LECTURE NOTES

ON

MOBILE COMPUTING

SUBJECT CODE: PECS 5301 (3-0-0)

PREPARED BY

DR. PRASHANTA KUMAR PATRA

COLLEGE OF ENGINEERING AND TECHNOLOGY, BHUBANESWAR

PECS5301 **MOBILE COMPUTING** (3-0-0)

Module - I 10 Hrs

Introduction to Personal Communications Services (PCS) : PCS Architecture, mobility management, Networks signaling, Global System for Mobile Communication (GSM) System overview : GSM Architecture, Mobility management, Network signaling.

General Packet Radio Services (GPRS): GPRS Architecture, GPRS Network Nodes, Mobile Data Communication; WLANs (Wireless LANs) IEEE 802.II standard, Mobile IP.

Module - II 14 Hrs

Wireless Application Protocol (WAP): The Mobile Internet standard, WAP Gateway and Protocols, wireless mark up Languages (WML), Wireless Local Loop (WLL) : Introduction to WLL Architecture, wireless Local Loop Technologies.

Third Generation (3G) Mobile Services: Introduction to International Mobile Telecommunications 2000 (IMT 2000) Vision, Wideband Code Division Multiple Access (W-CDMA), and CDMA 2000

Module - III 12 Hrs

Global Mobile Satellite Systems ; case studies of the IRIDIUM, ICO and GLOBALSTAR systems. Wireless Enterprise Networks : Introduction to Virtual Networks, Blue tooth technology, Blue tooth Protocols.

Server-side programming in Java, Pervasive web application architecture, Device independent example application.

Text Books:

1. Mobile Communication: J. Schiller, Pearson Education
2. Mobile Computing: P.K. Patra, S.K. Dash, Scitech Publications.
3. Mobile Computing: Talukder, TMH, 2nd Edition.

Reference Books:

1. Pervasive Computing: Burkhardt, Pearson Education.
2. Principles of Mobile Computing: Hansmann, Merk, Springer, 2nd Edition.
3. Wireless Communication & Networking: Garg, Elsevier
4. Third Generation Mobile Telecommunication Systems: P. Stavronlakis, Springer.
5. The Wireless Application Protocol: Sandeep Singhal, Pearson Education

Module-I

PCS (Personal Communication System)

PCS stands for Personal Communication System. The objective of PCS is to enable communication with a person at any time, at any place & in any form. It also manages their individual call services according to their service by providing unlimited reachability & accessibility.

Sprint was the first company to set up a PCS network, which was a GSM-1900 network in the Baltimore-Washington metropolitan area in the USA. PCS promises to provide a wide range of locations and equipment-independent services to a large number of users. According to the definition given by the US Federal Communications Commission (FCC), PCS is the system by which every user can exchange information with everyone, at anytime, in any place, through any type of services, using a single personal telecommunication number (PTN).

Key factors of PCS are:

1. Reachability with respect to Location (Home, office, in public, in transit)
1. Accessibility with respect to Device (Cellular phone, wired phone, fax etc.)
2. Management of Service

Architecture

Architecture consists of two parts

Radio Network

PCS users carry mobile stations (MS) to communicate with a BS in a PCS n/w. MS is also referred to as handset or mobile phone. The radio coverage of a base station is

called cell. In GSM n/w each cell is controlled by BSC which are connected to MS through BS. The BSCs are connected to MSC by landlines.

Wireline Transport Network

An MSC is a telephone exchange configured specially for mobile applications. It interfaces the MSC (via BS) with PSTN. MSCs are also connected with mobility database to track the location of MS and roaming management. The databases are HLR & VLR. HLR contains the authentication information like IMSI (International Mobile Subscriber Identity), identification information like name, address of the subscriber, billing information like prepaid or postpaid, operator selection, denial of service to a subscriber etc. VLR gives information about the location area of the subscriber while on roaming and power off status of the handset.

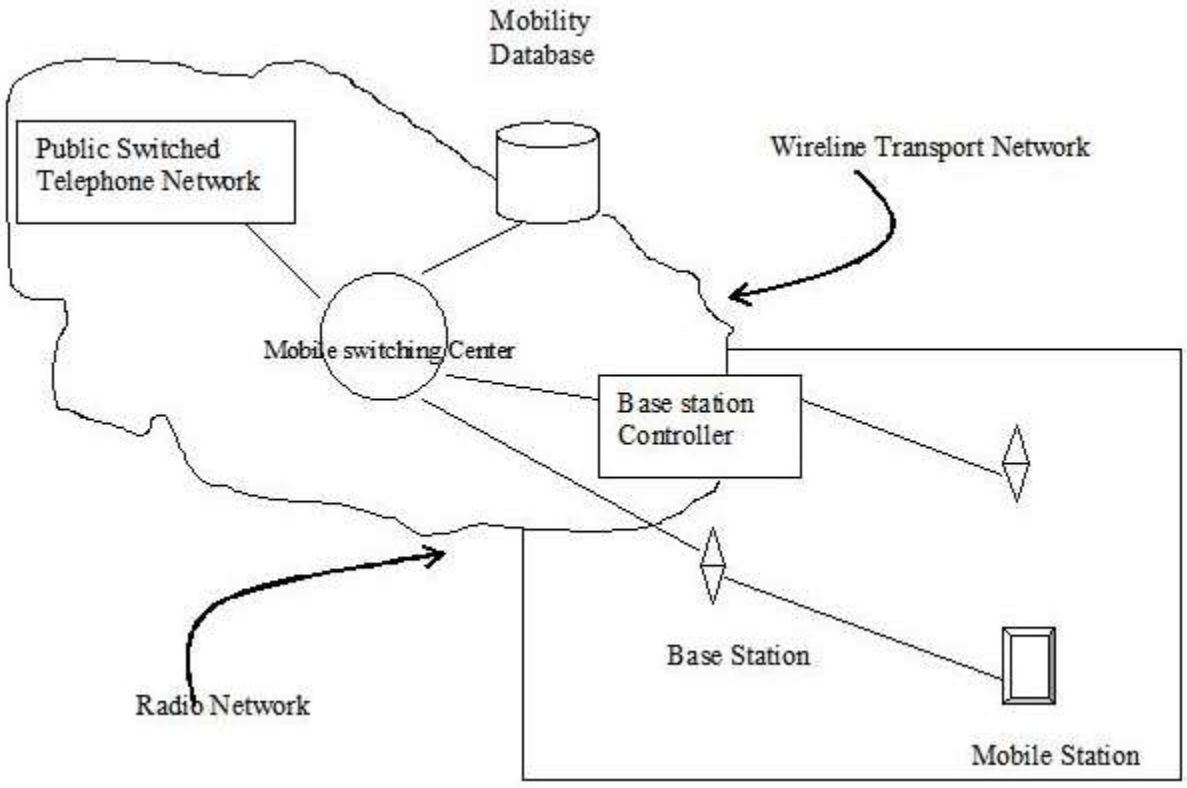


Fig 5.1 PCS network Architecture

5.4 Mobility Management

Mobility mgmt function handles the function that arises due to mobility of the subscriber.

Main objective of MM is location tracking & call set up. There are two aspects of mobility in a PCS n/w.

HANDOFF: When a mobile user is engaged in conversation, the MS is connected to BS via radio link. If the user moves to the coverage area of another BS, the radio link to old BS is disconnected and radio link to new BS is established to continue conversation. This process is called automatic link transfer or handoff. Depending on the mobility of MS, the handoff is divided into two categories:

Inter-BS Handoff/ Inter Cell Handoff:

Here MS usually moves from one BS to another BS under one MSC.

Action taken for communication:

1. The MS momentarily suspends conversation & initiates the hand-off procedure by picking a channel in new BS. Then is resumes the conversation in old BS.
2. When MSC receives that signal, he transfers the information to the new BS & sets up new conversation path to MS through that channel.
3. After MS has been transferred to new BS, it starts the conversation channel with new BS & then MSC disconnect the link with old BS.

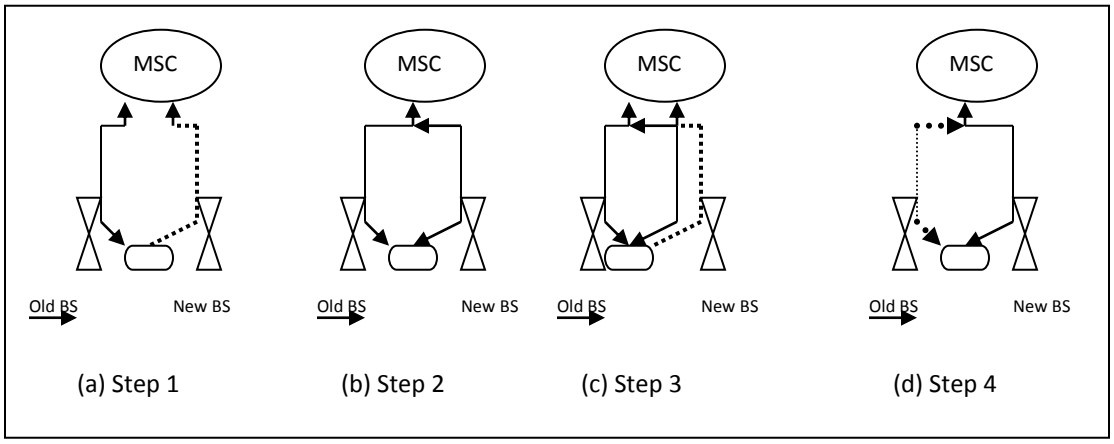


Fig 5.2 Inter-BS link Transfer

Inter-System Handoff/Inter-MSC Handoff

MS moves from one BS to another connected to two different MSCs.

Action taken for communication:

1. MSC1 requests MSC2 to perform handoff measurement on the call in progress.
2. MSC2 then selects a BS by interrogating the signal quality and sends the information to MSC1.
3. Then MSC1 asks MSC2 to setup a voice channel.
4. Assuming that a voice channel is available in BS2.MSC2 instructs MSC1 to start radio link transfer.
5. MSC1 sends the MS a handoff order. Now MS can access BS2 of MSC2.MSC2 informs MSC1 that handoff is successful.MSC1 then connects call path to MSC2.
6. In the intersystem handoff process, anchor MSC is always in call path before & after handoff.

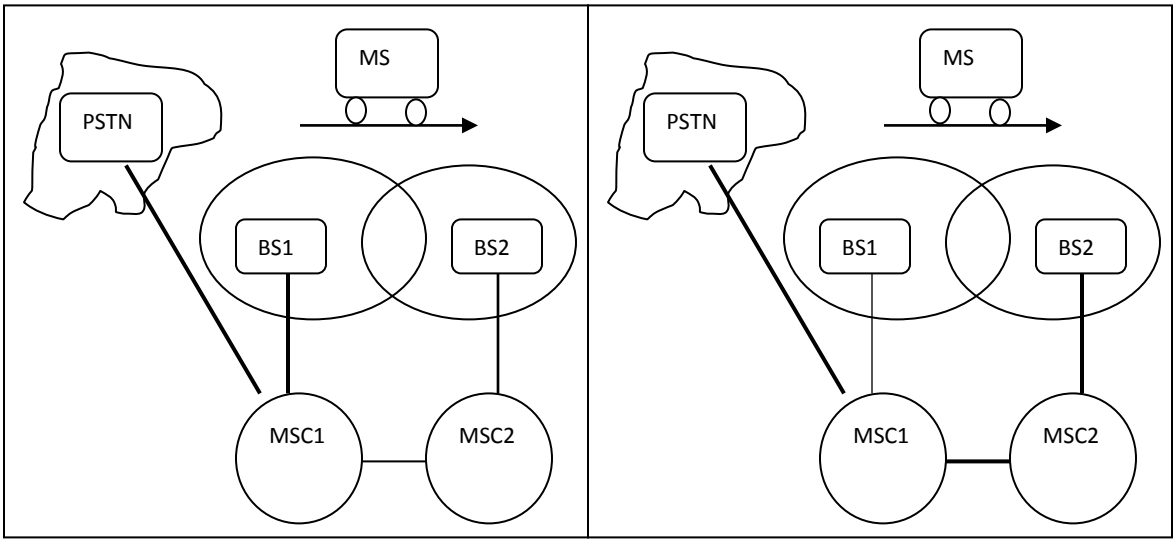


Fig 5.3 Inter System Handoff

Path Minimization- When MS moves to MSC3, MSC2 may be removed from the call path. The link between MSC1 and MSC2 is disconnected and MS connects to MSC3 directly. This process is called path minimization.

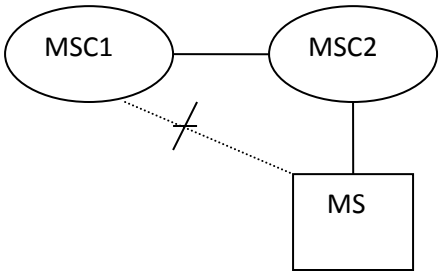


Fig 5.4 Handoff Forward

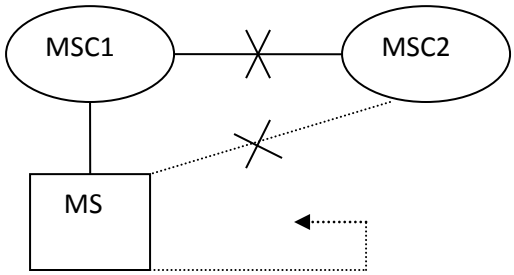


Fig 5.5 Handoff Backward

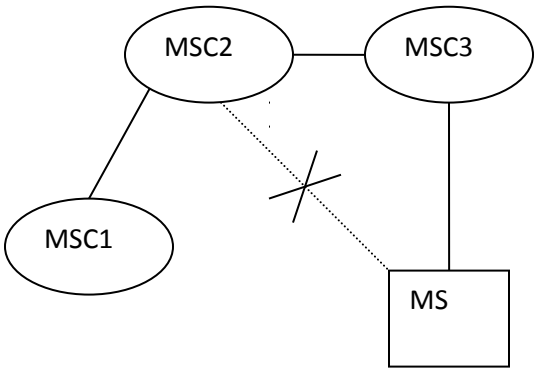


Fig 5.6Hand-off to 3rd

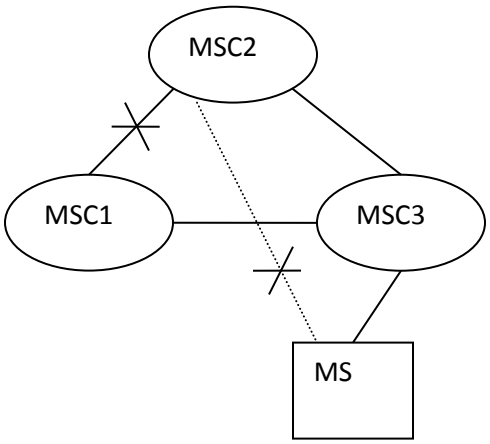


Fig 5.7 Path minimization

ROAMING: When a mobile user moves from one PCS system to another, then the system should be informed of the current location of the user. Otherwise it is impossible to deliver services.

Two basic operations are performed under roaming management.

1. **Registration (location update):** Where MS informs the system its current location.
2. **Location tracking**: Process during which a system locates MS. Location tracking is required when n/w attempts to deliver call to a mobile user.

The roaming management follows a two level strategy where two tier systems of home and visited databases are used. When a user subscribes to the services of a network, a record is created in the system's database called HLR. This is referred to as home

system of the mobile user. HLR is a n/w database, where MS's identity, profile, current location & validation period is stored.

When the mobile user visits a new network other than home system, a temporary record for the mobile user is created in the VLR of visited system. VLR temporarily stores information for visiting subscribers so that corresponding MSC can provide service.

Registration Procedure includes following steps:

1. When mobile user enters into new PCS n/w, it must register in VLR of new system.
2. The new VLR informs mobile user's HLR regarding the current location & address of user. The HLR sends an acknowledgement which includes MS's profile, to the new VLR.
3. New VLR informs MS about successful registration.
4. HLR sends a deregistration message to cancel the location record of MS in old VLR. The old VLR acknowledges the deregistration.

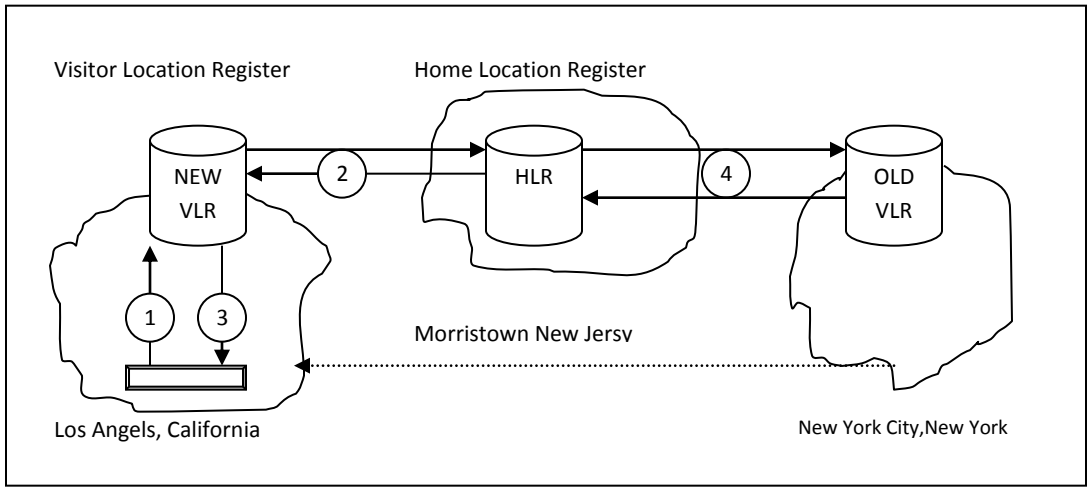


Fig 5.8 MS registration Process

To originate a call, MS first contacts with MSC in the new PCS n/w .The call request is forwarded to VLR for approval. If it is approved, MSC sets up the call to the user following the standard PSTN procedures.

1. If a wireline phone attempts to call a mobile subscriber, the call is forwarded to switch called the originating switch in PSTN. The switch masses a query to HLR to find current VLR of MS. The HLR queries the VLR in which MS resides to get a communicable address.
2. The VLR returns the address to switch through HLR.
3. Based on address, a communication link is established between MS through visited MSC.

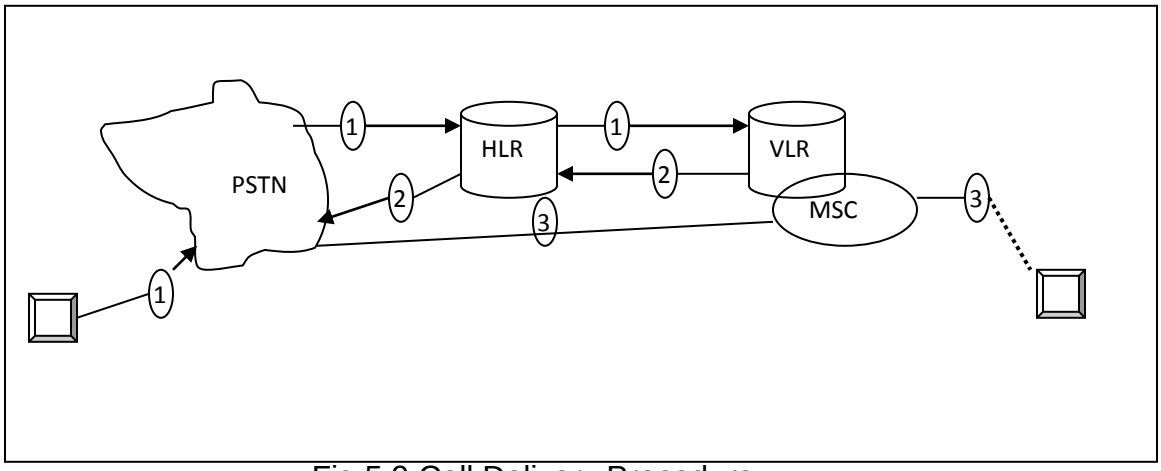


Fig 5.9 Call Delivery Procedure

GSM(Global System for Mobile Communication)

GSM is the most popular standard for mobile phones in the world. GSM (Global System for Mobile communication) is a digital mobile telephony system that is widely used in Europe and other parts of the world.

In 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Groupe Spécial Mobile (GSM) to develop a standard for a mobile telephone system that could be used across Europe. In 1989, GSM responsibility was transferred to the European Telecommunications Standards Institute (ETSI) and phase I of the GSM specifications were published in 1990.

The first GSM network was launched in 1991 by Radiolinja in Finland with joint technical infrastructure maintenance from Ericsson. The proposed GSM system had to meet certain business objectives:

- Support for International Roaming
- Good Speech Quality
- Ability to support handheld terminals
- Low terminal and service cost.
- Spectral Efficiency

GSM uses a combination of FDMA and TDMA. The GSM system has an allocation of 50 MHz bandwidth in the 900 MHz frequency band. Using FMA, this band is divided into 124 channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is further divided into 8 time slots. Therefore with combination of FDMA and TDMA we can realize a maximum of 992 channels for transmit and receive.

Cell: Cell is the basic service area: one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

Location Area: A group of cells form a Location Area. This is the area that is paged when a subscriber gets an incoming call. Each Location Area is assigned a Location Area Identity (LAI). Each Location Area is served by one or more BSCs.

GSM Architecture

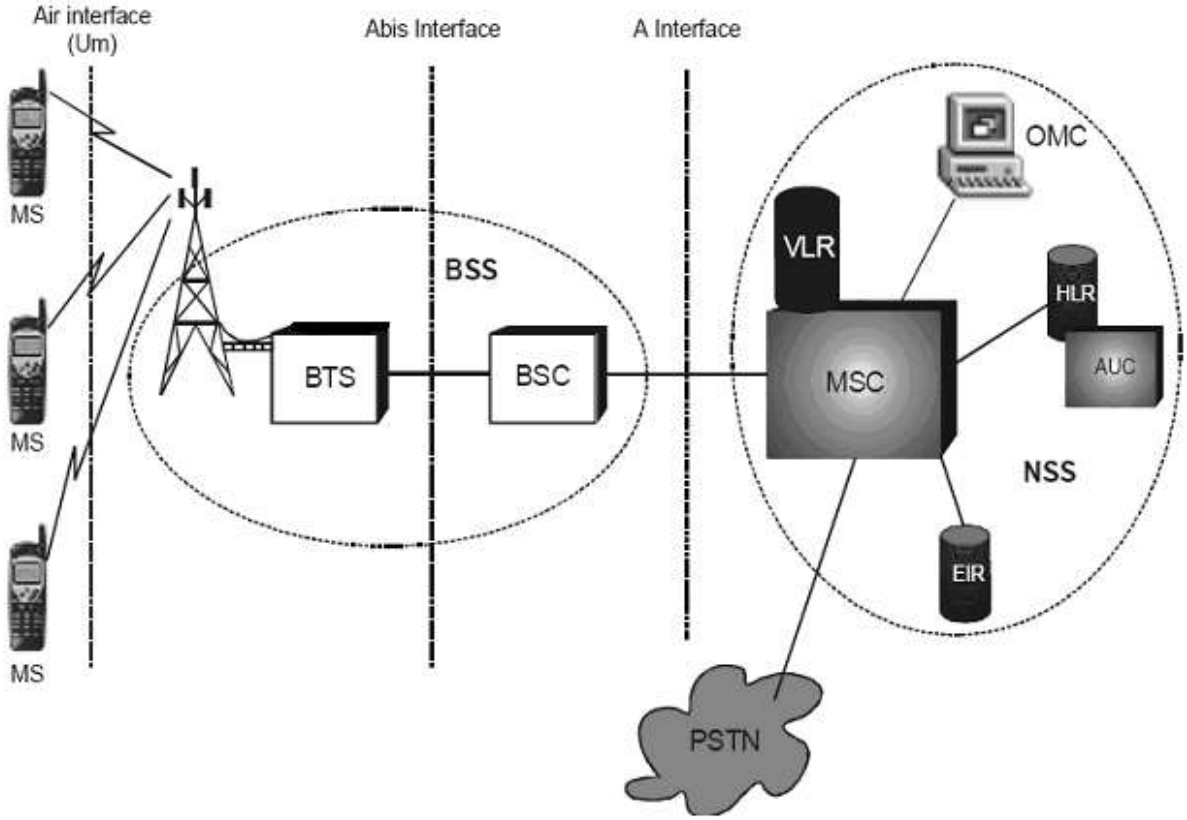


Fig 6.1 GSM Architecture overview

Abbreviations

MSC: Mobile switching center

BSC : Base station controller

BTS : Base transceiver station

TRX : Transceiver.

MS : Mobile station

OMC: Operations and Maintenance centre.

PSTN : Public switched telephone network.

BSS : Base station sub-system.

HLR : Home location register

VLR : Visitor locations register

AUC : Authentication centre

EIR : Equipment Identity Register.

GSM network can be divided into 4 groups.

MS (Mobile Station)

An MS is used by a mobile subscriber to communicate with the mobile network. Several types of MSs exist, each allowing the subscriber to make and receive calls. Manufacturers of MS offer a variety of design and features to meet the need of different market.

The mobile station consists of:

- Mobile Equipment (ME)
- Subscriber identity module (SIM)

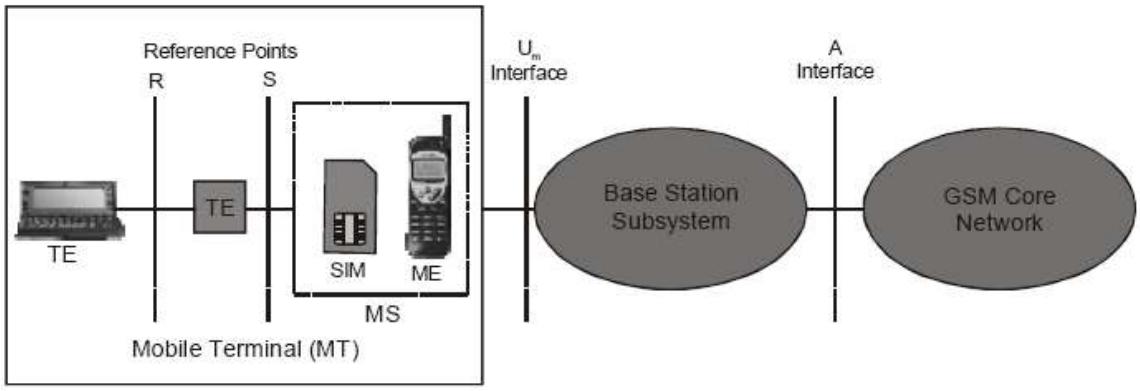


Fig 6.2 GSM Mobile Terminal

ME (Mobile Equipment)

"Cellular phone without SIM card"

The mobile equipment has a unique international mobile equipment identity (IMEI) which is used by EIR. The numbers of GSM terminal types are defined within the GSM specification. They are distinguished primarily by their power output rating. The range or coverage area of an MS is dependent on the output power capabilities and

consequently different ranges. For example, hand held MSs have a lower output power and shorter range than car-installed MSs with a roof mounted antenna

SIM (Subscriber Identity Module)

SIM card used in phones are smart processor cards. It possesses a processor and a small memory. The SIM stores permanent and temporary data about the mobile, the subscriber and the network. It contains **a serial no, PIN, PUK (Pin Unblocking Key), an authentication key (Ki), IMSI (International Mobile Subscriber Identity).**

The SIM can be plugged into any GSM mobile terminal. This brings the advantages of security and portability for subscriber. Example: Subscriber A's mobile terminal may have been stolen. However, A's own SIM can be used in another person's mobile terminal and the calls will be charged to subscriber A.

Functions of MS

Function of MS is transmission of signal from MS to BTS (using uplink) and reception of signal from BTS to MS (using down link).

BSS (Base Station Subsystem)

BSS contains two components:

- BTS
- BSC

BTS (Base Transceiver Station)

It comprises all radio equipments (e.g.: antenna, signal processing & amplifier required for transmission).It is placed in the center of a cell. Its transmitting power defines the size of a cell. It is connected to MS via Um interface and connected to BSC via Abis Interface. It manages the radio resources for BTSs. It handles & handover the radio frequency, radio channel set up from one BTS to other.

