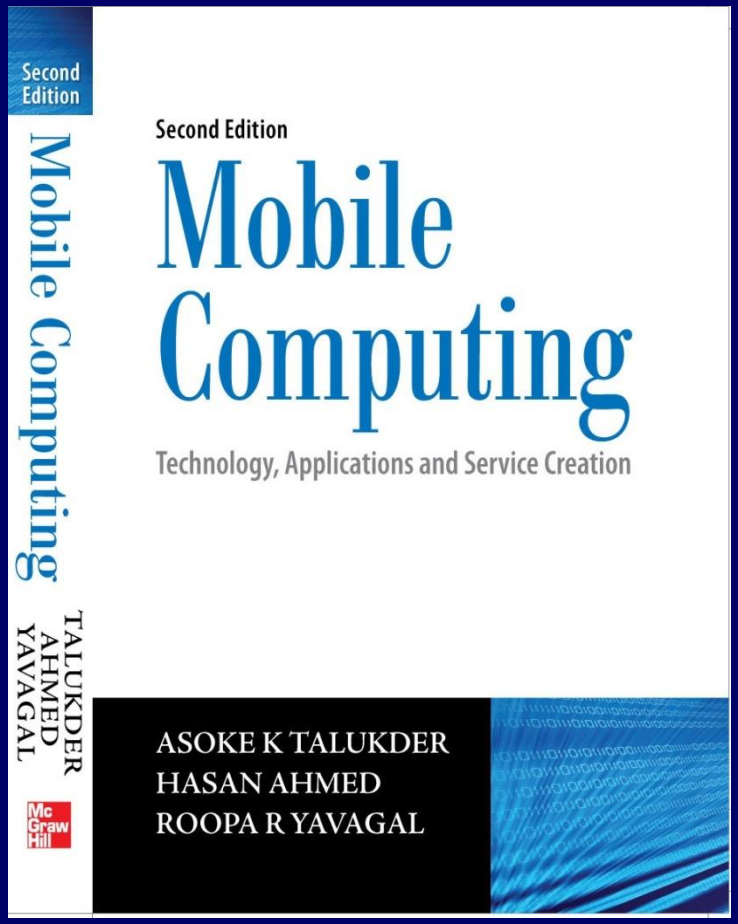


Mobile Computing

Chapter 7

GPRS

Asoke K Talukder

Hasan Ahmed

GPRS

- General Packet Radio Service
- Step to efficiently transport high-speed data over the current GSM and TDMA-based wireless network infrastructures
- Deployment of GPRS networks allows a variety of new applications ranging from mobile e-commerce to mobile corporate VPN access
- GPRS allows for data speeds of 14.4 KBps to 171.2 KBps, which allow for comfortable Internet access
- Allows for short ‘bursty’ traffic, such as e-mail and web browsing, as well as large volumes of data

GPRS

- No dial-up modem connection is necessary
- Offers fast connection set-up mechanism to offer a perception of being ‘always on’ or ‘always connected’
- Immediacy is one of the prime advantages of GPRS

QoS in GPRS

- Allows definition of QoS profiles using the parameters of service precedence, reliability, delay and throughput
- Service precedence is the priority of a service in relation to another service which can be either high, normal or low
- Reliability indicates the transmission characteristics required by an application and guarantees certain maximum values for the probability of loss, duplication, mis-sequencing and corruption of packets
- Delay parameters define maximum values for the mean delay
- Throughput specifies the maximum/peak bit rate and the mean bit rate

GPRS Network Architecture

- GPRS uses the GSM architecture for voice
- To offer packet data services through GPRS, a new class of network nodes called GPRS support nodes (GSN) are introduced
- GSNs are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN)
- Two main GSNs are Serving GSN (SGSN) and Gateway GSN (GGSN)

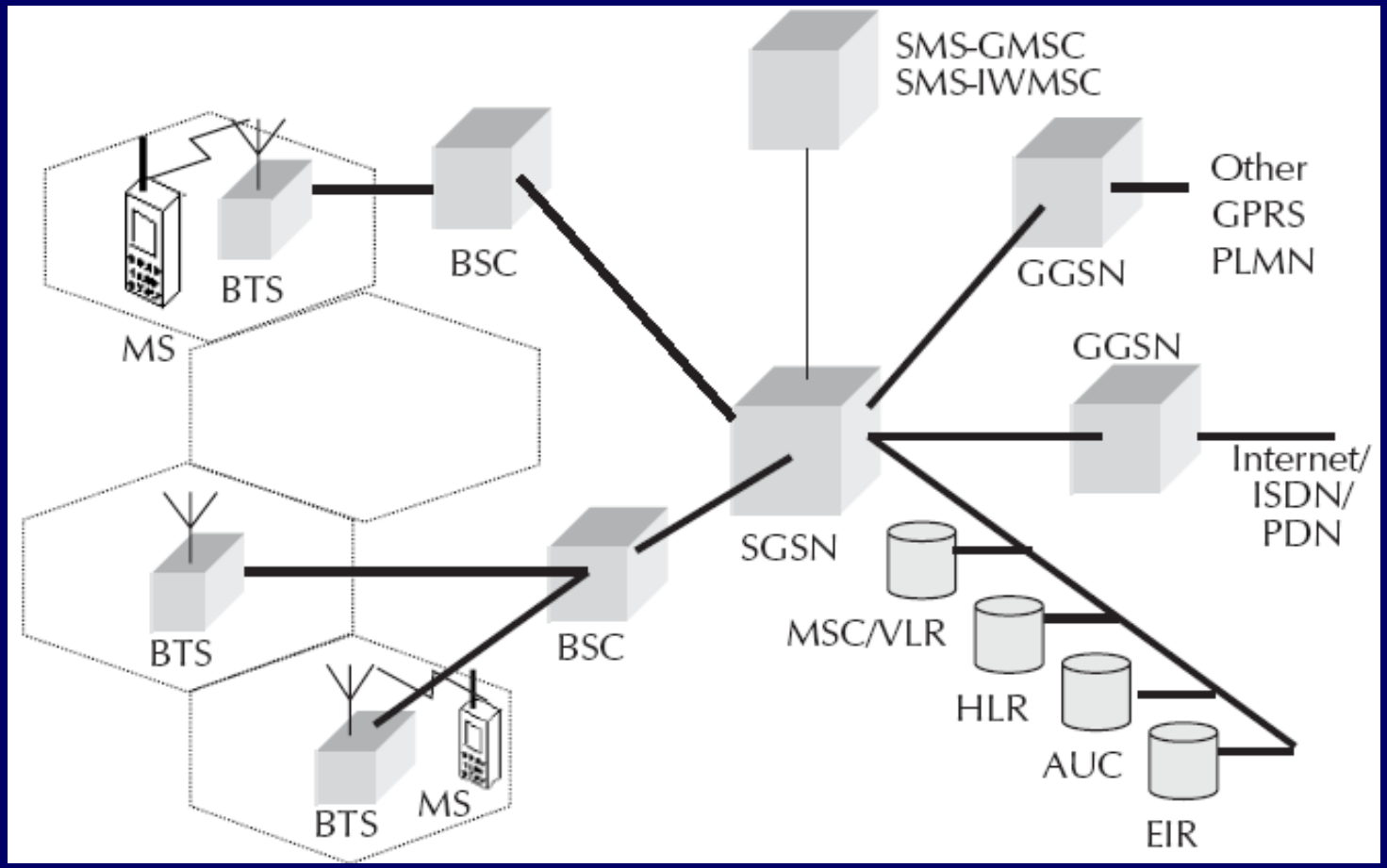
SGSN

- SGSN is at the same hierarchical level as the MSC and so, whatever MSC does for voice, SGSN does for packet data
- SGSN's tasks include packet switching, routing and transfer, mobility management, logical link management, authentication and charging functions
- SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area
- Location register of the SGSN stores location information (like current cell, current VLR, etc.) and user profiles of all GPRS users registered with this SGSN
- SGSN sends queries to HLR to obtain profile data of GPRS subscribers

GGSN

- GGSN acts as an interface between the GPRS backbone network and the external packet data networks and functions like a router in a LAN
- GGSN maintains routing information that is necessary to tunnel Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations
- GGSNs convert the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like Internet or X.25
- GGSN stores the current SGSN address of the user and user's profile in its location register while performing authentication and charging functions related to data transfer

GPRS System Architecture



GPRS Network Enhancements

- Base Station System (BSS) needs enhancement to recognize and send packet data and this includes BTS upgrade to allow transportation of user data to the SGSN. BTS, too, needs to be upgraded to support packet data transportation between BTS and MS (mobile station).
- HLR needs enhancement to register GPRS user profiles and respond to queries originating from GSNs regarding these profiles.
- MS (mobile station) for GPRS is different from that of GSM.
- SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN.

Attachment and Detachment in GPRS

- MS registers itself with SGSN of GPRS network through a GPRS attach which establishes a logical link between the MS and the SGSN.
- Network checks if MS is authorized to use the services; if so, it copies the user profile from HLR to SGSN and assigns a Packet Temporary Mobile Subscriber Identity (P-TMSI) to the MS.
- To exchange data packets with external PDNs after a successful GPRS attach, an MS must apply for an address which is called PDP (Packet Data Protocol) address.
- For each session, a PDP context is created which contains PDP type (e.g. IPv4), PDP address assigned to the mobile station (e.g. 129.187.222.10), requested QoS and address of the GGSN that will function as an access point to the PDN.

