WMT Repeated Questions with Solution

Note:

1. **Below mentioned questions are frequently asked question from university Question papers.**
2. **All of you are requested to refer complete syllabus for the exam, these questions are not sufficient for passing the external university exams.**
3. **Please refer reference books for complete syllabus.**
4. **Questions may be asked beyond this document.**

Q1. What is Bluetooth? Explain structure of Bluetooth network. Also give advantages and disadvantages.

Ans:

Bluetooth:

Bluetooth is a method for data communication that uses short-range radio links to replace cables between computers and their connected units. Industry-wide Bluetooth promises very substantial benefits for wireless network operators, end workers, and content developers of exciting new applications

Architecture:

Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48-bit unique device address (BD_ADDR) that is fixed.

Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel. Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet. Thus, each active device within a piconet is identifiable by a 3-bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet.

A master is the only one that may initiate a Bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master. Slaves are not allowed to talk to each other directly. All communication occurs within the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master. Each piconet uses a different frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM). A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

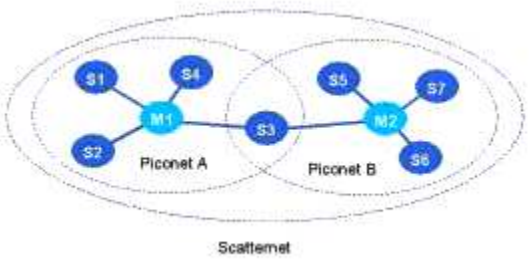
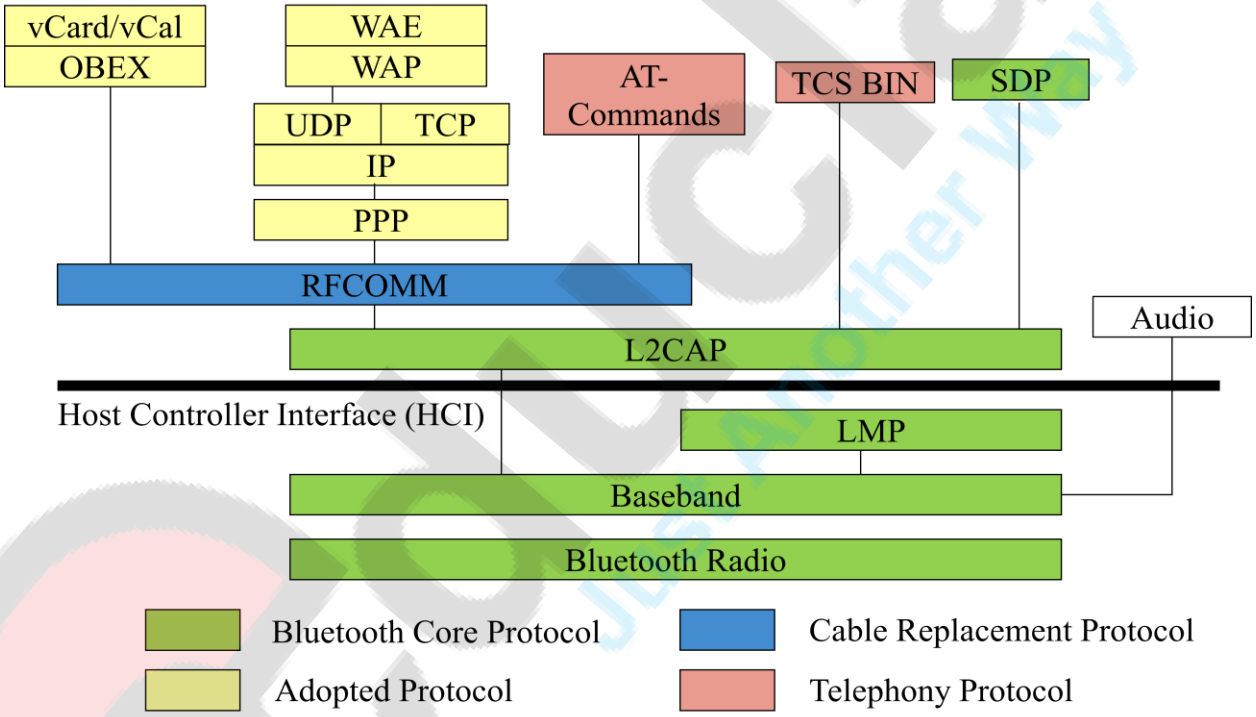


Fig1 : Bluetooth Scatternets and Piconets

Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis. A device may be a master in one piconet and a slave in another or a slave in more than one piconet.



Bluetooth is a layered protocol system. It consists of core protocols like Cable Replacement protocol, Telephony control protocol and Adopted control protocol.
Core protocol consists of following layers:

- **Bluetooth Radio:** specifics details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.
- **Baseband**: concerned with connection establishment within a piconet, addressing, packet format, timing and power control.

- **Link manager protocol (LMP)**: establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size
- **Logical link control and adaptation protocol (L2CAP)**: adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.

RFCOMM is a Cable replacement protocol. It is a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol. It also has connectionless and connection-oriented protocols.
Telephony control protocol (TCS BIN) maintains the call signal between 2 devices. It is a bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices.
Adopted protocol adapts upper layers into baseband layer.
It consists of:

- **PPP**: Point to point protocol is concerned with establishing connection with one device to another.
- **UDP**: User datagram protocol is concerned with packet transmission between two devices.
- **OBEX (OBject EXchange)** : Session-layer protocol for the exchange of objects, providing a model for object and operation representation.
- **WAE/WAP**: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

Advantages:

- It is cheap
- Easy to install
- It makes connecting to different devices convenient
- It is wireless
- It is free to use if the device is installed with it

Disadvantages:

- It can be hacked into
- If installed on a cellphone it is prone to receiving cell phone viruses
- It only allows short range communication between devices
- It can only connect two devices at once

Q2. Explain the operation of Piconet. Explain the inquiry and page procedure of the Bluetooth in a Piconet.
Answer-
Piconet is very important term of the context of Bluetooth. A Piconet is a collection of Bluetooth devices which synchronized to the same hopping sequence. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S). The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Two additional types of devices are shown:

parked devices (P) can not actively participate in the piconet ,but are known and can be reactivated. Devices in stand-by (SB) do not participate in the piconet.

Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked.