BSC (Base Station Controller)

It connects the BTS and MSC of NSS. It manages radio resources for one or more BTS. It handles and Handover the radio frequency, radio channel setup from one BTS to another.

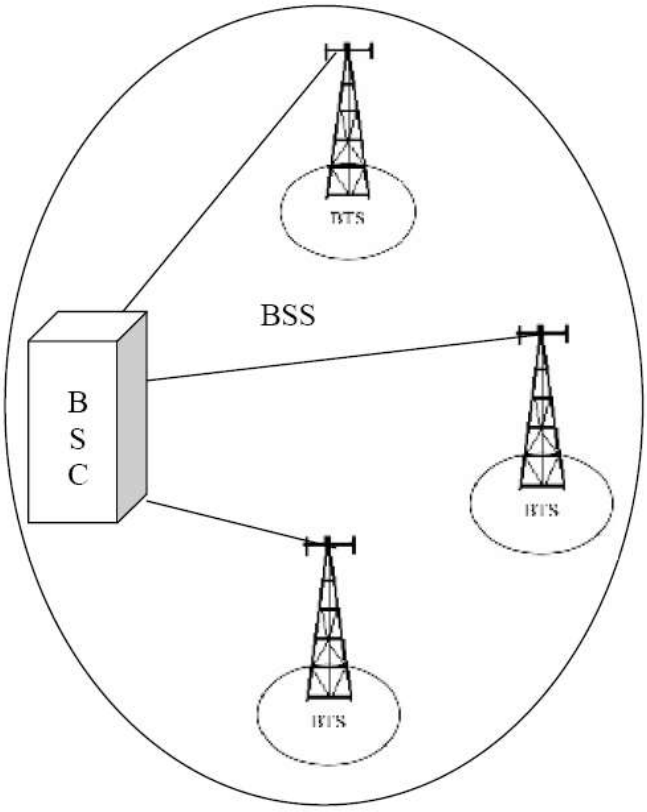


Fig 6.3 BSC & BTS Arrangement in GSM System

NSS (Network Switching Subsystem)

The NSS combines the call rotating switches (MSC and GMSC) with data base registered required to keep track of subscriber's movements and use of the system. Key elements of NSS are:

- MSC
- VLR
- HLR

MSC (Mobile Switching Centre)

The mobile-services switching centre is an exchange which performs all the switching and signaling functions for mobile stations located in a geographical area designated as the MSC area. These are high performance digital ISDN switches. It is used for connection between mobile phone to mobile phone within same network. It is used for connection between mobile phone to fixed phone within a network. It manages BSC within a geographical area.

GMSC (Gateway MSC)

Connection for another network MSC handles all the signaling needed for connection set up and connection release.

HLR (Home Location Register)

The HLR is a centralized network data base that stores and manages all mobile services belonging to a specific operator. It acts as a permanent store for a person's subscription information until that subscription is cancelled. It provides call routing and roaming facility by combining with MSC and VLR. It is considered as a Database which stores the information about the subscriber within covering area of MSC. Information includes current location of the mobile & all the service providing information, when a phone is powered off this information is stored in HLR. It is also a database but contains a temporary copy of some of important information stored in HLR. If a new MS user comes into location area, then VLR will provide relevant information by bringing it from HLR.

VLR (Visitor Location Resister)

It is a temporary storage device of GSM network. It stores subscribers' subscription information for MS which are within the particular MSC service Area. There is one VLR for each MSC service area

OSS (Operation and Support Subsystem)

It contains necessary function for network operation and maintenance.

Key Elements are

- OMC

- EIR
- AUC

OMC (Operation and maintenance center)

It is connected to different components of NSS & to BSC. It controls the traffic load of BSS.

EIR (Equipment Identity Register)

A database that contains a list of all valid mobile equipment within the network where each MS is identified by IMEI (International Mobile Equipment Identity).EIR contains a list of IMEI of all valid terminals. An IMEI is marked invalid if it is stolen. EIR allows the MSC to forbid calls from this stolen terminal. The equipment identification procedure uses the identity of the equipment itself (IMEI) to ensure that the MS terminal equipment is valid.

AUC (Authentication Center)

It is defined to protect user identity & transmission. It is a protected database and stores a copy of secret information stored in SIM card .These data help to verify user's identity.

Network Signaling

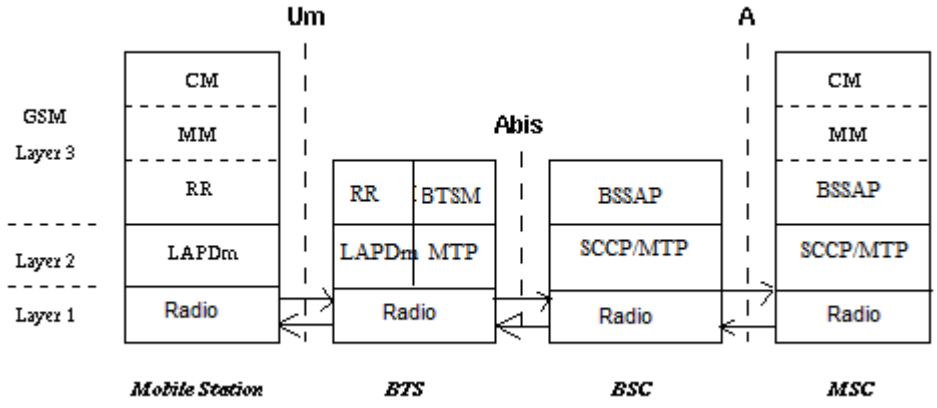


Fig 6.4 Network Signaling

Abbreviations

LAPD Link Access Procedure D-Channel Managed

RR: Radio Resource

MM: Mobility Management

CM: Call Management

BTSM: BTS MAnagement

BSSMAP: BSS Application Protocol

SCCP: Signaling Connection Control Part

The signaling protocol in GSM is structured into 3 layers.

- Layer1□Physical Layer
- Layer2□Data Link Layer
- Layer3□Network Layer

MS □□ BTS

The physical layer between MS & BTS is called Um interface. It performs following functions

- Full or half duplex access.
- Provides TDMA, FDMA, and CDMA.
- Framing of data.

The data link layer controls the flow of packets to and from network layer and provides access to various services like:

Connection: Provides connection between two terminals.

Teleservices -Services offered by a mobile network to users like: MMS, SMS, etc

The data link layer present between MS & BTS is LAPDm (Link Access Protocol managed). LAPDm protocol describes the standard procedure in GSM for accessing D-channel Link.

Its functions are:

- Dataflow control.
- Acknowledged / unacknowledged data Transmission.
- Address and sequence no. check.
- Segmentation.

The network layer has 3-sublayers

CM (Call Management)

Supports call establishment, maintenance, termination.

It supports SMS.

Support DTMF (Dual Tone multiple frequency) signaling.

MM (Mobility Management)

Control the issue regarding mobility Management, location updating & registration.

RRM (Radio Resource Management.)

It manages radio resources such as: frequency assignment, signal measurement.

BTS □□ BSC signaling protocols

The physical layer between BTS & BSC is called Abis interface, where voice is coded by using 64kbps PCM. The connection between BTS and BSC is through a wired network. The data link layer is LAPDm. Network Layer protocol is called BTS Management which interact with BSSAP.

BSC □□ MSC signaling protocol

Physical layer between BSC & MSC is called U interface. Data link layer protocol between BSC & MSC is MTP (Message Transfer Protocol) & SCCP (Signaling Connection Control Protocol). MTP and SCCP are part of the SS7 (Signaling System No7) used by interface A.

NETWORK layer protocols at the MSC are CM, MM and BSSAP (Base Subsystem Application Part).

GSM INTERFACES

Um Interface (MS to BTS)

The Um radio interface (between MS and base transceiver stations [BTS]) is the most important in any mobile radio system. It addresses the demanding characteristics of the radio environment. The physical layer interfaces to the data link layer and radio resource management sublayer in the MS and BS and to other functional units in the MS and network subsystem (which includes the BSS and MSC) for supporting traffic channels. The physical interface comprises a set of physical channels accessible through FDMA and TDMA.

Abis Interface (BTS to BSC)

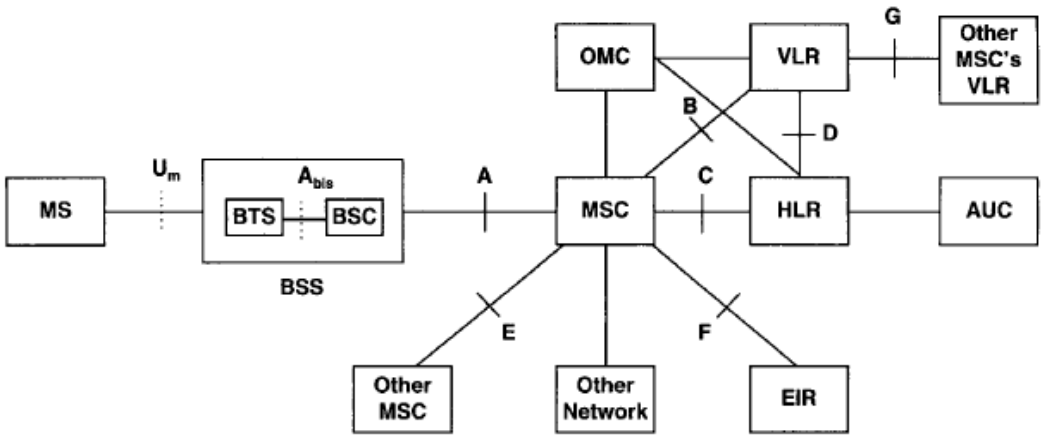
The interconnection between the BTS and the BSC is through a standard interface, Abis. The primary functions carried over this interface are traffic channel transmission, terrestrial channel management, and radio channel management. This interface supports two types of communications links: traffic channels at 64 kbps carrying speech or user data for a full- or half-rate radio traffic channel and signaling channels at 16 kbps carrying information for BSC-BTS and BSC-MSC signaling. The BSC handles the LAPD channel signaling for every BTS carrier.

There are two types of messages handled by the traffic management procedure part of the signaling interface—**transparent** and **nontransparent**. Transparent messages are between the MS and BSC-MSC and do not require analysis by the BTS. Nontransparent messages do require BTS analysis.

A Interface (BSC to MSC)

The A interface allows interconnection between the BSS radio base subsystem and the MSC. The physical layer of the A interface is a 2-Mbps standard Consultative Committee on Telephone and Telegraph (CCITT) digital connection. The signaling transport uses Message Transfer Part (MTP) and Signaling Connection Control Part (SCCP) of SS7. Error-free transport is handled by a subset of the MTP, and logical connection is handled by a subset of the SCCP. The application parts are divided between the BSS application part (BSSAP) and BSS operation and maintenance application part (BSSOMAP). The BSSAP is further divided into Direct Transfer Application Part (DTAP) and BSS management application part (BSSMAP). The DTAP is used to transfer layer 3 messages between the MS and the MSC without BSC involvement. The BSSMAP is responsible for all aspects of radio resource handling at the BSS. The BSSOMAP supports all the operation and maintenance communications of BSS.

Figure shows the various interfaces between the GSM entities.



GSM Channels

GSM has been allocated an operational frequency from 890 MHz to 960 MHz. GSM uses the frequency band 890 MHz-915 MHz for uplink (reverse) transmission, and for downlink (forward) transmission, it uses be frequency band 935 MHz-960 MHz. The available 25-MHz spectrum for each direction is divided into 124 Frequency Division Multiplexing (FDM) channels, each occupying 200 kHz with 100 kHz guard band at two edges of the spectrum as shown in fig.

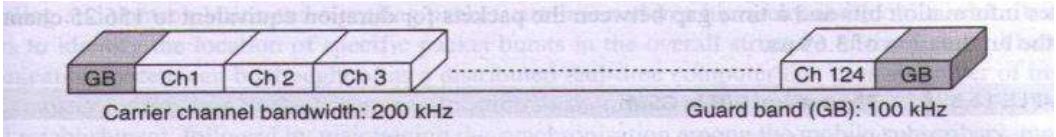


Table 11.2 Logical Channels in GSM

Channel type	*Channel group*	*Channel*	*Direction*
Control Channel (CCH)	Broadcast Channel (BCH)	Broadcast Control Channel (BCCH)	Downlink
		Frequency Correction Channel (FCCH)	Downlink
		Synchronization Channel (SCH)	Downlink
	Common control Channel (CCCH)	Paging Channel (PCH)	Downlink
		Random Access Channel (RACH)	Uplink
		Access Grant Channel (AGCH)	Downlink
	Dedicated control Channel (DCCH)	Standalone Dedicated Control Channel (SDCCH)	Uplink and Downlink
		Slow Associated Control Channel (SACCH)	Uplink and Downlink
		Fast Associated Control Channel (FACCH)	Uplink and Downlink
Traffic Channel (TCH)	Traffic Channel (TCH)	Half-rate Traffic Channel (TCH/H)	Uplink and Downlink
		Full-rate Traffic Channel (TCH/F)	Uplink and Downlink

The logical channels in the GSM network are divided into two principal categories: Control Channels (CCHs) and Traffic Channels (TCHs). Control channels carry signaling and synchronizing commands between the base station and the mobile station. Traffic channels carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link. GSM system uses a variety of logical control channels to ensure uninterrupted communication between MSs and the BS.

GSM Control Channels

There are three classes of control channels defined in GSM: Broadcast Channels (BCH), Common Control Channels (CCCH) and Dedicated Control Channels (DCCH). Each control channel consists of several logical channels that arc distributed in time to provide the necessary GSM control functions.

I. Broadcast Channel (BCH)

The BCH channels are broadcast from the BTS to MSs in the coverage area of the BTS and are one way channels. The broadcast channel operates on the forward link of a specific ARFCN within each cell and transmits data only in the first time slot of certain GSM frames. The BCH provides synchronization for all mobiles within the cell and is occasionally monitored by mobiles in neighboring cells. There are three separate broadcast channels:

1. **Broadcast Control Channel (BCCH):** This channel is used by BTS to broadcast system parameters such as frequency of operation in the cell, operator identifiers, cell ID and available services to all the MSs. Once the carrier, bit, and frame synchronization between the BTS and MS are established, the BCCH informs MS about the environment parameters associated with the BTS covering that area such as current a channel structure, channel availability, and congestion. The BCCH also broadcasts a list of channels are currently in use within the cell.
2. **Frequency Correction Control Channel (FCCH):** This is used by the BTS to broadcast frequency references and frequency correction burst of 148 bits length. An MS in the coverage area of a BTS uses broadcast FCCH signal to synchronize its carrier frequency and bit timing.
3. **Synchronization Channel (SCH):** This channel is used by the BTS to broadcast frame synchronization signals containing the synchronization training sequences burst of 64 bits length to all MSs. Using SCH, MSs will synchronize their counters to specify the location of arriving packets in the TDMA hierarchy. SCH is broadcast in Time Slot 0 of the frame immediately following the FCCH frame and is used to identify the serving base station while allowing each mobile to frame-synchronize with the base station.

II. Common Control Channels (CCCH)

The Common Control Channels (CCCH) are one-way channels used for establishing links between the and the BS for any ongoing call management. CCCHs are the most commonly used control channel and are used to page specific subscribers, assign

signaling channels to specific users, and receive mobile requests for service. There are three CCCH logical channels:

1. **Paging Channel (PCH):** This is a forward link channel and is used by the BTS to page or notify a specific individual MS for an incoming call in the cell. The PCH transmits the IMSI of the target subscriber, along with a request for acknowledgment from the mobile unit on the RACH.
2. **Random Access Channel (RACH):** This is a reverse link channel and is used by the MS either to access the BTS requesting the dedicated channel for call establishment or to acknowledge a page from the PCH. The RACH is used with implementation of a slotted-ALOHA protocol, which is used by MSs to contend for one of the available slots in the GSM traffic frames. The RACH is implemented on the short Random Access Burst (RAB).

III. Dedicated Control Channels (DCCH)

Dedicated Control Channels (DCCH) are two-way channels having the same format and function on both the forward and reverse links, supporting signaling and control for individual mobile subscribers. These are used along with voice channels to serve for any control information transmission during actual voice communication. There are three DCCH logical channels:

1. **Stand-alone Dedicated Control Channel (SDCCH):** This is a two-way channel allocated with SACCH to mobile terminal to transfer network control and signaling information for call establishment and mobility management. The SDCCH ensures that the mobile station and the base station remain connected while the base station and MSC verify the subscriber unit and allocate resources for the mobile. The SDCCH is used to send authentication and alert messages as the mobile synchronizes itself with the frame structure and waits for a TCH.
2. **Slow Associated Control Channel (SACCH):** This is a two-way channel associated with a TCH or a SDCCH and maps onto the same physical channel. The SACCH is used to exchange the necessary parameters between the BTS

and the MS during the actual transmission to maintain the communication link. Each ARFCN systematically carries SACCH data for all of its current users. The gross data rate of the SACCH channel is half of that of the SDCCH. On the forward link, the SACCH is used to send slow but regularly changing control information to the mobile subscriber. The reverse SACCH carries information about the received signal strength and quality of the TCH.

3. **Fast Associated Control Channel (FACCH):** This is a two-way channel used to support fast transitions such as a hand-off request in the channel when SACCH is not adequate. The FACCH is physically multiplexed with the TCH or SDCCH to provide additional support to the SACCH. FACCH is not a dedicated control channel but carries the same information as SDCCH. FACCH is a part of the traffic channel, while SDCCH is a part of the control channel.

Control information in GSM is mainly on two logical channels—the Broadcast Channel (BCCH) and the Paging Channel (PCH). The broadcast information is transmitted first, followed by paging information. **Figure 11.11** shows the structure of a GSM logical control channel.

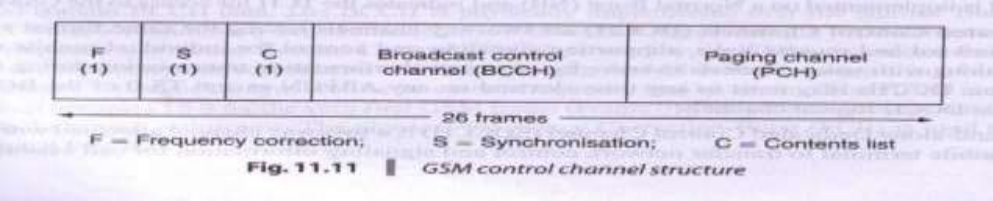


Fig. 11.11 GSM control channel structure

6.6.3 GSM Traffic Channels

Voice channels are called Traffic Channels (TCH) GSM. Traffic channels are two-way channels carrying the voice and data traffic between the MS and BTS. Traffic channels can carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link. One RF channel is shared by eight voice transmissions using TDMA. GSM works out to 25 kHz per voice channel.

Figure 11.12 illustrates how the TCH data is transmitted in consecutive frames.

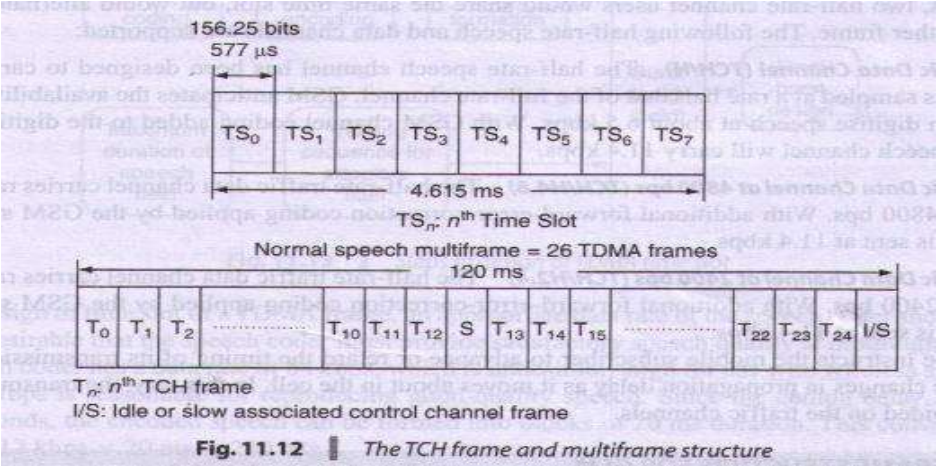


Fig. 11.12 *The TCH frame and multiframe structure*

Frames of TCH data are broken up every thirteenth frame by either Slow Associated Control Channel Data (SACCH) or idle frames. Each group of twenty-six consecutive TDMA frames is called a multiframe. For every twenty-six frames. the thirteenth and twenty-sixth frames consist of Slow Associated Control Channel (SACCH) data, or the idle frame, respectively. The twenty-sixth frame contains idle bits for the case when full-rate TCHs are used and contains SACCH data when half-rate TCHs are used. TCH logical channels are implemented over the normal burst There are two types of TCH channels:

Full-rate traffic channel (TCH/F): This channel uses a 13 kbps speech-coding scheme and 9.600 bps, 4.800 bps, and 2.400 bps data. After including signaling overhead, each full-rate traffic channel has a gross bit rate of 22.8 kbps for the network. When transmitted as full-rate, user data is contained within one time frame.

Half-rate traffic channel (TCH/H): This channel uses 16 time slots per frame that has a gross bit rate of 11.4 kbps. The half-rate TCH supports 4800 bps and 2400 bps rate only. When transmitted as half-rate, user data is mapped onto the same time slot, but is sent in alternate frames. That is, two half-rate channel users would share the same time slot, but would alternately transmit during every other frame.

Mobility Management in GSM

Mobility Management function handles the function that arises due to mobility of the subscriber.

Main objective of MM is location tracking & call set up. The current location of an MS is maintained by a 2-level hierarchical strategy with HLR & VLR. When an MS visits a new location it must register in the VLR of visited location. The HLR must be informed about the registration. The registration process of MS moving from one VLR to another VLR follows following steps.

STEP-1.MS periodically listens to the BCCH (Broadcast Control Channel) broadcast from BSS. If the MS detects that it has entered into a new location area, it sends a registration message to the new VLR by using SDCCH (Standalone Dedicated Control Channel) channel.

SDCCH: Used only for signaling & short message.

BCCH: Provides system information.

STEP-2.The new VLR communicates with old VLR to find HLR of MS. The new VLR then performs authentication process.

STEP-3.After MS is authenticated, new VLR sends a registration message to HLR. If the registration request is accepted, the HLR provides new VLR with all relevant subscriber information.

STEP-4.The new VLR informs the MS of successful registration.

STEP-5. Then the HLR sends a deregistration (Cancellation) message to old VLR. The old VLR cancels the record for MS & sends an acknowledgement to the HLR regarding cancellation.

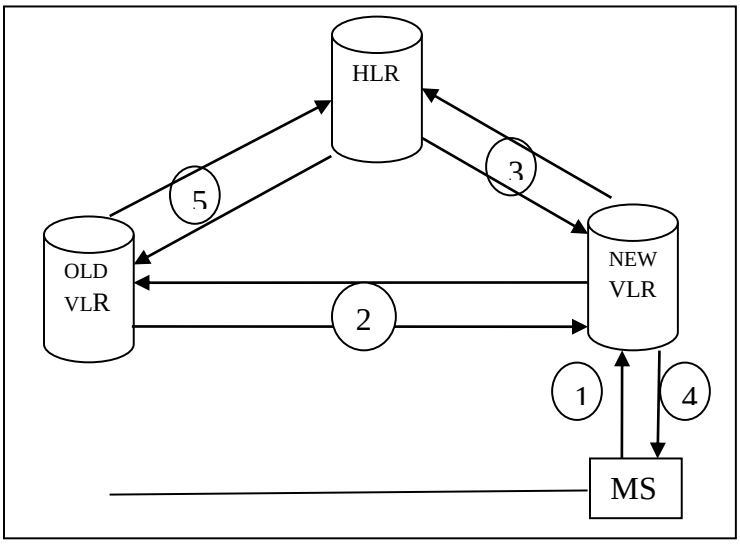


Fig 6.5 GSM Mobility Management

GSM Call Origination

1. MS sends the call origination request to MSC.
2. MSC forwards the request to VLR by sending **MAP_SEND_INFO_ FOR_OUGOING_CALL.**
3. VLR checks MS's profile & sends an ACK to MSC to grant call request.
4. MSC sets up communication link according to standard PSTN call set up procedure.

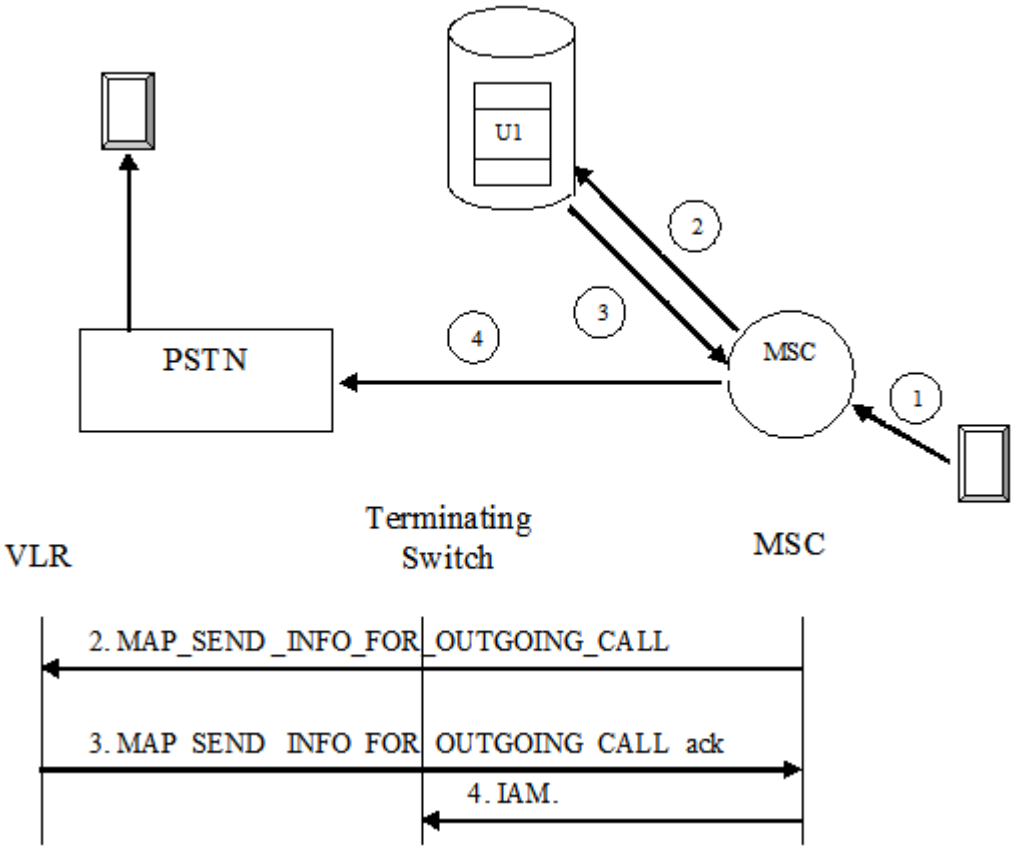


Fig 6.9 Call Origination Operation

Call Termination

When mobile station number is dialed by PSTN user, call is routed to GMSC by IAM (Initial Addressing Message) message.

1. To obtain routing information, GMSC interrogates HLR by sending M**AP_SEND_ROUTING_INFORMATION** to HLR.
2. HLR sends a **MAP_PROVIDE_ROAMING_NUMBER** message to VLR to obtain MSRN (MS Roaming Number). The message consists of IMSI, MSC number etc.
3. The VLR creates the MSRN by using MSC number stored in VLR record of MS. The MSRN no is sent back to GMSC through HLR.
4. MSRN provides address of target MSC where the MS resides. Then a message is directed from GMSC to target MSC to set communication link.