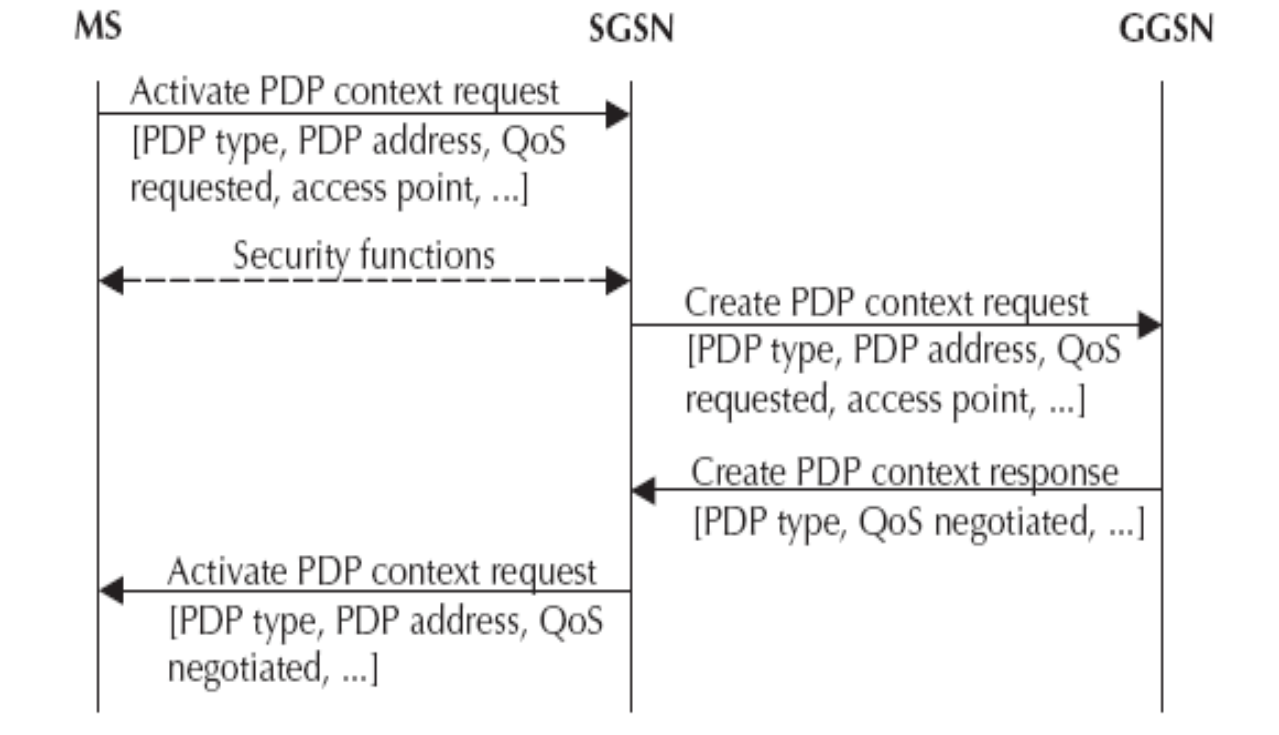
Attachment and Detachment in GPRS

- Such a context is stored in MS, SGSN and GGSN while with an active PDP context, the MS is ‘visible’ to the external PDN.
- A user may have several simultaneous PDP contexts active at a given time and user data is transferred transparently between MS and external data networks trough GTP encapsulation and tunneling.
- Allocation of the PDP address can be static or dynamic.
- In case of static address, the network operator permanently assigns a PDP address to the user while in other case, a PDP address is assigned to the user upon the activation of a PDP context.

PDP Context Activation

- Using the message ‘activate PDP context request’, MS informs the SGSN about the requested PDP context and if request is for dynamic PDP address assignment, the parameter PDP address will be left empty.
- After necessary security steps, if authentication is successful, SGSN will send a ‘create PDP context request’ message to the GGSN, the result of which is a confirmation message ‘create PDP context response’ from the GGSN to the SGSN, which contains the PDP address.
- SGSN updates its PDP context table and confirms the activation of the new PDP context to the MS.
- Disconnection from the GPRS network is called GPRS detach in which all the resources are released.

PDP Context Activation



Mobility Management

- Mobility Management functions are used to track its location within each PLMN in which SGSNs communicate with each other to update the MS's location in the relevant registers.
- Profiles of MSs are preserved in VLRs that are accessible to SGSNs via the local MSC.
- A logical link is established and maintained between the MS and the SGSN at each PLMN.
- At the end of transmission or when a mobile station moves out of area of a specific SGSN, the logical link is released and the resources associated with it can be reallocated.

Routing

- Routing is the process of how packets are routed in GPRS.
- Here, the example assumes two intra-PLMN backbone networks of different PLMNs. Intra-PLMN backbone networks connect GSNs of the same PLMN or the same network operator.
- These intra-PLMN networks are connected with an inter-PLMN backbone while an inter-PLMN backbone network connects GSNs of different PLMNs and operators. However, a roaming agreement is necessary between two GPRS network providers.
- Gateways between PLMNs and external inter-PLMN backbone are called border gateways which perform security functions to protect the private intra-PLMN backbones against malicious attacks.

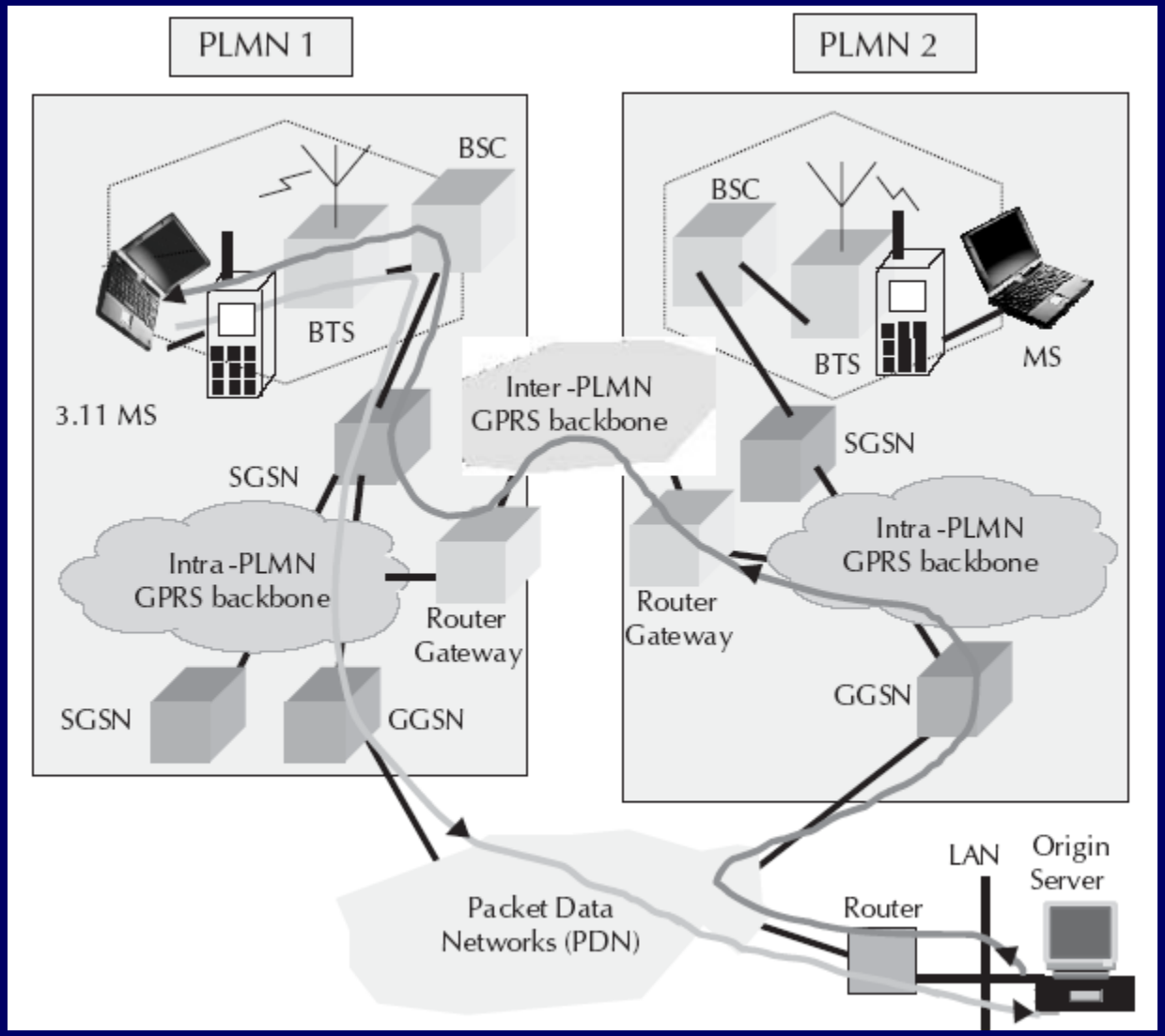
Routing

- Let's say that GPRS MS located in PLMN1 sends IP packets to a host connected to the IP network (e.g. to a Web server connected to the Internet).
- SGSN that the MS is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN.
- GGSN de-encapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network and finally, delivers the IP packets to the host.

Routing

- Let us also say that home-PLMN of the mobile station is PLMN2.
- An IP address has been assigned to MS by the GGSN of PLMN2 and so, MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2.
- Correspondent host is now sending IP packets to the MS onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1.
- It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1 while the SGSN de-encapsulates the packets and delivers them to the MS.

Routing


PLMN 1
PLMN 2
BSC
BTS
3.11 MS
SGSN
Intra -PLMN
GPRS backbone
Router
Gateway
SGSN
GGSN
Inter -PLMN
GPRS backbone
BSC
BTS
MS
SGSN
Intra -PLMN
GPRS backbone
Router
Gateway
GGSN
LAN
Origin
Server
Router
Packet Data
Networks (PDN)

Routing

- HLR stores the user profile, the current SGSN address and the PDP addresses for every GPRS user in the PLMN.
- When the MS registers with a new SGSN, HLR will send the user profile to the new SGSN.
- Signaling path between GGSN and HLR may be used by the GGSN to query a user's location and profile in order to update its location register.

Data Services in GPRS

- Any user is likely to use either of the two modes of the GPRS network: application mode or tunneling mode.
- In application mode, user uses the GPRS mobile phone to access the applications running on the phone itself. The phone here acts as the end user device.
- In tunneling mode, user uses GPRS interface as an access to the network as the end user device would be a large footprint device like laptop computer or a small footprint device like PDA. The mobile phone will be connected to the device and used as a modem to access the wireless data network.

