		L	T	P	C
17BECS602B	**Mobile and Pervasive Computing**	**3**	**0**	**0**	**3**

COURSE OBJECTIVES:

- Understand the advanced concepts of wireless mobile networks
- Apply transactions for complex model
- Explore the modern design structures of pervasive computing
- Analyze various advanced mobile network models

LEARNING OUTCOMES:

- Outline the basic problems, performance requirements of pervasive computing applications and the trends of pervasive computing and its impacts on future computing applications and society.
- Analyze and compare the performance of different data dissemination techniques and algorithms for mobile real-time applications
- Analyze the performance of different sensor data management and routing algorithms for sensor networks.
- Develop an attitude to propose solutions with comparisons for problems related to pervasive computing system through investigation.

UNIT I Introduction to Mobile Computing (9)

Mobility of bits and bytes – Wireless the beginning – Mobile computing- Dialogue control-Networks – Middleware and gateways- Application and services- Developing mobile computing applications-Security- Standards- Players in wireless space- Architecture for mobile computing-Three tier architecture- Design considerations-Mobile computing through internet-Making existing applications mobile enabled-Developing IVR application.

UNIT II Mobile Technologies (9)

Emerging technologies: Bluetooth-Radio frequency identification- Wireless broadband-Mobile IP-Internet protocol version 6-Java card- GSM- Short message services- General packet radio services: Packet data network Architecture-Operations-Data services-Application for GPRS-Limitations of GPRS-Wireless application protocol CDMA and 3G.

UNIT III Mobile Networking Wireless (9)

LAN advantage-Standards-Architecture-Mobility-Deploying-Mobile Ad Hoc networks and sensor networks-Security- Wi Fi verses 3G-Internet networks and interworking: Fundamentals of call processing – Intelligence in the networks-SS #7 signaling-IN conceptual model-Soft switch-Programmable networks-Client programming.

UNIT IV Introduction to Pervasive Computing (9)

Introduction to pervasive computing: Scenarios–Roaming environment-Pervasive computing infrastructure Personalized services – Pervasive computing market- m-business- Applications examples-Hardware - Human - Machine interfaces biometrics and Operating systems-Java for pervasive devices.

UNIT V Pervasive Computing Application Device (9)

Connectivity – Protocols, security and device management - Pervasive web application architecture
– Transcoding –Client authentication via internet- WAP and beyond - Voice technology: Speech application–Personal digital assistants: Device- Operating systems-Characteristics-Software components-Standards-Mobile applications.

Total Hours - 45

TEXT BOOKS:

1. Asoke K Talukder and Poopa R Yavagal, Mobile Computing,Tata McGraw-Hill,2nd edition,2010.
2. Jochen Buekhardt, Horst Henn, Stefan Hepper, Klaus Rintdorff and Thomas Schack, Pervasive Computing:Technology and architecture of mobile internet applications,Pearson Education,2009.

REFERENCES:

1. Reza B Fat and Roy T Fielding, Mobile Computing Principles, Cambridge University Press, 2010.
2. Hansmann Uwe, Merk Lothar and Nicklous Mart, Pervasive Computing: The Mobile World, Springer Professional, 2011.
3. Chimay J, Anumba and Xiangyu Wang, Mobile and Pervasive Computing, Springer Professional, 2012.

KARPAGAM ACADEMY OF HIGHER EDUCATION

Faculty of Engineering

Department of Computer Science and Engineering

Lecture Plan

Subject Name: Mobile and Pervasive Computing **Subject Code: 17BECS602B**

S.No	Topic Name	No.of Periods	Supporting Materials	Teaching Aids
	UNIT- I Introduction to Mobile Computing			
1	Mobility of bits and bytes	1	R[1]-1	BB
2	Wireless the beginning – Mobile computing	1	R[1]-1	BB
3	Dialogue control-Networks- Middleware and gateways	1	R[1]-5	PPT
4	Application and services- Developing mobile computing applications	1	R[1]-6	PPT
5	Uninformed search strategies	1	R[1]-6	PPT
6	Security- Standards- Players in wireless space	1	T[1]-95	PPT
7	Architecture for mobile computing	1	T[1]-95	PPT
8	Three tier architecture- Design considerations	1	T[1]-68	BB
9	Mobile computing through internet	1	Web	PPT
10	Making existing applications mobile enabled	1	T[1]-12	BB
11	Developing IVR application	1	Web	BB
Total		**11**		
	UNIT- II Mobile Technologies			
12	Emerging technologies: Bluetooth-Radio frequency identification	1	T[1]-200	PPT
13	Wireless broadband-Mobile IP	1	web	PPT
14	Internet protocol version 6-Java card	1	T[1] 201	BB
15	GSM- Short message services	1	T[1]214	PPT
16	General packet radio services: Packet data network Architecture	1	T[1]214	PPT
17	Operations-Data services	1	T[1]218	PPT
18	Application for GPRS	1	R[1]218	PPT
19	Limitations of GPRS	1	R[1]218	PPT
20	Wireless application protocol CDMA and 3G	1	R[1]221	BB
21	Games that include an element of chance	1	R[1]221	PPT
Total		**10**		
	UNIT- III Mobile Networking Wireless			

22	LAN advantage	1	web	PPT
23	Standards-Architecture	1	web	PPT
24	Mobility-Deploying	1	web	PPT
25	Mobile Ad Hoc networks	1	T[1]-488	BB
26	Sensor networks-Security	1	T[1]-193	PPT
27	Wi Fi verses 3G-Internet networks and interworking: Fundamentals of call processing	1	T[1]-266	BB
28	Intelligence in the networks	1	T[1]-305	PPT
29	SS #7 signaling- IN conceptual model	1	T[1]-343	BB
30	switch-Programmable networks	1	web	PPT
31	Client programming	1	web	PPT
Total		**10**		
	UNIT- IV Introduction to Pervasive Computing			
32	Introduction to pervasive computing	1	T[2]-139	PPT
33	Scenarios	1	T[2]-139	PPT
34	Roaming environment	1	T[1]-140	PPT
35	Pervasive computing infrastructure Personalized services	1	T[2]-152	BB
36	Pervasive computing market	1	T[2]-159	PPT
37	m-business- Applications examples	1	T[2]-162	BB
38	Hardware - Human	1	T[2]-163	PPT
39	Machine interfaces biometrics	1	T[2]-133	PPT
40	Operating systems-Java for pervasive devices.	1	web	PPT
41	Tutorial: Application Development	1	T[2]-133	BB
Total		**10**		
	UNIT- V Pervasive Computing Application Device			
42	Connectivity – Protocols	1	T[2]-248	PPT
43	Security and device management	1	T[2]-465	BB
44	Pervasive web application architecture	1	T[2]-465	BB
45	Transcoding –Client authentication via internet	1	T[2]-255	PPT
46	Voice technology: Speech application	1	T[2]-248	PPT
47	Personal digital assistants: Device	1	T[1]-1087	PPT
48	Operating systems	1	T[1]-1087	PPT
49	Characteristics-Software components	1	T[1]-690	BB
50	Mobile applications	1	T[1]-690	PPT
51	Revision	1	T[1]-752	BB
52	**Discussion on Previous University Question Papers**			
Total		**10**		
	Total Hours	**52**		

TEXT BOOKS

S.NO	Title of the book			Year of publication
1	Asoke K Talukder and Poopa R Yavagal, Mobile Computing,Tata McGraw-Hill,2nd edition.			2010
2	Jochen Buekhardt, Horst Henn, Stefan Hepper, Klaus Rintdorff and Thomas Schack, Pervasive Computing:Technology and architecture of mobile internet applications,Pearson Education.			2009

REFERNCE BOOKS

S.NO	Title of the book			Year of publication
1	Reza B Fat and Roy T Fielding, Mobile Computing Principles, Cambridge University Press.			2010
2	Hansmann Uwe, Merk Lothar and Nicklous Mart, Pervasive Computing: The Mobile World, Springer Professional.			2011
3	Chimay J, Anumba and Xiangyu Wang, Mobile and Pervasive Computing, Springer Professional			2012

WEBSITES

1. https://www.javatpoint.com/Artificial intelligence-tutorial
2. https://nptel.ac.in/content/syllabus_pdf/106105131.pdf

