communication for long distances, which is well beyond the line of sight.

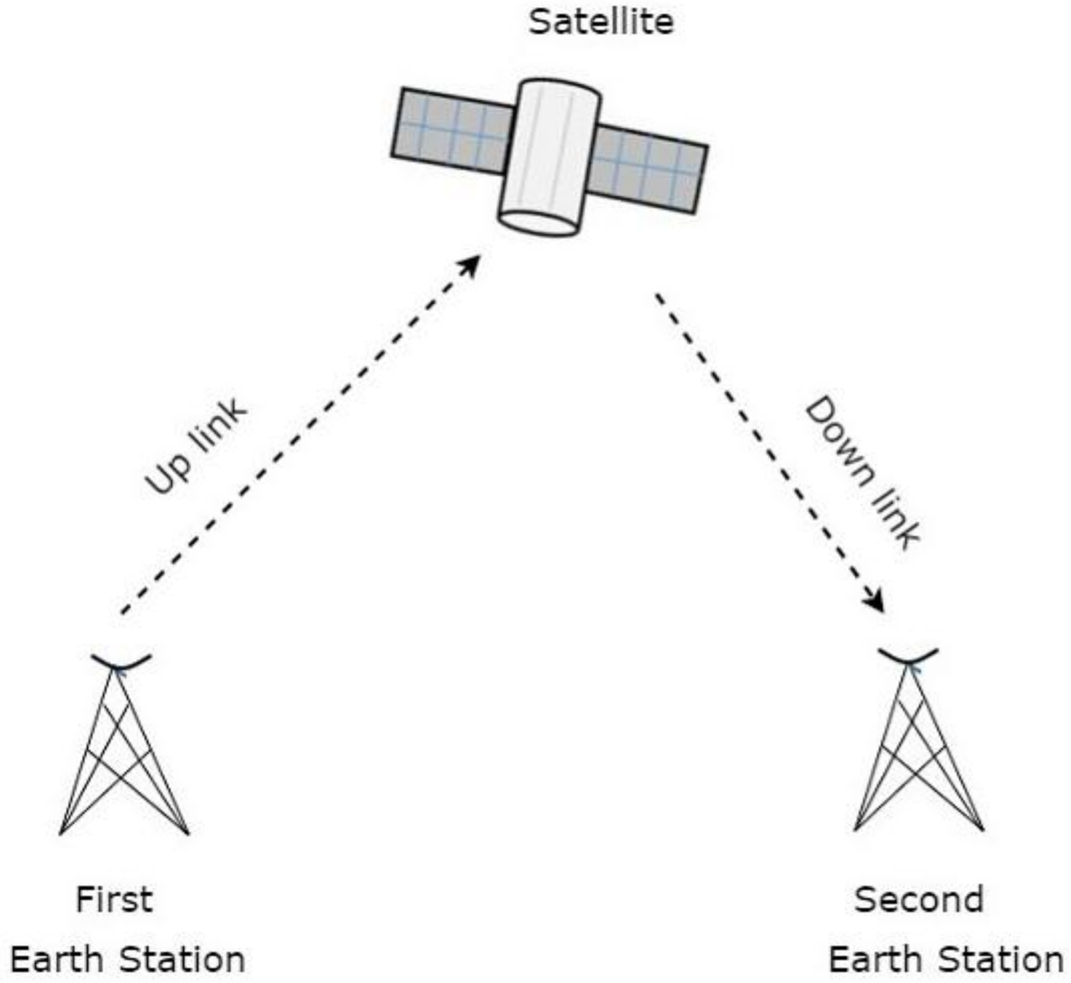
Since the satellites locate at certain height above earth, the communication takes place between any two earth stations easily via satellite. So, it overcomes the limitation of communication between two earth stations due to earth’s curvature.

How a Satellite Works

A satellite is a body that moves around another body in a particular path. A communication satellite is nothing but a microwave repeater station in space. It is helpful in telecommunications, radio and television along with internet applications.

A repeater is a circuit, which increases the strength of the received signal and then transmits it. But, this repeater works as a transponder. That means, it changes the frequency band of the transmitted signal from the received one.

The frequency with which, the signal is sent into the space is called as Uplink frequency. Similarly, the frequency with which, the signal is sent by the transponder is called as Downlink frequency. The following figure illustrates this concept clearly.



- The transmission of signal from first earth station to satellite through a channel is called as uplink. Similarly, the transmission of signal from satellite to second earth station through a channel is called as downlink.
- Uplink frequency is the frequency at which, the first earth station is communicating with satellite. The satellite transponder converts this signal into another frequency and sends it down to the second earth station. This frequency is called as Downlink frequency. In similar way, second earth station can also communicate with the first one.
- The process of satellite communication begins at an earth station. Here, an installation is designed to transmit and receive signals from a satellite in an orbit around the earth. Earth stations send the information to satellites in the form of high powered, high frequency (GHz range) signals.