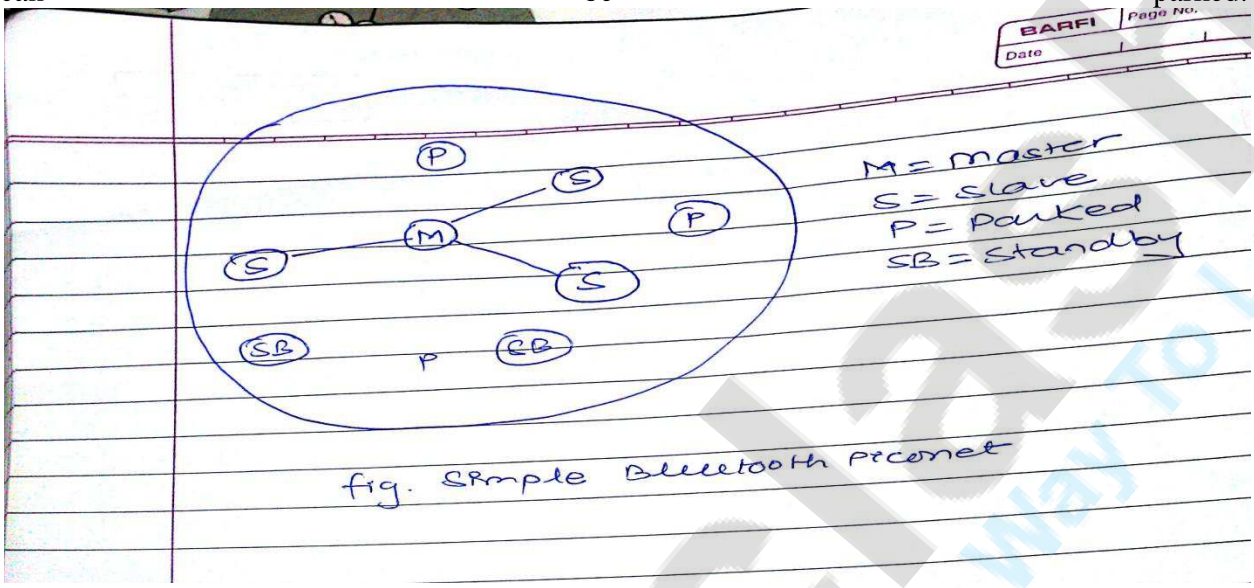


fig. Simple Bluetooth piconet

As all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID. All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave. There is no distinction between terminals and base stations, any two or more devices can forma piconet. The unit establishing the piconet automatically becomes the master, all other devices will be slaves. The hopping pattern is determined by the device ID, a48-bit worldwide unique identifier. The phase in the hopping pattern is deter-mined by the master's clock. After adjusting the internal clock according to the master a device may participate in the piconet. All active devices are assigned a3-bit active member address (AMA). All parked devices use an 8-bit parked member address (PMA). Devices in stand-by do not need an address.

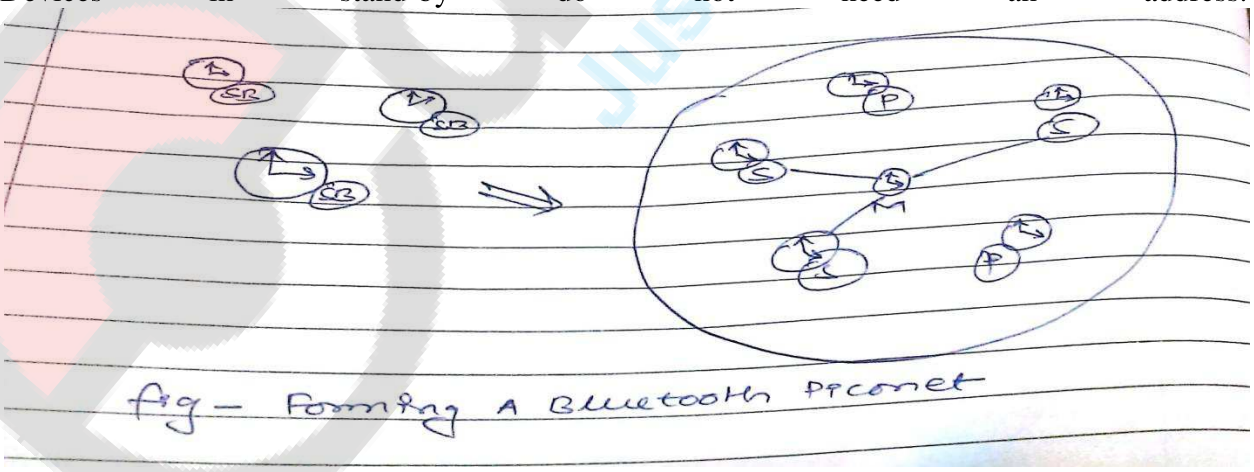


fig- Forming A Bluetooth Piconet

Inquiry- Establishing a connection begins with a phase called "**inquiry**", during which the master device sends an inquiry request to all devices found within its range, called *access points*. All devices which receive the query reply with their address.

Inquiry Procedure- It's a procedure for a potential master to identify devices in range that wish to participate in the piconet. The inquiry procedure begins when the potential master transmits an ID Packet with an Inquiry Access Code(IAC),which is a code common to all Bluetooth devices.

Of the 79 radio carriers ,32 are considered wakeup carriers. The master broadcast the IAC over each of 32 wakeup carriers in turn. Meanwhile devices in the standby state periodically enter the inquiry scan state to search for IAC message on the wakeup carriers. When a device is receive the inquiry it enter in the inquiry response state and ruturn and FHS packet containing its device address and timing information required by the master to initiate the connection.

Once a device in responded to an inquiry it moves to the page scan state to await a page from the master in order to establish a connection.

Page Procedure:

Once master has found the device within the range it is able to establish a connection to each device to setting up a Piconet. Master use the device address to calculate page frequency hopping sequence the aim of which is to connect the device during paging. The master pages by using an ID packet,this time with a device access code(DAC) of the spacefic slave.

The slave response by returning the same DAC ID packet to the master in same hopping sequence that was used by the master. The master responds to this in the next master to slave slot with its own FHS packet , containing its device address and its real time Bluetooth clock value. Once again, the slave sends a response DAC id packet to the master to confirm the receipt of the masters FHS packet. The slave at this point transition from the slave response state to the connection state and begin to use the connection hopping sequence defined in masters FHS packet. The master may continue to page until it has connected to all the desired slave, the master then enters the connection state.

Q3. Describe Bluetooth architecture?

Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocol, and adopted protocols. The core protocols form a five-layer stack consisting 0 the following elements:

- Radio: Specifies details of the air interface, including. Frequency, the use of frequency hopping, modulation scheme, and transmit power.
- Baseband: Concerned with connection establishment within a Piconet, addressing, packet format, timing, and power control.
- Link manager protocol (LMP): Responsible for Ii k setup between Bluetooth devices and ongoing link management. This includes security aspects such as authentication and encryption, plus the control and negotiation of baseband packet sizes.
- Logical link control and adaptation protocol (L2CAP): Adapts upper-layer protocols to the baseband layer. L2CAP provides both connectionless and connection-oriented services.

- Service discovery protocol (SDP): Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.

RFCOMM is the cable replacement protocol include in the Bluetooth specification. RFCOMM presents a virtual serial port that is designed to make replacement of cable technologies as transparent as possible. Serial port are one of the most common types of communications interfaces used with corrupting and communications devices. Hence, RFCOMM enables the replacement of serial port cables with the minimum of modification of existing devices. RFCOM M provides for binary data transport and emulates EIA-232 control signals over the Bluetooth baseband layer. EIA-232 (formerly known as RS-232) is a widely used serial port interface standard. Bluetooth specifies a telephony control protocol.

TCS BIN (telephony control specification-binary) is a bit-oriented protocol that defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. In addition, it defines mobility management procedures for handling groups of Bluetooth TCS devices. The adopted protocols are defined in specifications issued by other standards making organizations and incorporated into the overall Bluetooth architecture. The Bluetooth strategy is to invent only necessary protocols and use existing standards whenever possible. The adopted protocols include the following:

• PPP: The point-to-point protocol is an Internet standard protocol for transporting IP datagram's over a point-to-point link.