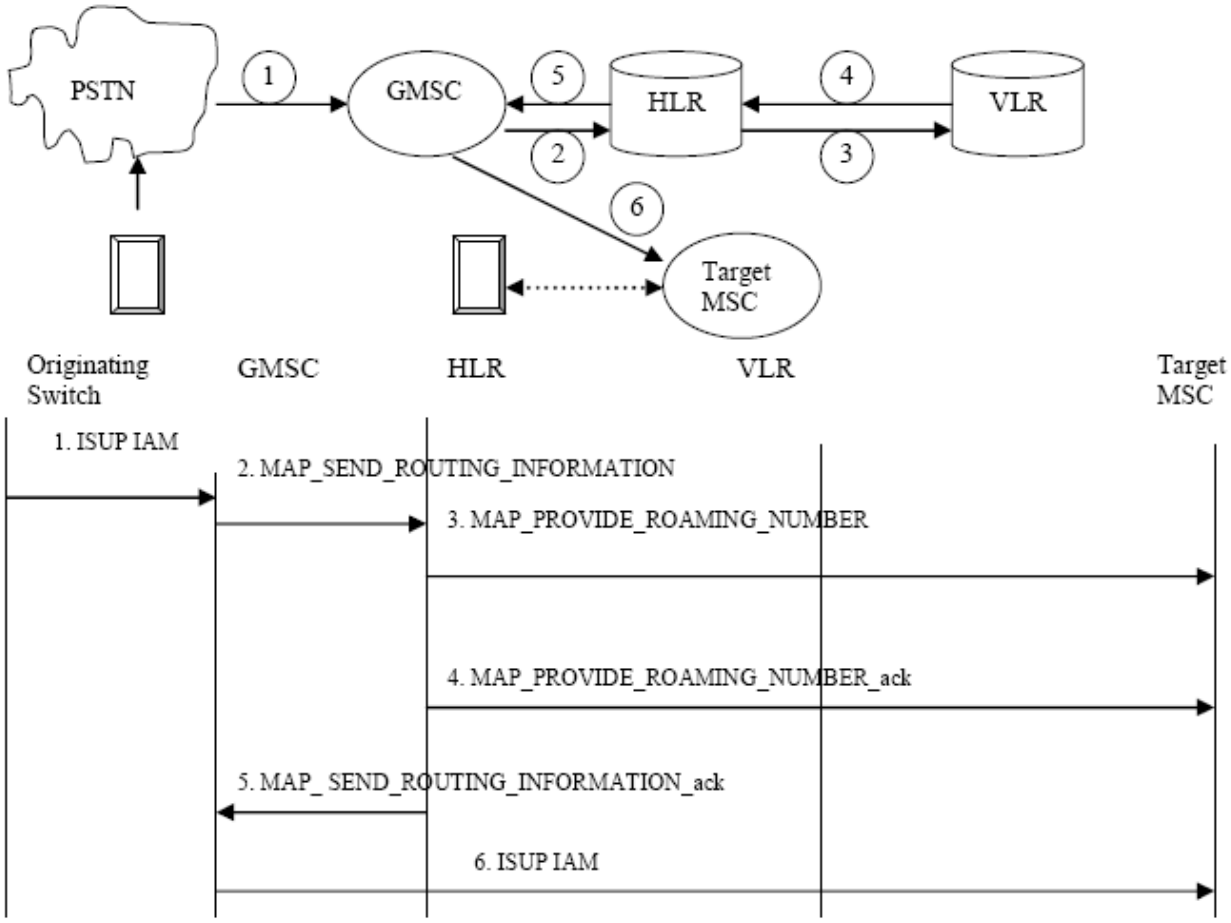


Fig 6.10 Call Termination Operation

GPRS (General Packet Radio Service)

GPRS is a packet oriented mobile data service available to users of the 2G cellular communication systems global system for mobile communications (GSM), as well as in the 3G systems. In the 2G systems, GPRS provides data rates of 56-114 kbit/s.

GPRS is a mechanism to transport high speed data over GSM.GPRS has the ability to offer data in small packet at speed of 14.4Kbps to 171.2Kbps.GPRS is a speed enhanced data transmission service designed for GSM system. Speed enhanced data transmission takes place by packetizing of data & simultaneous transmission of packets over different channels. GPRS standard is defined by ETSI (European Telecommunication Standard Institute).GPRS is a packet oriented service for mobile

data transmission and their access to internet. It uses unused slots and channels in TDMA mode of a GSM for packetized transmission from a mobile station.

GPRS upgrades GSM data services providing:

- Multimedia messaging service (MMS)
- Short message service (SMS)
- Push to talk over cellular (PoC/PTT)
- Instant messaging and presence—wireless village
- Internet applications for smart devices through wireless application protocol (WAP)
- Point-to-point (PTP) service: inter-networking with the Internet (IP)
- Future enhancements: flexibility to add new functions, such as more capacity, more users, new accesses, new protocols, new radio networks.

Architecture

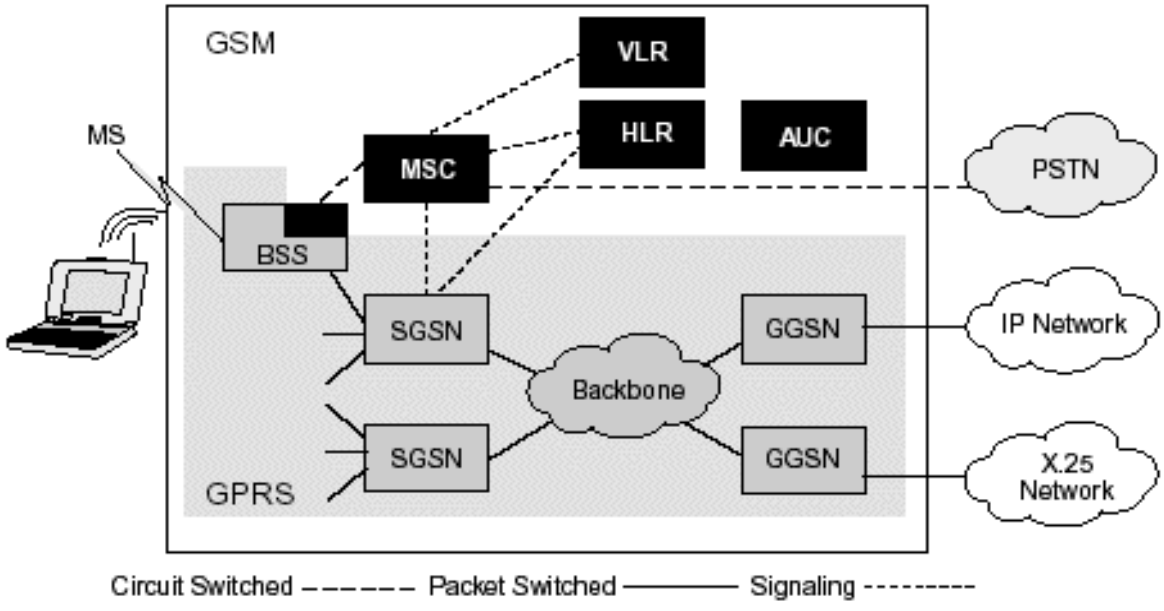


Fig 7.1 GPRS Architecture

GPRS uses GSM architecture for voice. GPRS supports a class of network nodes to offer packet data. These nodes are called as GPRS support nodes. GSN are responsible for delivery & routing of data packets between MS and external packet data network (PDN). An MS having GPRS capability stores CKSN (Cipher Key Sequence No) similar to cipher key stored in SIM & GSM. It also stores a TLLI (Temporary logical link identity) similar to TMSI. BSS system existing in the network needs enhancement to recognize and packet data. BTS also needs to be upgraded to support packet data transportation. HLR needs enhancement to register GPRS user profile and respond to queries originating from GSN.

The GPRS system brings some new network elements to an existing GSM network. These elements are:

Packet Control Unit (PCU)

The PCU separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively. It also performs most of the radio resource management functions of the GPRS network. The PCU can be either located in the BTS, BSC, or some other point between the MS and the MSC. There will be at least one PCU that serves a cell in which GPRS services will be available. Frame Relay technology is being used at present to interconnect the PCU to the GPRS core.

Serving GPRS Support Node (SGSN)

The SGSN is the most important element of the GPRS network. The SGSN of the GPRS network is equivalent to the MSC of the GSM network. There must at least one SGSN in a GPRS network. There is a coverage area associated with a SGSN. As the network expands and the number of subscribers increases, there may be more than one SGSN in a network.

Gateway GPRS Support Node (GGSN)

The GGSN is the gateway to external networks. Every connection to a fixed external data network has to go through a GGSN. The GGSN acts as the anchor point in a GPRS data connection even when the subscriber moves to another SGSN during roaming. The GGSN may accept connection request from SGSN that is in another

PLMN. Hence, the concept of coverage area does not apply to GGSN. There are usually two or more GGSNs in a network for redundancy purposes, and they back up each other up in case of failure.

Border Gateway

The Border Gateway (BG) is a router that can provide a direct GPRS tunnel between different operators' GPRS networks. This is referred to as an inter- PLMN data network. It is more secure to transfer data between two operators' PLMN networks through a direct connection rather than via the public Internet. The Border Gateway will commence operation once the GPRS roaming agreements between various operators have been signed. It will essentially allow a roaming subscriber to connect to company intranet through the Home GGSN via the visiting PLMN network.

Charging Gateway

GPRS users have to be charged for the use of the network. In a GSM network, charging is based on the destination, duration, and time of call. However, GPRS offers connectionless service to users, so it not possible to charge subscribers on the connection duration. Charging has to be based on the volume, destination, QoS, and other parameters of a connectionless data transfer. These GPRS charging data are generated by all the SGSNs and GGSNs in the network. This data is referred to as Charging Data Records or CDRs. One data session may generate a number of CDRs, so these need to collected and processed. The Charging Gateway (CG) collects all of these records, sorts them, processes it, and passes it on to the Billing System. Here the GPRS subscriber is billed for the data transaction. All CDRs contain unique subscriber and connection identifiers to distinguish it. A protocol called GTP' (pronounced GTP prime) is used for the transfer of data records between GSNs and the Charging Gateway.

GPRS interfaces

The GPRS system introduces new interfaces to the GSM network. Figure 4 illustrates the logical architecture with the interfaces and reference points of the combined GSM/GPRS network.

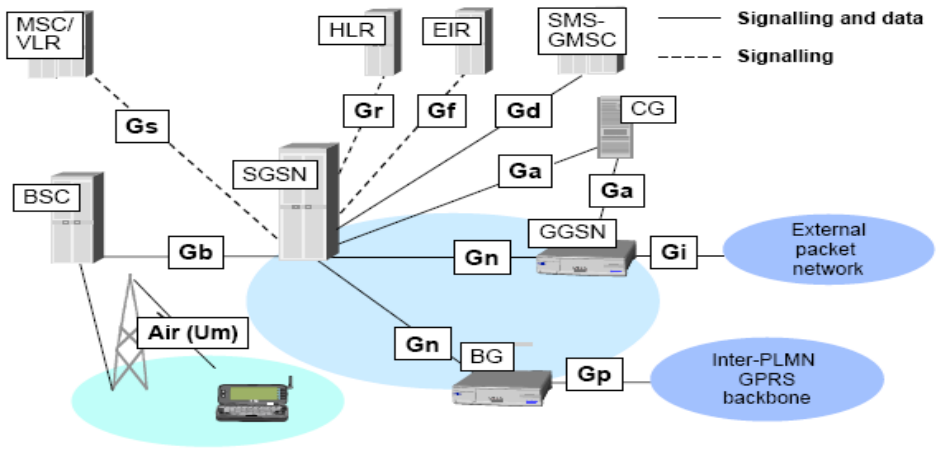


Figure 4. GPRS interfaces

The interfaces used by the GPRS system are described below:

- **Um** between an MS and the GPRS fixed network part. The Um is the access interface the MS uses to access the GPRS network. The radio interface to the BTS is the same interface used by the existing GSM network with some GPRS specific changes.
- **Gb** between a SGSN and a BSS. The Gb interface carries the GPRS traffic and signalling between the GSM radio network (BSS) and the GPRS network. Frame Relay based network services is used for this interface.
- **Gn** between two GSNs within the same PLMN. The Gn provides a data and signalling interface in the Intra-PLMN backbone. The GPRS Tunnelling Protocol (GTP) is used in the Gn (and in the Gp) interface over the IP based backbone network.
- **Gp** between two GSNs in various PLMNs. The Gp interface provides the same functionality as the Gn interface, but it also provides, together with the BG and the Firewall, all the functions needed for inter-PLMN networking, that is, security, routing, etc.
- **Gr** between an SGSN and the HLR. The Gr gives the SGSN access to subscriber information in the HLR. The HLR can be located in a different PLMN than the SGSN (MAP).

- **Ga** between the GSNs and the CG inside the same PLMN. The Ga provides a data and signalling interface. This interface is used for sending the charging data records generated by GSNs to the CG. The protocol used is GTP', an enhanced version of GTP.
- **Gs** between a SGSN and a MSC. The SGSN can send location data to the MSC or receive paging requests from the MSC via this optional interface. The Gs interface will greatly improve the effectiveness of the radio and network resources in the combined GSM/GPRS network. This interface uses BSSAP+ protocol.
- **Gd** between the SMS-GMSC and an SGSN, and between SMS-IWMSC and an SGSN. The Gd interface is available for more efficient use of the SMS services (MAP).
- **Gf** between an SGSN and the EIR. The Gf gives the SGSN access to GPRS user equipment information. The EIR maintains three different lists of mobile equipment: black list for stolen mobiles, grey list for mobiles under observation and white list for other mobiles (MAP).
- **Gc** between the GGSN and the HLR. The GGSN may request the location of an MS via this optional interface. The interface can be used if the GGSN needs to forward packets to an MS that is not active.

There are two different **reference points** in the GPRS network. The Gi is GPRS specific, but the R is common with the circuit switched GSM network:

- **Gi** between a GGSN and an external network. The GPRS network is connected to an external data networks via this interface. The GPRS not a standard interface, but merely a reference point.
- **R** between terminal equipment and mobile termination. This reference point connects terminal equipment to mobile termination, thus allowing, for example, a laptop-PC to transmit data over the GSM-phone. The physical R interface follows, for example, the ITU-T V.24/V.28 or the PCMCIA PC-Card standards.

GPRS Network Protocol

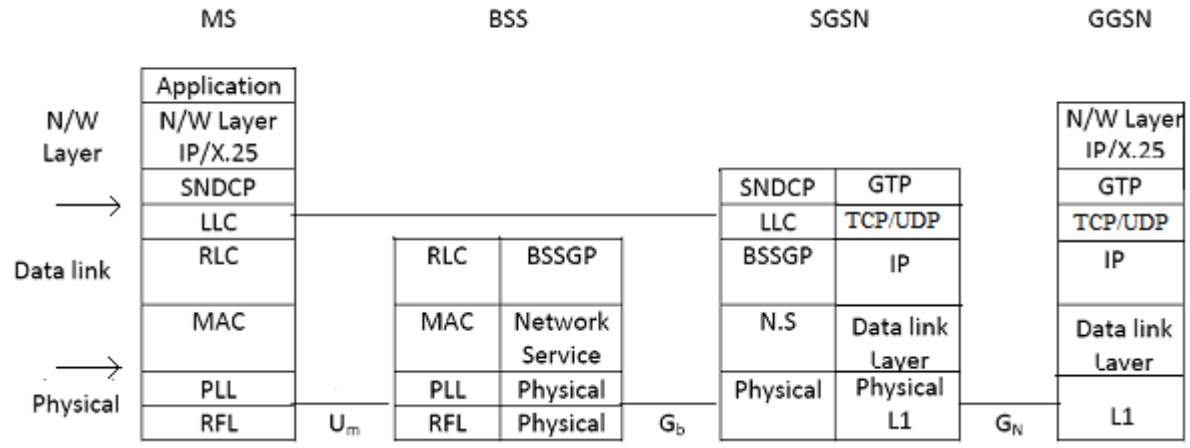


Fig 7.2 GPRS Networking Protocol

Abbreviations:

SNDCP: Subnetwork Dependent Convergence Protocol

LLC: Logical Link Control

RLC: Radio Link Control

MAC: Medium Access Control

PLL: Physical Link Layer

RFL: Radio Frequency LAYER

BSSGP: BSS GPRS Protocol

GTTP: GPRS Tunneling Protocol

TCP: Transmission Control Protocol

IP: Internet Protocol

Transmission protocols in the Um interface

A. Physical layer

The physical layer can be divided into the Radio Frequency (RF) layer and the Physical Link layer.

The Radio Frequency (RF) is the normal GSM physical radio layer. It performs the modulation of physical waveform based on sequence of bits received from PLL. RF layer specifies:

- the carrier frequency characteristics and GSM radio channel structures
- the radio modulation scheme used for the data
- the radio transmitter and receiver characteristics as well as performance requirements.

The Physical Link layer supports multiple MSs sharing a single physical channel and provides communication between the MSs and the network. Network controlled handovers are not used in the GPRS service. Instead, routing area updates and cell updates are used. The Physical Link layer is responsible for:

a. Forward Error Correction (FEC) coding, allowing the detection and correction of transmitted code words and the indication of incorrectable code words
b. the interleaving of one RLC Radio Block over four bursts in consecutive TDMA frames.

B. Medium Access Control (MAC)

The Medium Access Control (MAC) protocol handles the channel allocation and the multiplexing, that is, the use of physical layer functions. The RLC and the MAC together form the OSI Layer 2 protocol for the Um interface. The GPRS MAC function is responsible for:

- Providing efficient multiplexing of data and control signalling on both the uplink and downlink. This process is controlled by the network. On the downlink, multiplexing is controlled by a scheduling mechanism. Onusers (for example, in response to a service request).
- Mobile originated channel access, contention resolution between channel access attempts, including collision detection and recovery.
- Mobile terminated channel access, scheduling of access attempts, including queuing of packet accesses.

- Priority handling.

C. The Radio Link Control (RLC)

The Radio Link Control (RLC) protocol offers a reliable radio link to the upper layers. Two modes of operation of the RLC layer are defined for information transfer: unacknowledged and acknowledged. The RLC layer can support both modes simultaneously.

The RLC function is responsible for:

- Providing transfer of Logical Link Control layer PDUs (LLC-PDU) between the LLC layer and the MAC function.
- Segmentation and reassembly of LLC-PDUs into RLC Data Blocks. See Figure 2.
- Backward Error Correction (BEC) procedures enabling the selective retransmission of uncorrectable code words. This process is generally known as Automatic Request for Retransmission (ARQ).

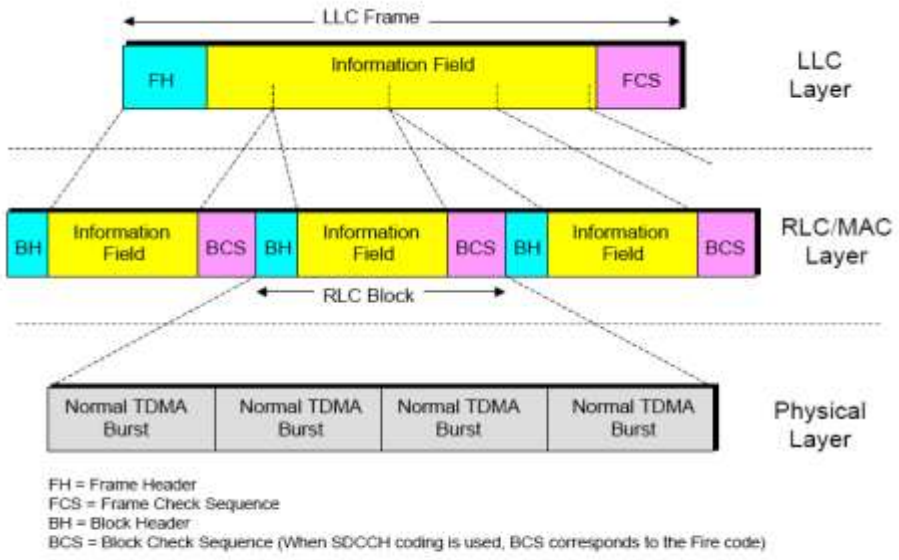


Figure 2. Segmentation of LLC-PDUs into RLC data blocks

D. Logical Link Control (LLC)

The Logical Link Control (LLC) layer offers a secure and reliable logical link between the MS and the SGSN for upper layer protocols, and is independent of the lower layers.

The LLC conveys signalling, SMS, and Subnetwork Dependent Convergence Protocol (SNDCP) packets. SNDCP exists between the MS and the SGSN and provides a mapping and compression function between the network layer (IP or X.25 packets) and the lower layers. It also performs segmentation, reassembly, and multiplexing.

Two modes of operation of the LLC layer are defined for information transfer: unacknowledged and acknowledged. The LLC layer can support both modes simultaneously.

- In acknowledged mode, the receipt of LLC-PDUs is confirmed. The LLC layer retransmits LLC-PDUs if confirmation has not been received within a certain timeout period.
- In unacknowledged mode, there is no confirmation required for LLU-PDUs.

Signalling and SMS is transferred in unacknowledged mode. In unacknowledged mode, the LLC layer offers the following two options:

- Transport of "protected" information means that if errors occur within the LLC information field, the frame will be discarded.
- Transport of "unprotected" information means that if errors occur within the LLC information field, the frame will not be discarded.

E. SNDCP (Subnetwork Dependent Convergence Protocol)

This is a convergence protocol used to transfer data packet and voice data between SGSN & MS through IP/X.25. Network layer protocols are intended to be capable of operating over a wide variety of subnetworks and data links. GPRS supports several network layer protocols providing protocol transparency for the users of the service. To enable the introduction of new network layer protocols to be transferred over GPRS without any changes to GPRS, all functions related to the transfer of Network layer Protocol Data Units (N-PDUs) are carried out in a transparent way by the GPRS network. This is one of the requirements of SNDCP. Another requirement of the SNDCP

is to provide functions that help to improve channel efficiency. This is achieved by means of compression techniques. The set of protocol entities above the SNDCP consists of commonly used network protocols. They all use the same SNDCP entity, which then performs multiplexing of data coming from different sources to be transferred using the service provided by the LLC layer.

A. Physical Layer Protocol

Several physical layer configurations and protocols are possible at the Gb interface and the physical resources are allocated by Operation & Maintenance (O&M) procedures. Normally a G703/704 2Mbit/s connection is provided.

B. Network Services layer

The Gb interface Network Services layer is based on Frame Relay. Frame Relay virtual circuits are established between the SGSN and BSS. LLC PDUs from many users are statistically multiplexed onto these virtual circuits. These virtual circuits may traverse a network of Frame Relay switching nodes, or may just be provided on a point to point link between the BSC and the SGSN (if the BSC and SGSN are co-located). Frame Relay is used for signalling and data transmission over the Gb interface.

C. Base Station System GPRS Protocol (BSSGP)

The Base Station System GPRS Protocol (BSSGP) transfers control and signaling information and user data between a BSS and the SGSN over the Gb interface.

The primary function of BSSGP is to provide Quality of Service (QoS), and routing information that is required to transmit user data between a BSS and an SGSN.

The secondary function is to enable two physically distinct nodes, the SGSN and BSS, to operate node management control functions. There is a one-to-one relationship between the BSSGP protocol in the SGSN and in the BSS. If one SGSN handles multiple BSSs, the SGSN has to have one BSSGP protocol device for each BSS.

A. Layer 1 and layer 2

The L1 and the L2 protocols are vendor dependent OSI layer 1 and 2 protocols that carry the IP datagrams for the GPRS backbone network between the SGSN and the GGSN.

B. Internet Protocol (IP)

The Internet Protocol (IP) datagram in the Gn interface is only used in the GPRS backbone network. The GPRS backbone (core) network and the GPRS subscribers use different IP addresses. This makes the GPRS backbone IP network invisible to the subscribers and vice versa. The GPRS backbone network carries the subscriber IP or X.25 traffic in a secure GPRS tunnel. All data from the mobile subscribers or external networks is tunnelled in the GPRS backbone.

C. TCP or UDP

TCP or UDP are used to carry the GPRS Tunnelling Protocol (GTP) PDUs across the GPRS backbone network. TCP is used for user X.25 data and UDP is used for user IP data and signalling in the Gn interface.

D. GPRS Tunnelling Protocol (GTP)

The GPRS Tunnelling Protocol (GTP) allows multi-protocol packets to be tunnelled through the GPRS backbone between GPRS Support Nodes (GSNs).GTP is defined both for the Gn interface, which is, the interface between GSNs within the same PLMN, and the Gp interface between GSNs in different PLMNs. The UDP/IP and TCP/IP are examples of paths that may be used to multiplex GTP tunnels. The choice of path is dependent on whether the user data to be tunnelled requires a reliable link or not. Two modes of operation of the GTP layer are therefore supported for information transfer between the GGSN and SGSN.

- unacknowledged (UDP/IP)
- acknowledged (TCP/IP).

A UDP/IP path is used when the user data is based on connectionless protocols, such as IP. A TCP/IP path is used when the user data is based on connection oriented protocols, such as X.25. The GTP layer can support both modes simultaneously.

Wireless LAN

WLAN is a LAN without wires. Mobile users can access information and network resources through LAN. The goal of WLAN is to replace office cabling to enable quicker access to internet and to higher flexibility communication. It is implemented as an extension to a wired LAN within a building or campus.

Wireless LAN Application

There are many area and applications of wireless LAN. Wireless LAN is best suited for dynamic environment. The applications are as follows:

- **Cross Building Interconnect –** Wireless can be used to connect LANs in nearby buildings. Here a point-to-point wireless link is used between two buildings. The devices connected are bridges and routers.
- **Nomadic Access –** It provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna such as laptop or notepad computer. Nomadic access is also useful in an extended environment such as a campus or a business operating out of a cluster of building.
- **Ad Hoc Networking –** An ad hoc network is a peer-to-peer network setup temporarily to meet some immediate need. For example, a group of employees, each with a laptop computer, may convene in a conference room for business. The employees link their computers in a temporary network just for the duration of the meeting.

Wireless LAN Requirements

A wireless LAN must meet the same sort of requirements typical of any LAN including high capability, ability to cover short distances and broadcast capability. There are also a number of requirements specific to wireless LAN environment. The following are the most important requirements:

- **Throughput:** The medium access control protocol should make as efficient use as possible of the wireless medium to maximize capacity.
- **Number of nodes**: Wireless LAN may need to support hundreds of nodes across multiple cells.

- **Connection to backbone LAN**: In case of Wireless LAN, an interconnection structure is required
- **Service area:** A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.
- **License free operation:** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.
- **Handoff/roaming:** The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.
- **Dynamic configuration:** the MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion and relocation of end systems without disruption to other users.
- **Battery power consumption**: Mobile workers use battery powered workstations that need to have a long battery life when used with wireless adapters. Wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.

Wireless LAN Advantages

- **Mobility:** Productivity increases when people have access to data and information from any location.
- **Low Implementation Cost:** WLANs are easy to set up, relocate, change and manage.
- **Installation Speed and Simplicity:** Installing a WLAN can be fast and can eliminate the need to install cable through walls.
- **Network Expansion:** Wireless Technology allows the network to reach where wires can not reach.
- **Reliability:** WLAN is resistant to different types of cable failures.
- **Scalability:** WLAN can be configured in a variety of topologies to meet the needs of specific applications and installations.
- **Usage of ISM band:** WLAN operates in the unregulated ISM bands available for use by anyone.

Wireless LAN Technology

Wireless LANs are generally categorized according to the transmission technique that is used. Current wireless LAN products fall into one of the following categories:

- **Infrared (IR) LANs:** An individual cell of an IR LAN is limited to a single room, because infrared light does not penetrate opaque walls. Three transmission techniques are used for IR data transmission. (i). Direct beam IR can be used to create point-to-point links. In this mode the range depends on the emitted power and on the degree of focusing. (ii) An omni directional configuration involves a single base station that is within line of sight of all other stations on the LAN. Typically this station is mounted on the ceiling. (iii) In diffused configuration, all of the IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling. IR radiation striking the ceiling is reradiated omnidirectionally and picked up by all of the receivers in the area.
- **Spread Spectrum LANs:** This type of LAN makes use of spread spectrum transmission technology. In most cases, these LANs operate in the ISM frequency bands.

  Spread spectrum LAN makes use of a multiple cell arrangement. With in a cell, the topology can be either hub or peer to peer. In a hub topology, the hub is typically mounted on the ceiling and connected to a backbone wired LAN to provide connectivity to stations attached to the wired LAN and to stations that are part of wireless LANs in other cells. A peer-to-peer technology is one in which there is no hub. A MAC algorithm such as CSMA is used to control access.
- **Narrowband microwave:** These LANs operate at microwave frequencies but do not use spread spectrum. The term narrowband microwave refers to the use of a microwave radio frequency band for signal transmission with relatively narrow bandwidth.

