18IT504

Hall Ticket Number:

III/IV B.Tech Regular DEGREE EXAMINATION

Feb, 2021 **Information Technology**

Fifth Semester **Wireless Networks**

Time: Three Hours **Maximum :** 50 Marks

Answer all questions from Part-A. (1X10= 10 Marks)
Answer ANY FOUR questions form Part-B. (4X10=40 Marks)

PART - A

Answer All Questions **(1 X 10 = 10 Marks)**

1.
a) What is Frequency Division Multiplexing?
b) What is Hidden Terminal Problem?
c) What is the purpose of HLR in GSM?
d) Define Handover
e) List the applications of Digital Video Broadcasting.
f) Draw the format of IEEE 802.11 PHY frame using FHSS.
g) What are the requirements of Mobile IP?
h) What is DHCP?
i) What are the advantages of Indirect TCP?
j) What is the function of WTLS in WAP architecture?

PART – B

UNIT-I

2. a) Discuss about Spread Spectrum 5M
b) Explain about simplified reference model of Mobile Computing. 5M

3. a) Discuss various modulation techniques. 5M
b) Compare SDMA/TDMA/FDMA/CDMA. 5M

UNIT-II

4. a) Discuss about the functional architecture of GSM system. 5M
b) Explain various applications of Satellite Systems. 5M

5. a) Explain in detail about handover mechanism in GSM 5M
b) Discuss about Digital Audio Broadcasting. 5M

UNIT-III

6. a) Explain about IEEE 802.11 protocol architecture. 5M
b) Discuss about Mobile IP. 5M

7. a) Explain about Infrared vs Radio Transmission. 5M
b) Discuss about DHCP. 5M

UNIT-IV

8. a) Discuss about Snooping TCP. 5M
b) Discuss about Wireless Datagram Protocol. 5M

9. a) Discuss about Indirect TCP. 5M
b) Explain about WAP architecture. 5M

Scheme of Evaluation

PART - A

Answer All Questions **(1 X 10 = 10 Marks)**

1.

a) What is Frequency Division Multiplexing?

Ans) Frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency bands, each of which is used to carry a separate signal.

b) What is Hidden Terminal Problem?

Ans) The hidden terminal problem is a transmission problem (collision of data) that arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient.

c) What is the purpose of HLR in GSM?

Ans) The HLR is the most important database in a GSM system as it stores all user-relevant information such as MSISDN number, IMSI number, MSRN number, current LA of MS, current VLR and MSC.

d) Define Handover

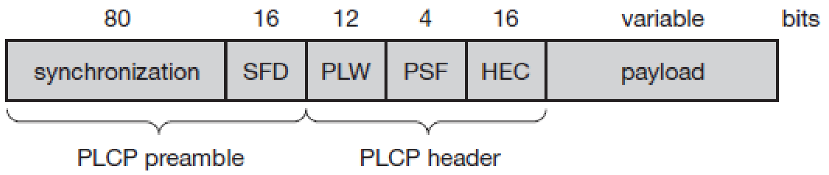
Ans) Handover is the process of transferring an outgoing call or data session from one cell to another cell to avoid call drop when mobile moves outside the range of a cell.

e) List the applications of Digital Video Broadcasting.

Ans) Digital Video Data Broadcasting, High Speed Internet Access, TV broadcasting

f) Draw the format of IEEE 802.11 PHY frame using FHSS.

Ans)



g) What are the requirements of Mobile IP?

Ans) Compatibility, Transparency, Scalability, Efficiency and Security

h) What is DHCP?

Ans) Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol).

i) What are the advantages of Indirect TCP?

Ans)

- ✓ I-TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network
- ✓ Only changes required in Wireless link part of TCP Connection

j) What is the function of WTLS in WAP architecture?

Ans) WTLS is a security transport protocol provided in WAP. WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks.

Part – B

2. a) Discuss about Spread Spectrum **5M**

Definition → 1M

Spread-spectrum techniques are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection.

Techniques → 4M

Two techniques for spreading narrowband signal:

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS): Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence (the chipping sequence consists of smaller pulses, called chips, with a duration tc). The spreading factor s = tb/tc determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs s·w after spreading. Wireless LANs complying with the standard IEEE 802.11 use, for example, the sequence 10110111000, a so-called Barker code, if implemented using DSSS.

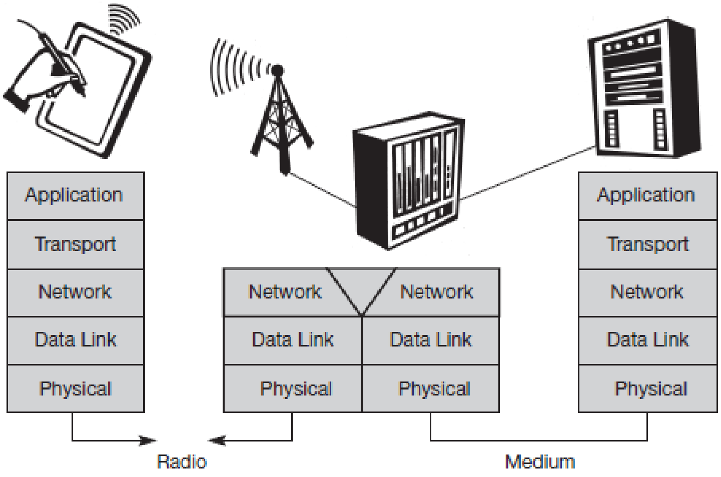
Frequency Hopping Spread Spectrum (FHSS) : In this the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels. Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. This system implements FDM and TDM. The pattern of channel usage is called the hopping sequence, the time spend on a channel with a certain frequency is called the dwell time. FHSS comes in two variants, slow and fast hopping.