The satellites receive and retransmit the signals back to earth where they are received by other earth stations in the coverage area of the satellite. Satellite's footprint is the area which receives a signal of useful strength from the satellite.

Pros and Cons of Satellite Communication

In this section, let us have a look at the advantages and disadvantages of satellite communication.

Following are the advantages of using satellite communication:

- Area of coverage is more than that of terrestrial systems
- Each and every corner of the earth can be covered
- Transmission cost is independent of coverage area
- More bandwidth and broadcasting possibilites

Following are the disadvantages of using satellite communication −

- Launching of satellites into orbits is a costly process.
- Propagation delay of satellite systems is more than that of conventional terrestrial systems.
- Difficult to provide repairing activities if any problem occurs in a satellite system.
- Free space loss is more
- There can be congestion of frequencies.

Applications of Satellite Communication

Satellite communication plays a vital role in our daily life. Following are the applications of satellite communication −

- Radio broadcasting and voice communications
- TV broadcasting such as Direct To Home (DTH)
- Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
- Military applications and navigations
- Remote sensing applications
- Weather condition monitoring & Forecasting

3.3 Voice XML

What is VoiceXML?

The Voice eXtensible Markup Language (VoiceXML) is an XML-based markup language for creating distributed voice applications that users can access from any telephone.

VoiceXML is an emerging industry standard defined by the VoiceXML Forum, of which IBM is a founding member. It has been accepted for submission by the World Wide Web Consortium (W3C) as a standard for voice markup on the Web.

The VoiceXML language lets you use a familiar markup style and Web server-side logic to deliver voice content to the Internet. The VoiceXML applications you create can interact with your existing back-end business data and logic.

Users interact with these Web-based voice applications by speaking or by pressing telephone keys rather than through a graphical user interface.

VoiceXML supports dialogs that feature:

- Spoken input
- Telephone keypad input
- Recording of spoken input
- Synthesized speech output ("text-to-speech")
- Recorded audio output
- Telephony features such as call transfer and disconnect
- Dialog flow control
- Scoping of input

  VoiceXML is the HTML of the voice web, the open standard markup language for voice applications. VoiceXML harnesses the massive web infrastructure developed for HTML to make it easy to create and deploy voice applications. Like HTML, VoiceXML has opened up huge business opportunities: the Economist even says that “VoiceXML could yet rescue telecoms carriers from their folly in stringing so much optical fibre around the world.”

- VoiceXML 1.0 was published by the VoiceXML Forum, a consortium of over 500 companies, in March 2000. The Forum then gave control of the standard to the World Wide Web Consortium (W3C), and now concentrates on conformance, education, and marketing. The W3C has just published VoiceXML 2.0 as a Candidate Recommendation. Products based on VoiceXML 2.0 are already widely available.

- While HTML assumes a graphical web browser with display, keyboard, and mouse, VoiceXML assumes a voice browser with audio output, audio input, and keypad input. Audio input is handled by the voice browser’s speech recognizer. Audio output consists both of recordings and speech synthesized by the voice browser’s text-to-speech system.

3.4 Telephony Application Programming Interface

What Does Telephony Application Programming Interface Mean?

Telephony Application Programming Interface (TAPI) is a set of standard application programming interfaces developed by Microsoft and Intel and implemented in Microsoft Windows for connecting a computer to telephone services. TAPI allows Microsoft Windows to auto detect and set up communication hardware installed on a personal computer.

Telephony Application Programming Interface

The Telephony Application Programming Interface receives requests from different applications and transmits them to appropriate telephony devices like telephones, modems and private branch exchanges. On different Windows versions, different versions of TAPI are available. From a computer applications perspective, TAPI can control different telephony functions that exist between the computer and the device, such as voice calls, data or fax. Basic functionalities such as dialing, answering and call holding along with supplementary functions such as conference and call park as well as other PBX functions are also supported.

Telephony Application Programming Interface is primarily used in controlling telephone system handsets or modems. It is also used to control voice-enabled telephony equipment like voice modems or voice-dedicated hardware. Other possible TAPI applications are interactive voice response systems, call center applications and multicast multimedia IP conferencing.

For application developers, TAPI-enabled applications can be created with the help of most programming languages such as Java, C, C++ or Visual Basic. TAPI helps application programmers in taking advantage of different telephone systems and providing services without completely understanding the inner details of the telephone systems. TAPI provides a high-level interface for call functionalities, and also provides a service provider interface for hardware vendors for generating the driver software.