• TCP/UDP/IP: These are the foundation protocols of the TCP/IP protocol suite .
• OBEX: The object exchange protocol is a session-Ievel protocol developed by the Infrared Data Association (IrDA) for the exchange of objects. OBEX provides functionality similar to that of HTTP, but in a simpler fashion. It also provides a model for representing objects and opera ions. Examples of content formats transferred by OBEX are vCard and v Calendar, which provide the format of an electronic business card and personal calendar entries and scheduling information, respectively.
• WAE/WAP: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

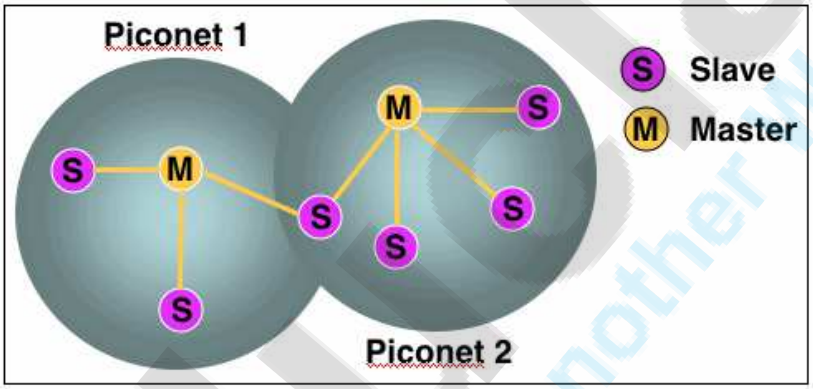
Q4. Short notes on piconet & scatternet.

- **Piconet**
- Basic unit of networking in BT.
- Consisting of a master and from 1 to 7 active slave devices.
- The radio designated as the master makes the determination of the channel and phase that shall be used by all devices on this piconet.
- A slave may only communicate with the master and may only communicate when granted permission by the master.

- A device in one piconet may also exist as part of another piconet and may function as either a slave or master in each piconet .

- A piconet is a computer network which links a wireless user group of devices using Bluetooth technology protocols.
- A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence).
- It allows one *master* device to interconnect with up to seven active *slave* devices. Up to 255 further slave devices can be inactive, or *parked*, which the master device can bring into active status at any time, but an active station must go into parked first.
- Some examples of piconets include a cell phone connected to a computer, a laptop and a Bluetooth-enabled digital camera, or several PDAs that are connected to each other.

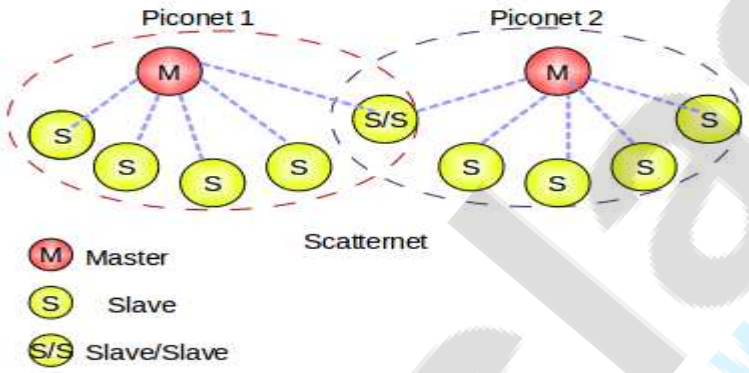
Diagram:



- **ScatterNets:**
  - Device in one piconet may exist as master or slave in another piconet. This form of overlapping is called a scatternet.
  - Allows many devices to share same area
  - Makes efficient use of bandwidth using spread spectrum techniques
  - Collision occur when device in different piconets, on different logical channel, happen to use the same hop frequency at the same time.
  - The physical area and the total bandwidth are shared by the scatternet.
  - The logical channel and data transfer are shared by a piconet.
  - A **scatternet** is a type of ad hoc computer network consisting of two or more piconets.
  - The terms 'scatternet' and 'piconet' are typically applied to Bluetooth wireless technology.
  - A *scatternet* is a number of interconnected piconets that supports communication between more than 8 devices.

- Scatternets have the potential to bring the interconnectivity of the Internet to the physical world through wireless devices.
- A number of companies have attempted to launch social networking and dating services that leverage early scatternet implementations (see Bluedating).
- Scatternets can also be used to enable ad hoc and communication interaction between autonomous robots and other devices.

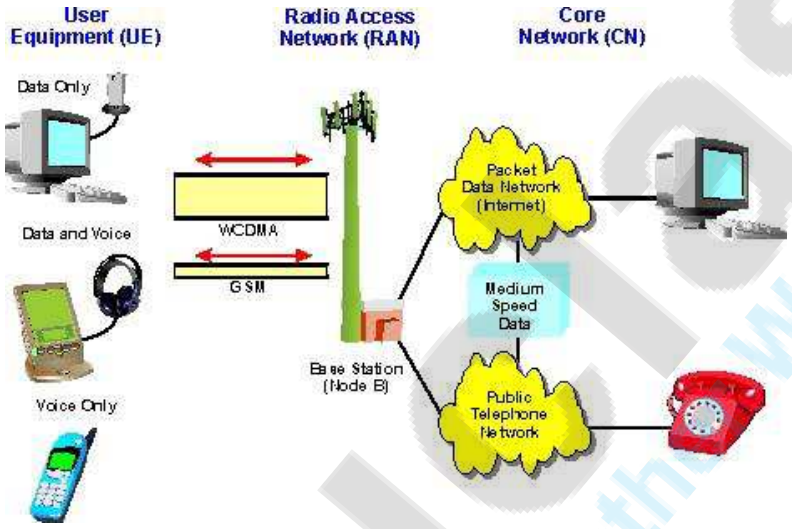
Diagram:



Q5. Short note on WCDMA

- Ans: Wideband CDMA is a third generation (3G) wireless standard which utilizes one 5MHZ channel for both voice and data,initially offering data speeds up to 384 kbps.
- WCDMA was the 3G technology used in the US by AT&T and T-moblie.
- Wideband code division multiple access is a **3rd generation mobile communication system** that uses code division multiple access (CDMA) technology over a wide frequency band to provide **high-speed multimedia** and efficient voice services.
- The WCDMA infrastructure is compatible with GSM mobile radio communication system. WCDMA provides for high-speed data and voice communication services.
- Installing or upgrading to WCDMA technology allows mobile service providers to offer their customers wireless broadband (high-speed Internet) services and to operate their systems more efficiently (more customers per cell site radio tower).
- The WCDMA system is composed of mobile devices (wireless telephones and data communication devices called **user equipment-UE**), radio towers (cell sites called **Node Bs**), and an **packet data interconnection system** (switches and data routers). The WCDMA system uses two types of radio channels; frequency division duplex (FDD) and time division duplex (TDD).
- The FDD radio channels are primarily used for wide area voice (audio) channels and data services.
- The TDD channels are typically used for systems that do not have the availability of dual frequency bands.

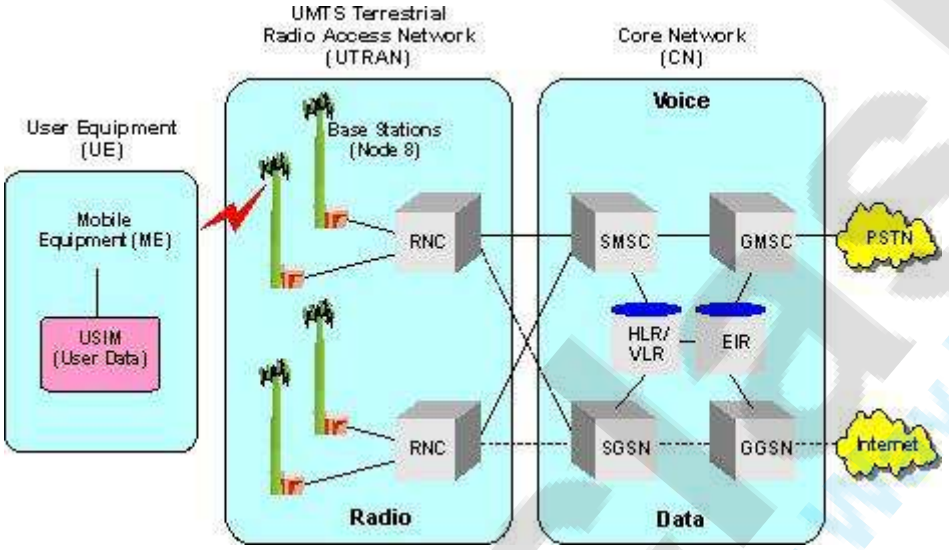
- This figure shows a simplified diagram of a WCDMA system. This diagram shows that the WCDMA system includes various types of mobile communication devices (called user equipment - UE) that communicate through base stations (node B) and a mobile switching center (MSC) or data routing networks to connect to other mobile telephones, public telephones, or to the Internet via a core network (CN).
- This diagram shows that the WCDMA system is compatible with both the **5 MHz wide WCDMA radio channel** and the narrow 200 kHz GSM channels.
- This example also shows that the core network is essentially divided between voice systems (circuit switching) and packet data (packet switching).