In slow hopping, the transmitter uses one frequency for several bit periods. Performing slow hopping, the transmitter uses the frequency f2 for , the transmitter hops to the next frequency f3. Slow hopping systems are typically cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping systems.

In Fast hopping systems, the transmitter changes the frequency several times during the transmission of a single bit. Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances to perform hopping at more or less the same points in time. However, these systems are much better at overcoming the effects of narrowband interference and frequency selective fading as they only stick to one frequency for a very short time.

2. b) Explain about simplified reference model of Mobile Computing. **5M**

Diagram → 1M



Layers → 4M

The following explains the functions of each layer in more detail in a wireless and mobile environment.

Physical layer: This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that can be transmitted on the sender side. The physical layer of the receiver then transforms the signals back into a bit stream. For wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection, modulation of data onto a carrier frequency and encryption.

Data link layer: The main tasks of this layer include accessing the medium, multiplexing of different data streams, correction of transmission errors, and synchronization (i.e., detection of a data frame). Altogether, the data link layer is responsible for a reliable point-to-point connection between two devices or a point-to-multipoint connection between one sender and several receivers.

Network layer: This third layer is responsible for routing packets through a network or establishing a connection between two entities over many other intermediate systems. Important topics are addressing, routing, device location, and handover between different networks.

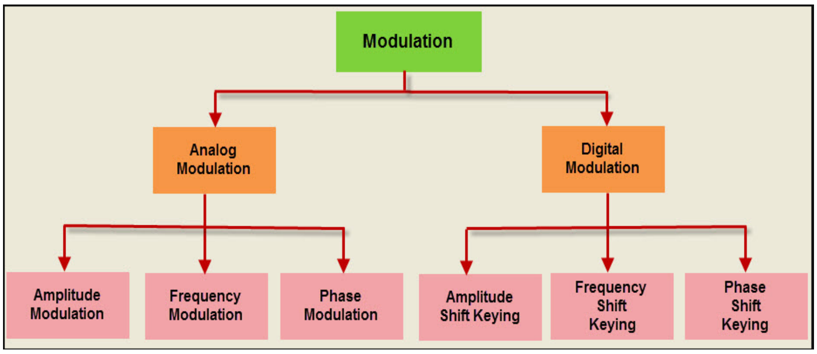
Transport layer: This layer is used in the reference model to establish an end-to-end connection. Topics like quality of service, flow and congestion control are relevant, especially if the transport protocols known from the Internet, TCP and UDP, are to be used over a wireless link.

Application layer: Finally, the applications are situated on top of all transmission oriented layers. Topics of interest in this context are service location, support for multimedia applications, adaptive applications that can handle the large variations in transmission characteristics, and wireless access to the world wide web using a portable device. Very demanding applications are video (high data rate) and interactive gaming (low jitter, low latency).

3. a) Discuss various Modulation Techniques **5M**

Diagram → 1M, Explanation → 4M

There are three aspects of a signal that can be modulated; amplitude, frequency, and phase**.** The amplitude is the power or intensity of the signal, the frequency is how often the signal repeated itself, and the phase describes where in the cycle the waveform is with respect to time. The following diagram shows different types of Modulation techniques.



AM (Amplitude Modulation): In amplitude modulation, the amplitude (signal strength) of the carrier wave is varied in proportion to that of the message signal being transmitted.

Used in AM radio, two way radios and citizens band radio, VHF aircraft radio.

FM (Frequency Modulation): Frequency modulation (FM) is used for everyday FM radio. The signals are imposed into the carrier by varying its frequency according to the career frequency.
Used in FM radio broadcasting, video broadcast systems, magnetic tape recording systems etc…

Phase modulation (PM): is a method of impressing data onto an alternating-current (AC) waveform by varying the instantaneous phase of the wave.
Used in Wifi, GSM, Satellite Television (digital transmissions)

Amplitude Shift Keying Modulation (ASK): ASK is a type of Amplitude Modulation which represents the binary data in the form of variations in the amplitude of a signal.

Any modulated signal has a high frequency carrier. The binary signal when ASK modulated, gives a zero value for Low input while it gives the carrier output for High input.
Used in Wireless Radio Transmission.

Frequency Shift Keying Modulation (FSK): FSK is the digital modulation technique in which the frequency of the carrier signal varies according to the digital signal changes. FSK is a scheme of frequency modulation.

Phase Shift Keying PSK: It is the digital modulation technique in which the phase of the carrier signal is changed by varying the sine and cosine inputs at a particular time. PSK technique is widely used for wireless LANs, bio-metric, contactless operations, along with RFID and Bluetooth communications.

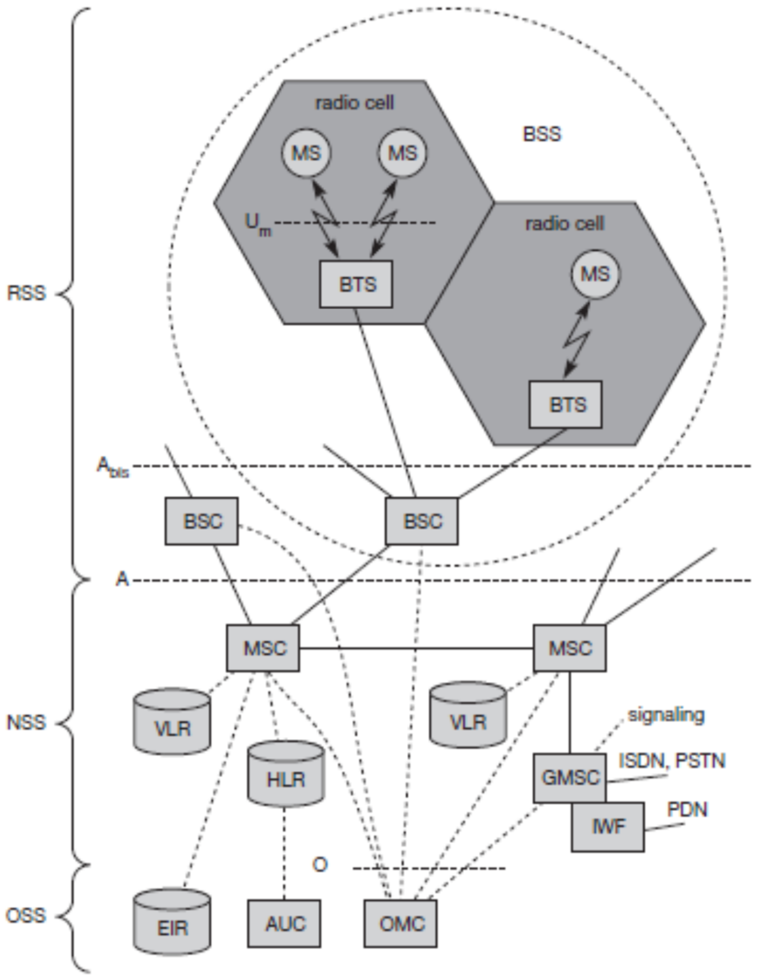
3. b) Compare SDMA/TDMA/FDMA/CDMA. 5M

Approach	**SDMA**	**TDMA**	**FDMA**	**CDMA**
Idea	Segment spaced into cells or sectors.	Segments sending time into disjoint time slots demand driven or fixed patterns.	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes.
Terminals	Only one terminal can be active in one cell or one sector.	All terminals are active for short periods of time on same frequency.	Every terminal has its own frequency uninterrupted	All terminals can be active at the same place at the same moment uninterrupted.
Signal Seperation	Cell structure, directed antennas	Synchronization in time domain	Filtering in the frequency domain.	Code plus special receivers.
Advantages	Very simple, increases capacity per sqr. Km.	Established fully digital, flexible	Simple, established, robust	Flexible, less frequency planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Guard space needed (multipath propagation), synchronization difficult	Inflexible, frequencies are scarce resource	Complex receivers, needs more complicated power control for senders

Approach	**SDMA**	**TDMA**	**FDMA**	**CDMA**
Comment	Only in combination with TDMA, FDMA or CDMA useful	Standards in fixed networks, together with FDMA or SDMA used in many mobile networks	Typically combined with TDMA and SDMA	Used in many 3G systems, higher complexity, lowered expectations; integrated with TDMA/FDMA
Transmission scheme	Continuous	Discontinuous	Continuous	Continuous
Cell capacity	Depends on cell area	Limited	Limited	No absolute limit on channel capacity but it is an interference limited system

4. a) Discuss about the functional architecture of GSM system **5M**

Diagram → 2M



Explanation → 3M

A GSM system consists of three subsystems,

1. Radio Sub System (RSS),
2. Network and Switching Subsystem (NSS),
3. Operation Sub System (OSS).

1. Radio subsystem

The **radio subsystem (RSS)** comprises all radio specific entities - i.e., the mobile stations (MS) and the base station subsystem (BSS).
Base station subsystem (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC).
Base transceiver station (BTS): A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission.

Base Station Controller (BSC): The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS.
Mobile Station (MS): The MS comprises all user equipment and software needed for communication with a GSM network.

2. Network and Switching Subsystem

The “heart” of the GSM system is formed by the Network and Switching Subsystem (NSS). The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries.

Mobile services Switching Center (MSC): MSCs are high-performance digital ISDN switches.
Home Location Register (HLR): The HLR is the most important database in a GSM system as it stores all user-relevant information.

Visitor Location Register (VLR): The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC.

3. Operation Sub System

The third part of a GSM system, the **Operation Sub System (OSS)**, contains the necessary functions for network operation and maintenance.

Operation and Maintenance Center (OMC): The OMC monitors and controls all other network entities via the O interface.

Authentication Centre (AuC): As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission.

Equipment Identity Register (EIR): The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network.

4. b) Explain various applications of Satellite Systems **5M**

Any 5 Applications → 5M

Weather forecasting: Several satellites deliver pictures of the earth using, e.g., infra red or visible light. Without the help of satellites, the forecasting of hurricanes would be impossible.

Radio and TV broadcast satellites: Hundreds of radio and TV programs are available via satellite. This technology competes with cable in many places, as it is cheaper to install and, in most cases, no extra fees have to be paid for this service. Today’s satellite dishes have diameters of 30–40 cm in central Europe, (the diameters in northern countries are slightly larger).

Military satellites: One of the earliest applications of satellites was their use for carrying out espionage. Many communication links are managed via satellite because they are much safer from attack by enemies.

Satellites for navigation: Even though it was only used for military purposes in the beginning, the global positioning system (GPS) is nowadays well-known and available for everyone. The system allows for precise localization worldwide, and with some additional techniques, the precision is in the range of some metres. Almost all ships and aircraft rely on GPS as an addition to traditional navigation systems. Many trucks and cars come with installed GPS receivers. This system is also used, e.g., for fleet management
of trucks or for vehicle localization in case of theft.

In the context of mobile communication, the capabilities of satellites to transmit data is of particular interest.

Global telephone backbones: One of the first applications of satellites for communication was the establishment of international telephone backbones. Instead of using cables it was sometimes faster to launch a new satellite (aka 'big cable in the sky').

Connections for remote or developing areas: Due to their geographical location many places all over the world do not have direct wired connection to the telephone network or the internet (e.g., researchers on Antarctica) or because of the current state of the infrastructure of a country. Satellites now offer a simple and quick connection to global networks.

Global mobile communication: The latest trend for satellites is the support of global mobile data communication. Due to the high latency, geostationary satellites are not ideal for this task; therefore, satellites using lower orbits are needed. The basic purpose of satellites for mobile communication is not to replace the existing mobile phone networks, but to extend the area of coverage. With the integration of satellite communication, however, the mobile phone can switch to satellites offering worldwide connectivity to a customer.

5. a) Explain in detail about handover mechanism in GSM 5M

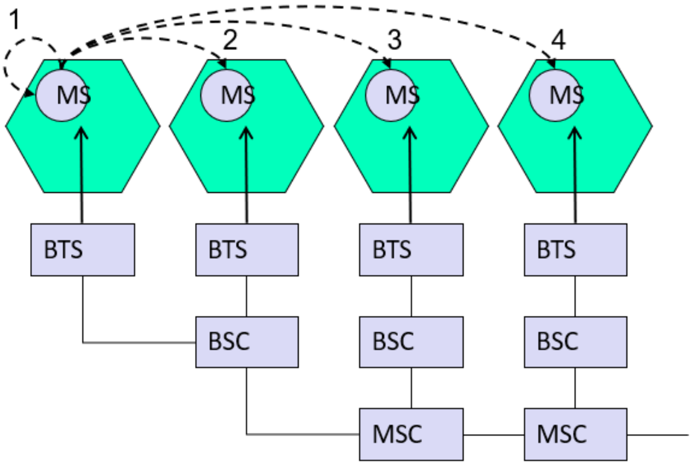
Diagram → 2M, Explanation → 3M

Cellular systems require handover procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities. The smaller the cell size and the faster the movement of a mobile station through the cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required. A handover should not cause a cut-off, also called call drop.
Reasons for handover are

1. When the mobile station moves out of the range of a BTS
2. Load Balancing

There are four types of handovers:

1. Intra-cell handover
2. Inter-cell, intra-BSC handover
3. Inter-BSC, intra-MSC handover
4. Inter MSC handover



The above diagram shows the types of handover in GSM.

The below diagram shows the typical signal flow during an inter-BSC, intra-MSC handover. The MS sends its periodic measurements reports, the BTSold forwards these reports to the BSCold together with its own measurements. Based on these values and, e.g., on current traffic conditions, the BSCold may decide to perform a handover and sends the message HO_required to the MSC. The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSCnew. This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTSnew to prepare for the arrival of the MS.

5.b) Discuss about Digital Audio Broadcasting. **5M**

DAB → 3M

DAB (Digital Audio Broadcasting)

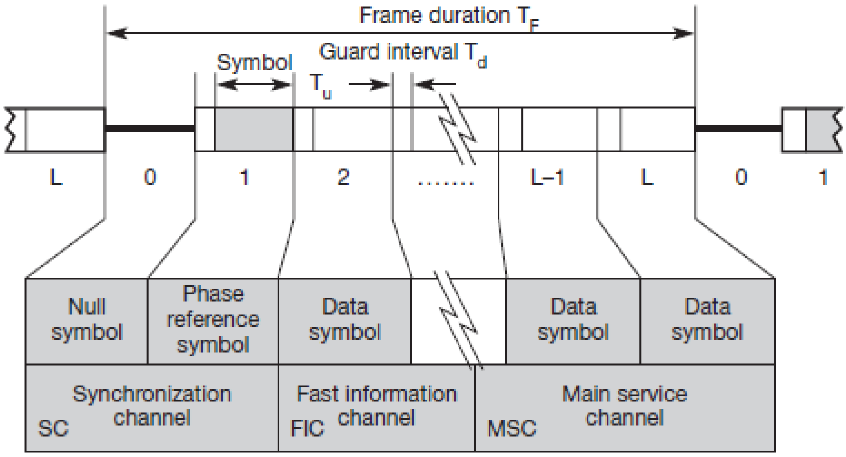
DAB systems can use **single frequency networks (SFN)**, i.e., all senders transmitting the same radio program operate at the same frequency. Using an SFN is very frequency efficient, as a single radio station only needs one frequency throughout the whole country. DAB transmission power per antenna is orders of magnitude lower compared to traditional FM stations. DAB uses VHF and UHF frequency bands.
The modulation scheme used is **DQPSK**.
DAB uses FEC to reduce the error rate and introduces **guard spaces** between single symbols during transmission.

DAB uses two basic transport mechanisms:
Main service channel (MSC): The MSC carries all user data, e.g. audio, multimedia data.
Fast information channel (FIC): The FIC contains **fast information blocks (FIB)** with 256 bits each (16 bit checksum).

Two transport modes have been defined for the MSC.
The **stream mode** offers a transparent data transmission from the source to the destination with a fixed bit rate in a sub channel.
The **packet mode** transfers data in addressable blocks (packets). These blocks are used to convey MSC data within a sub channel.
DAB defines many service information structures accompanying an audio stream.

Frame Structure & Explanation → 2M

The general frame structure of DAB



Each frame consists of three parts. The **synchronization channel (SC)** marks the start of a frame. It consists of a null symbol and a phase reference symbol to synchronize the receiver. The **fast information channel (FIC)** follows, containing control data in the FIBs. Finally, the **main service channel (MSC)** carries audio and data service components.

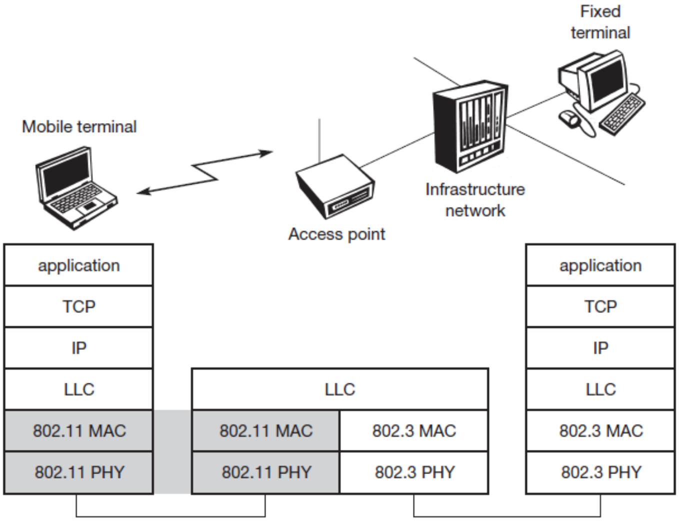
6. a) Explain about IEEE 802.11 protocol architecture. 5M

Diagram → 1M

Explanation → 4M

The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes. The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media. In many of today's networks, no explicit LLC layer is visible.

Figure 7.5
IEEE 802.11 protocol architecture and bridging



The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do. The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer PMD. The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption. The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sublayer handles modulation and encoding/decoding of signals.

Apart from the protocol sublayers, the standard specifies management layers and the station management. The MAC management supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power. MAC management also maintains the MAC management information base (MIB).

The main tasks of the PHY management include channel tuning and PHY MIB maintenance. Finally, station management interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

6. b) Discuss about Mobile IP. **5M**

Diagram → 1M

Explanation → 4M

The following diagram shows several entities and terms needed to understand mobile IP as defined in RFC 3344.

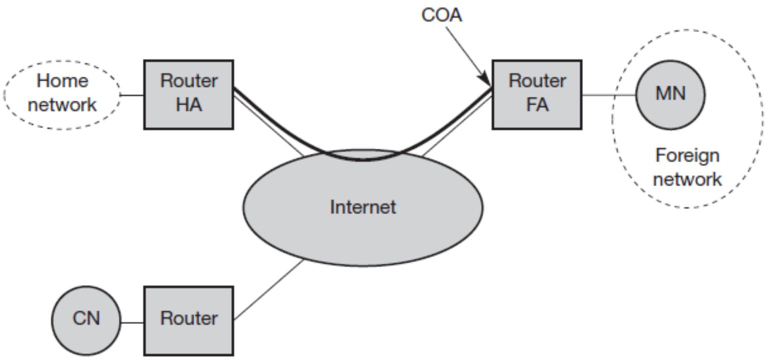


Figure 8.1
Mobile IP example network

Mobile node (MN): A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP. The MN keeps its IP address and can continuously communicate with any other system in the internet as long as link-layer connectivity is given. Mobile nodes are not necessarily small devices such as laptops with antennas or mobile phones; a router onboard an aircraft can be a powerful mobile node.

Correspondent node (CN): At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Home network: The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network.

Foreign network: The foreign network is the current subnet the MN visits and which is not the home network.

Foreign agent (FA): The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA (defined below), acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

Care-of address (COA): The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN

Home agent (HA): The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN’s location by the current COA.

he mobile IP process has following **three main phases**, which are:

1. **Agent Discovery** → During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).
2. **Registration** → The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.
3. **Tunneling** → A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.

7. a) Explain about Infrared vs Radio Transmission. 5M

Two different basic transmission technologies can be used to set up WLANs. One technology is based on the transmission of infra red light (e.g., at 900 nm wavelength), the other one, which is much more popular, uses **radio transmission** in the GHz range (e.g., 2.4 GHz in the license-free ISM band). Both technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desktop with a printer without a wire, or to support mobility within a small area. Almost all networks described in this book use **radio** waves for data transmission, e.g., GSM at 900, 1,800, and 1,900 MHz, DECT at 1,880 MHz etc.

Advantages of radio transmission include the long-term experiences made with radio transmission for wide area networks (e.g., microwave links) and mobile cellular phones. Again, the main advantage is also a big **disadvantage** of radio transmission. Shielding is not so simple.

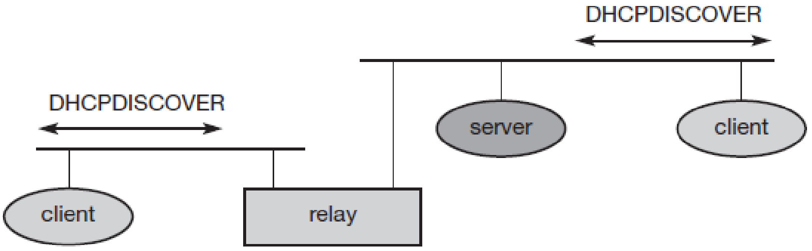
Infra red technology uses diffuse light reflected at walls, furniture etc. or directed light if a line-of-sight (LOS) exists between sender and receiver. Senders can be simple light emitting diodes (LEDs) or laser diodes. Photodiodes act as receivers.

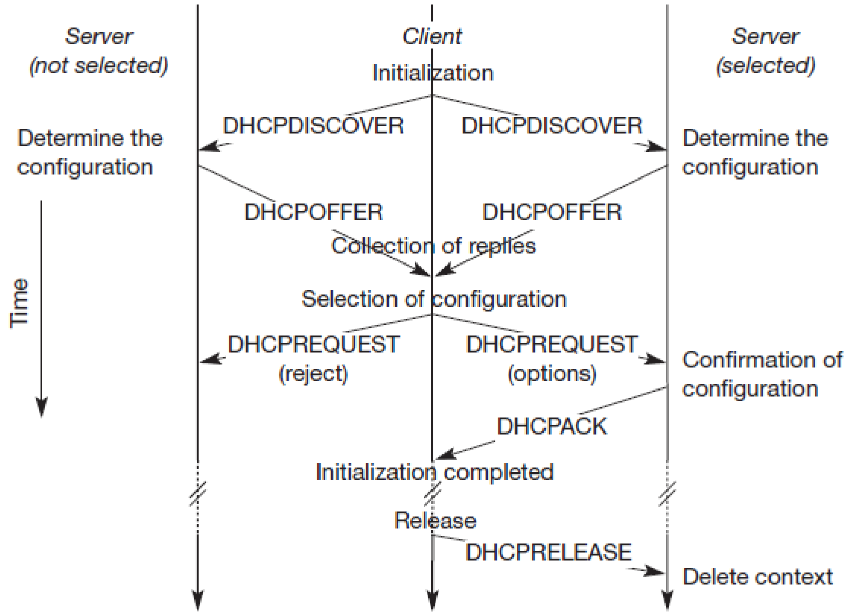
The main **advantages** of infra red technology are its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
Disadvantages of infra red transmission are its low bandwidth compared to other LAN technologies.

7. b) Discuss about DHCP. 5M

The dynamic host configuration protocol is mainly used to simplify the installation and maintenance of networked computers. If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the domain name, and an IP address. Providing an IP address, makes DHCP very attractive for mobile IP as a source of care-of-addresses.

DHCP is based on a client/server model. DHCP clients send a request to a server (DHCPDISCOVER in the example) to which the server responds. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.





8. a) Discuss about Snooping TCP. **5M**

Diagram → 1M
Explanation → 4M

One of the drawbacks of I-TCP is the segmentation of the single TCP connection into two TCP connections. This loses the original end-to-end TCP semantic. The following TCP enhancement works completely transparently and leaves the TCP end-to-end connection intact. The main function of the enhancement is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss. A good place for the enhancement of TCP could be the foreign agent in the Mobile IP context.

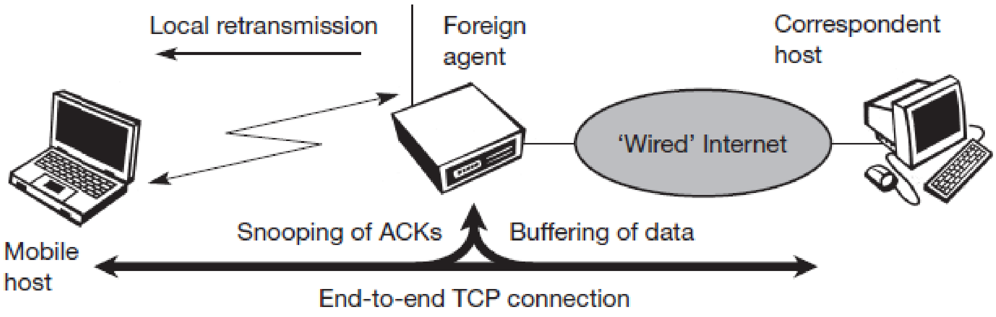


Figure 9.3
Snooping TCP as a transparent TCP extension

In this approach, the foreign agent buffers all packets with destination mobile host and additionally 'snoops' the packet flow in both directions to recognize acknowledgements. The reason for buffering packets toward the mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link.

The foreign agent buffers every packet until it receives an acknowledgement from the mobile host. If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost. Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet. Now the foreign agent retransmits the packet directly from the buffer, performing a much faster retransmission compared to the correspondent host. The time out for acknowledgements can be much shorter, because it reflects only the delay of one hop plus processing time.

To remain transparent, the foreign agent must not acknowledge data to the correspondent host. This would make the correspondent host believe that the mobile host had received the data and would violate the end-to-end semantic in case of a foreign agent failure. However, the foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host. If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission. The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link.

Data transfer from the mobile host with destination correspondent host works as follows. The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP. As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.

8. b) Discuss about Wireless Datagram Protocol. 5M

The **wireless datagram protocol (WDP)** operates on top of many different bearer services capable of carrying data. At the T-SAP WDP offers a consistent datagram transport service independent of the underlying bearer. To offer this consistent service, the adaptation needed in the transport layer can differ depending on the services of the bearer. The closer the bearer service is to IP, the smaller the adaptation can be. If the bearer already offers IP services, UDP is used as WDP. WDP offers more or less the same services as UDP.

WDP offers **source** and **destination port numbers** used for multiplexing and demultiplexing of data respectively. The service primitive to send a datagram is **TDUnitdata.req** with the **destination address (DA), destination port (DP), Source address (SA), source port (SP)**, and **user data (UD)** as mandatory parameters. Destination and source address are unique addresses for the receiver and sender of the user data. These could be MSISDNs (i.e., a telephone number), IP addresses, or any other unique identifiers. The **T-DUnitdata.ind** service primitive indicates the reception of data. Here destination address and port are only optional parameters.

If a higher layer requests a service the WDP cannot fulfill, this error is Indicated with the **T-DError.ind** service primitive. An **error code (EC)** is returned indicating the reason for the error to the higher layer. WDP is not allowed to use this primitive to indicate problems with the bearer service. It is only allowed to use the primitive to indicate local problems, such as a user data size that is too large.

If any errors happen when WDP datagrams are sent from one WDP entity to another, the **wireless control message protocol (WCMP)** provides error handling mechanisms for WDP and should therefore be implemented. WCMP contains control messages that resemble the internet control message protocol (ICMP for IPv4, for IPv6) messages and can also be used for diagnostic and informational purposes. WCMP can be used by WDP nodes and gateways to report errors. However, WCMP error messages must not be sent as response to other WCMP error messages. In IP-based networks, ICMP will be used as WCMP (e.g., CDPD, GPRS). Typical WCMP messages are **destination unreachable** (route, port, address unreachable), **parameter problem** (errors in the packet header), **message too big, reassembly failure**, or **echo request/reply**.

An additional **WDP management entity** supports WDP and provides information about changes in the environment, which may influence the correct operation of WDP. Important information is the current configuration of the device, currently available bearer services, processing and memory resources etc. Design and implementation of this management component is considered vendor-specific and is outside the scope of WAP.

If the bearer already offers IP transmission, WDP (i.e., UDP in this case) relies on the segmentation (called fragmentation in the IP context) and reassembly capabilities of the IP layer. Otherwise, WDP has to include these capabilities, which is, e.g., necessary for the GSM SMS. The WAP specification provides many more adaptations to almost all bearer services currently available or planned for the future.

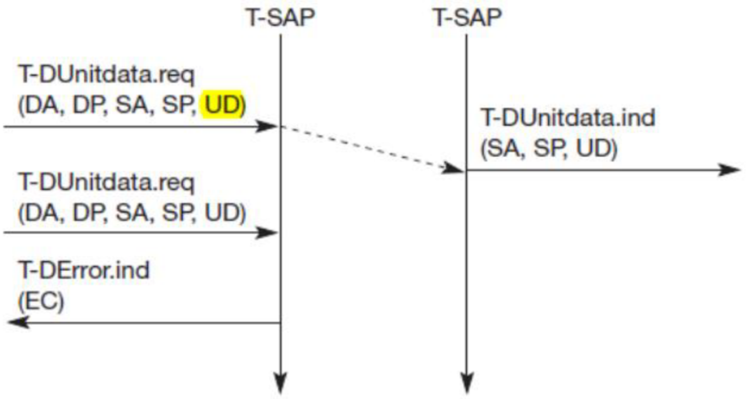


Figure 10.11
WDP service primitives

9 a) Discuss about Indirect TCP. **5M**

Diagram → 1M
Explanation → 4M

Two competing insights led to the development of indirect TCP (I-TCP). One is that TCP performs poorly together with wireless links; the other is that TCP within the fixed network cannot be changed. I-TCP segments a TCP connection into a fixed part and a wireless part. The correspondent node could also use wireless access. The following would then also be applied to the access link of the correspondent host.

Standard TCP is used between the fixed computer and the access point. No computer in the internet recognizes any changes to TCP. Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. This means that the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host. Between the access point and the mobile host, a special TCP, adapted to wireless links, is used. However, changing TCP for the wireless link is not a requirement. Even an unchanged TCP can benefit from the much shorter round trip time, starting retransmission much faster.

A good place for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP. The foreign agent controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on. However, one can also imagine separating the TCP connections at a special server, e.g., at the entry point to a mobile phone network.

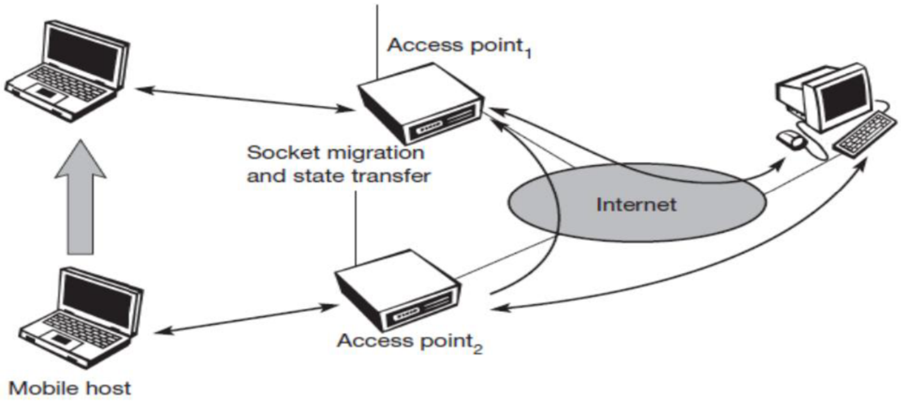
The correspondent host in the fixed network does not notice the wireless link or the segmentation of the connection. The foreign agent acts as a proxy and relays all data in both directions. If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host. If the mobile host receives the packet, it acknowledges the packet.

However, this acknowledgement is only used by the foreign agent. If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this. In this case, the foreign agent tries to retransmit this packet locally to maintain reliable data transport.

Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host. If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet. Packet loss in the wired network is now handled by the foreign agent.

QI-TCP requires several actions as soon as a handover takes place. Not only the packets have to be redirected using, e.g., mobile IP. In the example shown, the access point acts as a proxy buffering packets for retransmission. After the handover, the old proxy must forward buffered data to the new proxy because it has already acknowledged the data. After registration with the new foreign agent, this new foreign agent can inform the old one about its location to enable packet forwarding. Besides buffer content, the sockets of the proxy, too, must migrate to the new foreign agent located in the access point. The socket reflects the current state of the TCP connection, i.e., sequence number, addresses, ports etc. No new connection may be established for the mobile host, and the correspondent host must not see any changes in connection state. Correspondent host must not see any changes in connection state.

Figure 9.2
Socket and state migration after handover of a mobile host



9. b) Explain about WAP architecture. **5M**

The below diagram gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the world wide web.

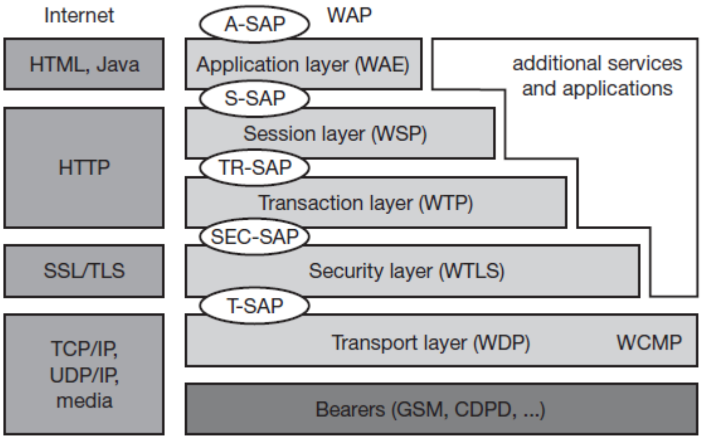


Diagram → 1M
Explanation → 4M

The basis for transmission of data is formed by different bearer services. WAP does not specify bearer services, but uses existing data services and will integrate further services.

Examples are:

- ✓ Message services, such as short message service (SMS) of GSM,
- ✓ Circuit-switched data, such as high-speed circuit switched data (HSCSD) in GSM
- ✓ or packet switched data, such as general packet radio service (GPRS) in GSM.

Many other bearers are supported, such as CDPD, IS-136, PHS.

No special interface has been specified between the bearer service and the next higher layer, the transport layer with its wireless datagram protocol (WDP) and the additional wireless control message protocol (WCMP), because the adaptation of these protocols are bearer-specific.

The transport layer offers a bearer independent, consistent datagram-oriented service to the higher layers of the WAP architecture. Communication is done transparently over one of the available bearer services. The transport layer service access point (T-SAP) is the common interface to be used by higher layers independent of the underlying network.

WTLS (Wireless Transport Layer Security):

The security layer with its wireless transport layer security protocol WTLS offers its service at the security SAP (SEC-SAP). WTLS is based on the transport layer security (TLS, formerly SSL, secure sockets layer) already known from the www. WTLS has been optimized for use in wireless networks with narrow-band channels. It can offer data integrity, privacy, authentication, and (some) denial-of-service protection.

WTP (Wireless Transaction Protocol):

The WAP transaction layer with its wireless transaction protocol (WTP) offers a lightweight transaction service at the transaction SAP (TR-SAP). This service efficiently provides reliable or unreliable requests and asynchronous transactions.

WSP (Wireless Session Protocol):

The session layer with the wireless session protocol (WSP) currently offers two services at the session-SAP (S-SAP), one connection-oriented and one connectionless if used directly on top of WDP. A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

WAE (Wireless Application Environment):

The application layer with the wireless application environment: (WAE) offers a framework for the integration of different www and mobile telephony applications. It offers many protocols and services with special service access points.

Signature of the Internal Examiner	**Signature of the HOD**	**Signature of the External Examiner**