CHAPTER 4

Emerging Technologies

4.1Bluetooth:

What is Bluetooth ?

Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

Points to remember for Bluetooth:

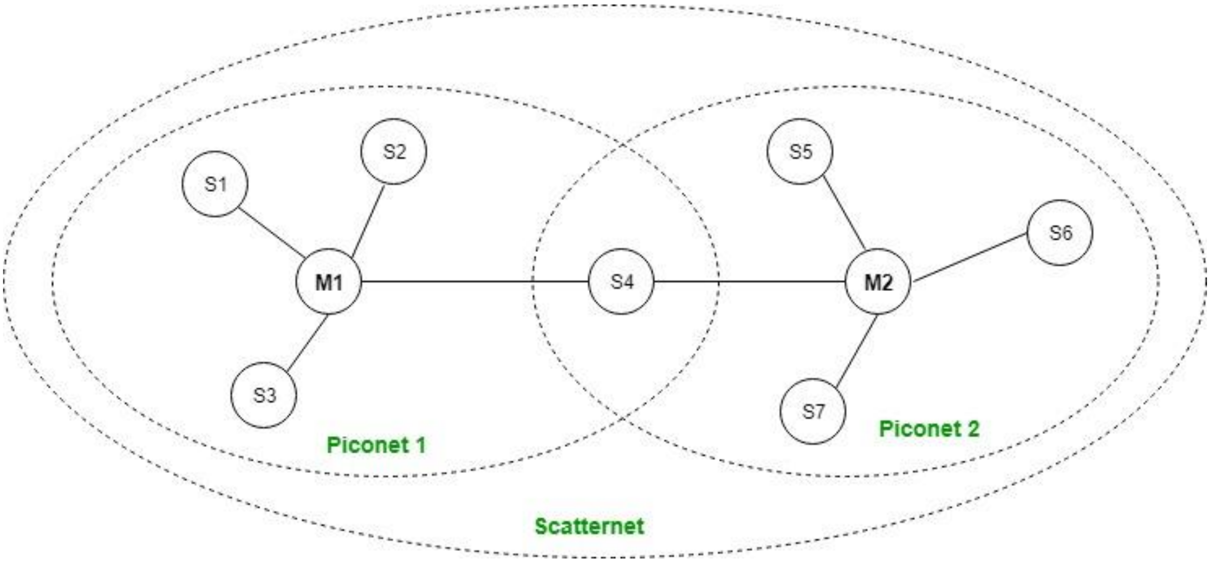
- Bluetooth Transmission capacity 720 kbps.
- Bluetooth is Wireless.
- Bluetooth is a Low-cost short-distance radio communications standard.
- Bluetooth is robust and flexible.
- Bluetooth is cable replacement technology that can be used to connect almost any device to any other device.
- The basic architecture unit of Bluetooth is a piconet.

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1.Piconet

2. Scatternet



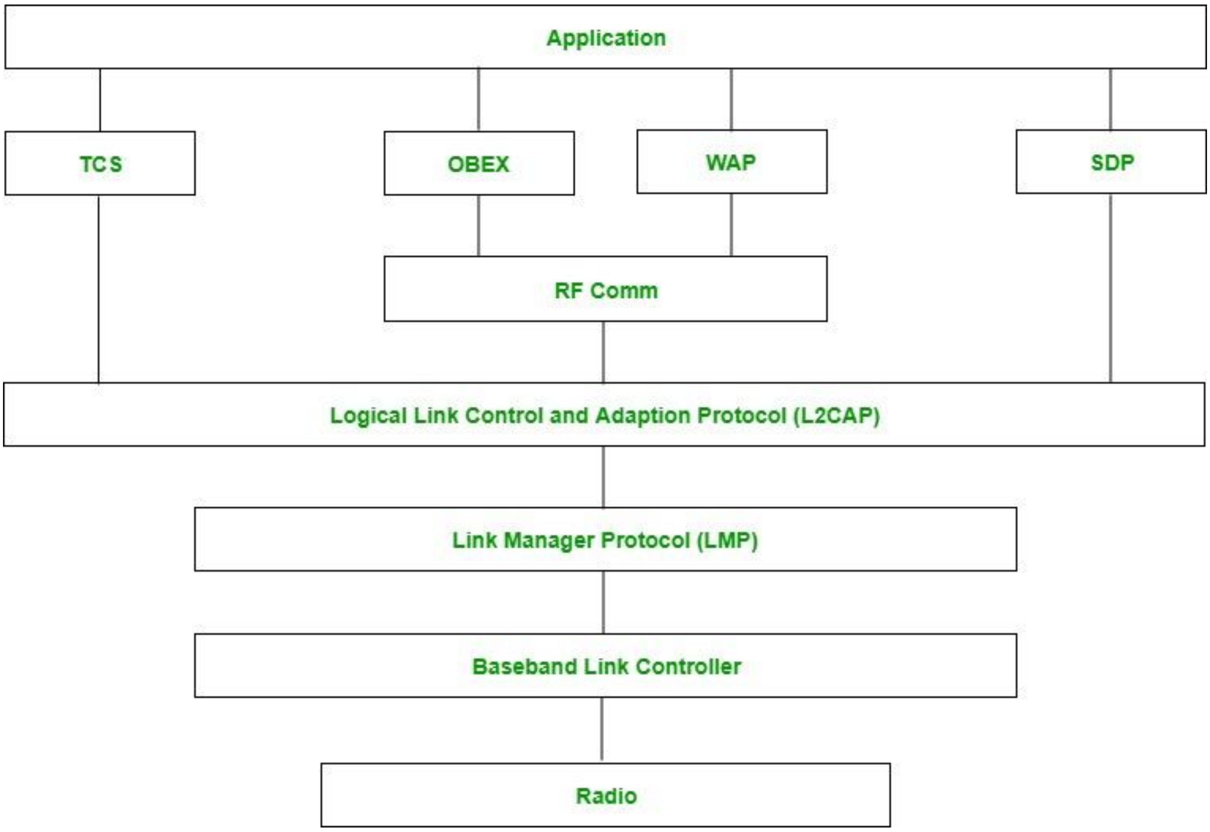
Piconet:

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet:

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Bluetooth protocol stack:


Application
TCS
OBEX
WAP
SDP
RF Comm
Logical Link Control and Adaption Protocol (L2CAP)
Link Manager Protocol (LMP)
Baseband Link Controller
Radio

- Radio (RF) layer: It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.

- Baseband Link layer: The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sublayer in LANs. It performs the connection establishment within a piconet, addressing, packet format, timing and power control.
- Link Manager protocol layer: It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.
- Logical Link Control and Adaption (L2CAP) Protocol layer: It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.

Service Discovery Protocol (SDP) layer: It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.

RF comm layer: It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.

OBEX: It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

WAP: It is short for Wireless Access Protocol. It is used for internet access.

TCS: It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.

Application layer: It enables the user to interact with the application.

<u>Types of Bluetooth</u>

Various types of Bluetooth are available in the market nowadays. Let us look at them.

In-Car Headset: One can make calls from the car speaker system without the use of mobile phones.

Stereo Headset: To listen to music in car or in music players at home.

Webcam: One can link the camera with the help of Bluetooth with their laptop or phone.

Bluetooth-equipped Printer: The printer can be used when connected via Bluetooth with mobile phone or laptop.

Bluetooth Global Positioning System (GPS): To use GPS in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

<u>Advantage:</u>

- It is a low-cost and easy-to-use device.

- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

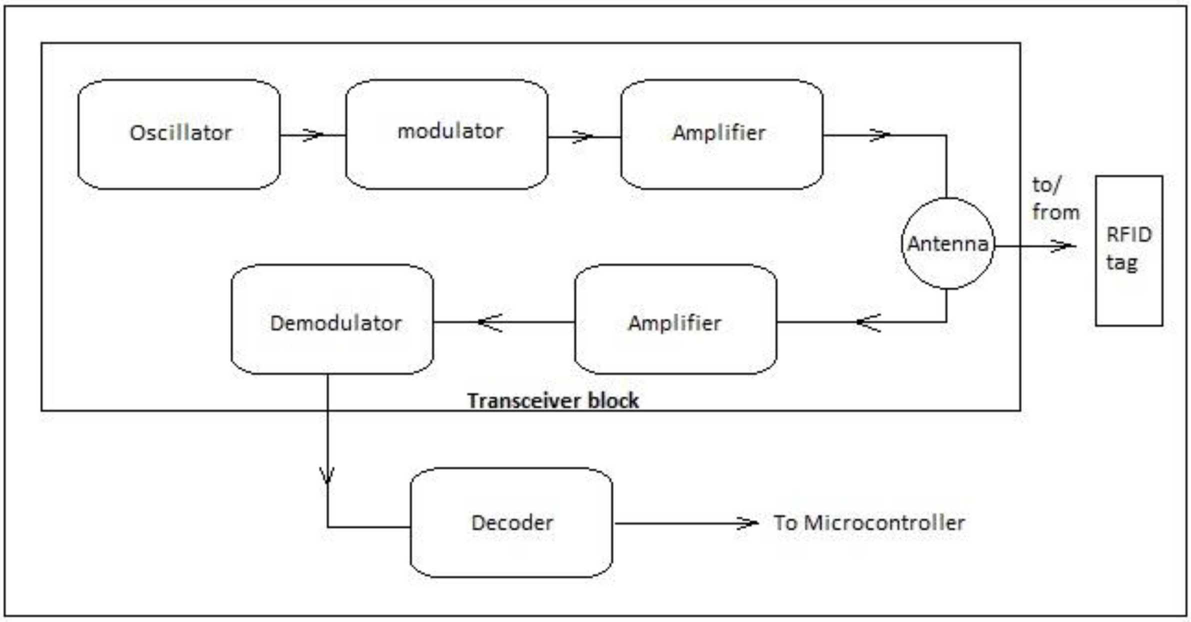
- It can be used in laptops, and in wireless PCs, printers.
- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wirelessly to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical health care, sports and fitness, Military.