Wideband Code Division Multiple Access -WCDMA Diagram

- This figure shows a simplified functional diagram of a WCDMA network. This diagram shows that the WCDMA system is composed of 3 **key parts**; the **user equipment (UE)**, **UMTS terrestrial radio access network (UTRAN)**, and a core interconnecting network.
- The UE is divided into 2 parts, the mobile equipment (ME) and the UMTS subscriber identity module (USIM) card. The UTRAN is composed of base stations (called Node B) and radio network controllers (RNCs).
- This example shows that the RNCs connect voice calls to mobile switching centers (MSCs) and connect data sessions to packet data service nodes (PDSNs).
- The core network is basically divided into circuit switched (primarily voice) and packet switched (primarily data) parts.
- The **core network** circuit switch parts contain the serving MSC and a gateway MSC. The serving MSC (SMSC) connects to the UTRAN system and the gateway MSC (GMSC) connects to the public telephone network.

- The core network packet switched parts contain the serving general packet radio service (GPRS) support node (SGSN) and a gateway GPRS service node (GGSN).
- The SGSN connects to the UTRAN system and the GGSN connects to data networks such as the Internet.



WCDMA Network Diagram

Q6. Explain in details IEEE 802.11 system architecture &discuss service provided by it.

Ans: A wireless LAN (WLAN or WiFi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure and 802.11 is a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in the year 1997.

Process

i) The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement.

ii) When two or more stations come together to communicate with each other, they form a Basic Service Set (BSS). The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.

iii) A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-Hoc Network. An ad-hoc network is a network where stations communicate only peer to peer.

iv) There is no base and no one gives permission to talk. Mostly these networks are spontaneous and can be set up rapidly. Ad-Hoc or IBSS networks are characteristically limited both temporally and spatially.

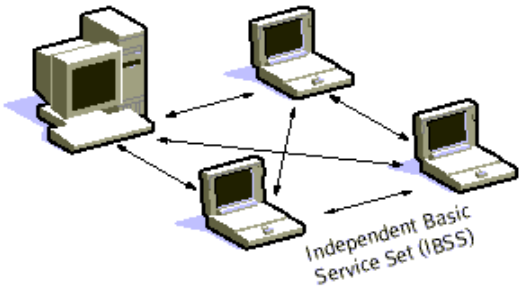


Fig 1: "Adhoc Mode"

v) When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network.

vi) Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

vii) Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations within the ESS can communicate or even move between BSS's transparently to the LLC.

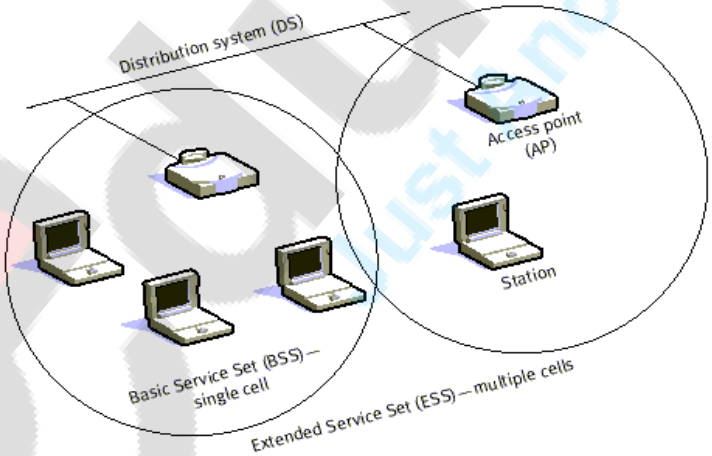


Fig 2: Infrastructure Mode

viii) One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11. It also can serve as the access point to the DS. All data going to an 802.11 LAN from an 802.X LAN must pass through a portal. It thus functions as bridge between wired and wireless.

ix) The implementation of the DS is not specified by 802.11. Therefore, a distribution system may be created from existing or new technologies. A point-to-point bridge connecting LANs in two separate buildings could become a DS.

Services

While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections

1. Station Services (SS)
2. Distribution System Services (DSS).

There are five services provided by the DSS

1. **Association**
2. **Reassociation**
3. **Disassociation**
4. **Distribution**
5. **Integration**

1)**Association**

a) The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition.

b) A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by Associating itself with an access point. Associations are dynamic in nature because stations move, turn on or turn off. A station can only be associated with one AP.

c) This ensures that the DS always knows where the station is.Association supports no-transition mobility but is not enough to support BSS-transition.

2) **Reassociation.** This service allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station.

3) **Disassociation** is when the association between the station and the AP is terminated. This can be initiated by either party. A disassociated station cannot send or receive data. ESS-transition are not supported. A station can move to a new ESS but will have to reinitiate connections.

4) **Distribution and Integration** are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver. The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same. So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.

Station services are:

1. **Authentication**
2. **Deauthentication**
3. **Privacy**

Authentication

a) There are two types of authentication services offered by 802.11. The first is Open System Authentication. This means that anyone who attempts to authenticate will receive authentication.
b) The second type is Shared Key Authentication. In order to become authenticated the users must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm.
c) The shared secret is delivered to all stations ahead of time in some secure method (such as someone walking around and loading the secret onto each station).

Deauthentication

a) Deauthentication is when either the station or AP wishes to terminate a stations authentication. When this happens the station is automatically disassociated. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic.
b) IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy. If WEP is not used then stations are "in the clear" or "in the red", meaning that their traffic is not encrypted. Data transmitted in the clear are called plaintext.
c) Data transmissions, which are encrypted, are called ciphertext. All stations start "in the red" until they are authenticated. MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

Privacy

a) Privacy is whether or not encryption is used. Wired Equivalent Privacy is used to protect authorized stations from eavesdroppers. WEP is reasonably strong. The algorithm can be broken in time. The relationship between breaking the algorithm is directly related to the length of time that a key is in use.
b) So, WEP allows for changing of the key to prevent brute force attack of the algorithm. WEP can be implemented in hardware or in software. One reason that WEP is optional is because encryption may not be exported from the United States. This allows 802.11 to be a standard outside the U.S. albeit without the encryption.

Q7. **Why is WEP is weak algorithm? Discuss WPA and WPA2**

- **Wired Equivalent Privacy (WEP)** is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard, its main objective is to provide data confidentiality as comparable to that of a traditional wired network.

- WEP was designed to protect users of a WLAN from casual eavesdropping .To provide privacy as well as data integrity, WEP uses an algorithm based on the **RC4** encryption algorithm.
- RC4 uses stream cipher technique. It is a symmetric algorithm uses the same key for both encryption and decryption.
- For each transmission the plain text is bitwise XORed with a pseudorandom key stream to produce cipher text.