Types of WLAN

- **IEEE 802.11**: In June 1997, IEEE finalized the initial specification for WLAN. It specifies 2.4 GHz frequency band with data rate of 2Mbps.This standard evolved into many variations using different encoding technologies.
- **HYPER LAN**: It began in Europe in 1996 by ETSI (European Telecommunication Standard Institute).ETSI broadband radio access network group. The current version Hyper LAN/1 works at 5 GHz frequency band and offers up to 24 Mbps bandwidth.
- **BLUETOOTH**: It is promoted by big industry leaders like IBM, ERICSON, NOKIA. It was named after Harold Bluetooth, king of Denmark. It offers 1Mbps data rate at 2.2 GHz band. It is also known as PAN (Personal area network).
- **MANET**: It is a working group to investigate and develop the standard for mobile ad-hoc network (MANET).

IEEE 802.11

The IEEE standard 802.11 specifies the most famous family of WLANs in which many products are available. The number in the standard indicates, it belongs to the group of 802.X LAN standards. The primary goal of the standard was the specification of a simple and robust WLAN which offers time bounded and asynchronous services.

Architecture

The smallest building block of a WLAN is a basic service set (BSS) which consist of some number of stations executing the same MAC protocol. A BSS may be isolated or it may connect to a backbone distribution system (DS) through an access point (AP). The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another. If one station in BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from originating station to the AP and from AP tp destination station.

When all the stations in the BSS are mobile stations, with no connection to other BSSs, the BSS is called an independent BSS (IBSS). An IBSS is an ad hoc network.

An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system. The distribution system is a wired backbone LAN but can be any communication network. The ESS appears as a single logical LAN to the logical link control level.

An access point is implemented as part of a station. The AP is the logic within a station that provides access to the DS by providing DS services in addition to acting as a station.

A Wireless networks can exhibit two different basic system architecture. WLAN are of 2 types:

- Infrastructure mode
- Ad-hoc mode

Infrastructure Mode

Here, MSs are connected with BS or access point. This is similar to star network communication takes place between wireless nodes and access point but not directly between wireless devices. Here access points acts as a bridge to other network.

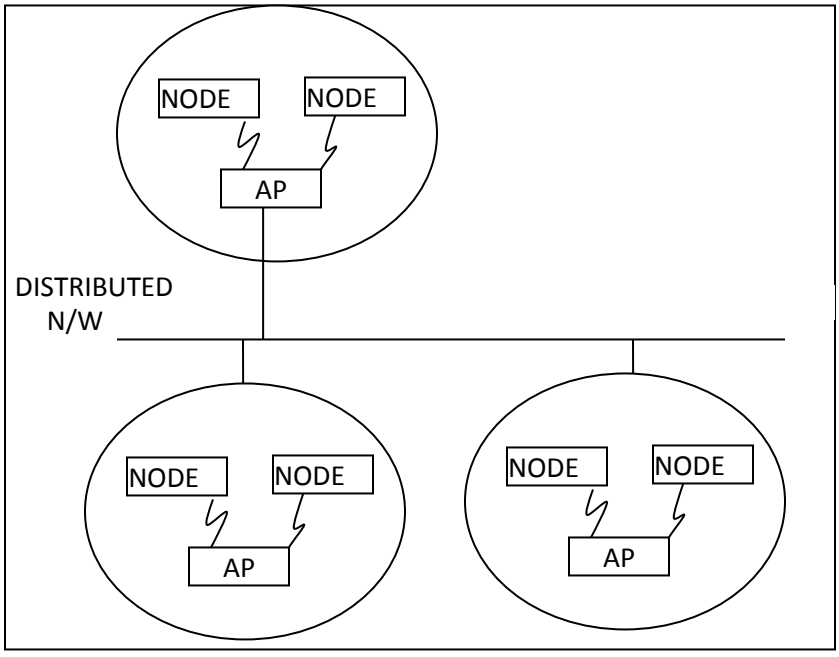


Fig 9.1 WLAN in Infrastructure Mode

Ad-hoc Mode

In ad-hoc mode there is no access point. A number of MS can communicate directly with each other. Nodes can communicate if they can reach each other physically i.e. they are given each other radio range.

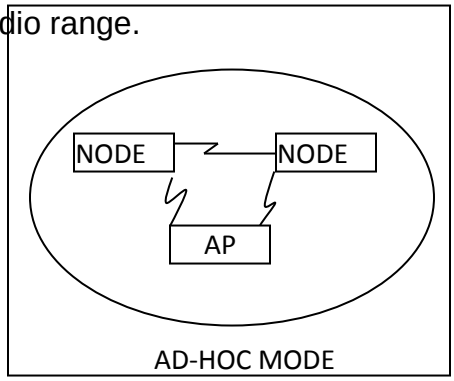


Fig 9.2 WLAN in Ad-hoc mode

IEEE 802.11 Services

IEEE 802.11 defines the following services that need to be provided by the Wireless LAN.

- **Distribution:** It is the primary service used by stations to exchange MAC frames when the frame must traverse the Ds to get from a station in one BSS to a station in another BSS.
- **Integration:** This service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN. The term integrated refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via integration services. The integration service takes care of address translation, media conversion logic required for exchange of data.
- **Association:** Establishes an initial association between a station and an AP.Before a station can transmit or receive frames on a wireless LAN, its identity and address must be known. For this purpose, a station must establish an association with an AP within a particular BSS. The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of address frames.

- **Reassociation:** Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
- **Disassociation:** A notification from either a station or an AP that an existing association is terminated. A station gives this notification before leaving an ESS or shutting down.
- **Authentication:** Used to establish the identity of stations to each other. This authentication service is used by stations to establish their identity with stations they wish to communicate with.
- **Deauthentication:** This service is invoked whenever an existing authentication is to be terminated.
- **Privacy:** Used to prevent the contents of message from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

Protocol Architecture

The protocol architecture of 802.11 consists of two layers physical layer and MAC layer. The physical layer is subdivided into physical layer convergence protocol (PLCP) and physical medium dependent sub layer (PMD). The basic task of MAC layer comprise medium access, fragmentation of user data, encryption. The PLCP layer provides carrier sense signal called clear channel assessment. It delivers the incoming frame from wireless medium to MAC protocol Data unit (MPDU) for data transfer. PMD layer handles modulation and encoding or decoding of signals. It provides the actual transmission and reception of physical layer entity between MS through wireless medium.

<table>
<tr><td colspan="3">802.11 MAC Management</td><td>MAC Layer</td><td>Data Link Layer</td></tr>
<tr><td>Frequency</td><td>Direct</td><td>Infrared</td><td>PLCP sub layer</td><td>Physical Layer</td></tr>
</table>

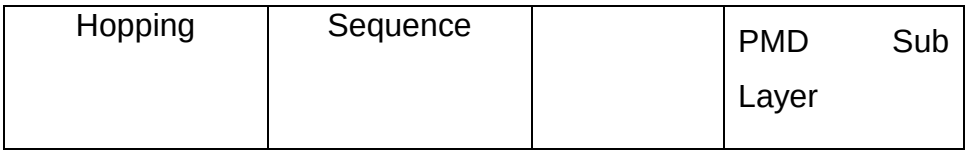


Fig 9.3 IEEE 802.11 protocol architecture

Physical Layer

IEEE 802.11 supports three different physical layers: one layer based on infra red and two layers based on radio transmission. All PHY variants include the provision of the clear channel assessment signal (CCA).This is needed for the MAC mechanisms controlling medium access and indicate if the medium is currently idle. The PHY layer offers a service access point (SAP) with 1 or 2 Mbits/transfer rate to the MAC layer.

Frequency hopping spread spectrum

Frequency hopping spread spectrum (FHSS) is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences.

The standard specifies Gaussian shaped FSK (frequency shift keying), GFSK, as modulation for the FHSS PHY. For 1 Mbits/s a 2 level GFSK is used, for 2Mbits/s a 4 level GFSK is used.

Figure shows a frame of the physical layer used with FHSS. The frame consists of two basic parts, the PLCP part (permeable and header) and the pay load part. While the PLCP part is always transmitted at 1Mbit/s, payload can use 1 or 2 Mbit/s.

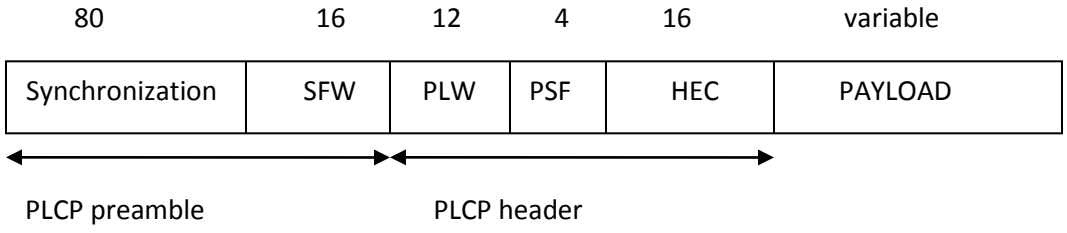


Fig 9.4 IEEE 802.11 PHY frame using FHSS

The field of the frame fulfills the following functions:

Synchronization: The PLCP permeable starts with 80 bit synchronization, which is a 010101….bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the CCA.

Start frame delimiter (SFD): The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is 0000110010111101.

PLCP_PDU length word (PLW): This first field of the PLCP header indicates the length of the payload in bytes including the 32 bit CRC at the end of the payload.PLW can range between 0 and 4095.

PLCP signaling field (PSF): This 4 bit field indicates the data rate of the payload following. All bit set to zero (0000) indicates the lowest data rate of 1Mbit/s, 2 Mbit/s is indicated by 0010 and the maximum is 8.5 Mbit/s (1111).

Header error check (HEC): PLCP header is protected by a 16 bit checksum

Direct sequence spread spectrum

Direct sequence spread spectrum (DSSS) is the alternative spread spectrum method separating by code and not by frequency.IEEE 802.11 DSSS PHY uses the 2.4 GHz ISM band and offers both 1 and 2 Mbit/s data rates. The system uses differential binary phase shift keying(DBPSK) for 1 Mbit/s transmission and differential quardrature phase shift keying(DQPSK) for 2 Mbit/s as modulation schemes.

Figure shows a frame of the physical layer using DSSS.The frame consists of two parts, one the PLCP part and the other Payload part while the PLCP part is always transmitted at 1Mbit/s,payload,.i.e MAC data can use1 or 2 Mbit/s.

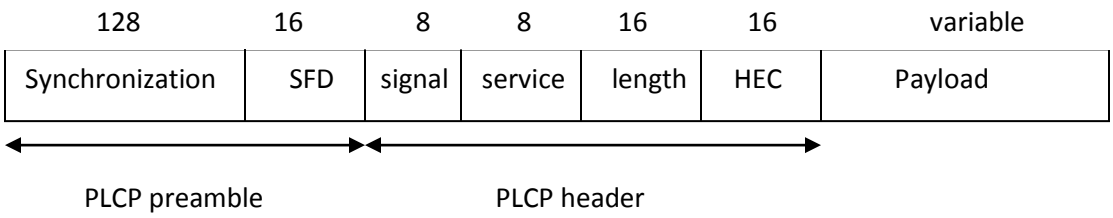


Fig 9.5 IEEE 802.11 PHY frame using DSSS

The field of the frame fulfills the following functions:

- **Synchronization:** The first 128 bits are used for synchronization, energy detection, frequency offset compensation. The synchronization field only consists of scrambled 1 bit.
- **Start frame delimiter (SFD):** This 16 bit field is used for synchronization at the beginning of the frame and consists of the pattern 1111001110100000.
- **Signal:** The values in this field indicate the data rate of the payload. The value 0x0A indicates 1 Mbit/s, 0x14 indicates2 Mbit/s. Other values have reserved for further use i.e. higher bit rates.
- **Service:** This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 complaint frame.
- **Length:** 16 bits are used for length indication of the payload in microseconds.
- **Header error check (HEC):** Signal, service and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomials.

Infra-red

The PHY layer based on infra-red (IR) transmission uses near visible light at 850-950 nm. Infra- red light is not regulated apart from safety restrictions (using lasers insteaded of LEDs).The standard does not require a line of sight between sender and receiver, but should also work with diffuse light. This allows for point-to-multipoint communications. The maximum range is about 10m if no sunlight or heat sources interfere with the transmission. Typically such a network will only work in buildings, e.g.-class rooms, meeting rooms etc.

Frequency reuse is very simple-a wall is more than enough to shield one IR based IEEE 802.11network from another.

MAC Layer

MAC layer is responsible for controlling the access medium, roaming, authentication, power conservation etc. The basic services provided by MAC layer are mandatory asynchronous data service and optional time bound service. Asynchronous data service

is provided in ad-hoc network medium and both services are available in infrastructure mode.

Access mechanisms defined under IEEE 802.11 are as follows:

- Carrier Sense Multiple Access with collision Avoidance
- Request to Send/ Clear to Send

These methods are called as Distributed Coordination Function (DCF) and offers asynchronous service.

Access mechanism using CSMA/CA

The mandatory access mechanism is based on carrier sense multiple access with collision access CSMA/CA. It employs a random back off mechanism with carrier sense and collision avoidance to reduce the probability of collision between 2 frames. The mechanism behind CSMA/CA is as follows:

- When a wireless station wants to communicate, it first listens to its media to check if it can sense radio wave from any other station.
- If the medium is free for a specified time then the station is allowed to transmit. This time interval is called Distributed Inter Frame Space (DIFS).
- If the current device senses carrier signal of another device on the same frequency, it does not transmit and initiates a random timeout.
- After the timeout has expired, the wireless station again listens to the radio spectrum and if it still senses another station transmitting, initiates another random time out.
- When it does not sense another wireless station transmitting, it starts transmitting its own carrier signal to communicate with other station.
- The receiving station checks the CRC of the received packet and sends an acknowledgement. Receipt of the acknowledgement indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgement then it retransmits the fragments until it receives acknowledgement.

Access mechanism using RTS/CTS

This mechanism is used to solve the problems of hidden terminals. This problem occurs if one station can receive two others, but those stations can not receive each other. The two stations may sense the channel is idle, send a frame and cause a collision at the receiver in the middle. In order to reduce the probability of two stations colliding because they can't sense each other's presence, the standard defines a mechanism called Virtual Carrier Sense (VCS).

- A station wants to transmit a packet first transmits a short control packet called RTS (Request to send) which includes source, destination and duration of transaction.
- The destination station after receiving this request packet responds with a response control packet called CTS (CLEAR TO SEND), which includes same duration information.
- All stations receiving either RTS of CTS set their virtual carrier sense indicator called Network Allocation Vector (NAV) for the given duration and uses this information together with physical carrier sense when sensing the medium. This mechanism reduces the probability of a collision on the receiver side by a station.
- The transmitter station when receives the CTS after sending a RTS; it reserve the medium busy until the end of transaction.

MAC Frames

Figure shows the basic structure of an IEEE 802.11 MAC frame.

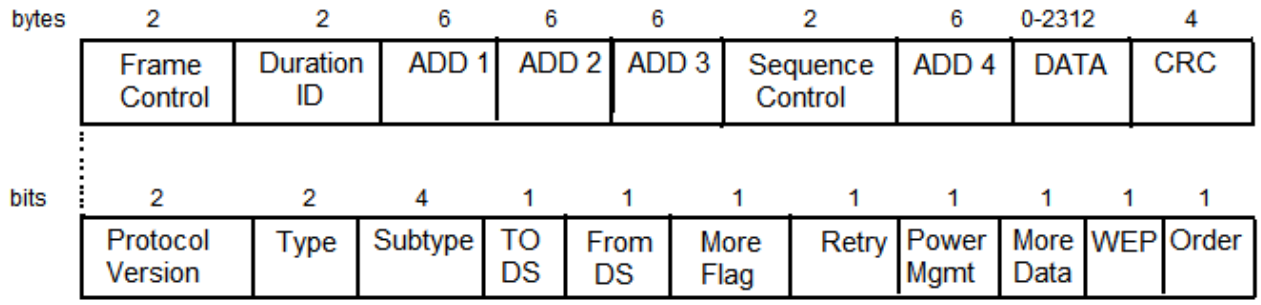


Fig 9.6 IEEE 802.11 MAC packet structure

- **Frame Control:** It is of two bytes and contains several sub-fields.
    1. **Protocol Version:** It is of two bit and indicate current protocol version.
    2. **Type**: This field determines function of a frame. For example: management (00), control (01), data (10)
    3. **Subtype:** If the above frame type is again sub-divided into various types. Ex- RTS is a control frame with sub type 1011.
    4. **To DS/From DS:** Frames can be transmitted between MS and AP. This field contains the address of source and destination Distributed system.
    5. **More Fragment**: This field is set to 1 if frames are of type data and management.
    6. **Retry:** If current frame is a retransmission of a earlier frame then this bit is set to 1.
    7. **Power Management:** This field indicates the power of a station after successful transmission of a frame .If one station is in power same mode.
    8. **More data:** This field is used to indicate a receiver that a sender has more data to send.
    9. **Wired Equivalent Privacy (WEP):** This field indicates the standard security mechanism of 802.11.
    10. **Order**: If this bit is set to 1 then the received frame must be processed in strict order.
- **Duration ID:** Indicating the period of time in which the medium is occupied for frame transfer.
- **Address 1 to 4:** The four address field contains IEEE802.MAC address.
- **Sequence Control**: A sequence no is maintained to filter duplicate frames.
- **Data**: MAC frame may contain arbitrary data, which is transferred from sender to receiver.
- **Checksum (CRC):**32 bit checksum is used to protect the frames.

MAC frames are of various types

Control Frame: Control frames assist in the reliable delivery of data frames. There are six types of control frame:

- **Power save-Poll (PS-Poll):** This frame is sent by any station to the station that includes the access point. Its purpose is to request that the AP (access point) transmit a frame that has been buffered for this station while the station was in power saving mode.
- **Request to Send (RTS):** This is the first frame in the four way frame exchange. The station sending this message is alerting a potential destination, and all other stations within reception range that it intends to send a data frame to that destination.
- **Clear to Send (CTS):** This is the second frame in the four way exchange. It is sent by the destination station to the source station to grant permission to send a data frame.
- **Acknowledgement:** Provides an acknowledgement from the destination to the source that the immediately preceding data, management, or PS-poll frame was received correctly.
- **Contention-free (CF)-End**: Announces the end of a contention-free period that is part of the point co-ordination function.
- **CF-End + CF-Ack**: Acknowledges the CF-End. This frame ends the contention-free period and releases stations from the restrictions associated with that period.

Data Frames: There are 8 data frame sub-types, organized into two groups. The first 4 subtypes define frames that carry upper level data from the source station to the destination station. The 4 data-carrying frames are as follows:

- **Data:** This is the simplest data frame. It may be used in both a contention period and a contention-free period.
- **Data + CF-Ack:** May only be sent during a contention-free period .In addition to carrying data, this frame acknowledges previously received data.

- **Data + CF-Poll:** Used by a point coordinator to deliver data to a mobile station and also to request that the mobile station send a data frame that it may have buffered.
- **Data + CF-Ack + CF-Poll:** Combines the functions of the Data + CF-Ack and Data + CF-Poll into a single frame.

MAC Management

- **Synchronization:** Function to support finding a wireless LAN, synchronization of internal clock.
- **Power Management:** Function to control transmitter activity for power conservation without missing a frame.

  The basic idea of power management is to switch off transceiver whenever it is not needed. The idea of power saving includes two states for a station: sleep and awake, and buffering of data in senders. If a sender intends to communicate with a power saving station it has to buffer data if the station is asleep. The sleeping station has to wake up periodically and stay awake for a certain time. During this time, all senders can announce the destinations of their buffered data frames. If a station detects that it is a destination of a buffered packet it has to stay awake until transmission takes place.
- **Roaming:** Moving between access points is called roaming. Steps for roaming between access points are:

  1. A station decides that the current link quality to its access point AP1 is too poor. The station then starts scanning for another access point.
  2. Scanning involves the active search for another BSS and can be used for setting up a new BSS. Scanning is of two types. Passive scanning means listening into the medium to find other networks. Active scanning comprises sending a probe on each channel and waiting for a response. Probe response contains the necessary information to join the new BSS.

3. The station then selects best access point for roaming based on signal strength and sends an association request to the selected access point AP2.
4. The new association point AP2 answers with an association response. If the response is successful, the station has roamed to the new access point.
5. The access point accessing an association request indicates the new station in its BSS to the distribution system. The DS then updates its database, which contains the current location of the wireless station.

Internet Protocol

The **Internet Protocol** (**IP**) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

The Internet Protocol (IP) is the protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Network Layer.

IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP Protocols. IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service. The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IPv6

The Internet Engineering Task Force (IETF) introduced a specification in 1995 for a next generation IP, known as IPng. This specification was turned into a standard in 1996 known as IPv6. IPv6 provides a number of functional enhancements over the existing IP. It was designed to accommodate high speed networks, support of mix of data stream including graphics and video etc. Ipv6 uses 128-bit address to specify source and destination.

Mobile IP

It is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

A standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address.

Mobile IP was developed to enable computers to maintain Internet Connectivity while moving from one Internet attachment point to another. When a user leaves the network with which his device is associated (home network) and enters the domain of a foreign network, the foreign network uses the Mobile IP protocol to inform the home network of a care-of address to which all packets for the user's device should be sent.

Goals of mobile IP

The major goals of mobile IP were as follows:

- To continue to work with the exiting TCP/IP protocol suite.
- To provide Internet wide mobility, allowing a host the same IP address, called ‘home address’.
- To optimeze local area mobility without sacrificing performance or functionality of the general case.
- To leave the transport layer and higher protocols untouched.
- To ensure that no application needs to change in order to run on or to be used from mobile hosts(MHs)
- To ensure theat the infrastructure, that is , non-MH, routers, routing protocols, etc are not changed either.
- To see the mobility is handled at the network layer.
- To ensure that the sollution scales well and minimizes potential points of failure, and
- To ensure mimimum power consumption, since mobile nodes are likely to be battery powered.

Operation of Mobile IP

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP. When the mobile node moves its attachment point to another network, that network is considered as a foreign network for the host.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address for sent packets. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent. The home agent looks for the care-of address (CoA) in a special table known as a binding table, and then tunnels the packets to the mobile node's care-of address by appending a new IP header to the original IP packet, which preserves the original IP header. The packets are decapsulated at the end of the tunnel to remove the IP header added by the home agent, and are delivered to the mobile node.

When acting as transmitter, mobile node simply sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network else the packets will be discarded by the router.

When IP datagrams are exchanged over a connection between the mobile node and another host following operation takes place

1. Server X transmits an IP datagram destined for mobile node A, with A’s home address in the IP Address. The IP datagram is routed to A’s home network.

2. At the home network, the incoming IP datagran is intercepted by home agent. The home agent encapsulates the entire datagram inside a new IP datagram and retransmits the datagram. This datagram is routed to the foreign agent.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network level PDU and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it uses X's IP address. Each datagram is sent by A to a router on the foreign network for routing to X.
5. The IP datagram from A to X travels directly across the internet to X, using X's IP address.

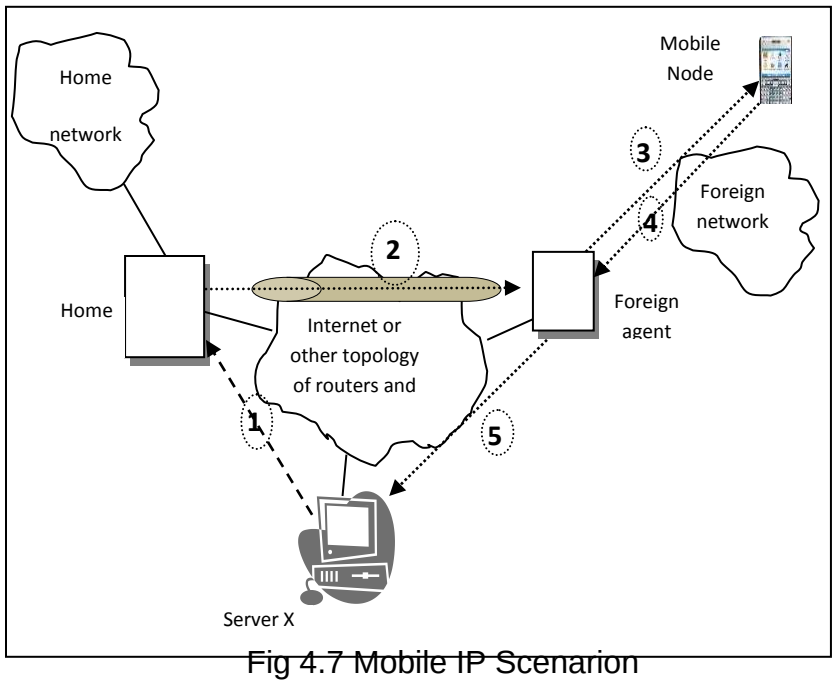


Fig 4.7 Mobile IP Scenarion

To support the operations given in the figure, Mobile IP includes three basic capabilities:

Discovery: A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.

The mobile node is responsible for an ongoing discovery process. It must determine the case(in home network or in foreign network) in which IP datagrams may be received without forwarding. As handoff from one network to another occurs at physical layer, a transition from home network to foreign network can occur at any time without notification to the network layer. For discovery a router can act as an agent to issue router advertisement ICMP message. The router advertisement message includes the IP address of the router and router's role as an agent. A mobile node listens for these agent advertisement messages. Because a foreign agent could be on mobile node's home network, the arrival of an agent advertisement does not necessarily tell the mobile node that it is on a foreign network. The mobile node must compare the network portion of the router's IP address with the network options of its own home address. If these network potions donot match, then mobile node is on a foreign network.

Registration: A mobile node uses an authenticated registration procedure to inform its home agent of its care of address.

Once a mobile node has recognized that it is on a foreign network and has acquired a care-of-address, it need to alert a home agent on its home network and request that the home agent forward its IP traffic. The registration process involves four steps:

1. The mobile node requests the forwarding service by sending a registration request to the foreign agent that mobile node wants to use.
2. The foreign agent relays this request to the mobile node's home agent.
3. The home agent either aceepts or denies the request and sends a registration reply to the foreign agent.
4. The foreign agent relays this reply to the mobile node.

Tunneling: It is used to forward IP datagrams from a home address to care-of-address.

Once a mobile node is registered with a home agent, the home agent must be able to intercept IP datagrams sent to the mobile node's home address so that these

datagram can be forwarded via tunneling. The home agent needs to inform other nodes on the same network that IP datagrams with a destination address of the mobile node should be delivered to this agent. To forward an IP datagram to a care-of-address, the home agent puts the entire IP datagram into an outer datagram by making encapsulation.

MODULE-II

WAP (Wireless Application Protocol)

WAP is a universal open standard developed by the WAP forum to provide mobile users of wireless phones and other wireless terminals. WAP standard represents the first successful attempt to establish a broadly accepted environment for delivering information, data and services to both enterprise and consumer users over wireless networks. WAP is based on existing internet standard such as IP, XML, HTML and HTTP. It also includes security features.

WAP Architecture

The WAP standard is a set of standards which together define how wireless data handset communicates with the wireless network and how contents and services are delivered and executed to their handsets. Using these standards the handset can establish a connection to a WAP data infrastructure, request content and services from infrastructure. WAP is based on layered architecture. The WAP stack is similar to the OSI network model. The architecture consists of a set of services encompassing network protocol, security and application environment. The WAP standard is layered i.e. one layer rests on top of another and therefore depend on another to provide services. Each layer in the network infrastructure are exposed to the interface layer above it and also exposed an interface directly to application and services. These layers are symmetric i.e. they run both on the client device and network infrastructure.