- The full form of RFID is Radio-frequency identification. It is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

- RFID transmits information from RFID tags to RFID readers. As in, the data is communicated with a system that contains RFID tags, an antenna, an RFID reader, and a transceiver.

- RFID is one method of automatic identification and data capture (AIDC). This tag can read from up to several feet away and doesn't require to be within direct line-of-sight of the reader to be tracked.

Below is an example diagram of RFID −



4.2 Radio Frequency Identification (RFID)

The working procedure of RFID is as follows −

- In the active RFID system, the reader sends signals to tags using an antenna.
- The tags receive this information and resend this along with the information in its memory.
- Readers receive this signal and transmit to the processor for further processing.
- Like barcode technology, RFID recognizes locations and identification identifies tagged items.
- It uses low-power radio frequencies to collect and store data. The transceiver reads radio frequencies and transmits to an RFID tag.
- The information is then transmitted from a computer chip (embedded in the tag) and broadcasted to the RFID reader.

Uses

The uses of RFID are as follows −

- RFID technology is helpful to track products which are similar to using barcodes for product identification.
- Tags are also used for electronic payment for transportation like smart tag and other payment systems, such as credit cards and smart cards.
- RFID also has several medical uses including tracking of new-borns in hospitals, storing information on surgical patients and procedures, and tracking medical equipment.

RFID Tags

A RFID system uses labels attached to the objects that need to be identified.

RFID tags are comprised of three parts −

- a microchip
- an antenna
- a substrate

Given below is the diagram of RFID Tag which is a non-volatile memory.

Types of RFID Tags

There are two types of RFID tags, which are as follows −

- Passive tags − These are powered by energy from the interrogating radio waves generated by RFID readers.
- Active tags − These are powered by a battery and so can be read at a greater range of up to hundreds of meters.

RFID tags are used in many industries. For instance, an RFID tag attached to an automobile or RFID-tagged pharmaceuticals can be used to track the progress of the product.

Advantages

The advantages of RFID are as follows –

- Efficiency
- Durability
- RFID provides more security than barcodes.
- RFID tags can be read from greater distances.
- RFID need not be positioned in a line of sight with the scanner.
- The faster rate of RFID is more than barcodes
- They can work within much greater distances.
- RFID tags are reusable
- RFID tags are protected by a plastic cover.

Disadvantages

The disadvantages of RFID are as follows −

- The materials used in RFID like metal & liquid can impact signal
- Sometimes When compared to barcode scanner the RFID is not accurate or reliable
- The Cost of RFID readers are 10x more expensive than barcode readers
- Implementation of RFID is difficult and it is time consuming
- RFID involves assembling and inserting a computerized chip which is more expensive.
- RFID readers face difficulties for picking up information when passing through metal or liquid.
- RFID still has two separate chips which cannot be read by the same machine.

4.3 Wireless Broadband (WIMAX)

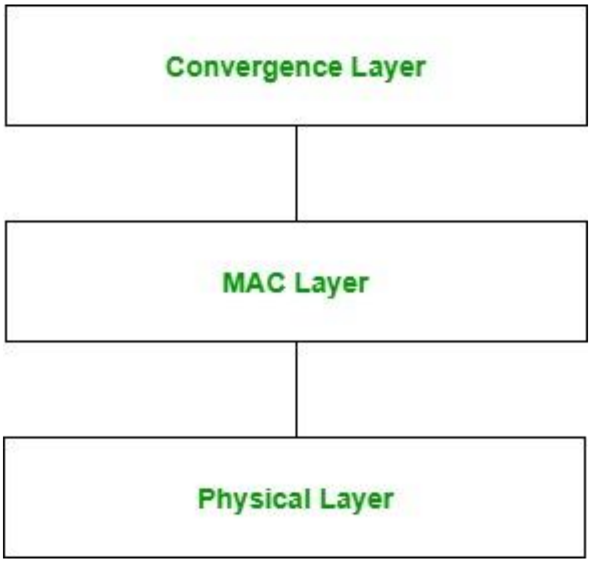
What is WiMax Technology?

