IT8076 Software Testing

UNIT – I
INTRODUCTION

SYLLABUS: Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies-MAC Protocols – SDMA- TDMA- FDMA- CDMA

PART – A

1. Define Mobile Computing.

Mobile Computing also called as Ubiquitous Computing or Nomadic Computing is described as the ability to compute remotely while on the move. It makes possible for people to access information from anywhere and at any time.
Mobile Computing = Mobility + Computing

2. What do you mean by the terms Mobility and Computing?

Mobility: Provides the capability to change location while communicating to invoke computing services at some remote computers.
Computing: Capability to automatically carry out certain processing related to services invocation on a remote computer.

3. Name the type of Mobility.

a) User Mobility
b) Device Portability

4. List out the advantages of Mobile Computing.May/June 2016

(i) Location Flexibility
(ii) User Mobility
(iii) Device Portability
(iv) Saves Time
(v) Enhanced Productivity
(vi) Entertainment

5. Mention the disadvantages of Mobile Computing.

(i) Expensive
(ii) Power Consumption
(iii) Small Screen Display
(iv) Slow Internet Speed
(v) Risky to carry
(vi) Security Concerns
(vii) Communication depends upon network

6. Compare Wired Networks and Mobile Networks.

S.No	Wired Networks	Mobile Networks
1.	Users cannot get any information at any place (does not support mobility)	Users can get information at any place (Supports Mobility)
2.	Bandwidth is high	Bandwidth is low
3.	Low bandwidth variability	High bandwidth variability
4.	Listen on wire	Hidden Terminal problem
5.	Productivity is low	Productivity is high
6.	High Power Machines	Low Power machines
7.	High Resource machines	Low Resource machines
8.	Need physical access	Need proximity
9.	Low delay	Higher delay
10.	Connected Operations	Disconnected Operations

7. List out the differences between Mobile Computing and Wireless Networking.

S.No	Mobile Computing	Wireless Networking
1.	It is a technology that access data through wireless network	It is a network that uses wireless data connections for connecting network nodes
2.	It denotes accessing information and remote computational services while on the move	It provides the basic communication infrastructure necessary for mobile computing
3.	It refers to computing devices that are not restricted to a desktop. Eg: Smart Phone, PDA, Laptop etc.,	It is a method of transferring information between a computing devices such as PDA & data sources without a physical connection
4.	It refers to a device performing computation that is not always connected to a central network	It refers to the data communication without the use of a landline. Eg. Cellular Telephone, Two way radio, Satellite, Wireless Connection.

8. Name some of the Mobile Computing Devices.

Mobile Phones
Laptops
PDA
Notebook PCs

9. Point out the problems faced by devices in Wireless Transmission?

1. Lower Bandwidth
2. Bandwidth Fluctuations
3. Host mobility
4. Intermittent disconnections
5. High bit error rate
6. Poor link reliability
7. Higher delay
8. Power consumption

10. What are the classifications of Wireless Networks?

i) Extension of Wired Networks: Uses fixed infrastructures such as base stations to provide single hop wireless communication (or) two-hop wireless communication.
   a. Example: WLAN, Bluetooth

ii) Adhoc Networks: It does not use any fixed infrastructure and it is based on multi-hop wireless communication.

Example: MANET, VANET.

11. What are the applications of mobile computing?

Emergency services
Stock BrokerVehicles
For Estate Agents
In courts
In companies
Stock Information Collection/Control
Credit Card Verification
Taxi/Truck Dispatch
Electronic Mail/Paging

12. List out the characteristics of Mobile Computing.

(i) Ubiquity
(ii) Location Awareness
(iii)Adaptation
(iv)Broadcast
(v) Personalization

13.What is multiplexing?

Multiplexing is a fundamental mechanism in communication system. Multiplexing describes how several users can share a medium with minimum or no interference.

14. **Define SAMA.**

Spread Aloha Multiple Access is a combination of CDMA and TDMA. The CDMA better suits for connection oriented services only and not for connection less bursty data traffic because it requires to program both sender and receiver to access different users with different codes

15. **Define CDMA.**

Code Division Multiple Access systems use codes with certain characteristics to separate different users. To enable access to the shared medium without interference. The users use the same frequency and time to transmit data.

16. **What are the categories of Mobile services?**

- Bearer services
- Tele services
- Supplementary services

17.What is meant by GPRS?

The General Packet Radio Service provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes.

18.Define Mobile Communication.

Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.

19. What are the types of transport mechanism used in DAB?

The two basic transport mechanisms used by DAB are:

- Main Service Channel(MSC).
- Fast Information Channel (FIC).

20. What is SDMA and TDMA?

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different quality.

Time Division Multiple Access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time.

21. Define FDMA.

Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme as presented Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).

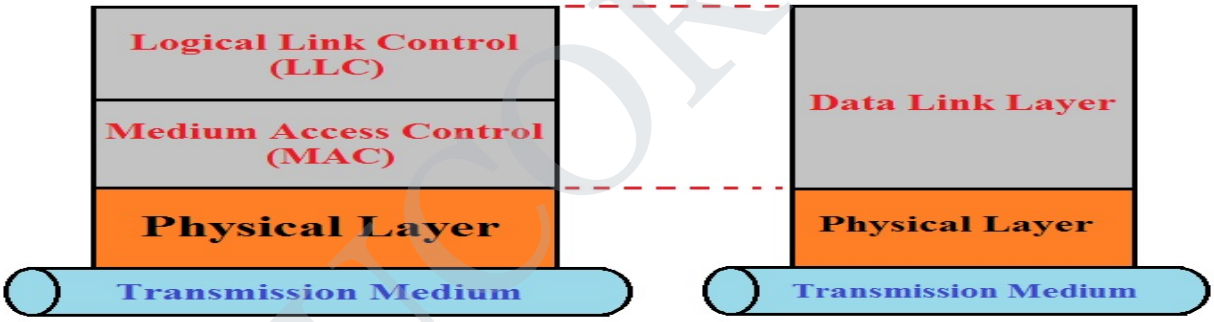
PART B

1.MEDIUM ACCESS CONTROL (MAC)

Medium Access Control (MAC) address is a hardware address use to uniquely identify each node of a network. It provides addressing and channel access control mechanisms to enable the several terminals or network nodes to communicate in a specified network. Medium Access Control of data communication protocol is also named as Media Access Control. In IEEE 802 OSI Reference model of computer networking, the Data Link Control (DLC) layer is subdivided into two sub-layers:

- **The Logical Link Control (LLC) layer**
- **The Medium Access Control (MAC) layer**

The MAC sub layer acts as a direct interface between the logical link control (LLC) Ethernet sub layer and the physical layer of reference model. Consequently, each different type of network medium requires a different MAC layer. On networks that don't conform they are part of IEEE 802 standards but they do conform that they participate OSI Reference Model then the node address is named the Data Link Control (DLC) address. The MAC sub layer emulates a full-duplex logical communication channel in a multipoint network system. **These communication channels may provide unicast, multicast and/or broadcast communication services.**



MAC address is suitable when multiple devices are connected with same physical link then to prevent from collisions system uniquely identify the devices one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. The MAC sub layer uses MAC protocols to prevent collisions and MAC protocols uses MAC algorithm that accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

Functions performed in the MAC sub layer:

Frame delimiting and recognition: This function is responsible to creates and recognizes frame boundaries.

Addressing: MAC sub layer performs the addressing of destination stations (both as individual stations and as groups of stations) and conveyance of source-station addressing information as well.

Transparent data transfer: It performs the data transparency over data transfer of LLC, PDUs, or of equivalent information in the Ethernet sub layer.

Protection: MAC sub layer function is to protect the data against errors, generally by means of generating and checking frame check sequences.

Access control: Control of access to the physical transmission medium form unauthorized medium access.

3.1.1 Hidden and exposed terminals

Consider the scenario with three mobile phones as shown in Figure 3.1. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa.

A starts sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. A is **hidden** for C and vice versa.

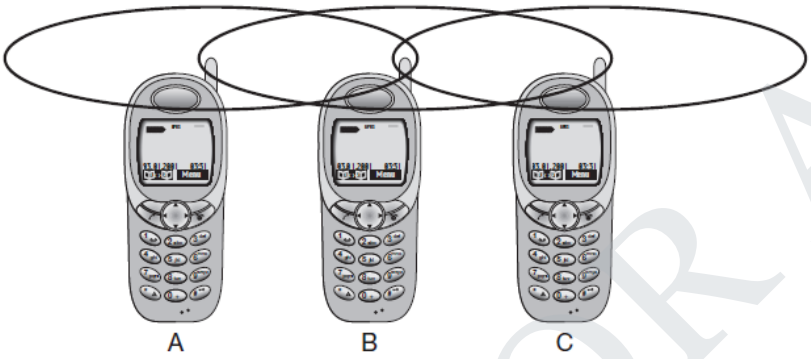


Figure 3.1 Hidden and exposed terminals

One of the most commonly used of MAC sub layer for wired networks i.e. **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**. Through MAC schema, a sender senses the medium (a wire or coaxial cable) before transmission of data to check whether the medium is free or not. If MAC senses that the medium is busy, the sender waits until it is free. When medium becomes free, the sender starts transmitting of data and continues to listen into the medium. If any kind of collision detected by sender while sending data, it stops at once and sends a jamming signal.

While hidden terminals may cause collisions, the next effect only causes unnecessary delay. Now consider the situation that B sends something to A and C wants to transmit data to some other mobile phone outside the interference ranges of A and B. C senses the carrier and detects that the carrier is busy (B's signal). C postpones its transmission until it detects the medium as being idle again. But as A is outside the interference range of C, waiting is not necessary. Causing a 'collision' at B does not matter because the collision is too weak to propagate to A. In this situation, C is **exposed** to B.

2.SDMA-TDMA-FDMA:

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different quality. A MAC algorithm could now decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code

(CDM) are still available (depending on the technology). Typically, **SDMA is never used in isolation but always in combination with one or more other schemes**. The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing space division multiplexing SDM).

The main advantage of SDMA is frequency reuse. Provided the reuse distance is preserved in the network architecture, interference can be near zero, even if mobile stations use the same allocated frequencies.

Time Division Multiple Access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time. Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access. Different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple. Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, Token Ring, ATM etc.

Now synchronization between sender and receiver has to be achieved in the time domain. Again this can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme. Dynamic allocation schemes require an identification for each transmission as this is the case for typical wired MAC schemes (e.g., sender address) or the transmission has to be announced beforehand. MAC addresses are quite often used as identification. This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message.

Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme as presented Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).

Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA. The latter example is the common practice for many wireless systems to circumvent narrowband interference at certain frequencies, known as frequency hopping. Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune to the right frequency. Hopping patterns are typically
fixed, at least for a longer period.

Main features:

- FDMA is compatible with both digital and analog signals.
- FDMA demands highly efficient filters in the radio hardware, contrary to CDMA and TDMA.
- FDMA is devoid of timing issues that exist in TDMA.

One disadvantage of FDMA is crosstalk, which can cause interference between frequencies and interrupt the transmission.

3. MAC PROTOCOLS

Multiple access techniques are used to allow a large number of mobile users to share the allocated spectrum in the most efficient manner.

- Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM.
- MAC is thus similar to traffic regulations in the highway example. Here regulation of traffic is enabled by the used of traffic lights.
- MAC belongs to layer 2, the data link control layer (DLC). Layer 2 is subdivided into the logical link control (LLC) and the MAC layer. The task of DLC is to establish a reliable point to point or point to multi-point connection between different devices over a wired or wireless medium.

Definition: In wireless network multiple users share the channel at the same time. **Medium Access Control (MAC) protocols** control access to the medium when multiple users try to transmit on the same shared channel. It is a sub layer of the data link layer protocol and directly invokes the physical layer protocol.

Objectives of MAC:

• Arbitrate channel access
• Maximize utilization of channels
• Minimize average latency of transmission
• MAC ensures that no node waits for an unduly long time

Properties required of MAC protocols:

• Implement rules to enforce discipline
• Max channel utilization
• Channel allocation should be fair
• Capability to support traffic with different bit rates
• Robust to face equipment failures and changing network conditions

UNIT 2

MOBILE TELECOMMUNICATION SYSTEM

GSM – Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security –GPRS- UMTS- Architecture

PART A

1. Expand GSM, GPRS and UMTS.

GSM – Global System for Mobile Communication
GPRS – General Packet Radio Services
UMTS – Universal Mobile Telecommunication Systems

2. What is meant by GSM?

Global System for Mobile Communication (GSM) is a wide area wireless communications system that uses digital radio transmission to provide voice, data and multimedia communication services. A GSM system coordinates the communication between a mobile telephones (Mobile Stations), base stations (Cell Sites) and switching systems.

3. What is the important characteristic of GSM?

GSM provides data services in addition to voice services and it is compatible to 1G system.

4. What is the use of GSM in mobile telecommunication? Nov/Dec 2011&12 May/June 12

This system was soon named the Global System for Mobile communications (GSM), The primary goal of GSM was to provide a mobile phone system that allows users to roam and provides voice services compatible to ISDN and other PSTN systems

5. Specify the three different categories of services defined by GSM

Bearer services
Tele services
Supplementary services

6. What is the use of emergency number?

Another service offered by GSM is the emergency number. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center.

7. List the important supplementary services offered by GSM.

User Identification
Call Forwarding (or Redirection)
Automatic call-back
Conferencing with up to 7 participants

8. What is meant by SMS and EMS?

A useful service for very simple message transfer is the short message service(SMS), which offers transmission of messages of up to 160 characters

The successor of SMS, the Enhanced Message Service (EMS), offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures

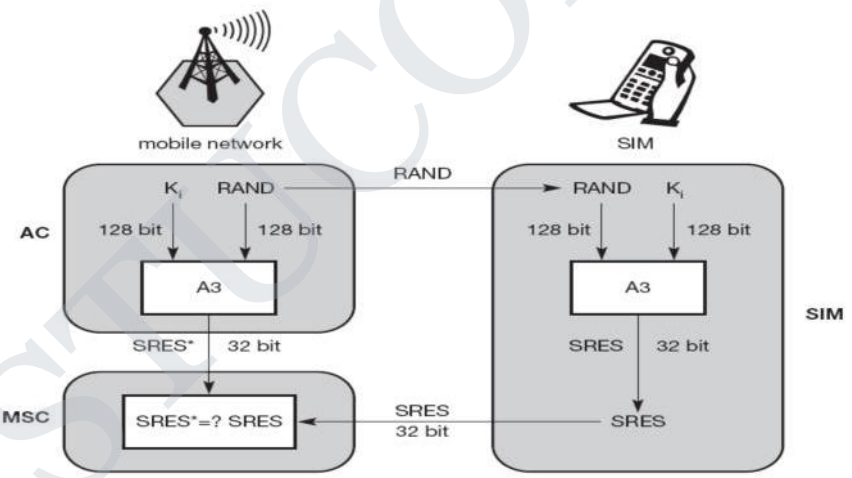
9. **List the 3 important features of GSM Security. May/June 2016**

1. **Authentication** – used to protect the network against unauthorized use.
2. **Confidentiality** – Data on the radio path is encrypted between the Mobile Equipment (ME) and the BTS which protects user traffic and sensitive signaling data against eavesdropping.
3. **Anonymity** – Anonymity is achieved by allocating Temporary Mobile Subscriber Identity (TMSI) instead of permanent identities to protect against tracking a user's location and obtaining information about a user's call log.

10. What are the characteristics of GSM?

1. Communication
2. Total Mobility
3. World Wide Connectivity
4. High Capacity
5. High Transmission Quality
6. Security Functions
7. SIM Card Bounded Service

11. Give the block diagram of GSM Authentication. May/June 2014



12. **What is meant by GPRS? May/June 12**

GPRS (General Packet Radio Services) is a packet-oriented mobile data service on the GSM of 3G and 2G cellular communication systems. It is a non-voice, high-speed and useful packet-switching technology for GSM networks.

13. List out the features of GPRS.

1. Speed
2. Immediacy

3. Packet Switched Resource Allocation (Spectrum Efficiency)
4. Flexible Channel Allocation
5. Traffic characteristics suitable for GPRS
6. Mobility
7. Localization

14. Explain in what ways is GPRS better than GSM?

GSM uses a billing system based on the time of connection whereas GPRS uses a billing system based on the amount of transmitted data.

15.What are the goals of GPRS?

1. Open Architecture
2. Consistent IP services
3. Same infrastructure for different air interfaces
4. Integrated telephony and Internet infrastructure
5. Service innovation independent of infrastructure

16. What are the services offered by GPRS?

GPRS offers end-to-end packet-switched data transfer services which can be categorized into the following two types:

1. Point-To-Point Service (PTP): It is between two users and can either be connectionless or connection-oriented.
2. Point-To-Multipoint Service (PTM): It is a data transfer service from one user to multiple users.

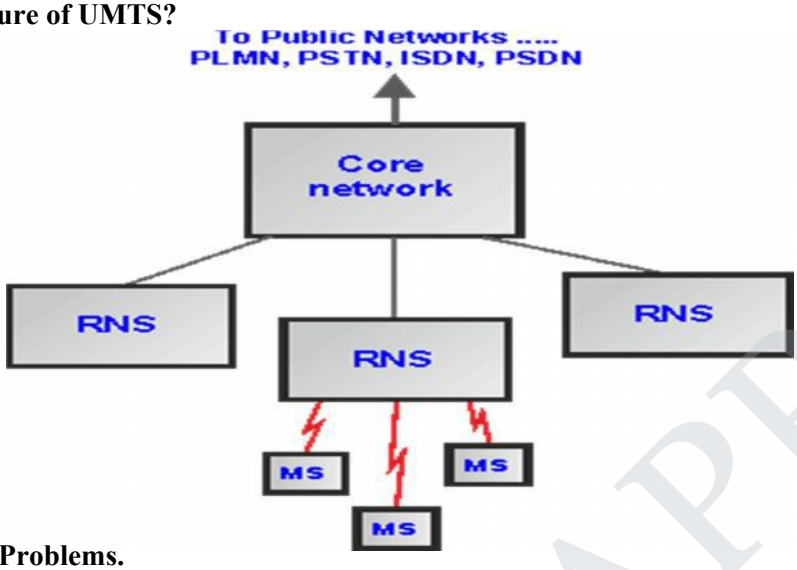
17. What is UMTS?

The Universal Mobile Telecommunications System (UMTS) is a 3G mobile communication system that provides a range of broadband services to wireless and mobile communications. The UMTS was developed mainly for countries with GSM networks.

18. What are the main elements of UMTS? May/June 2016

1. User Equipment / Mobile Station (MS): is the name by which a cell phone is referred to
2. Radio Network Subsystem (RNS): Equivalent of Base Station Subsystem (BSS) in GSM. It provides and manages the wireless interface for the overall network.
3. Core Network (CN): Equivalent of the Network Switching Subsystem (NSS) in GSM.

19. Draw Architecture of UMTS?



20. List out UMTS Problems.

Require more battery power
Can handoff UMTS to GSM but not GSM to UMTS
Initial poor coverage
More expensive than GSM

PART-B

1. Explain GSM architecture and its services with neat diagram. **[U] Nov/Dec2011&12, May/June 12, May /June 2013, Nov/Dec 2013, May/June 2014, Nov/Dec2014, May/June 2016**
2. Explain security service in GSM. **[U] December 2012, Nov/Dec 2013**
3. Explain GSM Authentication and Security. [U] **May/June 2016**
4. Draw a neat diagram of GPRS and explain its protocol architecture and services. **[An] Nov/Dec 2011&12, May/June 12, May /June 2013, Nov/Dec 2013, May/June 2014, Nov/dec2014, May/June 2016**
5. Explain in detail about UMTS Architecture and its Services. [U] **May/June 2016**

UNIT 3

WIRELESS NETWORKS

Wireless LANs and PANs – IEEE 802.11 Standard – Architecture – Services – Blue Tooth- Wi-Fi – WiMAX

PART A

1. What are the advantages (Features) of WLAN?

High flexibility
Simple Design
Easy planning
Low cost

2. Define IEEE802.11.

The IEEE 802.11 standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs. This standard offers the time bounded and asynchronous services. The data rate of this standard is 54 M bits/s at 5 GHZ.

3.What are the functions of MAC management?

Supports the association and re association of a station to an access point and roaming between different access points.
It maintains the MAC information base(MIB)
It also controls the authentication mechanisms, encryption, power management.

4. Define HIPERLAN.

HIPERLAN means High Performance Local Area Network. The ETSI standardized HIPERLAN1asaWLANallowing for node mobility and supporting infrastructure based adhoc topologies. It includes topology discovery, forwarding mechanism, user data encryption, power conservation mechanism.

5 .What are the features of HIPERLAN2?

High throughput transmission
Connection oriented
Security support
Quality of service support

6. What is ESS and BSS?

A distribution system is used to connect a several BSS via the access point to form a single network and there by extends the wireless coverage area. This network is called **Extended Service Set(ESS).**

BSS - Basic Service Set. The Basic Service Set is a term used to describe the collection of Stations which may communicate together within an 802.11 network. The BSS include AP (Access Point) which provide a connection onto a fixed distribution system such as an Ethernet network.

.

7. Write about Bluetooth and its applications.

Bluetooth is an open wireless technology standard for transmitting fixed and mobile electronic device data over short distances.

- The Bluetooth is used in wireless head sets.
- Bluetooth is used to transfer files, images and MP3 or MP4 between cell phones.
- Bluetooth using in laptops and notebooks.
- It is used in PDAs (personal digital assistant) and printers.
- Connecting Wireless mouse and keyboards.

8. Define Piconet and Scatternet.

A Piconet is a network of devices connected using Bluetooth technology. The network ranges from two to eight connected devices. When a network is established, one device takes the role of the master while all the other devices act as slaves.

A scatternet is a type of network that is formed between two or more Bluetooth-enabled devices, such as smart phones and newer home appliances. A scatternet is made up of at least two piconets.

9. What is WLAN Security Standards?

Wireless local area network security (WLAN security) is a security system designed to protect networks from the security breaches.

- Wired Equivalent Privacy (WEP)
- Wireless Intrusion Prevention Systems/Intrusion Detection Systems

PART-**B**

1. Wireless LAN: Features-Security standards

WLANs (Wireless LAN) are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers. The global goal of WLANs is to replace office cabling, to enable tether less access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.

Advantages of WLANs are:

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 down completely.
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. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly.
Disadvantages of WLANs are:
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.
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.

Design goals have to be taken into account for WLANs to ensure their commercial success:
Global operation: WLAN products should sell in all countries so, national and international frequency regulations have to be considered.
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.
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.). WLAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment.
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.
WLAN Security standards:
Wireless local area network security (WLAN security) is a security system designed to protect networks from the security breaches.

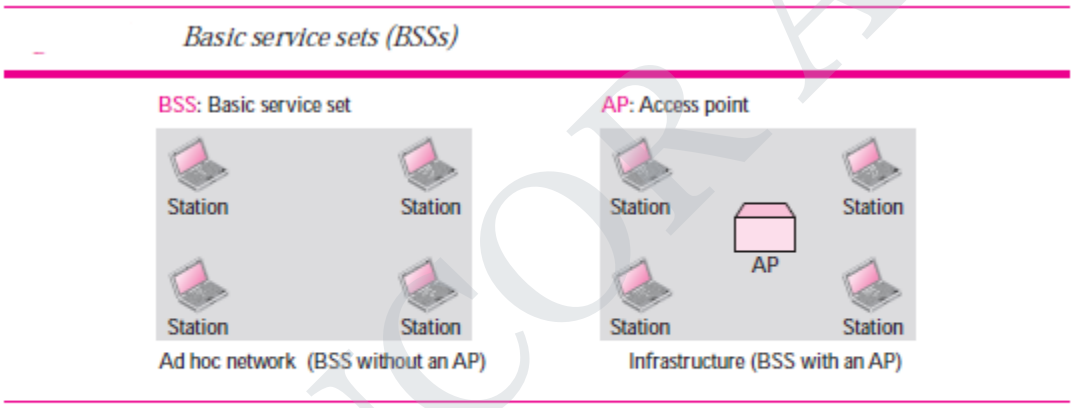
Wired Equivalent Privacy (WEP): An old encryption standard used to overcome security threats. WEP provides security to WLAN by encrypting the information transmitted over the air so that only the receivers with the correct encryption key can decrypt the information.

WPA/WPA2 (WI-FI Protected Access): Improved on WEP by introducing Temporal Key Integrity Protocol (TKIP). While still using RC4 encryption.

Wireless Intrusion Prevention Systems/Intrusion Detection Systems: Intrusion detection and prevention focuses on radio frequency (RF) levels. This involves radio scanning to detect rogue access points or ad hoc networks to regulate network access.

2.Wireless LAN(WLAN): Protocol Stack and Standards Architecture:

The standard defines two kinds of services: the **basic service set (BSS) and the extended service set (ESS)**. Basic Service Set IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).



Extended Service Set An **extended service set (ESS)** is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system*, which is usually a wired LAN. The distribution system connects the APs in the BSSs.

IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge. Applications should not notice any difference apart from the lower bandwidth and perhaps higher access time from the wireless LAN. 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.

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 sub layer PMD**. The basic tasks of the MAC layer comprise **medium access, fragmentation of user data, and encryption**.

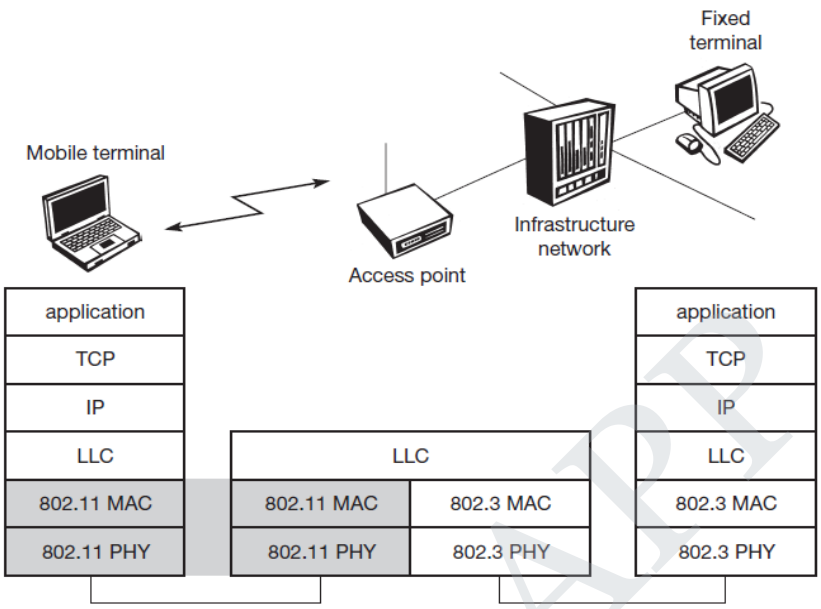


Figure IEEE 802.11 protocol architecture and bridging

PLCP sub layer 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 sub layer handles modulation and encoding/decoding of signals. The PHY layer (comprising PMD and PLCP).

Apart from the protocol sub layers, 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).

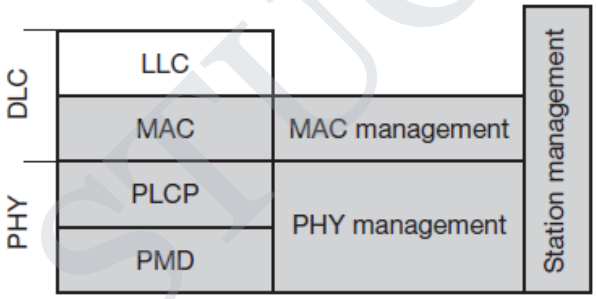
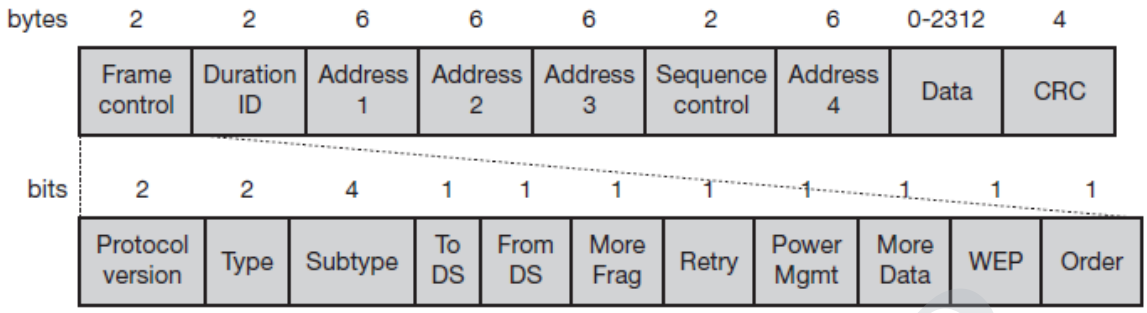


Figure Detailed IEEE 802.11 protocol architecture and management

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 sub layer PMD**. The basic tasks of the MAC layer comprise **medium access, fragmentation of user data, and encryption**.

3. WLAN (IEEE802.11) Frame format-Features:

The MAC layer frame consist of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



Frame Control(FC) –It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
Version: It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
Type: It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.
Subtype: It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request.
To DS: It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
From DS: It is a 1 bit long field which when set indicates frame coming from DS.
More frag (More fragments): It is 1 bit long field which when set to 1 means frame is followed by other fragments.
Retry: It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
Power Mgmt (Power management): It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
More data: It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
WEP: It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
Order: It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.
Duration/ID: It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in µs).
Address 1 to 4: These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.
SC (Sequence control): It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
Data: It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
CRC (Cyclic redundancy check): It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

4. HIPERLAN: Architecture-Standards

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. Over time, names have changed and the former **HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK**. The current focus is on HiperLAN2, a standard that comprises many elements from ETSI's **BRAN (broadband radio access networks) and wireless ATM activities.**

HIPERLAN 1 as a wireless LAN supporting priorities and packet life time for data transfer at 25 MBPS, including forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms. HIPERLAN 1 should operate at 5GHz with a range of 50 m in buildings at 1 W transmit power.

Elimination-yield non-preemptive priority multiple access (EY-NPMA) is not only a complex acronym, but also the heart of the channel access providing priorities and different access schemes. EY-NPMA divides the medium access of different competing nodes into three phases:

Prioritization: Determine the highest priority of a data packet ready to be sent by competing nodes.

Contention: Eliminate all but one of the contenders, if more than one sender has the highest current priority.

Transmission: Finally, transmit the packet of the remaining node.

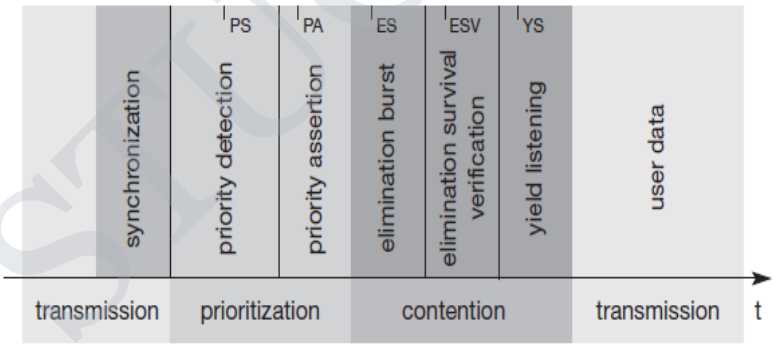


Figure Phases of the HIPERLAN 1 EY-NPMA access scheme

Yield phase:

During the yield phase, the remaining nodes only listen into the medium without sending any additional bursts. Again, time is divided into slots, this time called yield slots with a duration of IYS = 168 high rate bit-periods.

5. Bluetooth Architecture and Applications:

Bluetooth is connecting its mobile phones to other devices (e.g., laptops) without cables. Together with four other companies (IBM, Intel, Nokia, and Toshiba), it formed a SIG (Special Interest Group) in 1998 to develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios. The Bluetooth protocols let these devices find and connect to each other, an act called pairing, and securely transfer data.

Figure 4-34. Two piconets can be connected to form a scatternet.

The basic unit of a Bluetooth system is a **piconet**, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node that takes part in multiple piconets, as in Fig. An interconnected collection of piconets is called a **scatternet**.

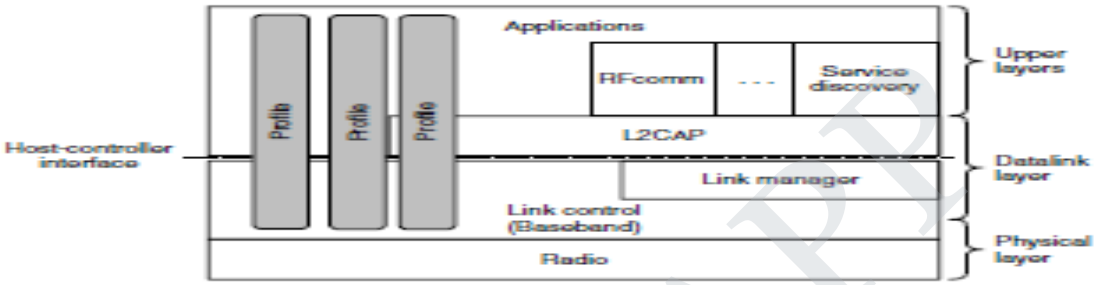
The reason for the master/slave design is that the designers intended to facilitate the implementation of complete Bluetooth chips for under $5. The consequence of this decision is that the slaves are fairly dumb, basically just doing whatever the master tells them to do. At its heart, a piconet is a centralized TDM system, with the master controlling the clock and determining which device gets to communicate in which time slot. All communication is between the master and a slave; direct slave-slave communication is not possible.

Bluetooth Protocol Stack:

The protocols in this group are designed to

- Allow devices to locate and connect.
- Carry audio and data traffic where audio traffic has higher priority.

- Support synchronous and asynchronous transmission for telephony grade voice communication.
- Manage physical and logical links between devices so that layers above and applications can pass data through connections.



The Bluetooth protocol architecture.

Baseband and radio layers:

The baseband layer is responsible for **searching other devices, assigning master and slave roles.** This layer also **controls Bluetooth unit's synchronization and transmission frequency hopping sequence.** It manages link between devices and determines packet types supported for synchronous and asynchronous traffic.

Logical link control and adaptation protocol layer (L2CAP):

- All data traffic is routed through this layer.
- This layer shields higher layers from details of lower layers.
- It segments larger packets from higher layers into smaller packets that can be easily handled by lower layers.
- It facilitates maintenance of desired grade of service in two peer devices.

Link manager layer (LML):

- It negotiates properties of Bluetooth air interface between communicating devices.
- These properties may be bandwidth allocation, support services of particular type, etc.
- This layer also supervises devices pairing.
- Device pairing generates and stores authentication key specific to a device

- It is also responsible for power control and may request adjustments in power levels.

Host Controller Interface (HCI):

The HCI allows higher layers of stack, including applications, to access the baseband, link manager, etc., through a single standard interface.

It serves the purpose of interoperability between host devices and Bluetooth modules.

RFCOMM layer:

It provides a virtual serial port for applications needed for scenarios like dial-up networking, etc.

This eliminates the use of cables.

Service Discovery protocol layer (SDP):

The SDP is a standard method for Bluetooth devices to discover and learn about the services offered by other device once a connection is established with it.

Bluetooth Applications:

- The Bluetooth is used in wireless head sets.
- Bluetooth is used to transfer files, images and MP3 or MP4 between cell phones.
- Bluetooth using in laptops and notebooks.
- It is used in PDAs (personal digital assistant) and printers.
- Connecting Wireless mouse and keyboards.
- Bluetooth using in data logging equipment data logging equipment that transmit data to a computer via Bluetooth technology.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Short range transmission of health sensor data from medical devices to mobile phone, set top box or dedicated tele health.

UNIT 4

MOBILE NETWORK LAYER

Mobile IP – DHCP – AdHoc– Proactive and Reactive Routing Protocols – Multicast Routing- Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security

1. Define Mobile IP.

Mobile IP is a standard protocol created by extending Internet Protocol (IP) to enable users to keep the same IP address while travelling from one network to a different network. Mobile IP = Mobility + Internet Protocol (IP)

2. Specify the goals of Mobile IP.

Allows mobile hosts to stay connected to the internet regardless of their location and without changing their IP address.

Enable packet transmission efficiently without any packet loss and disruptions in the presence of host and/or destination mobility.

3. What are the main requirements needed for mobile IP?

Compatibility
Transparency
Scalability and efficiency
Security

4. List out the various terminologies involved in Mobile IP.

a) Mobile Node
b) Home Network
c) Home Address
d) Foreign Agent
e) Correspondent Node
f) Care-of-Address
g) Tunnel
h) Foreign Network
i) Home Agent

5. What is encapsulation in Mobile IP.

Encapsulation refers to arranging a packet header and data and putting it into the data part of a new packet. Thus the encapsulated packet will contain the new destination address as “Address of COA” and the new source address as “Address of HA”.

6. What is multicast transmission?

In computer networking, **multicast** is group communication where data **transmission** is addressed to a group of destination computers simultaneously. **Multicast** can be one-to-many or many-to-many distribution. **Multicast** should not be confused with physical layer point-to-multipoint communication.

. Mobile IP:

Mobile IP is a communication protocol that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user's sessions or connections being dropped.

Requirements of Mobile IP:

- Transparency
- Scalability and Efficiency
- Security
- Compatibility

Terminologies:

Mobile Node (MN):

It is the hand-held communication device that the user caries e.g. Cell phone.

Home Network:

It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).

Home Agent (HA):

It is a router in home network to which the mobile node was originally connected

Home Address:

It is the permanent IP address assigned to the mobile node (within its home network).

Foreign Network:

It is the current network to which the mobile node is visiting (away from its home network).

Foreign Agent (FA):

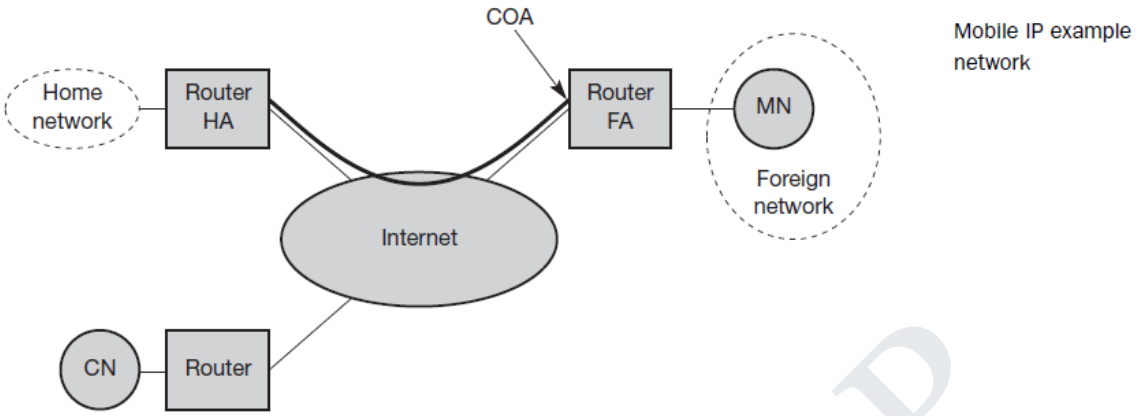
It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.

Correspondent Node (CN):

It is a device on the internet communicating to the mobile node.

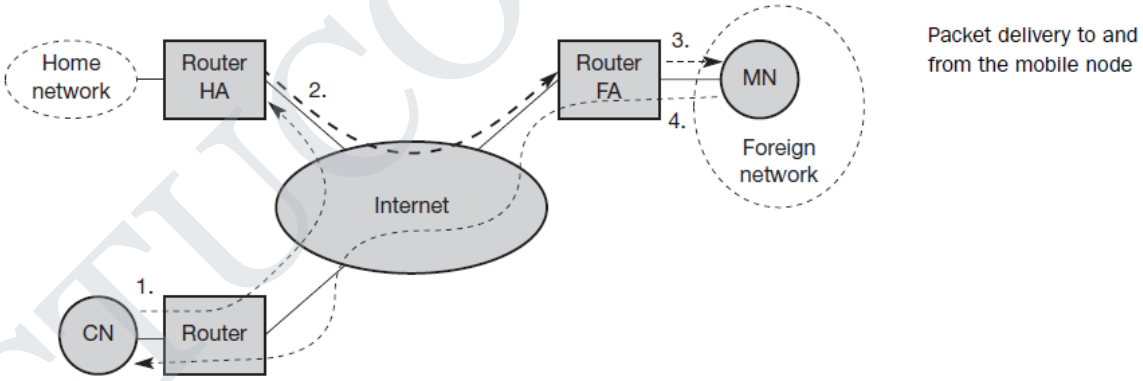
Care of Address (COA):

It is the temporary address used by a mobile node while it is moving away from its home network.



IP packet delivery:

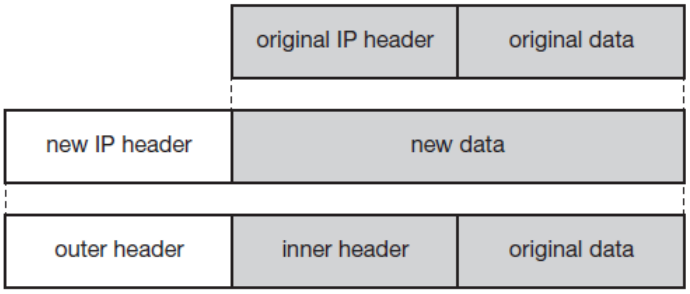
Figure illustrates packet delivery to and from the MN using the example network of Figure 8.1. A correspondent node CN wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of the MN. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN (step 1). This means that CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet.



The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination. The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node the remainder is in the fixed internet as usual. If CN were also a mobile node residing in a foreign network.

IP-in-IP encapsulation:

There are different ways of performing the encapsulation needed for the tunnel between HA and COA. Mandatory for mobile IP is IP-in-IP encapsulation as specified in RFC 2003



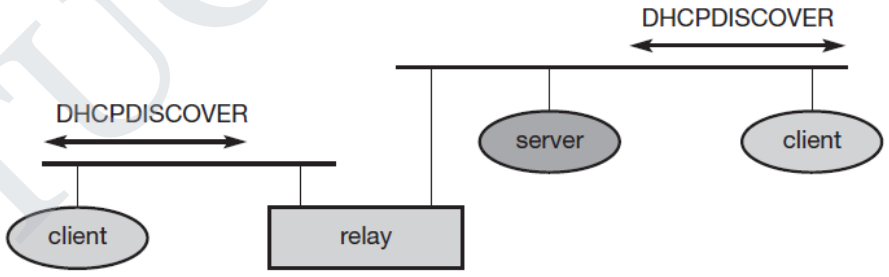
IP encapsulation

2. DHCP (Dynamic Host Configuration Protocol):

The **Dynamic Host Configuration Protocol (DHCP)** 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. While the basic DHCP mechanisms are quite simple, many options are available as described in RFC 2132. DHCP is based on a client/server model as shown in Figure. 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.

Figure
Basic DHCP configuration



Stages in DHCP:

1.DHCP discover message:

This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.

2. DHCP Offer message:

The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.

3. DHCP request message:

When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.

4. DHCP acknowledgement message:

In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

5. DHCP release:

A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

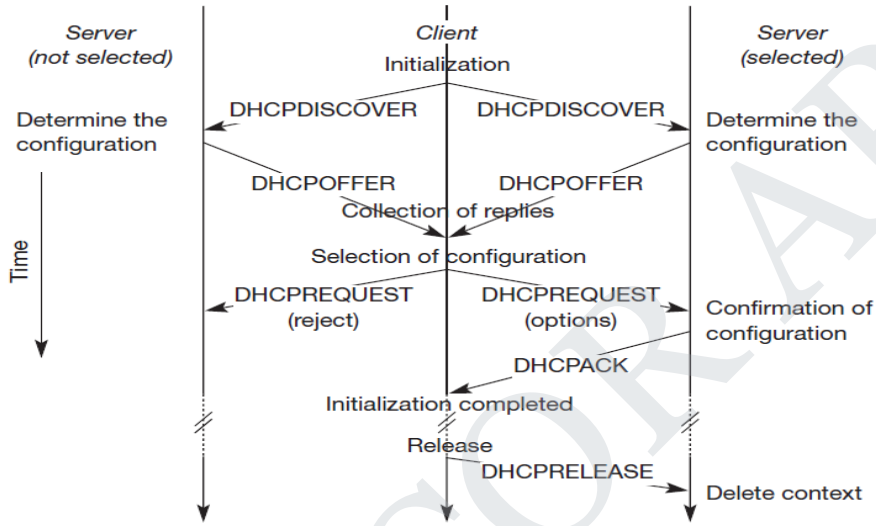


Figure 8.18 Client initialization via DHCP

Advantages of using DHCP:

- Centralized management of IP addresses.
- Ease of adding new clients to a network.
- Reuse of IP addresses reducing the total number of IP addresses that are required.
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.

Disadvantage of using DHCP:

- IP conflict can occur

UNIT 5

MOBILE TRANSPORT AND APPLICATION LAYER

Mobile TCP– WAP – Architecture – WDP – WTLS – WTP –WSP – WAE – WTA Architecture – WML

PART-A

1. What is WAP?

Wireless application protocol (WAP) is a common effort of many companies and organizations to set up a framework for wireless and mobile web access using many different transport systems. Eg. GSM, GPRS, UMTS.

2. What are the benefits of using WAP?

- Interoperable
- Scalable
- Efficient
- Security

3. Define WML.

WML (Wireless Markup Language), is a language that allows the text portions of Web pages to be presented on cellular telephones and personal digital assistants (PDAs) via wireless access. The Wireless Application Protocol works on top of standard data link protocols, such as Global System for Mobile communication, code-division multiple access, and Time Division Multiple Access, and provides a complete set of network communication programs comparable to and supportive of the Internet set of protocols.

4. Write about Synchronization Protocol.

A set of protocols and a markup language for synchronization of data in mobile scenarios is provided by the **SyncML (Synchronization Markup Language)** framework. **The synchronization protocol may run over HTTP, WSP, or the object exchange protocol OBEX**.

5. What are the different types of File System?

- Coda
- Little Work
- Ficus
- Mio-NFS

6.What is File System?

The general goal of a file system is to support efficient, transparent, and consistent access to files, no matter where the client requesting files or the server(s) offering files are located. Efficiency is of special importance

for wireless systems as the bandwidth is low so the protocol overhead and updating operations etc.

7.Define DDNS.

DDNS stands for Dynamic Domain Name System, It's a service that maps internet domain names to IP addresses. It's a DDNS service that lets you access your home computer from anywhere in the world.

8.What is Context- aware applications?

Context aware applications is used to identify the location of nodes, network devices and neighboring nodes and also retrieve the information about users , and what time of the day accessing the mobile network.

9.What is WCMP?

The wireless Control Message Protocol (WCMP) is used to provide the error handling mechanism for WDP. It contains control messages that resemble the ICMP messages for IPV4. it can be used for WDP nodes and gateways.

10. What are the different types of Security issues in mobile computing?

There are different kinds of issues within security like **confidentiality, integrity, availability, legitimacy, and accountability**.

PART-B

1. WAP(Wireless Application Protocol):

Wireless application protocol (WAP) is a common effort of many companies and organizations to set up a framework for wireless and mobile web access using many different transport systems. Eg. GSM, GPRS, UMTS.

The basic objectives of the WAP Forum is bring diverse internet content (e.g., web pages, push services) and other data services (e.g., stock quotes) to digital cellular phones and other wireless, mobile terminals (e.g., PDAs, laptops). Moreover, a protocol suite should enable global wireless communication across different wireless network technologies, e.g., GSM, CDPD, UMTS etc.

All solutions must be:

- **Interoperable**, i.e., allowing terminals and software from different vendors to communicate with networks from different providers.
- **scalable,** i.e., protocols and services should scale with customer needs and number of customers.
- **Efficient,** i.e., provision of QoS suited to the characteristics of the wireless and mobile networks.
- **Reliable,** i.e., provision of a consistent and predictable platform for deploying services.

● **Secure,** i.e., preservation of the integrity of user data, protection of devices and services from security problems.

WAP Architecture:

The following Figure 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. This comparison is often cited by the WAP Forum and it helps to understand the architecture. This comparison can be misleading as not all components and protocols shown at the same layer are comparable.

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 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.

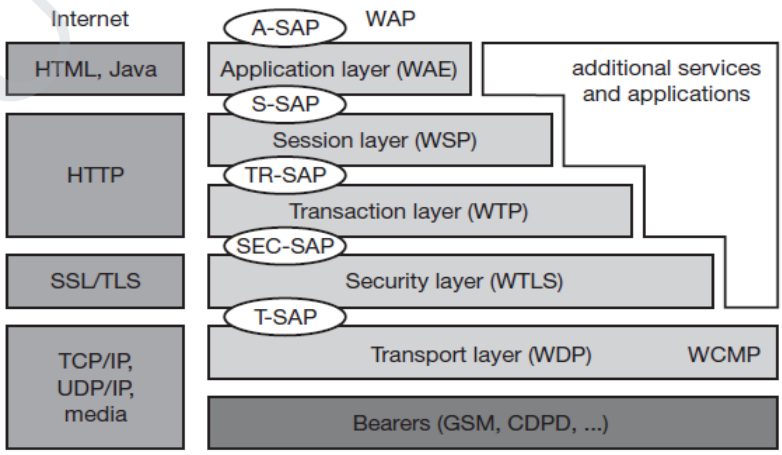


Figure Components and interface of the WAP 1.x architecture

The next higher layer, 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).

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.

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.

Finally the application layer with the **wireless application environment (WAE)** offers a framework for the integration of different www and mobile telephony applications.

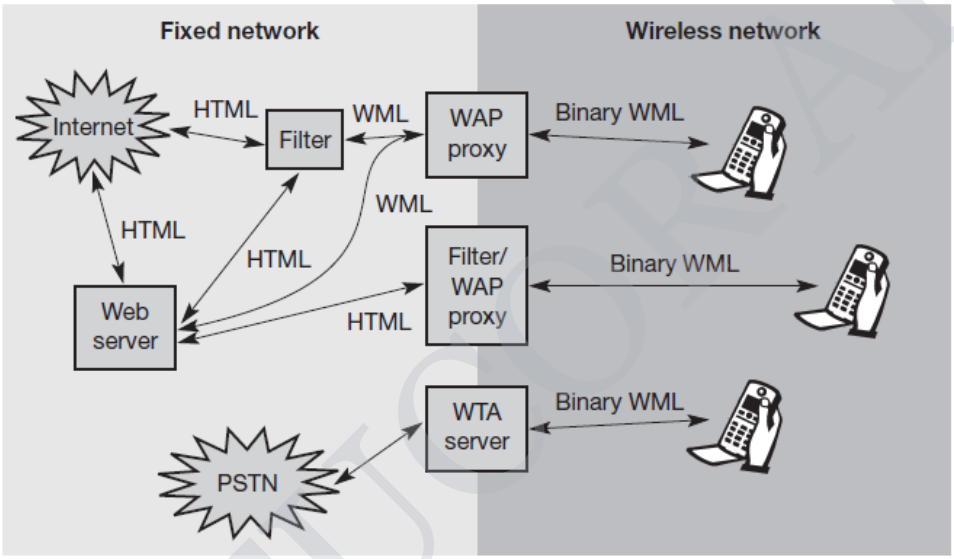


Figure : Examples for the integration of WAP components

The current www in the internet offers web pages with the help of HTML and web servers. To be able to browse these pages or additional pages with handheld devices, a **wireless markup language (WML)** has been defined in WAP. Special filters within the fixed network can now translate HTML into WML, web servers an already provide pages in WML, or the gateways between the fixed and wireless network can translate HTML into WML. WML is additionally converted into binary WML for more efficient transmission.

In a similar way, a special gateway can be implemented to access traditional telephony services via binary WML. This **wireless telephony application (WTA)** server translates, e.g., signaling of the telephone network (incoming call etc.) into WML events displayed at the handheld device.

2. DDNS (Dynamic Domain Name System):

DDNS stands for Dynamic Domain Name System, It's a service that maps internet domain names to IP addresses. It's a DDNS service that lets you access your home computer from anywhere in the world.

DDNS serves a similar purpose to the internet's Domain Name System (DNS) in that DDNS lets anyone hosting a web or FTP server advertise a public name to prospective users.

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like google.com or gmail.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

However, unlike **DNS which only works with static IP addresses**, **DDNS is designed to also support dynamic (changing) IP addresses**, such as those assigned by a DHCP server. That makes DDNS a good fit for home networks, which normally receive dynamic public IP addresses from their internet service provider.

How a DDNS Service Works:

To use DDNS, just sign up with a dynamic DNS provider and install their software on the host computer. The host computer is whichever computer is used as the server, be it a file server, web server, etc.

For example, if you have FTP software on your computer to turn that device into an FTP server, you'd install the DDNS application on that computer. That computer is the one that users will reach when they request your server, so it's the one that needs to always be updating the DDNS provider with its current IP address.

What the software does is monitors the dynamic IP address for changes. When the address changes (which it eventually will, by definition), the software contacts the DDNS service to update your account

with the new IP address.

This means that so long as the DDNS software is always running and can detect a change in the IP address, the DDNS name you have associated with your account will continue to direct visitors to the host server no matter how many times the IP address changes.

3.
4. Synchronization Protocol:

A set of protocols and a markup language for synchronization of data in mobile scenarios is provided by the **SyncML (Synchronization Markup Language)** framework.

The SyncML initiative is supported by companies like Ericsson, IBM, Motorola, Nokia, Openwave, Panasonic, Starfish, and Symbian. SyncML provides vendor independent mechanisms not only for synchronization of data, but also for the administration of devices and applications.

common standard for synchronization simplifies application design and usage of synchronization mechanisms. SyncML enhances servers and clients with sync server agents and sync client agents respectively. The agents execute the synchronization protocol. The synchronization protocol may run over HTTP, WSP, or the object exchange protocol OBEX. However, many more protocols such as SMTP or TCP/IP could be used. SyncML does not make many assumptions about the data structures. Each set of data must have a unique identifier. Clients and servers can use their individual identifiers for data sets. However, servers have to know the mapping between the identifiers. Clients and servers have to log changes and must be able to exchange these logs.

Several modes are specified for synchronization. Two-way synchronization exchanges change logs between server and client. If, for example, a client crashed and has lost all change information, a special slow synchronization can be used. This synchronization mode first transfers all data from the client to the server. The server then compares all data and sends the necessary changes back to the client. Several variants of one-way synchronization are available. In this case, only one party (client or server) is interested in change logs.

The messages exchanged for synchronization are based on XML. Tags have been specified to <add>, <copy>, <delete>, and <replace> data sets. Operations can be made <atomic> (i.e., either all or no change operations may be applied) or applied in a certain <sequence>. If a conflict occurs (e.g., the same data set has been changed on the client and the server) SyncML does not specify a conflict resolution strategy. Instead, several recommendations for conflict resolution are given. Data sets can be mixed, the client may override server changes (or vice versa), a duplicate of the data set can be generated, or a failure of synchronization is signaled. These examples show that SyncML has no general solution for the synchronization problem.

5. Context- aware applications:

Context aware applications is used to identify the location of nodes, network devices and neighboring nodes and also retrieve the information about users , and what time of the day accessing the mobile network.

Context awareness is the ability of a system or system component to gather information about its environment at any given time and adapt behaviors accordingly. Contextual or context-aware computing uses software and hardware to automatically collect and analyze data to guide responses.

Context includes any information that's relevant to a given entity, such as a person, a device or an application. As such, contextual information falls into a wide range of categories including time, location, device, identity, user, role, privilege level, activity, task, process and nearby devices/users.

Web browsers, cameras, microphones and Global Positioning Satellite (GPS) receivers and sensors are all potential sources of data for context-aware computing. A context-aware system may gather data through these and other sources and respond according to pre-established rules or through computational intelligence. Such a system may also base responses on assumptions about context. For user applications, context awareness can guide services and enable enhanced experiences including augmented reality, context-relevant information delivery and contextual marketing messages.

6. Analysis of existing wireless network:

Wireless networks represent a rapidly emerging area of growth and importance for providing ubiquitous networking connections. The common technologies can be classified into different categories according to the range of the service area. On a worldwide scale, telecommunication companies have been making significant progress in carrying voice and data traffic over their cellular networks; furthermore, the next generation infrastructure, under development all over the world, aims to provide higher bandwidth and better quality for multimedia traffic. In a metropolitan area, **WiMAX (IEEE 802.16) can provide users with high-speed broadband access to the Internet. In a local area, WiFi (IEEE 802.11)** enables users to establish wireless connections within a corporate or campus building. Moreover, in a personal area (often less than 10 meters), **Bluetooth (IEEE 802.15) can provide low-cost and short-range connectivity for portable devices.**

The focus of this dissertation is Wireless Local Area Networks (WLAN) based on IEEE 802.11a/b/g specifications. Compared with the current cellular networks, a WLAN system has much higher transmission rates and shorter transmission range; hence, it is suitable for home networking, small business, and large corporations and has been widely deployed since IEEE 802.11b first appeared in 1999. However, along with the popularity of WLAN, security is a serious concern because the wireless medium is open for public access within a certain range.

By driving a car along certain route through a district, people can discover the operating Access Points (APs), the corresponding Service Set Identifier (SSID), and even the physical locations of the APs, with only moderate equipment. Obviously these capabilities release sensitive information and unauthorized services to an outsider. Furthermore, if the discovered APs are not well-configured, the outsider is able to exploit bandwidth for free Internet access, steal confidential data for malicious usage, or install advanced attacks from this open base. Even worse, the legitimate user may be unaware of these activities because the outsider can physically stay inside his car along the road or in the parking lot. These dangers impose necessary requirements on the security of WLAN implementations.

7. Security in Wireless Network :

In a general network system, security has different contexts depending on different applications, among which the essential requirements are data **confidentiality and integrity, authentication, and availability.**

Data Confidentiality and Integrity

The network Must provide strong data confidentiality, integrity, and replay protection for every transmitted message. Data confidentiality and integrity, helping build a secure channel for the user to communicate in an insecure environment, mean that only the communicating users are able to understand the received messages, generate or modify valid messages. Furthermore, replayed messages should be recognized and discarded even though they may pass the integrity check. These requirements could be satisfied by well-designed cryptographic functions and appropriate replay protection techniques.

Mutual Authentication

The network Must provide mutual authentication, which means that the communicating peers authenticate each other's identity. If required, the authentication process should also combine with key generation, distribution and management to provide secret keys for the cryptographic function. Based on the authentication results, flexible authorization and access control policies could be deployed to restrict the privilege of users.

Availability:

Availability is a form of robustness, which is another important category of security requirements. The network should be able to prevent an adversary from shutting down the connectivity for a legitimate individual or the entire system. In other words, Denial of Service (DoS) attacks should be eliminated, or at least mitigated.

****