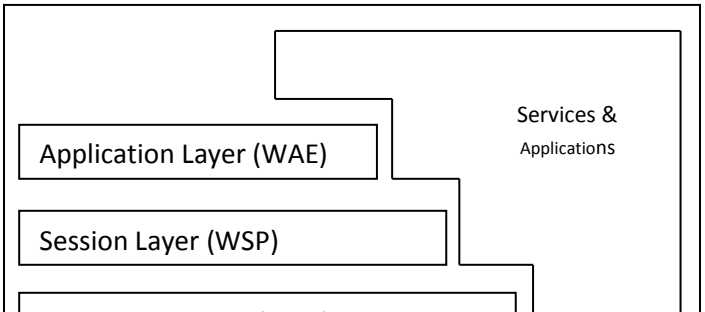


Fig 11.1 WAP Protocol Stack

Components of WAP Standard

Bearer Adaptation

Wireless networks employ a variety protocols for exchanging messages, packets, or frames to and from the client device. Dozens of these network protocols, also known as bearer protocols, exist. Each bearer protocol is associated with a particular type of network infrastructure, and each type of infrastructure typically associated with a particular set of suppliers or with particular regions of the world. Examples of various bearers are AMPS, CDPD, CDMA, GSM etc

WDP (Wireless Datagram Protocol)

The transport layer protocol in the WAP architecture is referred to as WDP. This layer operates above the bearer services and offers a consistent service to upper layers. WDP offer similar functions like UDP through T-SAP.

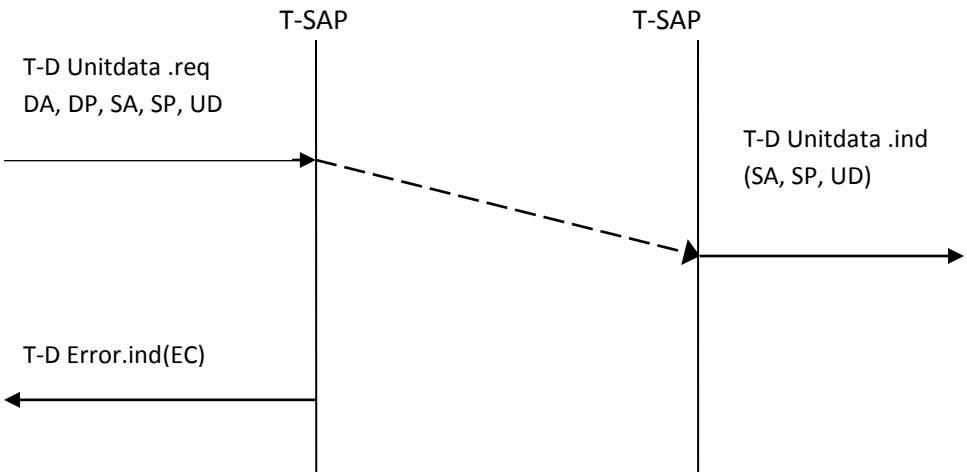


Fig 11.2 WDP Service Primitives

WDP offers source and destination port numbers used for multiplexing and demultiplexing of data .The service is initiated by sending a datagram. T-D Unitdata.req with Destination Address (DA), Destination Port (DP), Source Address (SA), Source Port (SP) and user data (UD). DA and SA are unique address of receiver and sender which may IP address or PSTN number. T-D Unitdata.ind service indicates the reception of data. Here DA, DP are optional. If that request can't be fulfilled by WDP, then an error is indicated with T-D Error.ind service. An error code (EC) is returned indicating reason for the error to higher layer. If any error occurs due to unsuccessful transmission of WDP data grams then WDP uses an error control mechanism known as WCMP (Wireless Control Message Protocol).WCMP is used by WDP nodes to report errors.

WTLS (Wireless Transport Layer Security)

WTLS is a security protocol based on TLS. If requested by an application, a security service (WTLS), can be integrated into the WAP architecture on top of WDP.

WTLS can provide different levels of security for privacy, authentication, and data integrity. WTLS takes into account the low processing power and very limited memory capacity. WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and connection oriented transport layer protocols.

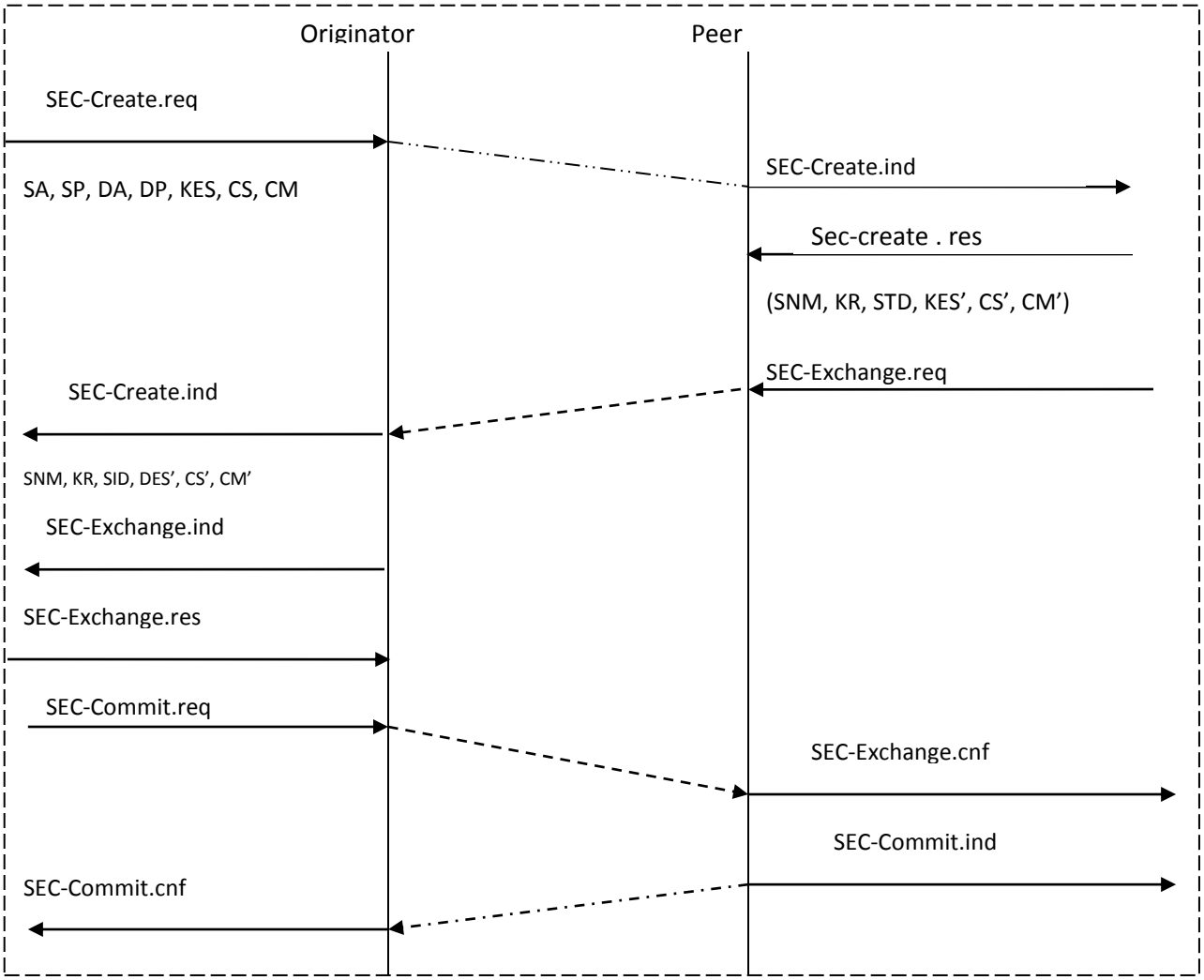


Fig 11.3 Establishment of Secure Session in WTLS

WTLS divides the whole transaction by two sections: originator and peer. First step is to initiate the session with SEC-Create.req. Parameters are SA, SP of the originator and DA, DP of peer. The originator proposes a key exchange suite KES (e.g. RSA), a cipher suit (CS) (for ex: DES), a compression method CM. The peer answers with parameter for SNM (Sequence Number Mode), KR (Key Refresh) cycle (i.e how after keys are refreshes within this secure session), the SID (session identifier) which is unique with each peer and DES', CS', CM'. Peer issues a SEC-exchange primitive. This indicates that peer wishes to perform public key authentication with the client i.e peer request a certificate from the originator.

In the first step of secure session, the negotiation of the security parameters is indicated on the originator's side followed by the request for a certificate. The originator answers with its certificate and issues a SEC-Commit.req primitive. This primitive indicates that the handshake is completed for originator's side and originator want to switch into new transaction .The certificate delivered to the peer side and SEC-Commit is indicated. This concludes the full handshake for secure session setup. After setting up a secure connection between two peers, user data can be exchanged. This is done using SEC-Unitdata primitive.

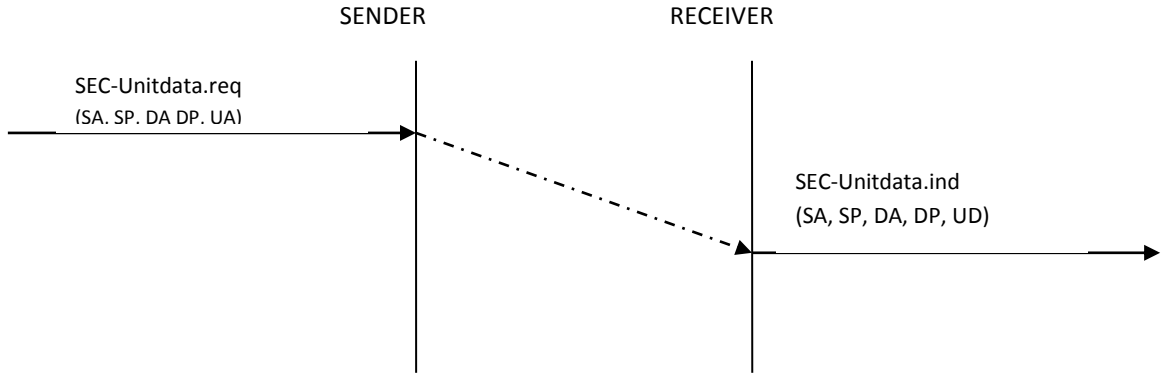


Fig 11.4 WTLS Datagram Transfer

WTP (Wireless Transaction Protocol)

WTP runs on top of a datagram service and provides transaction oriented protocol that is suitable for implementation in thin clients such a s mobile phones. WTP offers following advantages:

- Improved reliability over datagram services
- Improved efficiency over connection oriented services.
- Support for Transaction oriented services.

WTP supports three classes of transaction service:

- Class 0: Unreliable with no result message
- Class 1: Reliable with no result message
- Class 2: Reliable with one result message

WTP achieves reliability using duplicate removal, retransmission, acknowledgements and unique transaction identifier. WTP allows for asynchronous transaction, abort of transaction, concatenation of messages and can report success or failure of reliable messages. For reliable transmission of messages three service primitives are offered by WTP are as follows:

- TR-invoke: It is used to initiate a transaction.
- TR-result: It is used to send back a result of a previously initiated transaction.
- TR-abort: It is used to abort a normal transaction.

WTP Class-0 (Unreliable with no result message)

It offers an unreliable transaction service without a result message. The transaction is stateless and can not be aborted. The service is requested with TR-invoke. The parameters used in the request are Source Address (SA), Destination Address (DA), Source Port (SP), and Destination Port (DP).

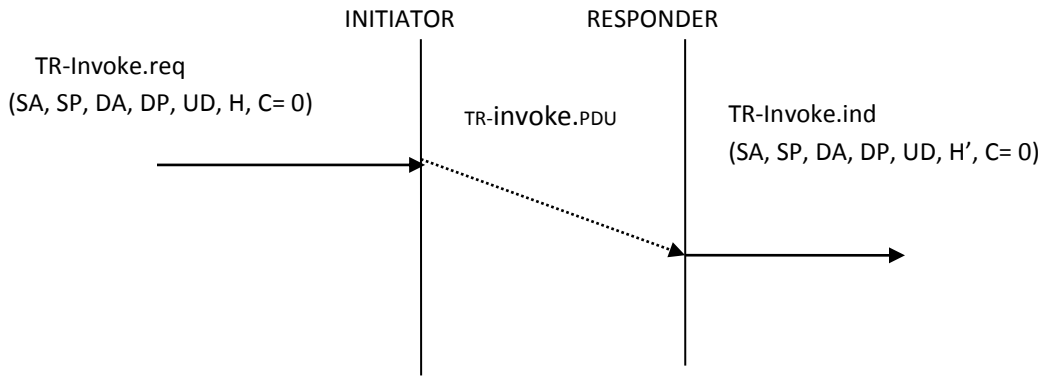


Fig 11.5 Class 0 Basic Transaction

The WTP entity at the initiator sends an invoke PDU which the responder receives. The WTP entity at the responder then generates a TR-Invoke.ind primitive with same parameters. In this class responder does not acknowledge the message and initiator does not perform any retransmission.

WTP Class-1(Reliable with no result message)

It offers reliable transaction service with no result message. The initiator sends an invoke PDU after a TR-Invoke.req from a higher layer. This time class equals to 1 and

no user acknowledgement has been selected. The responder signals the income invoke PDU by a TR-invoke to the higher layer. This specification allows the user on the responder side to send acknowledgement. For initiation, transaction ends with reception of acknowledgement. The responder gives the transaction state for some time to be able to retransmit the acknowledgement if it receives the same invoke PDU again.

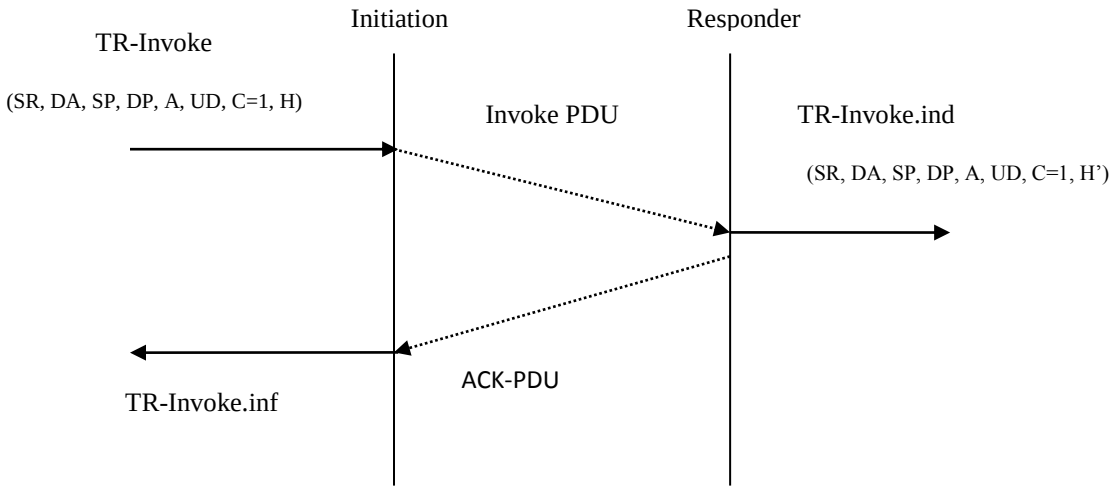


Fig 11.6 Class 1 Basic Transaction

WTP Class-2(Reliable with one result message)

Class 2 transaction service provides the reliable request/response transaction. A user on initiation side sends an invoke PDU to the responder. The WTP entity on responder's side indicates the request with TR-Invoke.ind. The responder now waits for processing of the request. The user on responder side can give the result to the WTP entity on the responder side using TR-result-request. The result PDU can now send back to initiator which implicitly acknowledges the invoked PDU. The initiator can indicate successful transmission of invoke message and result with 2 services TR-Invoke.cnf and TR-Result.ind. A user may respond to this result with TR-Result.res. An acknowledgement PDU is then generated which finally triggers the TR-Result.cnf primitive on the responder's side

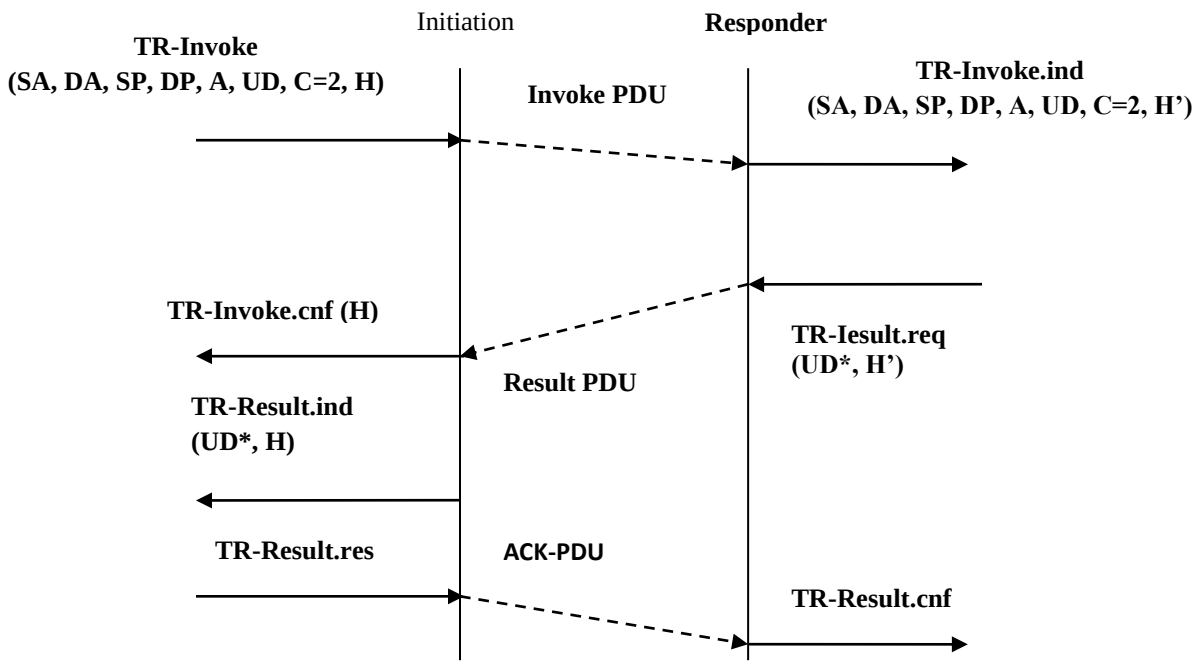


Fig 11.7 WTP Class 2 Transaction

WSP (Wireless Session Protocol)

The WSP provides a connection oriented service on top of WTP. It provides a consistent interface between two session services (client and server). WSP protocol is based on concept of request and a reply. Each WSP protocol data unit consists of a body (containing WML, WML script) and a header (containing information about the data). WSP provides applications with in interface for two session services. The connection oriented session services operates above WTP and connectionless session service operates above WDP. WSP offers following general features need for content exchange:

Session Management: WSP introduces a session that can be established form a client to a server and may exist for a long time. It is responsible for suspending and resuming a session of a mobile during its operation.

Capability Negotiation: Client and server can agree upon a common level of functionality to set upon a common level of functionality to set the capacity of a mobile

depending upon parameters such as client size, server size and maximum request it can handle.

Content Encoding: It defines encoding for transferring the contents.

Session establishment involves the exchange of S-Connect primitives. A WSP user acting as a client requests a session with a WSP user acting as a server by issuing an S-Connect.req. Parameters are Server Address (SA), Client address (CA), client header (CH), requested capabilities (RC). The client transfers the PDU to server where S-Connect.ind primitive indicates a new session. The server accepts the new session and answers with S-Connect.res. The parameters are Server Header (SH) and negotiated capabilities (NC). The PDU is then transferred to client. S-Connect.cnf confirms the session establishment.

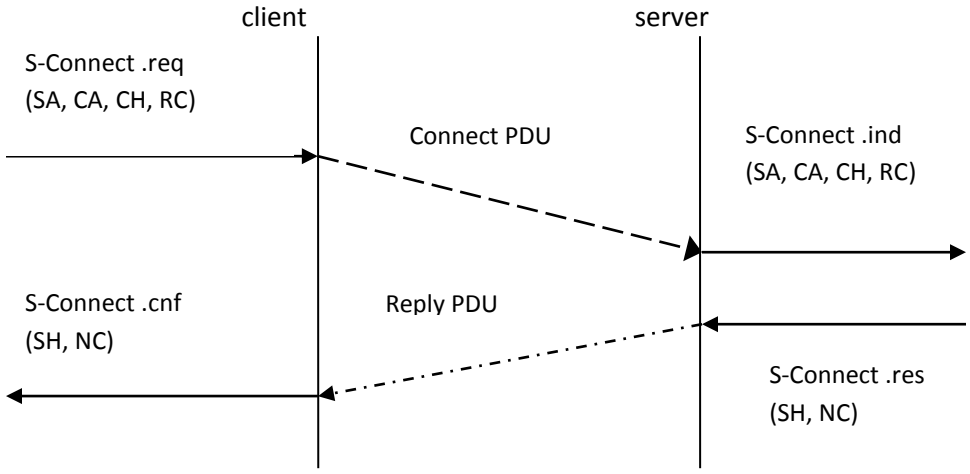


Fig 11.8 WSP Session Establishment

Terminating a session is done by using the S-Disconnect.req service primitive. These primitive aborts all current method used to transfer data. Disconnection is indicated on both sides using S-Disconnect.ind. The reason for disconnection can be network error, protocol error, congestion, maximum packet size exceeded etc.

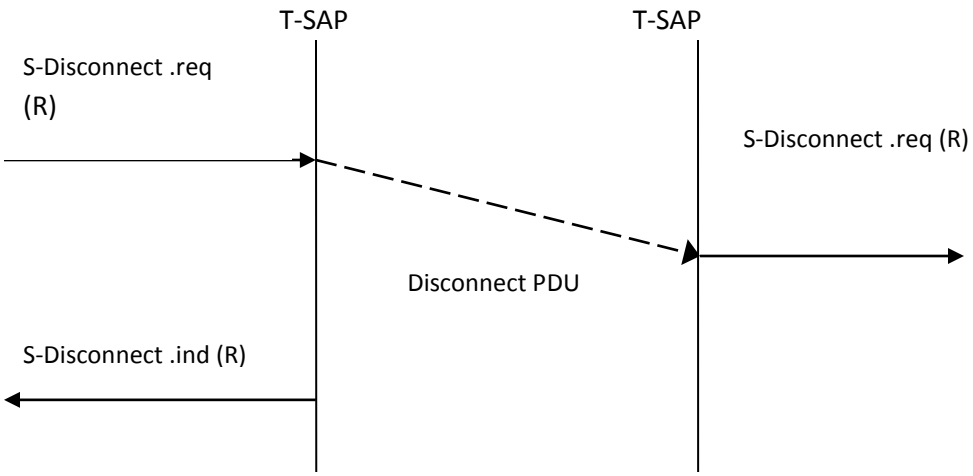


Fig 11.9 WSP Session Termination

WSP Supports session suspend and resume. If a client notices that the bearer network will be unable due to roaming to another network or the user switches off the device. The client can suspend the session. Session suspension will automatically abort all data transmission and freeze the current state of the session on the client and server side. A client suspends a session with S-Suspend.req, WTP transfers the suspend PDU to sever with class 0 transaction. SP will signal the suspension with S-Suspend.ind on the client and server side. The only parameter is the reason R for suspension. Reasons can be a user request or a suspension initiated by the service provider. A client can later resume a suspended session with S-Resume.req. The parameters are SA, CA (Client Address).

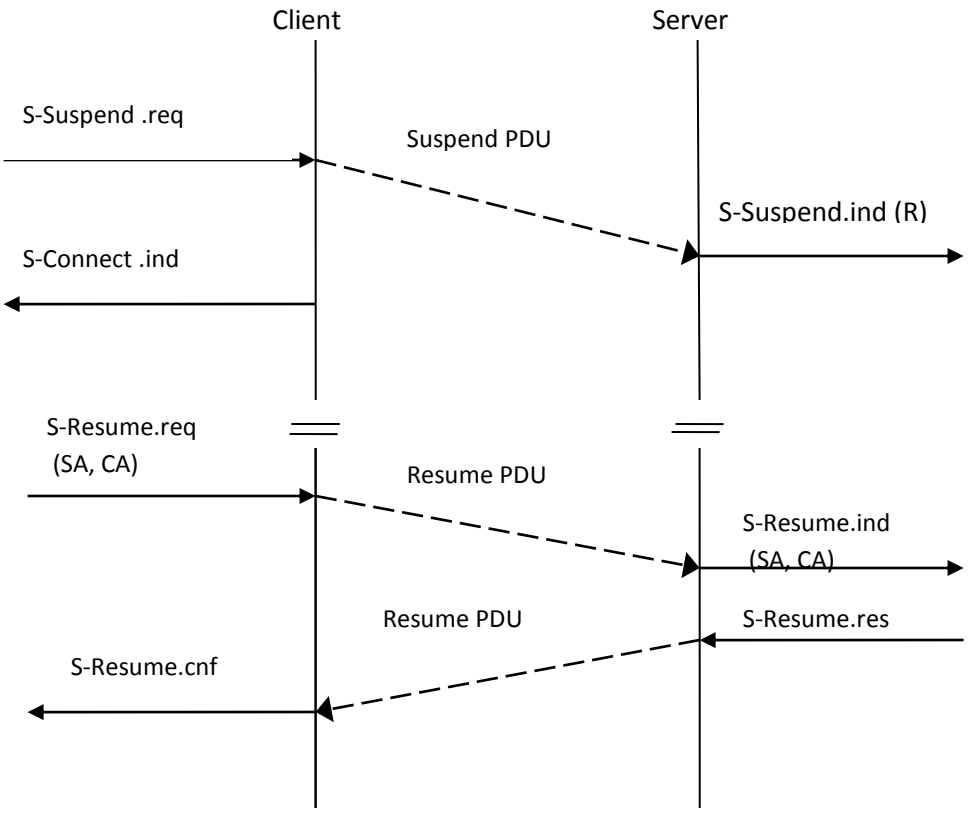


Fig 11.10 WSP session suspension and resume

WAE (Wireless Application Environment)

The objective of WAE is to provide an interoperable environment to build wireless services among operators and service providers. It offers a framework for the integration of different World Wide Web and mobile telephony application. The major elements of WAE are:

Wireless Telephony Application (WTA): A collection of telephonic features for call mechanism. Using WTA, application developers can use micro browser to originate telephone calls.

Content Generator: Application or services on origin servers that produce standard content formats in response to requests from user agents in the mobile terminal.

User Agent: The user agent signifies an agent who works on behalf of the user. In WWW and WAE content user agent is the user facing browser software.

Wireless Markup Language (WML): It is a mark-up language optimized for use in wireless devices similar to HTML.

The goal of WAE is to minimize over the-air traffic and resource consumption on handheld device. This goal can be implemented using WAE logical model. In logical model, a client uses an encoded request for an operation on a remote server. Encoding is necessary to minimize data sent over the air and to save resources on the handheld device. Decoders in a gateway translate the encoded request into a standard request as understood by origin server. The gateway transfers this request to the origin server. Origin server will respond to the request. The gateway encodes the response and transfers the encoded response with the content to the client.

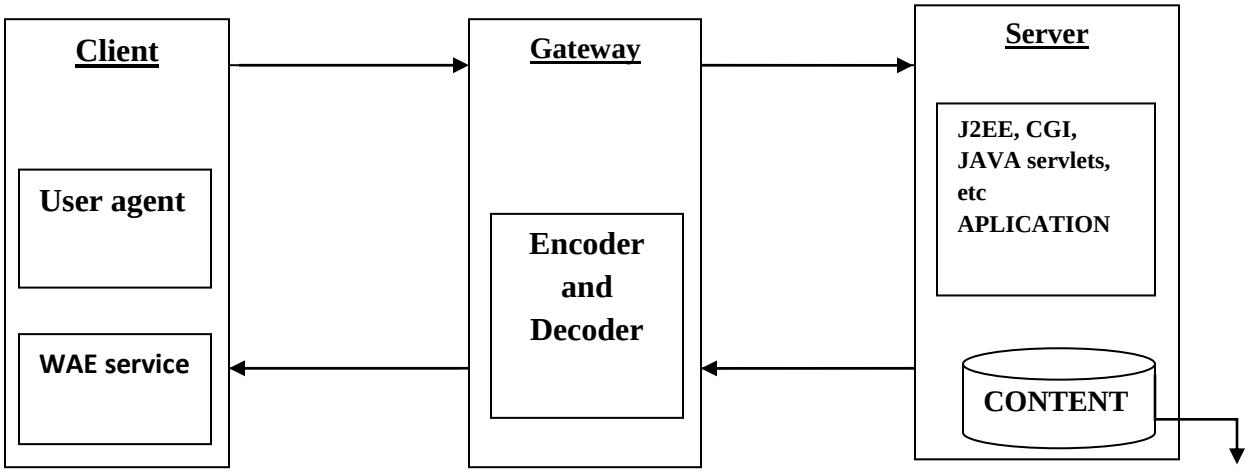


Fig 11.11 WAE Logical Model

WML (Wireless Markup Language)

WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability. It is designed to work with telephone keypads, styluses, and other input devises common to mobile, wireless communication. WML permits the scaling of displays for use on two-line screens found in some small devices, as well as the larger screens found on smart phones.