Bearers in GPRS

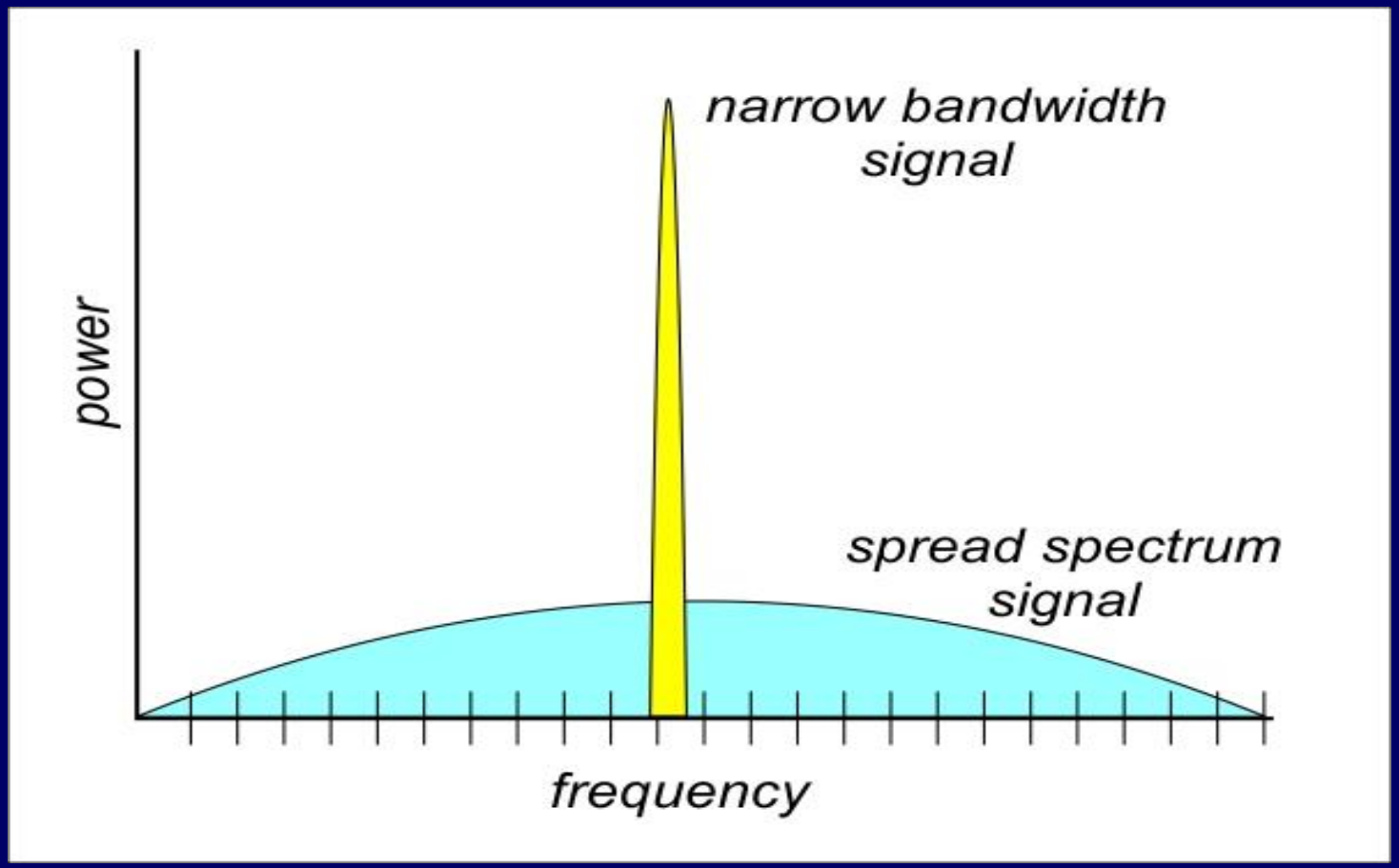
- Bearer services of GPRS offer end-to-end packet switched data transfer.
- GPRS supports two different kinds of data transport services: point-to-point (PTP) services and point-to-multipoint (PTM) services.
- GPRS continues to support SMS as a bearer.
- Wireless Application Protocol is a data bearer service over HTTP protocol, supported by GPRS.
- Multimedia Messaging Service, too, is supported by GPRS.

Applications of GPRS

- Chat
- Multimedia Services
- Virtual Private Network
- Personal Information Management
- Job Sheet Dispatch
- Unified Messaging
- Vehicle Positioning
- Location based services

CDMA AND 3G

- Conventional transmission system
- The information is modulated with a carrier signal and then transmitted through a medium
- All the power of the signal is transmitted centered around a particular frequency
- This frequency represents a specific channel
- Has a very narrow band


narrow bandwidth
signal
power
spread spectrum
signal
frequency

Spread Spectrum

- Transmission power is spread over the complete band
- Transmission signal bandwidth is much higher than the information bandwidth
- Does not attempt to allocate disjoint frequency or time slot resources
- There are numerous ways to cause a carrier to spread

- All spread spectrum systems can be viewed as two steps modulation process
  - Data to be transmitted is modulated
  - Carrier is modulated by the spreading code, causing it to spread out over a large bandwidth

IS 95(cdmaOne)

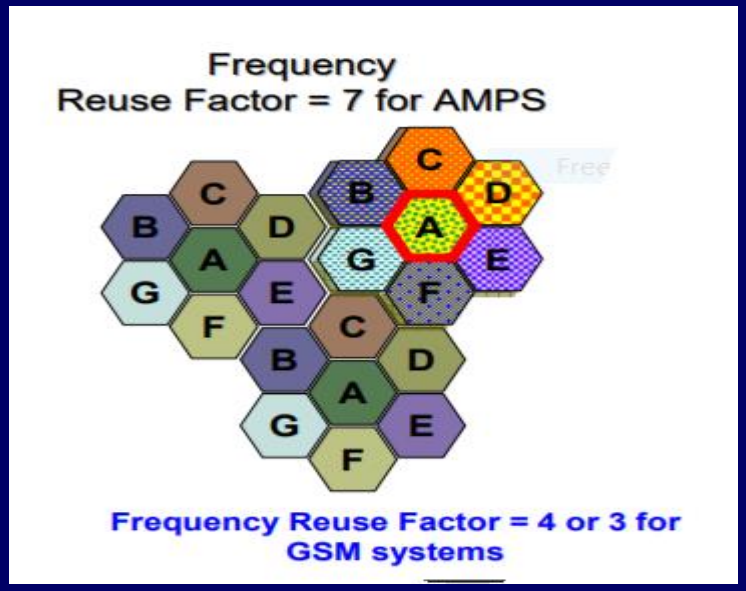
- 2G digital cellular standard
- Qualcomm developed first commercial spread spectrum based system for use in the cellular band
- Considered as an alternative to analogue FDMA technologies(AMPS) and TDMA systems(IS-54,GSM)
- Formed the basis for first CDMA systems
- Enhanced version:IS-95B
- Family of IS-95 standard is known as cdmaOne

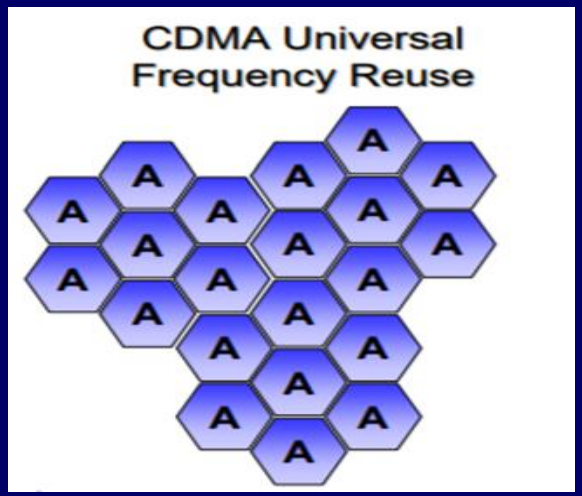
IS-95 System Features

- Digital Voice
- Uses Frequency Division Duplex(FDD): 824 to 849MHz for forward link(BS to MS) and 869 to 894MHz for reverse link(MS to BS)
- Uses a different modulation and spreading techniques for forward and reverse link
- Soft Handoff possible

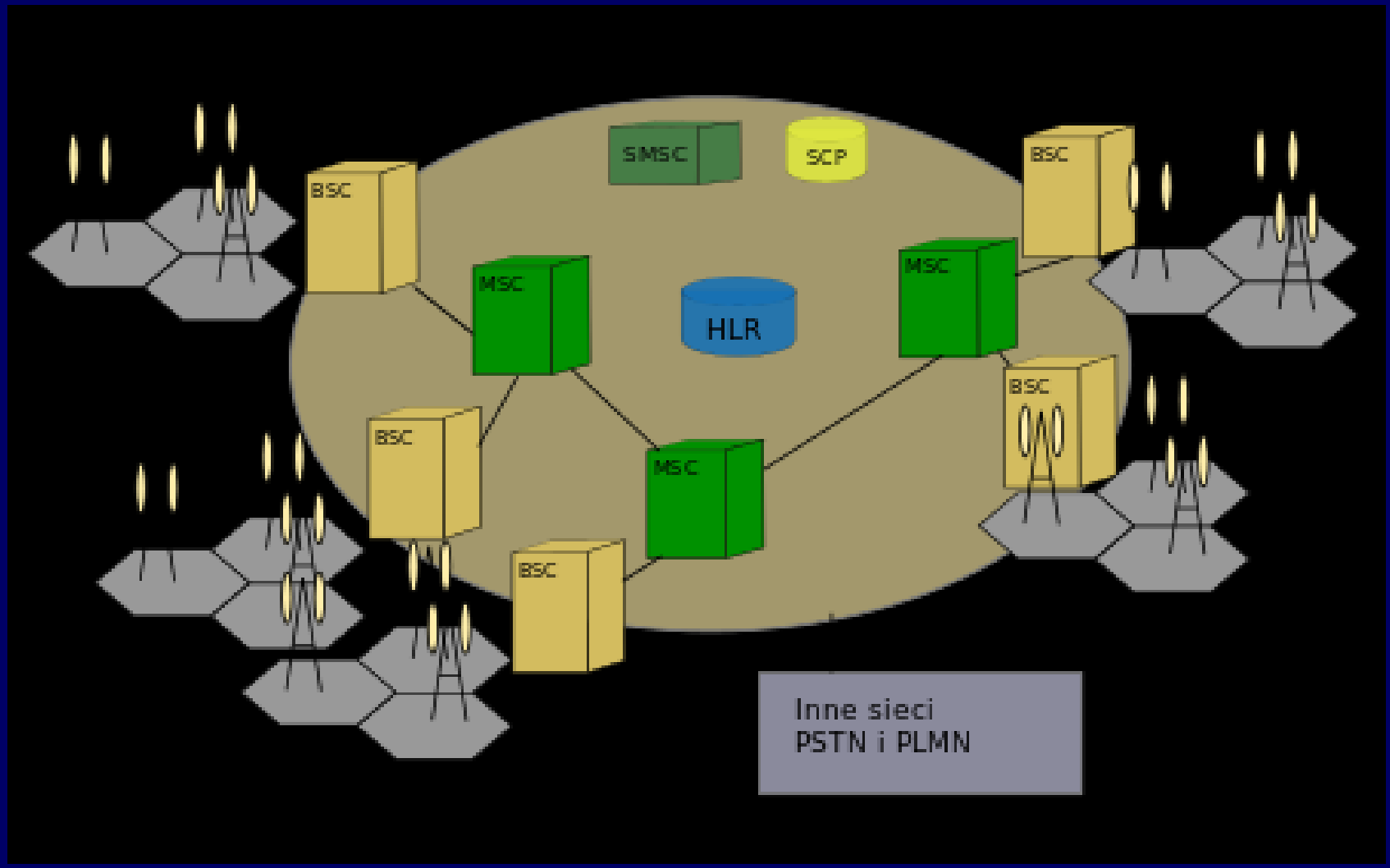
- Uses CDMA
  - Multiple users share a 1.25 MHz channel by using orthogonal spreading codes (Walsh codes)
- Traffic Channel
  - Several users share a radio channel separated by a code not a timeslot or frequency
  - Receiver performs a time correlation operation to detect only desired codeword
  - All other codewords appear as noise due to decorrelation
  - Receiver needs to know only codeword and frequency used by transmitter
  - Adjust power often to prevent near –far problem

