13BECS801 Mobile Computing

COURSE OBJECTIVES:

- To understand the basic concepts of mobile computing.
- To learn the basics of mobile telecommunication system .
- To be familiar with the network layer protocols and Ad-Hoc networks.
- To know the basis of transport and application layer protocols.
- To gain knowledge about different mobile platforms and application development.

UNIT I INTRODUCTION

Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies- Multiplexing – Spread spectrum -MAC Protocols – SDMA- TDMA- FDMA- CDMA

UNIT II MOBILE TELECOMMUNICATION SYSTEM

Introduction to Cellular Systems – GSM – Services & Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security – GPRS- UMTS – Architecture – Handover – Security

UNIT III MOBILE NETWORK LAYER

Mobile IP – DHCP – AdHoc– Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV , Hybrid routing –ZRP, Multicast Routing- ODMRP, Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security.

UNIT IV MOBILE TRANSPORT AND APPLICATION LAYER

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

UNIT V MOBILE PLATFORMS AND APPLICATIONS

Mobile Device Operating Systems – Special Constraints & Requirements – Commercial Mobile Operating Systems – Software Development Kit: iOS, Android, BlackBerry, Windows Phone – MCommerce – Structure – Pros & Cons – Mobile Payment System – Security Issues

TEXT BOOKS

1. Jochen Schiller, "Mobile Communications", PHI/Pearson Education, Second Edition, 2003. (Unit I Chap 1,2 &3- Unit II chap 4,5 &6-Unit III Chap 7.Unit IV Chap 8- Unit V Chap 9&10.)
2. William Stallings, "Wireless Communications and Networks", PHI/Pearson Education, 2002. (Unit I Chapter – 7&10-Unit II Chap 9)

REFERENCES

3. Kaveh Pahlavan, Prasanth Krishnamoorthy, "Principles of Wireless Networks", PHI/Pearson Education, 2003.
4. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, "Principles of Mobile Computing", Springer, New York, 2003.
5. Hazysztof Wesolowshi, "Mobile Communication Systems", John Wiley and Sons Ltd, 2002.

KARPAGAM UNIVERSITY
Faculty of Engineering
Department of Computer Science and Engineering

Lecture Plan

Subject Code: 13BECS801

Faculty Name : B.Arunkumar

Subject Name : Mobile Computing

Class : IV-BE-CSE

Session No	Topics to be covered	Ref (Page No)	Teaching Method
1	Introduction – History, Devices, Application & Reference Model.	1(3-7,9-14,18-20)	BB
2	Wireless Transmission- Frequencies & Regulations.	1(25-27),2(27-29)	BB
3	Signals, Antennas, Signal Propagation- Path loss –Delay Spread, propagation effects.	1(28-37),2(109-115)	BB
4	Multi path propagation, Multiplexing - Space Division Mux, FDM, TDM, CDM.	1(39-44)	BB
5	Modulation- ASK, FSK, PSK, MSK, BPSK, QPSK,DQPSK.	1(45-50)	BB
6	Modulation- QAM, OFDM, COFDM. Spread Spectrum: Introduction, DSSS - Transmitter and Receiver.	1(50-59),2(180-187)	BB
7.	FHSS – Transmitter and Receiver Cellular Systems.	1(59-64),2(175-180)	BB
8	Media Access Control: SDMA, FDMA, TDMA, CSMA, CDMA, Comparison of S/T/F/CDMA.	1(69-89)	BB/OHP
9	Cellular Wireless Networks.	2(278-329)	BB

Session No	Topics to be covered	Ref(Page No)	Teaching Method
10	Telecommunication Networks- Introduction, GSM – Services, System Architecture.	1(93-100),2(18-20)	BB/OHP
11	Radio Interface, Protocol, Localization and Calling.	1(105-113)	BB
12	Handover, Security-Authentication, Encryption.	1(117-122)	BB/OHP
13	Data Services - HSCPD, GPRS.	1(122-130)	BB/OHP
14	DECT- System Architecture, Protocol architecture.	1(130-134)	BB
15	UMTS & IMT 2000-UMTS architecture, UTRA FDD mode, UTRA TDD mode.	1(134-149)	BB/OHP
16	Satellite Networks- Basics.	2(251-252)	BB
17	Satellite Parameters & configurations-satellite orbits, GEO, LEO, MEO	2(252-259)	BB
18	Capacity Allocation- Frequency division- FAMA –FDMA, DAMA-FDMA, Time division – DAMA-TDMA, FAMA – TDMA	2(260-275)	BB/OHP
19	Broadcast Systems: Introduction, cyclic repetition of data, Digital Audio Broadcasting-Multimedia object transfer protocol.	1(183-190)	BB
20	Digital Video Broadcasting	1(191-195)	BB
	Continuous Assessment Test - I		

Session No	Topics to be covered	Time Mts	Ref(Page No)	Teaching Method
21	Wireless LAN: Introduction, Infrared and radio transmission Infrastructure & AdHoc Networks.	50	1(201-205)	BB

22	IEEE 802.11, System Architecture, Protocol Architecture.	50	1(207-210)	BB/OHP
23	Physical Layer: FHSS, DSSS.	50	1(211-213)	BB
24	Introduction-Media Access Control Layer, DFWMAC-DCF, RTS / CTS, PCF with polling.	50	1(214-224)	BB
25	MAC Management – Synchronization, Power Management, Roaming.	50	1(225-230)	BB/OHP
26	IEEE 802.11a,IEEE 802.11b standards, Hyperlan – Introduction, Protocol Architecture, Physical Layer.	50	1(231-238)	BB/OHP
27	Hyperlan – CAC Sub layer - Prioritization Phase, Elimination Phase, Yield Phase, Transmission Phase.	50	1(239-257)	BB
28	Hyperlan - MAC Sub layer.	50	1(257-268)	BB
29	Blue tooth – Physical Layer, MAC Layer, Networking, Security, Link Management.	50	1(269-293)	BB/OHP

Session No	Topics to be covered	**Time Mts**	**Ref(Page No)**	**Teaching Method**
30	Mobile IP – Requirements, Entities & Terminologies.	50	1(303-308),2(373-387)	BB
31	Mobile IP - IP Packet Delivery, Agent Advertisement, Discovery, Registration.	50	1(309-312)	BB
32	Mobile IP – Tunneling & Encapsulation, Optimization.	50	1(315-320)	BB
33	Mobile IP – Reverse Tunneling, IPV6.	50	1(321-324)	BB
34	DHCP.	50	1(328-330)	BB
35	Ad Hoc Network: - Routing, Types.	50	1(330-334)	BB

36	Ad Hoc Network: - Destination Sequence Distance Vector, Dynamic Source Routing.	50	1(335-338)	BB
37	Ad Hoc Network: - Hierarchical Algorithms.	50	1(339-343)	BB
38	Ad Hoc Network: - Alternative Metrics.	50	1(343-346)	BB
	Continuous Assessment Test - II			

Session No	Topics to be covered	**Time Mts**	**Ref(Page No)**	**Teaching Method**
39	Mobile Transport Layer : Traditional TCP- Congestion Control.	50	1(351-353)	BB
40	TCP: Slow Start, Fast retransmit / fast recovery, implication on mobility, Indirect TCP, Snooping TCP.	50	1(353-359)	BB
41	Mobile TCP, Fast Retransmit / fast recovery, Transmission/ timeout freezing.	50	1(360-363)	BB
42	Selective retransmission, Transaction oriented TCP.	50	1(363-365)	BB
43	Wireless Application Protocol- Architecture, Wireless Datagram Protocol.	50	1(392-394)	BB/OHP
44	Wireless Application Environment, Wireless Session Protocol.	50	1(394-397)	BB
45	Wireless Transaction Protocol, Wireless Markup Language, WML Script	50	1(400-416)	BB
	Continuous Assessment Test - III			

TEXT BOOKS

6. Jochen Schiller, “Mobile Communications”, PHI/Pearson Education, Second Edition, 2003. (Unit I Chap 1,2 &3- Unit II chap 4,5 &6-Unit III Chap 7.Unit IV Chap 8- Unit V Chap 9&10.)
7. William Stallings, “Wireless Communications and Networks”, PHI/Pearson Education, 2002. (Unit I Chapter – 7&10-Unit II Chap 9)

REFERENCES

8. Kaveh Pahlavan, Prasanth Krishnamoorthy, “Principles of Wireless Networks”, PHI/Pearson Education, 2003.
9. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, “Principles of Mobile Computing”, Springer, New York, 2003.
10. Hazysztof Wesolowshi, “Mobile Communication Systems”, John Wiley and Sons Ltd, 2002.

Staff Incharge HOD/CSE

UNIT I

WIRELESS COMMUNICATION FUNDAMENTALS

1.0 INTRODUCTION

Mobile computing means different things to different people. Ubiquitous, wireless and remote computing Wireless and mobile computing are not synonymous. Wireless is a transmission or information transport method that enables mobile computing.

Aspects of mobility:

- user mobility: users communicate (wireless) “anytime, anywhere, with anyone”
- device portability: devices can be connected anytime, anywhere to the network

Mobility Issues

- Bandwidth restrictions and variability
- Location-aware network operation
    - User may wake up in a new environment
    - Dynamic replication of data
- Querying wireless data & location-based responses
- Busty network activity during connections & handling disconnections
- Disconnection
    - OS and File System Issues - allow for disconnected operation
    - Database System Issues - when disconnected, based on local data

Portability Issues

- Battery power restrictions
- Risks to data
    - Physical damage, loss, theft

- Unauthorized access

- encrypt data stored on mobiles

- Backup critical data to fixed (reliable) hosts

- Small user interface
  - Small displays due to battery power and aspect ratio constraints

  - Cannot open too many windows

  - Difficult to click on miniature icons

  - Input - Graffiti, (Dictionary-based) Expectation

    - Gesture or handwriting recognition with Stylus Pen Voice matching or voice recognition

1.1 APPLICATIONS

Vehicles

- transmission of news, road condition, weather, music via DAB
- personal communication using GSM
- position via GPS
- local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
- vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance

Emergencies

- early transmission of patient data to the hospital, current status, first diagnosis
- Replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc.
- crisis, war, ...

Travelling salesmen

- direct access to customer files stored in a central location
- consistent databases for all agents
- mobile office

Replacement of fixed networks

- remote sensors, e.g., weather, earth activities

- flexibility for trade shows
- LANs in historic buildings

Entertainment, education,

- outdoor Internet access
- intelligent travel guide with up-to-date location dependent information
- ad-hoc networks for multi user games

Location dependent services

Location aware services

- what services, e.g., printer, fax, phone, server etc. exist in the local environment

Follow-on services

- automatic call-forwarding, transmission of the actual workspace to the current location

Information services

- „push“: e.g., current special offers in the supermarket
- „pull“: e.g., where is the Black Forrest Cherry Cake?

Support services

- caches, intermediate results, state information etc. „follow“ the mobile device through the fixed network Privacy
- who should gain knowledge about the location

Effects of device portability

Power consumption

- limited computing power, low quality displays, small disks due to limited battery capacity
- CPU: power consumption ~ CV2f
    - C: internal capacity, reduced by integration
    - V: supply voltage, can be reduced to a certain limit
    - f: clock frequency, can be reduced temporally

Loss of data

- higher probability, has to be included in advance into the design (e.g., defects, theft)

Limited user interfaces

- compromise between size of fingers and portability
- integration of character/voice recognition, abstract symbols

Limited memory

- limited value of mass memories with moving parts
- Flash-memory or? as alternative

Wireless networks in comparison to fixed networks

Higher loss-rates due to interference

- emissions of, e.g., engines, lightning

Restrictive regulations of frequencies

- frequencies have to be coordinated, useful frequencies are almost all occupied Low transmission rates

- local some Mbit/s, regional currently, e.g., 9.6kbit/s with GSM .Higher delays, higher jitter
- connection setup time with GSM in the second range, several hundred milliseconds for other wireless systems

Lower security, simpler active attacking

- radio interface accessible for everyone, base station can be simulated, thus attracting calls from mobile phones

Always shared medium

- secure access mechanisms important

Early history of wireless communication

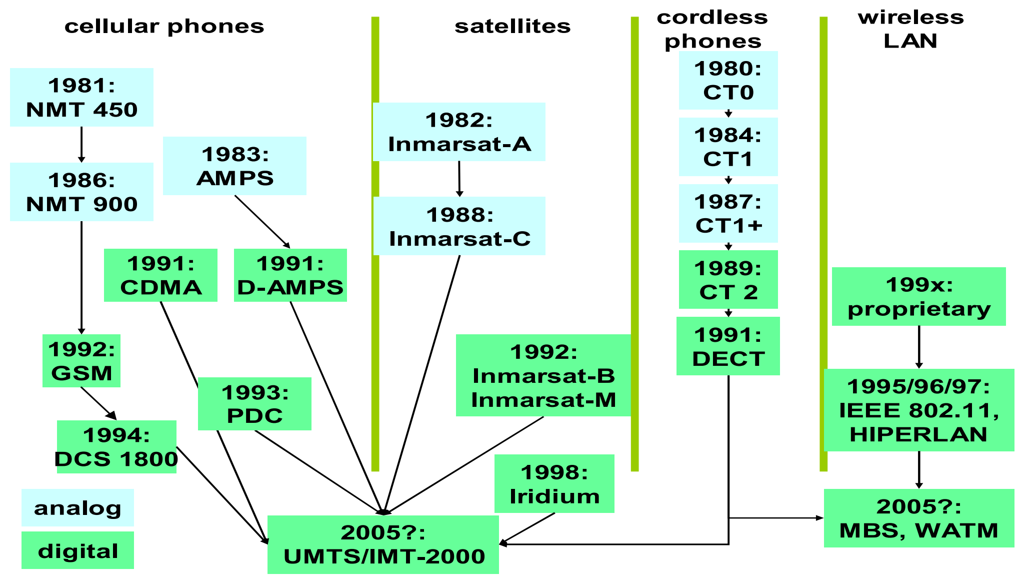
Many people in history used light for communication

- heliographs, flags („semaphore“), ...
- 150 BC smoke signals for communication;
  (Polybius, Greece)
- 1794, optical telegraph, Claude Chappe

Here electromagnetic waves are of special importance:

- 1831 Faraday demonstrates electromagnetic induction
- J. Maxwell (1831-79): theory of electromagnetic Fields, wave equations (1864)
- H. Hertz (1857-94): demonstrateswith an experiment the wave character of electrical transmission through space(1886, in Karlsruhe, Germany, at the location of today’s University of Karlsruhe)

Wireless systems: overview of the development



Areas of research in mobile communication

Wireless Communication

- transmission quality (bandwidth, error rate, delay)
- modulation, coding, interference
- media access, regulations

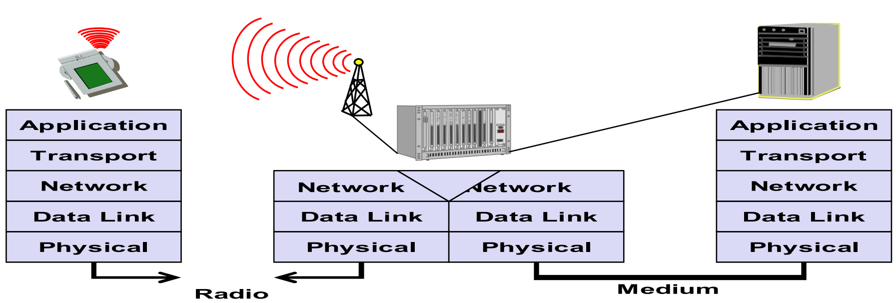
Mobility

- location dependent services
- location transparency
- quality of service support (delay, jitter, security)

Portability

- power consumption
- limited computing power, sizes of display, ...
- usability

Simple reference model used here



Influence of mobile communication to the LAYER MODEL

Application layer

- service location
- new applications, multimedia
- adaptive applications

Transport layer

- congestion and flow control
- quality of service

Network layer

- addressing, routing, device location
- hand-over

Data link layer

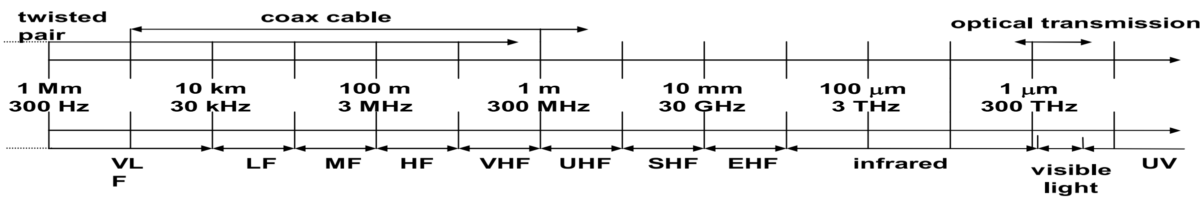
- authentication
- media access
- multiplexing
- media access control

Physical layer

- encryption
- modulation
- interference
- attenuation
- frequency

1.3 WIRELESS TRANSMISSION - FREQUENCIES FOR RADIO TRANSMISSION

Frequencies for communication



- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency

UHF = Ultra High Frequency
SHF = Super High Frequency
EHF = Extra High Frequency
UV = Ultraviolet Light

- Frequency and wave length:
- $\lambda = c/f$
- wave length λ, speed of light $c \cong 3\times10^8$ m/s, frequency f

Frequencies for mobile communication

- VHF-/UHF-ranges for mobile radio
  - simple, small antenna for cars
  - deterministic propagation characteristics, reliable connections

- SHF and higher for directed radio links, satellite communication
  - small antenna, focusing
  - large bandwidth available

- Wireless LANs use frequencies in UHF to SHF spectrum
  - some systems planned up to EHF
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
  - Weather dependent fading, signal loss caused by heavy rainfall etc.

Frequencies and regulations

ITU-R holds auctions for new frequencies, manages frequency bands worldwide (WRC, World Radio Conferences)

	Europe	USA	Japan
Mobile phones	**NMT** 453-457MHz, 463-467 MHz; **GSM** 890-915 MHz, 935-960 MHz; 1710-1785 MHz, 1805-1880 MHz	**AMPS**, **TDMA**, **CDMA** 824-849 MHz, 869-894 MHz; **TDMA**, **CDMA**, **GSM** 1850-1910 MHz, 1930-1990 MHz;	**PDC** 810-826 MHz, 940-956 MHz; 1429-1465 MHz, 1477-1513 MHz
Cordless telephones	**CT1+** 885-887 MHz, 930-932 MHz; **CT2** 864-868 MHz	**PACS** 1850-1910 MHz, 1930-1990 MHz **PACS-UB** 1910-1930 MHz	**PHS** 1895-1918 MHz **JCT** 254-380 MHz

1.4 SIGNALS

- physical representation of data
- function of time and location
- signal parameters: parameters representing the value of data

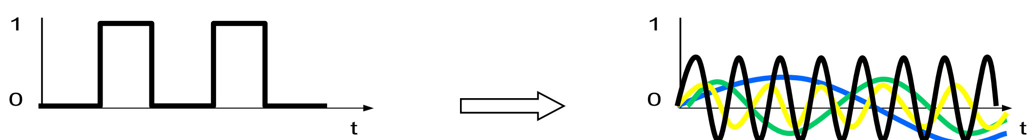
- classification
    - continuous time/discrete time
    - continuous values/discrete values
    - analog signal = continuous time and continuous values
    - digital signal = discrete time and discrete values

- signal parameters of periodic signals:
  period T, frequency f=1/T, amplitude A, phase shift φ
  - sine wave as special periodic signal for a carrier:

    s(t) = At sin(2 π ft t + φt)

Fourier representation of periodic signals

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$



Ideal periodic signal

Real composition (based on harmonics)

Different representations of signals

- amplitude (amplitude domain)
- frequency spectrum (frequency domain)
- phase state diagram (amplitude M and phase φ in polar coordinates)

Composed signals transferred into frequency domain using Fourier transformation

Digital signals need

- infinite frequencies for perfect transmission
- Modulation with a carrier frequency for transmission (analog signal!)

ANTENNAS

Isotropic radiator

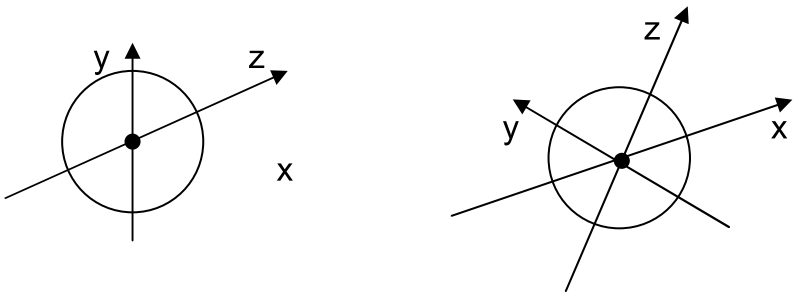
Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission

Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna

Real antennas always have directive effects (vertically and/or horizontally)

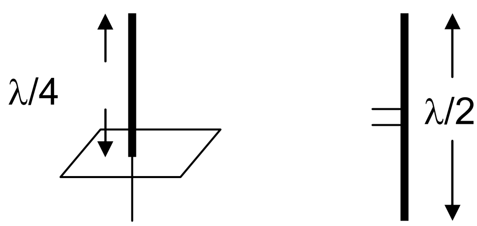
Radiation pattern: measurement of radiation around an antenna

Ideal isotropic radiator



Simple dipoles

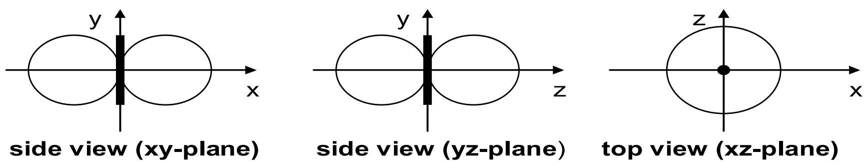
Real antennas are not isotropic radiators but, e.g., dipoles with lengths $\lambda/4$ on car roofs or $\lambda/2$ as Hertzian dipole,
shape of antenna proportional to wavelength



Example: Radiation pattern of a simple Hertzian dipole

- Real antennas are not isotropic radiators but, e.g., dipoles with lengths λ/4 on car roofs or λ/2 as Hertzian dipole shape of antenna proportional to wavelength

- Example: Radiation pattern of a simple Hertzian dipole

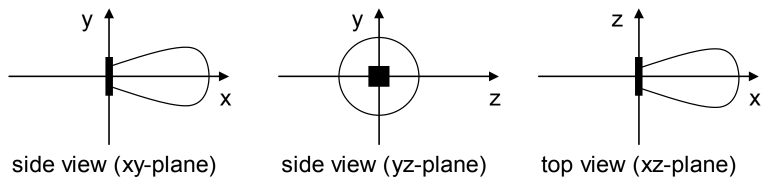


Simple dipole

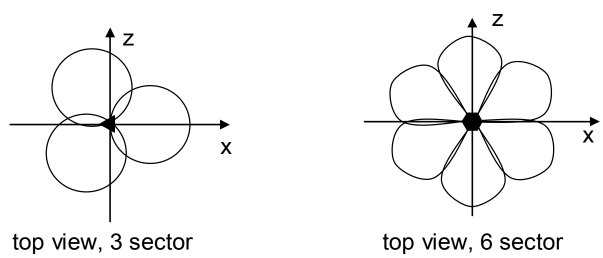
- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)

Directed and Sectorized

Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)



Directed antenna



Sectorized antenna

Antennas: diversity

Grouping of 2 or more antennas

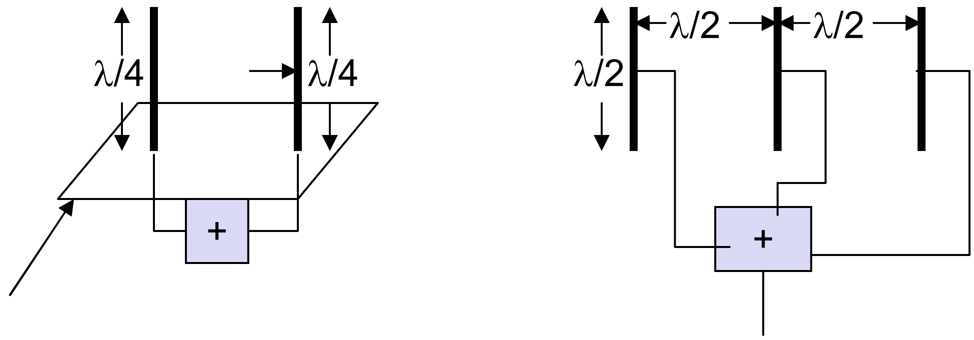
- multi-element antenna arrays

Antenna diversity

- switched diversity, selection diversity
    - receiver chooses antenna with largest output

diversity combining

- combine output power to produce gain
- cophasing needed to avoid cancellation



SIGNAL PROPAGATION

Transmission range

- communication possible
- low error rate

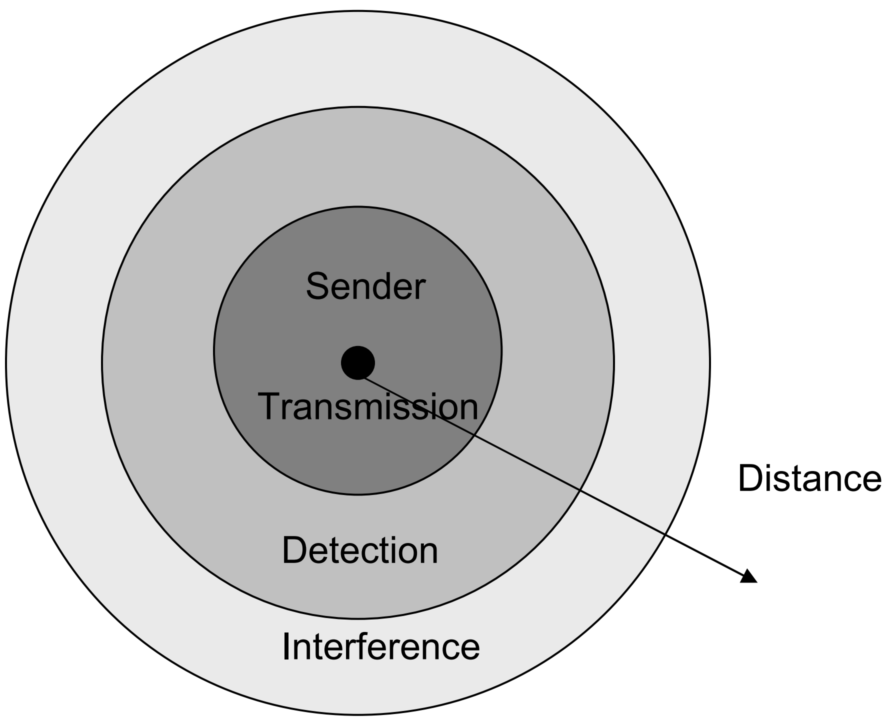
Detection range

- detection of the signal possible
- no communication possible

Interference range

- signal may not be detected

- signal adds to the background noise



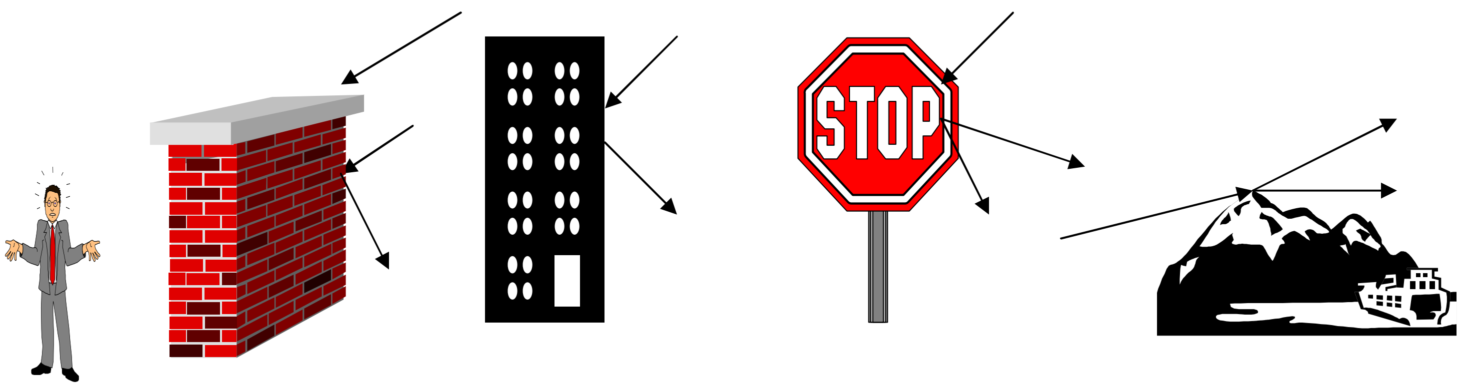
Signal propagation

Propagation in free space always like light (straight line)

Receiving power proportional to $1/d^2$
(d = distance between sender and receiver)

Receiving power additionally influenced by

- fading (frequency dependent)
- shadowing
- reflection at large obstacles
- scattering at small obstacles
- diffraction at edges



Shadowing **Reflection** **Scattering** **Diffraction**

Multipath propagation

Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction

Time dispersion: signal is dispersed over time

➔ Interference with “neighbor” symbols, Inter Symbol Interference (ISI)

The signal reaches a receiver directly and phase shifted

➔ Distorted signal depending on the phases of the different parts

Effects of mobility

Channel characteristics change over time and location

- signal paths change
- different delay variations of different signal parts
- different phases of signal parts

➔Quick changes in the power received (short term fading)

Additional changes in

- distance to sender
- obstacles further away

➔ Slow changes in the average power received (long term fading)

MULTIPLEXING

Multiplexing in 4 dimensions

- space (si)
- time (t)
- frequency (f)
- code (c)

Frequency Division Multiplexing - FDM

The oldest used technique used for multiplexing. Possible when the useful bandwidth of the medium exceeds that of the signals it has to carry. Each signal is modulated on a different carrier frequency. This results in shifting the spectrum of the signal around the carrier frequency. Sufficient guard-band is given so those neighboring signals do not overlap in the frequency domain.

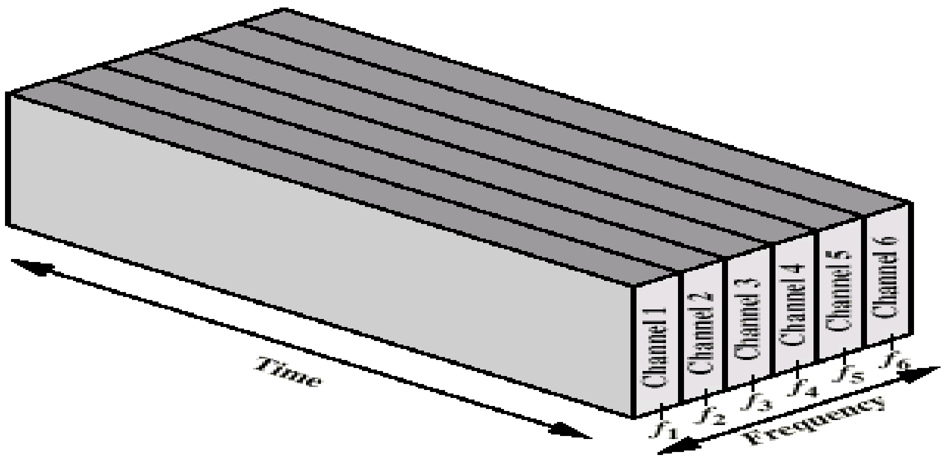
At the receiving end each signal is extracted by first passing it through a band-pass filter and then demodulating with the same carrier frequency that was used to modulate the signal. The signals carried using FDM may be analog signals or may be analog signals representing digital data. However FDM is mostly a technique from the era of analog communications. In FDM a device uses some of the channel all of the time. FDM is used in radio and television broadcasting. FDM is also used in high capacity long distance links in the telephone network.

Frequency division multiplexing (FDM) achieves multiplexing by using different carrier frequencies .Receiver can "tune" to specific frequency and extract modulation for that one channel .Frequencies must be separated to avoid interference - “Wastes” potential signal bandwidth for guard channels.Only useful in media that can carry multiple signals with different frequencies - high-bandwidth required .

Used in:

- The standard of the analog telephone network
- The standard in radio broadcasting
- The standard for video
    1. Broadcast
    2. Cable
    3. Satellite

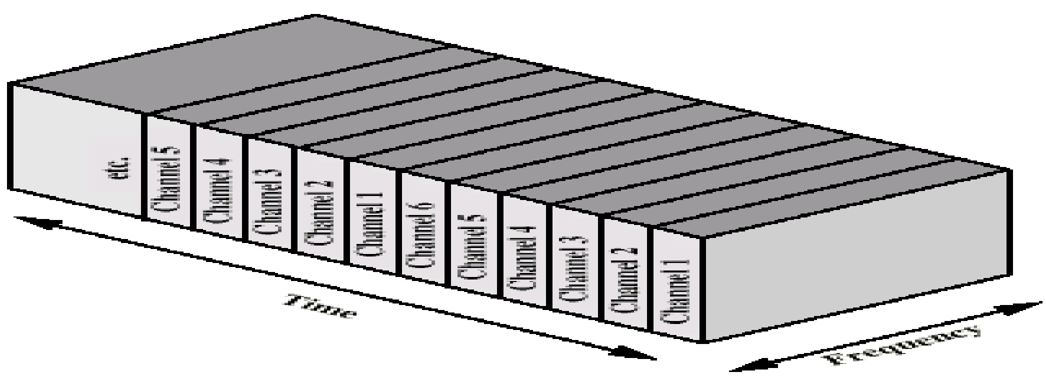
Frequency Division Multiplexing Diagram



Time Division Multiplexing - TDM

Time division multiplexing is more suitable for digital data. TDM can be used when the data rate available on a communication link exceeds the data rate required by any one of the sources. In TDM each source that is to use the link fills up a buffer with data. A TDM multiplexer scans the buffers in some predetermined order and transmits bits from each source one after the other.

- Requires digital signaling & transmission
- Requires data rate = sum of inputs + framing
- Data rate much higher than equivalent analog bandwidth uses
- Separates data streams in time not frequency
- The standard of the modern digital telephone system



Code Division Multiplexing - CDM

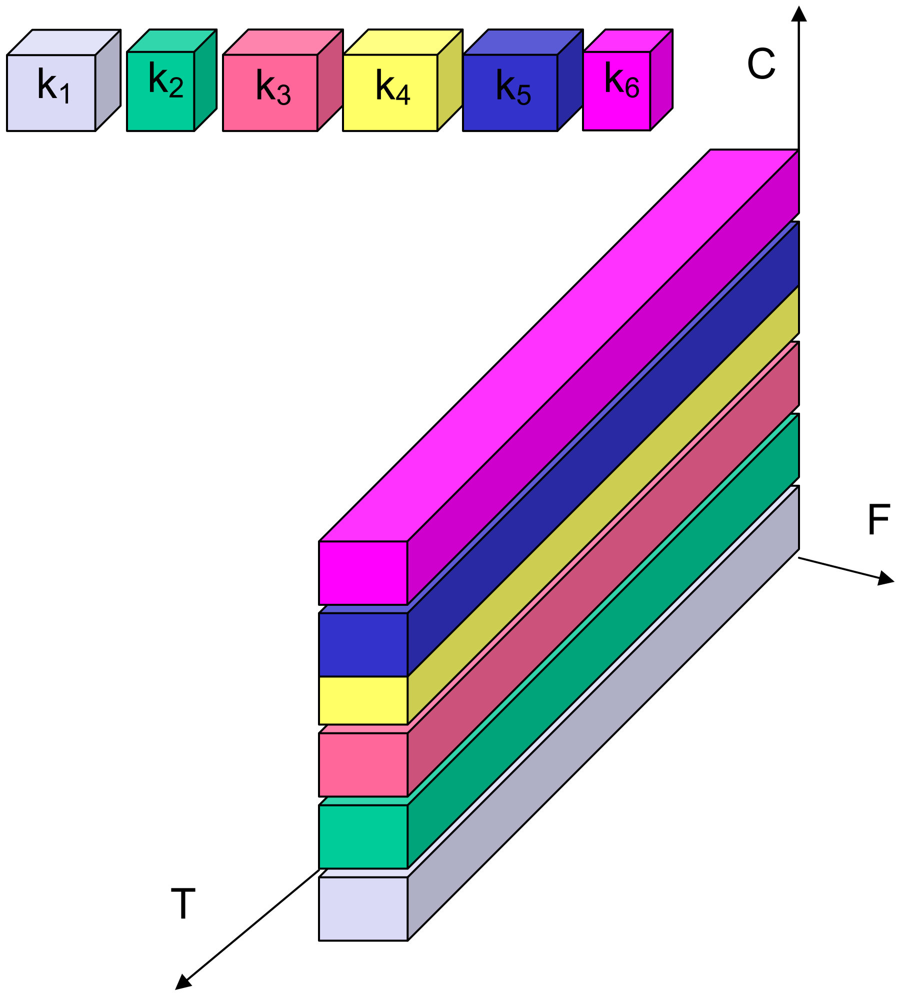
Each channel has a unique code. All channels use the same spectrum at the same time.

Advantages:

- bandwidth efficient
- no coordination and synchronization necessary
- good protection against interference and tapping

Disadvantages:

- lower user data rates
- more complex signal regeneration



k1
k2
k3
k4
k5
k6
C
F
T

MODULATIONS

Digital modulation

- digital data is translated into an analog signal (baseband)
- ASK, FSK, PSK - main focus in this chapter
- differences in spectral efficiency, power efficiency, robustness

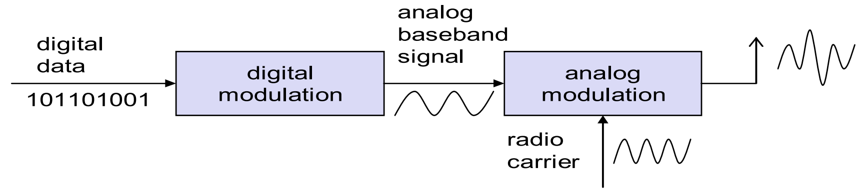
Analog modulation

- shifts center frequency of baseband signal up to the radio carrier Motivation
- smaller antennas (e.g., $\lambda/4$)
- Frequency Division Multiplexing
- medium characteristics

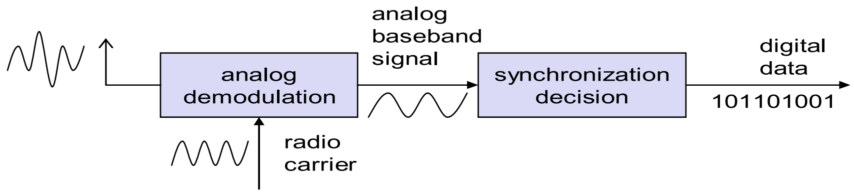
Basic schemes

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM)

Modulation and demodulation



Radio transmitter



Radio receiver

<u>Digital modulation</u>

Modulation of digital signals known as Shift Keying.

<u>Amplitude Shift Keying (ASK):</u>

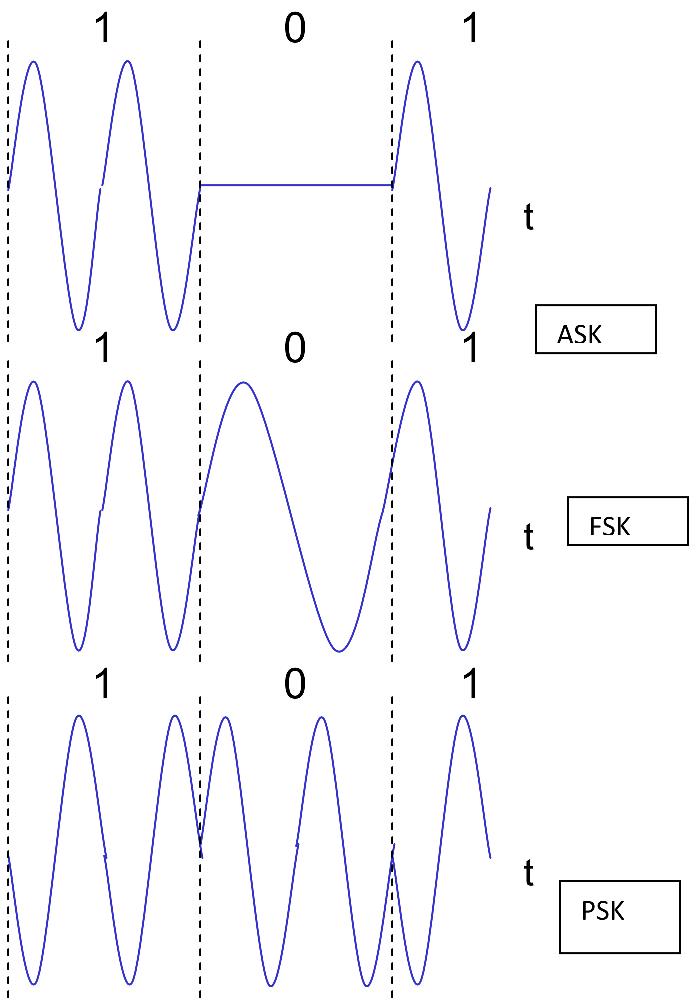
- very simple
- low bandwidth requirements
- very susceptible to interference

<u>Frequency Shift Keying (FSK):</u>

- needs larger bandwidth

Phase Shift Keying (PSK):

- more complex
- robust against interference



Advanced Frequency Shift Keying

- bandwidth needed for FSK depends on the distance between the carrier frequencies

- special pre-computation avoids sudden phase shifts
  ➔ MSK (Minimum Shift Keying)
- bit separated into even and odd bits, the duration of each bit is doubled
- depending on the bit values (even, odd) the higher or lower frequency, original or inverted is chosen
- the frequency of one carrier is twice the frequency of the other
- even higher bandwidth efficiency using a Gaussian low-pass filter
  ➔ GMSK (Gaussian MSK), used in GSM.

Advanced Phase Shift Keying

BPSK (Binary Phase Shift Keying):

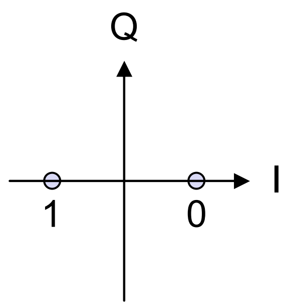
- bit value 0: sine wave
- bit value 1: inverted sine wave
- very simple PSK
- low spectral efficiency
- robust, used e.g. in satellite systems

QPSK (Quadrature Phase Shift Keying):

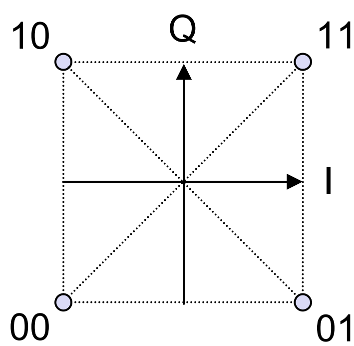
- 2 bits coded as one symbol
- symbol determines shift of sine wave
- needs less bandwidth compared to BPSK
- more complex

Often also transmission of relative, not absolute phase shift: DQPSK - Differential QPSK (IS-136, PACS, PHS

BPSK (Binary Phase Shift Keying):



QPSK (Quadrature Phase Shift Keying):



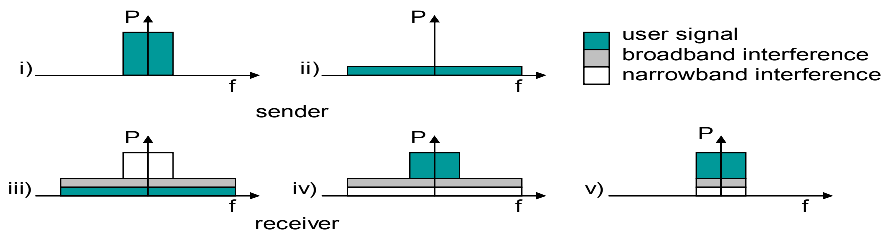
Quadrature Amplitude Modulation

Quadrature Amplitude Modulation (QAM): combines amplitude and phase modulation

- it is possible to code n bits using one symbol
- 2n discrete levels, n=2 identical to QPSK
- bit error rate increases with n, but less errors compared to comparable PSK schemes

SPREAD SPECTRUM

Effects of spreading and interference



DSSS (Direct Sequence Spread Spectrum)

XOR of the signal with pseudo-random number (chipping sequence)

- many chips per bit (e.g., 128) result in higher bandwidth of the signal

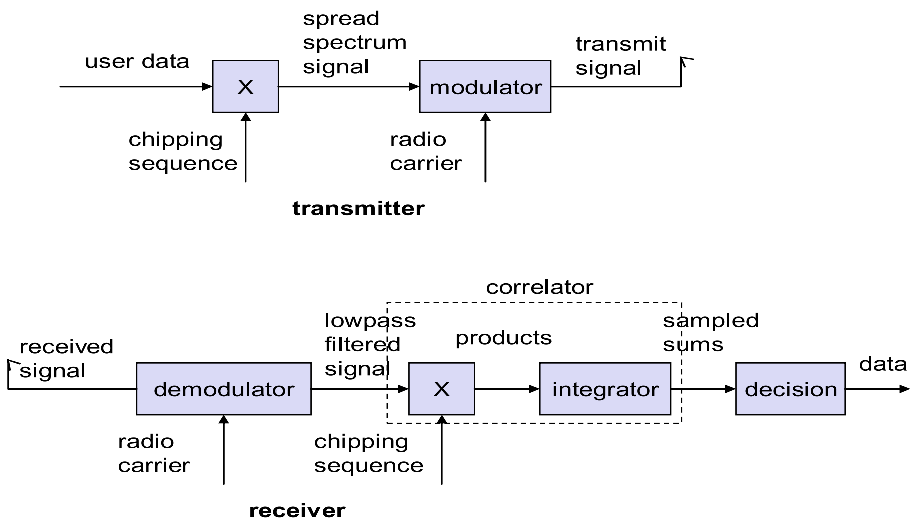
Advantages

- reduces frequency selective fading
- in cellular networks

- base station scan use the same frequency range several base stations can detect and recover the signal
- soft handover

Disadvantages

- precise power control necessary



FHSS (Frequency Hopping Spread Spectrum)

Discrete changes of carrier frequency

- sequence of frequency changes determined via pseudo random number sequence

Two versions

- Fast Hopping:
  several frequencies per user bit
- Slow Hopping:
  several user bits per frequency

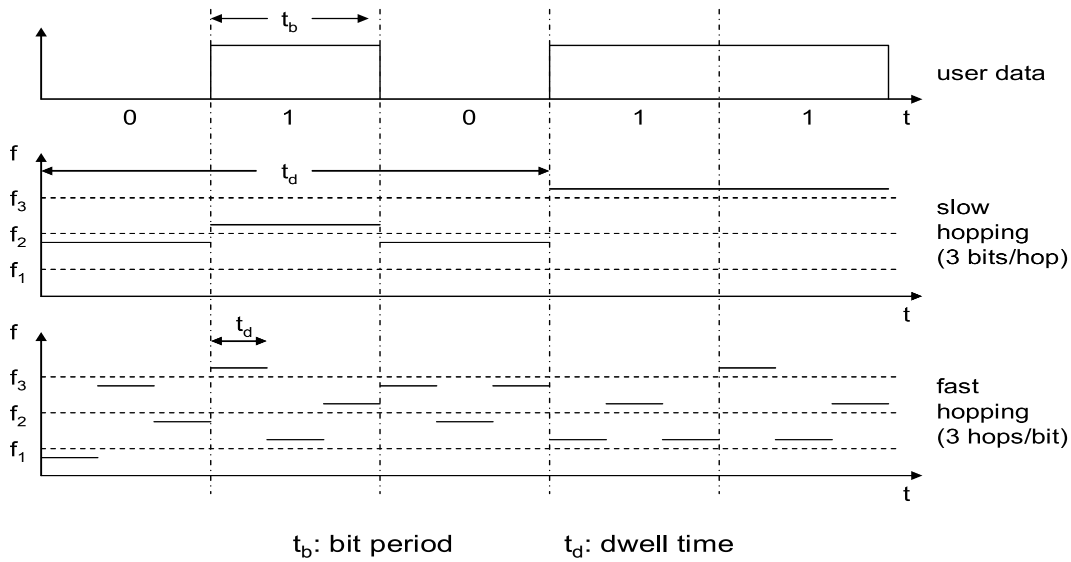
Advantages

- frequency selective fading and interference limited to short period
- simple implementation
- uses only small portion of spectrum at any time

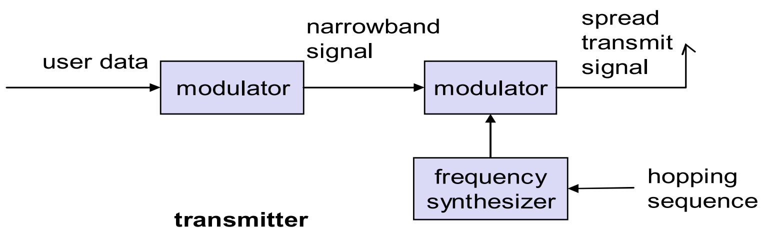
Disadvantages

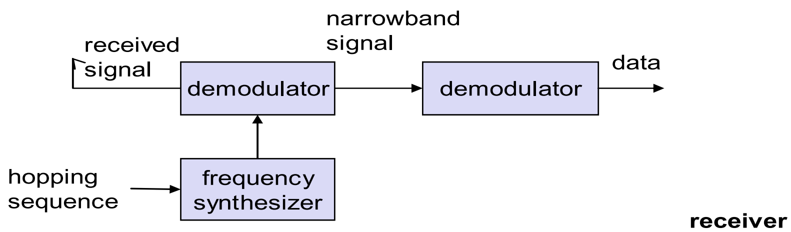
- not as robust as DSSS
- simpler to detect

FHSS (Frequency Hopping Spread Spectrum)



Frequency Hopping Spread Spectrum





MAC

Medium Access Control (MAC)

MAC protocol which were developed for nodes at short distance did not show good performance for nodes at longer distance so another protocol has to be developed Known as 2p MAC Protocol.

802.11 protocols were good for devices which had no power supply issue frequent charging were available to them etc.

1. This protocol based devices were not good for certain operation like monitoring the natural habitat of wildlife.
2. Sampling the water level of dam.

These applications do not require frequent human intervention and are required to run for a longer duration.

To fulfill the requirement other protocol was developed **sensor network (802.15.4)**

- Energy Budgets:-Main points which were discussed in this were how its protocol helps in saving power by cleverly managing the time when device should sleep when to wake up.
- MAC protocol used in 802.15.4.
- Routing and tree formation in ZigBee: - Routing protocol was developed by Zigbee firm.

Wireless MAC Issues

Wireless medium makes the MAC design more challenging than the wireline networks.

The three important issues are:

1. Half Duplex operation –> either send or receive but not both at a given time
2. Time varying channel
3. Burst channel errors

1. Half Duplex Operation

In wireless, it's difficult to receive data when the transmitter is sending the data, because:

When node is transmitting, a large fraction of the signal energy leaks into the receiver path

The transmitted and received power levels can differ by orders of magnitude

The leakage signal typically has much higher power than the received signal ->"Impossible to detect a received signal, while transmitting data"

Collision detection is not possible, while sending data

As collision cannot be detected by the sender, all proposed protocols attempt to minimize the probability of collision -> Focus on collision avoidance

2. Time Varying Channel

Three mechanisms for radio signal propagation

- **Reflection** – occurs when a propagating wave impinges upon an object that has very large dimensions than the wavelength of the radio wave e.g. reflection occurs from the surface of the earth and from buildings and walls
- **Diffraction** – occurs when the radio path between the transmitter and the receiver is obstructed by a surface with sharp edges
- **Scattering** – occurs when the medium through which the wave travels consists of objects with

The received signal by a node is a superposition of time-shifted and attenuated versions of the ransmitted signals the received signal varies with time .The time varying signals (time varying channel) phenomenon also known as multipath propagation.The rate of variation of channel is determined by the coherence time of the hannel Coherence time is defined as time within which When a node's received signal strength drops below a certain threshold the node is said to be in fade .Handshaking is widely used strategy to ensure the link quality is good enough for data communication. A successful handshake between a sender and a receiver (small message) indicates a good communication link.

3. Burst Channel Errors

As a consequence of time varying channel and varying signals strengths errors are introduced in the transmission (Very likely) for wire line networks the bit error rate (BER) is the probability of packet error is small .For wire line networks the errors are due to random For wireless networks the BER is as high.For wireless networks the errors are due to node being in fade as a result errors occur in a long burst. Packet loss due to burst errors - mitigation techniques

- » Smaller packets
- » Forward Error Correcting Codes
- » Retransmissions (Acks)
-

Location Dependent Carrier Sensing

Location Dependent Carrier Sensing results in three types of nodes that protocols need to deal with:

Hidden Nodes

Even if the medium is free near the transmitter, it may not be free near the intended receiver

Exposed Nodes

Even if the medium is busy near the transmitter, it may be free near the intended receiver

Capture

Capture occurs when a receiver can cleanly receive a transmission from one of two simultaneous transmissions

Hidden Node/Terminal Problem

A hidden node is one that is within the range of the intended destination but out of range of sender Node B can communicate with A and C both A and C cannot hear each other When A transmits to B, C cannot detect the transmission using the carrier sense mechanism C falsely thinks that the channel is idle

Exposed Nodes

An exposed node is one that is within the range of the sender but out of range of destination .when a node's received signal strength drops below a certain threshold the node is said to be in fade .Handshaking is widely used strategy to ensure the link quality is good enough for data communication. A successful handshake between a sender and a receiver (small message) indicates a good communication link.

In theory C can therefore have a parallel transmission with any node that cannot hear the transmission from B, i.e. out of range of B. But C will not transmit to any node because its an exposed node. Exposed nodes waste bandwidth.

Capture

Capture is said to occur when a receiver can cleanly receive a transmission from one of two simultaneous transmissions both within its range Assume node A and D transmit simultaneously to B. The signal strength received from D is much higher than that from A, and D’s transmission can be decoded without errors in presence of transmissions from A.D has captured A. Capture is unfair because it gives preference to nodes that are closer to the receiver. It may improve protocol performance

MULTIPLE ACCESS

FDMA

It is an ANALOQUE technique in time. Synchronization the transmission bandwidth is partitioned to frequency slots different users has different RF carrier frequencies, i.e. Each user is assigned a particular frequency slot.

users/signals are at the receiver by separated out FILTERING if all frequency slots are occupied then the system has reached its.

TDMA

It is a DIGITAL technique requires between users synchronization each user/signal is assigned a particular (within a time-frame) time slot.

CELLULAR WIRELESS NETWORKS

Implements space division multiplex: base station covers a certain transmission area (cell).Mobile stations communicate only via the base station

Advantages of cell structures:

- higher capacity, higher number of users
- less transmission power needed
- more robust, decentralized
- base station deals with interference, transmission area etc. locally

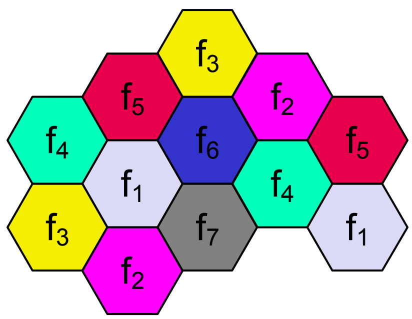
Problems:

- fixed network needed for the base stations
- handover (changing from one cell to another) necessary
- interference with other cells

Cell sizes from some 100 m in cities to, e.g., 35 km on the country side (GSM) - even less for higher frequencies

Frequency reuse only with a certain distance between the base stations

Standard model using 7 frequencies:



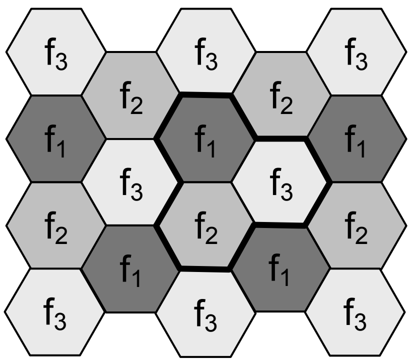
Fixed frequency assignment:

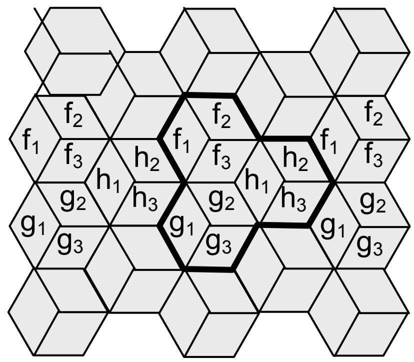
- certain frequencies are assigned to a certain cell
- problem: different traffic load in different cells

Dynamic frequency assignment:

- base station chooses frequencies depending on the frequencies already used in neighbor cells

- ❑ more capacity in cells with more traffic
- ❑ assignment can also be based on interference measurements





3 cell cluster **3 cell cluster with 3 sector antennas**

<u>Cell : Why Hexagon?</u>

- In reality the cell is an irregular shaped circle, for design convenience and as a first order approximation, it is assumed to be regular polygons

- The hexagon is used for two reasons:
  – A hexagonal layout requires fewer cells, therefore, fewer transmission site

    – Less expensive compared to square and triangular cells

- Irregular cell shape leads to inefficient use of the spectrum because of inability to reuse frequency on account of co channel interference uneconomical deployment of equipment, requiring relocation from one cell site to another

UNIT II

TELECOMMUNICATION NETWORKS

Telecommunication systems – GSM – GPRS – DECT – UMTS – IMT-2000 – Satellite Networks - Basics – Parameters and Configurations – Capacity Allocation – FAMA and DAMA – Broadcast Systems – DAB - DVB.

Telecommunication systems -GSM – GPRS – DECT – UMTS – IMT-2000

Building Blocks

- AMPS – Advanced Mobile Phone System
- TACS – Total Access Communication System
- NMT – Nordic Mobile Telephone System

AMPS – Advanced Mobile Phone System

- analog technology
- used in North and South America and approximately 35 other countries
- operates in the 800 MHz band using FDMA technology

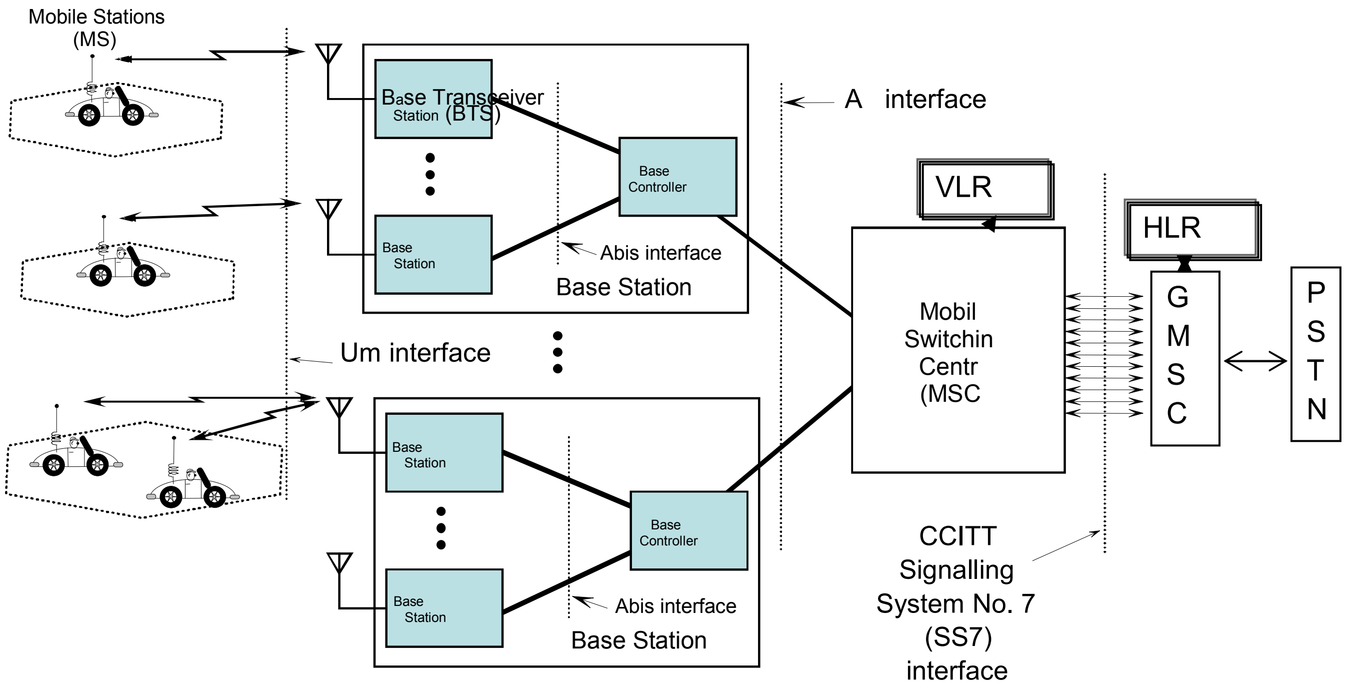
TACS – Total Access Communication System

- variant of AMPS
- deployed in a number of countries
- primarily in the UK

NMT – Nordic Mobile Telephone System

- analog technology
- deployed in the Benelux countries and Russia
- operates in the 450 and 900 MHz band
- first technology to offer international roaming – only within the Nordic countries

System Architecture



Mobile Station (MS)

Mobile Equipment (ME)

Subscriber Identity Module (SIM)

Base Station Subsystem (BBS)

Base Transceiver Station (BTS)

Base Station Controller (BSC)

Network Subsystem

Mobile Switching Center (MSC)

Home Location Register (HLR)

Visitor Location Register (VLR)

Authentication Center (AUC)

Equipment Identity Register (EIR)

- Mobile Station: is a subscriber unit intended for use while on the move at unspecified locations. It could be a hand-held or a portable terminal.

- Base Station: a fixed radio station used for communication with MS. It is located at the centre of a cell and consist of Transmitters and Receivers.

- Mobile Switching Centre: it coordinates the routing of calls, do the billing, etc.

Mobile Station (MS)

The Mobile Station is made up of two entities:

1. Mobile Equipment (ME)
2. Subscriber Identity Module (SIM

Mobile Equipment

- Produced by many different manufacturers
- Must obtain approval from the standardization body
- Uniquely identified by an IMEI (International Mobile Equipment Identity)

Subscriber Identity Module (SIM)

- Smart card containing the International Mobile Subscriber Identity (IMSI)
- Allows user to send and receive calls and receive other subscribed services
- Encoded network identification details
- Protected by a password or PIN
- Can be moved from phone to phone – contains key information to activate the phone

Base Station Subsystem (BBS)

Base Station Subsystem is composed of two parts that communicate across the standardized Abis interface allowing operation between components made by different suppliers

1. Base Transceiver Station (BTS)

1. Base Station Controller (BSC)

Base Transceiver Station (BTS)

- Houses the radio transceivers that define a cell
- Handles radio-link protocols with the Mobile Station
- Speech and data transmissions from the MS are recoded
- Requirements for BTS:
    - ruggedness
    - reliability
    - portability
    - minimum costs

Base Station Controller (BSC)

- Manages Resources for BTS
- Handles call set up
- Location update
- Handover for each MS

Network Subsystem

Mobile Switching Center (MSC)

- Switch speech and data connections between:
  Base Station Controllers

Mobile Switching Centers

GSM-networks

Other external networks

- Heart of the network
- Three main jobs:

1) Connects calls from sender to receiver

2) Collects details of the calls made and received

3) Supervises operation of the rest of the network component

Home Location Registers (HLR)

- contains administrative information of each subscriber

- Current location of the mobile

Visitor Location Registers (VLR)

- contains selected administrative information from the HLR

- authenticates the user
- tracks which customers have the phone on and ready to receive a call
- periodically updates the database on which phones are turned on and ready to receive calls

Authentication Center (AUC)

- mainly used for security
- data storage location and functional part of the network
- Ki is the primary element

Equipment Identity Register (EIR)

Database that is used to track handsets using the IMEI (International Mobile Equipment Identity)

- Made up of three sub-classes: The White List, The Black List and the Gray List
- Optional database

Basic Features Provided by GSM

- Call Waiting

- Notification of an incoming call while on the handset

- Call Hold

- Put a caller on hold to take another call

- Call Barring

- All calls, outgoing calls, or incoming calls

- Call Forwarding

- Calls can be sent to various numbers defined by the user

- Multi Party Call Conferencing

- Link multiple calls together

Advanced Features Provided by GSM

- Calling Line ID
  - incoming telephone number displayed
- Alternate Line Service
  - one for personal calls

  - one for business calls
- Closed User Group
  - call by dialing last for numbers
- Advice of Charge
  - tally of actual costs of phone calls
- Fax & Data
  - Virtual Office / Professional Office

- Roaming
  - services and features can follow customer from market to market

Advantages of GSM

- Crisper, cleaner quieter calls
- Security against fraud and eavesdropping
- International roaming capability in over 100 countries
- Improved battery life
- Efficient network design for less expensive system expansion
- Efficient use of spectrum
- Advanced features such as short messaging and caller ID
- A wide variety of handsets and accessories
- High stability mobile fax and data at up to 9600 baud
- Ease of use with over the air activation, and all account information is held in a smart card which can be moved from handset to handset

UMTS (Universal Mobile Telephone System)

- Reasons for innovations
  - new service requirements
  - availability of new radio bands

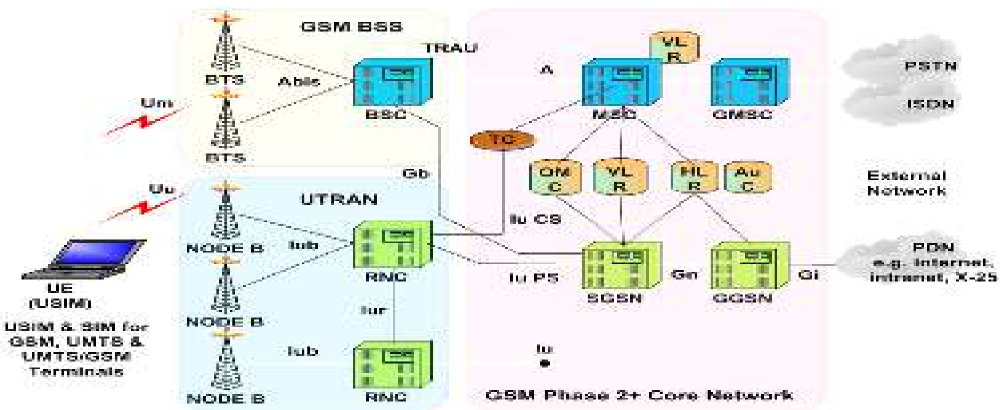
- User demands
  - seamless Internet-Intranet access
  - wide range of available services
  - compact, lightweight and affordable terminals
  - simple terminal operation
  - open, understandable pricing structures for the whole spectrum of available services

UMTS Basic Parameter

- Frequency Bands (FDD : 2x60 MHz):
  - 1920 to 1980 MHz (Uplink)
  - 2110 to 2170 MHz (Downlink)
- Frequency Bands (TDD: 20 + 15 MHz):
  - 1900 – 1920 MHz and 2010 – 2025 MHz
- RF Carrier Spacing:
  - 4.4 - 5 MHz

- RF Channel Raster:
  - 200 KHz
- Power Control Rate:
  - 1500 Cycles per Second

UMTS W-CDMA Architecture



SATELLITE NETWORKS

History of satellite communication

1945 Arthur C. Clarke publishes an essay about „Extra

Terrestrial Relays“

1957 first satellite SPUTNIK

1960 first reflecting communication satellite ECHO

1963 first geostationary satellite SYNCOM

1965 first commercial geostationary satellite Satellit „Early Bird“

(INTELSAT I): 240 duplex telephone channels or 1 TV

channel, 1.5 years lifetime

1976 three MARISAT satellites for maritime communication

1982 first mobile satellite telephone system INMARSAT-A

1988 first satellite system for mobile phones and data

communication INMARSAT-C

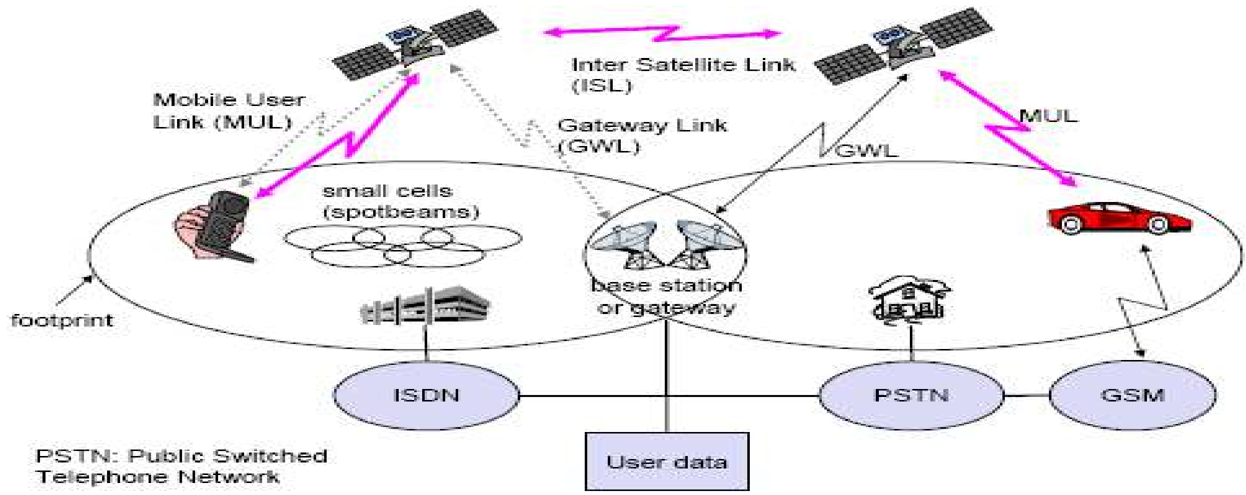
1993 first digital satellite telephone system

1998 global satellite systems for small mobile phones

Applications

- Traditionally
    - weather satellites
    - radio and TV broadcast satellites
    - military satellites
    - satellites for navigation and localization (e.g., GPS)
- Telecommunication
    - global telephone connections
    - backbone for global networks
    - connections for communication in remote places or underdeveloped areas
    - global mobile communication
- satellite systems to extend cellular phone systems (e.g., GSM orAMPS)

Classical satellite systems



Basics

Satellites in circular orbits

- attractive force $F_g = m\, g\, (R/r)^2$
- centrifugal force $F_c = m\, r\, \omega^2$
- m: mass of the satellite
- R: radius of the earth (R = 6370 km)
- r: distance to the center of the earth
- g: acceleration of gravity ($g = 9.81\ m/s^2$)
- ω: angular velocity (ω = 2 π f, f: rotation frequency)

Stable orbit

$F_g = F_c$

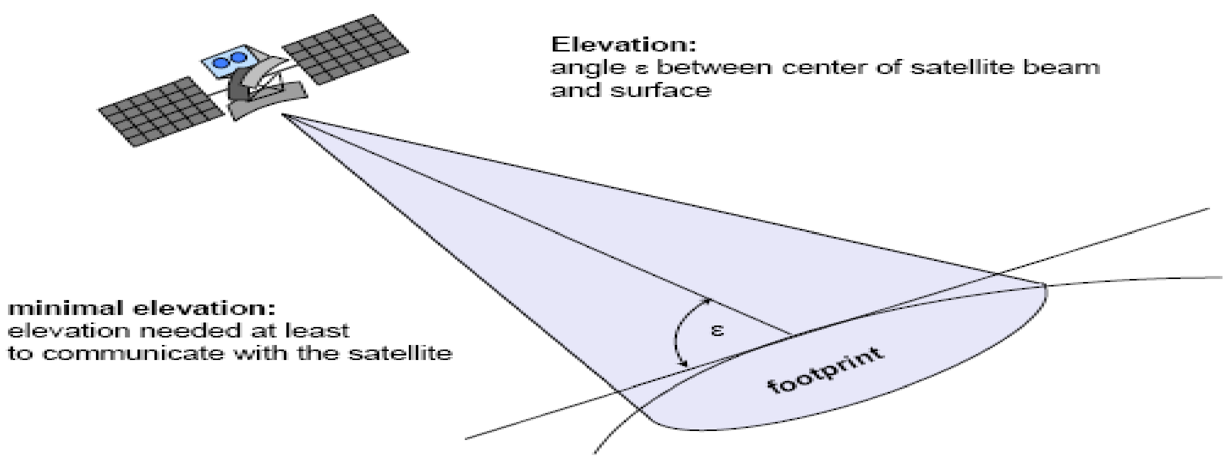
$$r = \sqrt[3]{\frac{gR^2}{(2\pi f)^2}}$$

Basics

- Elliptical or circular orbits
- Complete rotation time depends on distance satellite-earth
- Inclination: angle between orbit and equator
- Elevation: angle between satellite and horizon
- LOS (Line of Sight) to the satellite necessary for connection
    1. High elevation needed, less absorption due to e.g. buildings
- Uplink: connection base station - satellite
- Downlink: connection satellite - base station
- Typically separated frequencies for uplink and downlink
    1. Transponder used for sending/receiving and shifting of frequencies
    2. Transparent transponder: only shift of frequencies
    3. Regenerative transponder: additionally signal regeneration

I

Elevation



Link budget of satellites

Parameters like attenuation or received power determined by four parameters:

Sending power

Gain of sending antenna

Distance between sender and receiver

Gain of receiving antenna Problems

Varying strength of received signal due to multipath propagation

Interruptions due to shadowing of signal (no LOS) possible solutions

Link Margin to eliminate variations in signal strength

Satellite diversity (usage of several visible satellites at the same time) helps to use less sending power

$$L = \left(\frac{4\pi r f}{c} \right)^2$$

L: Loss

f: carrier frequency

r: distance

c: speed of light

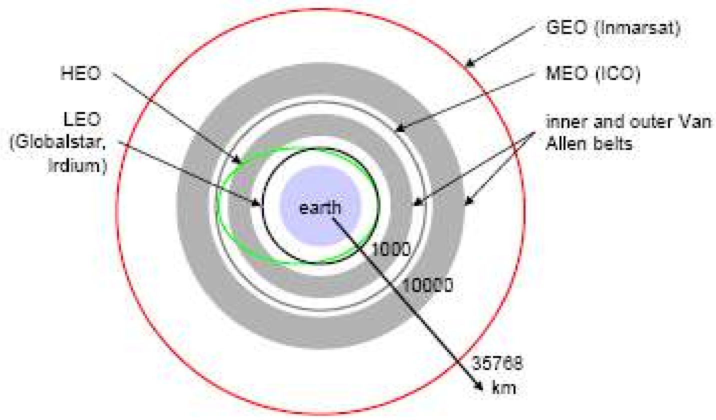
ORBITS

Four different types of satellite orbits can be identified depending on the shape and diameter of the orbit:

- GEO: geostationary orbit, ca. 36000 km above earth surface
- LEO (Low Earth Orbit): ca. 500 - 1500 km
- MEO (Medium Earth Orbit) or ICO (Intermediate Circular Orbit):

ca. 6000 - 20000 km

- HEO (Highly Elliptical Orbit) elliptical orbits



Van-Allen-Belts: ionized particles 2000 - 6000 km and 15000 - 30000 km above earth surface

Geostationary satellites

Orbit 35,786 km distance to earth surface, orbit in equatorial plane (inclination 0°)

Complete rotation exactly one day, satellite is synchronous to earth rotation

Fix antenna positions, no adjusting necessary

Satellites typically have a large footprint (up to 34% of earth surface!), therefore difficult to reuse frequencies

Bad elevations in areas with latitude above 60° due to fixed position above the equator

High transmit power needed

High latency due to long distance (ca. 275 ms)

Not useful for global coverage for small mobile phones and data transmission, typically used for radio and TV transmission

LEO systems

Orbit ca. 500 - 1500 km above earth surface

Visibility of a satellite ca. 10 - 40 minutes

Global radio coverage possible

Latency comparable with terrestrial long distance

Connections, ca. 5 - 10 ms

Smaller footprints, better frequency reuse

But now handover necessary from one satellite to another

Many satellites necessary for global coverage

More complex systems due to moving satellites

Examples:

Iridium (start 1998, 66 satellites)

Global star (start 1999, 48 satellites)

MEO systems

Orbit ca. 5000 - 12000 km above earth surface

Comparison with LEO systems:

Slower moving satellites

Less satellites needed

Simpler system design

For many connections no hand-over needed

Higher latency, ca. 70 - 80 ms

Higher sending power needed

Special antennas for small footprints needed

Example:

ICO (Intermediate Circular Orbit, Inmarsat) start ca. 2000

Routing

One solution: inter satellite links (ISL)

Reduced number of gateways needed

Forward connections or data packets within the satellite network as long as possible

Only one uplink and one downlink per direction needed for the connection of two mobile phones

Problems:

More complex focusing of antennas between satellites

High system complexity due to moving routers

Higher fuel consumption

Thus shorter lifetime

Iridium and Teledesic planned with ISL

Other systems use gateways and additionally terrestrial networks

Localization of mobile stations

Mechanisms similar to GSM

Gateways maintain registers with user data

HLR (Home Location Register): static user data

VLR (Visitor Location Register): (last known) location of the mobile station

SUMR (Satellite User Mapping Register):

Satellite assigned to a mobile station

Positions of all satellites

Registration of mobile stations

- Localization of the mobile station via the satellite's position
- Requesting user data from HLR
- Updating VLR and SUMR

Calling a mobile station

- Localization using HLR/VLR similar to GSM
- Connection setup using the appropriate satellite

Handover in satellite systems

Several additional situations for handover in satellite systems compared to cellular terrestrial mobile phone networks caused by the movement of the satellites

Intra satellite handover

- Handover from one spot beam to another
- Mobile station still in the footprint of the satellite, but in another cell

Inter satellite handover

- Handover from one satellite to another satellite
- Mobile station leaves the footprint of one satellite

Gateway handover

- Handover from one gateway to another
- Mobile station still in the footprint of a satellite, but gateway leaves the footprint

Inter system handover

- Handover from the satellite network to a terrestrial cellular network
- Mobile station can reach a terrestrial network again which might be cheaper, has a lower latency etc.

Overview of LEO/MEO systems

	Iridium	Globalstar	ICO	Teledesic
# satellites	66 + 6	48 + 4	10 + 2	288
altitude (km)	780	1414	10390	ca. 700
coverage	global	±70° latitude	global	global
min. elevation	8°	20°	20°	40°
frequencies [GHz (circa)]	1.6 MS 29.2 ↑ 19.5 ↓ 23.3 ISL	1.6 MS ↑ 2.5 MS ↓ 5.1 ↑ 6.9 ↓	2 MS ↑ 2.2 MS ↓ 5.2 ↑ 7 ↓	19 ↓ 28.8 ↑ 62 ISL
access method	FDMA/TDMA	CDMA	FDMA/TDMA	FDMA/TDMA
ISL	yes	no	no	yes
bit rate	2.4 kbit/s	9.6 kbit/s	4.8 kbit/s	64 Mbit/s ↓ 2/64 Mbit/s ↑
# channels	4000	2700	4500	2500
Lifetime [years]	5-8	7.5	12	10
cost estimation	4.4 B$	2.9 B$	4.5 B$	9 B$

UNIT III

WIRLESS LAN

Wireless LAN – IEEE 802.11 - Architecture – services – MAC – Physical layer – IEEE 802.11a - 802.11b standards – HIPERLAN – Blue Tooth.

WIRELESS LAN

Characteristics of wireless LANs

Advantages

- Very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Disadvantages

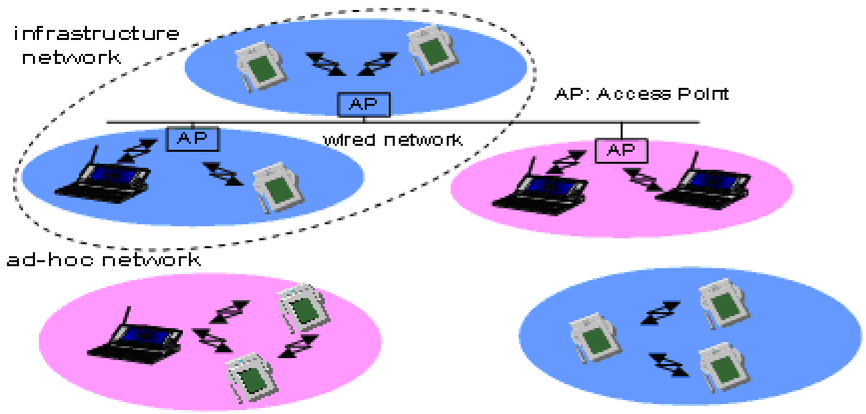
- Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
- Many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- Products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)

- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrastructure vs. ad-hoc networks



IEEE 802.11 - ARCHITECTURE – SERVICES - ARCHITECTURE – SERVICES – MAC – PHYSICAL LAYER – IEEE 802.11A - 802.11B STANDARDS

802.11 - Architecture of an infrastructure network

Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point

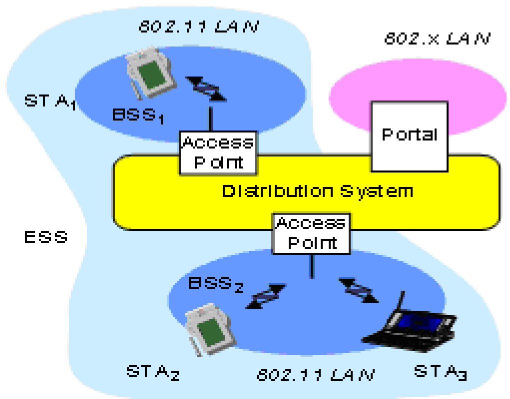
- station integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

Distribution System

- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS



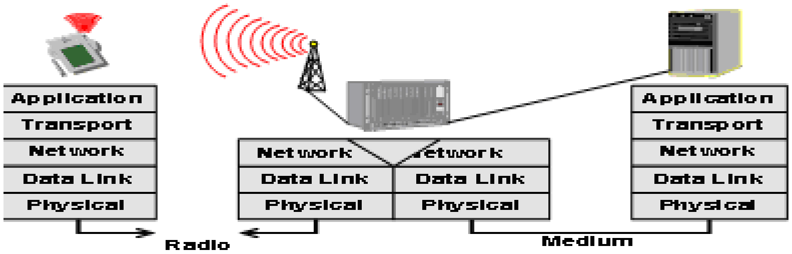
802.11 - Architecture of an ad-hoc network

Direct communication within a limited range

- Station (STA):
  terminal with access mechanisms to the wireless medium

- Basic Service Set (BSS):
  group of stations using the same radio frequency

IEEE standard 802.11



802.11 - Layers and functions

MAC

Access mechanisms, fragmentation, encryption

MAC Management

Synchronization, roaming, MIB, power management

PLCP Physical Layer Convergence Protocol

Clear channel assessment signal (carrier sense)

PMD Physical Medium Dependent

Modulation, coding

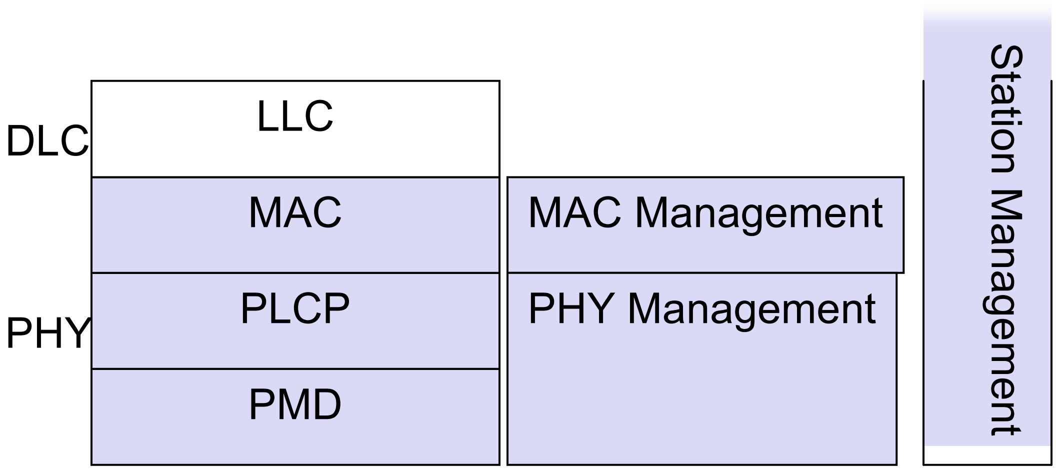
PHY Management

Channel selection, MIB

Station Management

Coordination of all management functions

802.11 - Layers



802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR

- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

802.11 - MAC layer I - DFWMAC

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods

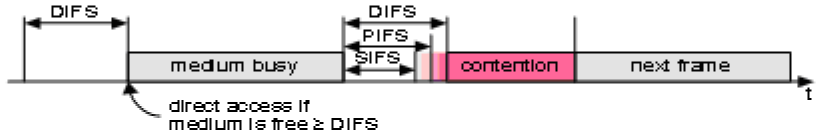
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem

- DFWMAC- PCF (optional)
    - access point polls terminals according to a list

Priorities

- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
    - lowest priority, for asynchronous data service

802.11 - MAC layer



MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System

AP: Access Point

DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier

RA: Receiver Address

TA: Transmitter Address

<u>MAC management</u>

Synchronization

- try to find a LAN, try to stay within a LAN
- timer etc.

Power management

- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

Association/Reassociation

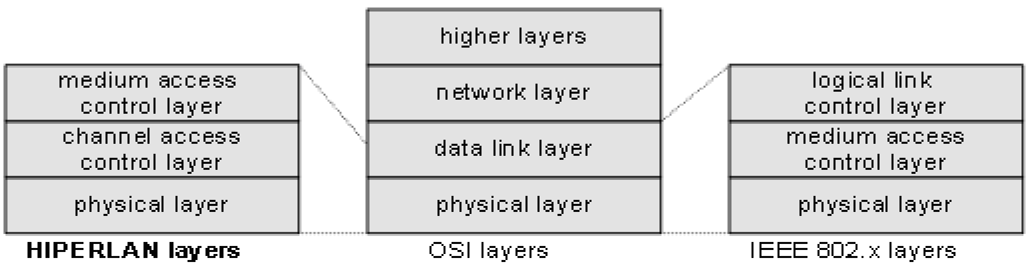
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base

- managing, read, write

HIPERLAN

- ETSI standard
  - European standard, cf. GSM, DECT, ...
  - Enhancement of local Networks and interworking with fixed networks
  - integration of time-sensitive services from the early beginning
- HIPERLAN family
  - one standard cannot satisfy all requirements
    - range, bandwidth, QoS support
    - commercial constraints
  - HIPERLAN 1 standardized since 1996



HIPERLAN 1 - Characteristics

Data transmission

- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services

- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

Topology

- infrastructure or ad-hoc networks
- transmission range can be larger then coverage of a single node („forwarding“ integrated in mobile terminals)

Further mechanisms

- power saving, encryption, checksums

Services and protocols

CAC service

- definition of communication services over a shared medium
- specification of access priorities
- abstraction of media characteristics

MAC protocol

- MAC service, compatible with ISO MAC and ISO MAC bridges
- uses HIPERLAN CAC

CAC protocol

- provides a CAC service, uses the PHY layer, specifies hierarchical access mechanisms for one or several channels

Physical protocol

- send and receive mechanisms, synchronization, FEC, modulation, signal strength

HIPERLAN 1 - Physical layer

Scope

- modulation, demodulation, bit and frame synchronization
- forward error correction mechanisms
- measurements of signal strength
- channel sensing

Channels

- 3 mandatory and 2 optional channels (with their carrier frequencies)
- mandatory
  - channel 0: 5.1764680 GHz
  - channel 1: 5.1999974 GHz
  - channel 2: 5.2235268 GHz
- optional (not allowed in all countries)
  - channel 3: 5.2470562 GHz
  - channel 4: 5.2705856 GHz

BLUETOOTH

Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many members

Scenarios

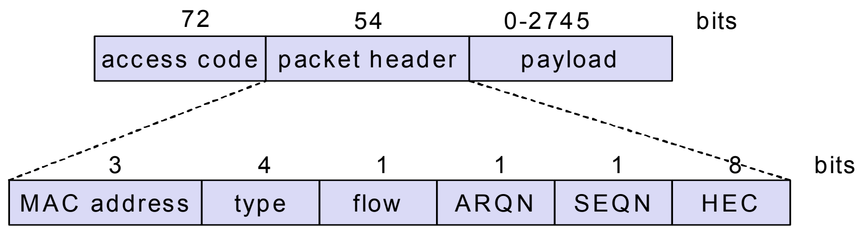
- connection of peripheral devices
    - loudspeaker, joystick, headset
- support of ad-hoc networking
    - small devices, low-cost
- bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop

Simple, cheap, replacement of IrDA, low range, lower data rates

- 2.4 GHz, FHSS, TDD, CDMA

Bluetooth MAC layer

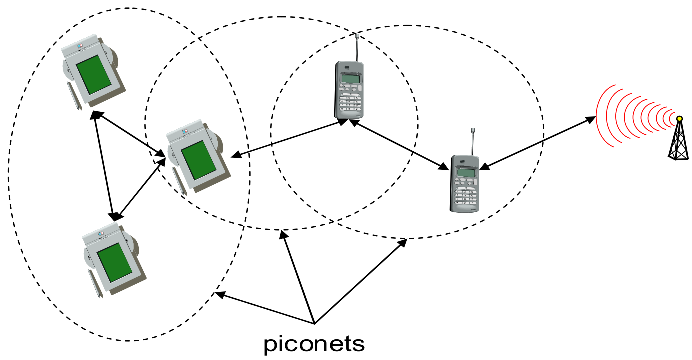
- Synchronous Connection-Oriented link (SCO)
  - symmetrical, circuit switched, point-to-point
- Asynchronous Connectionless Link (ACL)
  - packet switched, point-to-multipoint, master polls
- Access code
  - synchronization, derived from master, unique per channel
- Packet header
  - 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



7.48.1

Scatternets

- Each piconet has one master and up to 7 slaves
- Master determines hopping sequence, slaves have to synchronize
- Participation in a piconet = synchronization to hopping sequence
- Communication between piconets = devices jumping back and forth between the piconets



7.49.1

UNIT IV

MOBILE NETWORK LAYER

Mobile IP – Dynamic Host Configuration Protocol - Routing – DSDV – DSR – Alternative Metrics

Mobile IP

A standard for mobile computing and networking

Computers doesn't stay put.

Change location without restart its application or terminating any ongoing communication

IP Networking

- Protocol layer
    - Network Layer
    - Transport Layer
- What does IP do
    - moving packets from source to destination
    - No ’end-to-end’ guarantees
- IP addresses
    - Network-prefix
    - Host portion
- IP Routing
    - Packet Header
    - Network-prefix
    - Every node on the same link has the same network-prefix

<u>Mobile IP Solves the following problems</u>

f a node moves from one link to another without chnging its IP address, it will be unable to receive packets at the new link; and

If a node moves from one link to another without chnging its IP address, it will be unable to receive packets at the new link; and

<u>Mobile IP Overview</u>

- Solution for Internet
    - Scalable, robust, secure, maintain communication
    - Use their permanent IP address
- Routing protocol

Route packets to nodes that could potentially change location very rapidly

Layer 4-7, outside Mobile IP, but will be of major interest

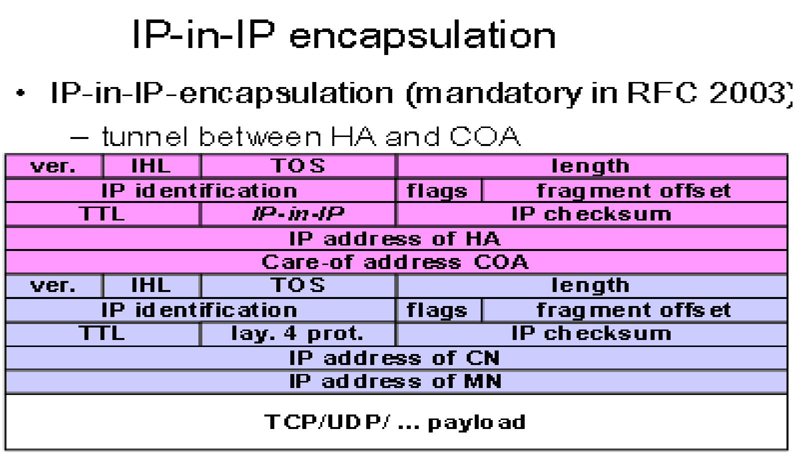
Mobile IP: Terminology

- Mobile Node (MN)
  - node that moves across networks without changing its IP address
- Correspondent Node (CN)
  - ost with which MN is “corresponding” (TCP)
- Home Agent (HA)
  - host in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP packets to the COA
- Foreign Agent (FA)
  - host in the current foreign network of the MN, typically a router
  - forwards tunneled packets to the MN, typically the default router for MN
- Care-of Address (COA)
  - address of the current tunnel end-point for the MN (at FA or MN)
  - actual location of the MN from an IP point of view

Tunneling

An encapsulating IP packet including a path and an original IP packet

IP-in-IP encapsulation



Mobile IP and IPv6

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols

- Security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address auto configuration
- No need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement;
- Addresses are always *co-located*
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
- soft"hand-over, i.e. without packet loss, between two subnets is supported

- MN sends the new COA to its old router
- the old router encapsulates all incoming packets for the MN and forwards them to the new COA
- Authentication is always granted

ROUTING

Motivation for Mobile IP

Routing

- based on IP destination address, network prefix (e.g. 129.13.42)
- determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?

- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?

- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take to long time

Requirements to Mobile IP

Transparency

- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility

- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security

- authentication of all registration messages

Efficiency and scalability

- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole
- Internet

IPv6 availability

- Generally available with (new) versions of most operating systems.
    - BSD, Linux 2.2 Solaris 8
- An option with Windows 2000/NT
- Most routers can support IPV6
- Supported in J2SDK/JRE 1.4

IPv6 Design Issues

- Overcome IPv4 scaling problem
    - Lack of address space.
- Flexible transition mechanism.
- New routing capabilities.
- Quality of service.

- Security.
- Ability to add features in the future.

Mobile ad hoc networks

Standard Mobile IP needs an infrastructure

- Home Agent/Foreign Agent in the fixed network
- DNS, routing etc. are not designed for mobility

Sometimes there is no infrastructure!

- remote areas, ad-hoc meetings, disaster areas
- Cost can also be an argument against an infrastructure!
- no default router available
- every node should be able to forward

Traditional routing algorithms

Traditional algorithms are pro-active – i.e. operate independent of user-message demands. Suitable for wired networks.

Distance Vector

- periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
- selection of the shortest path if several paths available Link State
- periodic notification of all routers about the current state of all physical links
- routers get a complete picture of the network Example
- ARPA packet radio network (1973), DV-Routing, up to 138 nodes
- every 7.5s exchange of routing tables including link quality
- updating of tables also by reception of packets
- routing problems solved with limited flooding

Problems of traditional routing algorithms

Dynamics of the topology

- Frequent changes of connections, connection quality, participants
- Limited performance of mobile systems
- periodic updates of routing tables need energy without contributing to the transmission of user data; sleep modes difficult to realize
- Limited bandwidth of the system is reduced even more due to the exchange of routing information
- Links can be asymmetric, i.e., they can have a direction dependent transmission quality

- Uncontrolled redundancy in links
- Interference – ‘unplanned links’ (advantage?)

DSDV

DSDV (Destination Sequenced Distance Vector)

Early work

- on demand version: AODV (Ad-hoc On-demand Distance Vector

Expansion of distance vector routing (but still pro-active)

Sequence numbers for all routing updates

- assures in-order execution of all updates
- avoids loops and inconsistencies

Decrease of update frequency (‘damping’)

- store time between first and best announcement of a path
- inhibit update if it seems to be unstable (based on the stored time values)

DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) is a network protocol for automatically assigning TCP/IP information to client machines. Each DHCP client connects to the centrally-located DHCP server which returns that client's network configuration, including the IP address, gateway, and DNS servers

DHCP is useful for automatic configuration of client network interfaces. When configuring the client system, the administrator can choose DHCP and instead of entering an IP address, netmask, gateway, or DNS servers. The client retrieves this information from the DHCP server. DHCP is also useful if an administrator wants to change the IP addresses of a large number of systems. Instead of reconfiguring all the systems, he can just edit one DHCP configuration file on the server for the new set of IP addresses. If the DNS servers for an organization changes, the changes are made on the DHCP server, not on the DHCP clients. Once the network is restarted on the clients (or the clients are rebooted), the changes take effect.

Furthermore, if a laptop or any type of mobile computer is configured for DHCP, it can be moved from office to office without being reconfigured as long as each office has a DHCP server that allows it to connect to the network.

Configuration File

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, while other options can be declared for individual client systems.

The configuration file can contain extra tabs or blank lines for easier formatting. Keywords are case-insensitive and lines beginning with a hash mark (#) are considered comments.

Two DNS update schemes are currently implemented — the ad-hoc DNS update mode and the interim DHCP-DNS interaction draft update mode. If and when these two are accepted as part of the Internet Engineering Task Force (IETF) standards process, there will be a third mode — the standard DNS update method. The DHCP server must be configured to use one of the two current schemes. Version 3.0b2pl11 and previous versions used the ad-hoc mode; however, it has been deprecated.

There are two types of statements in the configuration file:

Parameters — State how to perform a task, whether to perform a task, or what network configuration options to send to the client.

Declarations — Describe the topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.

Some parameters must start with the **option** keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

In **Example** the **routers**, **subnet-mask**, **domain-name**, **domain-name-servers**, and **time-offset** options are used for any **host** statements declared below it.

Additionally, a **subnet** can be declared, a **subnet** declaration must be included for every subnet in the network. If it is not, the DHCP server fails to start.

In this **example**, there are global options for every DHCP client in the subnet and a `range` declared. Clients are assigned an IP address within the `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;

        option time-offset              -18000;     # Eastern Standard Time

                range 192.168.1.10 192.168.1.100;
```

Dynamic source routing

Split routing into discovering a path and maintaining a path

Discovering a path

Only if a path for sending packets to a certain destination is needed and no path is currently available (reactive algorithm)

Maintaining a path

Only while the path is in use: make sure that it can be used continuously

Path discovery

Broadcast a packet (Route Request) with destination address and unique ID

- if a station receives a broadcast packet
- if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet) ⍰ if the packet has already been received earlier (identified via ID) then

Discard the packet

- otherwise, append own address and broadcast packet
- sender receives packet with the current path (address list)

Maintaining paths

- After sending a packet
- wait for a layer 2 acknowledgement (if applicable)
- listen into the medium to detect if other stations forward the packet (if possible)
- request an explicit acknowledgement
- if a station encounters problems it can inform the sender of a packet or look-up a new path locally

ALTERNATIVE METRICS.

Mobile IP with reverse tunneling

Router accepts often only “topological correct“addresses (firewall!)

- a packet from the MN encapsulated by the FA is now topological correct
- furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)

Reverse tunneling does not solve

- problems with firewalls, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
- optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)
- The standard is backwards compatible
- the extensions can be implemented easily and cooperate with current implementations without these extensions

Agent Advertisements can carry requests for reverse tunneling

World Wide Web and mobility

Protocol (HTTP, Hypertext Transfer Protocol) and language

(HTML, Hypertext Markup Language) of the Web have not been designed for mobile applications and mobile devices, thus creating many problems!

Typical transfer sizes

- HTTP request: 100-350 byte
- responses avg. <10 kbyte, header 160 byte, GIF 4.1kByte, JPEG
- 12.8 kbyte, HTML 5.6 kbyte
- but also many large files that cannot be ignored
- The Web is no file system
- Web pages are not simple files to download
- static and dynamic content, interaction with servers via forms, content transformation, push technologies etc.
- many hyperlinks, automatic loading and reloading, redirecting
- a single click might have big consequences!

UNIT V

TRANSPORT AND APPLICATION LAYERS

Traditional TCP – Classical TCP improvements – WAP, WAP 2.0.

TRADITIONAL TCP

TCP is an alternative transport layer protocol over IP.

- TCP provides:
  - Connection-oriented
  - Reliable
  - Full-duplex
  - Byte-Stream

Connection-Oriented

- *Connection oriented* means that a virtual connection is established before any user data is transferred.
- If the connection cannot be established - the user program is notified.
- If the connection is ever interrupted - the user program(s) is notified.

Reliable

- *Reliable* means that every transmission of data is acknowledged by the receiver.
- If the sender does not receive acknowledgement within a specified amount of time, the sender retransmits the data

Byte Stream

- *Stream* means that the connection is treated as a stream of bytes.
- The user application does not need to package data in individual datagrams (as with UDP**).**

Buffering

- TCP is responsible for buffering data and determining when it is time to send a datagram.
- It is possible for an application to tell TCP to send the data it has buffered without waiting for a buffer to fill up.

Full Duplex

- TCP provides transfer in both directions.
- To the application program these appear as 2 unrelated data streams, although TCP can piggyback control and data communication by providing control information (such as an ACK) along with user data.

TCP Ports

- Interprocess communication via TCP is achieved with the use of ports (just like UDP).
- UDP ports have no relation to TCP ports (different name spaces).

TCP Segments

- The chunk of data that TCP asks IP to deliver is called a *TCP segment*.
- Each segment contains:
  - data bytes from the byte stream
  - control information that identifies the data bytes

TCP Lingon

- When a client requests a connection it sends a "SYN" segment (a special TCP segment) to the server port.
- SYN stands for synchronize. The SYN message includes the client's ISN.
- ISN is Initial Sequence Number.
- Every TCP segment includes a *Sequence Number* that refers to the first byte of *data* included in the segment.
- Every TCP segment includes an *Acknowledgement Number* that indicates the byte number of the next data that is expected to be received.
  - All bytes up through this number have already been received.
- There are a bunch of control flags:
  - URG: urgent data included.
  - ACK: this segment is (among other things) an acknowledgement.
  - RST: error – connection must be reset.
  - SYN: synchronize Sequence Numbers (setup)
  - FIN: polite connection termination
- MSS: Maximum segment size (A TCP option)
- Window: Every ACK includes a Window field that tells the sender how many bytes it can send before the receiver will have to toss it away (due to fixed buffer size).

<u>CLASSICAL TCP IMPROVEMENTS</u>

TCP Connection Creation

- Programming details later - for now we are concerned with the actual communication.
- **A** *server* accepts a connection.
    - Must be looking for new connections!
- A *client* requests a connection.
    - Must *know* where the server is!

Client Starts

- A client starts by sending a SYN segment with the following information:
    - Client's ISN (generated pseudo-randomly)
    - Maximum Receive Window for client.
    - Optionally (but usually) MSS (largest datagram accepted).
    - No payload! (Only TCP headers)

Server Response

- When a waiting server sees a new connection request, the server sends back a SYN segment with:
    - Server's ISN (generated pseudo-randomly)
    - Request Number is Client ISN+1
    - Maximum Receive Window for server.
    - Optionally (but usually) MSS
    - No payload! (Only TCP headers)
- When the Server's SYN is received, the client sends back an ACK with:
    - Acknowledgment Number is Server's ISN+1

TCP 3-way handshake

Client: "I want to talk, and I'm starting with byte number *X*".

Server: "OK, I'm here and I'll talk. My first byte will be called number *Y*, and I know your first byte will be number *X+1*".

Client: "Got it - you start at byte number *Y+1*".

Bill: "Monica, I'm afraid I'll syn and byte your ack"

TCP Data and ACK

- Once the connection is established, data can be sent.
- Each data segment includes a sequence number identifying the first byte in the segment.
- Each segment (data or empty) includes a request number indicating what data has been received

Buffering

- Keep in mind that TCP is part of the Operating System. The O.S. takes care of all these details asynchronously.
- The TCP layer doesn't know when the application will ask for any received data.

- TCP buffers incoming data so it's ready when we ask for it.

TCP Buffers

- Both the client and server allocate buffers to hold incoming and outgoing data
    - The TCP layer does this.
- Both the client and server announce with every ACK how much buffer space remains (the Window field in a TCP segment).

Send Buffers

- The application gives the TCP layer some data to send.
- The data is put in a send buffer, where it stays until the data is ACK'd.
- The TCP layer won't accept data from the application unless (or until) there is buffer space.

ACKs

- A receiver doesn't have to ACK every segment (it can ACK many segments with a single ACK segment).
- Each ACK can also contain outgoing data (piggybacking).
- If a sender doesn't get an ACK after some time limit, it resends the data.

TCP Segment Order

- Most TCP implementations will accept out-of-order segments (if there is room in the buffer).
- Once the missing segments arrive, a single ACK can be sent for the whole thing.
- Remember: IP delivers TCP segments, and IP is not reliable - IP datagrams can be lost or arrive out of order.

Termination

- The TCP layer can send a RST segment that terminates a connection if something is wrong.
- Usually the application tells TCP to terminate the connection politely with a FIN segment.

TCP Sockets Programming

- Creating a *passive mode* (server) socket.
- Establishing an application-level *connection*.
- Sending/receiving data.
- Terminating a connection.

Establishing a passive mode TCP socket

Passive mode:

- Address already determined.
- Tell the kernel to accept incoming connection requests directed at the socket address.
    - ***3-way handshake***
- Tell the kernel to queue incoming connections for us.

Accepting an incoming connection

- Once we start listening on a socket, the O.S. will queue incoming connections
  - Handles the 3-way handshake
  - Queues up multiple connections.
- When our application is ready to handle a new connection, we need to ask the O.S. for the next connection.

Terminating a TCP connection

- Either end of the connection can call the close() system call.
- If the other end has closed the connection, and there is no buffered data, reading from a TCP socket returns 0 to indicate EOF

Client Code

- TCP clients can connect to a server, which:
  - takes care of establishing an endpoint address for the client socket.
    - don't need to call bind first, the O.S. will take care of assigning the local endpoint address (TCP port number, IP address).
  - Attempts to establish a connection to the specified server.
    - ***3-way handshake***

Reading from a TCP socket

- By default **read()** will block until data is available.
- Reading from a TCP socket may return less than max bytes (whatever is available).
- You must be prepared to read data 1 byte at a time!

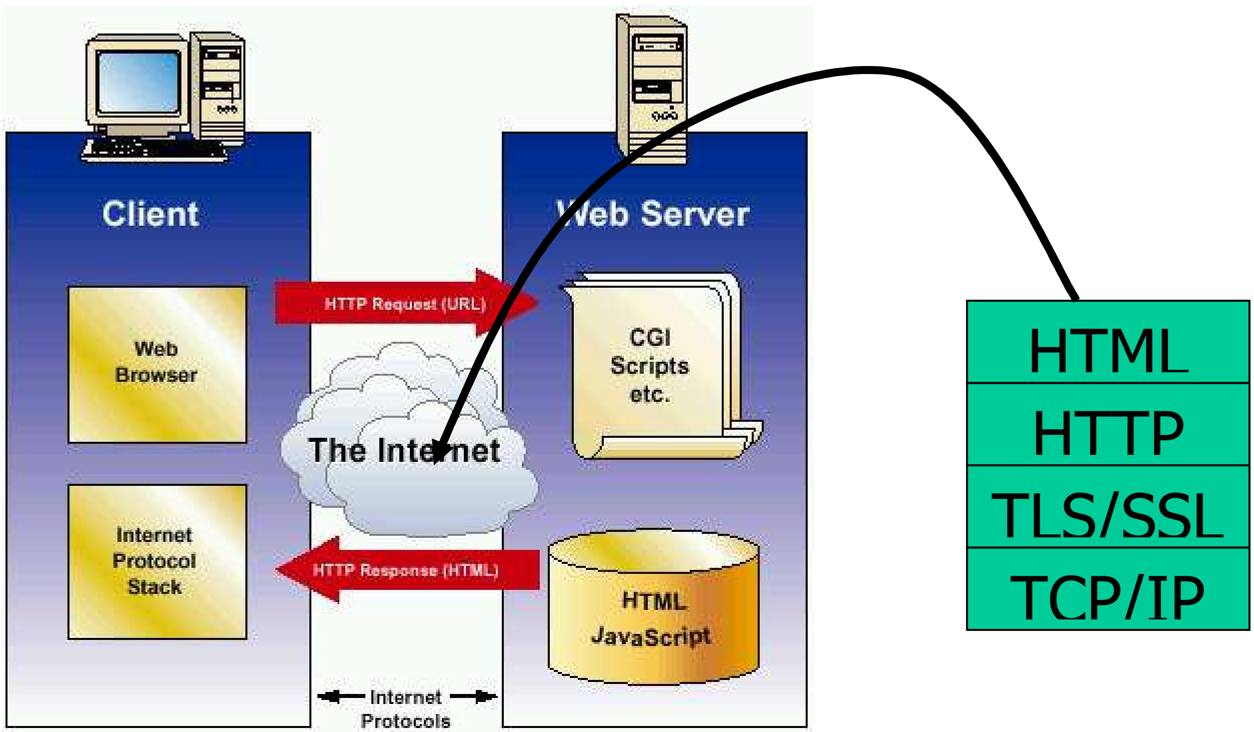
WIRELESS APPLICATION PROTOCOL (WAP)

- Empowers mobile users with wireless devices to easily access and interact with information and services.
- A "standard" created by wireless and Internet companies to enable Internet access from a cellular phone

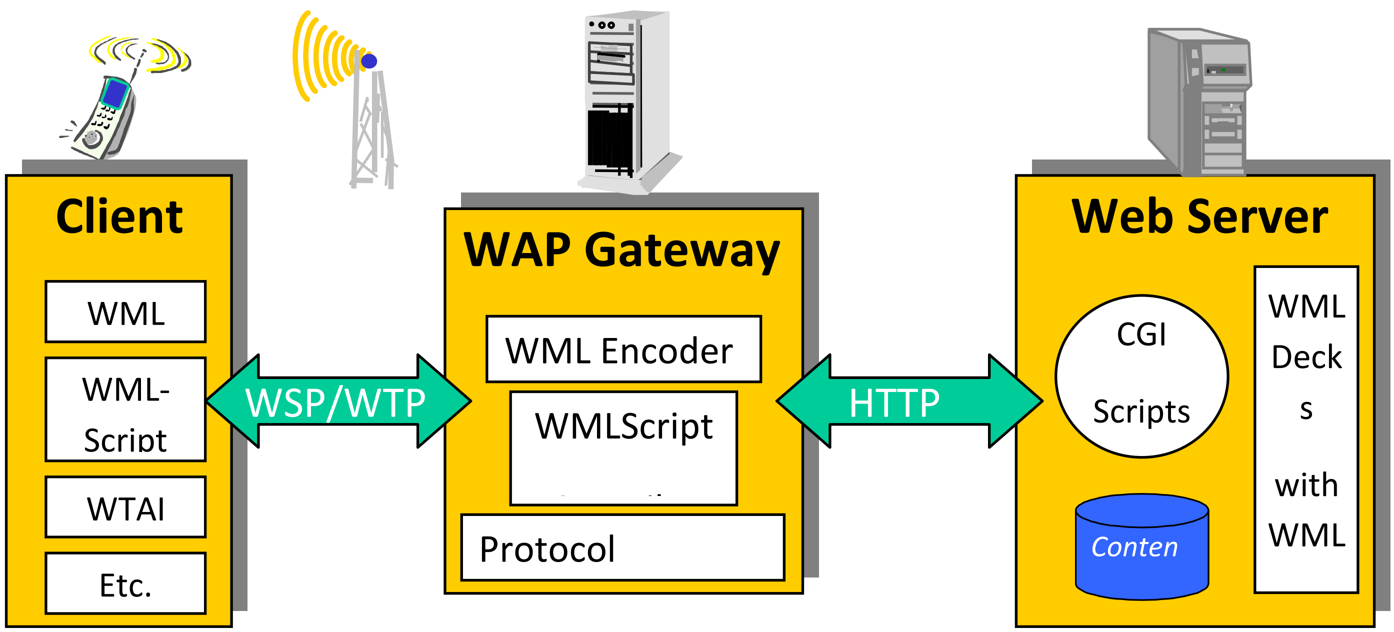
WAP: Main Features

- Browser
  - "Micro browser", similar to existing web browsers
- Markup language
  - Similar to HTML, adapted to mobile devices
- Script language
  - Similar to Javascript, adapted to mobile devices
- Gateway
  - Transition from wireless to wired world
- Server
  - "Wap/Origin server", similar to existing web servers
- Protocol layers
  - Transport layer, security layer, session layer etc.
- Telephony application interface
  - Access to telephony functions

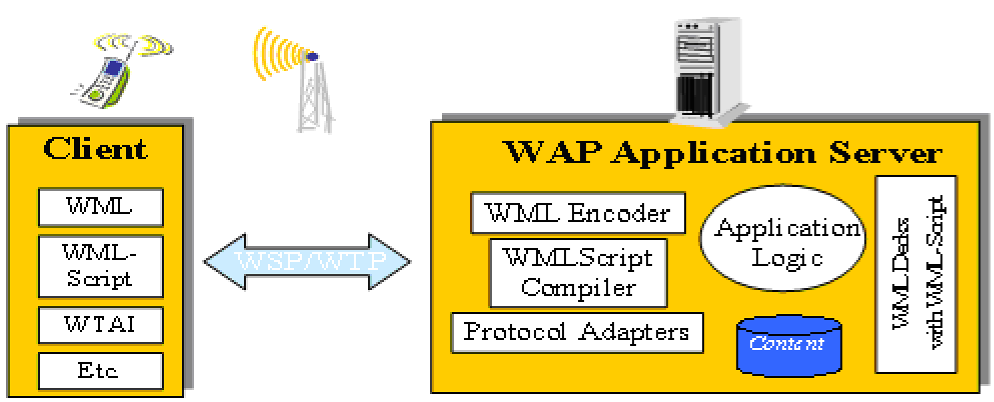
Internet Model



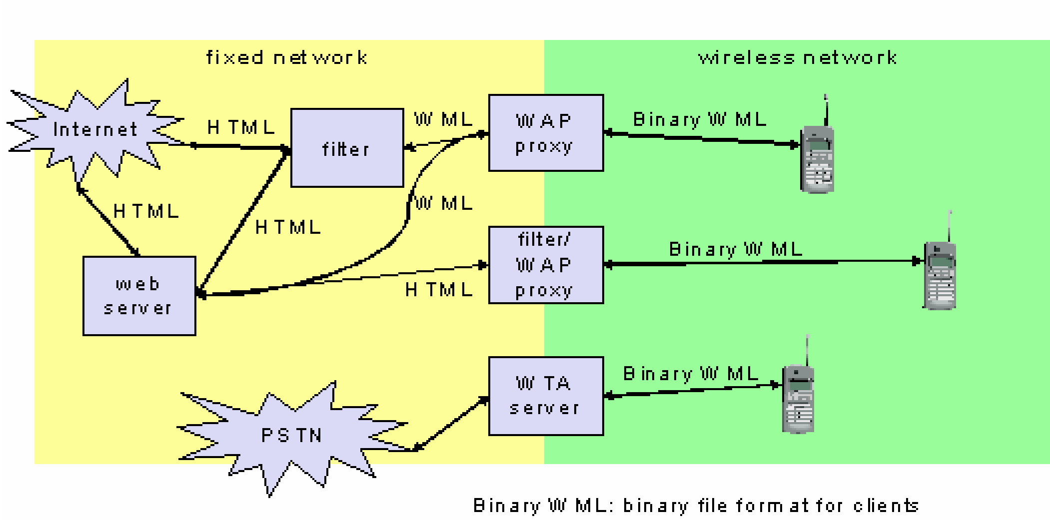
WAP Architecture



WAP Application Server



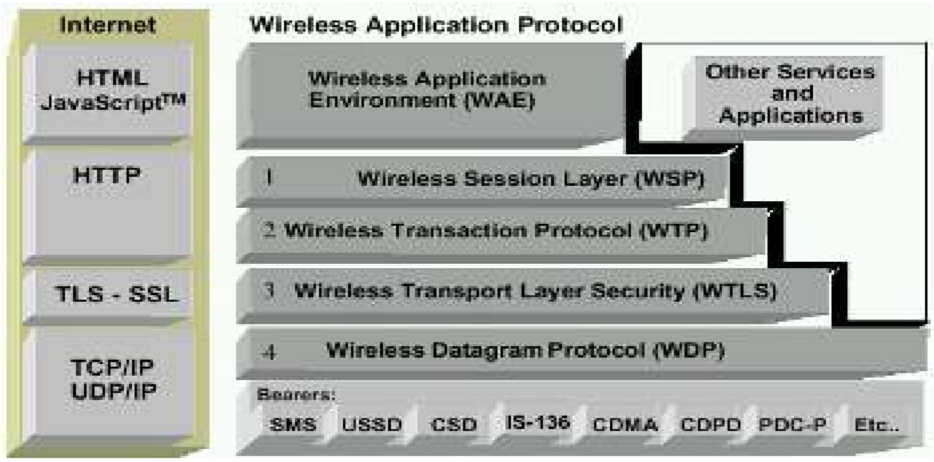
WAP: Network Elements



WAP Specifies

- Wireless Application Environment
  - WML Microbrowser
  - WMLScript Virtual Machine
  - WMLScript Standard Library
  - Wireless Telephony Application Interface (WTAI)
  - WAP content types
- Wireless Protocol Stack
  - Wireless Session Protocol (WSP)
  - Wireless Transport Layer Security (WTLS)
  - Wireless Transaction Protocol (WTP)
  - Wireless Datagram Protocol (WDP)
  - Wireless network interface definitions

WAP Stack



- WAE (Wireless Application Environment):
  - Architecture: application model, browser, gateway, server
  - WML: XML-Syntax, based on card stacks, variables, ...
  - WTA: telephone services, such as call control, phone book etc.

- WSP (Wireless Session Protocol):
  - Provides HTTP 1.1 functionality
  - Supports session management, security, etc.

- WTP (Wireless Transaction Protocol):
  - Provides reliable message transfer mechanisms
  - Based on ideas from TCP/RPC

- WTLS (Wireless Transport Layer Security):
  - Provides data integrity, privacy, authentication functions
  - Based on ideas from TLS/SSL

- WDP (Wireless Datagram Protocol):
  - Provides transport layer functions
  - Based on ideas from UDP

WHY WAP?

- Wireless networks and phones
    - have specific needs and requirements
    - not addressed by existing Internet technologies
- WAP
    - Enables any data transport
        - TCP/IP, UDP/IP, GUTS (IS-135/6), SMS, or USSD.
    - Optimizes the content and air-link protocols
    - Utilizes plain Web HTTP 1.1 servers
        - leverages existing development methodologies
        - utilizes standard Internet markup language technology (XML)
        - all WML content is accessed via HTTP 1.1 requests
    - WML UI components map well onto existing mobile phone user interfaces
        - no re-education of the end-users
        - leveraging market penetration of mobile devices
    - Several modular entities together form a fully compliant Internet entity

WAP: "Killer" Applications

- Location-based services
    - Real-time traffic reporting, Event/restaurant recommendation
- Enterprise solutions
    - Email access, Database access, "global" intranet access
    - Information updates "pushed" to WAP devices
- Financial services
    - Banking, Bill-paying, Stock trading, Funds transfers
- Travel services
    - Schedules and rescheduling, Reservations
- Gaming and Entertainment
    - Online, real-time, multi-player games
    - Downloadable horoscopes, cartoons, quotes, advice
- M-Commerce
    - Shopping on the go
    - Instant comparison shopping
    - Location-based special offers and sales

Wireless Application Environment (WAE)

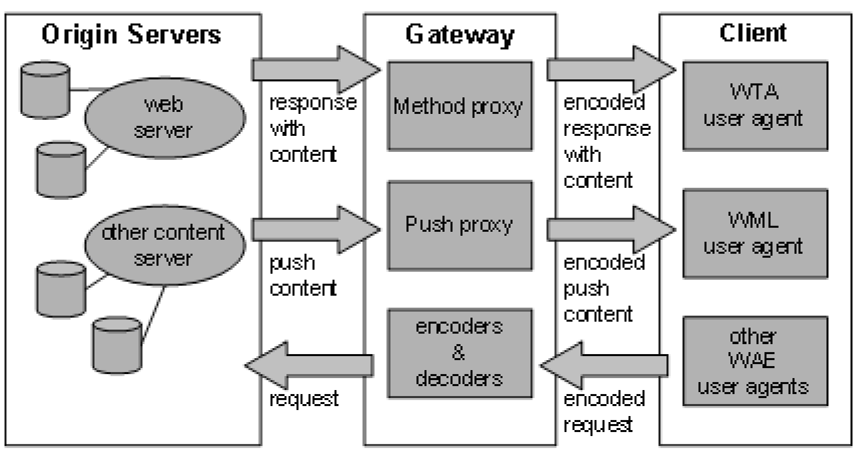
- Goals
    - device and network independent application environment

- for low-bandwidth, wireless devices
- considerations of slow links, limited memory, low computing power, small display, simple user interface (compared to desktops)
- integrated Internet/WWW programming model
- high interoperability

WAE Components

- Architecture
  - Application model, Microbrowser, Gateway, Server
- User Agents
  - WML/WTA/Others
  - content formats: vCard, vCalendar, Wireless Bitmap, WML, ...
- WML
  - XML-Syntax, based on card stacks, variables, ...
- WMLScript
  - procedural, loops, conditions, ... (similar to JavaScript)
- WTA
  - telephone services, such as call control, text messages, phone book, ... (accessible from WML/WMLScript)
- Proxy (Method/Push)

WAE: Logical Model



WML: Wireless Markup Language

- Tag-based browsing language:

  - Screen management (text, images)
  - Data input (text, selection lists, etc.)
  - Hyperlinks & navigation support
- Takes into account limited display, navigation capabilities of devices
- XML-based language
  - describes only intent of interaction in an abstract manner
  - presentation depends upon device capabilities
- Cards and Decks
  - document consists of many cards
  - User interactions are split into cards
  - Explicit navigation between cards
  - cards are grouped to decks
  - deck is similar to HTML page, unit of content transmission
- Events, variables and state mgmt
- The basic unit is a **card**. Cards are grouped together into **Decks** Document ~ Deck (unit of transfer)
- All decks must contain
  - Document prologue
    - XML & document type declaration
  - <WML> element
    - Must contain one or more cards

WML Example

```
WML>

 <CARD>

  <DO TYPE="ACCEPT">

   <GO URL="#eCard"/>

  </DO

  Welcome!

 </CARD>

 <CARD NAME="eCard">

  <DO TYPE="ACCEPT">

    <GO URL="/submit?N=$(N)&S=$(S)"/>

  </DO>

  Enter name: <INPUT KEY="N"/>
```

```
  Choose speed:

  <SELECT KEY="S">

   <OPTION VALUE="0">Fast</OPTION>

   <OPTION VALUE="1">Slow</OPTION>

  <SELECT>

 </CARD>

</WML>
```

WMLScript

- Complement to WML
  - Derived from JavaScript™
- Provides general scripting capabilities
  - Procedural logic, loops, conditionals, etc.
  - Optimized for small-memory, small-cpu devices

- Features
  - local user interaction, validity check of user input
  - access to device facilities (phone call, address book etc.)
  - extensions to the device software
    - configure device, download new functionality after deployment

- Bytecode-based virtual machine
  - Stack-oriented design, ROM-able
  - Designed for simple, low-impact implementation
- WMLScript compiler resides in the network

WMLScript Libraries

- Lang - VM constants, general-purpose math functionality, etc.
- String - string processing functions
- URL - URL processing

- Browser - WML browser interface
- Dialog - simple user interface
- Float - floating point functions

Wireless Telephony Application (WTA)

- Collection of telephony specific extensions
  - designed primarily for network operators
- Example
  - calling a number (WML)
    wtai://wp/mc;07216086415
  - calling a number (WMLScript)
    WTAPublic.makeCall("07216086415");
- Implementation
  - Extension of basic WAE application model
  - Extensions added to standard WML/WMLScript browser
  - Exposes additional API (WTAI)

WTA Features

- Extension of basic WAE application model
  - network model for interaction
    - client requests to server
    - event signaling: server can push content to the client
  - event handling
    - table indicating how to react on certain events from the network
    - client may now be able to handle unknown events
  - telephony functions
    - some application on the client may access telephony functions
- WTAI includes:
  - Call control
  - Network text messaging
  - Phone book interface
  - Event processing
- Security model: segregation
  - Separate WTA browser
  - Separate WTA port

WAP Push Services

- Web push
  - Scheduled pull by client (browser)
    - example: Active Channels
  - no real-time alerting/response
    - example: stock quotes
- Wireless push
  - accomplished by using the network itself
    - example: SMS
  - limited to simple text, cannot be used as starting point for service
    - example: if SMS contains news, user cannot request specific news item
- WAP push
  - Network supported push of WML content
    - example: Alerts or service indications
  - Pre-caching of data (channels/resources)

Push Access Protocol

- Based on request/response model
- Push initiator is the client
- Push proxy is the server
- Initiator uses HTTP POST to send push message to proxy
- Initiator sends control information as an XML document, and content for mobile (as WML)
- Proxy sends XML entity in response indicating submission status
- Initiator can
  - cancel previous push
  - query status of push
  - query status/capabilities of device

Push Proxy Gateway

- WAP stack (communication with mobile device)
- TCP/IP stack (communication with Internet push initiator)
- Proxy layer does
  - control information parsing
  - content transformation
  - session management
  - client capabilities
  - store and forward
  - prioritization

- address resolution
- management function

WTP Services and Protocols

- WTP (Transaction)
  - provides reliable data transfer based on request/reply paradigm
    - no explicit connection setup or tear down
    - optimized setup (data carried in first packet of protocol exchange)
    - seeks to reduce 3-way handshake on initial request
  - supports
    - header compression
    - segmentation /re-assembly
    - retransmission of lost packets
    - selective-retransmission
    - port number addressing (UDP ports numbers)
    - flow control
  - message oriented (not stream)
  - supports an Abort function for outstanding requests
  - supports concatenation of PDUs
  - supports User acknowledgement or Stack acknowledgement option
    - acks may be forced from the WTP user (upper layer)
    - default is stack ack

WAP 2.0.

WSP - Wireless Session Protocol

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

- WSP Services
  - provides shared state between client and server, optimizes content transfer
  - session management (establish, release, suspend, resume)
  - efficient capability negotiation
  - content encoding
  - push

- WSP/B (Browsing)
  - HTTP/1.1 functionality - but binary encoded
  - exchange of session headers
  - push and pull data transfer
  - asynchronous requests

WSP Overview

- Header Encoding
  - compact binary encoding of headers, content type identifiers and other well-known textual or structured values
  - reduces the data actually sent over the network
- Capabilities (are defined for):
  - message size, client and server
  - protocol options: Confirmed Push Facility, Push Facility, Session Suspend Facility, Acknowledgement headers
  - maximum outstanding requests
  - extended methods
  - header code pages
- Suspend and Resume
  - server knows when client can accept a push
  - multi-bearer devices
  - dynamic addressing
  - allows the release of underlying bearer resources
- Session Context and Push
  - push can take advantage of session headers
  - server knows when client can accept a push

- Connection-mode
  - long-lived communication, benefits of the session state, reliability

- Connectionless-mode
  - stateless applications, no session creation overhead, no reliability overhead

WAP: Ongoing Work

- WDP
  - Tunnel to support WAP where no (end-to-end) IP bearer available
- WTLS

- support for end-to-end security (extending WTLS endpoint beyond WAP Gateway)
  - interoperable between WAP and Internet (public key infrastructure)
  - integrating Smart Cards for security functions
- WTP
  - efficient transport over wireless links (wireless TCP)
  - bearer selection/switching
  - quality of service definitions
- WSP
  - quality of service parameters
  - multicast data, multimedia support
- WAE
  - User agent profiles: personalize for device characteristics, preferences etc

<u>UNIT II</u>

TELECOMMUNICATION NETWORKS

Telecommunication systems – GSM – GPRS – DECT – UMTS – IMT-2000 – Satellite Networks **-** Basics – Parameters and Configurations – Capacity Allocation – FAMA and DAMA – Broadcast Systems – DAB - DVB.

<u>Telecommunication systems -GSM – GPRS – DECT – UMTS – IMT-2000</u>

<u>Building Blocks</u>

- AMPS – Advanced Mobile Phone System
- TACS – Total Access Communication System
- NMT – Nordic Mobile Telephone System

<u>AMPS – Advanced Mobile Phone System</u>

- analog technology

- used in North and South America and approximately 35 other countries
- operates in the 800 MHz band using FDMA technology

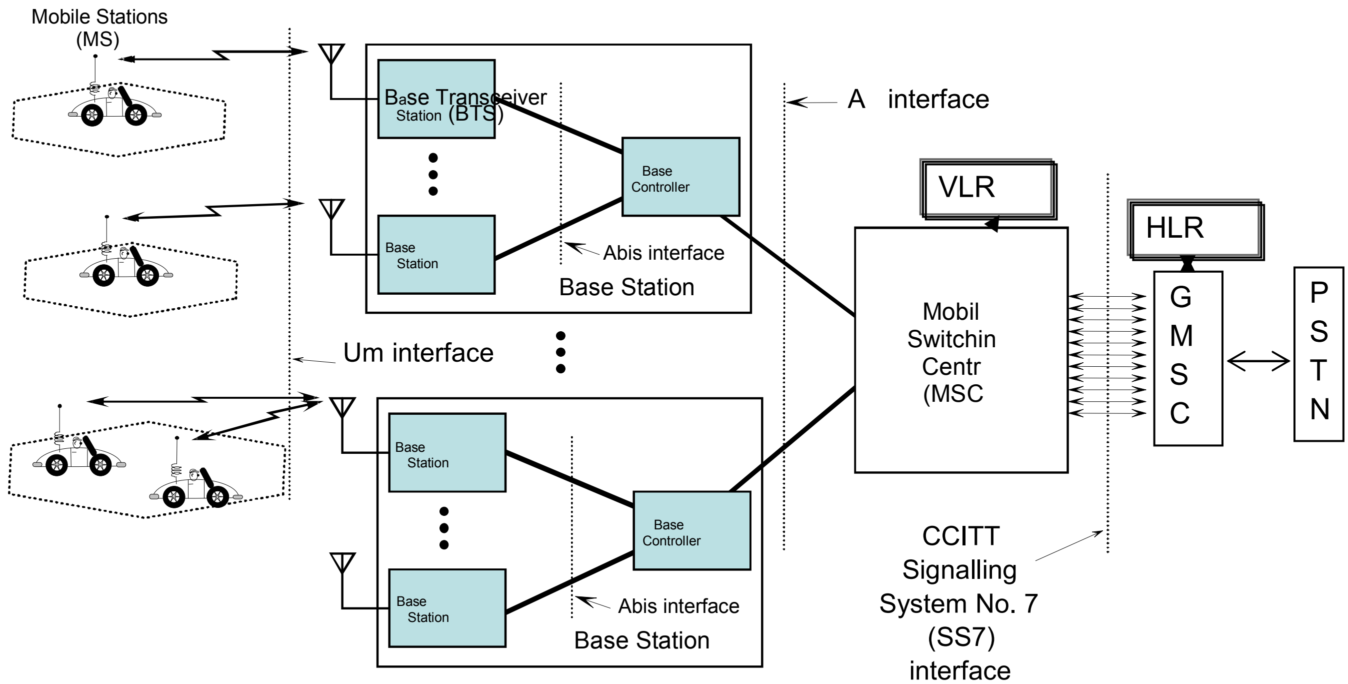
TACS – Total Access Communication System

- variant of AMPS
- deployed in a number of countries
- primarily in the UK

NMT – Nordic Mobile Telephone System

- analog technology
- deployed in the Benelux countries and Russia
- operates in the 450 and 900 MHz band
- first technology to offer international roaming – only within the Nordic countries

System Architecture



Mobile Station (MS)

Mobile Equipment (ME)

Subscriber Identity Module (SIM)

Base Station Subsystem (BBS)

Base Transceiver Station (BTS)

Base Station Controller (BSC)

Network Subsystem

Mobile Switching Center (MSC)

Home Location Register (HLR)

Visitor Location Register (VLR)

Authentication Center (AUC)

Equipment Identity Register (EIR)

- Mobile Station: is a subscriber unit intended for use while on the move at unspecified locations. It could be a hand-held or a portable terminal.

- Base Station: a fixed radio station used for communication with MS. It is located at the centre of a cell and consist of Transmitters and Receivers.

- Mobile Switching Centre: it coordinates the routing of calls, do the billing, etc.

<u>Mobile Station (MS)</u>

The Mobile Station is made up of two entities:

2. Mobile Equipment (ME)
2. Subscriber Identity Module (SIM

Mobile Equipment

- Produced by many different manufacturers
- Must obtain approval from the standardization body
- Uniquely identified by an IMEI (International Mobile Equipment Identity)

Subscriber Identity Module (SIM)

- Smart card containing the International Mobile Subscriber Identity (IMSI)
- Allows user to send and receive calls and receive other subscribed services
- Encoded network identification details
- Protected by a password or PIN
- Can be moved from phone to phone – contains key information to activate the phone

Base Station Subsystem (BBS)

Base Station Subsystem is composed of two parts that communicate across the standardized Abis interface allowing operation between components made by different suppliers

2. Base Transceiver Station (BTS)

2. Base Station Controller (BSC)

Base Transceiver Station (BTS)

- Houses the radio transceivers that define a cell
- Handles radio-link protocols with the Mobile Station
- Speech and data transmissions from the MS are recoded
- Requirements for BTS:
    - ruggedness
    - reliability
    - portability
    - minimum costs

Base Station Controller (BSC)

- Manages Resources for BTS
- Handles call set up
- Location update
- Handover for each MS

Network Subsystem

Mobile Switching Center (MSC)

- Switch speech and data connections between:
  Base Station Controllers

Mobile Switching Centers

GSM-networks

Other external networks

- Heart of the network
- Three main jobs:

1) Connects calls from sender to receiver

2) Collects details of the calls made and received

3) Supervises operation of the rest of the network component

Home Location Registers (HLR)

- contains administrative information of each subscriber

- Current location of the mobile

Visitor Location Registers (VLR)

- contains selected administrative information from the HLR

- authenticates the user
- tracks which customers have the phone on and ready to receive a call
- periodically updates the database on which phones are turned on and ready to receive calls

Authentication Center (AUC)

- mainly used for security
- data storage location and functional part of the network
- Ki is the primary element

Equipment Identity Register (EIR)

Database that is used to track handsets using the IMEI (International Mobile Equipment Identity)

- Made up of three sub-classes: The White List, The Black List and the Gray List
- Optional database

Basic Features Provided by GSM

- Call Waiting

- Notification of an incoming call while on the handset

- Call Hold

- Put a caller on hold to take another call

- Call Barring

- All calls, outgoing calls, or incoming calls

- Call Forwarding

- Calls can be sent to various numbers defined by the user

- Multi Party Call Conferencing

- Link multiple calls together

Advanced Features Provided by GSM

- Calling Line ID
  - incoming telephone number displayed
- Alternate Line Service
  - one for personal calls
  - one for business calls
- Closed User Group
  - call by dialing last for numbers
- Advice of Charge
  - tally of actual costs of phone calls
- Fax & Data
  - Virtual Office / Professional Office

- Roaming
    - services and features can follow customer from market to market

Advantages of GSM

- Crisper, cleaner quieter calls
- Security against fraud and eavesdropping
- International roaming capability in over 100 countries
- Improved battery life
- Efficient network design for less expensive system expansion
- Efficient use of spectrum
- Advanced features such as short messaging and caller ID
- A wide variety of handsets and accessories
- High stability mobile fax and data at up to 9600 baud
- Ease of use with over the air activation, and all account information is held in a smart card which can be moved from handset to handset

UMTS (Universal Mobile Telephone System

- Reasons for innovations
    - new service requirements
    - availability of new radio bands

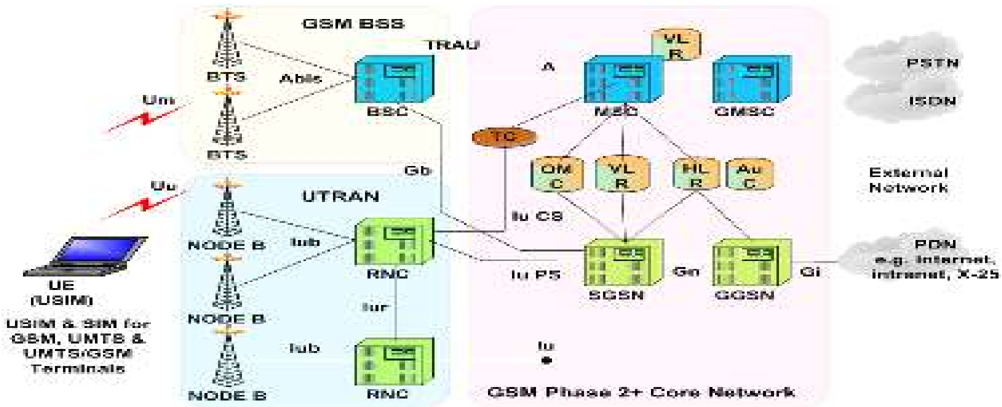
- User demands
    - seamless Internet-Intranet access
    - wide range of available services
    - compact, lightweight and affordable terminals
    - simple terminal operation
    - open, understandable pricing structures for the whole spectrum of available services

UMTS Basic Parameter

- Frequency Bands (FDD : 2x60 MHz):
    - 1920 to 1980 MHz (Uplink)
    - 2110 to 2170 MHz (Downlink)
- Frequency Bands (TDD: 20 + 15 MHz):
    - 1900 – 1920 MHz and 2010 – 2025 MHz
- RF Carrier Spacing:
    - 4.4 - 5 MHz

- RF Channel Raster:
  - 200 KHz
- Power Control Rate:
  - 1500 Cycles per Second

UMTS W-CDMA Architecture



SATELLITE NETWORKS

History of satellite communication

1945 Arthur C. Clarke publishes an essay about „Extra

Terrestrial Relays“

1957 first satellite SPUTNIK

1960 first reflecting communication satellite ECHO

1963 first geostationary satellite SYNCOM

1965 first commercial geostationary satellite Satellit „Early Bird“

(INTELSAT I): 240 duplex telephone channels or 1 TV

channel, 1.5 years lifetime

1976 three MARISAT satellites for maritime communication

1982 first mobile satellite telephone system INMARSAT-A

1988 first satellite system for mobile phones and data

communication INMARSAT-C

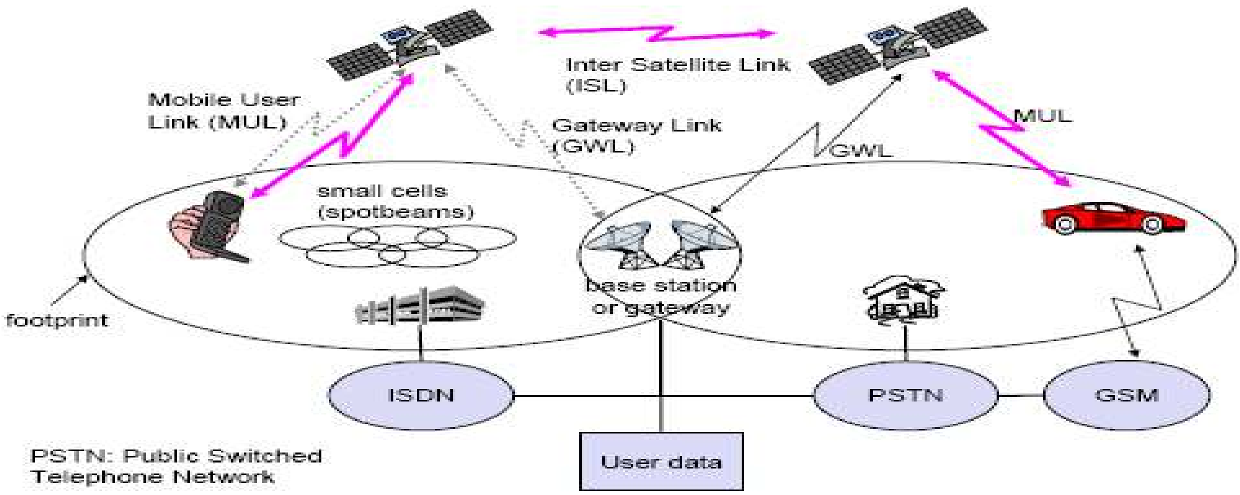
1993 first digital satellite telephone system

1998 global satellite systems for small mobile phones

Applications

- Traditionally
  - weather satellites
  - radio and TV broadcast satellites
  - military satellites
  - satellites for navigation and localization (e.g., GPS)
- Telecommunication
  - global telephone connections
  - backbone for global networks
  - connections for communication in remote places or underdeveloped areas
  - global mobile communication
- satellite systems to extend cellular phone systems (e.g., GSM orAMPS)

Classical satellite systems



Basics

Satellites in circular orbits

- attractive force $F_g = m\, g\, (R/r)^2$
- centrifugal force $F_c = m\, r\, \omega^2$
- m: mass of the satellite
- R: radius of the earth (R = 6370 km)
- r: distance to the center of the earth
- g: acceleration of gravity ($g = 9.81\ m/s^2$)
- ω: angular velocity ($\omega = 2\pi f$, f: rotation frequency)

Stable orbit

$F_g = F_c$

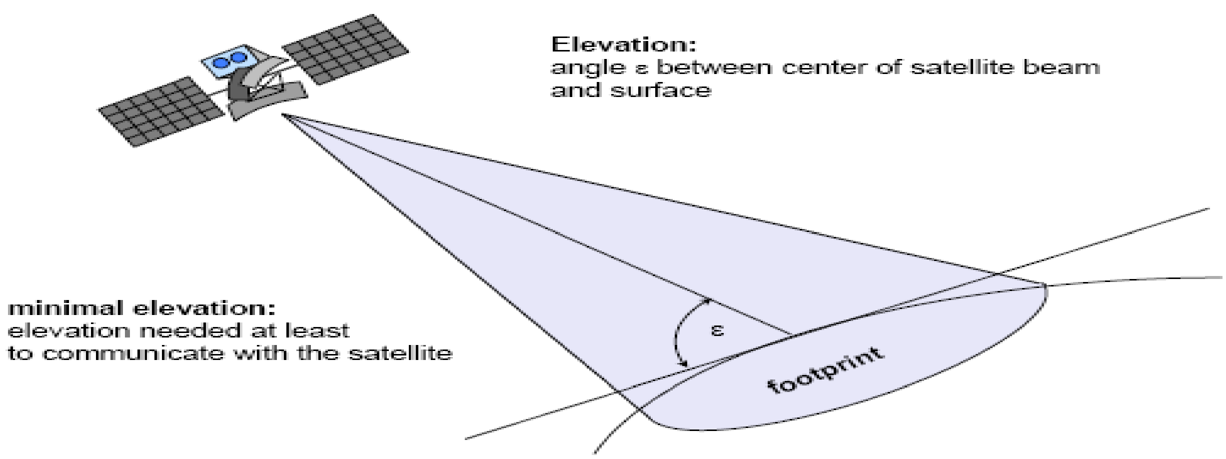
$$r = \sqrt[3]{\frac{gR^2}{(2\pi f)^2}}$$

Basics

- Elliptical or circular orbits
- Complete rotation time depends on distance satellite-earth
- Inclination: angle between orbit and equator
- Elevation: angle between satellite and horizon
- LOS (Line of Sight) to the satellite necessary for connection
    1. High elevation needed, less absorption due to e.g. buildings
- Uplink: connection base station - satellite
- Downlink: connection satellite - base station
- Typically separated frequencies for uplink and downlink
    1. Transponder used for sending/receiving and shifting of frequencies
    2. Transparent transponder: only shift of frequencies
    3. Regenerative transponder: additionally signal regeneration

I

Elevation



Link budget of satellites

Parameters like attenuation or received power determined by four parameters:

Sending power

Gain of sending antenna

Distance between sender and receiver

Gain of receiving antenna Problems

Varying strength of received signal due to multipath propagation

Interruptions due to shadowing of signal (no LOS) possible solutions

Link Margin to eliminate variations in signal strength

Satellite diversity (usage of several visible satellites at the same time) helps to use less sending power

$$L = \left(\frac{4\pi r f}{c} \right)^2$$

L: Loss

f: carrier frequency

r: distance

c: speed of light

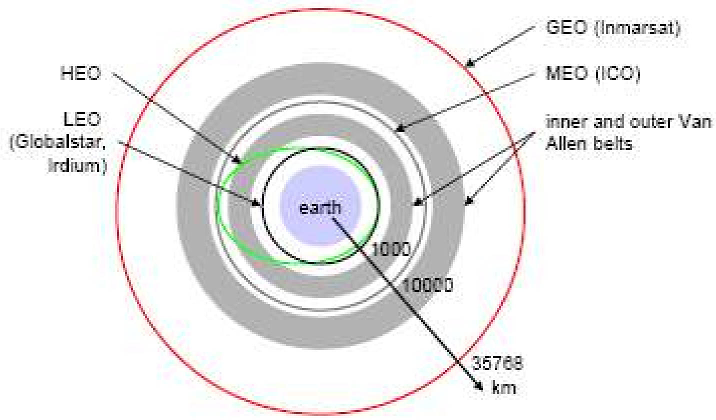
ORBITS

Four different types of satellite orbits can be identified depending on the shape and diameter of the orbit:

- GEO: geostationary orbit, ca. 36000 km above earth surface
- LEO (Low Earth Orbit): ca. 500 - 1500 km
- MEO (Medium Earth Orbit) or ICO (Intermediate Circular Orbit):

ca. 6000 - 20000 km

- HEO (Highly Elliptical Orbit) elliptical orbits



Van-Allen-Belts: ionized particles 2000 - 6000 km and 15000 - 30000 km above earth surface

Geostationary satellites

Orbit 35,786 km distance to earth surface, orbit in equatorial plane (inclination 0°)

Complete rotation exactly one day, satellite is synchronous to earth rotation

Fix antenna positions, no adjusting necessary

Satellites typically have a large footprint (up to 34% of earth surface!), therefore difficult to reuse frequencies

Bad elevations in areas with latitude above 60° due to fixed position above the equator

High transmit power needed

High latency due to long distance (ca. 275 ms)

Not useful for global coverage for small mobile phones and data transmission, typically used for radio and TV transmission

LEO systems

Orbit ca. 500 - 1500 km above earth surface

Visibility of a satellite ca. 10 - 40 minutes

Global radio coverage possible

Latency comparable with terrestrial long distance

Connections, ca. 5 - 10 ms

Smaller footprints, better frequency reuse

But now handover necessary from one satellite to another

Many satellites necessary for global coverage

More complex systems due to moving satellites

Examples:

Iridium (start 1998, 66 satellites)

Global star (start 1999, 48 satellites)

MEO systems

Orbit ca. 5000 - 12000 km above earth surface

Comparison with LEO systems:

Slower moving satellites

Less satellites needed

Simpler system design

For many connections no hand-over needed

Higher latency, ca. 70 - 80 ms

Higher sending power needed

Special antennas for small footprints needed

Example:

ICO (Intermediate Circular Orbit, Inmarsat) start ca. 2000

Routing

One solution: inter satellite links (ISL)

Reduced number of gateways needed

Forward connections or data packets within the satellite network as long as possible

Only one uplink and one downlink per direction needed for the connection of two mobile phones

Problems:

More complex focusing of antennas between satellites

High system complexity due to moving routers

Higher fuel consumption

Thus shorter lifetime

Iridium and Teledesic planned with ISL

Other systems use gateways and additionally terrestrial networks

Localization of mobile stations

Mechanisms similar to GSM

Gateways maintain registers with user data

HLR (Home Location Register): static user data

VLR (Visitor Location Register): (last known) location of the mobile station

SUMR (Satellite User Mapping Register):

- Satellite assigned to a mobile station
- Positions of all satellites

Registration of mobile stations

- Localization of the mobile station via the satellite’s position
- Requesting user data from HLR
- Updating VLR and SUMR

Calling a mobile station

- Localization using HLR/VLR similar to GSM
- Connection setup using the appropriate satellite

Handover in satellite systems

Several additional situations for handover in satellite systems compared to cellular terrestrial mobile phone networks caused by the movement of the satellites

Intra satellite handover

- Handover from one spot beam to another
- Mobile station still in the footprint of the satellite, but in another cell

Inter satellite handover

- Handover from one satellite to another satellite
- Mobile station leaves the footprint of one satellite

Gateway handover

- Handover from one gateway to another
- Mobile station still in the footprint of a satellite, but gateway leaves the footprint

Inter system handover

- Handover from the satellite network to a terrestrial cellular network
- Mobile station can reach a terrestrial network again which might be cheaper, has a lower latency etc.

Overview of LEO/MEO systems

	Iridium	Globalstar	ICO	Teledesic
# satellites	66 + 6	48 + 4	10 + 2	288
altitude (km)	780	1414	10390	ca. 700
coverage	global	±70° latitude	global	global
min. elevation	8°	20°	20°	40°
frequencies [GHz (circa)]	1.6 MS 29.2 ↑ 19.5 ↓ 23.3 ISL	1.6 MS ↑ 2.5 MS ↓ 5.1 ↑ 6.9 ↓	2 MS ↑ 2.2 MS ↓ 5.2 ↑ 7 ↓	19 ↓ 28.8 ↑ 62 ISL
access method	FDMA/TDMA	CDMA	FDMA/TDMA	FDMA/TDMA
ISL	yes	no	no	yes
bit rate	2.4 kbit/s	9.6 kbit/s	4.8 kbit/s	64 Mbit/s ↓ 2/64 Mbit/s ↑
# channels	4000	2700	4500	2500
Lifetime [years]	5-8	7.5	12	10
cost estimation	4.4 B$	2.9 B$	4.5 B$	9 B$

UNIT III

WIRLESS LAN

Wireless LAN – IEEE 802.11 - Architecture – services – MAC – Physical layer – IEEE 802.11a - 802.11b standards – HIPERLAN – Blue Tooth.

WIRELESS LAN

Characteristics of wireless LANs

Advantages

- Very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

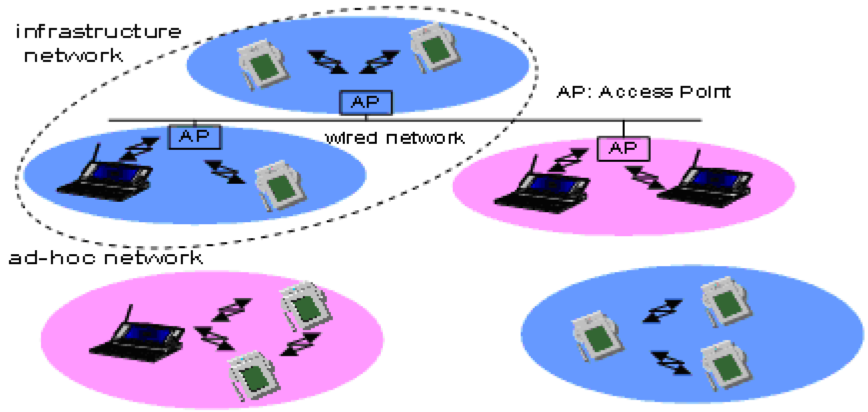
Disadvantages

- Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
- Many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- Products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrastructure vs. ad-hoc networks



IEEE 802.11 - ARCHITECTURE – SERVICES - ARCHITECTURE – SERVICES – MAC – PHYSICAL LAYER – IEEE 802.11A - 802.11B STANDARDS

802.11 - Architecture of an infrastructure network

Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point

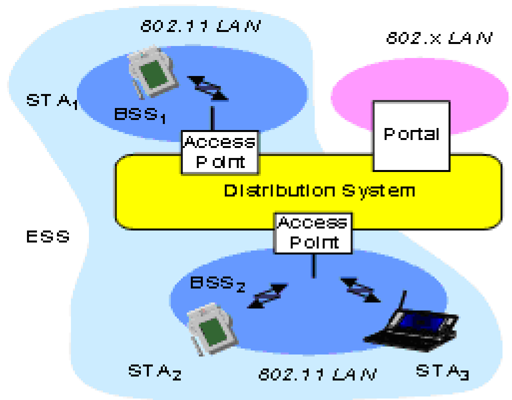
- station integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

Distribution System

- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

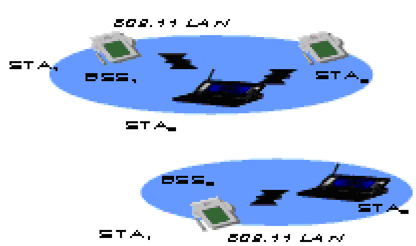


802.11 - Architecture of an ad-hoc network

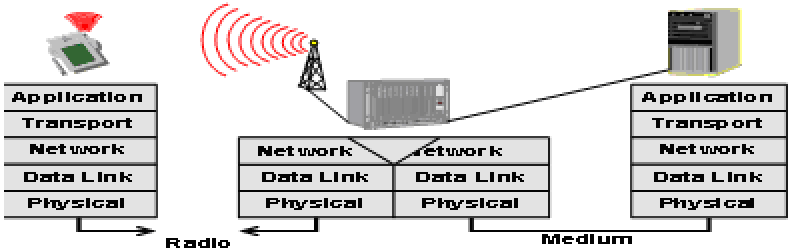
Direct communication within a limited range

- Station (STA):
  terminal with access mechanisms to the wireless medium

- Basic Service Set (BSS):
  group of stations using the same radio frequency



IEEE standard 802.11



802.11 - Layers and functions

MAC

Access mechanisms, fragmentation, encryption

MAC Management

Synchronization, roaming, MIB, power management

PLCP Physical Layer Convergence Protocol

Clear channel assessment signal (carrier sense)

PMD Physical Medium Dependent

Modulation, coding

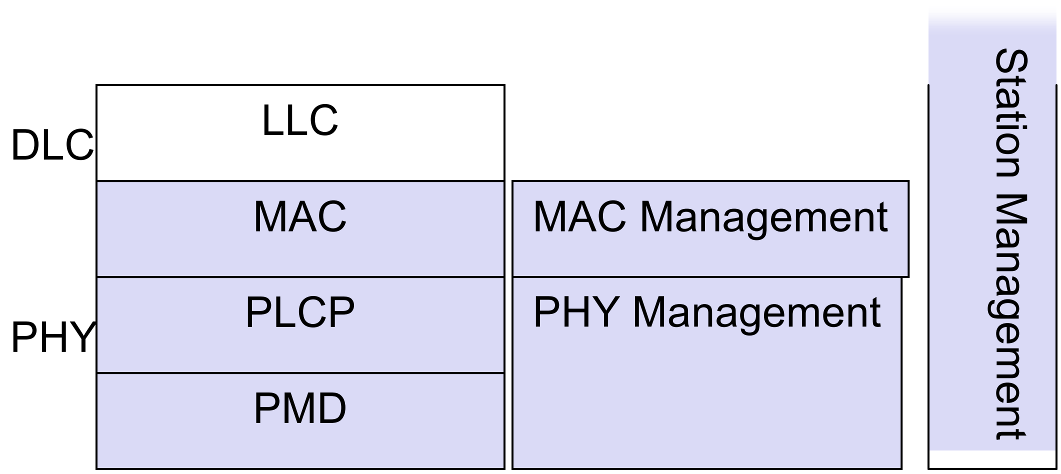
PHY Management

Channel selection, MIB

Station Management

Coordination of all management functions

802.11 - Layers



802.11 - Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR

- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

802.11 - MAC layer I - DFWMAC

Traffic services

- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods

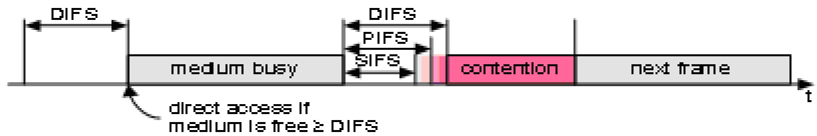
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)

- access point polls terminals according to a list

Priorities

- defined through different inter frame spaces
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service

802.11 - MAC layer



MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System

AP: Access Point

DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier

RA: Receiver Address

TA: Transmitter Address

<u>MAC management</u>

Synchronization

- try to find a LAN, try to stay within a LAN
- timer etc.

Power management

- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

Association/Reassociation

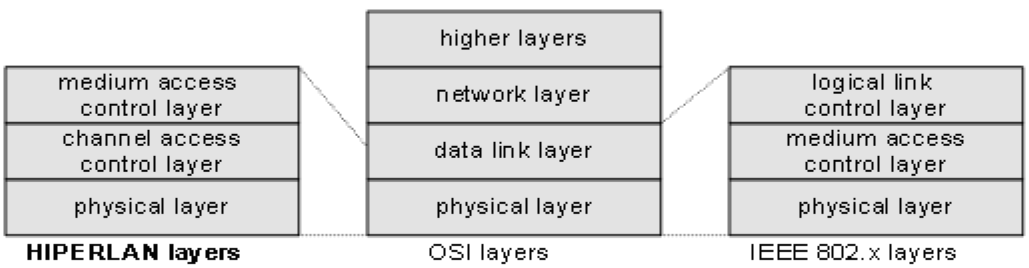
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base

- managing, read, write

HIPERLAN

- ETSI standard
  - European standard, cf. GSM, DECT, ...
  - Enhancement of local Networks and interworking with fixed networks
  - integration of time-sensitive services from the early beginning
- HIPERLAN family
  - one standard cannot satisfy all requirements
    - range, bandwidth, QoS support
    - commercial constraints
  - HIPERLAN 1 standardized since 1996



HIPERLAN 1 - Characteristics

Data transmission

- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services

- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

Topology

- infrastructure or ad-hoc networks
- transmission range can be larger then coverage of a single node („forwarding" integrated in mobile terminals)

Further mechanisms

- power saving, encryption, checksums

Services and protocols

CAC service

- definition of communication services over a shared medium
- specification of access priorities
- abstraction of media characteristics

MAC protocol

- MAC service, compatible with ISO MAC and ISO MAC bridges
- uses HIPERLAN CAC

CAC protocol

- provides a CAC service, uses the PHY layer, specifies hierarchical access mechanisms for one or several channels

Physical protocol

- send and receive mechanisms, synchronization, FEC, modulation, signal strength

HIPERLAN 1 - Physical layer

Scope

- modulation, demodulation, bit and frame synchronization
- forward error correction mechanisms
- measurements of signal strength
- channel sensing

Channels

- 3 mandatory and 2 optional channels (with their carrier frequencies)
- mandatory
    - channel 0: 5.1764680 GHz
    - channel 1: 5.1999974 GHz
    - channel 2: 5.2235268 GHz
- optional (not allowed in all countries)
    - channel 3: 5.2470562 GHz
    - channel 4: 5.2705856 GHz

BLUETOOTH

Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many members

Scenarios

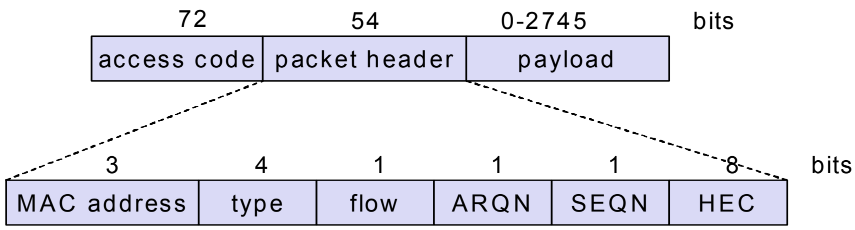
- connection of peripheral devices
  - loudspeaker, joystick, headset
- support of ad-hoc networking
  - small devices, low-cost
- bridging of networks
  - e.g., GSM via mobile phone - Bluetooth - laptop

Simple, cheap, replacement of IrDA, low range, lower data rates

- 2.4 GHz, FHSS, TDD, CDMA

Bluetooth MAC layer

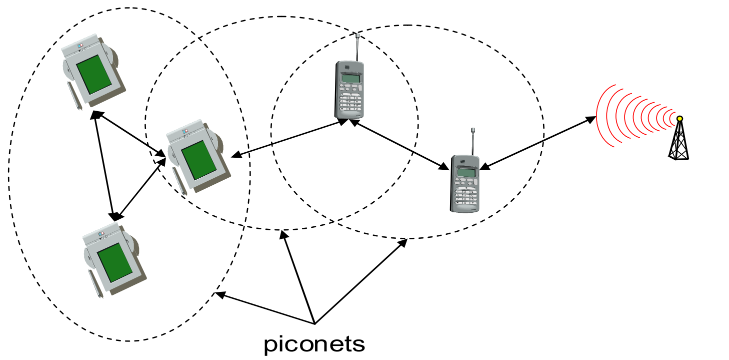
- Synchronous Connection-Oriented link (SCO)
  - symmetrical, circuit switched, point-to-point
- Asynchronous Connectionless Link (ACL)
  - packet switched, point-to-multipoint, master polls
- Access code
  - synchronization, derived from master, unique per channel
- Packet header
  - 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



7.48.1

Scatternets

- Each piconet has one master and up to 7 slaves
- Master determines hopping sequence, slaves have to synchronize
- Participation in a piconet = synchronization to hopping sequence
- Communication between piconets = devices jumping back and forth between the piconets



7.49.1

UNIT IV

MOBILE NETWORK LAYER

Mobile IP – Dynamic Host Configuration Protocol - Routing – DSDV – DSR – Alternative Metrics

Mobile IP

A standard for mobile computing and networking

Computers doesn't stay put.

Change location without restart its application or terminating any ongoing communication

IP Networking

Protocol layer

Network Layer

Transport Layer

What does IP do

moving packets from source to destination

No ’end-to-end’ guarantees

IP addresses

Network-prefix

Host portion

IP Routing

Packet Header

Network-prefix

Every node on the same link has the same network-prefix

Mobile IP Solves the following problems

f a node moves from one link to another without chnging its IP address, it will be unable to receive packets at the new link; and

If a node moves from one link to another without chnging its IP address, it will be unable to receive packets at the new link; and

Mobile IP Overview

Solution for Internet

Scalable, robust, secure, maintain communication

Use their permanent IP address

Routing protocol

Route packets to nodes that could potentially change location very rapidly

Layer 4-7, outside Mobile IP, but will be of major interest

<u>Mobile IP: Terminology</u>

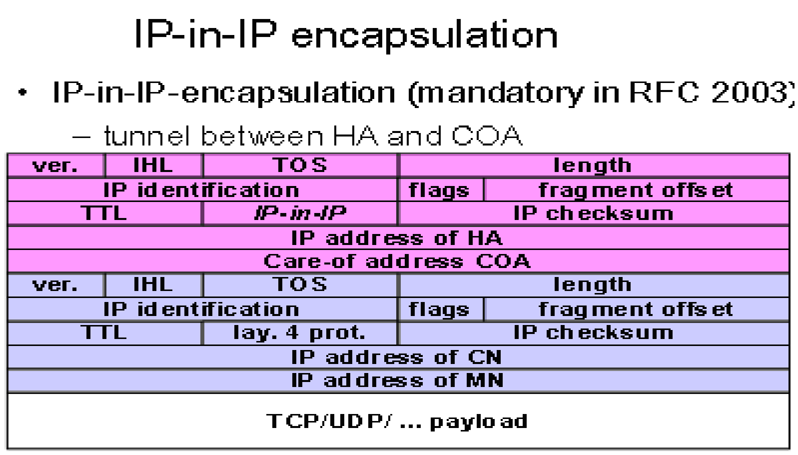
- Mobile Node (MN)
  - node that moves across networks without changing its IP address
- Correspondent Node (CN)
  - ost with which MN is “corresponding” (TCP)
- Home Agent (HA)

  - host in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP packets to the COA
- Foreign Agent (FA)
  - host in the current foreign network of the MN, typically a router
  - forwards tunneled packets to the MN, typically the default router for MN
- Care-of Address (COA)
  - address of the current tunnel end-point for the MN (at FA or MN)
  - actual location of the MN from an IP point of view

<u>Tunneling</u>

An encapsulating IP packet including a path and an original IP packet

IP-in-IP encapsulation



<u>Mobile IP and IPv6</u>

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols

- Security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address auto configuration
- No need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement;
- Addresses are always *co-located*
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
- soft"hand-over, i.e. without packet loss, between two subnets is supported

- MN sends the new COA to its old router
- the old router encapsulates all incoming packets for the MN and forwards them to the new COA
- Authentication is always granted

ROUTING

Motivation for Mobile IP

Routing

- based on IP destination address, network prefix (e.g. 129.13.42)
- determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?

- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?

- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take to long time

Requirements to Mobile IP

Transparency

- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility

- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security

- authentication of all registration messages

Efficiency and scalability

- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole
- Internet

IPv6 availability

- Generally available with (new) versions of most operating systems.
    - BSD, Linux 2.2 Solaris 8
- An option with Windows 2000/NT
- Most routers can support IPV6
- Supported in J2SDK/JRE 1.4

IPv6 Design Issues

- Overcome IPv4 scaling problem
    - Lack of address space.
- Flexible transition mechanism.
- New routing capabilities.
- Quality of service.
- Security.

- Ability to add features in the future.

Mobile ad hoc networks

Standard Mobile IP needs an infrastructure

- Home Agent/Foreign Agent in the fixed network
- DNS, routing etc. are not designed for mobility

Sometimes there is no infrastructure!

- remote areas, ad-hoc meetings, disaster areas
- Cost can also be an argument against an infrastructure!
- no default router available
- every node should be able to forward

Traditional routing algorithms

Traditional algorithms are pro-active – i.e. operate independent of user-message demands. Suitable for wired networks.

Distance Vector

- periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
- selection of the shortest path if several paths available Link State
- periodic notification of all routers about the current state of all physical links
- routers get a complete picture of the network Example
- ARPA packet radio network (1973), DV-Routing, up to 138 nodes
- every 7.5s exchange of routing tables including link quality
- updating of tables also by reception of packets
- routing problems solved with limited flooding

Problems of traditional routing algorithms

Dynamics of the topology

- Frequent changes of connections, connection quality, participants
- Limited performance of mobile systems
- periodic updates of routing tables need energy without contributing to the transmission of user data; sleep modes difficult to realize
- Limited bandwidth of the system is reduced even more due to the exchange of routing information
- Links can be asymmetric, i.e., they can have a direction dependent transmission quality
- Uncontrolled redundancy in links
- Interference – ‘unplanned links’ (advantage?)

DSDV

DSDV (Destination Sequenced Distance Vector)

Early work

- on demand version: AODV (Ad-hoc On-demand Distance Vector

Expansion of distance vector routing (but still pro-active)

Sequence numbers for all routing updates

- assures in-order execution of all updates
- avoids loops and inconsistencies

Decrease of update frequency (‘damping’)

- store time between first and best announcement of a path
- inhibit update if it seems to be unstable (based on the stored time values)

DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) is a network protocol for automatically assigning TCP/IP information to client machines. Each DHCP client connects to the centrally-located DHCP server which returns that client's network configuration, including the IP address, gateway, and DNS servers

DHCP is useful for automatic configuration of client network interfaces. When configuring the client system, the administrator can choose DHCP and instead of entering an IP address, netmask, gateway, or DNS servers. The client retrieves this information from the DHCP server. DHCP is also useful if an administrator wants to change the IP addresses of a large number of systems. Instead of reconfiguring all the systems, he can just edit one DHCP configuration file on the server for the new set of IP addresses. If the DNS servers for an organization changes, the changes are made on the DHCP server, not on the DHCP clients. Once the network is restarted on the clients (or the clients are rebooted), the changes take effect.

Furthermore, if a laptop or any type of mobile computer is configured for DHCP, it can be moved from office to office without being reconfigured as long as each office has a DHCP server that allows it to connect to the network.

Configuration File

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, while other options can be declared for individual client systems.

The configuration file can contain extra tabs or blank lines for easier formatting. Keywords are case-insensitive and lines beginning with a hash mark (#) are considered comments.

Two DNS update schemes are currently implemented — the ad-hoc DNS update mode and the interim DHCP-DNS interaction draft update mode. If and when these two are accepted as part of the Internet Engineering Task Force (IETF) standards process, there will be a third mode — the standard DNS update method. The DHCP server must be configured to use one of the two current schemes. Version 3.0b2pl11 and previous versions used the ad-hoc mode; however, it has been deprecated.

There are two types of statements in the configuration file:

- **Parameters** — State how to perform a task, whether to perform a task, or what network configuration options to send to the client.

- **Declarations** — Describe the topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.

Some parameters must start with the **option** keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

In **Example** the **routers**, **subnet-mask**, **domain-name**, **domain-name-servers**, and **time-offset** options are used for any **host** statements declared below it.

Additionally, a **subnet** can be declared, a **subnet** declaration must be included for every subnet in the network. If it is not, the DHCP server fails to start.

In this **example**, there are global options for every DHCP client in the subnet and a `range` declared. Clients are assigned an IP address within the `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers              192.168.1.254;
    option subnet-mask          255.255.255.0;

    option domain-name          "example.com";
    option domain-name-servers  192.168.1.1;

    option time-offset          -18000;    # Eastern Standard Time

        range 192.168.1.10 192.168.1.100;
```

<u>Dynamic source routing</u>

Split routing into discovering a path and maintaining a path

Discovering a path

Only if a path for sending packets to a certain destination is needed and no path is currently available (reactive algorithm)

Maintaining a path

Only while the path is in use: make sure that it can be used continuously

Path discovery

Broadcast a packet (Route Request) with destination address and unique ID

- if a station receives a broadcast packet
- if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet) if the packet has already been received earlier (identified via ID) then

Discard the packet

- otherwise, append own address and broadcast packet
- sender receives packet with the current path (address list)

Maintaining paths

- After sending a packet
- wait for a layer 2 acknowledgement (if applicable)
- listen into the medium to detect if other stations forward the packet (if possible)
- request an explicit acknowledgement
- if a station encounters problems it can inform the sender of a packet or look-up a new path locally

ALTERNATIVE METRICS.

Mobile IP with reverse tunneling

Router accepts often only "topological correct"addresses (firewall!)

- a packet from the MN encapsulated by the FA is now topological correct
- furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)

Reverse tunneling does not solve

- problems with firewalls, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
- optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)
- The standard is backwards compatible
- the extensions can be implemented easily and cooperate with current implementations without these extensions

Agent Advertisements can carry requests for reverse tunneling

World Wide Web and mobility

Protocol (HTTP, Hypertext Transfer Protocol) and language

(HTML, Hypertext Markup Language) of the Web have not been designed for mobile applications and mobile devices, thus creating many problems!

Typical transfer sizes

- HTTP request: 100-350 byte
- responses avg. <10 kbyte, header 160 byte, GIF 4.1kByte, JPEG
- 12.8 kbyte, HTML 5.6 kbyte
- but also many large files that cannot be ignored
- The Web is no file system
- Web pages are not simple files to download
- static and dynamic content, interaction with servers via forms, content transformation, push technologies etc.
- many hyperlinks, automatic loading and reloading, redirecting
- a single click might have big consequences!

UNIT V

TRANSPORT AND APPLICATION LAYERS

Traditional TCP – Classical TCP improvements – WAP, WAP 2.0.

TRADITIONAL TCP

TCP is an alternative transport layer protocol over IP.

- TCP provides:
  - Connection-oriented
  - Reliable
  - Full-duplex
  - Byte-Stream

Connection-Oriented

- *Connection oriented* means that a virtual connection is established before any user data is transferred.
- If the connection cannot be established - the user program is notified.
- If the connection is ever interrupted - the user program(s) is notified.

Reliable

- *Reliable* means that every transmission of data is acknowledged by the receiver.
- If the sender does not receive acknowledgement within a specified amount of time, the sender retransmits the data

Byte Stream

- *Stream* means that the connection is treated as a stream of bytes.
- The user application does not need to package data in individual datagrams (as with UDP**).**

Buffering

- TCP is responsible for buffering data and determining when it is time to send a datagram.
- It is possible for an application to tell TCP to send the data it has buffered without waiting for a buffer to fill up.

Full Duplex

- TCP provides transfer in both directions.
- To the application program these appear as 2 unrelated data streams, although TCP can piggyback control and data communication by providing control information (such as an ACK) along with user data.

TCP Ports

- Interprocess communication via TCP is achieved with the use of ports (just like UDP).
- UDP ports have no relation to TCP ports (different name spaces).

TCP Segments

- The chunk of data that TCP asks IP to deliver is called a *TCP segment*.
- Each segment contains:
    - data bytes from the byte stream
    - control information that identifies the data bytes

TCP Lingon

- When a client requests a connection it sends a “SYN” segment (a special TCP segment) to the server port.
- SYN stands for synchronize. The SYN message includes the client’s ISN.
- ISN is Initial Sequence Number.
- Every TCP segment includes a *Sequence Number* that refers to the first byte of *data* included in the segment.
- Every TCP segment includes an *Acknowledgement Number* that indicates the byte number of the next data that is expected to be received.
    - All bytes up through this number have already been received.
- There are a bunch of control flags:
    - URG: urgent data included.
    - ACK: this segment is (among other things) an acknowledgement.
    - RST: error – connection must be reset.
    - SYN: synchronize Sequence Numbers (setup)
    - FIN: polite connection termination
- MSS: Maximum segment size (A TCP option)

- Window: Every ACK includes a Window field that tells the sender how many bytes it can send before the receiver will have to toss it away (due to fixed buffer size).

CLASSICAL TCP IMPROVEMENTS

TCP Connection Creation

- Programming details later - for now we are concerned with the actual communication.
- **A** *server* accepts a connection.
  - Must be looking for new connections!
- A *client* requests a connection.
  - Must *know* where the server is!

Client Starts

- A client starts by sending a SYN segment with the following information:
  - Client's ISN (generated pseudo-randomly)
  - Maximum Receive Window for client.
  - Optionally (but usually) MSS (largest datagram accepted).
  - No payload! (Only TCP headers)

Server Response

- When a waiting server sees a new connection request, the server sends back a SYN segment with:
  - Server's ISN (generated pseudo-randomly)
  - Request Number is Client ISN+1
  - Maximum Receive Window for server.
  - Optionally (but usually) MSS
  - No payload! (Only TCP headers)
- When the Server's SYN is received, the client sends back an ACK with:
  - Acknowledgment Number is Server's ISN+1

TCP 3-way handshake

Client: "I want to talk, and I'm starting with byte number *X*".

Server: "OK, I'm here and I'll talk. My first byte will be called number *Y*, and I know your first byte will be number *X+1*".

Client: "Got it - you start at byte number *Y+1*".

Bill: "Monica, I'm afraid I'll syn and byte your ack"

TCP Data and ACK

- Once the connection is established, data can be sent.
- Each data segment includes a sequence number identifying the first byte in the segment.
- Each segment (data or empty) includes a request number indicating what data has been received

Buffering

- Keep in mind that TCP is part of the Operating System. The O.S. takes care of all these details asynchronously.
- The TCP layer doesn't know when the application will ask for any received data.
- TCP buffers incoming data so it's ready when we ask for it.

TCP Buffers

- Both the client and server allocate buffers to hold incoming and outgoing data
  - The TCP layer does this.
- Both the client and server announce with every ACK how much buffer space remains (the Window field in a TCP segment).

Send Buffers

- The application gives the TCP layer some data to send.
- The data is put in a send buffer, where it stays until the data is ACK'd.
- The TCP layer won't accept data from the application unless (or until) there is buffer space.

ACKs

- A receiver doesn't have to ACK every segment (it can ACK many segments with a single ACK segment).
- Each ACK can also contain outgoing data (piggybacking).
- If a sender doesn't get an ACK after some time limit, it resends the data.

TCP Segment Order

- Most TCP implementations will accept out-of-order segments (if there is room in the buffer).
- Once the missing segments arrive, a single ACK can be sent for the whole thing.
- Remember: IP delivers TCP segments, and IP is not reliable - IP datagrams can be lost or arrive out of order.

Termination

- The TCP layer can send a RST segment that terminates a connection if something is wrong.
- Usually the application tells TCP to terminate the connection politely with a FIN segment.

TCP Sockets Programming

- Creating a *passive mode* (server) socket.
- Establishing an application-level *connection*.
- Sending/receiving data.
- Terminating a connection.

Establishing a passive mode TCP socket

Passive mode:

- Address already determined.
- Tell the kernel to accept incoming connection requests directed at the socket address.
  - ***3-way handshake***
- Tell the kernel to queue incoming connections for us.

Accepting an incoming connection

- Once we start listening on a socket, the O.S. will queue incoming connections
  - Handles the 3-way handshake
  - Queues up multiple connections.
- When our application is ready to handle a new connection, we need to ask the O.S. for the next connection.

Terminating a TCP connection

- Either end of the connection can call the close() system call.
- If the other end has closed the connection, and there is no buffered data, reading from a TCP socket returns 0 to indicate EOF

Client Code

- TCP clients can connect to a server, which:
  - takes care of establishing an endpoint address for the client socket.
    - don't need to call bind first, the O.S. will take care of assigning the local endpoint address (TCP port number, IP address).
  - Attempts to establish a connection to the specified server.
    - ***3-way handshake***

Reading from a TCP socket

- By default **read()** will block until data is available.
- Reading from a TCP socket may return less than max bytes (whatever is available).
- You must be prepared to read data 1 byte at a time!

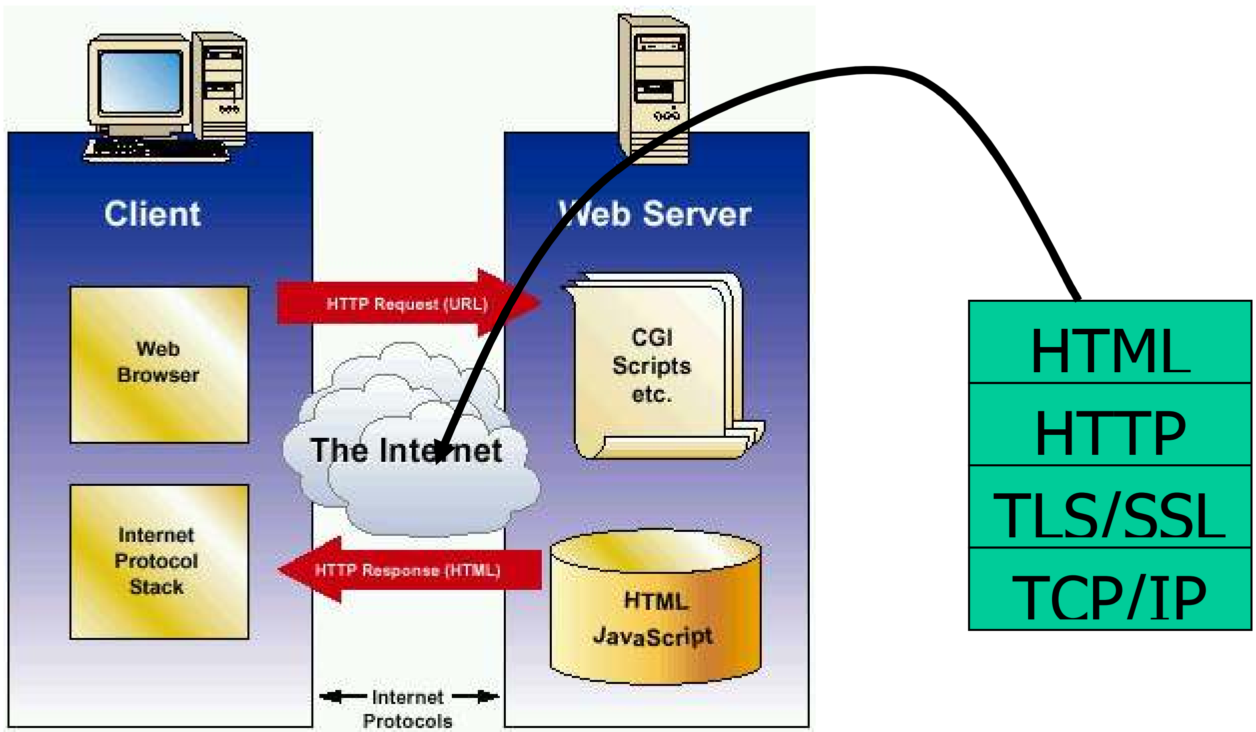
<u>WIRELESS APPLICATION PROTOCOL (WAP)</u>

- Empowers mobile users with wireless devices to easily access and interact with information and services.
- A “standard” created by wireless and Internet companies to enable Internet access from a cellular phone

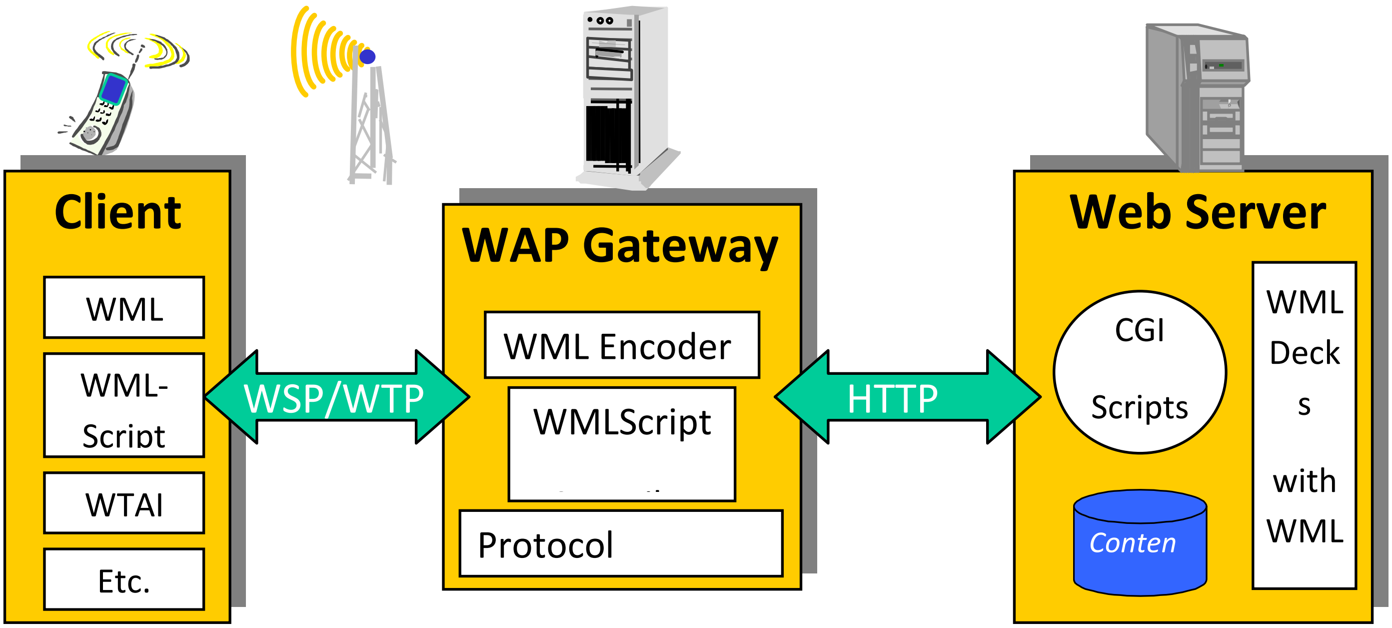
WAP: Main Features

- Browser
  - “Micro browser”, similar to existing web browsers
- Markup language
  - Similar to HTML, adapted to mobile devices
- Script language
  - Similar to Javascript, adapted to mobile devices
- Gateway
  - Transition from wireless to wired world
- Server
  - “Wap/Origin server”, similar to existing web servers
- Protocol layers
  - Transport layer, security layer, session layer etc.
- Telephony application interface
  - Access to telephony functions

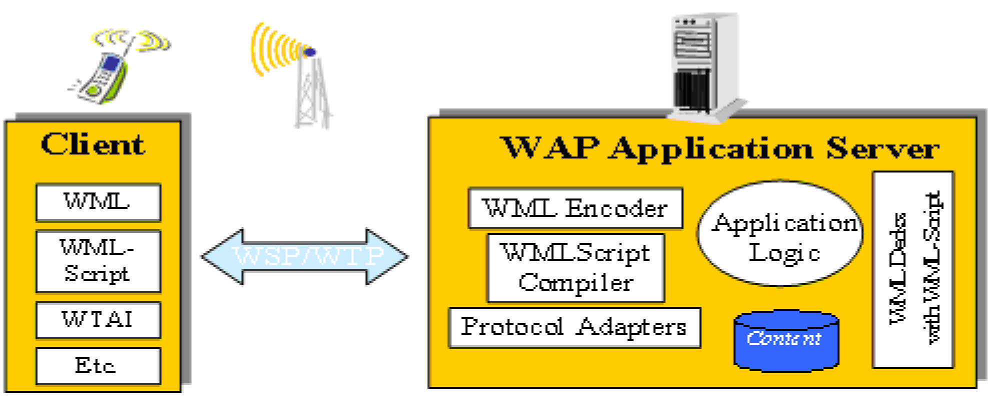
Internet Model



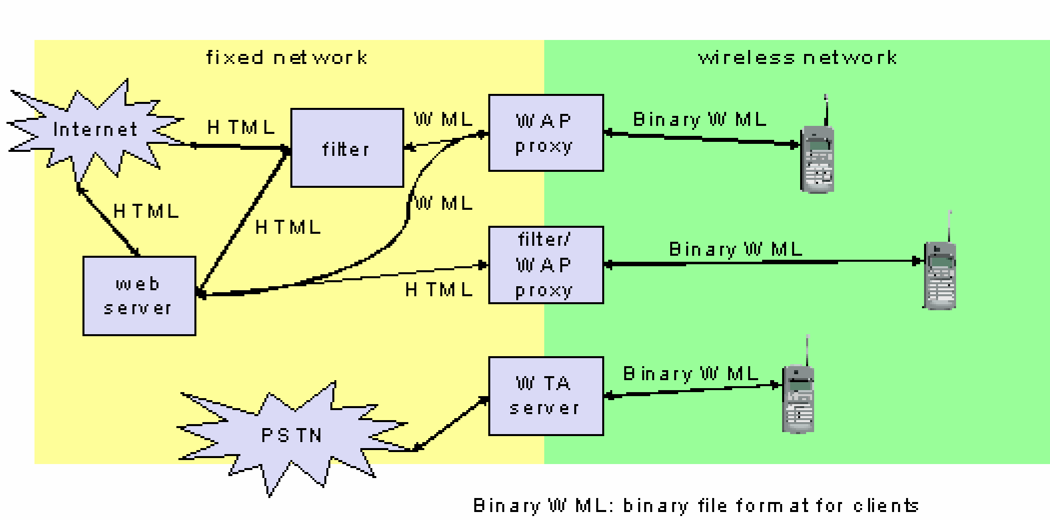
WAP Architecture



WAP Application Server



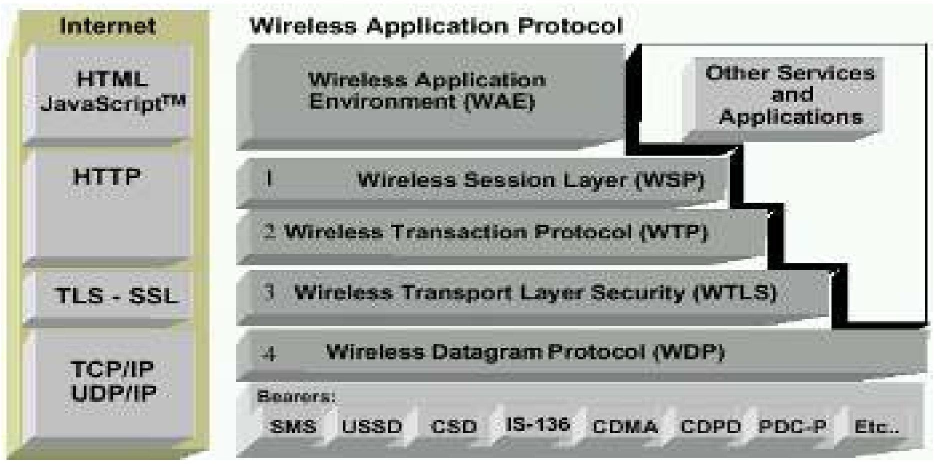
WAP: Network Elements



WAP Specifies

- Wireless Application Environment
  - WML Microbrowser
  - WMLScript Virtual Machine
  - WMLScript Standard Library
  - Wireless Telephony Application Interface (WTAI)
  - WAP content types
- Wireless Protocol Stack
  - Wireless Session Protocol (WSP)
  - Wireless Transport Layer Security (WTLS)
  - Wireless Transaction Protocol (WTP)
  - Wireless Datagram Protocol (WDP)
  - Wireless network interface definitions

WAP Stack



- WAE (Wireless Application Environment):
  - Architecture: application model, browser, gateway, server
  - WML: XML-Syntax, based on card stacks, variables, ...
  - WTA: telephone services, such as call control, phone book etc.

- WSP (Wireless Session Protocol):
  - Provides HTTP 1.1 functionality
  - Supports session management, security, etc.

- WTP (Wireless Transaction Protocol):
  - Provides reliable message transfer mechanisms
  - Based on ideas from TCP/RPC

- WTLS (Wireless Transport Layer Security):
  - Provides data integrity, privacy, authentication functions
  - Based on ideas from TLS/SSL

- WDP (Wireless Datagram Protocol):
  - Provides transport layer functions
  - Based on ideas from UDP

WHY WAP?

- Wireless networks and phones
  - have specific needs and requirements
  - not addressed by existing Internet technologies
- WAP
  - Enables any data transport
    - TCP/IP, UDP/IP, GUTS (IS-135/6), SMS, or USSD.
  - Optimizes the content and air-link protocols
  - Utilizes plain Web HTTP 1.1 servers
    - leverages existing development methodologies
    - utilizes standard Internet markup language technology (XML)
    - all WML content is accessed via HTTP 1.1 requests
  - WML UI components map well onto existing mobile phone user interfaces
    - no re-education of the end-users
    - leveraging market penetration of mobile devices
  - Several modular entities together form a fully compliant Internet entity

WAP: "Killer" Applications

- Location-based services
  - Real-time traffic reporting, Event/restaurant recommendation
- Enterprise solutions
  - Email access, Database access, "global" intranet access
  - Information updates "pushed" to WAP devices
- Financial services
  - Banking, Bill-paying, Stock trading, Funds transfers
- Travel services
  - Schedules and rescheduling, Reservations
- Gaming and Entertainment
  - Online, real-time, multi-player games
  - Downloadable horoscopes, cartoons, quotes, advice
- M-Commerce
  - Shopping on the go
  - Instant comparison shopping
  - Location-based special offers and sales

Wireless Application Environment (WAE)

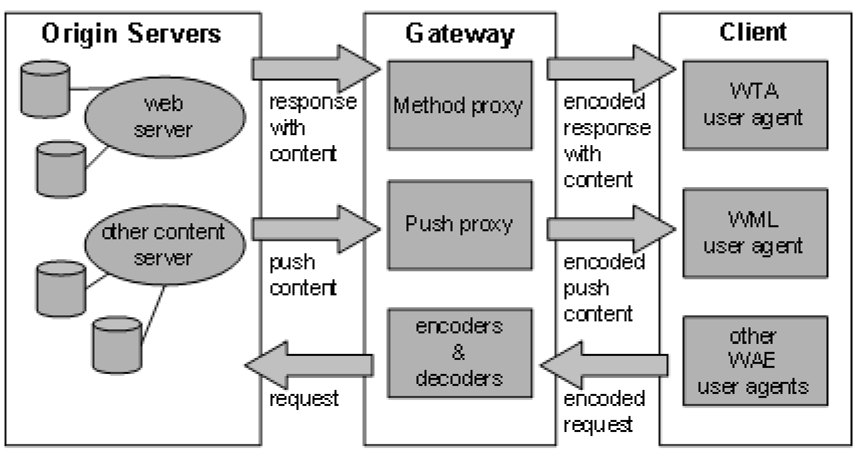
- Goals
  - device and network independent application environment

- for low-bandwidth, wireless devices
- considerations of slow links, limited memory, low computing power, small display, simple user interface (compared to desktops)
- integrated Internet/WWW programming model
- high interoperability

WAE Components

- Architecture
  - Application model, Microbrowser, Gateway, Server
- User Agents
  - WML/WTA/Others
  - content formats: vCard, vCalendar, Wireless Bitmap, WML, ...
- WML
  - XML-Syntax, based on card stacks, variables, ...
- WMLScript
  - procedural, loops, conditions, ... (similar to JavaScript)
- WTA
  - telephone services, such as call control, text messages, phone book, ... (accessible from WML/WMLScript)
- Proxy (Method/Push)

WAE: Logical Model



WML: Wireless Markup Language

- Tag-based browsing language:

    - Screen management (text, images)
    - Data input (text, selection lists, etc.)
    - Hyperlinks & navigation support
- Takes into account limited display, navigation capabilities of devices
- XML-based language
    - describes only intent of interaction in an abstract manner
    - presentation depends upon device capabilities
- Cards and Decks
    - document consists of many cards
    - User interactions are split into cards
    - Explicit navigation between cards
    - cards are grouped to decks
    - deck is similar to HTML page, unit of content transmission
- Events, variables and state mgmt
- The basic unit is a **card**. Cards are grouped together into **Decks** Document ~ Deck (unit of transfer)
- All decks must contain
    - Document prologue
        - XML & document type declaration
    - <WML> element
        - Must contain one or more cards

<u>WML Example</u>

WML>

<CARD>

<DO TYPE="ACCEPT">

<GO URL="#eCard"/>

</DO

Welcome!

</CARD>

<CARD NAME="eCard">

<DO TYPE="ACCEPT">

<GO URL="/submit?N=$(N)&S=$(S)"/>

</DO>

Enter name: <INPUT KEY="N"/>

```
  Choose speed:

  <SELECT KEY="S">

   <OPTION VALUE="0">Fast</OPTION>

   <OPTION VALUE="1">Slow</OPTION>

  <SELECT>

 </CARD>

</WML>
```

WMLScript

- Complement to WML
  - Derived from JavaScript™
- Provides general scripting capabilities
  - Procedural logic, loops, conditionals, etc.
  - Optimized for small-memory, small-cpu devices

- Features
  - local user interaction, validity check of user input
  - access to device facilities (phone call, address book etc.)
  - extensions to the device software
    - configure device, download new functionality after deployment

- Bytecode-based virtual machine
  - Stack-oriented design, ROM-able
  - Designed for simple, low-impact implementation
- WMLScript compiler resides in the network

WMLScript Libraries

- Lang - VM constants, general-purpose math functionality, etc.
- String - string processing functions
- URL - URL processing

- Browser - WML browser interface
- Dialog - simple user interface
- Float - floating point functions

Wireless Telephony Application (WTA)

- Collection of telephony specific extensions
  - designed primarily for network operators

- Example
  - calling a number (WML)
    wtai://wp/mc;07216086415
  - calling a number (WMLScript)
    WTAPublic.makeCall("07216086415");

- Implementation
  - Extension of basic WAE application model
  - Extensions added to standard WML/WMLScript browser
  - Exposes additional API (WTAI)

WTA Features

- Extension of basic WAE application model
  - network model for interaction
    - client requests to server
    - event signaling: server can push content to the client
  - event handling
    - table indicating how to react on certain events from the network
    - client may now be able to handle unknown events
  - telephony functions
    - some application on the client may access telephony functions
- WTAI includes:
  - Call control
  - Network text messaging
  - Phone book interface
  - Event processing
- Security model: segregation
  - Separate WTA browser
  - Separate WTA port

WAP Push Services

- Web push
  - Scheduled pull by client (browser)
    - example: Active Channels
  - no real-time alerting/response
    - example: stock quotes
- Wireless push
  - accomplished by using the network itself
    - example: SMS
  - limited to simple text, cannot be used as starting point for service
    - example: if SMS contains news, user cannot request specific news item
- WAP push
  - Network supported push of WML content
    - example: Alerts or service indications
  - Pre-caching of data (channels/resources)

Push Access Protocol

- Based on request/response model
- Push initiator is the client
- Push proxy is the server
- Initiator uses HTTP POST to send push message to proxy
- Initiator sends control information as an XML document, and content for mobile (as WML)
- Proxy sends XML entity in response indicating submission status
- Initiator can
  - cancel previous push
  - query status of push
  - query status/capabilities of device

Push Proxy Gateway

- WAP stack (communication with mobile device)
- TCP/IP stack (communication with Internet push initiator)
- Proxy layer does
  - control information parsing
  - content transformation
  - session management
  - client capabilities
  - store and forward
  - prioritization

- address resolution
- management function

WTP Services and Protocols

- WTP (Transaction)
  - provides reliable data transfer based on request/reply paradigm
    - no explicit connection setup or tear down
    - optimized setup (data carried in first packet of protocol exchange)
    - seeks to reduce 3-way handshake on initial request
  - supports
    - header compression
    - segmentation /re-assembly
    - retransmission of lost packets
    - selective-retransmission
    - port number addressing (UDP ports numbers)
    - flow control
  - message oriented (not stream)
  - supports an Abort function for outstanding requests
  - supports concatenation of PDUs
  - supports User acknowledgement or Stack acknowledgement option
    - acks may be forced from the WTP user (upper layer)
    - default is stack ack

WAP 2.0.

WSP - Wireless Session Protocol

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

- WSP Services
  - provides shared state between client and server, optimizes content transfer
  - session management (establish, release, suspend, resume)
  - efficient capability negotiation
  - content encoding
  - push

- WSP/B (Browsing)
  - HTTP/1.1 functionality - but binary encoded
  - exchange of session headers
  - push and pull data transfer
  - asynchronous requests

WSP Overview

- Header Encoding
  - compact binary encoding of headers, content type identifiers and other well-known textual or structured values
  - reduces the data actually sent over the network
- Capabilities (are defined for):
  - message size, client and server
  - protocol options: Confirmed Push Facility, Push Facility, Session Suspend Facility, Acknowledgement headers
  - maximum outstanding requests
  - extended methods
  - header code pages
- Suspend and Resume
  - server knows when client can accept a push
  - multi-bearer devices
  - dynamic addressing
  - allows the release of underlying bearer resources
- Session Context and Push
  - push can take advantage of session headers
  - server knows when client can accept a push

- Connection-mode
  - long-lived communication, benefits of the session state, reliability

- Connectionless-mode
  - stateless applications, no session creation overhead, no reliability overhead

WAP: Ongoing Work

- WDP
  - Tunnel to support WAP where no (end-to-end) IP bearer available
- WTLS

- support for end-to-end security (extending WTLS endpoint beyond WAP Gateway)
    - interoperable between WAP and Internet (public key infrastructure)
    - integrating Smart Cards for security functions
- WTP
    - efficient transport over wireless links (wireless TCP)
    - bearer selection/switching
    - quality of service definitions
- WSP
    - quality of service parameters
    - multicast data, multimedia support
- WAE

User agent profiles: personalize for device characteristics, preferences etc

ONLINE QUESTIONS

UNIT-I

QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION4	ANSWERS
The advantage of cable based transmission is	No mobility of transmission	No interference	Fixed transmitter and receiver	Limited no of interconnections	No interference
The range of wavelength and frequency of infrared is	Wavelength between 1.0 µm and 2.0 µm and (1.5 to 3) x 1014 Hz	Wavelength between 0.70 µm and 0.40 µm and (4.3 to 7.5) x 1014Hz	Wavelength between 0.90 µm and 0.85 µm and (3.3 to 3.35) x 1014Hz	Wavelength less than 0.40 and frequency greater than 750 THz	Wavelength between 0.90 µm and 0.85 µm and (3.3 to 3.35) x 1014Hz
In which shift keying technique the phase angle of a carrier shifts to one of eight different angles in one of eight octets between 0^0 to 360^0 as per eight combinations	Binary shift keying	Gaussian shift keying	Quadrature phase shift keying	Eight phase shift keying	Eight phase shift keying
In which modulation technique there is 4-PSK(QPSK) modulation with 16 distinct quadruplets.	Phase modulation	Frequency modulation	Quadrature amplitude modulation	Amplitude modulation	Quadrature amplitude modulation
The frequency rate at which a symbol XORs with the modulating signal to generate a rate is called as	Frequency rate	Modulation rate	Chipping rate	Signal rate	Chipping rate
This is the method of data transmission in which a communication channel is once established continues to be used till the transmission completes	Packet switching	Circuit switching	Channel switching	Data switching	Circuit switching
Line of Sight of propagation is the transmission of signals without______n between the transmitter and receiver	Refraction	Diffraction	Scattering	All the above	All the above
Signal strength decreases due to _________when obstacles in the path of signal are greater in size than wavelength of the signal	Blocking	Reflected	Attenuation	Scattering	Attenuation
. A dipole antenna is to be mounted on a conducting surface. Calculate the length of the required antenna for transmitting a GSM signal of frequency 600 MHz	12.5 cm	12 m	1.25 cm	1.25 m	12.5 cm

The reflected signal suffers a_________in reaching its destination	time	frequency	wavelength	delay	delay
. _________is an access method which entails assignment of different frequency-slices to different users for accessing the same carrier.	SDMA	TDMA	FDMA	CDMA	FDMA
. Which mobile devices communicate at higher data rates	2.5G	3G	2G	2.5G+	3G
A standard which is used for object exchanges datas provided short distance upto 1m or 100m range as per radio spectrum is	GPRS	GSM	WiMax	Bluetooth	Bluetooth
A technique in which amplitude, frequency or phase angle parameters of carrier frequency or subcarrier frequencies varied with time according to signal bit 1 or 0	Amplitude modulation	Frequency modulation	Analog modulation	Digital modulation	Digital modulation
_________is a method for a multi-carrier and multi-tone access method for transmitting multiple carriers for a set of symbol	QPSK	OFDM	QAM	PSK	OFDM
A_________is a part of data that can take a distinct path from other packets from the same source and each packet can have variable delays.	circuit	code	packet	signal	packet
._________.is a technique in which phase angle of carrier shifts in one of four quadrants between 0^0 and 360^0	QPSK	ASK	PSK	BPSK	QPSK
A technique in which a wireless transmitter channel transmits a modulated signal and accesses in a time-slice another modulated signal accesses in another time.	SDMA	TDMA	FDMA	CDMA	TDMA
The delay time for given $t_{indirect=}$ 4.95µs and $t_{direct=}$4.33 µs is	0.62 µs	6.2 µs	62 µs	0.062 µs	0.62 µs
The Electricals signals are transmitted by converting them into _________	wavelength	frequency	electromagnetic radiations	signal	electromagnetic radiations

A WPAN standard that is IEEE 802.15.4-based is called	Bluetooth	WiMax	iMode	ZigBee	ZigBee
__________based communication devices are also used for short distance communication when there are no obstacles such as walls between the devices.	visible light	ultravoilet	infrared	UHF	infrared
Which provides web contents to small area display devices in mobile phones	WAP	WML	GSM	GPRS	WAP
Which computing refers to blending of computing devices with environmental objects	Mobile computing	Ubiquitous computing	Pervasive computing	Soft computing	Ubiquitous computing
Which is the next generation computing technique which takes into account with communication technology used by everyone everywhere at all times.	Fuzzy logic	Genetic algorithm	Ubiquitous computing	Pervasive computing	Pervasive computing
__________means without the impact of location due to mobility, access protocol deployed and hardware or software failure.	Mobile computing	Adaptability	Transparency	None of the above	Transparency
Which mobile phone contains the additional polyphonic ring tone application for personalizing your device	Smart phones	Cordless phone	2G device	All the above	Smart phones
Which is the payment system employed during a purchase activated through text-message exchanges between the customer and retail outlet of service provider	m-commerce	Sensors	m-cheque	Smartcards	m-cheque
__________is called as producer-consumer problem	Music and video	Supply chain management	Sensors	m-commerce	Supply chain management
Which occurs in wireless signals and affects the quality of service(QOS)	Interference	Bandwidth	Network issues	Security constraint	Interference
The varying protocol standards prescribed and available between different regions may lead to __________glitches	Resources constraint	Dynamic changes	Interoperability	Bandwidth	Interoperability
The language used for mobile computing is	Java/J2SE	C/C++	Visual C++	All the above	All the above

What enables the user to run an application without considering the hardware specification and functionalities?	GUI	Phone API	OS	GUI API	OS
Middleware is used	for service discovery, application adaptability, retrieving backend database	for application adaptability and retrieving backend database	for connecting to a mobile service	as a software component between the OS and hardware	for service discovery, application adaptability, retrieving backend database
The interchanges between the two diversified and distributed components needs	Hardware and software	Protocols and standards	Gateway and network	Interface and network	Protocols and standards
Which layer is used for establishing end -to -end connectivity	Physical layer	Data link	Networking	Wireless transport	Wireless transport
A network in which space is divided into cells such that each has a base station for providing service to mobile devices when mobile device roams into another cell.	Cellular Network	WLAN Network	LAN Network	System Network	Cellular Network
A mobile device such as pocket computer or a laptop connects to an access point called a	Router	LAN	Hotspot	Device point	Hotspot
. Data dissemination mechanisms are	Pushes data, pulling data and hybrid of push-pull	Pushes of database by server	Pulling database	Pulling the voice, data on server on demand	Pushes data, pulling data and hybrid of push-pull
Data Synchronization is “the ability for data in different databases to be kept__________so that repository contains the same information”.	Without interference	Without virus	Up to date	Unicast data	Up to date
.__________means maintaining uninterrupted signal connectivity when a mobile device changes location from within a cell to another cell	Infrastructure management	Registration management	Location management	Mobility management	Mobility management
. Which function is used to create a small digital fingerprint of the data to be transmitted?	Digital function	Decryption function	Hash function	Encryption function	Hash function
. A method by which multimedia files are distributed over the internet is	Podcasting	iTunes	Access point	Pushing and pulling	Podcasting

The pen based devices which enable the user to write on the LCD screen using a pen-like stick called	joystick	Pylons	PDA stick	Stylus	Stylus
An Access service that describes a WLAN network access IEEE technology or application using 802.11 standards is	WLAN	WiMax	WiFi	WPAN	WiFi
Which issues the authority of holders name, public key and expiration date	Digital signature	Digital certificate	MAC function	Certification authority	Certification authority
. In the case of a heavy load in one cell and light load in a neighboring cell it could make sense of	Dynamic allocation	Fixed allocation	Borrowing channel allocation	Channel allocation	Borrowing channel allocation
CDM cells are commonly said to	Clusters	Planning	Breathe	Drop out	Breathe
The primary goal of GSM was to provide a mobile phone system that allows users to __________thought Europe and provides voice services compatible to ISDN	Communicate	Data transmission	Voice transmission	Roam	Roam
GSM 1900 is also called as __________Digital cellular network	Personal communication service	GSM rail		GSM transit network	GSM rail
GSM rail contains__________exclusive channels	14	19	18	16	19
The transparent bearer services uses the function of__________layer to transmit data	Physical layer	Data link layer	Session layer	Network layer	Physical layer
Which is the heart of GSM	Radio subsystem	Network and switching subsystem	Operation subsystem	Maintenance subsystem	Network and switching subsystem
Which is an interesting interface?	A	Abis	O	Um	Um
.__________is used to avoid overlapping with other burst due to different delay	Tail	User data	Guard space	Training	Guard space
Temporary mobile subscriber identity (TMSI) is selected by	VLR	HLR	EIR	BSC	VLR
In which handover mechanism MS moves from one cell to another but remains in same BSC.	Intra cell handover	Inter cell, Intra BSC handover	Inter BSC, Intra MSC handover	Inter MSC handover	Inter cell, Intra BSC handover

Which is the networking unit between the GPRS network and the external packet data networks?	GPRS support node	Gateway GPRS support node	Serving GPRS support node	Register GPRS support node	Gateway GPRS support node
. Which is used to convey routing and QoS-related information between the BSS and SGSN	LLC	UDP/TCP	RLC	BSSGP	BSSGP
. An MS having GPRS capability stores a _________in the SIM in GSM	PUK number	PIN number	Cipher key number	none of the above	Cipher key number

UNIT-II

QUESTION	A	B	C	D
The task of DLC is to establish a reliable point to point or point to multipoint connection between different devices over a	Network	Wired medium	Wireless medium	Wired medium o Wireless mediur
MAC comprises all mechanisms that regulate user access to a medium using multiplexing and is similar to	Modulation	Multiplexing regulation	TDM regulation	Traffic regulatio
In wireless network the CSMA/CD is not really interested in collision at	Sender	Receiver	Both sender and receiver	Either sender or receiver
A is outside is the interference range of C. Causing a 'collision' at B does not matter since the collision is too weak . What is the problem in this situation?	Hidden problem	Near and far problem	Exposed problem	None of these
The strength of a signal ______to the square of the distance to the sender	increase proportionally	decreases proportionally	drowns up	drowns high

The new application of SDMA comes up together with_____antenna arrays	Time-forming	Beam-forming	code-forming	frequency-formi
The frequencies from base station to mobile station and from mobile station to base station are	uplink	downlink	uplink and downlink	downlink and up
All uplinks and downlinks which are regulated by the national authority use the band between	890.2 and 915 MHz, and 935.2 to 960 MHz	880.2 and 915 MHz, and 935.2 to 970 MHz	890.2 and 915 MHz, and 945.2 to 960 MHz	880.2 and 915 M and 935.2 to 96 MHz
The classical aloha scheme was invented and used in ALOHANET wireless connection of several station by	University of Hawaii	University of Halsal	University of Greenland	University of O
In non-persistent CSMA stations sense the carrier and sending immediately if the medium is idle. If the medium is busy the station_______	Checks the priority	Uses backoff algorithm	Pauses for random time	Checks probabil
In which scheme the stations can reserve future slots in the transmission period	PRMA	CSMA	DAMA	DSMA
Hidden terminal problem is solved by	PRMA	CSMA	DAMA	MACA
Using the free slots can be based on a simple round-robin scheme guarantees	Fixed TDMA	Reservation TDMA	TDMA	CDMA
Inhibit sense multiple access is also called as	PRMA	CSMA	DAMA	DSMA
The two vectors (2, 5,0) and (0,0,17) are	Orthogonal	Auto correlation	Barker code	Spreading code
Integrating over noise results for a values close to	1	2	-1	0
If we use CDMA with only one code the resulting scheme is called	PRMA	SAMA	TSMA	DSMA

Comparing to other mechanisms which scheme comprises Flexible, less planning needed with soft handover	SDMA	TDMA	CDMA	SAMA
Which scheme is standard in fixed networks together with FDMA/SDMA used in many mobile networks?	TDMA	CSMA	FDMA	SDMA
______is slotted and used for some reservation mechanisms are applied to guarantee access delay and bandwidth.	Time	Fixed TDMA	Codes	Aloha
The inner product of the vectors a and b with a=(a1,a2,…an) and b=(b1,b2,…..,bn)Is defined as	$a*b=\sum a_i b_i$	$a+b=\sum a_i * b_i$	$a*b=\sum a_i / b_i$	$a*b=\sum a$
The power level spread signal can be much____than that of original narrow band signal	Higher	Lower	All the above	Mediun
_____different channels use FDM for multiplexing which means that each channel has its own narrow frequency band for transmission	1	2	6	7
The combination of spread spectrum and CDM is becoming more and more attractive for ____applications	Mobile	Wireless	Everyday	Wired
_____system takes a user bit stream and performs an XOR to form chipping sequence	DSSS	CDM	ISSS	Narrowband

If the chipping sequence is generated properly it appears as random noise and is also called ____sequence	Code noise	Pseudo code nose	Pseudo noise	Digital noise
For _____system, total available bandwidth is split into many channels of smaller bandwidth	FHSS	DSSS	Race receiver	Integrator
In hopping sequence the time spend on a channel with a certain frequency is called as	Fast time	Decision time	Dwell time	Hopping time
_____the transmitter changes the frequency several times during the transmission of a single bit	Slow hopping	Fast hopping	Frequency hopping	Hopping sequen
Calculating the products of chips and signal, and adding the product in an integrator is also called as	Integration	Correlation	Decision unit	Rake receiver ur
The GSM hopping rate is ____	205.4 Hops/s	204.5 Hops/s	204.7 Hops/s	207.4 Hops/s
____codes requires synchronization between the transmitter and receiver as they do not exhibit a strong autocorrelation property	Best	Wireless	Orthogonal	Scrambling
____codes are generated from a matrix called Hadamard matrix	Best	Walsh	Orthogonal	Scrambling
____codes are used for channelization due to their orthoganality property	Walsh	Best	Carrier modulation	Scrambling
There are ____channels in forward link	1	2	3	4

Data rate matching with a fixed rate for a channel is used to transmit multi-encoded signals using a constant spread factor and___codes	Fixed length	Same length	Different length	Equal length
______is a technique which enables the use of idle time-slots in the frames has a predefined bit	Traffic channel	Data rate matching	Multi encoding	Block interleavi
A _____is used for identifying a traffic channel.	Long code	Block code	Paging code	*Q* pilot
The synchronous channel message is used for synchronization of ships sequence at the____	BS	MS	BTS	BSC
The objective of the ser signal waveform encoding is to ______the bit error rate at the receiver.	Increase	Reduce	Deviate	Changes
SCI=1 indicates ______of the message.	End	Beginning	Stop	Continues
The 1.25 MHz modulated output of the reverse link channel has access and ___traffic channels	Forward	Reverse	Direct	Indirect
The user signal waveform is mapped with the ________walsh codes	Orthogonal	Synchronous	Block	Pagging
IS-95 was ________ with multiple analog channel forming one digital carrier.	824 -849 MHZ and 869 – 894 MHZ	834 -854 MHZ and 859 – 893 MHZ	844 -864 MHZ and 849 – 894 MHZ	824 -849 MHZ a 829 – 894 MHZ
Orthogonal codes have almost zero cross correlation and are used in identifying the	user	channel	carrier	All the above
The walsh code used in IS-95 CDMA one has __________ matrix.	3*3	product	2*2	64*64

Two codes of n chips are orthogonal if the SOP of their component is ____	1	0	-1	+ or – 1
The vector with 16 elements is called	Orthogonal	Mask vector	Code vector	Sequence vector
WCDMA uses _________-	State code	Gold code	Orthogonal code	mask code
The synchronization of last WS is more_____ than that off slow FHSS	complex	simple	both	neither simple n complex
Each chipping frequency can be transmitted at much _________power as compared to the case of narrow band transmission.	less	high	medium	All the above
Chipping frequencies are coded distinctly for different__________station	wired	wireless	MS	BS
___________methods are used for enabling multiple access to the medium	modulation	multiplexing	MAC	CDMA
In____________techniques for a large number of channels and terminals accessing the medium at the same time using the same frequency band.	DSSS	FDMA	TDMA	CDMA
In which the data packet arrival follows a Poisson distribution.	Classical aloha	Slotted aloha	CSMA	DAMA
Assigning different slots for uplink and downlink using the same frequency is called	TDD	FDD	EY-NMPA	P-Persistant
Which is an explicit reservation scheme	DAMA	PRMA	CSMA	Polling
Round-Robin scheme is example for	Fixed TDM	Reservation TDMA	Slotted aloha	PRMA
With MACA A does not start its transmission at once but sends a___________	CTS	ACK	RTS	NAK

Fixed pattern that still allows some random access is exhibited by	Fixed TDM	Reservation TDMA	Slotted aloha	PRMA

UNIT-III

QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWERS
________________within radio coveragenodes can communicate with out further restriction.	Flexibility	Planning	Design	Robustness	Flexibility
A 32 bit_________________ is used to protect the frame as its common practice in all 802.x networks.	Checksum	Arbitary data	Design	Sequence number	Checksum
The MAC frame contains ______________.	Frame control	Planning	Design	Arbitary data	Arbitary data
The____________field determines the function of the frame:management(=00)control(=01)or data(=10).	Type	Sequence number	Arbitary data	Design	Type
______________field indicates the mode of a station after sucessful transmission of a frame.	Type	Power management	Design	Arbitary data	Power management
A_______________contains a timestamp and other management information used for power management and roaming.	Wep	Beacon	Design	Arbitary data	Beacon
__________________ allowing terminals and software from different vendors to communicate with networks from different providers.	Interoperable	Scalable	Reliable	None of the above	Scalable
The basis of transmission of data is formed by different ______________	Bearer Services	Data Services	Application Services	Network service	Bearer Services

__________ does not specify bearer services, but uses existing data services and will integrate further services	WAP	WDP	WCMP	WCSP	WAP
The ____________ is the common interface to be used by higher layers independent of the underlying network.	WTLS	T-SAP	WAE	W-SAP	T-SAP
The _____________ operates on top of many different bearer services capable of carrying data.	WAP	WDP	WTP	None of the above	WDP
The _____________ service primitive indicates the reception of data.	T-DUnitdata.ind	T-DError.ind	T-Dinvoke.ind	T-Dinvoke.exe	T-DUnitdata.ind
The _________________ Provides error handling mechanism for WDP.	Wireless Control Message Protocol	Wireless Transaction protocol	Wireless Application protocol	Wireless Application System	Wireless Control Message Protocol
The first Step in WTLS is to initiate the session with the ____________ Primitive.	SEC_ Connect	SEC_ Create	SEC_ Commit	SEC_direct	SEC_ Create
___________ offers an unreliable transaction service without a result message.	WTP class 0	WTP class 1	WTP class 2	WTP class -4	WTP class 0
The responder signals the incoming invoke PDU via the ______________ primitive to the higher layer and acknowledges automatically without user intervention.	TR-Invoke.ind	TR-Invoke.res	TR-Invoke.req	TR-Invoke.res.req	TR-Invoke.ind
The ____________ has been designed to operate on top of the datagram service WDP or the transaction service WTP.	Wireless Session Management	Wireless Session Protocol.	Wireless Session Control.	Wireless Session System.	Wireless Session Protocol.
A Wide range of mobile telecommunication technologies have been adopted and integrated into the ______________________.	Wireless Application Environment	Wireless Telephony application	Wireless Control Message Application.	None of the above	Wireless Application Environment

Decoders in a ______________ now translate this encoded request into a standard request as understood by the origin servers.	Gateway	Router	Client	drive	Gateway
The ______________ provides many functions to handle telephony events.	Wireless Telephony application interface.	Wireless identity module.	Wireless transport layer Security.	None of the above	Wireless Telephony application interface.
The _______________ library contains functions to set up, accept, and release calls.	Call control	Network text	Phone book	Call text	Call control
The ______________ can also access a URI via the WTA server. In this case, the URI plus content was not stored in the repository.	User agent	Server	Gateway	Client	Server
The Repository represents a ________________ on the client for content required to offer WTA services.	Persistent Storage	Permanent Storage	Partial Storage	Temporary Storage	Persistent Storage
The ________________ controls communication between PI and PPG.	Push access Protocol	Push over the air Protocol	Pull access Protocol	None of the above	Push access Protocol
___________is the common interface to be used by higher layers independent of the network .	T-SAP	SEC-SAP	TR-SAP	WSP	T-SAP
Setting up a secure connection between two peers ,user data can be exchanged using a primitive ___________	SAP-unit data	SEC-unit data	TR-unit data	WSP-unit dat	SEC-unit data
Two types of acknowledgements _______and______acknowledgements.	user,update	abort ,result	user,automatic	request ,response.	user,automatic
The peer also issues SEC-Exchange primitives,which requests a ___________from the originator.	Client Certificate	compression certificate	cipher certificate	commit certificate	compression certificate
The Originator now answers with its certificate and issues a___________primitive.	SAP-commit.req	SEC-result.cnf	SAP-invoke.req	SEC-commit.req.	SEC-commit.req.

It is quite clear that due to computing power on the handled devices the___________provided cant be very strong.	Encryption	Decryption	Compression	decompression.	Encryption
___________follows a deck and card method.	WAE	WML	WSP	WSP/B	WML
WSP/B uses three classes of WTO are___________	class 0,1,2	class 1,2,3	class1,2,0	class 0,1,3	class 0,1,2
If any errors happen when WDP datagrams are sent from one entity to another the___________provides error handling mechanisms for WDP.	WCMP	WDP	WSP	WAE	WCMP
WTLS provides a different levels of security and has been optimized for ___________bearer networks.	low BW ,low density	low BW ,high density	high BW ,high density	none	low BW ,high density
Which is not a component of WAP___________	Wireless datagram protocol(WDP)	wireless application environment(WAE)	wireless session protocol(WSP)	wireless security protocol(WSP)	wireless security protocol(WSP)
The _________primitive is used to request that an operation is executed by the server in WSP.	S-Method PDU	S-MethodResult	S-MethodInvoke	S-MethodRequest	S-MethodInvoke
The call control, network text, phonebook services are associated mainly with _________	public services	common network services	network specific services	private services	common network services
The client is connected via a mobile network with a _________other telephone networks and a _________	WTA server, WAP gateway	WTA gateway, WAP server	WAP server, WAP gateway	WTA server, WTA gateway	WTA server, WAP gateway
One difference between WTA servers and other servers besides security is the tighter control of …………………	Certifications	Integrity	Acknowledgement	Quality of service	Quality of service
Infrared trmission having ______ bandwidth compared to other LAN Technologies.	Low	High	Medium	None of the above	Low
IEEE 802.11 Supports_____ different physical layer.	Four	Three	Five	Six	Three

____ is a spread spectrum technique which allows for the co- existence of multiple networks in the same area.	a.FHSS	b.DSSS	c.DHSS	d.FSSS	a.FHSS
The physical layer convergence protocol preamble starts with ______bit synchronization.	32	48	80	64	80
________ Mechanisms are also called distributed foundation wireless medium access control.	SAC	MAC	IR	Radio trmission	MAC
SIFS stands for _______________.	Simple inter frame spacing	Short inter frame spacing	Slow inter frame spacing	Single inter frame spacing	Short inter frame spacing
MIB stands for ___________	Managemen t information base	Management interface base	Management intermediate base	Managemen t interference base	Management information base
___________ scanning simply me listening into the medium to find other networks.	Active	Passive	Sensitive	Insensitive	Passive
_________ scanning comprises sending a probe on each channel and waiting for a response.	Active	Passive	Sensitive	Insensitive	Active
Like IEEE 802.11b, Bluetooth operates in the _______ ISM band.	2.3 GHZ	5 GHZ	2 GHZ	2.4 GHZ	2.4 GHZ
___________ provides a fixed point to point connection with up to 155 Mbit/s.	HIPERLINK	HIPERLAN1	HIPERLAN2	HIPERACCES S	HIPERLINK
In Bluetooth technology all the active devices are assigned a________ active member address.	4	8	3	6	3
Each piconet has a________ hopping pattern.	Unique	Different	Equal	Medium	Unique
________ support the association of a station to an access point and roaming between different access points.	MAC Managemen t	PHY Management	Station Management	Control Managemen t	MAC Management

__________ is the alternative spread spectrum method separating by code and not frequency.	DHSS	FHSS	FSSS	DSSS	DSSS
The length of the long trport channel is _________bytes.	54	9	27	15	54
The ________ in the access point splits the access time into super frame periods.	Point coordinator	Point controller	Sequence coordinator	Sequence controller	Point coordinator
The _________Service primitive indicates the reception of data.	Tdes-unit.ind	T-Dunitdata.ind	Tsorceunit.ind	T-Derror.ind	T-Dunitdata.ind
Wireless transport layer security (WTLS) supports datagram and _________transport layer protocols.	A.connection-less	connection-oriented	levels of security	request/reply	connection-oriented
WTP transfers the _________to server S-SAP where an S-Connect.ind primitive indicates a new session.	connreply PDU	connect PDU	post PDU	Resume PDU	connect PDU

UNIT-IV

QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWERS
_______ layer is used for networking through a chain of in-between routers	Physical	L2	L3	Application layer	L3
_______ defines how the data from the port is to be presented of formatted	Transport layer	Session layer	Application layer	Presentation layer	Presentation layer
Communication between two address on a physical network is carried out through _________	Routers	Bridges	Repeaters	IP	Routers
When a message or a packet is transmitted to one designated IP	Broadcst	Multicast	Unicast	Packet switching	Unicast

address then it is called __________					
When a message or packet is transmitted to a group of IP address then the message or packet is said to be _______	Podcast	Multicast	Unicast	Point to point	Multicast
A_________ is stateless meaning that a datagram is not a sequential successor of a previous one or a predecessor of the next.	Protocol	Datagram	Data	UDP	Datagram
________ is one such protocol used to send the datagram using a connectionless protocol	TCP	IP	ICMP	UDP	UDP
__________ is another connectionless protocol which is a part of the IP network protocol suite	TCP/IP	UDP	MOBILE IP	ICMP	ICMP
The use of the existing IP protocol by a large number of MNs will lead to ________in the network throughput	increase	decrease	change	stability	decrease
Routing of packets through the routers is performed when an______ moves within one paging area	HA	HLR	MN	VLR	MN

_______transmit a message for connection establishment or a packet using the IP protocol	MN	CN	IP	TCP/IP	CN
When visiting a foreign network a mobile node must discover a __________	home agent	foreign agent	mobile node	correspondent node	foreign agent
What is COA	care of address	corresponding address	co-address	collocating address	care of address
__________ is a method by which an MN visits a network and discovers the FA and the COA	Agent discovery	Agent Advertisement	Agent Solicitation	Location Management	Agent Solicitation
_________ is a term used to specify a data stream between two connected ends	COA	Lifetime	Pipe	Tunnel	Pipe
The data stream is inserted from one end and is retrieved as________ from other end	LIFO	FIFO	32 bit word	Set of words	FIFO
Packets received at the HA are transmitted through ________after encapsulation.	Pipe	Registration	Tunnel	Router	Tunnel
The FA reads the first _________words in ME	6	7	5	9	5
The _________word in the sixth item is changed and specifies the CN IP address in case the flag bit is set to	7	7	9	10	10

The advantage of reverse tunneling is multicasting by using __________	Unidirectional	Point to point	Bidirectional	GRE	Bidirectional
Bi-directional tunneling refers to tunneling from ____________	HA to FA	FA to HA	HA to MN	MN to HA	HA to FA
______ defines the number of attempts to hop before the expiry of packets at the network	GRE	Tunneling	Time to live	COA	Time to live
______COA is obtained by the DHCP	Co-located	Bi-located	Home agent	Foreign agent	Co-located
The tunnel does not need an extra _______, though it has fixed source and destination end points	time	COA	Hop	DHCP	Hop
______is a process of recovering the original packet from A after using the header	DHCP	Encapsulation	Decapsulation	Agent discovery	Decapsulation
______ is a process in which a computing system receives the packets on the internet in which it uses new protocol	DHCP	Encapsulation	Decapsulation	Agent discovery	Encapsulation
________ is an agent presented either at an interconnected hosts or at a router of packets on the internet	Agent	Home agent	Foreign agent	COA	Foreign agent

________ is an agent either at an interconnected host or presented at a router of packets on the internet	Agent	Home agent	Foreign agent	COA	Home agent
________ is a network providing services to a mobile terminal equipment and having a MSC	Home agent	Foreign agent	Home network	Foreign network	Home network
_________ is an address of 32 bits assigned to a node such that IP packets can be transmitted or received by the node on the internet	home address	foreign address	IP address	Source address	IP address
________ is a set of 32 bit words transmitted along with a packet after appending them as per the IP protocol	Source	Destination	IP address	IP header	IP header
________ are interconnected through the routers and the subnets on the internet using the IP protocol	IP nodes	Home nodes	Foreign node	Nodes	IP nodes
A part of data is called_______ which consists of a maximum of 216 bytes	IP node	IP header	Packet	IP address	Packet
A _______ binding created for providing mobility to a mobile node after registration at a foreign	Agent	Mobility	Network	Source	Mobility
After the de-registering, the mobile node receives the IP packets which reach	Encapsulation	Tunneling	Decapsulation	Binding	Tunneling

the home agent by_______ to the new agent					
While routing, the routers use _________ bits only for the routing addresses of other routers for the next hop	8,16,24	7,14,21	24,16,8	32	8,16,24
_______ is required for advertisement	Routing	Flooding	Subnets	Protocols	Flooding
When a packet is transmitted to all the IP addresses which are set for listening and this type of transmission is called as________	Unicasting	Multicasting	Broadcasting	Flooding	Broadcasting
The problem with the use of IP protocol is that of ________in the routing table	Transparency	Non-transparency	Both	None of the above	Non-transparency
A home network is a mobile radio subsystems network within an area known as ___________ area	Home	Foreign	Paging	Routing	Paging
When DHCP server confirms the binding through a message it sends __________	DHCPOFFER	DHCPDISCOVER	DHCPACK	None of these	DHCPOFFER
A router table is regularly___________	changed	deleted	added	updated	updated
Each router has a ________bit IP address	8	16	24	32	32

From the source computer the packet is transmitted to a source router using __________	ARP	Router	Subnet	RARP	RARP
________has a home agent for a set of home networked MNs as well as a foreign agent for the visiting MNs	Mobile IP	ICMP	Router	Mobile node	Router
______routing is a method in which the source of a packet provides the route information	GRE	HA	Source	FA	Source
Advantage of reverse tunneling become apparent when a ________is employed	Routing table	COA	Firewall	Duplication	Firewall
_________ filters the packets assigned to an IP address received from another IP address	Routing table	COA	Firewall	Duplication	Firewall
__________ are used by MNs to discover home and foreign agents while moving from one network area to another	Agent Advertisement	Location management	Agent discovery	Agent Solicitation	Agent Advertisement
When _________ is co-located the registration is simple	FA	HA	Mobile node	Home node	FA
________ is the mechanism of attaching a new header to the existing packet.	Tunnel	Packets	Decapsulation	Encapsulation	Encapsulation
After receiving a COA the mobile node has to register with_________	FA	HA	Home network	Foreign network	HA

The function of ________is to inform the HA the current location for forward of packets	GRE	COA	HA	Registrati on	Registration
Which is a method of encapsulation	registratio n	GRE	TTL	None of the above	GRE
A ________ is required to limit the rate at which is sends broadcast or multicast agent advertisement	Mobility agent	Foreign agent	Home agent	Agent solicitation	Mobility agent
The advantage of multicasting is that there is no________	Missing of entries	Additional entries	Reconfigurat ion	Duplicatio n	Reconfigurat ion
________ registry informs the current location of the mobile network with the help of current COA	home registry	foreign registry	home network	location	location
Domain name system is a ______which has logical name and its equivalent IP address	Directory	File	Table	Folder	Table
The mobile node informs all its partners about the change in______	IP address	Home address	Location address	Network address	IP address

UNIT-V

QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWERS
In UDP there is no ____________	Session establishment	Data flow and congestion control	Both a & b	Only a	Both a & b
A_______ is a service access point for data input and output through which a service is rendered by a node	protocol	port	data	datagram	port

The function of the transport layer is__________ the port data	Synchronize	Add	Identify	Transport	Transport
The application layer data is transmitted and received as a ________consisting of sequences	bits	bytes	stream	node	stream
Handshaking of packets is used for ____________and all transactions are sequentially acknowledged	buffering	acknowledg ement	receive	none of these	acknowled gement
The TCP transport layer delivers the segments in a _______order	Linear	Sequential	Non linear	Conventio nal	Sequential
The congestion control method for TCP over wireless is ______________	ECN	NCE	CEN	NEC	ECN
The TCP __________is used at the subsequent layers during transmission of data from ports up to the transport layer at the receiver	buffer	data streams	data ram	header	header
The sequence number field is reset to _________ in the case that there are no more octets left to transmit from the segment	1	0	Flags	Fragment s	0
The _________ field specifies the word from where the application layer data octets will begin	header	source	offset	checksum	offset
The ___________field specifies the number of bytes the sender is willing to receive	header	window size	fragment	offset	window size
Urgent field communicates an _______value to be added to get a sequence number	receiver value	sender value	offset value	data value	offset value
Data streams are delivered using a virtual connection between__________	header	source	socket	destinatio n	socket
TPDU depends on _________ presentable in a given network state	TCP	UDP	MTU	IP	MTU

The bytes that do not reach the receiver successfully within a timeout period are _________	discarded	transmitted	lost	retransmitted	retransmitted
_______ in case of no acknowledgement ensures reliable guaranteed and error free data transfer	transmission	re-transmission	Non transparent	Transparent	re-transmission
Window size is adjusted and throughput depends on_________ interval for the acknowledgment	MTU	RTT	TTR	PACK	RTT
___________shows the recovery of lost packets or data received after a delay at the TCP end	TCP tuning	PACK	DACK	ACK	DACK
One method of data flow control is to adjust the ___________ field	header	flag	fragments	window-size	window-size
During high speed data transfer________________ method is used	cumulative acknowledgement	duplicate acknowledgement	sliding window	window scaling	window scaling
The ____________ is known as exponential growth phase or slow start phase	first phase	second phase	congestion avoidance	fast recovery	first phase
Which method uses the split TCP?	Indirect TCP	Selective repeat TCP	Mobile-end TCP	All the above	All the above
The word snoop means secretly looking into or _____________ something	examining	calculating	analyzing	reporting	examining
Indirect TCP suggests splitting of the TCP layer into __________ TCP sub-layers	one	two	five	four	two
A modification of the indirect TCP is the ___________ repeat protocol	split	selective	socket	modified	selective
The MN has a mechanism for retransmission in case of a request from the____________	MN	BTS	Protocol	Agent	Agent
The TCP split is _______________	symmetric	asymmetric	two layers	sub layers	asymmetric

The FRR phase stes in after _____________ DACKS	one	two	three	four	three
The advantage of TCP Reno ____________ the window size after fast retransmission sets the larger RTT	increase	decrease	modifies	recovers	increase
Timeout freezing of transmission is also used in situations whose the MN faces long durations of______________	connection	disconnection	transmission	retransmission	disconnection
The advantage of selective retransmission is that it is very ___________as only the lost bytes from a sequence number are retransmitted	difficult	efficient	robust	portable	efficient
________ on the packets help in taking into account whether the delays are due to the propagation path	Transmission	Data rates	Timestamp	FEC	Timestamp
An ________ has the utility programs	TCP	UDP	OS	System	OS
A _____________ is a program unit which runs when scheduled to do by OS and each state is controlled by OS	software	file manager	process	application	process
A ____________ is an application process which runs according to its schedule set by the OS	Task	Process	Program	Message	Task
A___________ is an application process or process unit which runs and controlled by OS as a light weight process	Task	Process	Program	Thread	Thread
An___________ is a program unit which runs when a hardware or software event occurs	Task	ISR	IIR	Process	ISR
A software even can be ____________ or illegal operation code provided to CPU	Detection	Condition	Peripheral	Exception	Exception

__________ is a unit of memory which can load from a program stored in a hard drive or from any other storage device	Task	Thread	Process	Page	Page
A __________ table is used for address mapping	Schedule	Exception	Page	Address	Page
The query development support platform __________is written using HTML and ported at Palm device	PQA	PAQ	AQP	APQ	PQA
The mobile OS enables the programmer to __________the devices.	Abstract	Encapsulat e	Close	Connect	Abstract
The OS provides the functions used for scheduling the multiple task in a system carried out through______________	files	process	tokens	threads	tokens
Palm OS assumes that there is a ______________memory card	5GB	256GB	256MB	5MB	256MB
Palm OS file manager manages each file as a ____________which has multiple records and information fields	Table	Record	Databas e	All the above	Database
PalmOS uses _______net library for internet connectivity	HTTP/HTTPS	TCP/IP	UDP	IrDA	HTTP/HTT PS
A __________ has digitization software which converts analog signals to digital ones	smart phones	pocket Pc	Embedd ed system	Phone pad	pocket Pc
The windows mobile microsoft___________platform is an open platform	java	VB	.Net	C++	.Net
Windows CE ___________manages data as a database or object file	file manager	storage memory	program memory	cache	file manager
Highest priority level means___________ priority	idle	time critical	latency	thread	time critical
Symbion based devices use _____________ synchronization	SyncML	MD5	RSA	ARM	SyncML

__________ is a association which promotes linux and develops standards in embedded system	ELC	LEC	ECL	CEL	ELC
__________memory associated with the memory addresses for the LCD ,printer, keyboard and serial port	File	Storage	Buffer	Flash	Buffer
__________ is a mechanism is which a process or thread is to provide a wait object to a higher priority process	paging	swapping	priority inheritan ce	none of these	priority inheritance
Real time is a ____________ once set and then used for synchronization of all process and threads	system time	paging time	applicati on time	active time	system time
The user gets a personal computer like feel and windows like GUI when using a__________device	Windows CE	Palm OS	Linux	Pocket PC	Windows CE
_____________ is divided into two sublayers	page	OS	Code	Kernel	Kernel
___________ consisting of source code and network abstraction sublayer	page	OS	Code	Kernel	Kernel
The Windows CE kernel is ____________ from the kernel of windows 98,2000 and developed versions of windows	same	different	compact	optimized	different
Application development means defining additional events and coding for the corresponding ____________	File	Table	Process	Handler	Handler