WiMAX is a wireless broadband access technology based on an internet protocol and its performance is equivalent to Wi-Fi networks/802.11 by the coverage & quality of service of cellular networks. WiMAX full form is “Worldwide Interoperability for Microwave Access. A wireless digital communication system like WiMAX is also called IEEE 802.16 that is designed for wireless MANs (metropolitan area networks).

WiMAX communication system provides BWA (broadband wireless access) up to 50 kilometers for fixed stations and also for mobile stations from 5 to 15 km. WiMAX is a broadband wireless technology that provides broadband access services for enterprise & residential customers in a reasonable method.

Architecture:

-



Physical Layer: This layer specifies frequency band, synchronization between transmitter and receiver data rate and multiplexing scheme.

This layer is responsible for encoding and decoding of signals and manages bit transmission and reception. It converts MAC layer frames into signals to be transmitted. Modulation schemes which are used on this layer includes: QPSK, QAM-16 and QAM-64.

MAC Layer:

This layer provides and interface between convergence layer and physical layer of WiMax protocol stack. It provides point to multipoint communication and is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The MAC layer is responsible for transmitting data in frames and controlling access to shared wireless medium. The MAC protocol defines how and when a subscriber may initiate a transmission on the channel.

Convergence Layer:

This layer provides the information of the external network. It accepts higher layer protocol data unit (PDU) and converts it to lower layer PDU. It provides functions depending upon the service being used.

Standards of WiMax Technology

The different IEEE standards of WiMax are discussed below.

802.16-2001

This is the first version of the IEEE standard which is approved in the year 2001

802.16a-802.16c

After the 802.16-2001 version, the versions like 802.16a-802.16c were approved which are simply the alterations of the above version.

802.16-2004

This is the current IEEE standard and it is approved in June 2004 which makes the previous versions 802.16-2001 through its improvements 802.16a-802.16c outdated.

802.16-2005 (802.16e)

The IEEE 802.16-2004 standard addresses simply fixed systems. An adjustment is within the works which include mobility component toward the standard. This adjustment comes in a new standard like IEEE 802.16-2005, which is approved in Dec 2005 and is formerly called 802.16e.

Remote Stations/Mobile Stations

These stations are the user apparatus like mobile and that may be placed within the location of the consumer.

ASN (Access Service Network)

The access service network in the region of the WiMAX network and forms the radio access network on the border. This network includes one or several gateways and base stations.

CSN (Connectivity Service Network)

The connectivity service network is one of the main elements of the WiMAX network that provides internet protocol connectivity & all the functions of the internet protocol core network.

The WiMAX network includes different entities which include the following.

SS (Subscriber Station) or MS (Mobile Station)

The Subscriber station or SS is frequently known as CPE or Customer Premises Equipment which uses different forms like indoor CPE otherwise outdoor CPE. The indoor customer premises equipment can be placed by the operator. These are frequently available in a dongle form which is used for a laptop and different applications. The outdoor customer premises equipment provides good performance.

Base Station or BS

For the WiMAX network, the base station or BS forms an important element to provide the air interface for mobile stations & the subscriber. The base station is responsible for extra functionality of micro-mobility management functions like the establishment of the tunnel, handoff triggering, policy enforcement of QoS, radio resource management, classification of traffic, Dynamic Host Control Protocol(DHCP) proxy, multicast group management, session management & key management.

Advantages of WiMAX:

- Wide Coverage Area: WiMAX can cover an area of up to 50 kilometers, making it suitable for providing broadband access in rural and underserved areas.
- High Data Rates: WiMAX can provide data rates of up to 75 Mbps, which is higher than many other wireless technologies.
- Scalability: WiMAX can be easily scaled to support a large number of users and devices.
- Interoperability: WiMAX is based on an international standard, which allows for interoperability between different vendors' equipment.
- Cost-effective: WiMAX is a cost-effective solution for providing broadband access in areas where it is not economically feasible to deploy wired infrastructure.

Disadvantages of WiMAX:

- Limited Mobility: WiMAX is designed for fixed or nomadic (semi-fixed) use, not for mobile use.

- Interference: WiMAX operates in the same frequency range as other wireless technologies, which can lead to interference.
- Security Concerns: WiMAX uses a shared spectrum, which can make it vulnerable to security threats such as eavesdropping and jamming.
- Limited device availability: WiMAX devices are not as widely available as devices for other wireless technologies, such as WiFi.
- Limited penetration: WiMAX signals may have trouble penetrating through walls, buildings and other obstacles.

Applications:

- WiMAX technology is used in a variety of real-life applications, including:
- Broadband Internet Access: WiMAX is used to provide high-speed internet access in rural and underserved areas where traditional wired broadband is not available.