For an ordinary PC, a web browser provides contents in the form of web coded with the Hypertext Markup Language (HTML). To translate an HTML-coded webpage into WML with content and format suitable for wireless devices, much of the information, especially graphics and animation, must be stripped away. WML presents mainly text-

based information that attempts to capture the essence of web page and that is organized for easy access for users of mobile devices.

Important features of WML include the following:

- **Text and image support**: Formatting and layout commands are provided for text and limited image capability.
- **Deck/card organizational metaphor**: WML documents are subdivided into small, well-defined units of user interaction called cards. Users navigate by moving back and forth between cards. A card specifies one or more unit of interaction (a menu, a screen of text, or a text entry field). A WML deck is similar to an HTML page in that it is identified by a web address (URL) and is the unit of content transmission.
- **Support for navigation among cards and decks**: WML includes provisions for event handling, which is used for navigation or executing scripts.

In an HTML-based web browser, a user navigates by clicking on links. At a WML-capable mobile device, a user interacts with cards, moving forward and back through the deck.

WML is tagged language, similar to HTML, in which individual language elements are delineated by lowercase tags enclosed in angle brackets. Typically, The WML definition of a card begins with the non visible portion, which contains executable elements, followed the visible content. As an example, consider the following simple deck with one card form :

```
<wml>
        <card id='card1'>
        <p>
            Hello WAP World.
        </p>
        </card>
```

</wml>

The tags <wml>, <card>, and <p> enclose the deck, cards, and paragraph, respectively. Like HTML, most elements end with a terminating tag that is identical to the starting tag with the addition of the character “\”. When a wireless device receives this code, it will display the message “hello WAP world” on the terminal’s screen.

WML Script

WML Script is a scripting language with similarities to JavaScript. It is designed for defining script-type programs in a user device with limited processing power and memory.

WLL (Wireless in Local Loop)

Wireless local loop (WLL) provides two-way calling services to the stationary or “fixed” users, which is intended to replace its wireline Counterpart. It is a system that connects a subscriber to PSTN using wireless technology and use radio signals to provide standard telephone service. It is a broadcast connection system that uses high frequency radio links to deliver voice and data without fiber optic cables.

In telephony, loop is defined as the circuit connecting a subscriber’s station (e.g., telephone set) with the line terminating equipment in a central office (a switch in the telephone network). The trunks start from the central office in the loop, and are broken down into several smaller bundles of circuits after some distance from the central office. These circuits are eventually separated into individual drops for the residence houses. The central office switch is typically the first point of traffic concentration in the public switched telephone

Network (PSTN). Newer installations use fiber optics to connect residential neighborhoods or business campuses to the central office and statistical multiplexers to concentrate traffic.

Architecture

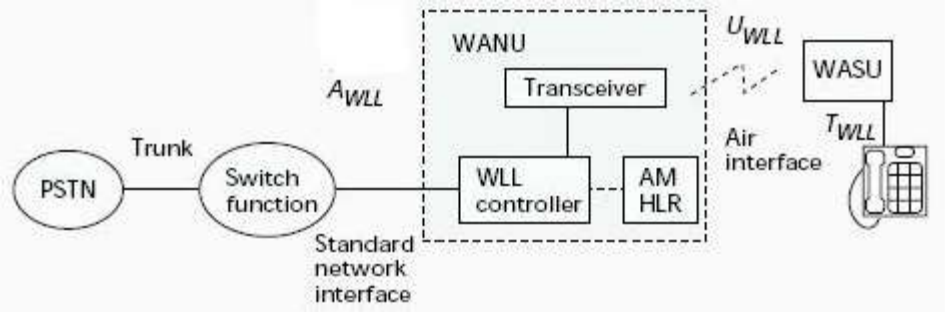


Fig 12.2 WLL Architecture

A simplified version architectural reference model for WLL is shown in Fig. In this figure, the wireless access network unit (WANU) consists of the base station transceivers (BTS) or radio ports (RP), the radio controller (RPCU), an access manager (AM), and home location register (HLR), as required. The interface between the WANU and the switch is called A_{WLL}. The air interface between the WANU and the user side is called U_{WLL}. The WANU should provide for the authentication and privacy of the air interface, radio resource management, limited mobility management, and over-the-air registration of subscriber units (SUs). It may also be required to provide Operation and Maintenance (OAMP), routing, billing and switching functions as appropriate or necessary. The WANU also provides protocol conversion and transcoding of voice and data. The wireless access subscriber unit (WASU) provides an air interface toward the network and a "traditional" interface T_{WLL} to the subscriber. This interface includes protocol conversion and transcoding, authentication functions, local power, OAMP, dual tone multi frequency (DTMF), dialtone. In this reference model the switching fabric (SF) can be a digital switch with or without Advanced Intelligent Network (AIN) capability, an ISDN switch, or a mobile switching center (MSC).

It consists of 3 major components.

WANU (Wireless Access Network Unit)

It consists of several BST or radio parts, a RPCU (Radio port control unit), an AM (access Manager, Responsible for working of RPCU), a HLR. It is responsible authentication, air registration of Subscriber. It may also be required to provide OAM, routing, billing, switching, protocol conversion Trans-coding of voice and data.

WASU (Wireless access subscriber unit)

It provides an air interface “Uwll” towards n/w and “Pwll” interface towards subscriber. It is responsible for voice trans-coding authentication and signaling function.

SF (Switching Fabric)

It is associated with a switch that can be a digital switch, MSC, ISDN switch. The transmission between WANU and SF can be leased line, microwave or optical fiber. Switch is connected to WANU through “Awll” interface.

The Wireless Local Loop Technologies

The WLL systems are typically based on one of the following four technologies

Satellite-Based Systems: These systems provide telephony services for rural communities and isolated areas such as islands. These systems can be of two types:

- Technology designed specifically for WLL applications
- Technology piggybacked onto mobile satellite systems as an adjunct service

Of these, the former offers quality and grade of service comparable to wireline access, but it may be expensive. The latter promises to be less costly but, due to bandwidth restrictions, may not offer the quality and grade of service comparable to plain old telephone service (POTS).

An example of a satellite based technology specifically designed for WLL is the HNS telephony earth station (TES) technology. This technology can make use of virtually any geostationary earth orbit (GEO) C-band or Ku-band satellite. Satellite technology has been used to provide telephony to remote areas of the world for many years. Such systems provide an alternative to terrestrial telephony systems where land lines are not cost effective or where an emergency backup is required. There are many proposed systems for mobile satellite service, including the Inmarsat International Circular Orbit (ICO) system, Iridium, Globalstar, Odyssey, American Mobile Satellite Corporation (AMSC), Asia Cellular Satellite (ACeS) and Thuraya mobile satellite system. These systems are specialized to support low-cost mobile terminals primarily for low bit rate voice and data applications.

Cellular-Based Systems: These systems provide large power, large range, median subscriber density, and median circuit quality WLL services. Cellular WLL technologies are primarily used to expand the basic telephony services. Typically, they operate in the mobile frequency bands at 800-900 MHz, 1.8- 1.9 GHz, and sometimes at 450 MHz or 1.5 GHz .

This approach offers both mobility and fixed wireless access from the same cellular platform. Cellular systems are optimized for high-tier coverage. Support for mobiles traveling in excess of 100 mph and cell sizes up to 10 mi in radius is required. To achieve the above goals, extensive signal processing is required, which translates into high delay, high overhead and low user bandwidth. These systems are not well suited to deployment indoors and in picocells. Additional complexity of the air interface with the same low user bandwidth is required.

Low-Tier PCS or Microcellular-Based Systems: These systems provide low power, small range, high subscriber density, and high circuit quality WLL services. These technologies are considered to facilitate rapid market entry and to expand the capacity of the existing infrastructure. They are typically operated at 800 MHz, 1.5 GHz, 1.8 GHz, and 1.9 GHz frequency bands.

Compared with the cellular-based WLL, more base stations are required to cover the same service area. Operators may consider low-tier WLL technologies when an existing infrastructure is in place to support backhaul from many base stations to the switch, or when wireline-like services and quality are essential.

Fixed Wireless Access Systems: These systems are proprietary radio systems designed specifically for fixed wireless applications, which may or may not be extensible to PCS or cordless. The primary disadvantage of the cellular approach is its limitation on tollquality voice (new toll-quality vocoders designed for cellular technologies may eliminate this problem), and signaling transparency. The primary disadvantage of low-tier PCS and microcellular approaches is their range. Nonstandard fixed wireless access (FWA) technology can address these issues and become more efficient. FWA systems for zonal areas are designed to cover the local telephone area directly from the

PSTN switches. The systems for rural areas provide connection at the remote ends of rural links to the end users.

Examples of WLL Products

HNS Terminal Earth Station Quantum System

The HNS terminal earth station (TES) product is used for the Intelsat network to provide remote access telephone service. In total there are approximately 100 TES networks worldwide, in addition to the Intelsat network, and more than 10,000 remote site stations. The TES system is a satellite based telephony and data communications network providing mesh connectivity between multiple earth stations. The system provides call-by-call demand-assigned multiple access (DAMA) circuits and preassigned circuits, via single hop single channel per carrier (SCPC) communications paths between earth stations. It supports both public and private networks, and is capable of operating with any telephony interface from individual subscribers to toll switches and major gateways.

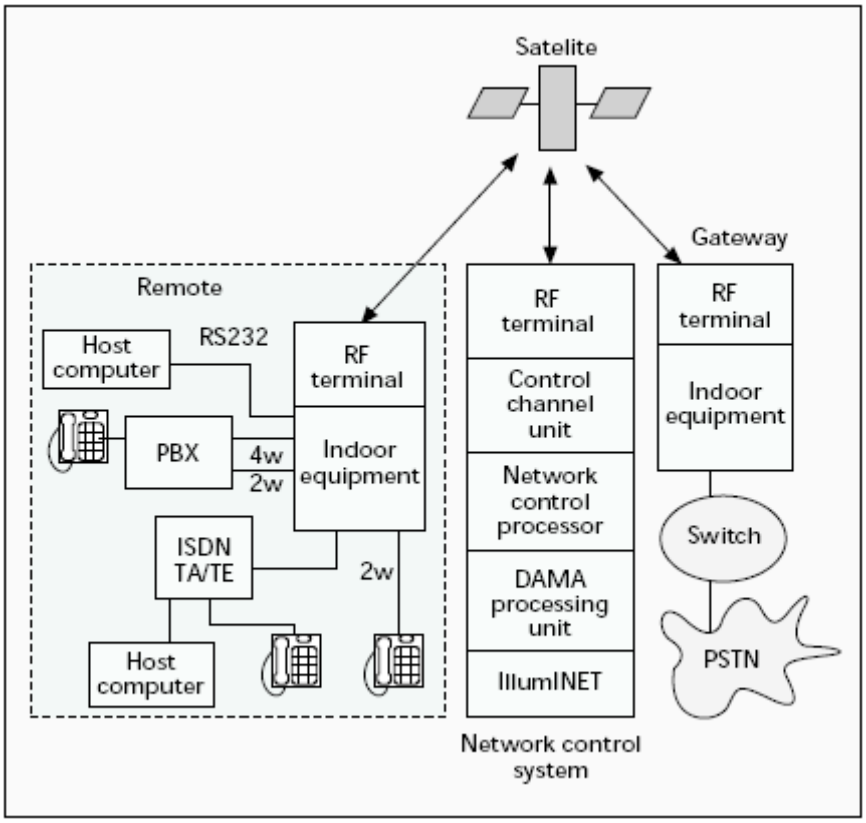


Fig 12.3 TES quantum topology.

Lucent Wireless Subscriber System

Lucent Wireless Subscriber System (Lucent WSS) is a cellular- based WLL . This system typically supports 800-5000 subscribers per switch controlled area (the capacity can be enhanced v

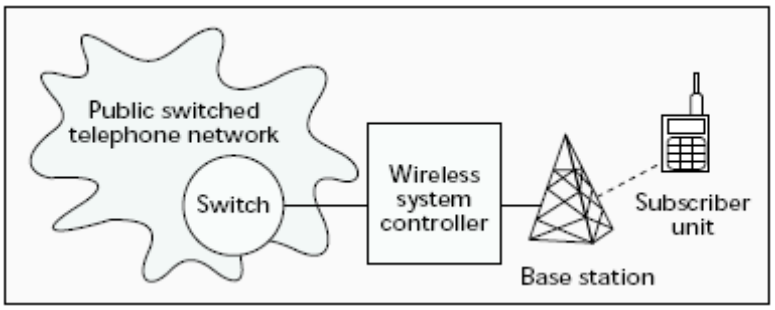


Fig 12.4 The Lucent wireless subscriber system architecture

HNS E-TDMA

E-TDMA is an extension to the IS-136 TDMA standard that provides support for WLL with increased capacity and improved network performance while maintaining the large coverage area feature of other cellular standards.

E-TDMA offers a choice of subscriber unit platforms including single subscriber units (SSU) and multiple subscriber units (MSU) capable of supporting up to 96 lines, depending on the subscriber traffic load and MSU provisioning. The single subscriber unit supports high capacity digital voice, fax, and data transparently using a standard RJ-11 interface, and enables multiple terminal connections as simple extensions on a single access unit or per directory number. Such units are appropriate for locations with low population densities such as residences and small businesses. Multiple subscriber units provide access to the WLL system in areas of high population densities such as hotels and apartment buildings. MSU and radio resources are allocated on a call-by-call basis, thereby reducing the required hardware. Operations and maintenance of both SSUs and MSUs are supported by a full set of remote terminal diagnostic protocols to assess performance and respond to end-user issues. Over the-air activation protocols

are also supported to improve system installation. The system supports software downloads to subscriber units to take full advantage of system upgrades remotely.

The PACS WLL System

The ANSI standard personal access communications system (PACS) WLL system is a low-tier PCS-based WLL. The low power PCS technology supports high circuit quality (32 kb/s voice coding) and low latency data with high user bandwidths. PACS is designed to cover a broad range of venues not optimally served by typical cellular systems, including high density WLL. PACS has features that set it apart from other PCS and cellular standards.

For example, PACS supports both public and private key authentication and privacy. It operates in both FDD and TDD mode, and can interoperate across a wide variety of public and private networks in licensed and unlicensed spectrum. It has a rich suite of data protocols, including packet and circuit protocols. It spans a wide range of venues from large outdoor microcells to indoor picocells.

There are two types of user terminals in PACS/WLL: portable handset (subscriber unit) and fixed access unit. The fixed access units convert the radio signal to an RJ-11 interface signal to the customer premises equipment.

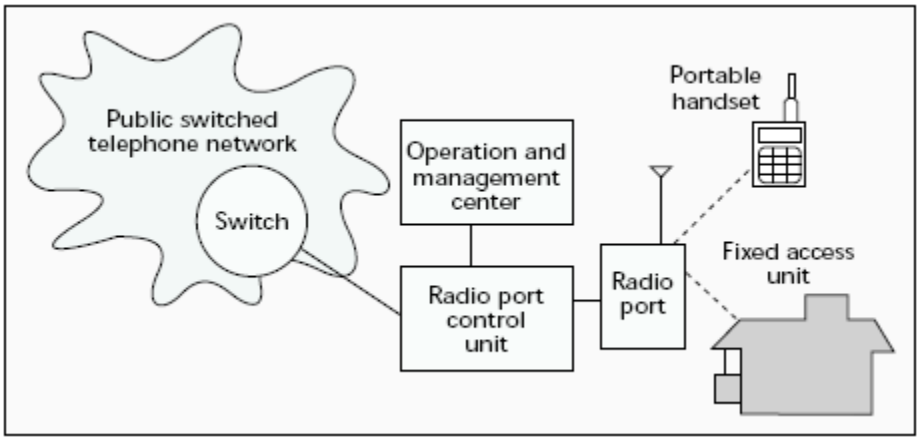


Fig 12.5 The PACS/WLL architecture.

Qualcomm QCTel

Qualcomm's QCTel CDMA WLL System is an FWA WLL. A basic six-sector QCTel system may support 24,000 subscribers. The QCTel technology supports 8 kb/s voice and up to 7.2 kb/s data rate. QCTel supports limited mobility, and the subscriber unit can be a portable handset.

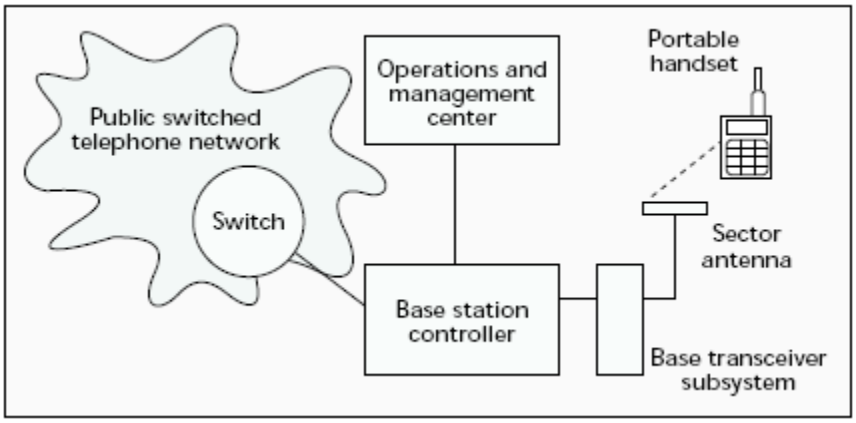


Fig 12.6 The Qualcomm QCTel architecture.

IMT 2000 (International Mobile Telecommunications-2000)

IMT 2000 known as 3G or 3rd Generation, is a family of standards for mobile telecommunications defined by the International Telecommunication Union, which includes EDGE, UMTS, and CDMA2000 as well as DECT and WiMAX. Services include wide-area wireless voice telephone, video calls, and wireless data, all in a mobile environment. 3G allows simultaneous use of speech and data services and higher data rates (up to 14.0 Mbit/s on the downlink and 5.8 Mbit/s on the uplink). Thus, 3G networks enable network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency. The Internal Telecommunication Union- Radio communication developed 3G specification to facilitate a global wireless infrastructure. Internal Mobile Telecommunication-2000 (IMT 2000) is the global standard for 3rd generation mobile communication. IMT 2000 is a standard name used for all 3G systems. Earlier the name was Future Public Land Mobile Telecommunication System (FPLMTS).The number 2000 in IMT 2000 indicates the start of the system in the year (2000+x) and spectrum

used (around 2000 MHz). IMT 2000 provides a framework for worldwide access by linking the systems in satellite based networks

Vision

- Common worldwide spectrum
- Multiple radio environment (LAN, satellite, cordless, cellular)
- Worldwide roaming capability
- High quality, enhanced security and performance
- Small terminal for worldwide use
- Integration of satellite and terrestrial system

Services provided

High bearer rate capabilities

- 2 Mbps for fixed environment
- 384 Kbps for indoor and outdoor pedestrian environment
- 144 kbps for vehicular environment

Standardization work

- Europe- ETIS –UMTS (Universal Mobile Telecommunication System)
- Japan- ARIB (Association of Radio Industries and Business) – WCDMA
- USA- TIA(Telecom Industry Association) – CDMA 2000

IMT 2000 Family

ITU standardized five groups of 3G radio access technology

- IMT-DS: Direct spread technology comprises wideband CDMA systems (W-CDMA). It is used by European provider. It is specified for UTRA FDD system
- IMT–TC: It stands for time code and specified for UTRA FDD system. It uses time division CDMA.

- IMT-SC: It is a single carrier technology originally promoted by the Universal Wireless Communications Consortium. It is now integrated to the 3GPP efforts. This technology is implemented in DECT.
- IMT-FT: A frequency time technology. It is an enhanced version of the cordless telephone standard DECT.
- IMT-MC: CDMA 2000 is a muti-carrier technology standardized by 3GPP2, which was formed shortly after3GPP to represent the second main stream in 3G technology.

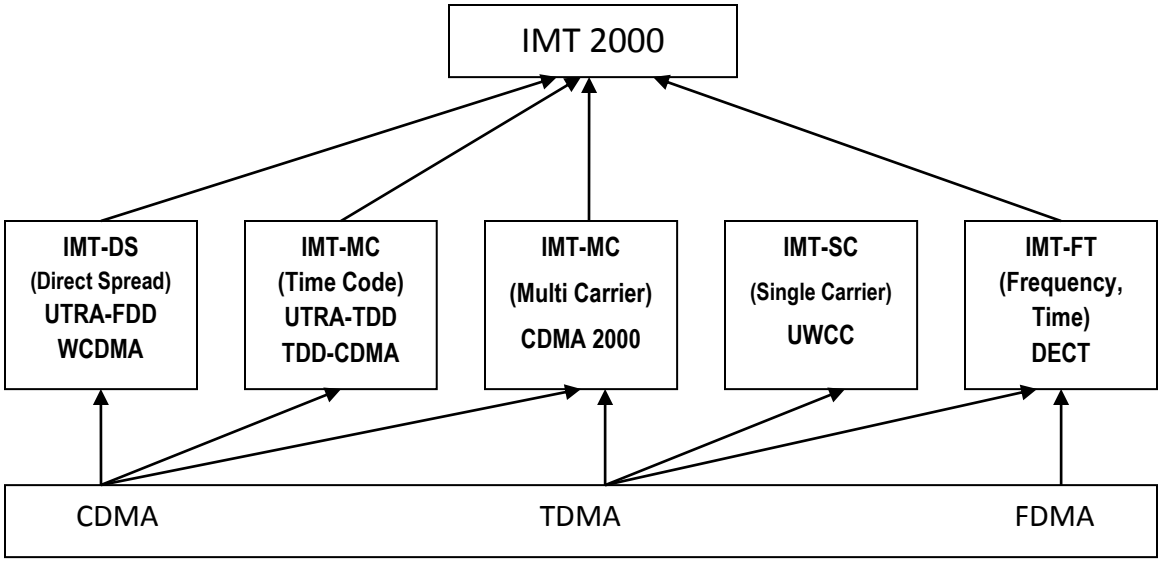


Fig 14.1 IMT 2000 Family

WCDMA

Wideband Code-Division Multiple-Access (W-CDMA) is one of the main technologies for the implementation of third-generation (3G) cellular systems. It is base on radio access technique proposed by ETSI Alpha group and the specifications was finalised 1999. WCDMA supports data rates of 2Mbps or higher for short distances and 384 kbps for long distances. It is also referred to as UTRA-FDD (universal terrestrial radio access-frequency division duplex). WCDMA access is either FDD or TDD. FDD separates reverse-link AND FORWARD LINK frequencies. These are 1.920-1.980 GHz for uplink

and 2.110-2.170 GHz for downlink and each uses a 5MHz bandwidth. It is wider as compared to the 1.25 MHz of the IS-95 SYSTEM.

The key features of WCDMA processing units are as follows:

- Asynchronous base stations
- Employing the same direct sequencing FDD made 1 transmission, same canalization codes (OVSF), same modulation (QPSK), and same carrier modulation (QPSK) for both uplink and downlink.
- Chipping rate of 3.84 MHz
- Multi-rate transmission of signals by spread factor control
- Use of variable data rates.

Protocol Architecture

Protocol architecture consist of 3 layer

- L1-Physical layer
- L2-Datalink layer
- L3-Network layer

The physical layer of WCDMA uses DSSS technique. Physical layer supports 2 modes operation TDD & FDD. Physical layer offers different transport channels to MAC. A transport channel is characterized by how info is transferred over radio interface. MAC offers different logical channel to RLC sub layer of layer2 (L2). A logical cannel is characterized by type of information transferred. L2 is split into following sub layer: RLC, MAC, PDCP, BMC

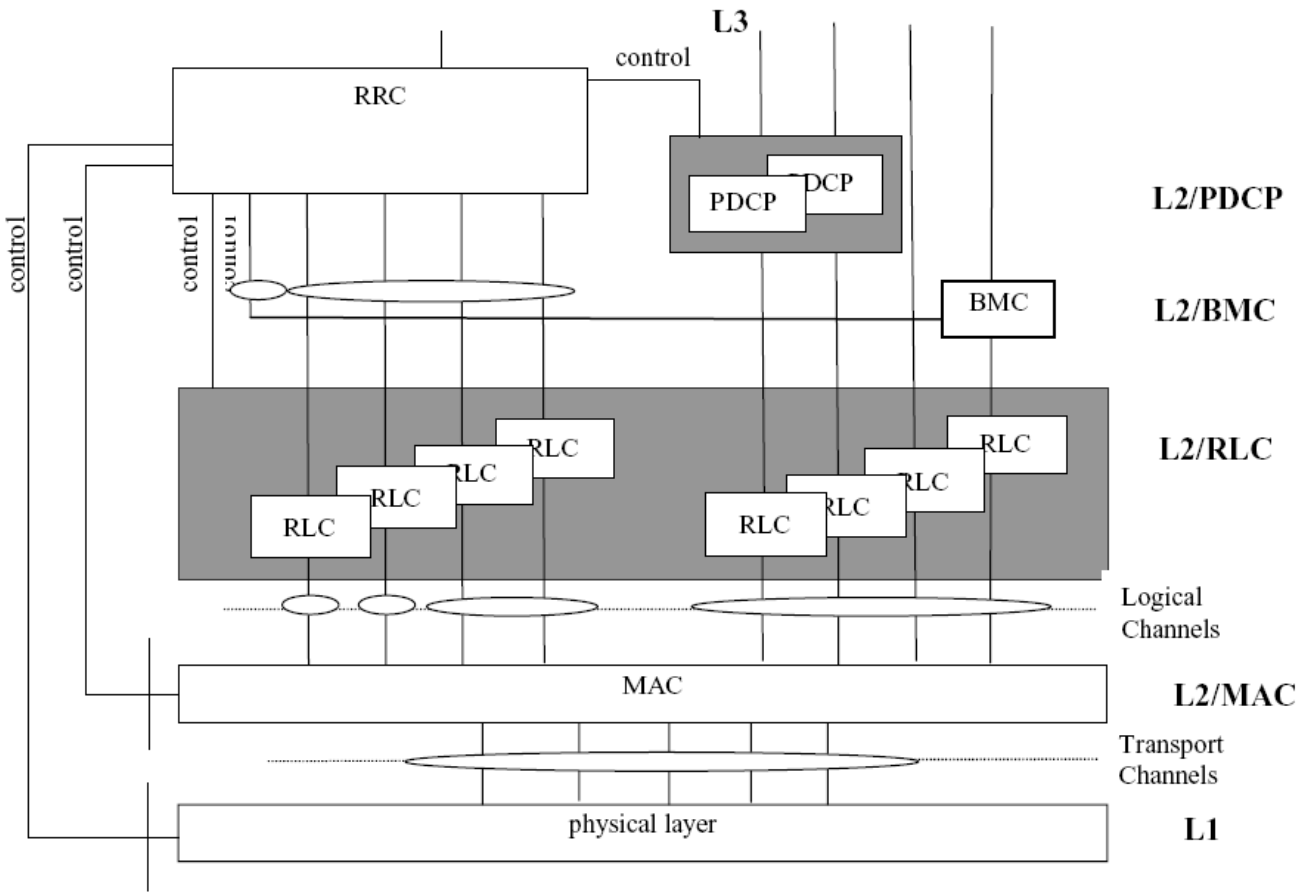


Fig 14.2 WCDMA Protocol Architecture

Logical Channels

MAC layer provides data transfer services on logical channel. A set of logical channel type is defined for different kinds of data transfer services offered by MAC. Each logical channel type is defined by the type of information that is transferred. Logical Channels are classified into two groups:

- Control channel- These channels are used to transfer control information
- Traffic channel-:These channels are used to transfer user information

Table Logical Control Channels

Broadcast Control	Downlink channel for broadcasting system control

Channel(BCCH)	information
Paging Control channel (PCCH)	Downlink channel that transfers paging information and is used when: • Network does not know the location cell of the mobile station • The mobile station is in the cell connected state(utilizing sleep mode procedures)
Common control channel (CCCH)	Bidirectional channel that transfers control information between network and mobile stations. This channel is used: • By the mobile stations having no RRC connection wit the network • By the mobile stations using common transport channels when accessing a new cell after cell reselection
Dedicated Control channel (DCCH)	Point-to-point bidirectional channel that transfers control information between a mobile station and the network. This channel is established through RRC connection set up procedure
ODMA Common Control Channel (OCCCH)	Bidirectional channel for transmitting control information between mobile stations
ODMA Dedicated Control Channel (ODCCH)	Point-to-point bidirectional channel that transmits dedicated control information between mobile stations. This channel is established through RRC connection setup procedure

Table Logical Traffic Channels

Dedicated Traffic Channel (DTCH)	Point-to-point channel, dedicated to one mobile station for the transfer. DTCH can exist both in uplink and downlink.
ODMA Dedicated Traffic Channel	Point-to-point channel, dedicated to one mobile station for the transfer. DTCH can exist both in uplink and downlink. An ODTCH exists in relay link. A point-to-multipoint unidirectional channel for transfer of dedicated user information.