- Stream ciphers vulnerable to several attacks. If an attacker flips a bit in the cipher text, then upon decryption, the corresponding bit in the plaintext will be flipped. Also.
- If an eavesdropper intercepts two cipher texts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts.
- The statistical attacks become increasingly practical as more cipher texts that use the same key stream are known. Once one of the plaintexts becomes known, it is easy to recover all of the others. Hence its not a good choice to prefer to use WEP algorithm for wireless communication.

B) Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)

- WPA and WPA2 protect the wireless network from a variety of threats, including lost or stolen devices and hacker attacks such as **'man-in-the-middle', authentication forging, replay, key collision, weak keys, packet forging attacks.**
- This programs was developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).
- **WPA** protocol implements much of the IEEE 802.11 standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change.
- WPA addresses the weaknesses of original WEP security resulting from WEP's imperfect encryption key implementation and its lack of authentication.
- TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.
- Using TKIP, it brings an enhanced encryption algorithm and with IEEE 802.1X/EAP authentication it brings standards-based mutual authentication to Wi-Fi networks.
- WPA contains a **message integrity check**, which is designed to prevent an attacker from altering and resending data packets. This replaces the cyclic redundancy check(CRC) that was used by the WEP standard.

2) WPA2 is an update version of WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11. In particular, it includes mandatory support for CCMP, an AES-based encryption mode with strong security.

- WPA2 offers advanced protection from wireless network attacks. Using AES, government grade encryption and IEEE 802.1X/EAP authentication **WPA2 provides stronger standards-based mutual authentication and advanced encryption to protect the Wi-Fi network from a variety of attacks**
- WPA2 contains a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed to use for home users without an enterprise authentication server.
- To encrypt a network with WPA2-PSK you provide your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long.
- Using a technology called TKIP(for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. Although WEP also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F.Its recommended to use WPA2 than using WPA or WEP security protocol

Q8. **Explain features of WIMAX along with its system reference architecture?**

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the salient features are:

Two Type of Services

WiMAX can provide two forms of wireless service:

- **Non-line-of-sight:** service is a WiFi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).
- **Line-of-sight:** service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it's able to send a lot of data with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.

Features of wimax:

OFDM-based physical layer:

The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

Very high peak data rates:

WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.

Scalable bandwidth and data rate support:

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth.

Adaptive modulation and coding (AMC):

WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed on a per user and per frame basis, based on channel conditions.AMC is an effective mechanism to maximize throughput in a time-varying channel.

WiMAX uses OFDM:

Mobile WiMAX uses Orthogonal frequency division multiple access (OFDM) as a multiple-access technique, whereby different users can be allocated different subsets of the OFDM tones.

Flexible and dynamic per user resource allocation:

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

Robust security:

WiMAX supports strong encryption, using Advanced Encryption Standard (AES), and has a robust privacy and key-management protocol.

Support for mobility:

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

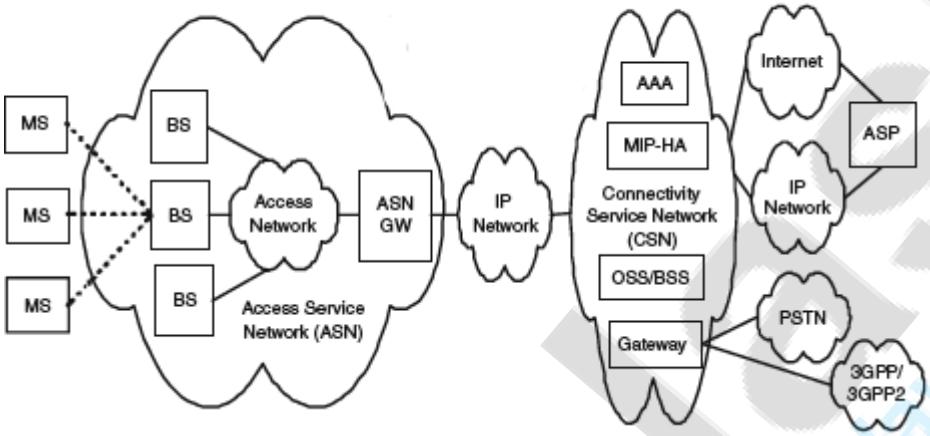
The WiMAX NWG has developed a network reference model to serve as an architecture framework for WiMAX deployments and to ensure interoperability among various WiMAX equipment and operators.

The network reference model envisions a unified network architecture for supporting fixed, nomadic, and mobile deployments and is based on an IP service model. Below is simplified illustration of an IP-based WiMAX network architecture. The overall network may be logically divided into three parts:

- Mobile Stations (MS) used by the end user to access the network.
- The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.
- Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.
- The network reference model developed by the WiMAX Forum NWG defines a number of functional entities and interfaces between those entities. Fig below shows some of the more important functional entities.
- **Base station (BS):** The BS is responsible for providing the air interface to the MS. Additional functions that may be part of the BS are micromobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, DHCP (Dynamic Host Control Protocol) proxy, key management, session management, and multicast group management.
- **Access service network gateway (ASN-GW):** The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN. Additional functions that may be part of the ASN gateway include intra-ASN location management and paging, radio resource management, and admission control, caching of subscriber profiles, and encryption keys, AAA client functionality, establishment, and management of mobility tunnel with base stations, QoS and policy enforcement, foreign agent functionality for mobile IP, and routing to the selected CSN.
- **Connectivity service network (CSN):** The CSN provides connectivity to the Internet, ASP, other public networks, and corporate networks. The CSN is owned by the NSP and includes AAA servers that support authentication for the devices, users, and specific

services. The CSN also provides per user policy management of QoS and security. The CSN is also responsible for IP address management, support for roaming between different NSPs, location management between ASNs, and mobility and roaming between ASNs.

IP-Based WiMAX Network Architecture



The WiMAX architecture framework allows for the flexible decomposition and/or combination of functional entities when building the physical entities. For example, the ASN may be decomposed into base station transceivers (BST), base station controllers (BSC), and an ASNGW analogous to the GSM model of BTS, BSC, and Serving GPRS Support Node (SGSN).

Q9. Explain the operation of mobile IP

Mobile IP (or **MIP**) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

The Mobile IP allows for location-independent routing of IP datagram's on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagram's to the mobile node through the tunnel.

Mobile IP is most often found in wireless WAN environments where users need to carry their mobile devices across multiple LANs with different IP addresses.

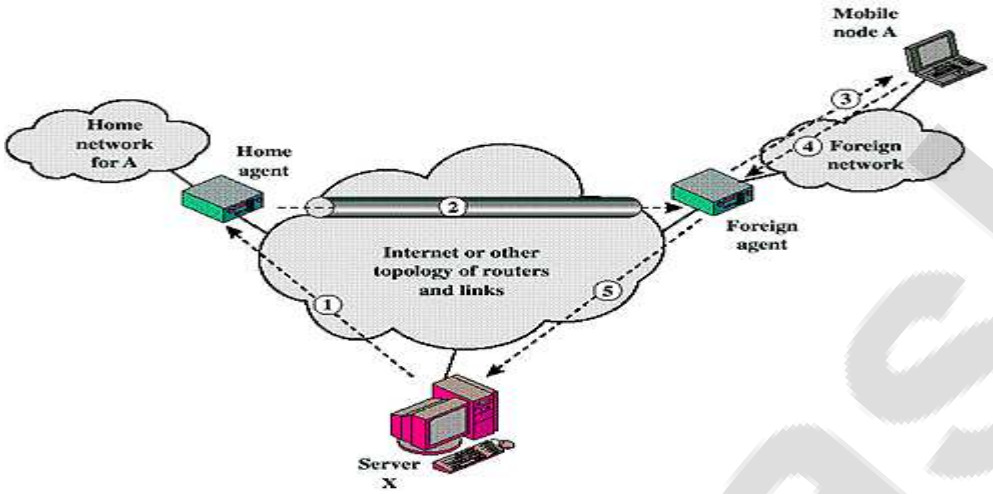


Figure shows in general terms how Mobile IP deals with the problem of dynamic IP addresses. A mobile node is assigned to a particular network, known as its home network. Its IP address on that network, known as its home address, is static.