- Wireless Backhaul: WiMAX is used to provide a wireless link between a cellular base station and the core network, eliminating the need for a wired connection.

- Mobile Broadband: WiMAX is used to provide mobile broadband services, allowing users to access high-speed internet on the go.

- Public Safety: WiMAX is used to provide wireless connectivity for public safety networks, allowing emergency responders to communicate and share information in real-time.

- Smart Grid: WiMAX is used to provide wireless connectivity for smart grid systems, allowing utilities to remotely monitor and control the power grid.

- Telemedicine: WiMAX is used to provide wireless connectivity for telemedicine systems, allowing healthcare professionals to remotely diagnose and treat patients.

- VoIP (Voice over Internet Protocol) : WiMAX is also used to provide a wireless link for Voice over IP (VoIP) phone services, allowing users to make phone calls over the internet.

- Video Surveillance: WiMAX is used to provide wireless connectivity for video surveillance systems, allowing security personnel to monitor and record video footage remotely.

Freature	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz

Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

4.4 Mobile IP

What is Mobile IP?

Mobile IP or MIP is an Internet Engineering Task Force (IETF) RFC 2002, De-Facto standard communication protocol. It is created by extending Internet Protocol, IP.

The Mobile IP allows mobile device users to move from one network to another while maintaining the same permanent IP address.

The concept and role of Mobile IP are very important in the field of mobile computing technology.

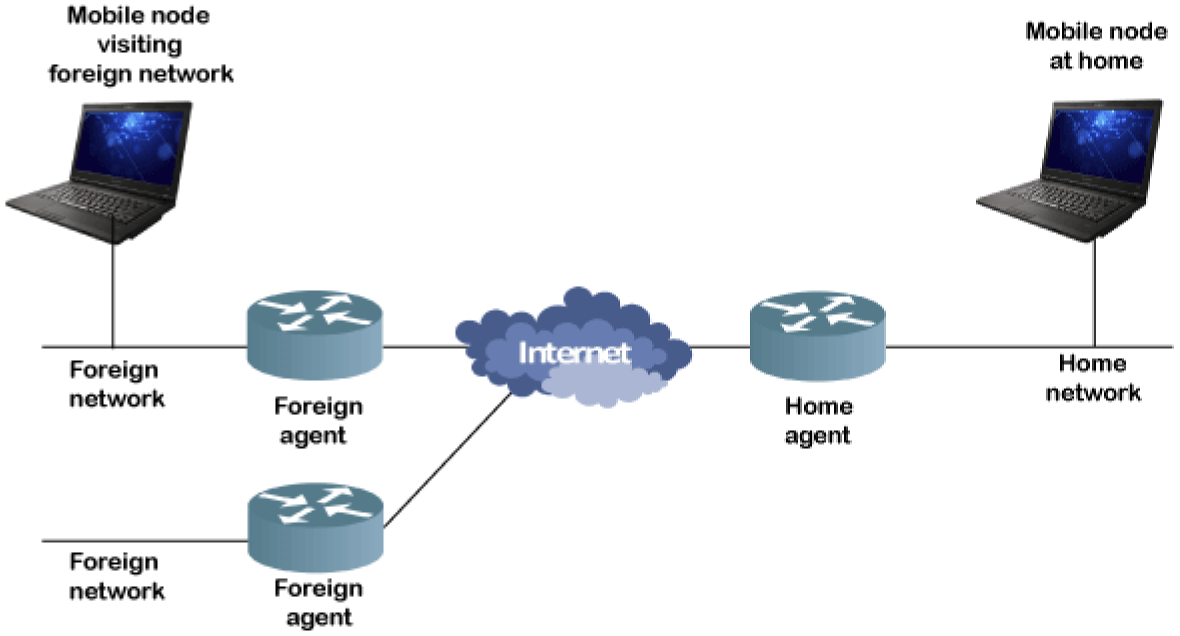
The mobile IP makes the communication flawless and ensures that the communication will occur without the user's sessions or connections being dropped.

Mobile IP is based on IP, so it is scalable for the Internet. Any media that supports IP can also support Mobile IP.

Introduction to Mobile IP Technology

In IP networks, when a device is within its home network, the routing is based on the static IP addresses. The device within a network is connected through normal IP routing by the IP address assigned on the network. It is the same as how a postal letter is delivered to the fixed address on the envelope. The problem occurs when a device goes away from its home network and is no longer reachable using normal IP routing. In this condition, the active sessions of the device are terminated. The idea of Mobile IP was introduced to resolve this issue. It facilitates users to keep the same IP address while going to a different network or a different wireless operator without being communication disrupted or without sessions or connections being dropped.