Transport channels

A transport channel is defined by how and with what characteristics data is transferred over the air interface. There exist two types of transport channels:

- Dedicated channels
- Common channels

There is one dedicated transport channel that is dedicated channel (DCH). It is a downlink or uplink transport channel. The DCH is transmitted over the entire cell or over only a part of the cell using beam-forming antennas.

The common transport channels are mentioned in the table below.

Table Common Transport Channels

Broadcast channel (BCH)	Downlink transport channel that is used to broadcast system and cell-specific information. The BCH is always transmitted over the entire cell with a low fixed bit rate.
Forward access channel	Downlink transport channel. The FACH is transmitted over the entire cell or over only a part of the cell

(FACH)	using beam-forming antennas. The FACH uses slow power control.
Random Access Channel(RACH)	Uplink transport channel. The RACH is always received from the entire cell. The RACH is characterized by a limited size Data field , a collision risk and by the use of open loop power control
Common packet channel(CPCH)	Uplink transport channel. The CPCH is a contention-based random access channel used for transmission of bursty data traffic. CPCH is associated with a dedicated channel on the downlink, which provides power control for the uplink CPCH.
Downlink shared channel(DSCH)	Downlink transport channel shared by several mobile stations . The DSCH is associated with a DCH
Paging channel(PCH)	Downlink transport channel. The PCH is always transmitted over the entire cell. The transmission of the PCH is associated with the transmission of a physical layer signal, the paging indicator, to support efficient sleep made procedures.

Physical Channel

The transport channels are mapped on the physical channels. Physical channels are merged in physical layer which consist of radio frame and time slot. The length of radio frame is 10ms and one frame consists of 15 time slot. Time slot is unit which consists of fields consisting of bits. A time slot is a unit which consist of field containing bits. The number of bits per time slot depends on the physical channel. Normally physical layer consists of 2 uplink and one downlink channel.

Uplink Physical Channels

There are two uplink dedicated and two common physical channels:

- The uplink dedicated physical data channel (uplink DPDCH) and the uplink dedicated physical control channel (uplink DPCCH)
- The physical random access channel (PRACH) and physical common packet channel (PCPCH)

Dedicated Physical Data Channel (DPDCH): It is used to carry dedicated data generated at L2 and above. There may be zero or several uplink DPDCH.

Dedicated Physical Control Channel DPCCH): The uplink DPCCH is used to carry control information generated by Layer-1. Control information consists of pilot bits, transmit power control, feedback information etc.

Physical Random Access Channel (PRACH): It is used to carry the RACH. The random-access transmission is based on a slotted ALOHA approach with fast acquisition indication.

Physical Common Packet Channel (PCPCH): The PCPCH is used to carry the CPCH transport channel. The CPCH transmission is based on DSMA-CD approach with fast acquisition indication.

Downlink Physical Channels

There is one downlink dedicated physical channel, one shared and five common control channels:

- Downlink Dedicated Physical Channel (DPCH)
- Primary downlink Shared Channel (DSCH)
- Primary and secondary common pilot channels (CPICH)
- Primary and secondary common control physical channels (CCPCH)
- Synchronisation Channel (SCH)

Downlink Dedicated Physical Channel (DPCH): On the DPCH, the dedicated transport channel is transmitted time multiplexed with control information generated at layer 1.

Dedicated Shared Channel (DSCH): It is always associated with a downlink DPCH. It is shared by users based on code multiplexing.

Common Pilot Channel (CPICH): It is a downlink physical channel which carries a predefined bit/symbol sequence. There are two types of common pilot channel Primary and Secondary CPICH

- Primary CPICH: There exist one primary CPICH per cell. It is broadcasted over the entire cell
- Secondary CPICH: There may be zero, one or more secondary CPICH. They are broadcasted over only a part of the cell

Common Control Physical Channel (CCPCH): It is a downlink physical channel used to carry the BCH. There are two types of common pilot channel Primary and Secondary CPCCH

- Primary CPCH: It is used to carry the BCH.
- Secondary CPCH: It is used to carry FACH and PCH.

Synchronisation Channel (SCH): This channel is used for searching the cell. The SCH consists of two sub channels:

- Primary SCH consists of a modulated code of length 256 chips.
- Secondary SCH consists of repeatedly transmitting a length 15 sequence of modulated codes of length 256 chips.

CDMA 2000

CDMA2000 is a family of 3G mobile technology standards, which use CDMA channel access, to send voice, data, and signaling data between mobile phones and cell sites. It is also known as also known as IMT Multi-Carrier (IMT-MC) . Cdma2000 specification was developed by the Third Generation Partnership Project 2 (3GPP2), a partnership

consisting of five telecommunications standards bodies: ARIB and TTC in Japan, CWTS in China, TTA in Korea and TIA in North America. The set of standards includes: CDMA2000 1X, CDMA2000 EV-DO Rev. 0, CDMA2000 EV-DO Rev. A, and CDMA2000 EV-DO Rev. B. All are approved radio interfaces for the ITU's IMT-2000.

CDMA2000 can support mobile data communications at speeds ranging from 144 Kbps to 2 Mbps. Versions have been developed by Ericsson and Qualcomm. As of March 2006, the CDMA Development Group reports more than 250,300,000 subscribers worldwide.

Protocol Architecture

In CDMA 2000, four different protocols are specified.

1. Physical layer-Layer1
2. MAC sub layer-layer2
3. Link Access Control (LAC) sub layer (Layer 2)

CDMA 2000 Physical layer (Layer 1)

The physical layer is responsible for:

1. Transmitting and receiving bits over the physical medium, which is the air. The bits have to convert into waveforms by modulation.
2. Carrying out coding functions to perform error control functions at the bit and frame levels.

Cdma2000 accepts both signal carrier and multiple career implementations. It also has proposed two kinds of multiplexing: FDD and TDD. The physical layer channels for both FDD and TDD are the same.

Physical Channels:

Physical channels are distinguished in two groups: dedicated and common channel.

Dedicated Physical Channel (DPHCH)

1. **Forward dedicated Physical Channel (F-DPHCH):** There are 4 dedicated channels.

- Fundamental channel (F-FCH): Provides for transportation of dedicated data.
- Supplemental Channel (F-SCH): Allocated dynamically to supply a required data rate.
- Dedicated control channel (F-DCCH): Used to transport mobile specific control information.
- Dedicated auxiliary pilot channel (F-DAPICH): Used with antenna beam forming and beam-steering to increase coverage or data rate of a desired user. This channel is optional.

2. **Reverse Dedicated Physical Channel (R-DPHCH):** There are 3 dedicated channels.
   - Fundamental channel (R-FCH): Same function as F-FCH.
   - Supplemental Channel (R-SCH): Same function as F-SCH.
   - Dedicated control channel (R-DCCH)

Common Physical Channel (CPHCH)

1. **Forward Common Physical Channel(F-CPHCH)**
   - **Pilot channel (F-PICH):** Carries the Pilot symbol and provides capabilities for channel estimation and coherent detection and soft handoff.
   - **Common Auxiliary Pilot Channel (F-CAPICH):** Provides a fine tuning on coherent detection and hand off.
   - **Sync Channel (F-SYNC):** Provides the mobile station with system information and synchronization.
   - **Common Assignment Channel (F-CACH):** Support the reservation access mode on the R-EACH (Enhanced Access Channel).The message that assigns the
   - **R-CCCH** is transmitted on the F-CACH

- **Paging Channel (F-PCH):** It can enable paging functions, also provides a means for short burst data communications. Each mobile is assigned an 80-ms slot and decodes periodically to receive page messages. Two channels F-BCCH and F-CCCH can substitute it
- **Broadcast Control Channel (F-BCCH):** Serve to broadcast system-specific and cell-specific overhead information.
- **Common Control Channel (F-CCCH):** It provides a means for paging functions and support different data rates for short burst data communications.
- **Quick Paging Channel (FQPCH):** The idea of having F-QPCH is to decrease the time and mobile station needs to monitor the F-PCH or FCCCH. The period at which the mobile station must decide F-PCH or FCCCH as short as 1.28 ms.
- **Common power control of the (F-CPCCH):** Serve two purposes. To allow power control of the R-RCCH and R-PICH works during the reservation access. To control the P-; ICH when the mobile station is in the traffic state.
- **Packet Data Control (F-PDCH):** A shared packet data channel that supports high-speed operation traffic. Access to this channel is handled through MAC layer scheduling.

2. **Reverse Common Physical Channel**

- **Access Channel(R-ACH):** Used for mobile stations communications messages to the base station for backward compatibility reasons.
- **Common Control Channel (RCCCH):** To transport control information.
- **Enhanced Access Channel(R-EACH):** An enhanced access product relative to that of the R-ACH.
- **Dedicated Control Channel(R-DCCH):** Same function as F-DCCH.
- **Pilot Channel(R-PICH):** Provides the signal for coherent detection.

- **Channel Quality Indicator Channel(R-CQICH):** A support channel for adoptive coding and modulation over the F-PDCH.
- **Acknowledgement channel(R-ACKCH):** Check whether the CRC of the decoded packed has passed or failed.

CDMA 2000 MAC Sub layer (Layer 2)

In the MAC sub layer, there are four different entities. Radio Link Protocol (RLP), signalling Radio Burst Protocol (SRBP), Common Channel Multiplex Sublayer and Dedicated Channel Multiplex sub layer.

- The radio link protocol (RLP) handles user packet data. RLP is performing in the Dedicated Channel Multiplex Sub-layer.
- The Signalling Radio Burst Protocol (SRBP) handles common-channel signalling using radio burst techniques. The SRBP is performing in the common channel Multiplex sublayer.
- The Common Channel Multiplex Sublayer performs the mapping between the logical common channels.
- Dedicated channel multiplex sub layer performs the mapping between the logical dedicated channel (i.e. , those channels are dedicated to specific users) and the physical dedicated cahnnels.

The primary function of the MAC sublayer is to multiplex logical channels before sending and to de-multiplex physical channels into different logical channel after receiving. The two multiplex sublayers of the MAC as mentioned above handle these two functions.

The dedicated channels can be used for both signalling and user data; common channels are only used for signalling. The same arrangement of channels appears in WCDMA. However, the transport channels used in WCDMA for exchanging information between physical layer and logical channels reply MAC layer directly as a means to exchange information between Layer 1 and Layer 2.

Primitives

The messages sending and receiving between layers/sub layers are primitives, a form of these communication messages. Two widely used types of primitives are:

Request primitives: A service requester (MS) uses request primitives to request a service or a resource

Indication Primitives: A service provider uses indication primitives to indicate an event requested by service requester has occurred.

Logical channels

The multiplex sub layers, both common channels and dedicated channels, are responsible for the mapping between logical channels and physical channels. The forward-dedicated traffic channel (F-DTCH) Logical Channel Data (common or dedicated) should be reliably delivered from end to end. In executing reliable delivery, the MAC sub layer assembles data received from higher layers and passes the assembled data to the physical layer for transmission. The MAC sublayer also receives data from the physical layer, disassembles the data, and passes the disassembled data to higher layers.

SDU

On the transmit site, the MAC sub layer assembles data blocks received from a higher layer into an SDU and delivers the SDU to the physical layer for transmission. The MAC sub layer receives an SDU, disassembles the SDU into data blocks and delivers them into higher layers.

Adding one or more data blocks with a header can assemble another SDU. All SDUs can be sent either by common channels or dedicated channels.

Multiplex Sublayer's Interaction

Multiplex sub layers can interact not only with physical layer (Layer 1) below, but can interact with four entities above it, RLP and voice service on the dedicated channel side, LAC (Link Access Protocol), and SRBP on the common channel side.

RLP Layer

RLP controls the process of user packet data that travels on the dedicated user channels. The RLP layer is a Layer 2 protocol that responds for the delivery and receipt of user packet data. An important function of Layer 2 entity is to control packet errors introduced by the physical layer. There are several techniques to control packet data errors.

1. Positive acknowledgement (ACK): Acknowledgement of receiving successfully
2. Negative acknowledgement (NAK): Acknowledgement of receiving unsuccessfully
3. Retransmission: Retransmit when neither and acknowledgement nor a NAK is received.

Other data link control protocols in Layer 2 are:

1. Logical Link Control (LLC): for operating over a LAN using IEEE 802 standards
2. Link Access Protocol: balanced for connecting a device to a packet switched network using the X.25 standard

Three classes of frames on RLP

1. Control frames: carrying control information that have the highest priority
2. Retransmitted data frames: retransmit old data frames
3. New data frames: with lowest priority

Three service types of RLP

RLP 1: Implement packet data services over IS-95A traffic channels, with a data rate of 9.6 or 14.4 kbps

RLP 2: implement packet data service over IS-95B traffic channels, which are fundamental and supplemental code channels.

RLP 3: Implements packet data service over CDMA 2000 traffic channels with a data rate up to 2 Mbps

SRBP (Signalling Radio Burst Protocol) Layer

Functions of SRBP:

A. The SRBP controls the process of signalling messages that travel on the common signalling channels in the physical layer. There are six forward common signalling channels: F-SYNCH, F-CPCCH, F-CCCH, F-PCH, F-CACH and F-BCCH. There are reverse common signalling channels: R-ACH, R-EACH and R-CCCH. SRBP is the entity that computes and generates parameters, such as the power level of each successive access probe, the randomization delay of each access sub-attempt for the transmission and reception of common signalling messages.

B. The SRBP also assembles SDUs for the physical layer to transmit on the physical channels and pass received SDUs from the physical layer to the LAC sub-layer.

MODULE-III

Global Mobile Satellite Systems

Satellite is an object which has been placed into orbit by human endeavor. Such objects are sometimes called artificial satellites to distinguish them from natural satellites such as the Moon.

In general, a satellite is anything that orbits something else, as, for example, the moon orbits the earth. In a communications context, a satellite is a specialized wireless receiver/transmitter that is launched by a rocket and placed in orbit around the earth. There are hundreds of satellites currently in operation. They are used for such diverse purposes as weather forecasting, television broadcast, amateur radio communications, Internet communications, and the Global Positioning System, (GPS).

The first artificial satellite, launched by Russia (then known as the Soviet Union) in the late 1950s, was about the size of a basketball. It did nothing but transmit a simple Morse code signal over and over. In contrast, modern satellites can receive and re-transmit thousands of signals simultaneously, from simple digital data to the most complex television programming.

Application

1. Traditional:
    i. Weather satellite
    ii. Radio & TV broadcast
    iii. Military application
2. Telecommunication:
    i. Global telephone communication
    ii. Global mobile communication
    iii. Connection for communication in remote area

Types of Satellite Systems

There are four general system designs, which are differentiated by the type of orbit in which the satellites operate: Geostationary Orbit (GEO), Low-earth Orbit, Medium-earth Orbit (MEO), and Highly Elliptical Orbit (HEO). Each of these has various strengths and weaknesses in its ability to provide particular communications services.

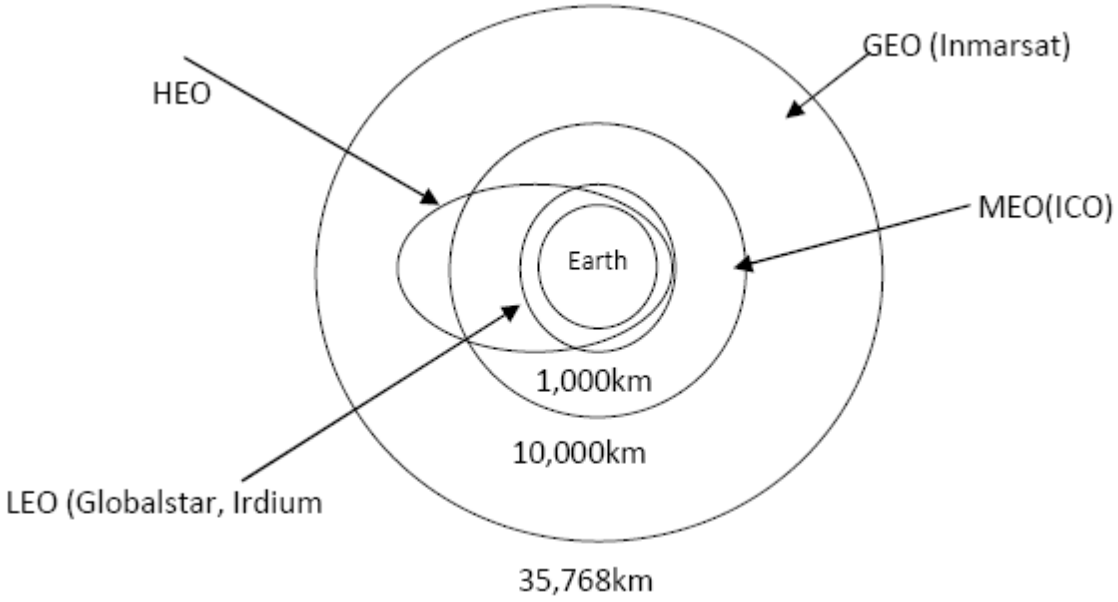


Fig 8.2 Orbits of Different Satellites

Geostationary (GEO)

GEO systems orbit the Earth at a fixed distance of 35,786 kilometers (22,300 miles). The satellite's speed at this altitude matches that of the Earth's rotation, thereby keeping the satellite stationary over a particular spot on the Earth. Examples of GEO systems include INTELSAT, Inmarsat, and

Geostationary satellites orbit the Earth above the equator and cover one third of the Earth's surface at a time. The majority of communications satellites are GEOs and these systems will continue to provide the bulk of the communications satellite capacity for many years to come.

Medium Earth Orbit (MEO)

Stands for medium earth orbit or ICO (intermediate circular orbit)

MEO systems operate at about 10,000 kilometers (between 1,500 and 6,500 miles) above the Earth, which is lower than the GEO orbit and higher than most LEO orbits. The MEO orbit is a compromise between the LEO and GEO orbits. Compared to LEOs, the more distant orbit requires fewer satellites to provide coverage than LEOs because each satellite may be in view of any particular location for several hours. Compared to GEOs, MEOs can operate effectively with smaller, mobile equipment and with less latency (signal delay). Typically, MEO constellations have 10 to 17 satellites distributed over two or three orbital planes

Low Earth Orbit (LEO)

LEO systems fly about 1,000 kilometers above the Earth (between 400 miles and 1,600 miles) and, unlike GEOs, travel across the sky. A typical LEO satellite takes less than two hours to orbit the Earth, which means that a single satellite is "in view" of ground equipment for a only a few minutes. As a consequence, if a transmission takes more than the few minutes that any one satellite is in view, a LEO system must "hand off" between satellites in order to complete the transmission. In general, this can be accomplished by constantly relaying signals between the satellite and various ground stations, or by communicating between the satellites themselves using "inter-satellite links."

Highly Elleptical orbit (HEO)

The satellites orbit the Earth in an elliptical path rather than the circular paths of LEOs and GEOs. The HEO path typically is not centered on the Earth, as LEOs, MEOs and GEOs are. This orbit causes the satellite to move around the Earth faster when it is traveling close to the Earth and slower the farther away it gets. In addition, the satellite's beam covers more of the Earth from farther away, as shown in the illustration.

Example- Ellipso, Pentriad

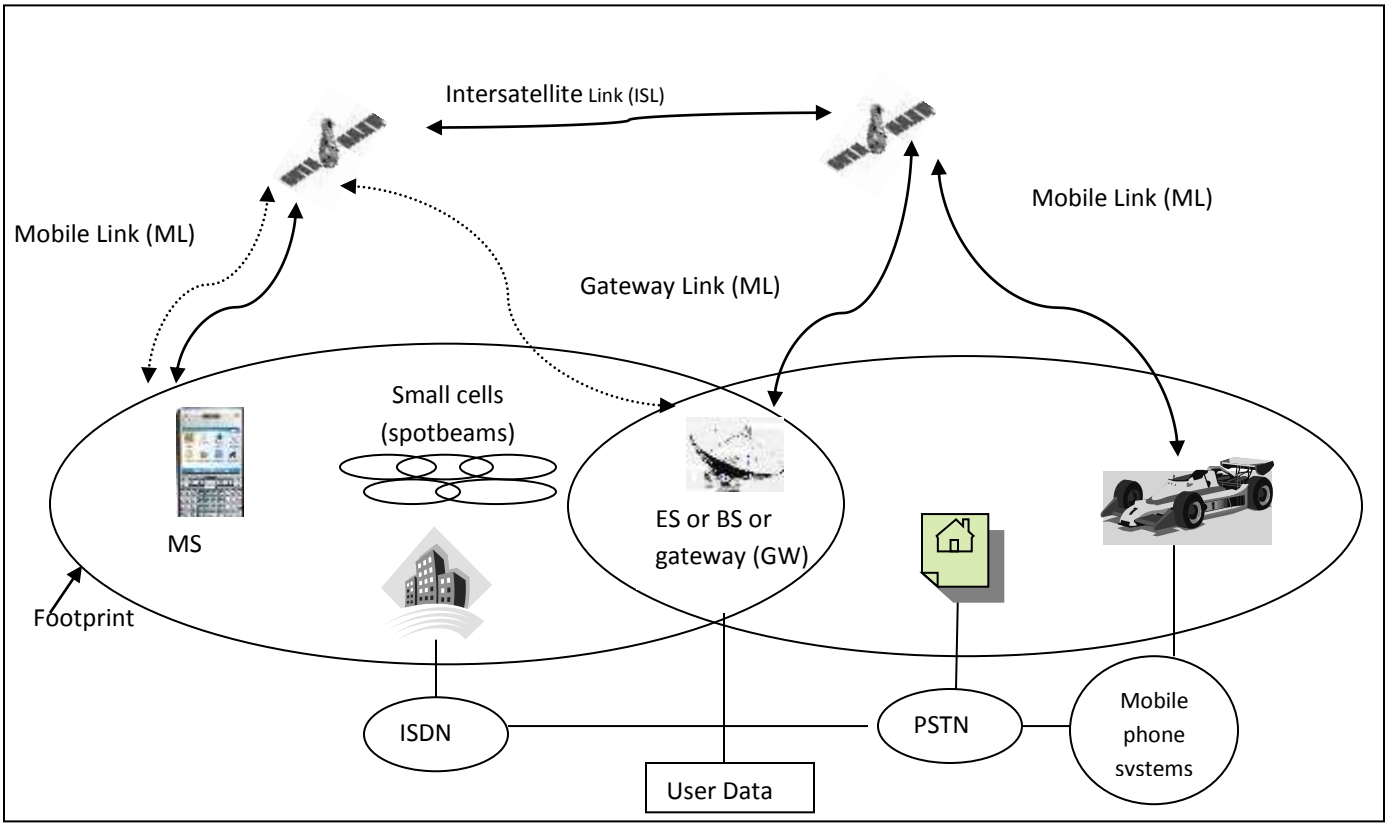


Fig 8.3 A typical Satellite System

CASE STUDIES

IRRIDIUM

It is a satellite based wireless personal communication network designed to permit any type of telephone transmission (voice and data).It is an extension of existing wireless system to provide mobile service to remote areas that are not covered by terrestrial cellular services. It is a LEO satellite.

CONCEPT

The concept of using a constellation of LEO satellite to provide telecommunication services to mobile users was originated by Motorola in 1987.The initial proposal was for 77 satellites in constellation and the system was called IRRIDIUM which has 77 electrons in its orbit. Later on the no of satellite was reduced to 66 which were adequate to provide target services. The 66 satellites are grouped in 6 orbital planes and there are 11 active satellites in each plane with uniform nominal spacing of 32.7^0. The satellites have circular orbit at an altitude of 783 km. The satellite travels one side of the earth crossing over near the North Pole and then traveling down the other side. The adjacent planes are called **co-rotating plane** excluding the first and last which is known as **counter-rotating plane**. The angle between co-rotating planes is 31.6^0. The angle between counter-rotating planes is 22^0. In iridium system, each satellite is equipped with 4 two way communication, 1 each with its neighbors in the same plane and those with in the adjacent planes. Each iridium satellite uses 48 beam antenna patterns and each beam has a minimum diameter of 600 km. In satellite system beams are equivalent to cells associated with mobile system.

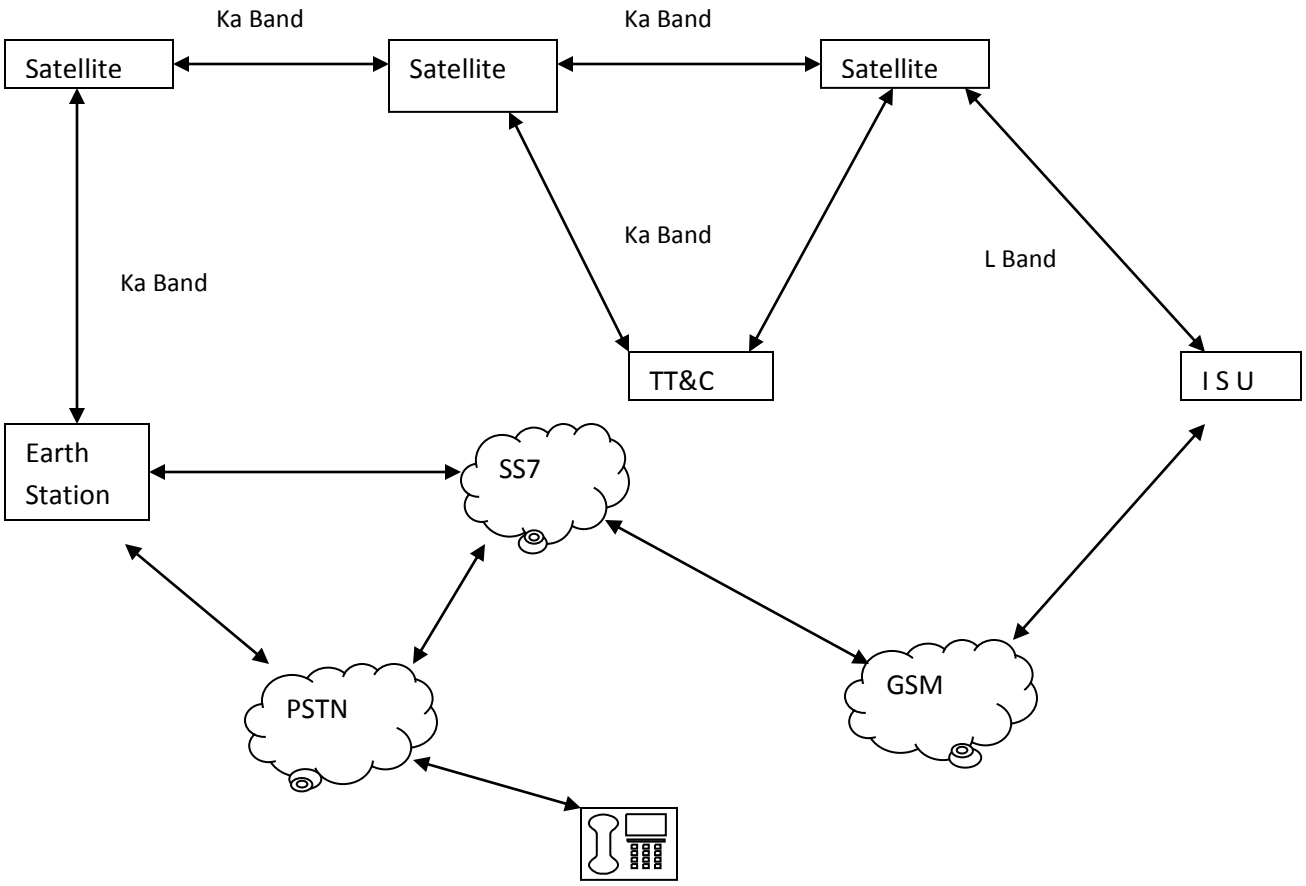


Fig 8.5 Network Architecture for Iridium System

GLOBALSTAR

Globalstar is a low Earth orbit (LEO) satellite constellation for satellite phone and low-speed data communications The Globalstar project was launched in 1991 as a joint venture of Loral Corporation and Qualcomm

It is a Global satellite based system on 48 LEO satellites. Initial service was scheduled in late 1999.It doesn't use inter-satellite links but depends on a large no. of interconnected earth stations or Gateways for efficient call routing but delivery of the terrestrial network. It is designed to complement the terrestrial mobile network to provide telephony and messaging services to subscribers in location that are not covered ,inadequately covered by wire line/wireless network.