When the mobile node moves its attachment point to another network, that's considered a foreign network for this host. Once the mobile node is reattached, it makes its presence known by registering with a network node, typically a router, on the foreign network known as a foreign agent.

The mobile node then communicates with a similar agent on the user's home network, known as a home agent, giving the home agent the care-of address of the mobile node; the care-of address identifies the foreign agent's location. Typically, one or more routers on a network will implement the roles of both home and foreign agents.

Mobile IP scenario

When IP datagram's are exchanged over a connection between the mobile node (A) and another host (server X), the following operations occur:

1. Server X transmits an IP datagram destined for mobile node A; with A's home address in the IP header. The IP datagram is routed to A's home network.
2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram that has A's care-of address in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as tunneling.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level protocol data unit or PDU (such as a LAN LLC frame), and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it uses X's IP address. In our example, this is a fixed address; that is, X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network for routing to X. Typically, this router is also the foreign agent.
5. The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

To support the operations illustrated in Mobile IP includes three basic capabilities:

- **Discovery.** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.

- **Registration.** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
- **Tunneling.** Tunneling is used to forward IP datagrams from a home address to a care-of address.

Q10. **What are the functions supported by WML? In brief describe WTLS security and services.**

Wireless Markup Language

- WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability.
- It is designed to work with telephone keypads, styluses, and other input devices common to mobile, wireless communication.
- WML permits the scaling of displays for use on two-line screens found in some small devices, as well as the larger screens found on smart phones.
- For an ordinary PC, a Web browser provides content in the form of Web pages coded with the Hypertext Markup Language (HTML).
- To translate an HTML coded Web page into WML with content and format suitable for wireless devices, much of the information, especially graphics and animation, must be stripped away.
- WML presents mainly text-based information that attempts to capture the essence of the Web page and that is organized for easy access for users of mobile devices.

Important features of WML include the following:

- Text and image support: Formatting and layout commands are provided for text and limited image capability.
- Deck/card organizational metaphor: WML documents are subdivided into small, well-defined units of user interaction called cards. Users navigate by moving back and forth between cards. A card specifies one or more units of interaction (a menu, a screen of text, or a text-entry field). A WML deck is similar to an HTML page in that it is identified by a Web address (URL) and is the unit of content transmission.
- Support for navigation among cards and decks: WML includes provisions for event handling, which is used for navigation or executing scripts.

Wireless Transport Layer Security (WTLS):

- WTLS provides security services between the mobile device (client) and the WAP gateway.
- WTLS is based on the industry-standard Transport Layer Security (TLS) Protocol, which is a refinement of the secure sockets layer (SSL).
- TLS is the standard security protocol used between Web browsers and Web servers.
- WTLS is more efficient that TLS, requiring fewer message exchanges.

- To provide end-to-end security, WTLS is used between the client and the gateway, and TLS is used between the gateway and the target server.
- WAP systems translate between WTLS and TLS within the WAP gateway.
- Thus, the gateway is a point of vulnerability and must be given a high level of security from external attacks.

WTLS provides the following features:

- Data integrity: Ensures that data sent between the client and the gateway are not modified, using message authentication.
- Privacy: Ensures that the data cannot be read by a third party, using encryption
- Authentication: Establishes the authentication of the two parties, using digital certificates
- Denial-of-service protection: Detects and rejects messages that are replayed or not successfully verified.

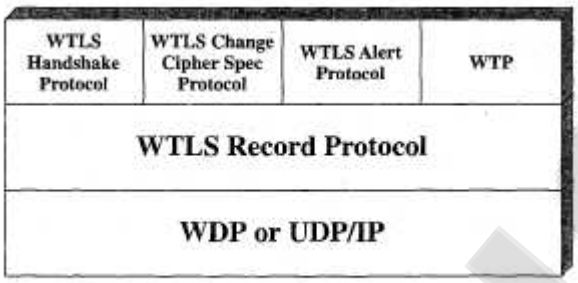


Figure 12.16 WTLS Protocol Stack

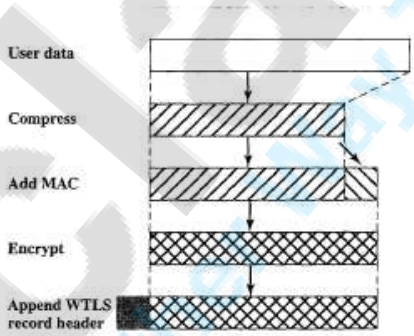


Figure 12.17 WTLS Record Protocol Operation

Q11. Describe WAP protocol stack

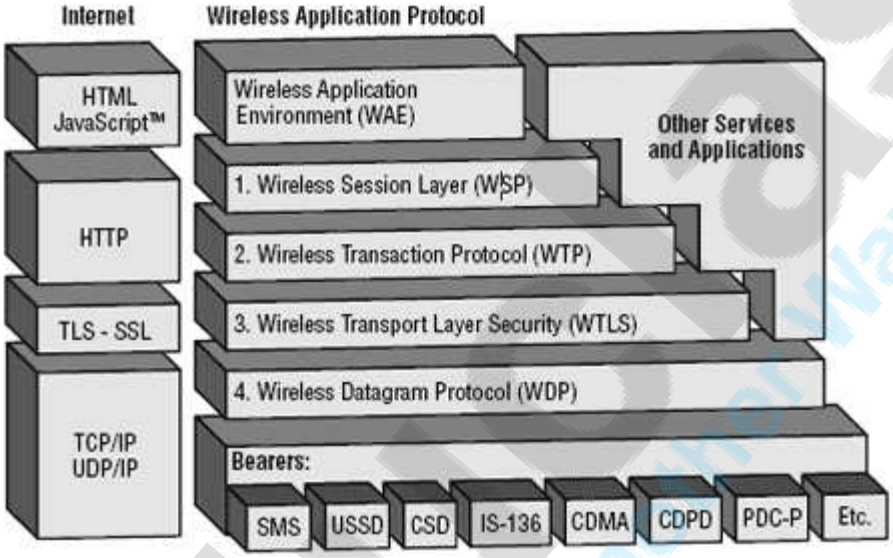
Ans: WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers:

- **Application Layer**
  Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.
- **Session Layer**
  Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.
- **Transaction Layer**
  Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.
- **Security Layer**
  Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.
- **Transport Layer**

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.



Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.

Q12. **Write a note on WAP Programming Model.**

Ans:WAP (Wireless Application Protocol) Programming Model:

1. The Wireless Application Protocol (WAP) is a universal, open standard developed by the WAP Forum to provide mobile users of wireless phones and other wireless terminals.
2. WAP is designed to work with all wireless network technologies (e.g., GSM, CDMA, and TDMA).
3. WAP is based on existing Internet standards, such as IP, XML, HTML, and HTTP, as much as possible. It also includes security facilities.
4. WAP affects use of mobile phones and terminals for data services are the significant limitations of the devices and the networks that connect them. The devices have limited processors, memory, and battery life.
5. The WAP specification includes
    - A programming model based on the WWW Programming Model
    - A markup language, the Wireless Markup Language, adhering to XML
    - A specification of a small browser suitable for a mobile, wireless terminal

- A lightweight communications protocol stack

6. The WAP Programming Model is based on three elements:
   a) Client
   b) Gateway
   c) Original Server
7. HTTP is used between the gateway and the original server to transfer content.
8. The gateway acts as a proxy server for the wireless domain.
9. It processor provide services that offload the limited capabilities of the hand-held, mobile, wireless terminals.
10. For example, the gateway provides DNS services, converts between WAP protocol stack and the WWW stack (HTTP and TCP/IP), encodes information from the Web into a more compact form that minimizes wireless communication, and, in the other direction, and decodes the compacted form into standard Web communication conventions.
11. The gateway also caches frequently requested information.