- The mobility function of the Mobile IP is performed on the network layer rather than the physical layer.
- The architecture of Mobile IP Technology
- The components of the Mobile IP and the relationship among them are specified in the following image:



This is the architecture of Mobile IP technology. It consists of the following components:

- Mobile Node (MN)
- Home Agent (HA)
- Foreign Agent (FA)
- Home Network (HN)
- Foreign Network (FN)
- Corresponding Node (CN)
- Care of Address (COA)

Mobile Node

The Mobile Node is a device or a user or a router that can frequently change their network positions without changing its original IP address. Examples of mobile nodes are cell phone, personal digital assistant (PDA), laptop, etc. whose software enables network roaming capabilities.

Home Agent

The Home Agent is a router on the home network. It serves as the anchor point for communication with the Mobile Node.

Foreign Agent

The Foreign Agent is a router that provides several services such as tunneling data-grams whenever a mobile node visits a foreign network. It is responsible for delivering packets from the Home Agent to the Mobile Node.

Home Network

The home network is the base station network to which the mobile node originally belongs to.

4.5 Internet Protocol version 6 (IPv6)

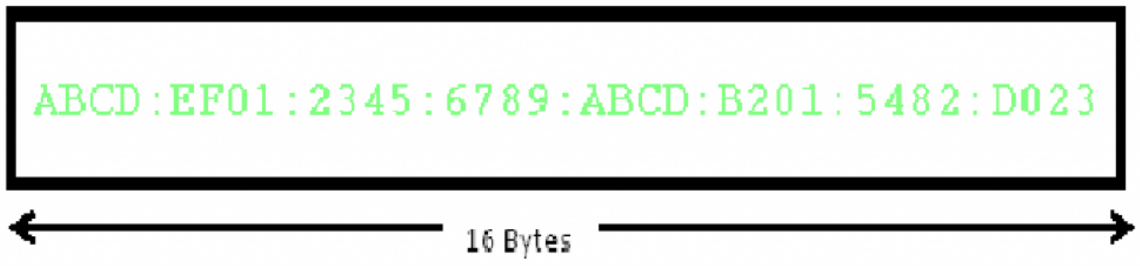
IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2128, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) .

Components in Address format :

There are 8 groups and each group represents 2 Bytes (16-bits).

Each Hex-Digit is of 4 bits (1 nibble)

Delimiter used – colon (:)



Need for IPv6:

The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security. IPv6 protocol responds to the above issues using the following main changes in the protocol:

1. Large address space

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

2. Better header format

IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

3. New options

IPv6 has new options to allow for additional functionalities.

4. Allowance for extension

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

5. Support for resource allocation

In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

6. Support for more security

The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

In IPv6 representation, we have three addressing methods :

- Unicast
- Multicast
- Anycast

Addressing methods

1. Unicast Address

Unicast Address identifies a single network interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2. Multicast Address

Multicast Address is used by multiple hosts, called as groups, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address. And every node is configured in the same way. In simple words, one data packet is sent to multiple destinations simultaneously.

3. Anycast Address

Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

The following are the main issues of the current IPv4 protocol:

Rapid depletion of the address space.

- This has led to the use of Network Address Translators (NATs) that map multiple private addresses to a single public IP address. The main problems created by this mechanism are processing overhead and lack of end-to-end connectivity.

Lack of hierarchy support.

- Because of its inherent predefined class organization, IPv4 lacks true hierarchical support. It is impossible to structure the IP addresses in a way that truly maps the network topology. This crucial design flaw creates the need for large routing tables to deliver IPv4 packets to any location on the Internet.

Complex network configuration

- With IPv4, addresses must be assigned statically or using a configuration protocol such as DHCP. In an ideal situation, hosts would not have to rely on the administration of a DHCP infrastructure. Instead, they would be able to configure themselves based on the network segment in which they are located.

- Lack of built-in authentication and confidentiality.

- IPv4 does not require support for any mechanism that provides authentication or encryption of the exchanged data. This changes with IPv6. Internet Protocol security (IPSec) is an IPv6 support requirement.

- A new protocol suite must satisfy the following basic requirements:
- Large-scale routing and addressing with low overhead.
- Auto-configuration for various connecting situations.
- Built-in authentication and confidentiality.

IPv6 addressing

With IPv6, addresses are 128 bits long. One reason for such a large address space is to subdivide the available addresses into a hierarchy of routing domains that reflect the Internet's topology. Another reason is to map the addresses of network adapters (or interfaces) that connect devices to the network. IPv6 features an inherent capability to resolve addresses at their lowest level, which is at the network interface level, and also has auto-configuration capabilities.

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM	It does not support VLSM.

	means that Ipv4 converts IP addresses into a subnet of different sizes.	
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.