UNIT 1 - MOBILE NETWORKS

PART A

1. What are the advantages of GSM?(Nov 2014)
   - Localization and calling
   - Handover
   - Security
     - Authentication, confidentiality, Anonymity.
2. What are the four types of handover available in GSM? (Nov 2014)
   - Intra-cell handover
   - Inter-cell, intra-BSC handover
   - Inter-BSC, Intra-MSC handover
   - Inter MSC handover
3. What are the types of services in GSM?(May 2014)
   - Bearer Services
   - Tele Services
   - Supplementary services
4. What are the disadvantages of Cellular systems? (May 2014)
   Infrastructure needed, Handover needed and Frequency planning.
5. What are the different types of access mechanisms? (Nov 2013)
   - Space Division Multiple Access(SDMA)
   - Frequency Division Multiple Access(FDMA)
   - Time Division Multiple Access(TDMA)
   - Code Division Multiplexing (CDM).
6. How is authentication done in GSM network?(Nov 2013)
   The AUC is a processor system; it performs the "authentication" function. It will normally be co-located with the Home Location Register (HLR) as it will be required to continuously access and update, as necessary, the system subscriber records. The AUC/HLR centre can be co-located with the MSC or located remote from the MSC. The authentication process will usually take place each time the subscriber "initializes" on the system.
7. What does the Mobility Management (MM) layer do? (May/June 2013)
   The main function of the Mobility Management sub layer is to support the mobility of user terminals, such as informing the network of its present location and providing user identity confidentiality. A further function of the MM sub layer is to provide connection management services to the different entities of the upper Connection Management (CM) sub layer.
8. What is called burst and normal burst?
   Data is transmitted in small portions called bursts, normal burst are used for data transmission inside a slot (user and signalling data).
9. What are the basic groups of logical channels?
   GSM specifies 2 basic groups: Traffic channels and Control channels.
10. What is Network and Switching subsystem?
    The heart of the GSM is formed by the Network and Switching System (NSS). NSS consists of the following switches and databases:
    • Mobile Services switching center (MSC)
    • Home Location register (HLR)
    • Visitor Location Register (VLR)
11. What are the advantages of cellular systems?
    Higher capacity, less transmission power, Local interface only and Robustness.
12. What is guard space?
    Guard spaces are needed to avoid frequency band overlapping is also called channel interference.
13. What is hopping sequence?
    Transmitter and receiver stay on one of these channels FDM and TDM. The pattern of channel usage is called the hopping sequence.
14. What is BCA?
    In the case of a heavy load in one cell and a light load in a neighbouring cell, for instance it could make sense to borrow frequencies. Cells with more traffic are dynamically allotted more frequencies. This scheme is

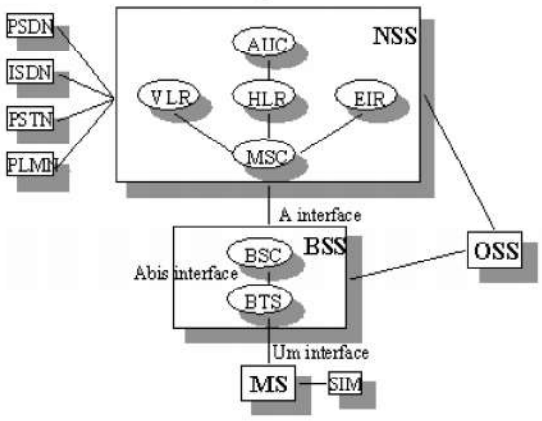
known as Borrowing channel Allocation (BCA).

15. How does near and far effect influence CDMA? What are counter measurements?
    The near and far effect is a server problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength. Precise power control is needed to receive all senders with the same strength at a receiver.
16. What is Roaming?
    Changing of VLR's with uninterrupted availability of all services is called Roaming .It can take place within the network of one provider, between two providers in one country, also between different providers in different countries.
17. Define FCA and DCA.
    Allocating a fixed frequencies for a channel is called as Fixed channel Allocation (FCA). In Dynamic Channel Allocation (DCA) scheme frequencies can only be borrowed, but it is also possible to freely allocate frequencies to cells. With dynamic assignment of frequencies to cells, the danger of the interference with cells with same frequency exists. Thus the borrowed frequencies in the surroundings cells can be blocked.
18. What limits the number of user in TDM and FDM compared to CDM?
    The code space is huge compared to the frequency space and time space. Because of the limited time space and frequency space, the number of user in TDM and FDM are limited.
19. What are the main benefits of a spread spectrum?
    The main benefit of spread spectrum is the resistance to narrow band interference. The spread spectrum converts the narrow band into broad band signal. The energy needed to transmit the signal is the same, but it is now spread over a large frequency range. Thus the power level of the signal can be much lower than that of the original narrowband signal.
20. What is authentication centre?
    As the radio interface and mobile stations are particularly vulnerable a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
21. What is browsing channel allocation and fixed channel allocation?
    Cells with more traffic are dynamically allotted more frequencies. This scheme is known as browsing channel allocation, while the first fixed scheme is called fixed channel allocation.
22. What is dwell time?
    The time spend on a channel with a certain frequency is called the dwell time.
23. What is a Handover?
    A single cell do not cover the whole service area. The process of transferring an ongoing call or data session from one channel connected to the core network to another channel.
24. What is the use of Phase Lock Loop (PLL)?
    To receive the signal correctly, the receiver must synchronize in frequency and phase with the transmitter.
25. What are the 3 fundamental propagation behaviors depending on their frequency?
    Ground Wave, Sky Wave and Line of Sight.

PART-B

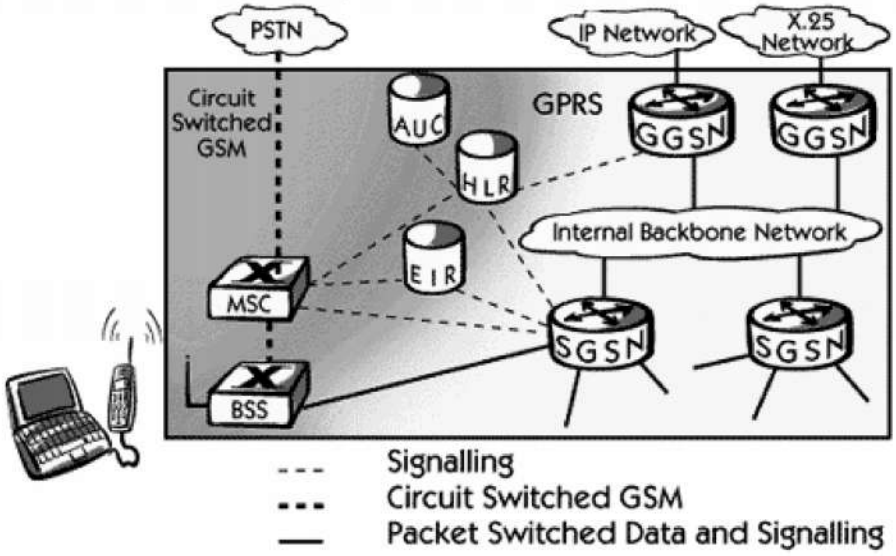
1. Explain the architecture of GSM in detail.(May-2012,Nov-2011,Nov-2012, May/June 2014, Nov/Dec 2014)
   GSM network can be divided into four main parts:
   - The Mobile Station (MS).
   - The Base Station Subsystem (BSS).
   - The Network and Switching Subsystem (NSS).
   - The Operation and Support Subsystem (OSS).

The architecture of the GSM network is presented below



2. Explain the architecture of GPRS in detail.(Nov-2011,May/June 2014, Nov/Dec 2014)

GPRS is a data network that overlays a second-generation GSM network. This data overlay network provides packet data transport at rates from 9.6 to 171 kbps. Additionally, multiple users can share the same air-interface resources simultaneously.



3. Explain connection establishment and frequency allocation in GSM. (Nov/Dec 2013)

One of the main features of GSM system is the automatic, worldwide localization of it's users. The GSM system always knows where a user is currently located, and the same phone number is valid worldwide. To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off. The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes. Changing VLRs with uninterrupted availability of all services is also called roaming. Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

To locate an MS and to address the MS, several numbers are needed:

MSISDN (Mobile Station International ISDN Number)16. The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS. The MSISDN follows the E.164, this standard is also used in fixed ISDN networks.

IMSI (International Mobile Subscriber Identity). GSM uses the IMSI for internal unique identification of a subscriber.

TMSI (Temporary Mobile Subscriber Identity). To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the 4 byte TMSI for local subscriber identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.

MSRN (Mobile Station [Subscriber] Roaming Number)17. This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR. The MSRN is comprised of the current **VCC** (Visitor Country Code), the VNDC (Visitor National Destination Code) and the identification of the current MSC together with the subscriber number, hence the MSRN is essential to help the HLR to find a subscriber for an incoming call.

All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station. The following scenarios below shows a MTC (Mobile Terminate Call) and a MOC (Mobile Originated Call).

4. Explain the Localization, calling and handover in GSM. (May/June 2013, 2014)

One of the main features of GSM system is the automatic, worldwide localization of it's users. The GSM system always knows where a user is currently located, and the same phone number is valid worldwide. To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off. The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes. Changing VLRs with uninterrupted availability of all services is also called roaming. Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

To locate an MS and to address the MS, several numbers are needed:

MSISDN (Mobile Station International ISDN Number)16. The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS. The MSISDN follows the E.164, this standard is also used in fixed ISDN networks.

IMSI (International Mobile Subscriber Identity). GSM uses the IMSI for internal unique identification of a subscriber.

TMSI (Temporary Mobile Subscriber Identity). To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the 4 byte TMSI for local subscriber identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.

MSRN (Mobile Station [Subscriber] Roaming Number)17. This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR. The MSRN is comprised of the current **VCC** (Visitor Country Code), the VNDC (Visitor National Destination Code) and the identification of the current MSC together with the subscriber number, hence the MSRN is essential to help the HLR to find a subscriber for an incoming call.

All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station. The following scenarios below shows a MTC (Mobile Terminate Call) and a MOC (Mobile Originated Call).