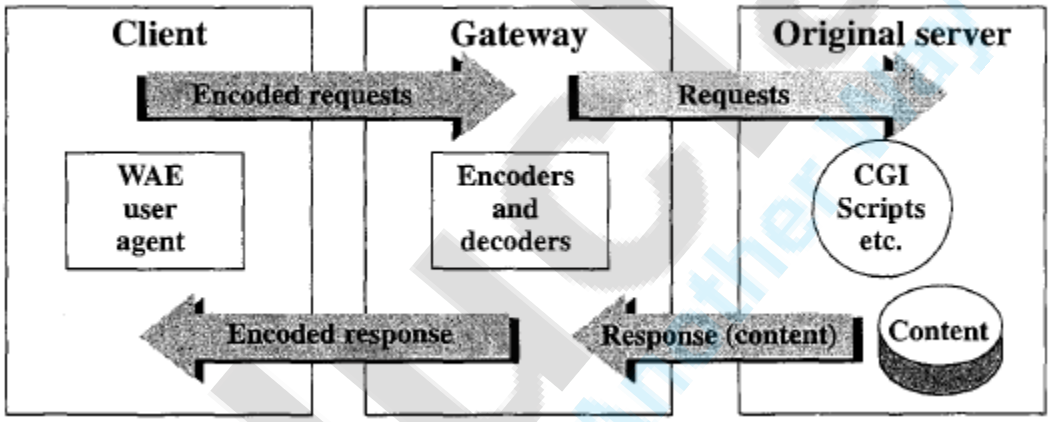


Figure: WAP Programming Model

Q13. Explain indirect TCP, selective TCP and snooping TCP with its advantages and disadvantages

Traditional TCP

- Transport protocols typically designed for
  - Fixed end-systems
  - Fixed, wired networks
- TCP congestion control
  - packet loss in fixed networks typically due to (temporary) overload situations
  - router have to discard packets as soon as the buffers are full

- TCP recognizes congestion only indirect via missing acknowledgements, retransmissions unwise, they would only contribute to the congestion and make it even worse

TCP handles the congestion using two methods

- TCP Congestion control Mechanism-1
- TCP Congestion control Mechanism-2

TCP Congestion control Mechanism-1

- TCP slow-start algorithm
  - Sender calculates a congestion window for a receiver
  - Start with a congestion window size equal to one segment
  - If the sender receives the ack for one packet, it increases the congestion window by one packet
  - This schemes doubles the congestion window every time the ack come back
  - Exponential increase of the congestion window up to the congestion threshold, then linear increase
  - Missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window
  - Congestion window starts again with one segment

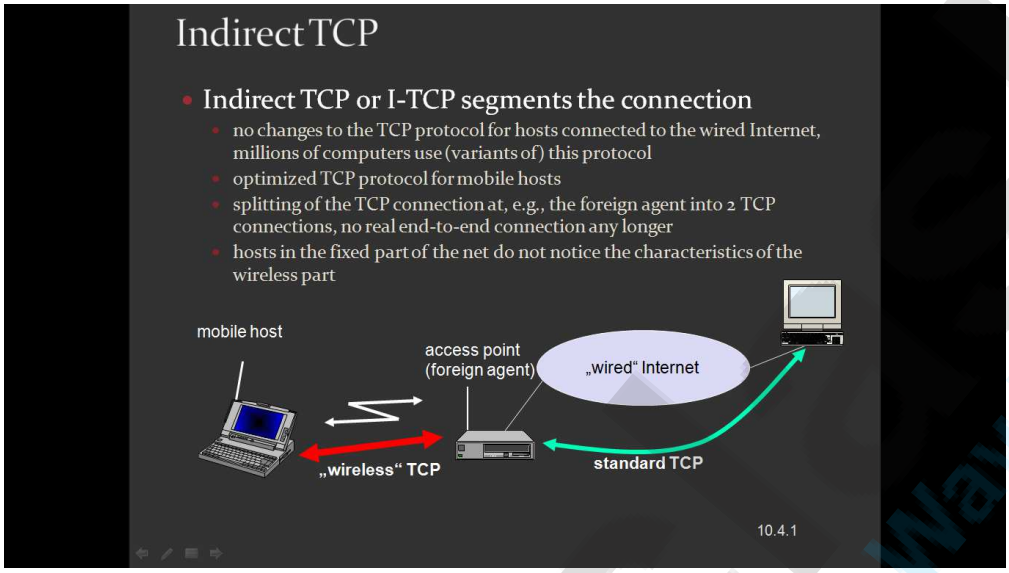
TCP Congestion control Mechanism-2

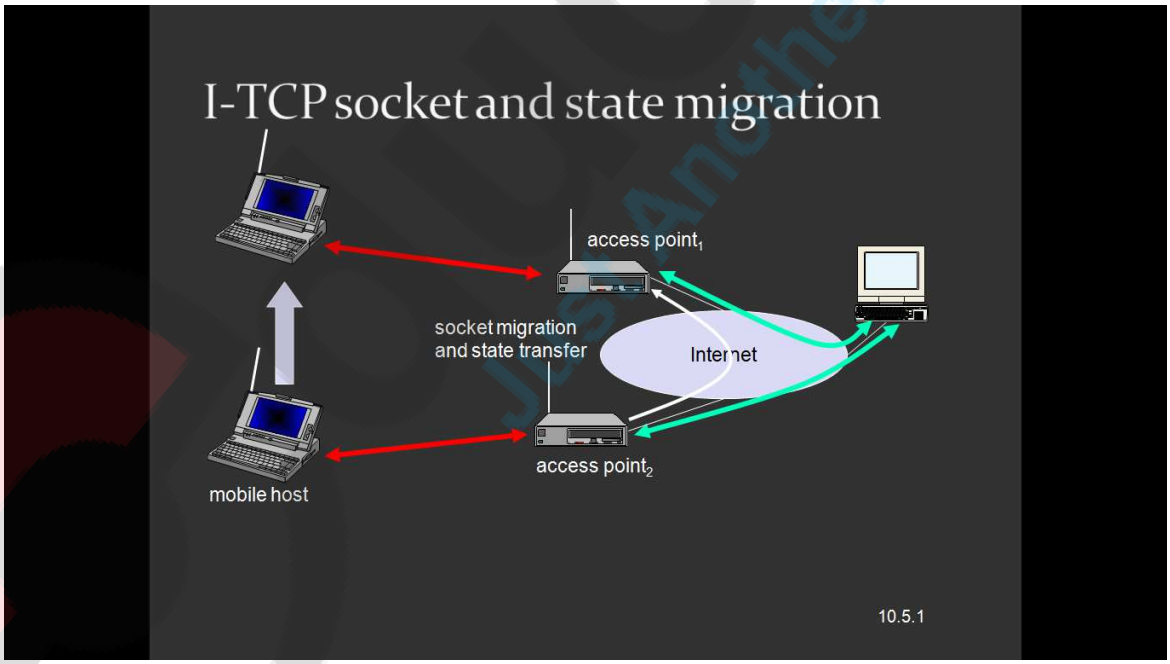
- TCP fast retransmit/fast recovery
  - TCP sends an acknowledgement only after receiving a packet
  - If a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver
  - However, the receiver got all packets up to the gap and is actually receiving packets
  - Therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start)
  - The sender now retransmits the missing packets before the timer expires(fast recovery)
  - This mechanism can improves the efficiency of TCP dramatically