- Universal frequency reuse (frequency reuse cluster size K =1)
- All cells in the same area can employ the same spectral band, because the various signals are sorted out by the spread spectrum process rather than by frequency discrimination





IS 95 architecture



Handoff

- Handover in GSM
- When a subscriber moves away from a base station, the signal power reduces resulting in a potential drop in connection
- To ensure that the call does not break, some other base station closer to the mobile station needs to attach the mobile to it and let the call to continue without any interruption

- The spectrum is spread and everybody gets the same signal
- Logically, a MS is always connected to different base stations at the same time
- Handoff is managed by changing the attachment

Types of handoffs in CDMA

- Soft handoff
  - Intercell handoffs
  - Mobile keeps two radio links during the process
  - Make before break
- Hard handoff
  - Interfrequency handoff
  - Mobile drops original link before establishing new link
- Softer handoff
  - Mobile communicates with two sectors of the same cell
  - Signals from multiple sectors are combined instead of switching from one sector to another

	GSM	IS-95
Technology	TDMA, FDMA	CDMA
Channel Bandwidth	Total 25MHz bandwidth with 200 KHz per channels, 8 timeslots per channels with frequency hopping	Total 12 MHz with 1.25 MHz for the spread spectrum
SMS	160 characters of text support	120 characters
SIM Card	Yes	No
Handoff	Hard	Soft
System Capacity	Fixed and limited	Flexible and higher than GSM

Third Generation Networks(3G)

- Upgrade for 2G and 2.5G GPRS networks for faster internet speed
- Use services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union(ITU)
- Offer plethora of services – voice, multimedia, video calls and conferencing, high speed data etc, maps, TV streaming etc

- First major step in the evolution to 3G- introduction of GPRS(2.5G)
  - Offered moderate data bandwidth sufficient for MMS, WAP services, low bandwidth internet
- GPRS evolved into Enhanced Data rates for GSM Evolution(EDGE-2.75G)
  - Offered high bandwidth packet data capable of multimedia video

International Mobile Telecommunications-2000 (IMT-2000)

- Global standard for 3G wireless communications defined by set of ITU recommendations
- Provides a framework for worldwide access of services by linking the diverse systems
- Services advertised as 3G are required to meet IMT-2000 technical standards, including standards for reliability and speed (data transfer rates)
- To meet the IMT-2000 standards, a system is required to provide peak data rates of at least 200 kbit/s (about 0.2 Mbit/s)

- Includes standards:
  - EDGE
  - CDMA 2000
  - UMTS
  - DECT
  - WIMAX

- Evolutionary
  - Backward compatible to interoperate with preexisting 2G networks
- Revolutionary
  - Require all new networks and frequency allocation

CDMA-2000

- Developed by 3GPP2 as a backwards-compatible successor to second-generation cdmaOne (IS-95) set of standards
- Uses CDMA technology as its underlying modulation technology
- Addresses IMT-2000 specification for indoor, indoor to outdoor, pedestrian and vehicular environment
- Used especially in North America and South Korea

- Data services provided by CDMA 2000
- Packet data
  - Internet browsing or mails
- High speed circuit switched data
  - Video applications

Phased development of CDMA 2000

- Phase 1(CDMA 1x)
  - Employs 1.25MHz of frequency bandwidth
  - Delivers a peak data rate of 144Kbps for stationary or mobile applications
- Phase 2(CDMA 3x)
  - Employs 5MHz of frequency bandwidth
  - Data rate upto 2Mbps

UMTS/WCDMA

- Some of the encoding techniques are patented by Qualcomm
- To avoid copyright issues, a different flavour of CDMA was devised-Wideband CDMA(WCDMA)
- Universal Mobile Telecommunication Systems (UMTS) is the 3G successor to the GSM family of standards including GPRS and EDGE
- UMTS uses WCDMCA(WCDMA is the air interface technology being used in UMTS networks)

- Also known as UTRAN(UMTS Terrestrial Radio Access Network)
- Uses direct sequence spread spectrum modulation
- Channel bandwidth:5MHz
- Wider bandwidth results in higher data rates
- Two modes of operation: FDD and TDD

Fixed wireless 3G

- 3G specification includes the fixed wireless as well
- Useful in Geographies where wired infrastructure is inadequate
- Business and home networking

Applications

- Virtual Home Environment
- Environment is created in a foreign network so that the mobile users can experience the same computing experience as they have in their home or corporate computing environment while they are mobile and roaming
- “a system concept for personalization service portability across network boundaries and between terminals”

- Personal Communication Networks
- Supports personal numbering, individual service selection, call anytime anywhere etc

- USIM
- Smart card for 3G mobile phones
- Provides enhanced personalization in the form of comprehensive phonebooks
- High performance processors & cryptography capabilities
- 64 Kbytes memory
- Backwards compability

- Audio/Video
- Voice over Internet Protocol(VoIP/Voice over Packet Network)
- Electronic agents
  - Programs that go places in the network to carry out their owner's instructions
- Downloading of software and contents

S.no	GSM	CDMA
1	The GSM is based on wedge spectrum called a carrier.	The CDMA is based on spread spectrum technology.
2	This carrier is divided into time slots, and each user is assigned a different time slot. Thus, until the ongoing call is finished, no other user can access the same slot.	This technology allows each user to transmit over the entire frequency spectrum all the time.
3	Less security compared to CDMA technology.	More security is provided in CDMA technology.

4	No built-in encryption.	It has built-in encryption
5	Signals can be detected as the GSM signals are concentrated in the narrow bandwidth.	The signals cannot be detected easily in CDMA.
6	The GSM network operates in the frequency spectrum of 850MHz and 1900MHz.	The CDMA network operates in the frequency spectrum of 850MHz and 1900MHz.
7	GSM is used over 80% of the world's mobile network.	CDMA is exclusively used in the United States, Canada and Japan.

8	GSM uses EDGE data transfer technology.	CDMA has faster data transfer as EVDO ready data transfer technology is used
9	It offers a maximum download speed of 384 Kbps.	It offers a maximum download speed of 2 Mbps.
10	A SIM card is required for the working of GSM device.	CDMA phones do not have these pulses.

11	A GSM is more flexible than CDMA as the SIM can be replaced with other GSM devices.	A CDMA is not flexible.
12	GSM phones emit continuous wave pulse. Thus, there is a need to reduce the exposures to electromagnetic fields.	CDMA phones do not have these pulses.
13	GSM phone emits about 28 times more radiations on an average as compared to CDMA.	Very less radiation

4G technology

- Fourth generation of broadband cellular network technology
- A 4G system must provide capabilities defined by ITU in IMT Advanced
- Popular applications: IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television.

LTE(Long-Term Evolution)

- A standard for wireless broadband communication for mobile devices and data terminals
- It increases the capacity and speed using a different radio interface together with core network improvements
- Developed by the 3GPP (3rd Generation Partnership Project)
- Offers speed up to 100 Mbit/s in the downlink and 50 Mbit/s in the uplink if a 20 MHz channel is used

Mobile WiMAX (IEEE 802.16e)

- Offers peak data rates of 128 Mbit/s downlink and 56 Mbit/s uplink over 20 MHz wide channels