5. Explain the operations of cellular system. (Nov/Dec 2013)

A **cellular network** or **mobile network** is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell uses a different set of frequencies from neighbouring cells, to avoid interference and provide guaranteed bandwidth within each cell.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Cellular networks offer a number of advantages over alternative solutions:

flexible enough to use the features and functions of almost all public and private networks

- increased capacity
- reduced power use
- larger coverage area
- reduced interference from other signals

6. Explain about Mobility management.

Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

Mobility Management- as a mobile station moves from one area to another, mobility management functions are used to track its location within each PLMN. SGSNs communicate with each other and update the user

location. The mobile station's profiles are preserved in the VLRs that are accessible to SGSNs via the local MSC (mobile services switching centre). A logical link is established and maintained between the mobile station and the SGSN at each PLMN. At the end of transmission or when a mobile station moves out of the area of a specific SGSN, the logical link is released and the resources associated with it can be reallocated.

7. Explain the Mobile services in GSM?

GSM Permits the integration of different voice and data services and the interworking with existing networks.

3 kinds of services

- Bearer Services- It permits transparent and non-transparent, Synchronous or asynchronous data transmission. Transparent bearer services only use the functions of the physical layer to transmit data. on-Transparent bearer services use protocol of layers two and three to implement error correction and flow control.
- Tele Services- GSM mainly focuses on voice-oriented tele services.Thes comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN. Another service offered by GSM is **Emergency number**. Also provides Short message services.
- Supplementary Services- These services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user identification, Call redirection, or forwarding of on-going calls. Closed user groups (CUG) and multi party communication may be available.

8. How is data routing done in GPRS? In what aspect it data routing different from voice routing? State its limitations and applications. (Nov/Dec – 2013)

Routing and Data Transfer - once a mobile station begins data transmission, routing is performed by the GSNs on a hop-by-hop basis through the mobile network using the destination address in the message header. Routing tables are maintained by the GSNs utilizing the GTP layer which may carry out address translation and mapping functions to convert the external PDN (public data network) addresses to an address that is usable for routing within PLMNs. The data itself will go through several transformations as it travels through the network. Depending on the destination PDN, the data can be:

Forwarded - using the relay function, to go from one node to the other in the route

Tunnelled - to transfer data from one PLMN to another

Compressed - to use the radio path in an efficient manner (compression algorithms may be used for manufacturers to differentiate themselves, however, they may face interoperability issues in heterogeneous networks)

Encrypted - to protect the mobile station from eavesdropping (encryption algorithms can also be used as a differentiating factor).

Mobility Management- as a mobile station moves from one area to another, mobility management functions are used to track its location within each PLMN. SGSNs communicate with each other and update the user location. The mobile station's profiles are preserved in the VLRs that are accessible to SGSNs via the local MSC (mobile services switching centre). A logical link is established and maintained between the mobile station and the SGSN at each PLMN. At the end of transmission or when a mobile station moves out of the area of a specific SGSN, the logical link is released and the resources associated with it can be reallocated.

Applications:

Still images

Moving images

Web browsing

Audio reports

9. Explain in detail the need for a specialized MAC.

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is a SOHO router, for which the ISP grants access to only one MAC address (used previously to inserting the router) so the router

must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.

10. Explain about spread aloha multiple accesses in CDMA.
    Advantage to using a single code for all transmitters in a CDMA network, esp. for small cell sizes and multiple access satellite apps
    - Choice of a multiple-access protocol depends on traffic characteristics and state of the technology at deployment time:
    - DAMA (demand assigned multiple access): users request on a separate control channel; request protocol introduces delay and just moves the multiple-access problem to the (lower-bandwidth) request channel
    - DAMA w/random access: e.g. INMARSAT uses pure ALOHA for request channel. OK since allocation tends to be long-lived; no good if transmissions are bursty or short-lived
    - Multiple access protocols
    - **Slotted or pure ALOHA**. Efficiency (r): eff. channel capacity divided by capacity of a continuous channel with same power & bandwidth. For ALOHA, r=.18, asymptotically optimal for the special case of small values of throughput and S/N ratio.
    - **Spread spectrum**: max channel capacity in bits per Nyquist sample: C = .5 log (1+P/N) based on Shannon & Nyquist relations. "Spread spectrum" means C << 1.
    - **CDMA.** Multiply channel signals by orthogonal set of spreading signals; multiply by cx conjugate at receiver. Requires multiple receivers at CDMA BS to demodulate received signal.
    - **Qualcomm CDMA (IS-95 std)**. Spreading code is dynamically assigned via separate ALOHA channel when call request is made. Up to 64 codes can be active at once.
    - We can choose same spreading code for all CDMA users and the channel will still have multiple-access capability (spread ALOHA):
    - Each sub channel's bits will be offset by a constant amount *g* from the previous sub channel's bits within the frame
    - With *k* sub channels, prob. that 2 bits will not overlap is (1-1/*g*)^*k*; then total traffic $G = k/g$.
    - Get the noise-immunity of spread-spectrum with the nice queuing properties of slotted ALOHA.
    - Previous studies: no compelling evidence that there is a clear advantage for multiple-code CDMA systems, despite their complexity

UNIT 2 WIRELESS NETWORKS

PART-A

1. What are the design goals of 802.11? (Nov 2014) (May 2014)
    - To deliver services in wired networks, to achieve high throughput
    - To achieve highly reliable data delivery
    - To achieve continuous network connection
2. What are the three low power states provided by the Bluetooth? (Nov 2014)
    1. Sniff state 2. Hold state 3. Park State.
3. Mention the elements of Bluetooth core protocols? (May 2014)
    - Link Manager protocol
    - Logical link control and adaptation protocol(L2CAP)
    - Service discovery protocol
4. How does a new Bluetooth device discover a Bluetooth network? (Nov 2013)
    Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz[2]) from fixed and mobile devices, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.
5. How is power conservation achieved in HIPERLAN? (Nov 2013)
    In Hiper lan usage of batteries requires power conservation management functions. To switch off the transceiver when carrier sensing is not needed! Two state are defined, sleep state: In this state MT cannot transmit and receive packets (invoked periodically, awake state: In this state MT may perform all operations.

6. Distinguish between Wi Fi and Wi Max? (May/June 2013)
   Wifi : Generally the most common usage of Wi fi technology is for lap top users to gain internet access in locations such as airports, coffee shops, and so on.It can be used to help consumers in their pursuit of work – based or recreational internet usage.
   Wi Max: It provides a higher speed wireless internet access, it can be running at a speed up to 70M, three times as faster as 3G networks. It provides the last mile of internet access; it can connect WiFi hotspots to the internet and provide a wireless alternative to cables and DSL.
7. What do you mean by Bluetooth?(Nov-2012)
   Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating PAN with high levels of security.
8. What are the services of IEEE 802.11?(May-2012)
   Station services: authentication, de-authentication, privacy, delivery of data Distribution Services (A thin layer between MAC and LLC sub layer) Association, disassociation, re association distribution, Integration.
9. What is Hiper Lan? (May/June 2013)
   HiperLAN (High Performance Radio LAN) is a Wireless LAN standard. It is a European alternative for the IEEE 802.11 standards (the IEEE is an international organization). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the BRAN project (Broadband Radio Access Networks). The HiperLAN standard family has four different versions.
10. Define Moblie Adhoc Network.(Nov-2012)
    A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.
11. What do you mean by Wimax?
    WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and mobile Internet access. The current WiMAX revision provides up to 40 MB with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds. The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.
12. What do you mean by Wifi?
    Wi-Fi is a trademark of the Wi-Fi Alliance. A Wi-Fi enabled device such as a personal computer, video game console, smart phone, and digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access points — called hotspots when offering public access — generally comprises an area the size of a few rooms but may be expanded to cover many square miles, depending on the number of access points with overlapping coverage.
13. What is PAN?
    A personal area network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body. The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).
14. List the applications of Mobile Adhoc Network
    - Environmental monitoring -Traffic, habitat, security
    - Industrial sensing and diagnostics-Manufacturing, supply chains
    - Context-aware computing-Intelligent homes
    - Military applications: Multi-target tracking
    - Infrastructure protection: Power grids
15. Explain the Problems with Wireless Networks
    - Operates in a less controlled environment, so is more susceptible to interference, signal loss, noise, and eavesdropping.
    - Generally, wireless facilities have lower data rates than guided facilities.
    - Frequencies can be more easily reused with guided media than with wireless media.
16. Why 802.11a?
    - Greater bandwidth (54Mb)
    - Less potential interference (5GHz)
    - More non-overlapping channels

17. Explain WLL services

Desirable:

- Wireless feature should be transparent
- Wire line Custom features

Other:

- Business related
- Call transfers
- Conference calling
- Calling cards, coin phones
- V.29 (9600bps)ISDN (64kbps)