Influences of mobility on TCP-mechanisms

- TCP assumes congestion if packets are dropped
  - typically wrong in wireless networks, here we often have packet loss due to transmission errors
  - furthermore, mobility itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible
- The performance of an unchanged TCP degrades severely

- however, TCP cannot be changed fundamentally due to the large base of installation in the fixed network, TCP for mobility has to remain compatible
- the basic TCP mechanisms keep the whole Internet together



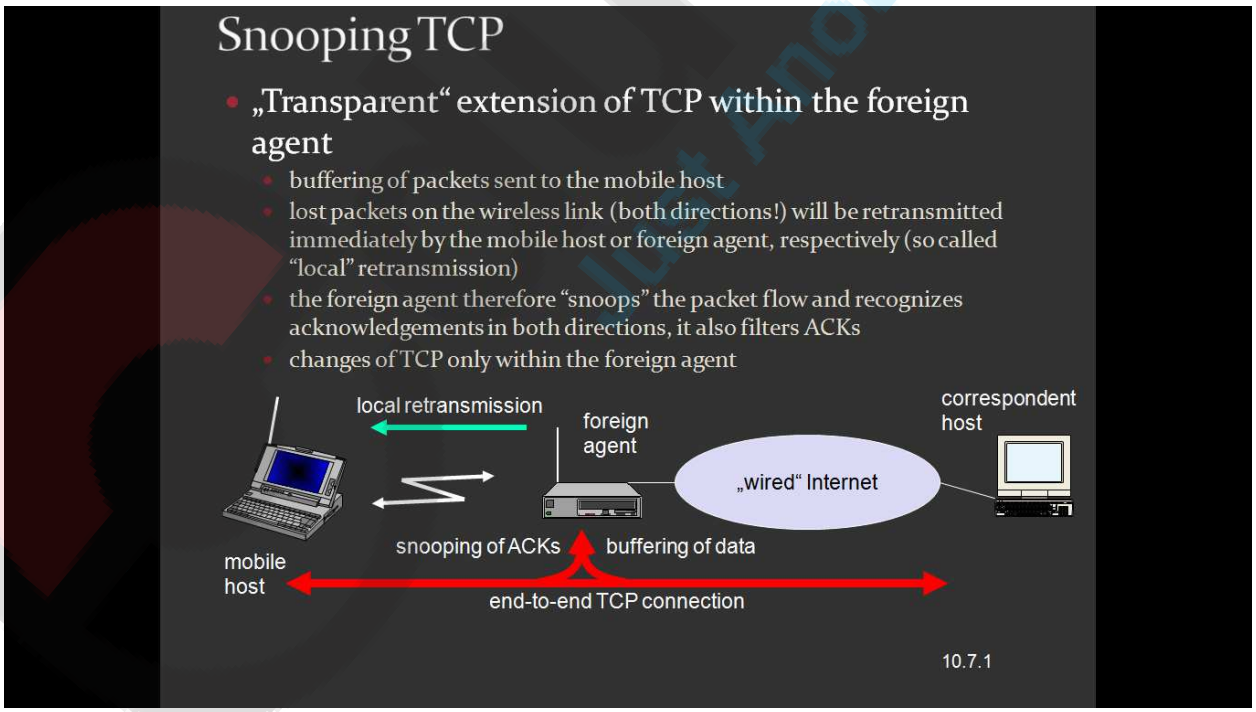


Advantages of I- TCP

- No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- Transmission errors on the wireless link do not propagate into the fixed network
- Packets in sequence without any gaps leave the foreign agent
- Simple to control, mobile TCP is used only for one hop between, e.g., A foreign agent and mobile host
- An optimized TCP with precise timeout can guarantee fast retransmission
- Partitioning into two connections allows the use of a different transport layer protocol between the foreign agent (which acts as a gateway) and the mobile host or the use of compressed headers

Disadvantages of I-TCP

- Loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash
- The correspondent host does not know anything about the partitioning, so the crashing node may also crash the application running on the corresponding node
- Higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent
- Need of the foreign agent to be integrated into all the security mechanism
- Segmentation of the single TCP into two TCP connections



Snooping TCP

- Data transfer to the mobile host
  - FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
  - fast retransmission possible, transparent for the fixed network
- Data transfer from the mobile host
  - FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
  - MH can now retransmit data with only a very short delay
- Integration of the MAC layer
  - MAC layer often has similar mechanisms to those of TCP
  - thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them
- Problems
  - snooping TCP does not isolate the wireless link as good as I-TCP
  - snooping might be useless depending on encryption schemes

Mobile TCP

- Special handling of lengthy and/or frequent disconnections
- M-TCP splits as I-TCP does
  - unmodified TCP fixed network to supervisory host (SH)
  - optimized TCP SH to MH
- Supervisory host
  - no caching, no retransmission
  - monitors all packets, if disconnection detected
    - set sender window size to 0
    - sender automatically goes into persistent mode
  - old or new SH reopen the window after detecting the connectivity
  - The sender can continue sending at full speed
  - No change required on the sender's TCP
  - The wireless side uses an adapted TCP that can recover faster, does not use slow start
  - M-TCP needs a bandwidth manager to implement fair sharing over the wireless link
- Advantages
  - maintains semantics, supports disconnection, no buffer forwarding
- Disadvantages
  - loss on wireless link propagated into fixed network
  - adapted TCP on wireless link requires a bandwidth manager

Fast retransmit/fast recovery

- Change of foreign agent often results in packet loss
  - TCP reacts with slow-start although there is no congestion
- Forced fast retransmit
  - as soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
  - this forces the fast retransmit mode at the communication partners, ie. the corresponding host continues to send with the same rate it did before the mobile host moved to the new foreign agent
  - additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration
- Advantage
  - simple changes result in significant higher performance
- Disadvantage
  - Further mix of IP and TCP, no transparent approach

Transmission/time-out freezing

- Mobile hosts can be disconnected for a longer time
  - no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells ,with higher priority traffic
  - TCP disconnects after time-out completely
- TCP freezing
  - MAC layer is often able to detect interruption in advance
  - MAC can inform TCP layer of upcoming loss of connection
  - TCP stops sending, but does now not assume a congested link
  - MAC layer signals again if reconnected
- Advantage
  - scheme is independent of data
- Disadvantage
  - TCP on mobile host has to be changed, mechanism depends on MAC layer

Selective retransmission

- TCP acknowledgements are often cumulative
  - ACK n acknowledges correct and in-sequence receipt of packets up to n
  - if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n), thus wasting bandwidth
- Selective retransmission as one solution
  - RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps
  - sender can now retransmit only the missing packets
- Advantage
  - much higher efficiency

- Disadvantage
  - more complex software in a receiver, more buffer needed at the receiver

Transaction oriented TCP

- TCP phases
  - connection setup, data transmission, connection release
  - using 3-way-handshake needs 3 packets for setup and release, respectively
  - thus, even short messages need a minimum of 7 packets!
- Transaction oriented TCP
  - RFC1644, T-TCP, describes a TCP version to avoid this overhead
  - connection setup, data transfer and connection release can be combined
  - thus, only 2 or 3 packets are needed
- Advantage
  - efficiency
- Disadvantage
  - requires changed TCP
  - mobility not longer transparent

Comparison of different approaches for a "mobile" TCP

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent