EC6802 WIRELESS NETWORKS

2 MARKS QUESTIONS & ANSWERS

UNIT I WIRELESS LAN

1. **What are advantages of WLANs?**

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc.
- **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break
- **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost.

2. What are the disadvantages of WLANs?

Quality of service: WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms.

- **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols).
- **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference.
- **Safety and security:** Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. Special precautions have to be taken to prevent safety hazards.

3. What are the commercial successes of WLAN?

Global operation: WLAN products should sell in all countries so, national and international frequency regulations have to be considered. In contrast to the infrastructure of wireless WANs, LAN equipment may be carried from one country into another – the operation should still be legal in this case.

- **Low power:** Devices communicating via a WLAN are typically also wireless devices running on battery power. The LAN design should take this into account and implement special power-saving modes and power management functions.

● **License-free operation:** LAN operators do not want to apply for a special license to be able to use the product. The equipment must operate in a license-free band, such as the 2.4 GHz ISM band.
● **Robust transmission technology:** Compared to their wired counterparts, WLANs operate under difficult conditions. If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.).
● **Simplified spontaneous cooperation:** To be useful in practice, WLANs should not require complicated setup routines but should operate spontaneously after power-up. These LANs would not be useful for supporting, e.g., ad-hoc meetings.
● **Easy to use:** In contrast to huge and complex wireless WANs, wireless LANs are made for simple use. They should not require complex management, but rather work on a plug-and-play basis.
● **Protection of investment:** A lot of money has already been invested into wired LANs. The new WLANs should protect this investment by being interoperable with the existing networks.
● **Safety and security:** Wireless LANs should be safe to operate, especially regarding low radiation if used, e.g., in hospitals. Users cannot keep safety distances to antennas. The equipment has to be safe for pacemakers, too.

4. What are the 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.

5. What are the advantages of infra red technology?
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.
PDAs, laptops, notebooks, mobile phones etc. have an infra red data association (IrDA) interface.
Version 1.0 of this industry standard implements data rates of up to 115 kbit/s, while IrDA 1.1 defines higher data rates of 1.152 and 4 Mbit/s.
No licenses are needed for infra red technology and shielding is very simple. Electrical devices do not interfere with infra red transmission.

6. State **Disadvantages** of infra red transmission?
Disadvantages of infra red transmission are its low bandwidth compared to other LAN technologies. Typically, IrDA devices are internally connected to a serial port limiting transfer rates to 115 kbit/s. Even 4 Mbit/s is not a particularly high data rate. However, their main disadvantage is that infra red is quite easily shielded. Infra red transmission cannot penetrate walls or other obstacles. Typically, for good transmission quality and high data rates a LOS, i.e., direct connection, is needed.

7. What are IEEE standard 802.11?

The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available. As the standard's number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. This means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to higher layers to maintain interoperability.

8. What are the types of system architectures of IEEE 802.11?

Wireless networks can exhibit two different basic system architectures:

1. Infrastructure-based &
2. Ad-hoc.

The components of an infrastructure are:

- Stations (STAi)
- Access points (AP).
- Basic service set (BSSi).
- Distribution system.
- Extended service set (ESS)

9. What is the architecture of Ad –Hoc system architecture?

In ad-hoc networks between stations, It forms one or more independent BSSs (IBSS). In this case, an IBSS comprises a group of stations using the same radio frequency. Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies (then the IBSSs could overlap physically).

10. What is division of IEEE 802.11 standard?

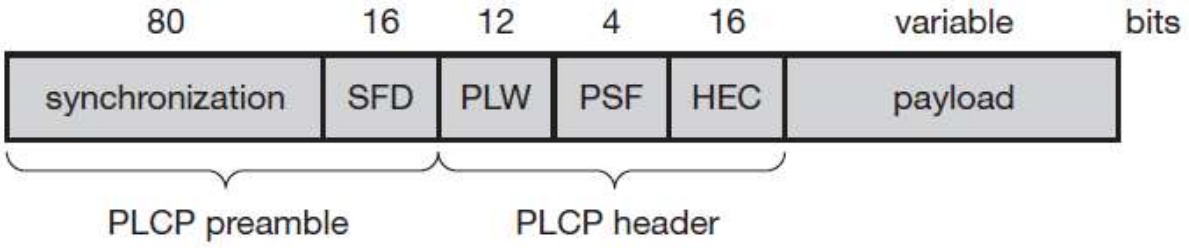
The IEEE 802.11 standard only covers the physical layer **PHY** and medium access layer **MAC** like the other 802.x LANs do. The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent** sublayer **PMD.**

11. What are the types of physical layers of IEEE 802.11?

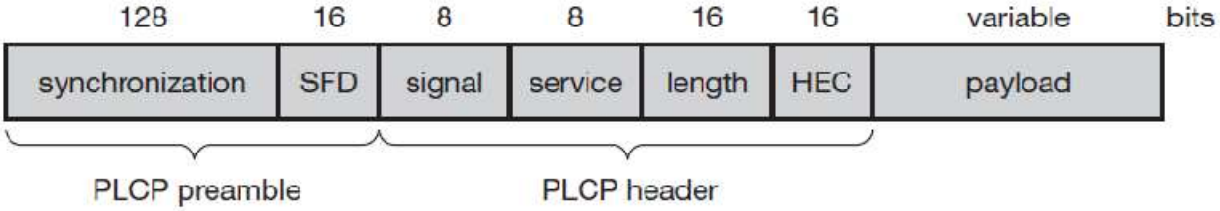
IEEE 802.11 supports three different physical layers: one layer based on infra red and two layers based on radio transmission (primarily in the ISM band at 2.4 GHz, which is available worldwide). All PHY variants include the provision of the **clear channel assessment** signal **(CCA)**. This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.

12. Draw the Format of an IEEE 802.11 PHY frame using FHSS & DSSS.

IEEE 802.11 PHY frame using FHSS



IEEE 802.11 PHY frame using DHSS



13. Write the three basic access mechanisms have been defined for IEEE 802.11?

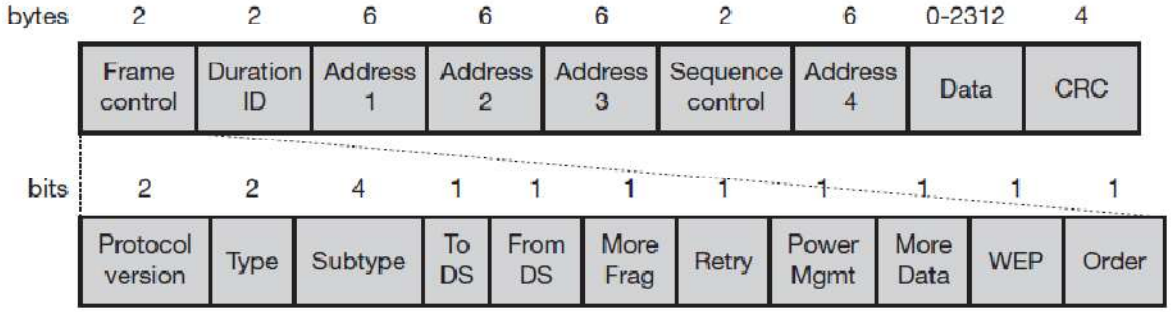
The first two methods are also summarized as **distributed coordination function (DCF)**, the third method is called **point coordination function (PCF**). DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention. The MAC mechanisms are also called **distributed foundation wireless medium access control (DFWMAC)**.

14. What are SIFS, PIFS & DIFS?

Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is 10 μs and for FHSS it is 28 μs.

- **PCF inter-frame spacing (PIFS):** A waiting time between DIFS and SIFS (and thus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium access. PIFS is defined as SIFS plus one slot time.
- **DCF inter-frame spacing (DIFS):** This parameter denotes the longest waiting time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period. DIFS is defined as SIFS plus two slot times.

15. Draw the format of IEEE 802.11 MAC packet structure.



16. What are the four scenarios in addressing of IEEE 802.11?

- **Ad-hoc network:** If both DS bits are zero, the MAC frame constitutes a packet which is exchanged between two wireless nodes without a distribution system. **DA** indicates the **destination address**, **SA** the **source address** of the frame, which are identical to the physical receiver and sender addresses respectively. The third address identifies the **basic service set (BSSID)**

● **Infrastructure network, from AP:** If only the 'from DS' bit is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second address identifies the BSS, the third address specifies the logical sender, the source address of the MAC frame. This case is an example for a packet sent to the receiver via the access point.

● **Infrastructure network, to AP:** If a station sends a packet to another station via the access point, only the 'to DS' bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.

● **Infrastructure network, within DS:** For packets transmitted between two access points over the distribution system, both bits are set. The first **receiver address (RA)**, represents the MAC address of the receiving access point. Similarly, the second address **transmitter address (TA)**, identifies the sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of the frame and the original source of the frame SA. Without these additional addresses, some encapsulation mechanism would be necessary to transmit MAC frames over the distribution system transparently.

17. What is roaming?

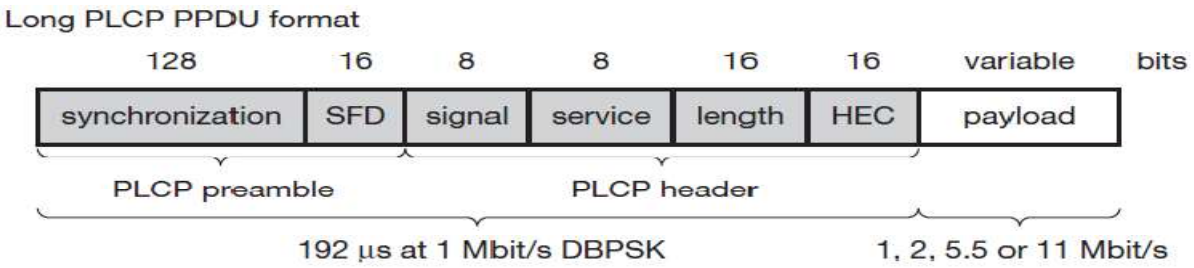
Wireless networks within buildings require more than just one access point to cover all rooms. Depending on the solidity and material of the walls, one access point has a transmission range of 10–20 m if transmission is to be of decent quality. Each storey of a building needs its own access point(s) as quite often walls are thinner than floors. If a user walks around with a wireless station, the station has to move from one access point to another to provide uninterrupted service. Moving between access points is called **roaming**.

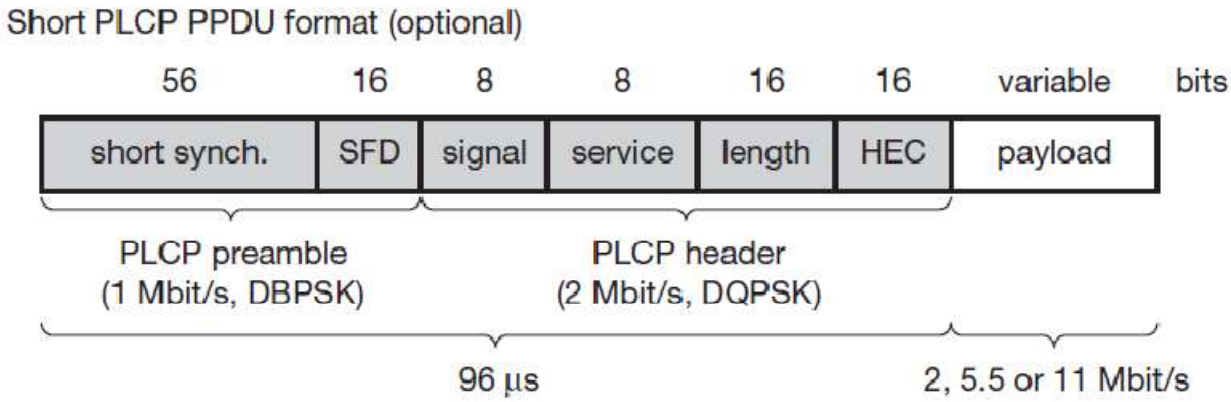
18. What is IEEE 802.11b?

This standard describes a new PHY layer and is by far the most successful version of IEEE 802.11 available today. Depending on the current interference and the distance between sender and receiver 802.11b systems offer 11, 5.5, 2, or 1 Mbit/s. Maximum user data rate is approx 6 Mbit/s. The lower data rates 1 and 2 Mbit/s use the 11-chip Barker sequence.

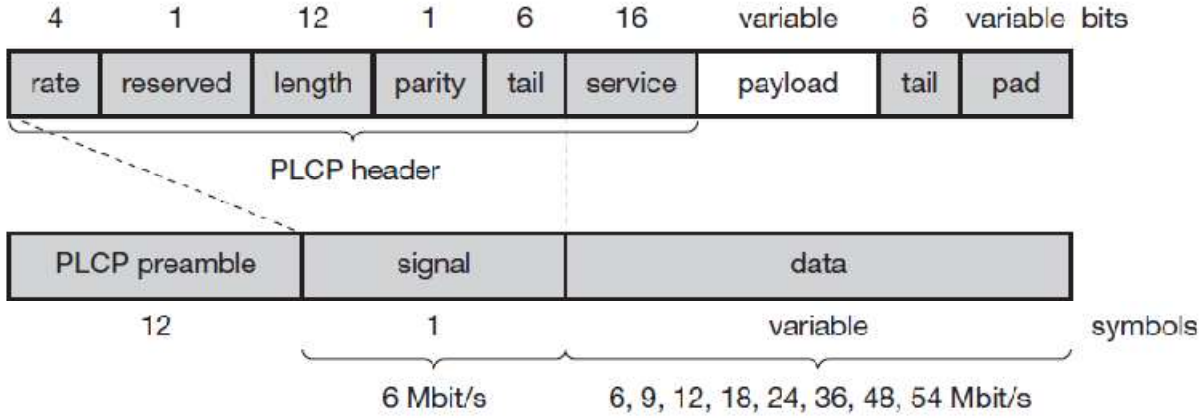
19. What are the two packet formats standardized for 802.11b?

1. Mandatory format is called **long PLCP PPDU**
2. Optional **short PLCP PPDU**





20. Draw the IEEE 802.11a physical layer PDU.



21. What is HIPERLAN?

HIPERLAN stands for **high performance local area network**.) **HIPERLAN 1** was originally one out of four HIPERLANs envisaged, as ETSI decided to have different types of networks for different purposes. The key feature of all four networks is their integration of time-sensitive data transfer services. The current focus is on HiperLAN2, a standard that comprises many elements from ETSI's **BRAN** (broadband radio access networks) and **wireless ATM** activities.

22. What is WATM?

Wireless ATM (WATM; sometimes also called wireless, mobile ATM, wmATM) does not only describe a transmission technology but tries to specify a complete communication system. While many aspects of the IEEE WLANs originate from the data communication community, many WATM aspects come from the telecommunication industry (Händel, 1994). This specific situation can be compared to the case of competition and merging with regard to the concepts TCP/IP and ATM (IP-switching, MPLS). Similar to fixed networks where ATM never made it to the desktop, WATM will not make it to mobile terminals. However, many concepts found in WATM can also be found in QoS supporting WLANs such as HiperLAN2.

23. What are three different parts of MQoS?

Wired QoS: The infrastructure network needed for WATM has the same QoS properties as any wired ATM network. Typical traditional QoS parameters are link delay, cell delay variation, bandwidth, cell error rate etc.

● **Wireless QoS:** The QoS properties of the wireless part of a WATM network differ from those of the wired part. Again, link delay and error rate can be specified, but now error rate is typically some order of magnitude that is higher than, e.g., fiber optics. Channel reservation and multiplexing mechanisms at the air interface strongly influence cell delay variation.
● **Handover QoS:** A new set of QoS parameters are introduced by handover. For example, handover blocking due to limited resources at target access points, cell loss during handover, or the speed of the whole handover procedure represent critical factors for QoS.

24. Four different network types of BRAN?
- **HIPERLAN 1:** This high-speed WLAN supports mobility at data rates above 20 Mbit/s. Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure.

● **HIPERLAN/2:** This technology can be used for wireless access to ATM or IP networks and supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration. Transmission range is 50 m with support of slow (< 10 m/s) mobility (ETSI, 1997). This standard has been modified over time and is presented in section 7.4.4 as a high performance WLAN with QoS support.
● **HIPERACCESS:** This technology could be used to cover the 'last mile' to a customer via a fixed radio link, so could be an alternative to cable modems or xDSL technologies (ETSI, 1998c). Transmission range is up to 5 km, data rates of up to 25 Mbit/s are supported. However, many proprietary products already offer 155 Mbit/s and more, plus QoS.
● **HIPERLINK:** To connect different HIPERLAN access points or HIPERACCESS nodes with a high-speed link, HIPERLINK technology can be chosen. HIPERLINK provides a fixed point-to-point connection with up to 155 Mbit/s. Currently, there are no plans regarding this standard.

UNIT II MOBILE NETWORK LAYER

1.What are the requirements for mobile IP as a standard?

Compatibility: The installed base of Internet computers, i.e., computers running TCP/IP and connected to the internet, is huge. A new standard cannot introduce changes for applications or network protocols already in use.

Transparency: Mobility should remain 'invisible' for many higher layer protocols and applications.

Scalability and efficiency: Introducing a new mechanism to the internet must not jeopardize its efficiency. Enhancing IP for mobility must not generate too many new messages flooding the whole network.

Security: Mobility poses many security problems. The minmum requirement is that of all the messages related to the management of Mobile IP are authenticated.

2. What is tunneling?

A **tunnel** establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel, is achieved by using encapsulation.

3. What is Encapsulation & decapsulation?

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation**. Encapsulation and decapsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively. Here these functions are used within the same layer.

4. What are Generic routing encapsulation?

While IP-in-IP encapsulation and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP. **Generic routing encapsulation** (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

5. What is the important of recursion control field in IP-in-IP?

The **recursion control** field (rec.) is an important field that additionally distinguishes GRE from IP-in-IP and minimal encapsulation. This field represents a counter that shows the number of allowed recursive encapsulations. As soon as a packet arrives at an encapsulator it checks whether this field equals zero. If the field is not zero, additional encapsulation is allowed – the packet is encapsulated and the field decremented by one. Otherwise the packet will most likely be discarded. This mechanism prevents indefinite recursive encapsulation which might happen with the other schemes if tunnels are set up improperly.

6. What is triangular routing?

If the Japanese sends a packet to the German, his computer sends the data to the HA of the German, i.e., from Hawaii to Germany. The HA in Germany now encapsulates the packets and tunnels them to the COA of the German laptop on Hawaii. This means that although the computers might be only meters away, the packets have to travel around the world! This

inefficient behavior of a nonoptimized mobile IP is called **triangular routing**. The triangle is made of the three segments, CN to HA, HA to COA/MN, and MN back to CN.

7. What is the need for NAT?

Network address translation (NAT) is used by many companies to hide internal resources (routers, computers, printers etc.) and to use only some globally available addresses, tries to solve the problems arising when using NAT together with mobile IP).

8. What are the Advantage & disadvantage of Cellular IP?

Advantage

● Manageability: Cellular IP is mostly self-configuring, and integration of the CIPGW into a firewall would facilitate administration of mobility-related functionality. This is, however, not explicitly specified in.

Disadvantages

● Efficiency: Additional network load is induced by forwarding packets on multiple paths.
● Transparency: Changes to MNs are required.
● Security: Routing tables are changed based on messages sent by mobile nodes. Additionally, all systems in the network can easily obtain a copy of all packets destined for an MN by sending packets with the MN's source address to the CIPGW.

9. What is Hawaii?

HAWAII (Handoff-Aware Wireless Access Internet Infrastructure, tries to keep micro-mobility support as transparent as possible for both home agents and mobile nodes (which have to support route optimization). Its concrete goals are performance and reliability improvements and support for quality of service mechanisms.

10. What are the Advantage & disadvantage of HAWAII?

Advantages

● Security: Challenge-response extensions are mandatory. In contrast to Cellular IP, routing changes are always initiated by the foreign domain's infrastructure.
● Transparency: HAWAII is mostly transparent to mobile nodes.

Disadvantages

● Security: There are no provisions regarding the setup of IPSec tunnels.
● Implementation: No private address support is possible because of collocated COAs.

11. What is HMIPv6?

Hierarchical mobile IPv6 (HMIPv6) provides micro-mobility support by installing a **mobility anchor point (MAP)**, which is responsible for a certain domain and acts as a local HA within this domain for visiting MNs.

12. What are the Advantage & disadvantage of HMIPv6?

Advantages

● Security: MNs can have (limited) location privacy because LCOAs can be hidden.
● Efficiency: Direct routing between CNs sharing the same link is possible

Disadvantages

● Transparency: Additional infrastructure component (MAP).

● Security: Routing tables are changed based on messages sent by mobile nodes. This requires strong authentication and protection against denial of service attacks. Additional security functions might be necessary in MAPs.

13. What is the need for DHCP?

The dynamic host configuration protocol (DHCP) is mainly used to simplifiy 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.

14. Write the benefits of ad-hoc networks.

Instant infrastructure: Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure. Infrastructures need planning and administration.

● **Disaster relief:** Infrastructures typically break down in disaster areas. Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers. Emergency teams can only rely on an infrastructure they can set up themselves. No forward planning can be done, and the set-up must be extremely fast and reliable. The same applies to many military activities, which is, to be honest, one of the major driving forces behind mobile ad-hoc networking research.

● **Remote areas:** Even if infrastructures could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas.

● **Effectiveness:** Services provided by existing infrastructures might be too expensive for certain applications.

15. List the fundamental differences between wired networks and ad-hoc wireless networks?

Asymmetric links: Routing information collected for one direction is of almost no use for the other direction. However, many routing algorithms for wired networks rely on a symmetric scenario.

● **Redundant links:** Wired networks, too, have redundant links to survive link failures. In ad-hoc networks nobody controls redundancy, so there might be many redundant links up to the extreme of a completely meshed topology. Routing algorithms for wired networks can handle some redundancy, but a high redundancy can cause a large computational overhead for routing table updates.

● **Interference:** In wired networks links exist only where a wire exists, and connections are planned by network administrators. This is not the case for wireless ad-hoc networks. Links come and go depending on transmission characteristics, one transmission might interfere with another, and nodes might overhear the transmissions of other nodes. Interference creates new problems by 'unplanned' links between nodes: if two close-by nodes forward two transmissions, they might interfere and destroy each other. On the other hand, interference might also help routing. A node can learn the topology with the help of packets it has overheard.

● **Dynamic topology:** The greatest problem for routing arises from the highly dynamic topology. In adhoc networks, routing tables must somehow reflect these frequent changes in topology, and routing algorithms have to be adapted. Routing algorithms used in wired networks would either react much too slowly or generate too many updates to reflect all changes in topology.

16. Define DSDV.

Destination sequence distance vector (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks. DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols currently discussed. Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to the count-to-infinity problem.

17. What are the two things add in DSDV compared to distance vector algorithm?

- **Sequence numbers:** Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.
- **Damping:** Transient changes in topology that are of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the topology currently stored are therefore not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.

18. Write the concept of DSR.

Dynamic source routing (DSR), therefore, divides the task of routing into two separate problems:

- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.

19. What are the different types of routing algorithms in Ad-Hoc network?

Routing algorithm are divided into three categories: flat routing, hierarchical routing, and geographic-position-assisted routing.

20. What are the Advantage & disadvantage of proactive protocols?

A general **advantage** of proactive protocols is that they can give QoS guarantees related to connection set-up, latency or other real time requirements. As long as the topology does not change too fast, the routing tables reflect the current topology with a certain precision. The propagation characteristics (delay, bandwidth etc.) of a certain path between a sender and a receiver are already known before a data packet is sent.

Big disadvantages of proactive schemes are their overheads in lightly loaded networks. Independent of any real communication the algorithm continuously updates the routing tables. This generates a lot of unnecessary traffic and drains the batteries of mobile devices.

21. What are the Advantage & disadvantage of reactive protocols?

Advantage of on-demand protocols is scalability as long as there is only light traffic and low mobility. Mobile devices can utilize longer low-power periods as they only have to wake up for data transmission or route discovery.

However, these protocols also exhibit **disadvantages**. The initial search latency may degrade the performance of interactive applications and the quality of a path is not known *a priori*. Route caching, a mechanism typically employed by on-demand protocols, proves useless in high mobility situations as routes change too frequently.

UNIT III MOBILE TRANSPORT LAYER

1.What are main difference between UDP and TCP?

The main difference between UDP and TCP is that TCP offers connections between two applications. Within a connection TCP can give certain guarantees, such as in-order delivery or reliable data transmission using retransmission techniques. TCP has built-in mechanisms to behave in a 'network friendly' manner. If, for example, TCP encounters packet loss, it assumes network internal congestion and slows down the transmission rate. This is one of the main reasons to stay with protocols like TCP. One key requirement for new developments in the internet is 'TCP friendliness'. UDP requires that applications handle reliability, in-order delivery etc. UDP does not behave in a network friendly manner, i.e., does not pull back in case of congestion and continues to send packets into an already congested network.

2.What is slow start?

TCP's reaction to a missing acknowledgement is quite drastic, but it is necessary to get rid of congestion quickly. The behavior TCP shows after the detection of congestion is called **slow start**

3. What is fast retransmit?

In TCP, a receiver sends acknowledgements only if it receives any packets from the sender. Receiving acknowledgements from a receiver also shows that the receiver continuously receives something from the sender. The gap in the packet stream is not due to severe congestion, but a simple packet loss due to a transmission error. The sender can now retransmit the missing packet(s) before the timer expires. This behavior is called **fast retransmit.**

4. What is the need for fast recovery?

The receipt of acknowledgements shows that there is no congestion to justify a slow start. The sender can continue with the current congestion window. The sender performs a **fast recovery** from the packet loss. This mechanism can improve the efficiency of TCP dramatically.

5. What are the advantages with I-TCP?

I-TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network or other hosts in a wireless network that do not use this optimization.

- Due to the strict partitioning into two connections, transmission errors on the wireless link, i.e., lost packets, cannot propagate into the fixed network.
- It is always dangerous to introduce new mechanisms into a huge network such as the internet without knowing exactly how they will behave.
- The authors assume that the short delay between the mobile host and foreign agent could be determined and was independent of other traffic streams. An optimized TCP could use precise time-outs to guarantee retransmission as fast as possible.
- Partitioning into two connections also allows the use of a different transport layer protocol between the foreign agent and the mobile host or the use of compressed headers etc.

6. What are the disadvantages with I-TCP?

The loss of the end-to-end semantics of TCP might cause problems if the foreign agent partitioning the TCP connection crashes. cIn practical use, increased handover latency may be much more problematic. All packets sent by the correspondent host are buffered by the foreign agent besides forwarding them to the mobile host (if the TCP connection is split at the foreign agent). The foreign agent must be a trusted entity because the TCP connections end at this point.

7. Define the term ' Snooping TCP'.

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.

8. What are the advantages of Snooping TCP?

The end-to-end TCP semantic is preserved. No matter at what time the foreign agent crashes (if this is the location of the buffering and snooping mechanisms), neither the correspondent host nor the mobile host have an inconsistent view of the TCP connection as is possible with I-TCP.
The correspondent host does not need to be changed; most of the enhancements are in the foreign agent. It does not need a handover of state as soon as the mobile host moves to another foreign agent. It does not matter if the next foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

9. What are the disadvantages of Snooping TCP?

Snooping TCP does not isolate the behavior of the wireless link as well as ITCP. Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts. All efforts for snooping and buffering data may be useless if certain encryption schemes are applied end-to-end between the correspondent host and mobile host.

10. Write the concept of M-TCP.

M-TCP (mobile TCP)1 approach has the same goals as I-TCP and snooping TCP: to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems. M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover. Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.

11. What are advantages of M-TCP.

It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0. Since it does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

13. What are the disadvantages of MTCP?
As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager.

14. Define the term 'time-out freezing'.
The MAC layer can inform the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion. TCP can now stop sending and 'freezes' the current state of its congestion window and further timers. If the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed. With a fast interruption of the wireless link, additional mechanisms in the access point are needed to inform the correspondent host of the reason for interruption. Otherwise, the correspondent host goes into slow start assuming congestion and finally breaks the connection.

15. What are the advantages of time-out freezing''?
It offers a way to resume TCP connections even after longer interruptions of the connection. It is independent of any other TCP mechanism, such as acknowledgements or sequence numbers, so it can be used together with encrypted data.

16. What are the disadvantages of time-out freezing?
Not only does the software on the mobile host have to be changed, to be more effective the correspondent host cannot remain unchanged. All mechanisms rely on the capability of the MAC layer to detect future interruptions. Freezing the state of TCP does not help in case of some encryption schemes that use time-dependent random numbers. These schemes need resynchronization after interruption.

17. What is Selective retransmission?
TCP can indirectly request a selective retransmission of packets. The receiver can acknowledge single packets, not only trains of in-sequence packets. The sender can now determine precisely which packet is needed and can retransmit it.

18. What are the advantages of Selective retransmission?
The **advantage** of this approach is obvious: a sender retransmits only the lost packets. This lowers bandwidth requirements and is extremely helpful in slow wireless links. The gain in efficiency is not restricted to wireless links and mobile environments. Using selective retransmission is also beneficial in all other networks.

19. What are the disadvantages of Selective retransmission?
More buffers is necessary to resequence data and to wait for gaps to be filled. But while memory sizes and CPU performance permanently increase, the bandwidth of the air interface remains almost the same. Therefore, the higher complexity is no real disadvantage any longer as it was in the early days of TCP.

20. What are the advantage & disadvantage of Transaction-oriented TCP?

The obvious **advantage** for certain applications is the reduction in the overhead which standard TCP has for connection setup and connection release. However, T/TCP is not the original TCP anymore, so it requires changes in the mobile host and all correspondent hosts, which is a major **disadvantage**. This solution no longer hides mobility.

21. What are the characteristics have to be considered when deploying applications over 2.5G/3G wireless links?

Data rates: While typical data rates of today's 2.5G systems are 10–20 kbit/s uplink and 20–50 kbit/s downlink, 3G and future 2.5G systems will initially offer data rates around 64 kbit/s uplink and 115–384 kbit/s downlink.

Latency: All wireless systems comprise elaborated algorithms for error correction and protection, such as forward error correction (FEC), check summing, and interleaving.

Jitter: Wireless systems suffer from large delay variations or 'delay spikes'.

Packet loss: Packets might be lost during handovers or due to corruption. Thanks to link-level retransmissions the loss rates of 2.5G/3G systems due to corruption are relatively low

22. What are the configuration parameters to adapt TCP to wireless environment?

Large windows: TCP should support large enough window sizes based on the bandwidth delay product experienced in wireless systems.

Limited transmit: This mechanism, defined in RFC 3042 is an extension of Fast Retransmission/Fast Recovery and is particularly useful when small amounts of data are to be transmitted

Large MTU: The larger the MTU (Maximum Transfer Unit) the faster TCP increases the congestion window.

Selective Acknowledgement (SACK): SACK allows the selective retransmission of packets and is almost always beneficial compared to the standard cumulative scheme.

Explicit Congestion Notification (ECN): ECN as defined in RFC 3168 allows a receiver to inform a sender of congestion in the network by setting the ECN-Echo flag on receiving an IP packet that has experienced congestion.

Timestamp: TCP connections with large windows may benefit from more frequent RTT samples provided with timestamps by adapting quicker to changing network conditions.

No header compression: As the TCP header compression mechanism according to RFC 1144 does not perform well in the presence of packet losses this mechanism should not be used.

UNIT IV WIRELESS WIDE AREA NETWORK

1. What are responsibilities of an RNC?

- ✓ Intra UTRAN handover
- ✓ Macro diversity combining/splitting of Iub data streams
- ✓ Frame synchronization
- ✓ Radio resource management
- ✓ Outer loop power control
- ✓ Iu interface user plane setup
- ✓ Serving RNS (SRNS) relocation
- ✓ Radio resource allocation (allocation of codes, etc.)
- ✓ Frame selection/distribution function necessary for soft handover (functions
- ✓ of UMTS radio interface physical layer)
- ✓ UMTS radio link control (RLC) sublayers function execution
- ✓ Termination of MAC, RLC, and RRC protocols for transport channels,
- ✓ i.e., DCH, DSCH, RACH, FACH
- ✓ Iub's user plane protocols termination

2. What are responsibilities of the Node B?

- ✓ Termination of *Iub* interface from RNC
- ✓ Termination of MAC protocol for transport channels RACH, FACH
- ✓ Termination of MAC, RLC, and RRC protocols for transport channels:
- ✓ BCH, PCH
- ✓ Radio environment survey (BER estimate, receiving signal strength, etc.)
- ✓ Inner loop power control
- ✓ Open loop power control
- ✓ Radio channel coding/decoding
- ✓ Macro diversity combining/splitting of data streams from its cells (sectors)
- ✓ Termination of *Uu* interface from UE
- ✓ Error detection on transport channels and indication to higher layers

3. What are layers of protocol structure?

The protocol structure contains two main layers, the radio network layer (RNL) and the transport network layer (TNL). In the RNL, all UTRAN-related functions are visible, whereas the TNL deals with transport technology selected to be used for UTRAN but without any UTRAN-specific changes.

4. What are *Iur* functions?

Basic inter-RNC mobility support
Support of SRNC relocation
Support of inter-RNC cell and UTRAN registration area update
Support of inter-RNC packet paging
Reporting of protocol errors

5. Write the CS domain contains functional entities?

The CS domain contains the functional entities: mobile switching center (MSC) and gateway MSC (GMSC) (see Figure 15.28). The PS domain comprises the functional entities: serving

GPRS support node (SGSN), gateway GPRS support node (GGSN), domain name server (DNS), dynamic host configuration protocol (DHCP) server, packet charging gateway, and firewalls.

5. List out the functionality provided by the 3G-MSC?

The following functionality is provided by the 3G-MSC:

- ✓ Mobility management: Handles attach, authentication, updates to the HLR, SRNS relocation, and intersystems handover.
- ✓ Call management: Handles call set-up messages from/to the UE.
- ✓ Supplementary services: Handles call-related supplementary services such as call waiting, etc.
- ✓ CS data services: The IWF provides rate adaptation and message translation for circuit mode data services, such as fax.
- ✓ Vocoding.

7. What are function provide by 3G-SGSN?

- ✓ SMS: This functionality allows the user to send and receive SMS data to and from the SMS-GMSC /SMS-IWMSC.
- ✓ Mobility management: Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.
- ✓ Subscriber database functionality: This database (similar to the VLR) is located within the 3G-SGSN and serves as intermediate storage for subscriber data to support subscriber mobility.
- ✓ Charging: The SGSN collects charging information related to radio network usage by the user.
- ✓ OAM agent functionality.

8. What is 3G-SGSN?

The 3G-SGSN is the main CN element for PS services. The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN. It also provides the appropriate signaling and data interfaces including connection to an IP-based network toward the 3G-GGSN, SS7 toward the HLR/EIR/AUC and TCP/IP or SS7 toward the UTRAN.

9. What is called *Iu* and *Gn* MAP interface in 3G-SGSN?

The 3G-SGSN is able to complete originating or terminating sessions in the network by interaction with other entities of a mobile network, e.g., GGSN, HLR, AUC. It also controls/communicates with UTRAN using RANAP.

10. What is 3G-GGSN?

The GGSN provides interworking with the external PS network. It is connected with SGSN via an IP-based network. The GGSN may optionally support an SS7 interface with the HLR to handle mobile terminated packet sessions.

11. What are function provide by 3G-GGSN?

The 3G-GGSN provides the following functions:

- ✓ Maintain information locations at SGSN level (macro-mobility) Gateway between UMTS packet network and external data networks (e.g. IP, X.25)

- ✓ Gateway-specifi c access methods to intranet (e.g. PPP termination)
- ✓ Initiate mobile terminate Route Mobile Terminated packets
- ✓ User data screening/security can include subscription based, user controlled, or network controlled screening.
- ✓ Charging: The GGSN collects charging information related to external data network usage by the user.
- ✓ OAM functionality

12. What is User level address allocation?
User level address allocation: The GGSN may have to allocate (depending on subscription) a dynamic address to the UE upon PDP context activation. This functionality may be carried out by use of the DHCP function.

13. What is SMS-GMSC?
The SMS-GMSC is an MSC capable of receiving a terminated short message from a service center, interrogating an HLR for routing information and SMS information, and delivering the short message to the SGSN of the recipient UE.

14. **What are function provide by SMS-GMSC?**
The SMS-GMSC provides the following functions:
- ✓ Reception of short message packet data unit (PDU)
- ✓ Interrogation of HLR for routing information
- ✓ Forwarding of the short message PDU to the MSC or SGSN using the routing information

15. **What are function provide by SMS-IWMSC?**
The SMS-IWMSC provides the following functions:
- ✓ Reception of the short message PDU from either the 3G-SGSN or 3G-MSC
- ✓ Establishing a link with the addressed service center
- ✓ Transferring the short message PDU to the service center

16. What is SMS-IWMSC?
The SMS-IWMSC is an MSC capable of receiving an originating short message from within the PLMN and submitting it to the recipient service center.

17. What is Firewall?
This entity is used to protect the service providers' backbone data networks from attack from external packet data networks. The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable.

18. What is DNS/DHCP?
The DNS server is used, as in any IP network, to translate host names into IP addresses, i.e., logical names are handled instead of raw IP addresses. Also, the DNS server is used to translate the access point name (APN) into the GGSN IP address. It may optionally be used to allow the UE to use logical names instead of physical IP addresses.

A dynamic host configuration protocol server is used to manage the allocation of IP configuration information by automatically assigning IP addresses to systems configured to use DHCP.

19. What is Adaptive Multi-Rate Codec for UMTS?

The adaptive multi-rate (AMR) codec is the new codec that will be used in UMTS and GSM. The AMR codec has eight source rates; 4.75, 5.15, 5.90, 6.70 (PDC-EFR), 7.40 (IS-641), 7.95 (VSELP), 10.2 and 12.2 kbps (GSM-EFR). The AMR codec rates are controlled by a radio access network and do not depend on speech activity as in the cdma2000. During high cell loading, such as during busy hours, the AMR codec uses lower bit rates to offer higher capacity while providing slightly lower speech quality.

20. What are two parts of UMTS bearer service?

The UMTS bearer service has two parts: the *radio access bearer* (*RAB*) service and the *core network bearer* (*CNB*) service. Both these services are aimed at optimizing the UMTS bearer service over the respective wireless network topology by taking into consideration aspects such as mobility and mobility subscriber profiles.

21. Write the UMTS QoS classes?

UMTS defines four different QoS classes. These are conversational class, streaming class, interactive class, and background class. The main distinguishing factor between these classes is how delay sensitive the traffic is. The conversational class is meant for traffic, which is very delay sensitive, whereas the background class is the most delay insensitive traffic class.

22. What is High-Speed Downlink Packet Access (HSDPA)?

HSDPA is evolved from and backward compatible with Release 99 WCDMA systems. HSDPA is based on the same set of technologies as high data rate (HDR) to improve spectral effi ciency for data services — such as shared downlink packet data channel and high peak data rates — using high-order modulation and adaptive modulation and coding, hybrid ARQ (HARQ) retransmission schemes, fast scheduling and shorter frame sizes.

23. List out the new channels introduced in HSDPA.

The new channels introduced in HSDPA are high-speed downlink shared channel (HS-DSCH), high-speed shared control channel (HS-SCCH), and high speed dedicated physical control channel (HS-DPCCH).

24. What is HS-DSCH?

It is the primary radio bearer. Its resources can be shared among all users in a particular sector. The primary channel multiplexing occurs in a time domain, where each TTI consists of three time slots (each 2 ms). TTI is also referred to as a sub-frame. Within each 2 ms TTI, a constant spreading factor (SF) of 16 is used for code multiplexing, with a maximum of 15 parallel codes allocated to HS-DSCH. Codes may all be assigned to one user, or may be split across several users. The number of codes allocated to each user depends on cell loading, QoS requirements, and UE code capabilities.

25. What is HS-SCCH?

It is a fixed rate 960 kbps used to carry downlink signaling between Node B and UE before the beginning of each scheduled TTI. It includes UE identity, HARQ-related information and the parameters of the HS-DSCH transport format selected by the link-adaptation mechanism. Multiple HS-SCCHs can be configured in each sector to support parallel HS-DSCH transmissions. A UE can be allocated a set of up to four HS-SCCHs, which need to be monitored continuously.

26. What is HS-DPCCH?

It carries ACK/NACK signaling to indicate whether the corresponding downlink transmission was successfully decoded, as well as a channel quality indicator (CQI) to be used for the purpose of link adaptation. The CQI is based on a common pilot channel (CPICH) and is used to estimate the transport block size, modulation type, and number of channelization codes that can be supported at a given reliability level in downlink transmission. The feedback cycle of CQI can be set as a network parameter in predefined steps of 2 ms.

27. What is Freedom of Mobile multimedia Access (FOMA)?

Based on the WCDMA system, FOMA is providing the dramatic evolution of i-mode, other web-connection services, and innovative data-rich applications. FOMA supports full-motion video image transmission, music and game distribution, and other high-speed, large-capacity data communications. The service also offers roaming in various countries around the world. With packet data transfer speeds of 64 to 384 kbps, FOMA service supports a variety of applications including Internet access, e-mail, fi le transfer, remote login, and Internet phone applications.

UNIT V 4G NETWORKS

1. What is 4G?

The 4G systems will encompass all systems from various networks, public to private, operator-driven broadband networks to personal areas, and ad hoc networks. The 4G systems will be interoperable with 2G and 3G systems, as well as with digital (broadband) broadcasting systems. The 4G intends to integrate from satellite broadband to high altitude platform to cellular 2G and 3G systems to wireless local loop (WLL) and broadband wireless access (BWA) to WLAN, and wireless personal area networks (WPANs), all with IP as the integrating mechanism.

2. What is the vision of 4G?

The future 4G systems will consist of a set of various networks using IP as a common protocol. 4G systems will have broader bandwidth, higher data rate, and smoother and quicker handoff and will focus on ensuring seamless service across a multiple of wireless systems and networks. The key is to integrate the 4G capabilities with all the existing mobile technologies through the advanced techniques of digital communications and networking.

3. Explain the term '4G'.

The term 4G is used broadly to include several types of broadband wireless access communication systems, not only cellular systems. 4G is described as MAGIC — **M**obile multimedia, **any** time anywhere, **G**lobal mobility support, **integrated** wireless solution, and **C**ustomized personal service. The 4G systems will not only support the next generation mobile services, but also will support the fixed wireless networks. The 4G systems are about seamlessly integrating terminals, networks, and applications to satisfy increasing user demands.

4. What are the key features of 4G?

Some key features (primarily from users' points of view) of 4G mobile networks are as follows:

- ✓ High usability: anytime, anywhere, and with any technology
- ✓ Support for multimedia services at low transmission cost
- ✓ Personalization
- ✓ Integrated services.

5. What are the key challenges of 4G?

	Key challenges	Proposed solutions
Mobile Station		
Multimode user terminals	To design a single user terminal that can operate in different wireless networks, and overcome design problems such as limitations in device size, cost power consumption, and backward compatibilities to systems	A software-defined radio approach can be used: the user terminal adapts itself to the wireless interfaces of the networks.
Wireless system discovery	To discover available wireless systems by processing the signals sent from different wireless systems (with different access protocols and incompatible with each other)	User- or system-initiated discoveries, with automatic download of software modules for different wireless systems

6. What is the expectation with 4G?
It is expected that when 4G services are launched, users in widely different locations, occupations, and economic classes will use the services. In order to meet the demands of these diverse users, service providers will design personal and customized service for them. 4G systems will also provide facilities for integrated services. Users can use multiple services from any service provider at the same time.

7. What is the application of 4G?
The following are some of the applications of the 4G system:
Virtual presence
Virtual navigation.
Tele-medicine.
Tele-geo-processing applications — 4G will combine geographical information systems (GIS) and global positioning systems (GPS) in which a user will get location querying.
Education — 4G will provide a good opportunity to people anywhere in the world to continue their education on-line in a cost-effective manner.

8. What is virtual presence & navigation?
Virtual presence — 4G will provide user services at all times, even if the user is off-site.
Virtual navigation -4G will provide users with virtual navigation through which a user can access a database of streets, buildings, etc., of a large city. This requires high speed transmission.

9. What is telemedicine?
4G will support the remote health monitoring of patients via video conference assistance for a doctor at anytime and anywhere.

10. What is Multicarrier modulation?
Multicarrier modulation (MCM) is a derivative of frequency-division multiplexing. It is not a new technology. Forms of multicarrier systems are currently used in DSL modems and digital audio/video broadcast (DAB/DVB).

11. What are advantages of MCM?
MCM's advantages are better performance in the inter-symbol-interference environment, and avoidance of single-frequency interferers. However, MCM increases the peak to average ratio of the signal, and to overcome inter-symbol-interference a cyclic extension or guard band must be added to the data.

12. What is peak to average ration?
The difference, *D, of the* peak-to-average ratio between MCM and a single carrier system is a function of the number of subcarriers, *N, as:*

$$D(\mathrm{dB}) = 10 \log N$$

13. What are the types of MCM?
Two different types of MCM are likely candidates for 4G. These include multicarrier code division multiple access (MC-CDMA) and orthogonal frequency division multiplexing (OFDM) using time division multiple access (TDMA).

MC-CDMA is actually OFDM with a CDMA overlay. Similar to single-carrier CDMA systems, the users are multiplexed with orthogonal codes to distinguish users in MC-CDMA. However, in MC-CDMA, each user can be allocated several codes, where the data is spread in time or frequency. Either way, multiple users simultaneously access the system.

14. What are the modes of smart antennas?

- ✓ Single-Input, Single-Output (SISO)
- ✓ Single-Input, Multiple-Output (SIMO)
- ✓ Multiple-Input, Single-Output (MISO)
- ✓ Multiple-Input, Multiple-Output (MIMO)

15. What is SIMO?

Single-input, multiple-output: There are N antennas at the receiver. If the signals received on the antennas have on average the same amplitude, then they can be added coherently to produce an N^2 increase in signal power. There are N sets of noise sources that are added coherently and result in an N-fold increase in noise power. Hence, the overall increase in SNR will be:

$$\text{SNR} \approx \frac{N^2 \times (\text{signal power})}{N \times (\text{noise})} = N \times \text{SNR}_0$$

16. What is MISO?

Multiple-input, single-output: We have M transmitting antennas. The total power is divided into M transmitter branches. If the signals add coherently at the receiving antenna, we get an M-fold increase in SNR as compared to SISO. Because there is only one receiving antenna, the noise level is same as SISO. The overall increase in SNR is approximately

$$\text{SNR} \approx \frac{M^2 \cdot [(\text{signal power})/M]}{\text{noise}} = M \times \text{SNR}_0$$

17. What is MIMO?

Multiple-input, multiple-output: MIMO systems can be viewed as a combination of MISO and SIMO channels. In this case, it is possible to achieve approximately an MN-fold increase in the average SNR_0 giving a channel capacity equal to

$$C \approx B \log_2(1 + M \times N \times \text{SNR}_0)$$

18. What is OFDM-MIMO Systems?

OFDM and MIMO techniques can be combined to achieve high spectral efficiency and increased throughput. The OFDM-MIMO system transmits independent OFDM modulated data from multiple antennas simultaneously. At the receiver, after OFDM demodulation, MIMO decodes each subchannel to extract data from all transmits antennas on all the subchannels.

19. What is reason for degradation of the wireless system performance?
In general, TCP/IP is designed for a highly reliable transmission medium in wired networks where packet losses are seldom and are interpreted as congestion in the network. On the other hand, a wireless network uses a time varying channel where packet losses may be common due to severe fading. This is misinterpreted by TCP as congestion which leads to inefficient utilization of the available radio link capacity. This results in significant degradation of the wireless system performance.

20. What is Bell Labs Layered Space Time (BLAST)?
BLAST is a space division multiplexing (SDM)-based MIMO system. It provides the best trade-off between system performance (spectral efficiency and capacity) and system implementation complexity. The spectral efficiency of BLAST ranges from 20 to 40 bps/Hz.

21. What are the four recursive steps?
1. Ordering: Determine the optimal detection order.
2. Nulling: Choose the nulling vector to null out all the weaker transmit signals and obtain the strongest transmit signal.
3. Slicing: Detect the estimated value of the strongest signal by slicing to the nearest value in the signal constellation.
4. Cancellation: Cancel the effect of the strongest signal from the received signal vector to reduce the detection complexity for the remaining transmit signal. Go to step 2 — nulling process.

22. What is Software-Defi ned Radio?
A software-defined radio (SDR) system is a radio communication system which Uses software for the modulation and demodulation of radio signals. An SDR performs significant amounts of signal processing in a general purpose computer, or a reconfigurable piece of digital electronics. The goal of this design is to produce a radio that can receive and transmit a new form of radio protocol just by running new software.

23. What is Cognitive Radio?
With the CR paradigm, spectrum can be efficiently shared in a more flexible fashion by a number of operators/users/systems. The CR can be viewed as an enabling technology that will benefit several types of users by introducing new communications and networking models for the whole wireless world, creating better business opportunities for the incumbent operators and new technical dimensions for smaller operators, and helping shape an overall more efficient approach regarding spectrum requirements and usage in the next generation wireless networks.

24. What is goal of Cognitive Radio?
It is not implicit that a CR must be software-defined radio. It is possible to implement CR features — the ability to detect and avoid (protect) incumbent users — while using relatively conventional radio transmitter/receiver architectures and techniques. The goal of CR is to relieve radio spectrum overcrowding, which actually translates to a lack of access to full radio spectrum utilization.