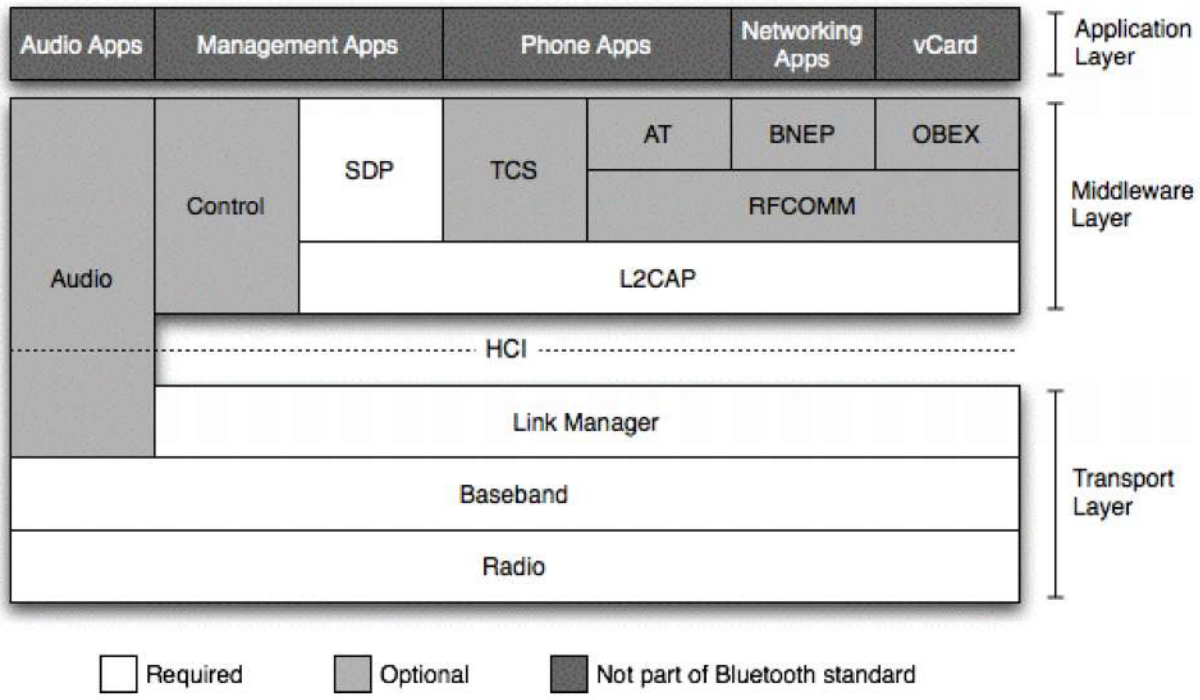
18. Explain the AMPS Components?
    - Mobile Units contains a modem that can switch between many frequencies identification numbers: electronic serial number, system ID number, mobile ID number
    - Base Transceiver full-duplex communication with the mobile
    - Mobile Switching Center
19. What are the components of the IEEE 802.11?
    Station, BSS - Basic Service Set, ESS - Extended Service Set, DS – Distribution System.
20. What is MSDU?
    MAC Service Data Unit (MSDU): Data Frame passed between user & MAC.
21. What is PLCP?
    PLCP Packet (PL CP_PDU): Data Packet passed from PHY to PHY over the Wireless Medium.
22. What is WLL?
    WLL is a system that connects subscribe to the local telephone station wirelessly.
23. What are all the parts of M-QoS?
    - Wired QoS
    - Wireless QoS
    - Handover QoS
24. What are all the modes that HiperLAN2 can operate?
    a. Centralized mode b. Direct mode.
25. What is Service Discovery protocol(SDP)?
    It defines only the discovery of services, not their usage. Discovered services can be cached and gradual discovery is possible. Devices that want to offer a service have to install an SDP server. For all other devices SDP client is sufficient.

PART –B

1. Explain the major concept of IEEE 802.11 standard. (Nov 2011,May-2012,Nov 2012,May/June- 2013, Nov/Dec 2013, May/June 2014, Nov/Dec 2014)
   The 802.11 family consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11a was the first widely accepted one, followed by 802.11b and 802.11g. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.
   802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap - see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.
2. Explain MAC layer of Bluetooth. (Nov/Dec 2013, 2014, May/June 2014)
   Each piconet has a unique frequency hopping sequence. The sequence is determined by the Bluetooth Device Address of the master of the piconet. Since different piconets have different hopping sequence, they can communicate without interfering with each other, when the number of adjacent piconets is small. In typical office environment, up to 10 overlapped piconets can work very well with little impact on one another. The

channel is time divided to slots of length 625 M S. Each packet can occupy 1, 3 or 5 slots. The hopping frequency keeps constant within a packet. The master uses the odd-numbered slots to transmit packets and the slaves use the even numbered slots. Duplex between master and slaves is achieved by time division. One slave is only allowed to send packet to the master if the preceding packet is addressed to it. So this is a centralized TDD scheme totally controlled by the master unit.

3. Draw the Bluetooth Protocol and explain. (May/June 2014)
Wireless data exchange standard Bluetooth uses a variety of protocols. Core protocols are defined by the trade organization Bluetooth SIG. Additional protocols have been adopted from other standards bodies. This article gives an overview of the core protocols and those adopted protocols that are widely used.
The Bluetooth protocol stack is split in two parts: a "controller stack" containing the timing critical radio interface, and a "host stack" dealing with high level data. The controller stack is generally implemented in a low cost silicon device containing the Bluetooth radio and a microprocessor. The host stack is generally implemented as part of an operating system, or as an installable package on top of an operating system. For integrated devices such as Bluetooth headsets, the host stack and controller stack can be run on the same microprocessor to reduce mass production costs; this is known as a *hostless* system.



4. Explain briefly about wireless networks (May/June 2014).
Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.
5. Explain the concept of Wimax. (Nov 2011, Nov/Dec 2014).
WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations. The name "WiMAX" was created by the **WiMAX Forum**, which was formed in June 2001 to promote conformity and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.
6. Explain the concept of Wifi.(Nov 2011)
Wi-Fi (also spelled *Wifi* or *WiFi*) is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over acomputer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".

Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" trademark.

7. Compare Hiper Lan and Bluetooth.(May 2012).
   Wireless LAN technology is about to undergo dramatic advances, and the number and types of applications that wireless LANs will enable will sprout like weeds. Two technologies pushing the rapid evolution of this market are High Performance Radio LAN (HiperLAN) and Bluetooth (named after a 10th century Danish king).
   HiperLAN, which comes in several flavors, is a next-generation, high-speed wireless LAN technology that offers end users throughputs as high as 25Mbits/sec. This article will focus on one particular version: HiperLAN2. Bluetooth is more of a personal productivity wireless technology, with a range of about 10 meters. It is designed to eliminate all those pesky cables that hamper the use of high-tech gadgetry. Both technologies are huge innovations in applying state-of-the-art methods to practical ends.
   Whereas HiperLAN2 is a powerful LAN technology, Bluetooth connects devices in a user's immediate vicinity.
   Bluetooth promises to be an industry force. Its major selling points are its extremely low cost (it may eventually go as low as $5 per device) and its impending ubiquity (huge numbers of devices will soon incorporate it).
   In addition, Bluetooth enjoys wide industry support from approximately 1,400 companies that now belong to the Bluetooth Special Interest Group (SIG). And unlike most other wireless technologies, Bluetooth does not have direct competition (other than cables). The Bluetooth specification could become an official standard if adopted by IEEE 802.15, which seeks to develop a standard for Personal Area Networks (PANs).
8. Explain about Wireless PAN.
   Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure
9. Explain the concept which is used in hotspot and wifi card in wifi system.
   A device that can use Wi-Fi (such as a personal computer, video-game console, smart phone, digital camera, tablet or digital audio player) can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (65 feet) indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves or as large as many square miles this is achieved by using multiple overlapping access points.
10. Explain the major differences between wifi and wimax.
    WiMAX **is a long range system, covering many kilometer**s, that uses licensed or unlicensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user. Different 802.16 standards provide different types of access, from mobile (analogous to access via a cell phone) to fixed (an alternative to wired access, where the end user's wireless termination point is fixed in location.)
    Wi-Fi is a shorter range system, typically hundreds of meters, that uses unlicensed spectrum to provide access to a network, typically covering only the network operator's own property. Typically Wi-Fi is used by an end user to access their own network, which may or may not be connected to the Internet. If WiMAX provides services analogous to a cell phone, Wi-Fi is more analogous to a cordless phone.

UNIT: 3 ROUTING

PART A

1. List the requirements for Mobile IP. (Nov 2014, Nov 2011)
   Compatibility, Transparency, Scalability and efficiency and Security.
2. Distinguish between proactive and active routing. (Nov 2014, June 2013)
   Proactive routing: Every node maintain one or more tables representing the entire topology of the network, this table are updated regularly. In order to maintain an up to date routing information from each node to every other node. It maintains up to date routing information and topology information on a regular basis.
   Reactive routing: Table maintenance is different from proactive protocol. Attempt to discover route only on-demand basis.

3. Define triangular routing. (May 2014)
   The inefficient behaviour of a non-optimized mobile IP is called triangular routing. The triangle is made up of three segments, CN to HA, HA to COA\MN, and MN back to CN.
   Triangular routing is a method for transmitting packets of data in communications networks. It uses a form of routing that sends a packet to a proxy system before transmission to the intended destination. Triangular routing is a problem in mobile IP, however it finds applications in other networking situations
4. What is the basic purpose of DHCP? (May 2014,May 2013)
   The dynamic host configuration protocol is mainly used to simplify the installation and maintenance of networked computers
5. Write any two factors that affect the performance of ADHOC networking? (Nov 2013)
   Node speed, pause-time, network size, number of traffic sources, and type of routing (source Versus distributed), that affect the performance of ad hoc networks.
6. What do you mean by zone routing protocol? (Nov 2013)
   ZRP is a hybrid Wireless Networking routing protocol that uses both proactive and reactive routing protocols when sending information over the network. ZRP was designed to speed up delivery and reduce processing overhead by selecting the most efficient type of protocol to use throughout the route.
7. What is the goal of M-TCP? (Nov 2011)
   The goal of M-TCP is to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems. It wants
   - To provide overall throughput
   - To lower the delay
   - To maintain end-to-end semantics of TCP
   - To provide a more efficient handover.
8. What led to the development of Indirect TCP?(Nov 2012,may 2012)
   - TCP performs poorly together with wireless links
   - TCP within the fixed network cannot be changed.

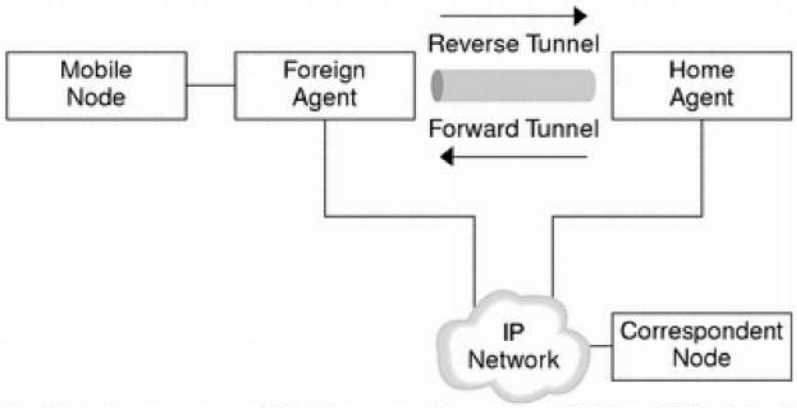
   This led to the development of I-TCP which segments a TCP connection into a fixed part and a wireless part.
9. Define a tunnel.(may 2012)
   A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.
10. What do you mean by persistent mode?
    Persistent mode is the state of the sender will not change no matter how long the receiver is disconnected.This means that the sender will not try to retransmit the data.
11. Mention the different entities in a mobile IP.
    Mobile Node, Correspondent Node, Home Network, Foreign Network, Foreign Agent, Home Agent, Care-Of address, Foreign agent COA and Co-located COA.
12. What do you mean by mobility binding?
    The Mobile Node sends its registration request to the Home Agent. HA now sets up a mobility binding containing the mobile node's home IP address and the current COA.
13. Define binding request.
    Any node that wants to know the current location of an MN can send a binding request to the HA. The HA can check if the MN has allowed dissemination of its current location. If the HA is allowed to reveal the location it sends back a binding update.
14. What is known as Binding update?
    This message sent by the HA to CNs reveals the current location of the MN. The message contains the fixed IP address of the MN and the COA. The binding update can request an acknowledgement.
15. Explain cellular IP.
    Cellular IP provides local handovers without renewed registration by installing a single cellular IP gateway for each domain, which acts to the outside world as a foreign agent.
16. What are the advantages of cellular IP?
    Manageability, Efficiency, Transparency and Security.
17. What is known as mobility anchor point?
    HMIPv6 provides micro-mobility support by installing a mobility anchor point, which is responsible for a certain domain and acts as a local HA within this domain for visiting MNs.
18. Explain destination sequence distance vector routing.
    Destination sequence distance vector routing is an enhancement to distance vector routing for ad-hoc networks and is used as routing information protocol in wired networks.

19. What are the general problems of mobile IP regarding security and support of quality of service?
Mobility poses many security problems. A minimum requirement is the authentication of all messages related to the management of mobile IP. It must be sure for the IP layer if it forwards a packet to a mobile host that this host really is the receiver of the packet. The IP layer can only guarantee that the IP addresses of the receiver is correct. There are no ways of preventing faked IP address or other attacks. According to Internet philosophy this is left to higher layers.
20. Why is routing in AdHoc networks complicated?
Traditional routing algorithms for wired networks will not work Routing in wireless network cannot rely on layer three knowledge alone. Centralized approaches will not work. Many nodes need routing capabilities.
21. What is encapsulation?
Encapsulation is the mechanism of taking a packet consisting of packet header and data putting it into the data part of a new packet.
22. What is the use of network address translation?
The network address translation is used by many companies to hide internal resources and to use only some globally available addresses.
23. Define binding warning.
If a node decapsulates a packet for a MN, but it is not the current FA for this MN, this node sends a binding warning. The warning contains MN's home address and a target node address.
24. What is meant by generic routing encapsulation?
Generic routing encapsulation allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.
25. What is meant by a binding cache?
One way to optimize the route is to inform the CN of the current location by caching it in a binding cache which is a part of the local routing table for the CN.

PART-B

1. Explain in detail the entities in mobile IP.(May 2012,nov-2011, Nov/Dec 2014)
A mobile node has two addresses - a permanent home address and a care-of address (CoA), which is associated with the network the mobile node is visiting. Two kinds of entities comprise a Mobile IP implementation:
   - A *home agent* stores information about mobile nodes whose permanent home address is in the home agent's network.
   - A *foreign agent* stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP. If there is no foreign agent in the host network, the mobile device has to take care of getting an address and advertising that address by its own means. A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the remote address through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node. When acting as transmitter, a mobile node sends packets directly to the other communicating node, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing or "route optimization" (RO) mode. If needed, the foreign agent could employ *reverse tunneling* by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers check that the source IP address of the mobile host belongs to their subnet or discard the packet otherwise. In Mobile IPv6 (MIPv6), "reverse tunneling" is the default behavior, with RO being an optional behavior.
2. Explain tunneling and encapsulation in mobile IP.(nov 2012,May/June 2014)
GRE (Generic Routing Encapsulation) or IP tunneling (IP encapsulation) is a technique that encapsulates IP datagrams within IP datagrams. GRE is a technique that allows datagrams to be encapsulated into IP packets and then redirected to an intermediate host. At this intermediate destination, the datagrams are de capsulated and then routed to the next leg. In doing so, the trip to the intermediate host appears to the inner datagrams as one hop.

3. Describe Dynamic host configuration protocol.(May 2012,nov 2011, Nov/Dec 2013, 2014)
   The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network(known as hosts) so they can communicate on that network using the Internet Protocol (IP). It involves clients and a server operating in a client-server model.
   `One common example of its use is in a typical personal home local area network (LAN). In this case, the server is a router[1] while the clients are hosts (eg. personal computers, smart phones, printers, etc.). The router receives the configuration information through a modem from an internet service provider, which also operates DHCP servers with this router as one of the clients. The clients request configuration settings using the DHCP protocol such as an IP address, a default route and one or more DNS server addresses. Once the client implements these settings, the host is able to communicate on that internet.
   The DHCP server maintains a database of available IP addresses and configuration information. When the server receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address or prefix that is appropriate for the client, and sends configuration information appropriate for that client. DHCP servers typically grant IP addresses to clients only for a limited interval. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it.
4. Explain in detail about reverse tunneling and optimization in Mobile IP. (May/June 2013, 2014)
   The previous description of Mobile IP assumes that the routing within the Internet is independent of the data packet's source address. However, intermediate routers might check for a topologically correct source address. If an intermediate router does check, you should set up a reverse tunnel. By setting up a reverse tunnel from the mobile node's care-of address to the home agent, you ensure a topologically correct source address for the IP data packet. A mobile node can request a **reverse tunnel** between its foreign agent and its home agent when the mobile node registers. A reverse tunnel is a tunnel that starts at the mobile node's care-of address and terminates at the home agent. The following illustration shows the Mobile IP topology that uses a reverse tunnel.
   Mobile IP With a Reverse Tunnel



5. Explain the concept of Multicast routing protocol.(Nov 2011, Nov/Dec 2013, 2014)
   The Simple Multicast Routing Protocol (SMRP) is a transport layer protocol developed to route multimedia data streams over AppleTalk networks. It supports Apple Computer's QuickTime Conferencing (QTC) technology. SMRP provides connectionless, best-effort delivery of multicast datagrams and relies on underlying network layer protocols for services. In particular, SMRP facilitates the transmission of data from a single source to multiple destinations. This article focuses on the functional elements and protocol operations of SMRP.
6. Discuss in detail about the Dynamic source routing with an example. (May/June 2013)
   Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence.
   The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. The destination node, on receiving a Route Request packet, responds by sending a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received. Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a Route Request packet. This

Route Request is flooded throughout the network. Each node, upon receiving a Route Request packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded. Each Route Request carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a Route Request packet, checks the sequence number on the packet before forwarding it.

The packet is forwarded only if it is not a duplicate Route Request. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same Route Request by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a Route Request packet during the route construction phase. A destination node, after receiving the first Route Request packet, replies to the source node through the reverse path the Route Request packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase.

7. What are the requirements of a mobile IP? Explain in detail.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the remote address through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node. When acting as transmitter, a mobile node sends packets directly to the other communicating node, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing or "route optimization" (RO) mode. If needed, the foreign agent could employ *reverse tunneling* by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers check that the source IP address of the mobile host belongs to their subnet or discard the packet otherwise. In Mobile IPv6 (MIPv6), "reverse tunneling" is the default behavior, with RO being an optional behavior.

8. Differentiate wired and Adhoc Routing (May 2012)

Ad hoc and infrastructure modes differ greatly in how the network is set up. In an ad hoc network, each device's network adapter directly communicates with other devices through the use of software. This software can be included with the device's operating system or purchased from a third party. This provides an inexpensive and quicker way to connect than using infrastructure mode. Another benefit of an ad hoc network is that the connection speeds can be significantly faster than when using a wireless accent point with infrastructure mode.

Infrastructure networks consist of the networked devices and the wireless access point or wireless router. Each device must connect to the access point before having access to other computers on the network. While both ad hoc and infrastructure networks can provide a secure connection, infrastructure mode supports various encryption methods. Additional security features allow the use of passwords and allow computers to connect by checking a device's media access control (MAC) address.

9. Explain routing in IPv6.

Routing is the process of forwarding packets between connected network segments. For IPv6-based networks, routing is the part of IPv6 that provides forwarding capabilities between hosts that are located on separate segments within a larger IPv6-based network.

IPv6 is the mailroom in which IPv6 data sorting and delivery occur. Each incoming or outgoing packet is called an IPv6 packet. An IPv6 packet contains both the source address of the sending host and the destination address of the receiving host. Unlike link-layer addresses, IPv6 addresses in the IPv6 header typically remain the same as the packet travels across an IPv6 network. Routing is the primary function of IPv6. IPv6 packets are exchanged and processed on each host by using IPv6 at the Internet layer. Above the IPv6 layer, transport services on the source host pass data in the form of TCP segments or UDP messages down to the IPv6 layer. The IPv6 layer creates IPv6 packets with source and destination address information that is used to route the data through the network. The IPv6 layer then passes packets down to the link layer, where IPv6 packets are converted into frames for transmission over network-specific media on a physical network. This process occurs in reverse order on the destination host. IPv6 layer services on each sending host examine the destination address of each packet, compare this address to a locally maintained routing table, and then determine what additional forwarding is required. IPv6 routers are attached to two or more IPv6 network segments that are enabled to forward packets between them.

10. Describe in detail about Proactive protocol.
    In networks utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node.
    To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. One the other hand, routes will always be available on request.
    Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR) which is discussed in section OLSR.

UNIT-IV
TRANSPORT AND APPLICATION LAYERS

PART-A

1. What are the requirements of WAP? (Nov 2014)
   Interoperable, scaleable, Efficient, reliable and secure.
2. Define WSP. (Nov 2014)
   The Wireless Session Protocol has been designed to operate on top of the datagram service WDP or the transaction service WTP. It provides a shared state between a client and a server to optimize content transfer.
3. What is wireless telephony application? (May 2014)
   Wireless telephony applications (*WTA*): A collection of telephony-specific extensions for call and feature control mechanisms that provide authors advanced *mobile* network services.
4. List the classes of transaction service of WTP. (May 2014)
   WTP stands for Wireless Transaction Protocol. It has been designed to run on very thin clients such as mobile phones. It has three classes.
   - Class 0: provides unreliable message transfer without any result message.
   - Class 1: provides reliable message transfer without exactly one reliable result message.
   - Class 2: provides reliable message transfer with exactly one reliable result message.
5. Mention the features present in WSP/B in addition to that present in WSP. (Nov 2013)
   Validity check of user input, check input before sent to server, access to device facilities, hardware and software (phone call, address book, etc.), local user interaction, interaction without round-trip delay, extensions to the device software, configure device, download new functionality after deployment.
6. State the applications of Wireless telephony. (Nov 2013)
   Wireless Telephony Applications (WTA) are those applications designed to interact with the telephony-related functions present in a phone. The web browser supports: Originating a call – Click to Dial, Adding entries to the phonebook (Add to Speed Dial entries). Other way we can define WTA as, " A collection of telephony-specific extensions for call- and feature-control mechanisms that make advanced mobile network services available to end users. WTA essentially merges the features and services of data networks with the services of voice networks".
7. What are the features of WML?(Nov 2012)
   Text and Images, User interaction, Navigation and Context Management.
8. What do you mean by WAE?(Nov 2011)
   The Wireless Application Environment (WAE) provides a application framework for small devices. WAE leverages other technologies such as WAP, WTP, and WSP.
9. What is the use of WML? (May/June 2013)
   WML stands for Wireless Markup Language. It is a mark – up language inherited from HTML, but WML is based on XML, so it is much stricter than HTML. WML is to create pages that can be displayed in a WAP browser. Pages in WML are called DECKS. Decks are construed as a set of cards.
10. What is WAP? (May/June 2013)
    Wireless Application Protocol, open for everyone to participate, protocol specifications will be proposed to standardization bodies.
11. What do you mean by WML?
    Wireless Markup Language specification describes the markup language, WML including its XML document type definition (DTD) and its encoding extensions.

12. What is WML script?
WMLScript Standard Libraries Specification (WAEStdLib) - describes standard libraries available to *WMLScript* ... WML is designed with the constraints of small *mobile* devices in mind.
13. What is the use of congestion threshold?
The exponential growth of the congestion window in the slow start mechanism is dangerous as it doubles the congestion window at each step. So a congestion threshold is set at which the exponential growth stops.
14. Name the layers of WAP.
Transport layer, Security layer, Transaction layer, Session layer and Application layer
15. Name some ICMP messages.
Destination unreachable, Parameter problem, Message too big, Reassembly failure and Echo request/reply
16. Name the operations performed by PAP.
Push submission, Result notification, Push cancellation, Status query and Client capabilities query.

17. What are the components of WAP2.0?
The protocol framework of WAP2.0 consists of four components:
    - Bearer networks
    - Transport services
    - Transfer services
    - Session services
18. What is SyncML (Synchronization Markup Language)?
SyncML is the leading open industry standard for universal synchronization of remote data and personal information across multiple networks, platforms and devices.

19. What do you mean by WDP?
Wireless Datagram Protocol (WDP) works as the transport layer of WAP. WDP processes datagrams from upper layers to formats required by different physical datapaths, bearers, that may be for example GSM SMS or CDMA Packet Data. WDP is adapted to the bearers available in the device so upper layers don't need to care about the physical level
20. What is I-TCP?
The TCP connection between the mobile host (MH) and the correspondent host (CH) is split at the mobility support router (MSR). The connection between the MSR and MH has independent, optimized flow and congestion control from the MSR to CH link. In fact, a separate transport protocol can be used.
21. What is WTLS?
WTLS can provide different levels of security(for privacy, data integration ,and authentication) and has been optimized for low bandwidth, high-delay bearer networks.
22. What are the technical differences between i-Mode and WAP?
The main difference between i-Mode and WAP is the markup language used. i-Mode uses Compact HTML, while WAP uses Wireless Markup Language (WML), which is not compliant with HTML standards. Key Differences are outlined below:

Developed by NTT DoCoMo	Developed by Wireless Phone Industry
HTML as markup language	WML as markup language
only in Japan/Hong Kong at present	around the World

23. What are the advantages of WML Script?
    - Validity check of user input.
    - Access to device facilities
    - Local user interaction
    - Extensions to the device software.
24. What are the classes of libraries?
Common network services, Network specific services and Public services.

25. Name some features of WSP adapted to web browsing.
HTTP/1.1 functionality, Exchange of session headers, Push and pull data transfer and Asynchronous request

PART-B

1. Write about Mobile TCP. (may 2012, May/June 2013, 2014, Nov/Dec 2014)
In networks utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node.
To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. One the other hand, routes will always be available on request. Many proactive protocols stream from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).
2. Write short notes on WAP architecture.(Nov 2011, May/June 2014, Nov/Dec 2014)
WAP is designed in a layered fashion so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers:
Application Layer
Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains, among other things, device specifications and the content development programming languages, WML and WMLScript.
Session Layer
Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.
Transaction Layer
Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.
Security Layer
Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.
Transport Layer
Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.
3. Explain in detail about wireless telephony application. (Nov/Dec 2014)
The original WAP model provided a simple platform for access to web-like WML services and e-mail using mobile phones in Europe and the SE Asian regions. As of 2009 it continues with a considerable user base. The later versions of WAP, primarily targeting the United States market, were designed for a different requirement - to enable full web XHTML access using mobile devices with a higher specification and cost, and with a higher degree of software complexity. Considerable discussion has addressed the question whether the WAP protocol design was appropriate. Some have suggested that the bandwidth-sparing simple interface of Gopher would be a better match for mobile phones and Personal digital assistants (PDAs). The initial design of WAP specifically aimed at protocol independence across a range of different protocols (SMS, IP over PPP over a circuit switched bearer, IP over GPRS, etc.). This has led to a protocol considerably more complex than an approach directly over IP might have caused.
4. Explain in detail about WTP.(Nov 2011,Nov 2012,May 2012, Nov/Dec 2014)
Wireless transaction protocol is a standard used in mobile telephony. It is a layer of the Wireless Application Protocol (WAP) that is intended to bring Internet access to mobile phones.
5. Write short notes on wireless markup language and WML script.
Wireless markup language (WML) and WML Script are programming languages that are used to provide information services to portable wireless devices. This book explains how and why companies use WML to develop and provide information services to mobile communication devices. WML protocols and scripts are used to create web pages that are compatible with them. This book describes why and how to use gateways and script languages to convert standard Internet web pages into formats that can be used by portable devices and some of the problems that this can cause. The reader will learn the structure of the WML language and how to create script files that can controls the display of information on mobile devices and the different ways

that users can control content delivery of information with the limited keypads on mobile devices. Some of the most important topics featured are: . Why a different programming language is needed for wireless devices. How to create web pages that are compatible with mobile telephones and PDAs. Ways to use a gateway to convert standard Internet web pages into formats that can be used by portable devices. How WML script can control the display of information. Ways that users can control content delivery of information with the limited keypads on mobile devices. What are some of the challenges of converting Internet content into different formats needed by mobile devices. How to create information services (push services) that can automatically provide information to the mobile user without the need to request information. The methods used to handle large file transfers. . How to convert complex web pages such as frames and animation into formats and controls that allow navigation by mobile devices.

6. Explain in detail about WSP?

Goals

- HTTP 1.1 functionality
  - Request/reply, content type negotiation, ...
- support of client/server, transactions, push technology
- key management, authentication, Internet security services
- session management (interruption, resume,...)

Services

- session management (establish, release, suspend, resume)
- capability negotiation
- content encoding

WSP/B (Browsing)

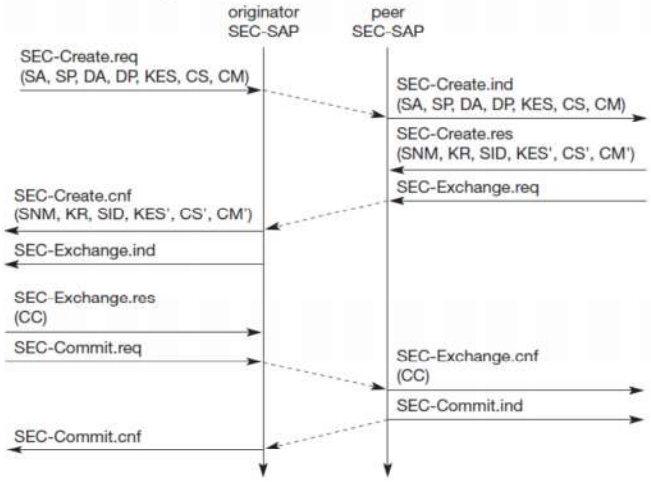
- HTTP/1.1 functionality - but binary encoded
- exchange of session headers
- push and pull data transfer
- asynchronous requests

7. Explain Wireless transport layer security?

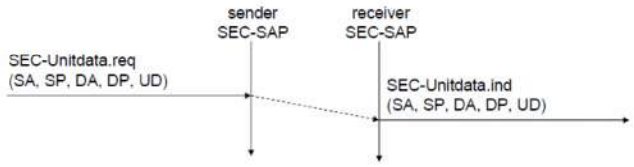
Goals

- data integrity
  - prevention of changes in data
- privacy
  - prevention of tapping
- authentication
  - creation of authenticated relations between a mobile device and a server
- protection against denial-of-service attacks
  - protection against repetition of data and unverified data

Secure session, full handshake



- WTLS
  - is based on the TLS (Transport Layer Security) protocol (former SSL, Secure Sockets Layer)
  - optimized for low-bandwidth communication channels



8. What are all the various flavours of TCP available? Explain them in detail?(Nov 2013)
    1. Indirect TCP- I-TCP segments a TCP connection into a fixed part and a wireless part.
    2. Snooping TCP- Here the foreign agent buffers all packets with destination mobile host and additionally snoops the packet flow in both directions to recognize acknowledgements.
    3. Mobile TCP- 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.
    4. Fast Transmit/Fast Recovery
    5. Transmission/Time-out freezing
    6. Selective retransmission
    7. Transaction-oriented TCP.
9. Write short notes on protocols used in WAP.
   The original WAP model provided a simple platform for access to web-like WML services and e-mail using mobile phones in Europe and the SE Asian regions. As of 2009 it continues with a considerable user base. The later versions of WAP, primarily targeting the United States market, were designed for a different requirement - to enable full web XHTML access using mobile devices with a higher specification and cost, and with a higher degree of software complexity. Considerable discussion has addressed the question whether the WAP protocol design was appropriate. Some[] have suggested that the bandwidth-sparing simple interface of Gopher would be a better match for mobile phones and Personal digital assistants (PDAs). The initial design of WAP specifically aimed at protocol independence across a range of different protocols (SMS, IP over PPP over a circuit switched bearer, IP over GPRS, etc.). This has led to a protocol considerably more complex than an approach directly over IP might have caused.
10. Explain in detail about WWW programming Model.
    Having presented WAP architectures and protocols, let's re-examine the fundamental difference between the WWW and WAP models. The WAP programming model is very much tailored toward the web-based programming model. This is because Web-based applications are foreseen to be the main platform for both wired and wireless users.
    The original WWW model comprises a Web client and server. It is based on an RPC paradigm, where clients convey their intentions and requests to servers for processing and execution. In the WWW, applications and content are presented in standard data formats, and are browsed by clients known as Web browsers. In this model, the Web browser sends requests for named data objects to a network server, which responds with the data encoded using the standard format.

UNIT V-PERVASIVE COMPUTING

PART A

1. What is Pervasive computing? (Nov 2014,May 2014, may 2012,nov 2011)
   Pervasive computing goes beyond the realm of personal computers: it is the idea that almost any device, from clothing to tools to appliances to cars to homes to the human body to your coffee mug, can be imbedded with chips to connect the device to an infinite network of other devices.
2. What are the limitations of accessing pervasive computing via WAP? (Nov 2014)
    - Small display
    - Restricted input capability
    - Limited memory and processing power
    - Low speed network connections with high latency.
3. List some types of Biometric devices. (May 2014)
   Finger print, signature ,hand geometry, face recognition, voice recognition, iris scan.

4. Give some application areas of pervasive computing. (Nov 2013,May 2013)
   Retail, Airlines check in and booking, Health Care, Tracking, Car Information System, mail.
5. What are principles of pervasive computing?
   - Decentralization
   - Diversification
   - Connectivity
   - Simplicity
6. Give the Security features of pervasive computing
   - Multilevel
   - Flexibility and customizability
   - Context-Awareness
   - Interoperability
   - Extended boundaries
7. Define Biometrics. (nov 2012, May/June 2013, 2014)
   Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.
8. List out the devices for pervasive computing?(may 2012,nov 2012)
   Devices, Sensors, processors, actuators
9. What is SLP?
   SLP is a mechanism for facilitating the association of entities that have services to offer or need of services.
10. What do you mean by PDA?
    A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Many PDAs employ touch screen technology.
11. What are the protocols used in pervasive computing
    Sync Ml ,Jini, Service Location protocol
12. Give the Security features of pervasive computing
    - Multilevel
    - Flexibility and customizability
    - Context-Awareness
    - Interoperability
    - Extended boundaries
13. What are the operating system for pervasive computing.
    Centralised OSes, Networked OSes, Distributed OSes, Classification based on Kernel / Core Styling, Monolithic Kernel based OSes, Microkernel based OSes, Exokernel based OSes, classification based on hardware form-factor and scope, Server-class OSes (with and without real-time support).
14. Write about EPOC os?
    - It is specifically designed for phones .It supports Unicode, It can display 256 colours.
    - It consists of the following features.
    - User Management, Task Management, User interface, Memory management.
15. What are the things required for Human-Machine Interfaces?
    - Navigation
    - Haptic Interfaces
    - Keyboards
    - Handwriting recognition
    - Speech recognition
16. What are the steps for connection to mobile node?
    - Discover the care-of address
    - Register the care-of address
    - Tunnel the care-of address.
17. What do you mean by Handheld Computers?
    Handheld computers comprise largest group of Internet connectable pervasive devices.

18. What do you mean by smart phone?
    Smart phones combine a mobile phone with a handheld organizer into an all in one communication system
19. Give any four pervasive device names?
    - Information access device
    - Intelligent appliances
    - Smart controls
    - Entertainment systems
20. Define Devices.
    PCS devices are likely to assume many different forms and sizes, from handheld units (similar to mobile phones) to near-invisible devices set into 'everyday' objects (like furniture and clothing). These will all be able to communicate with each other and act 'intelligently'.
21. Define Sensors.
    Sensors: input devices that detect environmental changes, user behaviours, human commands etc..
22. Define Processors.
    Processors: electronic systems that interpret and analyse input-data;
23. What do you mean by embedded control?
    It describes how pervasive information technology will be used in embedded home and automotive settings.
24. Give the hardware parts of hand device?
    Battery, Displays, Memory, Processors.

25. What are all the types of Keyboards?
    - On-Screen keyboard(Qwerty)
    - Fitaly Keyboard
    - Octave

PART-B

1. Explain the Pervasive computing infrastructure(May 2012, May/June 2014)
   As mobile and embedded computing devices become more pervasive, it is becoming obvious that the nature of interactions between users and computers must evolve. Applications need to become increasingly autonomous and invisible, by placing greater reliance on knowledge of context and reducing interactions with users. Moreover, applications must cope with highly dynamic environments in which resources, such as network connectivity and software services, frequently vary over time.
2. Explain the Pervasive computing applications(Nov 2011, Nov/Dec 2014)

   - Information access
   - Text retrieval
   - Multimedia document retrieval
   - Automatic indexing
   - Pervasive devices
   - Palm top computers
   - Smart badges
   - Electronic books
   - User sensitive devices
   - Mobility and networking
   - Device discovery
   - Wireless protocols
   - Security
   - Voice and video over IP
   - Perceptive interfaces
   - Biometric person ID
   - Speech recognition
   - Gesture recognition

3. Explain the Pervasive web application infrastructure (May/June 2014, Nov/Dec 2014)
   Multi-user communication and interaction via public displays together the pervasive and seamless access to the WWW in public areas via mobile phones or handheld devices is enabled via the WebWall system. A software framework for the operation of WebWalls has been developed, strictly separating WebWall access technologies (like HTTP, email, SMS, WAP, EMS, MMS or even simple paging protocols found on mobile phones) from the physical display technologies used and the presentation logic involved.
   The architecture integrates ubiquitous wireless networks (GSM, IEEE802.11b), allowing a vast community of mobile users to access the WWW via public communication displays in an ad-hoc mode. A centralized backend infrastructure hosting content posted by users in a display independent format has been developed together with rendering engines exploiting the particular features of the respective physical output devices installed in public areas like airports, train stations, public buildings, lecture halls, fun and leisure centres and even car navigation systems. A variety of different modular service classes has been developed to support the

posting or pulling of WWW media elements ranging from simple sticky notes, opinion polls, auctions, image and video galleries to mobile phone controlled web browsing.

4. Explain about Accessing from PDAs and PCs.(Nov 2013)
   A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. PDAs are largely considered obsolete with the widespread adoption of smart phones. In fact smart phones are PDAs, and it is just a name change. The difference is that not every PDA (especially old) can be called smart phone, because "phone" means calling and request of some network (e.g. GSM) access.
   Nearly all current PDAs have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, all current models also have audio capabilities enabling use as a portable media player, and also enabling most of them to be used as mobile phones. Most PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Most PDAs employ touch screen technology.
5. Explain the applications of WAP.
   Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol.
   Before the introduction of WAP, mobile service providers had limited opportunities to offer interactive data services, but needed interactivity to support Internet and Web applications such as:

   - Email by mobile phone
   - Tracking of stock-market prices
   - Sports results
   - News headlines
   - Music downloads

6. Explain the concept of embedded control in pervasive computing.
   Pervasive Computing (also known as Ubiquitous Computing) refers to a new class of applications based on small, inexpensive, and networked devices that "instrument" the physical world and make the computers almost "invisible" while making our daily lives easier. Examples include smart homes, smart spaces, wireless sensor networks for environmental/habitat monitoring, wearable computers for virtual reality and health monitoring, among many others. On the other hand, Embedded Computers are part of larger and special-purpose systems that interact with real world in real-time. As such, they typically involve control and monitoring of critical functions, and require different design techniques. More than 99% of all processors sold world-wide each year are deployed in embedded systems -- they are everywhere: cell phones, PDAs, DVD and multimedia players, cameras and office appliances, automobile engines, aircraft/spacecraft control systems, industrial automation systems, health informatics, nuclear plant control systems. Pervasive and embedded computing can and often do intersect, such as in the case of wireless sensor networks deployed in a "pervasive" monitoring application deploying embedded CPUs in a sensor mote. While they offer great promises, the pervasive and embedded computers often have to meet strict operational constraints with limited resources (limited memory, battery power, CPU frequency).
7. Explain the concept of Smartcard.(Nov 2012)
   A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, generally polyvinyl chloride, but sometimes polyethyleneterephthalate based polyesters, acrylonitrile but a polycarbonate.
   Smart cards can provide identification, authentication, data storage and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.
8. Describe device connectivity and device management in pervasive computing.(Nov 2013)
   Device Connectivity:
   1.Protocols- Standardized protocols are basic prerequisites for meaningful use of pervasive computing devices.
   Wireless Protocols:WAP,OBEX,IrDA,Bluetooth, and mobile phone technologies.
   Mobile phone Technologies : GSM,1st Generation mobile systems,2nd generation mobile systems,3rd generation mobile systems.
   Mobile Internet Protocol- Mobile IP.
   Distributed Services- Jini,universal plug and play.
   Message and transaction based protocols.

2. Security- It focuses on server-side aspects security aspects of pervasive computing applications.
Security concepts- Identification,Authentication,Authorization,Transaction authorization,Digital Signatures,Transaction authorization numbers,Non-repudiation.
Device security.
Server-side security.
Cryptographic algorithms-DES,3DES,AES,Public-key algorithms,RSA,DSA.
Device Management:
1.Device Management challenges:

- **Tracking the device location.**
- **Device-user relationship**
- **Version control,software updates,etc.**

2.Software distribution: Hardware capabilities,Hardware version managements,software version management, OS updates, Insecure and unstable connections.

9. Explain the Protocols in Pervasive Computing.
   The design of security protocols for perform should support a high degree of user mobility, transparency and portability across devices. The challenge is to design protocols such that successful completion of protocol handshakes and trust establishment is not based on a user having access to a designated device or workstation
10. Explain about Accessing via WAP .(Nov 2011).
    Prior to wireless networks, setting up a computer network in a business, home or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the creation of the wireless Access Point (AP), network users are now able to add devices that access the network with few or no cables. An AP normally connects directly to a wired Ethernet connection and the AP then provides wireless connections using radio frequency links for other devices to utilize that wired connection. Most APs support the connection of multiple wireless devices to one wired connection. Modern APs are built to support a standard for sending and receiving data using these radio frequencies. Those standards, and the frequencies they use are defined by the IEEE. Most APs use IEEE 802.11 standards.

Question Bank for ESE

1. Write Short notes on
   i) Mobility of bits and bytes
   ii) Mobile Computing
   iii) Dialogue Control Networks
2. i) What is three tier Architecture?

ii) What are the security standards available for Mobile Computing?

3. Explain the architecture of GPRS in detail.
4. Explain the architecture of GSM in detail.
5. List the differences between 3G and 4G.
6. Write short notes on
   i) Soft switch
   ii) Adhoc networks
   iii) Machine interface biometrics.
7. How pervasive computing is available for personalized services?
8. Depict the scenarios of roaming environment.
9. Explain pervasive web application architecture.
10. Elaborate WAP in details.

11. Write Short notes on
    i) Middleware and gateways
    ii) Mobile computing through internet
    iii) Wireless the beginning
12. How to develop mobile computing applications?

13. Illustrate Bluetooth Architecture with a neat diagram.
14. Write the features of CDMA
15. Illustrate the fundamentals of call processing.
16. Write in detail about SS #7 Signaling.

17. Write short notes on

i) Pervasive computing market

ii) M-Business

iii) Java for pervasive devices

18. Elaborate human machine interface biometric and operating systems
19. Depict the applications of voice technologies.
20. How protocols, security and device management is done in pervasive computing
21. How to develop IVR applications?
22. Write Short notes on
    i) Mobility of bits and bytes
    ii) Mobile Computing
    iii) Dialogue Control Networks

23 .Write the features of CDMA

24. i) Elaborate the applications of GPRS

ii) List the limitations of GPRS

25. Write short notes on
    - i) IN conceptual model
    - ii) Programmable Networks
    - iii) Client Programming

26. How to deploy mobile Adhoc network and sensor networks

27. Depict the scenarios of roaming environment.

28. Write short notes on
    - i) Pervasive computing market
    - ii) M-Business
    - iii) Java for pervasive devices

29. How client is authenticated via internet?

30. Elaborate Personal Digital Assistance

31. i) What is three tier Architecture?

ii) What are the security standards available for Mobile Computing?

32. Write Short notes on
    - i) Middleware and gateways

ii) Mobile computing through internet

iii) Wireless the beginning

33. Explain the architecture of GPRS in detail.

34. Explain the architecture of GSM in detail.

35. How to deploy mobile Adhoc network and sensor networks

36. List the advantages of LAN and differentiate wired and wireless networks.

37. Elaborate human machine interface biometric and operating systems

38. How protocols, security and device management is done in pervasive computing

39. How client is authenticated via internet?

40. How to develop mobile computing applications?

41. How to develop IVR applications?

42. Illustrate Bluetooth Architecture with a neat diagram.

43. Write the features of CDMA

44. List the differences between 3G and 4G.

45. Write short notes on
    - iv) Soft switch
    - v) Adhoc networks
    - vi) Machine interface biometrics.

46. How pervasive computing is available for personalized services?

47. Depict the scenarios of roaming environment.

48. Explain pervasive web application architecture.

49. Elaborate WAP in details.