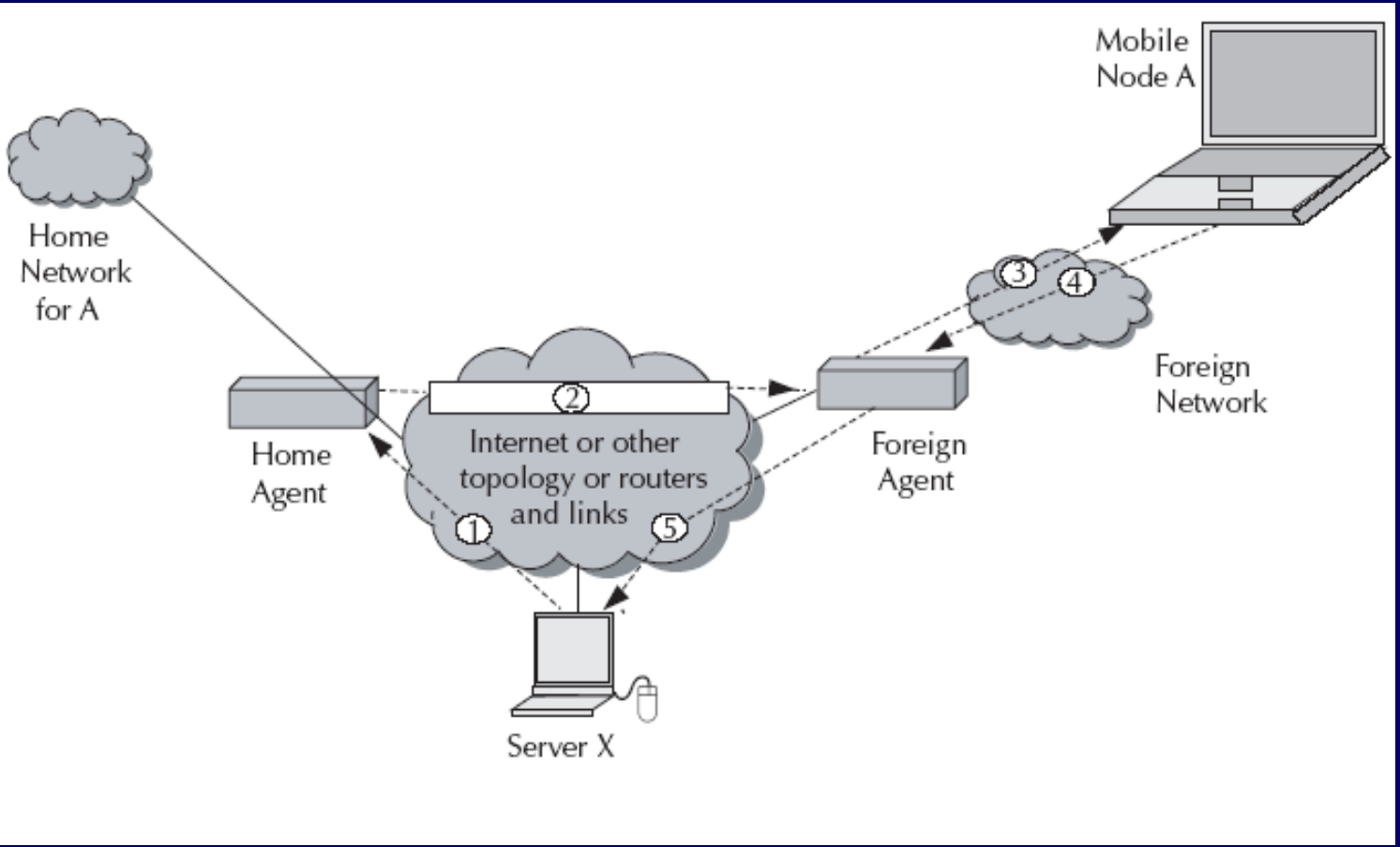
Features

- IPv6 support
- Advanced antenna systems
- Open-wireless Architecture and Software-defined radio
- Support interactive multimedia, voice, video, wireless internet and other broadband services.
- High speed, high capacity and low cost per bit
- HD voice and video calls

Mobile IP

- ‘Mobile IP’ signifies that, while a user is connected to applications across the Internet and the user’s point of attachment changes dynamically, all connections are maintained despite the change in underlying network properties
- Similar to the handoff/roaming situation in cellular network
- Mobile IP allows the mobile node to use two IP addresses called home address and care of address
- The home address is static and known to everybody as the identity of the host
- The care of address changes at each new point of attachment and can be thought of as the mobile node’s location specific address

Working of Mobile IP



Working of Mobile IP

Let's take the case of mobile node (A) and another host (server X). The following steps take place:

- Server X wants to transmit an IP datagram to node A. The home address of A is advertised and known to X. X does not know whether A is in the home network or somewhere else. Therefore, X sends the packet to A with A's home address as the destination IP address in the IP header. The IP datagram is routed to A's home network.

Working of Mobile IP

- At the A's home network, the incoming IP datagram is intercepted by the home agent. The home agent discovers that A is in a foreign network. A care of address has been allocated to A by this foreign network and available with the home agent. The home agent encapsulates the entire datagram inside a new IP datagram, with A's care of address in the IP header. This new datagram with the care of address as the destination address is retransmitted by the home agent.
- At the foreign network, the incoming IP datagram is intercepted by the foreign agent. The foreign agent is the counterpart of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to A.

Working of Mobile IP

- A intends to respond to this message and sends traffic to X. In this example, X is not mobile; therefore X has a fixed IP address. For routing A's IP datagram to X, each datagram is sent to some router in the foreign network. Typically, this router is the foreign agent. A uses X's IP static address as the destination address in the IP header.
- The IP datagram from A to X travels directly across the network, using X's IP address as the destination address.

Working of Mobile IP

- Discovery - A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- Registration - A mobile node uses a registration procedure to inform its home agent of its care-of address.
- Tunneling - Tunneling procedure is used to forward IP datagrams from a home address to a care of address.

Discovery

- Agent advertisements are transmitted by both home and foreign agents to advertise their services on a link
- Mobile nodes use these advertisements to determine their current point of attachment to the Internet
- Using the procedure, the mobile node determines whether it is in a foreign network
- For the purpose of discovery, an agent periodically issues a advertisement message

Discovery

- The mobile node on receiving this advertisement packet, compares the network portion of the router IP address with the network portion of its own IP address allocated by the home network
- If these network portions do not match, then the mobile node knows that it is in a foreign network
- A router advertisement can carry information about default routers and information about one or more care of addresses
- If a mobile node needs a care of address without waiting for the agent advertisement, the mobile node can broadcast a solicitation that will be answered by the foreign network

Registration

- Once a mobile node obtained a care of address from the foreign network, the same needs to be registered with the home agent
- The mobile node sends a registration request to the home agent with the COA information
- When the home agent receives this request, it updates its routing table and sends a registration reply back to the mobile node

Registration

- As part of registration, the mobile node needs to authenticated
- Registration messages between a mobile node and its home agent must be authenticated
- Using 128 bit key and hashing algorithm, a digital signature is generated
- Each mobile node and a home agent shares a common secret
- This secret makes the digital signature unique and allows the agent to authenticate the mobile node

Registration

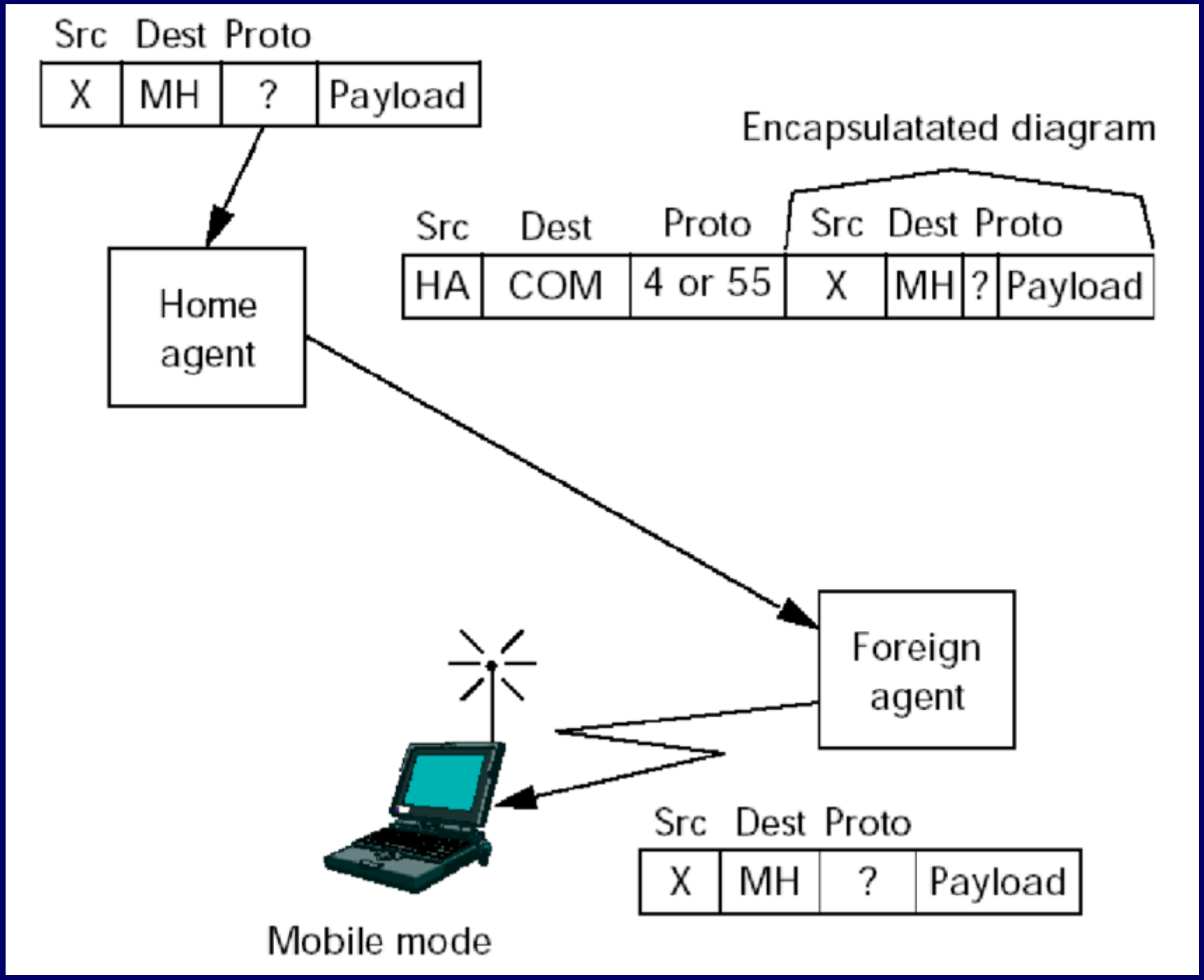
- At the end of the registration a triplet containing a home address, care of address and registration lifetime is maintained in the home agent
- This is called a binding for the mobile node
- The home agent maintains this association until the registration life expires

Steps in Registration

- The mobile node requests for forwarding service from the foreign network by sending registration request to the foreign network
- The foreign agent relays this registration request to the home agent of that mobile node
- The home agent either accepts or rejects and sends a registration reply to the foreign agent
- The foreign agent relays this reply to the mobile node

Tunneling

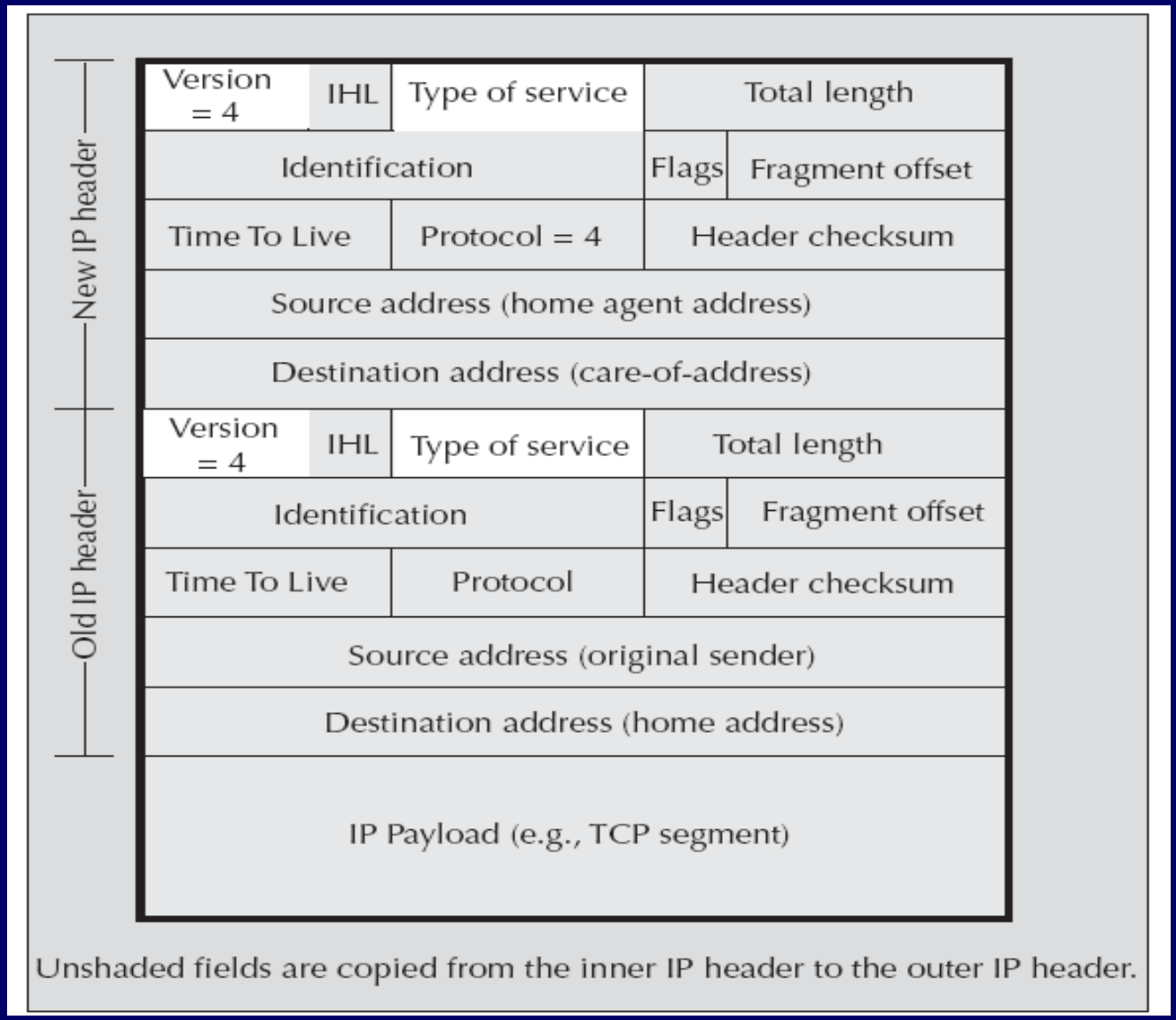
- In the mobile Ip, an IP within IP encapsulation mechanism is used
- Using IP within IP, the home agent adds a new IP header called tunnel header
- Tunnel header uses the mobile node's care of address as the tunnel destination IP address
- The tunnel source IP address is the home agent's IP address
- The entire original IP header is preserved as the first part of the payload of the tunnel header; the foreign agent after receiving the packet, drops the tunnel header and delivers the rest to the mobile node


Src Dest Proto
X MH ? Payload
Encapsulatated diagram
Src Dest Proto
HA COM 4 or 55
Src Dest Proto
X MH ? Payload
Home agent
Foreign agent
Src Dest Proto
X MH ? Payload
Mobile mode

Tunneling

- When a mobile node is roaming in a foreign network, the home agent must be able to the intercept all IP datagram packets sent to the mobile node so that these datagrams can be forwarded via tunneling
- The home agent therefore needs to inform other nodes in the home network that all IP datagrams with the destination address of the mobile node should be delivered to the home agent

IP headers in Mobile IP



Unshaded fields are copied from the inner IP header to the outer IP header.

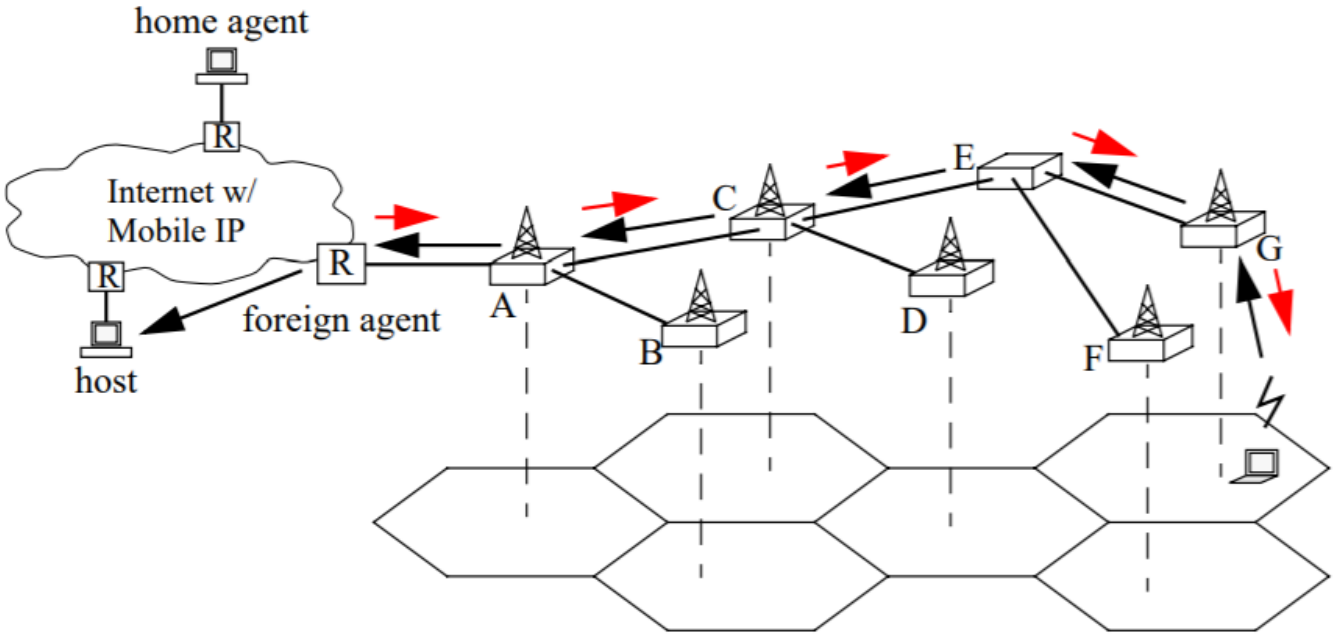
Cellular IP

- Whenever the mobile host moves to a new subnet managed by a different foreign agent, the dynamic care of address will change
- This changed COA needs to be communicated to the home agent
- This process works for slowly moving hosts
- For a high speed mobile host, the rate of update of the addresses needs to match the rate of change of addresses; otherwise packets will be forwarded to the wrong(old) addresses
- Mobile IP fails to update the addresses properly for high speed mobility

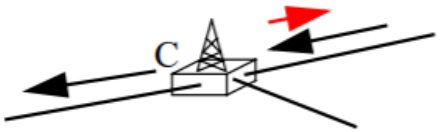
Cellular IP

- In a cellular IP, none of the nodes know the exact location of a mobile host
- Packets addressed to a mobile host are routed to its current base station on a hop-by-hop basis where each node only needs to know on which of its outgoing ports to forward packets
- This limited routing information (referred as mapping) is local to the node and does not assume that nodes have any knowledge of the wireless network topology
- Mappings are created and updated based on the packets transmitted by mobile hosts.

Cellular IP



Node is “self-sufficient”:

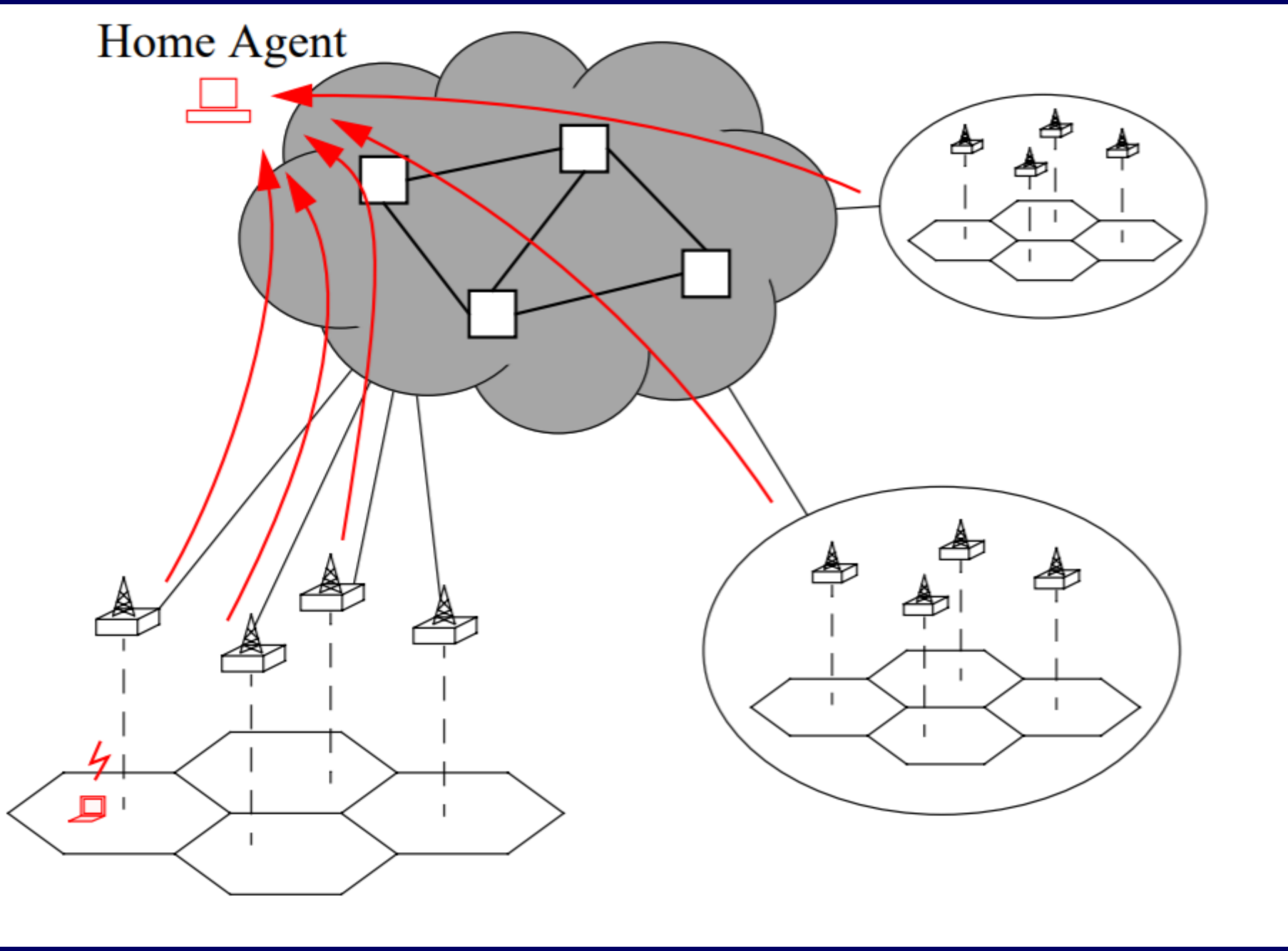


Cellular IP

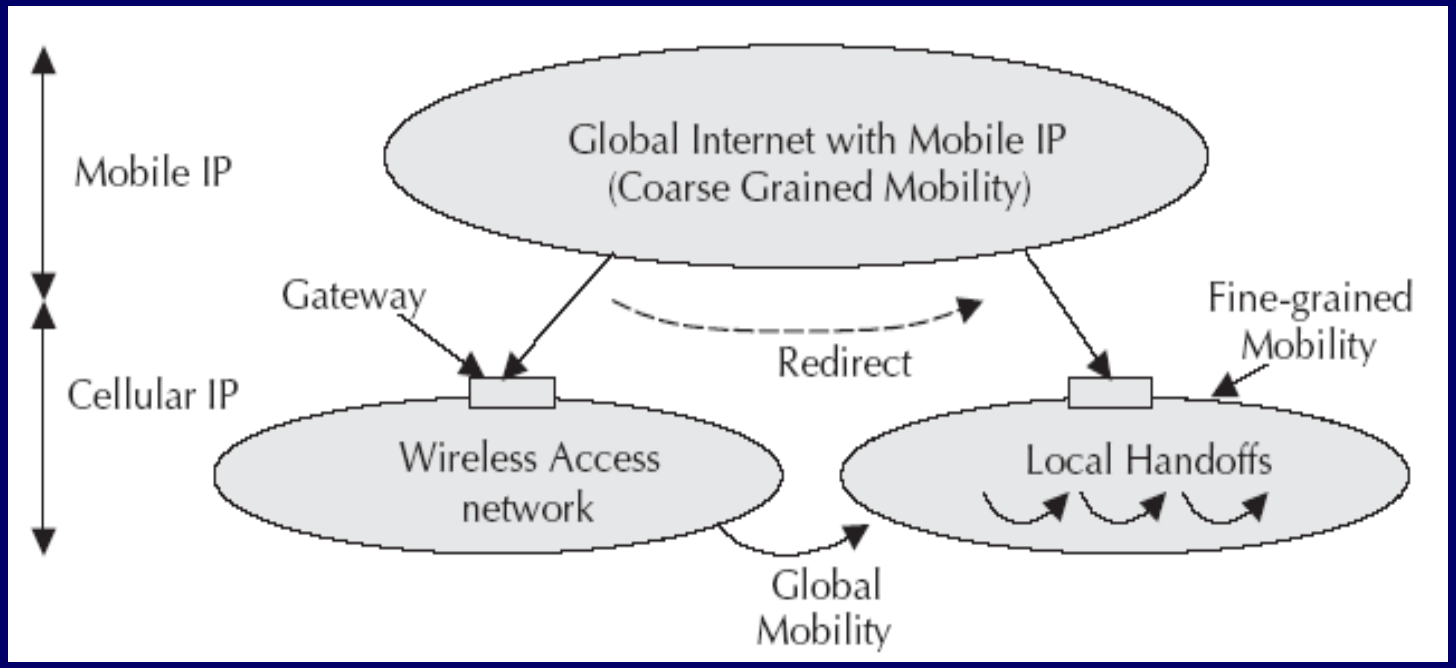
- Mobile IP represents a simple & scalable global mobility solution, but is not appropriate in support of fast & seamless handoff control.
- Cellular IP is a new robust protocol that is optimized to support local mobility but efficiently interworks with Mobile IP to provide wide area mobility
- Cellular IP shows great benefit in comparison to existing host mobility protocols for environments where mobile hosts migrate frequently. This is very much valid as wireless internet becomes widespread.
- CIP can accommodate large no of users by maintaining distributed Paging and Routing caches
- Also CIP requires no new packet formats, encapsulations, or address space allocations beyond what is present in IP.

Cellular IP

- Mobile IP-suitable for slowly moving hosts; cellular IP is ideal where mobile hosts migrate frequently
- Mobile IP is an officially endorsed international standard. Cellular IP is a "micro-mobility" proposed protocol. This routes IP traffic within a fixed range over wireless devices. Cellular IP competes with other micro-mobility solutions.
- Mobile IP is not appropriate for cell granularity, but can provide global mobility support; Cellular IP does scale to a global level but it provides fast and smooth handoffs on a local scale
- Mobile IP is developed to provide wide area mobility support. Cellular IP is optimized to support local mobility but efficiently interworks with Mobile IP

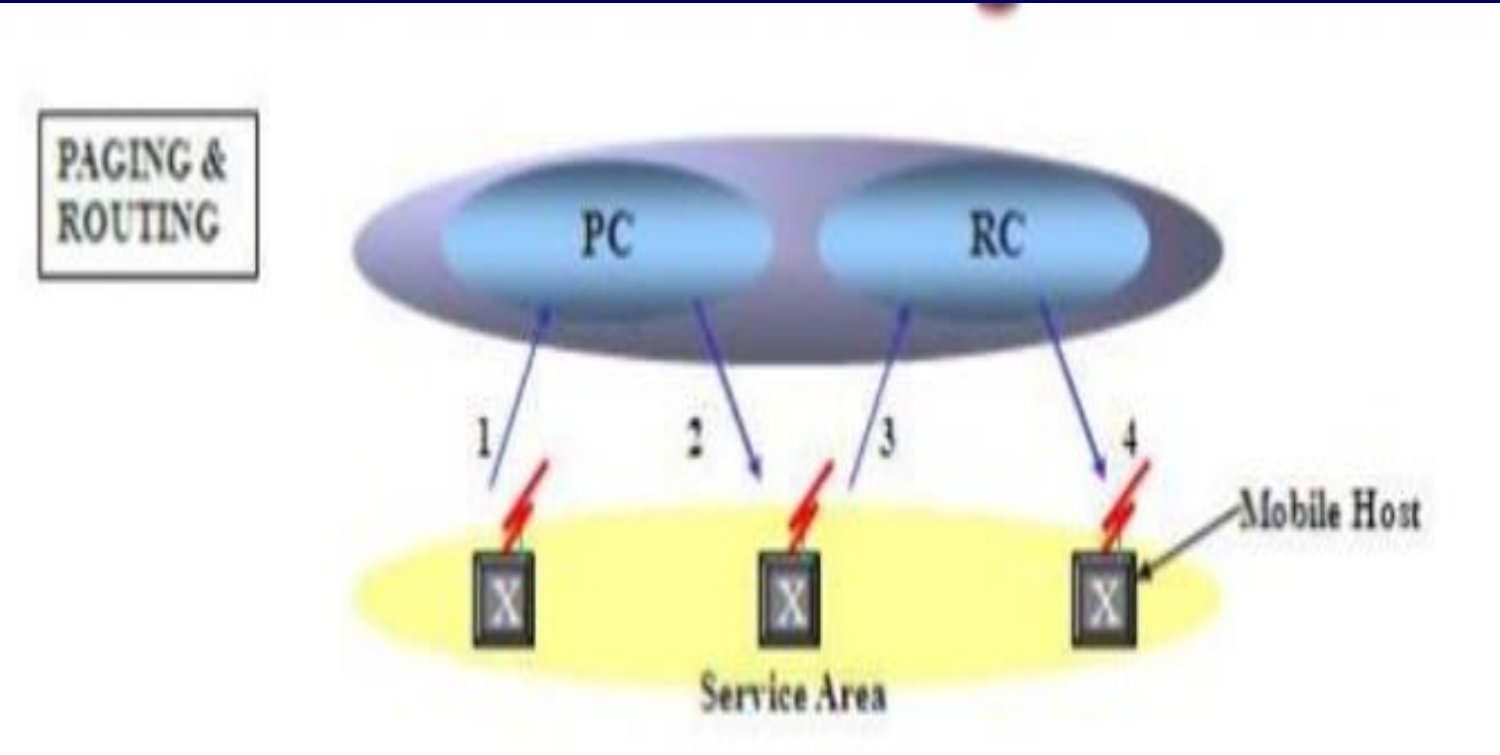

Home Agent

Relationship between Mobile IP and Cellular IP



Cellular IP

- Uses two parallel structures of mappings through Paging Caches (PC) and Routing Caches (RC)
- PCs maintain mappings for stationary and idle (not in data communication state) hosts
- RC maintains mappings for mobile hosts
- Mapping entries in PC have a large timeout interval, in the order of seconds or minutes. RCs maintain mappings for mobile hosts currently receiving data or expecting to receive data


PAGING &
ROUTING
PC
RC
1
2
3
4
Mobile Host
X
X
X
Service Area

- While idle at location1, the mobile host X keeps PCs up to date by transmitting dummy packets at a low frequency
- Let us assume that the host is mobile and moved to location 2. while at location 2, there are data packets to be routed to the mobile host X, the PC mappings are used to find the host
- As there is data transmission, the mapping database to be used will be the RC
- As long as data packets keep arriving, the host maintains RC mappings, either by its outgoing data packets or through the transmission of dummy packets

Bluetooth

- Allows users to make ad hoc wireless connections between devices wirelessly
- Operates in a globally available frequency band ensuring worldwide interoperability
- Managed and maintained by Bluetooth Special Interest Group

Bluetooth Protocol

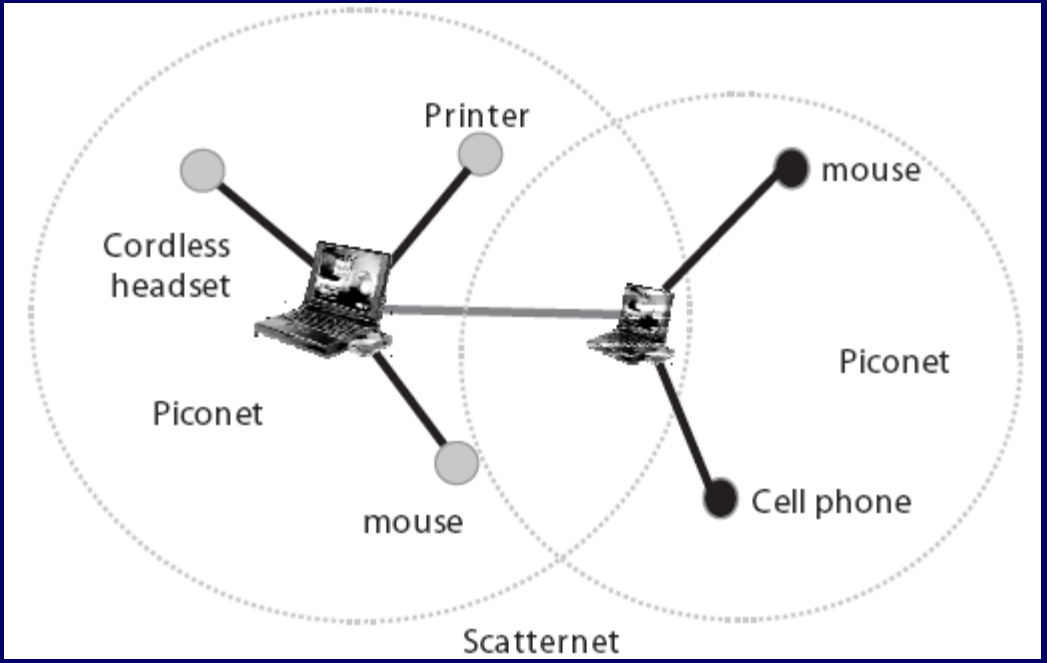
- Uses the unlicensed 2.4 GHz ISM (Industrial Scientific and Medical) frequency band
- 79 available channels spaced 1 MHz apart from 2.402 GHz to 2.480 GHz
- Allows power levels starting from 1mW (covering 10 centimetres) to 100mW (covering upto 100 meters) suitable for short device zone to personal area networks within a home
- Supports both unicast (point-to-point) and multicast (point-to-multipoint) connections
- Bluetooth protocols are a collection of many inter-related protocols

Bluetooth Protocol

- Uses the master and slave relationship
- Master and slaves together form a Piconet when master allows slaves to talk
- Up to seven ‘slave’ devices can be set to communicate with a ‘master’ in a Piconet
- Scatternet is formed when several of piconets are linked together to form a larger network in an ad hoc manner

Bluetooth Protocol

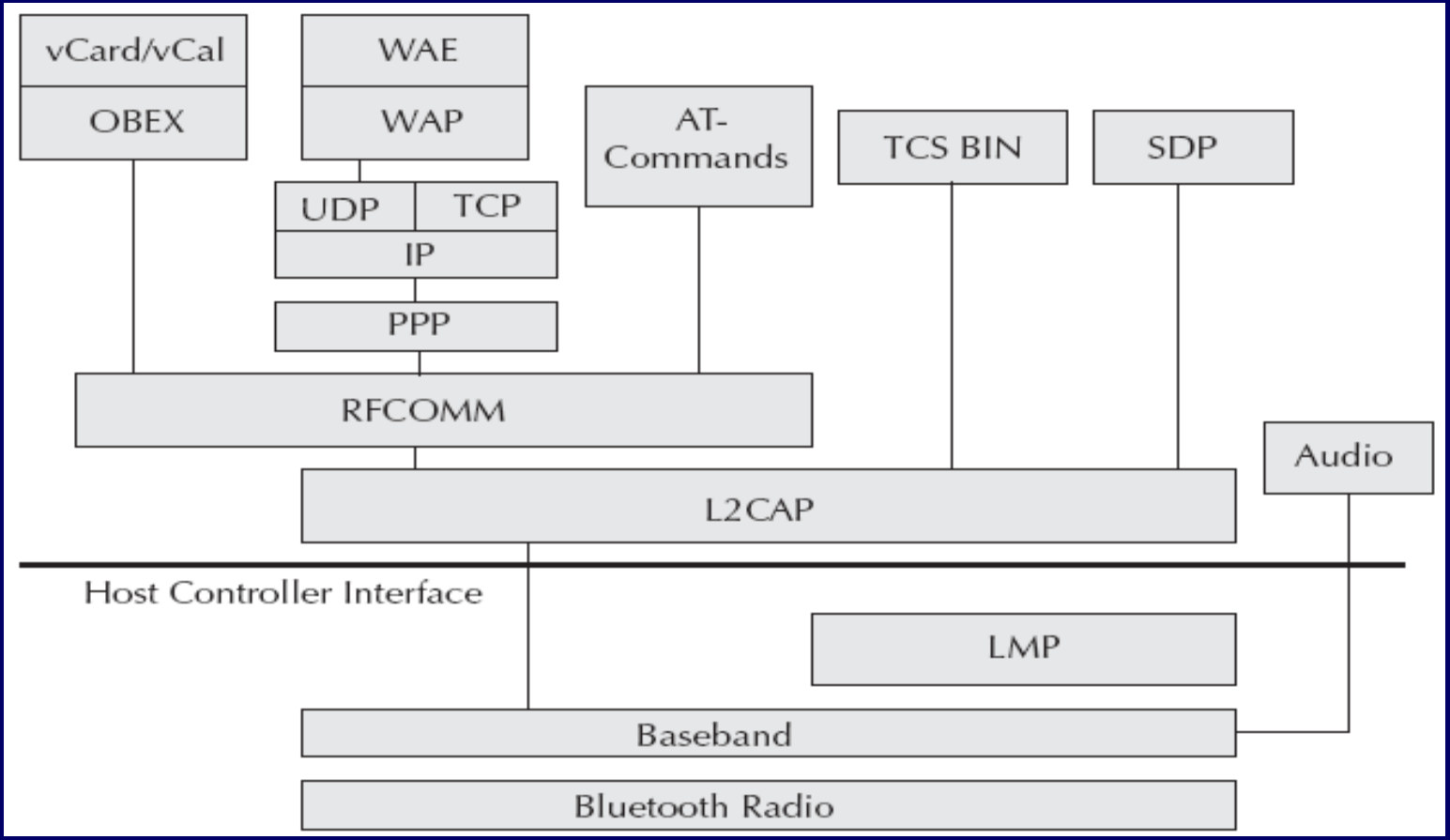
- Scatternet is a topology where a device from one piconet also acts as a member of another piconet wherein a device being a master in one piconet can simultaneously be a slave in the other one



Bluetooth Protocol

- Bluetooth Core protocols plus Bluetooth radio protocols are required by most of Bluetooth devices
- Uses spread spectrum technologies at the Physical Layer while using both direct sequence and frequency hopping spread spectrum technologies
- Uses connectionless (ACL–Asynchronous Connectionless Link) and connection-oriented (SCO–Synchronous Connection-oriented Link) links
- Cable Replacement layer, Telephony Control layer and Adopted protocol layer form application-oriented protocols

Bluetooth Protocol Stack



OBEX – Object Exchange Protocol

WAE – Wireless Application Environment

WAP – Wireless Application Protocol

LMP – Link Manager Protocol

TCS BIN – Telephony Control Specification Binary

SDP – Service Discovery Protocol

RFCOMM – Radio Frequency Communication

L2CAP – Logical Link Control and Adaptation Protocol

Bluetooth Protocol Stack

1. Bluetooth Core Protocols
2. Cable Replacement Protocol
3. Telephony Control Protocols
4. Adopted Protocols

Bluetooth Core Protocols

- Baseband – enables physical RF link
- It performs the connection establishment within a piconet.
- This layer uses inquiry and paging procedures to synchronize the transmission with different Bluetooth device

- Link Manager Protocol (LMP) – when two Bluetooth devices come within each other's radio range, link manager of either device discover each other
- LMP then engages itself with peer to peer message exchange
- Also performs generation and exchange of encryption keys
- Performs link setup, negotiation of baseband packet size
- manages devices in range, power modes, connections

Bluetooth Core Protocols

- Logical Link Control and Adaptation Protocol (L2CAP) – responsible for segmentation and re-assembly of fragmented packets
- Also responsible for multiplexing of Bluetooth packets from different applications

Bluetooth Core Protocols

- Service Discovery Protocol (SDP) – Enables a device to join a piconet
- Using SDP, a device enquires what services are available in a piconet and how to access them
- Uses client server model where server has a list of services defined through service records
- If a device provides multiple services, one SDP acts on behalf of all of them

Bluetooth Core Protocols

- A Bluetooth device in an inquiry mode broadcasts packets on 32 frequency channels of the inquiry hopping sequence.
- It sends two packets every 625ms and listens for responses
- At this point unique identity of the devices called Bluetooth globalID is exchanged
- Upon matching of the device profile, a connection is set up, and devices exchange data
- Paging device becomes master and paged device becomes slave

Cable Replacement Protocol

- Radio Frequency Communication (RFCOMM) - emulates RS-232 control and data signals over Bluetooth baseband protocol

Telephony Control Protocols

- Telephony Control Specification Binary (TCS BIN) - defines the call control signaling protocol and handles mobility management for groups of Bluetooth TCS devices
- Attention (AT) Commands - defines a set of commands by which a mobile phone can be used and controlled as a modem for fax and data transfers

Adopted Protocols

- Point-to-Point Protocol (PPP) - means of taking IP packets to/from the PPP layer and placing them onto the LAN
- Transmission Control Protocol/Internet Protocol (TCP/IP) - used for communication across the Internet
- Object Exchange (OBEX) Protocol - session protocol to exchange objects and used to browse the contents of folders on remote devices
- Content Formats - used to exchange messages and notes and synchronize data amongst various devices

Bluetooth Security

- Offers security infrastructure starting from authentication, key exchange to encryption
- Uses the publicly available cipher algorithm known as SAFER+ to authenticate a device's identity

Bluetooth Application Models

Each application model in Bluetooth is realized through a Profile. Profiles define the protocols and protocol features supporting a particular usage model. Some common profiles are:

- File Transfer
- Internet Bridge
- LAN Access
- Synchronization
- Headset