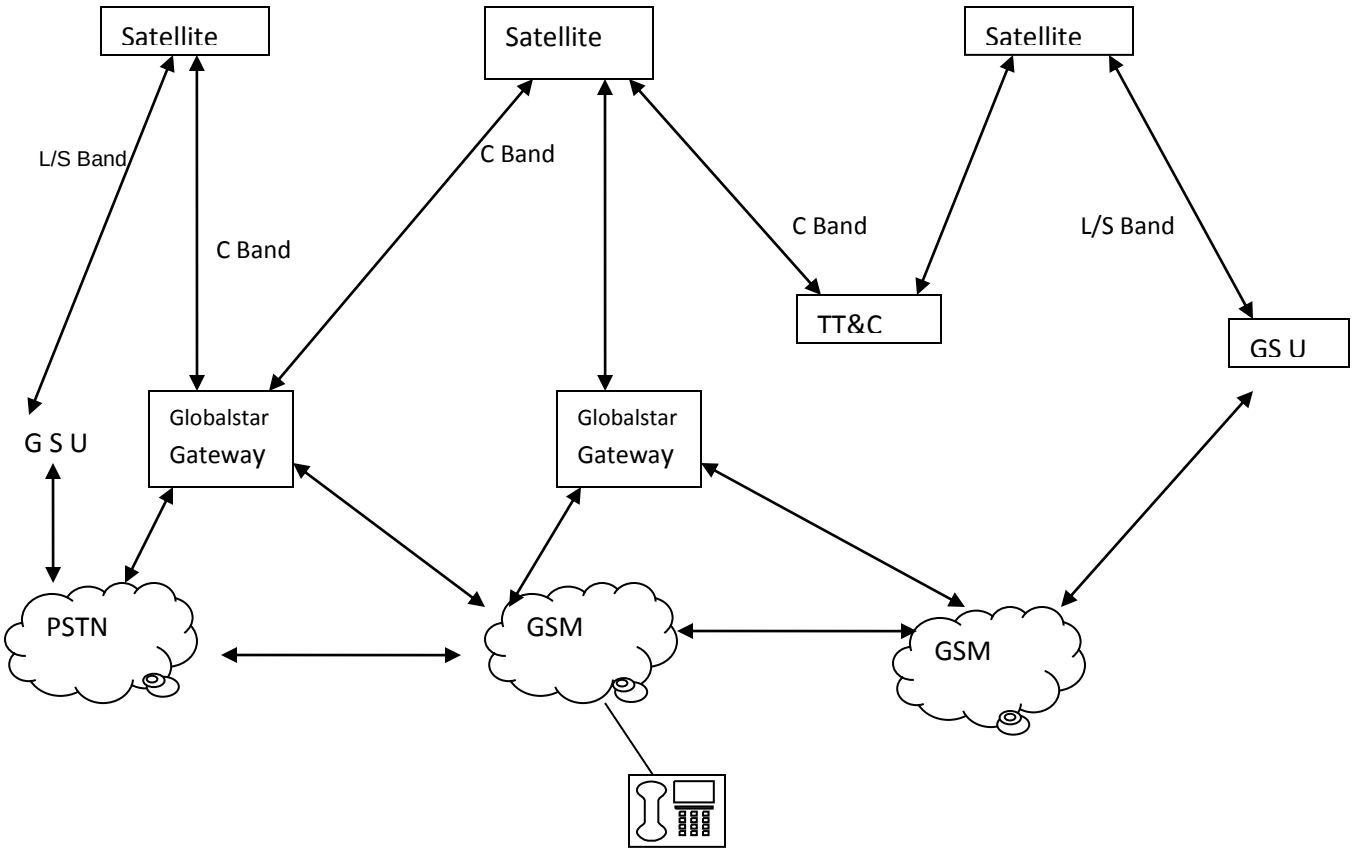


Fig 8.6 Network Architecture for Globalstar System

Concept

Global star constellation of 48 LEO satellites is designed to orbit at an altitude of 1414km above the earth surface in 8 orbital planes inclined at 52^0.Each plane is occupied by 6 satellites and nominal weight of each satellite is 450 kg and working life is 7.5 years. Each satellite supports a 16 beam antenna pattern with an average beam diameter of 2250km.In the absence of ISL Globalstar makes maximum use of international terrestrial network (both wireline/wireless).Calls from the subscriber are routed via a satellite to the nearest earth station or gateway and from there they'll be routed over the existing network. A globalstar gateway is designed to serve an area of 3000 km in diameter. Globalstar uses CDMA technology for service link and FDMA/FDD for gateway link.

ICO

The ICO is a medium earth orbit (MEO) mobile satellite system, which is designed primarily to provide services to handheld phones. ICO will use TDMA as the radio transmission technology. ICO has submitted this proposal to the ITU-R evaluation/selection process as a potential candidate RTT for the satellite component of IMT 2000- the third generation mobile telecommunication system being specified by the ITU. The ICO system is planned to go in service in August 2000. The system is designed to offer digital voice, data, facsimile and short targeted messaging services to its services to its subscribers. ICO's primary target customers are users from the existing terrestrial cellular system who expect to travel to locations in which coverage is unavailable or inadequate.

Concept

ICO system is designed to use a constellation of 10 MEO satellites in intermediate circular orbit (ICO), at an altitude of 10,355 km above the earth's surface. The nominal weight of these satellites at launch is less than 2000 kg. The satellites with an expected life of 12 years are arranged in two planes with five satellites (one and one spare) in each plane: orbital planes inclined at 45 degrees relative to the equator. Each satellite has antennas to provide 163 transmit and service link beams. The orbital configuration provides coverage of earth's entire surface at all times and ensures significant overlap so that two or more satellites are visible to the user and the satellite access nodes (SAN) at any time. Further, at least one of the satellites appears at a high elevation angle, thereby minimizing the probability of blocking due to shadowing effects.

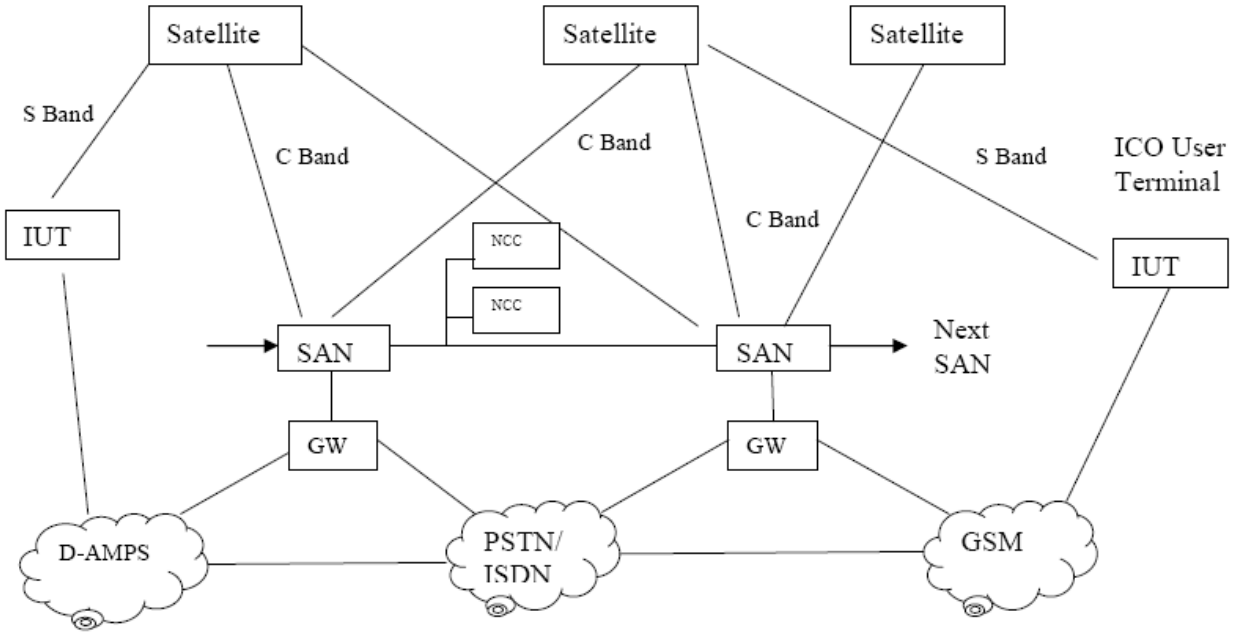


Fig 8.7 Network Architecture for ICO System

VPN (Virtual Private Network)

A VPN is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A communications network tunneled through another network, and dedicated for a specific network. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure. Phone companies have provided private shared resources for voice messages for over a decade. A virtual private network makes it possible to have the same protected sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it

at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted.

Working of VPN

Routers with VPN software works like normal router, filtering packets. To achieve the desired effect of secured private network on the public network VPN performs the following functions:

- A router implementing VPN software is configured such that
    - It rejects all incoming packets except those that arrive from a router which belongs to the authorized network.
    - It rejects all outgoing packets except those which belong to the authorized network**.**
- VPN software encrypts each outgoing packet before transmission. Received packets are decrypted

Goals of VPN

The design goals for a VPN are as follows:

Confidentiality

Confidentiality protects the privacy of information being exchanged between communicating parties. Towards this end, every VPN solution provides encryption of some sort.

Integrity

Integrity ensures that information being transmitted over the public Internet is not altered in any way during transit.

Authentication

Authentication ensures the **identity** of all communicating parties.

Types of VPN

Remote-Access VPN

Also called a **virtual private dial-up network** (**VPDN**) is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an **enterprise service provider** (**ESP**). The ESP sets up a **network access server** (**NAS**) and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network.

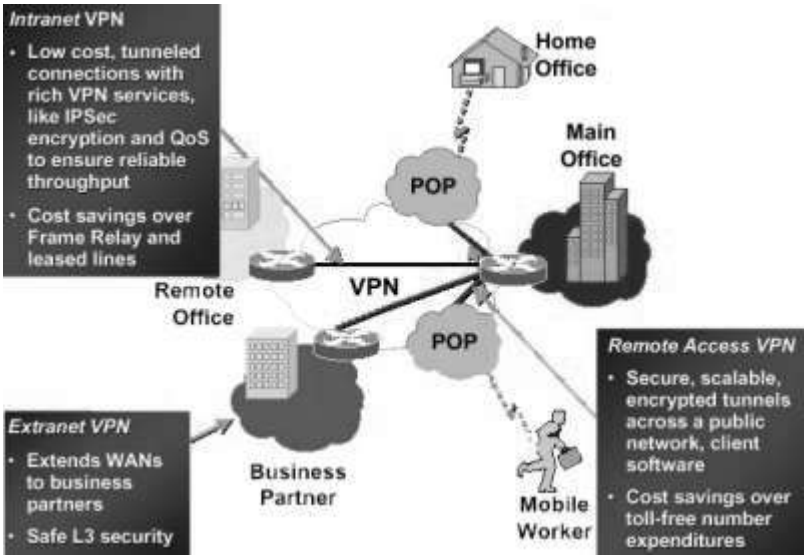


Fig 13.1 Remote Access VPN

Site-to-Site VPN

Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Site-to-site VPNs can be one of two types:

- **Intranet-based** - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

- **Extranet-based** - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

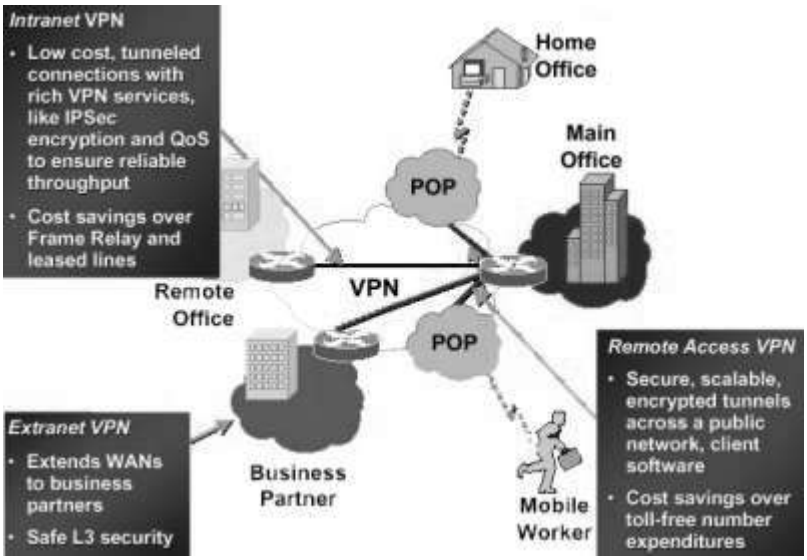


Fig 13.2 Site-to-Site VPN

VPN Protocols

Three protocols are widely used to provide authenticity, confidentiality and integrity. These are as follows:

Internet Protocol Security (IPSec)

It is a set of authentication and encryption protocols, developed by the Internet Engineering Task Force (IETF) and designed to address the inherent lack of security for IP-based networks. It is designed to address data confidentiality, integrity, authentication and key management, in addition to tunneling. IPSec encapsulates a packet by wrapping another packet around it. It then encrypts the entire packet. This encrypted stream of traffic forms a secure tunnel across an otherwise unsecured network.

Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP)

PPTP is a tunneling protocol which provides remote users encrypted, multi-protocol access to a corporate network over the Internet. Network layer protocols are encapsulated by the PPTP protocol for transport over the Internet. PPTP can support only one tunnel at a time for each user. L2TP (a hybrid of PPTP and another protocol, L2F) can support multiple, simultaneous tunnels for each user. L2TP will be incorporated in Windows 2000 and can support IPSec for data encryption and integrity

Socks5

SOCKS version 5 is a circuit-level proxy protocol that was originally designed to facilitate authenticated firewall traversal. It provides a secure, proxy architecture with extremely granular access control, making it an excellent choice for extranet configurations. SOCKS v5 supports a broad range of authentication, encryption, tunneling and key management schemes, as well as a number of features not possible with IPSec, PPTP or other VPN technologies. SOCKS v5 provides an extensible architecture that allows developers to build system plug-ins, such as content filtering and extensive logging and auditing of users. When SOCKS is used in conjunction with other VPN technologies, it's possible to have a more complete security solution than any individual technology could provide.

Bluetooth

Bluetooth is an open specification for a radio system that provides the network infrastructure to enable short range wireless communication of data and voice. It comprises of a hardware component and a software component. The specification also describes usage models and user profiles for these models. Bluetooth was the nickname of a Danish king Harald Blatand, who unified Denmark and Norway in the 10th century. The concept behind Bluetooth wireless technology was unifying the telecom and computing industries. Bluetooth technology allows users to make ad hoc wireless connections between devices like mobile phones, desktop or notebook computers without any cable. Devices carrying Bluetooth-enabled chips can easily transfer data at a speed of about 720 Kbps within 50 meters (150 feet) of range or beyond through walls, clothing and even luggage bags.

Bluetooth Protocol

Bluetooth protocol uses a combination of circuit and packet switching. The channel is slotted and slots can be reserved for synchronous packets. Bluetooth protocol stack can support an asynchronous connection-less (ACL) link for data and upto three simultaneous synchronous connection-oriented (SCO) links for voice or a combination of asynchronous data and synchronous voice (DV packet type). Each voice channel supports a 64 Kb/s synchronous channel in each direction. The asynchronous channel can support maximum of 723.2 Kb/s uplink and 57.6 Kb/s downlink (or vice versa) or 433.9 Kb/s symmetric links. The stack primarily has a baseband for physical layer and link manager and controller for link layer. The upper layer interface depends on how these two layers are implemented and used with applications. The stack is shown below.

Piconet and Scatternet

Bluetooth supports both unicast (point-to-point) and multicast (point-to-multipoint) connections. Bluetooth protocol uses the concept of master and slave. In a master-slave protocol a device cannot talk as and when they desire. They need to wait till the time the master allows them to talk. The master and slaves together form a piconet. The master determines the hopping pattern in the piconet and the slaves have to synchronise to this pattern. Two additional types of devices are also present: Parked (P) and Standby (SB). Parked devices cannot actively participate in the piconet but are known and can be reactivated within some milliseconds. Devices in stand-by do not participate in piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked.Several of these **piconets** can be linked together to form a larger network in an ad hoc manner. The topology can be thought as a flexible, multiple piconet structure. This network piconets is called scatternet. A scatternet is formed when a device from one piconet also acts as a member of another piconet. In this scheme, a device being master in one piconet can simultaneously be a slave in the other one.

Bluetooth protocol is a combination of different protocols. The Bluetooth Core protocols plus the Bluetooth radio protocols are required by most of Bluetooth devices, while the rest of the protocols are used by different applications as needed. At the physical layer Bluetooth uses spread spectrum technologies. It uses both direct sequence and frequency hopping spread spectrum technologies. Bluetooth uses connectionless (ACL-Asynchronous Connectionless Link) and connection-oriented (SCO-Synchronous Connection-oriented Link) links. Together, the Cable Replacement layer, the Telephony Control layer, and the Adopted protocol layer form application-oriented protocols enabling applications to run over the Bluetooth Core protocols.

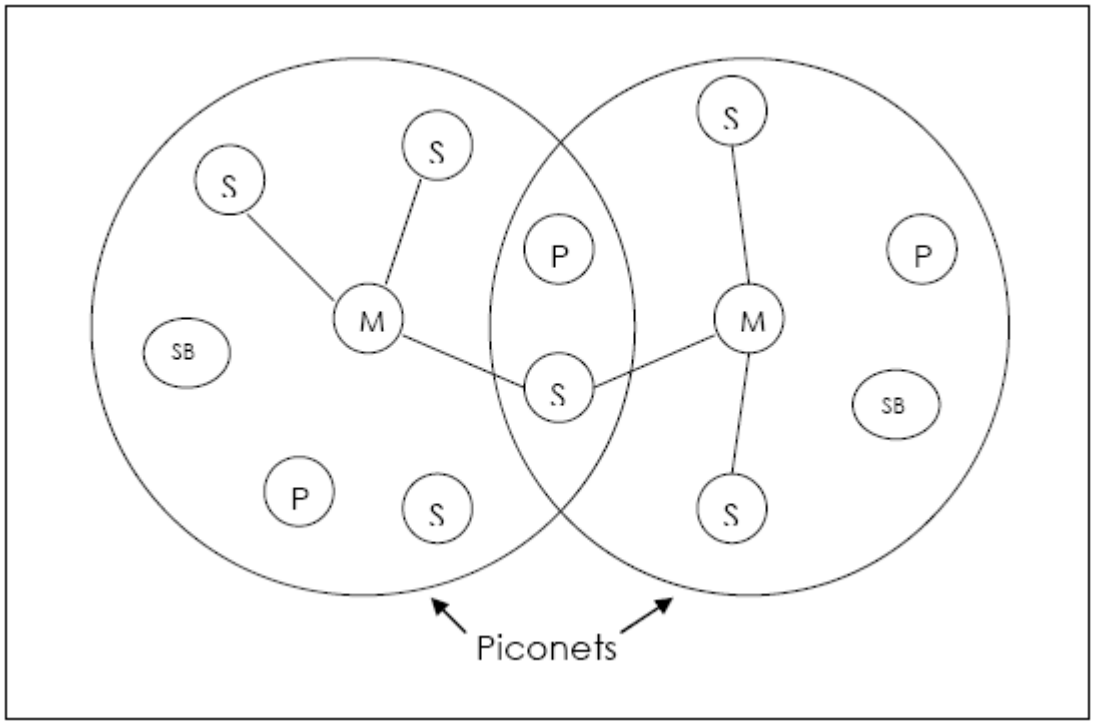


Figure 10.1 Bluetooth scatternet as a combination of Piconets

Bluetooth Protocol Stack

Bluetooth protocol stack can be thought of combination of multiple application specific stacks as depicted in Figure 4.2. Different applications run over one or more vertical slices from this protocol stack. These are RFCOMM (Radio Frequency COMMunication), TCS Binary (Telephony Control Specification), and SDP (Service

Discovery Protocol). Each application environments use a common data link and physical layer. RFCOMM and the TCS binary (Telephony Control Specification) protocol are based on the ETSI TS 07.10 and the ITU-T Recommendation Q.931 respectively. Some applications have some relationship with other protocols, e.g., L2CAP (Logical Link Control and Adaptation Protocol) or TCS may use LMP (Link Manager Protocol) to control the link manager.

Bluetooth protocol stack can be divided into four basic layers according to their functions. These are: **Bluetooth Core Protocols** this comprises of Baseband, Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), and Service Discovery Protocol (SDP).

Baseband

Baseband is the physical layer of the Bluetooth which manages physical channels and links apart from other services like error correction, data whitening, hop selection and Bluetooth security. Baseband lies on top of Bluetooth radio in Bluetooth stack and essentially acts as a link controller and works with link manager for carrying out link level routines like link connection and power control. Baseband also manages asynchronous and synchronous links, handles packets and does paging and inquiry to access and inquire the Bluetooth devices. Baseband transceiver applies a time-division duplex (TDD) scheme.

ACL and SCO links

Baseband handles two types of links: SCO (Synchronous Connection-Oriented) and ACL (Asynchronous Connection-Less) link. The SCO link is a symmetric point-to-point link between a master and a single slave in the piconet. The master maintains the SCO link by using reserved slots at regular intervals (circuit switched type). The SCO link mainly carries voice information. The master can support up to three simultaneous SCO links while slaves can support two or three SCO links. SCO packets are never retransmitted. SCO packets are used for 64 kB/s speech transmission.

The ACL link is a point-to-multipoint link between the master and all the slaves participating on the piconet. In the slots not reserved for the SCO links, the master can

establish an ACL link on a per-slot basis to any slave, including the slave already engaged in an SCO link (packet switched type). Only a single ACL link can exist. For most ACL packets, packet retransmission is applied.

Logical Channels

Bluetooth has five logical channels which can be used to transfer different types of information. LC (Control Channel) and LM (Link Manager) channels are used in the link level while UA, UI and US channels are used to carry asynchronous, isosynchronous and synchronous user information.

Bluetooth Addressing

There are basically four types of device addresses in Bluetooth:

- BD_ADDR: 48 bit Bluetooth device address. It is divided into LAP (Lower Address Part of 24 bits), UAP (Upper Address Part of 8 bits) and NAP (Non-significant Address Part of 16 bits).
- AM-ADDR: 3 bit active member address. The all zero AM_ADDR is for broadcast messages.
- PM_ADDR: 8-bit member address that is assigned to parked slaves.
- AR_ADDR: The access request address is used by the parked slave to determine the slave-to-master half slot in the access window it is allowed to send access messages.

Bluetooth packets

The data on the piconet channel is conveyed in packets. The general packet is shown below:

ACCESS CODE (72)	HEADER (54)	PAYLOAD (0-2754)

Fig 10.2 Bluetooth Packet

Access code is used for timing synchronization, offset compensation, paging and inquiry. There are three different types of Access code: Channel Access Code (CAC), Device Access Code (DAC) and Inquiry Access Code (IAC). The channel access code identifies a piconet (unique for a piconet) while DAC is used for paging and its responses. IAC is used for inquiry purposes. The header contains information for packet acknowledgement, packet numbering for out-of-order packet reordering, flow control, slave address and error check for header. The packet payload can contain either voice field, data field or both. The packet can occupy more than one slot (multi-slot packets) and can continue transmission in the next slot. The payload also carries a 16-bit CRC for error detection and correction in the payload. SCO packets do not include CRC.

Flow control and synchronization

Bluetooth recommends using FIFO queues in ACL and SCO links for transmission and receive. Link Manager fills these queues and link controller empties the queues automatically.

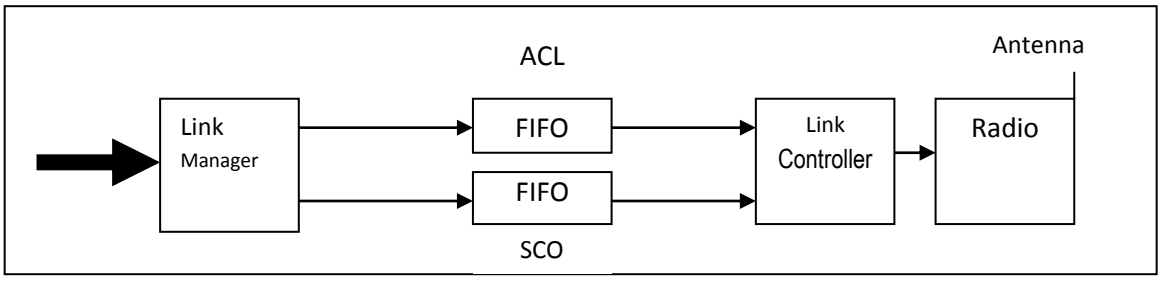


Fig 10.3 Flow Control and Synchronization

If these FIFO queues are full, flow control is used to avoid dropped packets and congestion. If data cannot be received, a STOP indication is transmitted inserted by the Link Controller of the receiver into the header of the return packet. When the transmitter

receives the STOP indication, it freezes its FIFO queues. If receiver is ready it sends a GO packet which resumes the flow again.

Controller States

Bluetooth controller operates in two major states: **Standby** and **Connection.** There are seven sub states which are used to add slaves or make connections in the piconet. These are **page, page scan, inquiry, inquiry scan, master response, slave response and inquiry response.**

The **Standby** state is the default low power state in the Bluetooth unit. Only the native clock is running and there is no interaction with any device whatsoever. In the **Connection** state, the master and slave can exchange packets using the channel (master) access code and the master Bluetooth clock. The hopping scheme used is the channel hopping scheme.

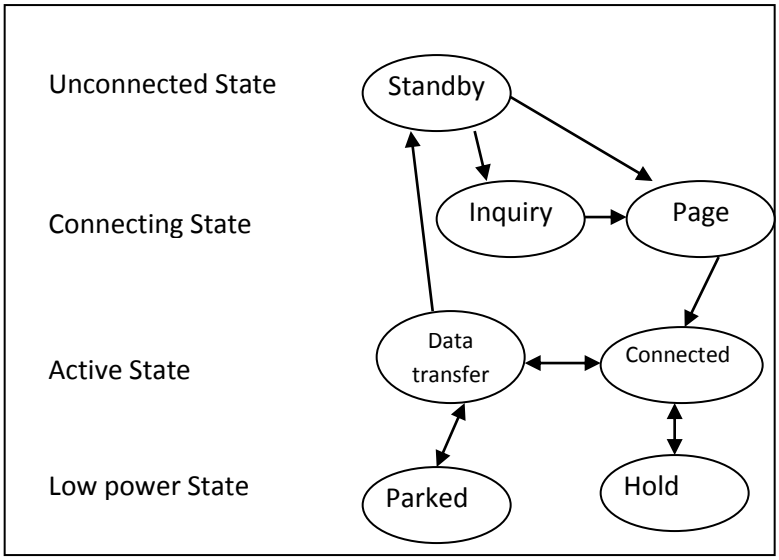


Fig 10.4 Bluet0oth Controller States

A connection between two devices occurs in the following fashion. First master uses the GIAC and DIAC to inquire about the Bluetooth devices in the range If any nearby Bluetooth device is listening for these inquiries, it responds to the master by sending its address and clock information to the master. After sending the information, the slave

may start listening for page messages from the master. The master after discovering the in range Bluetooth devices may page these devices for connection setup. The slave in page scan mode if paged by this master will respond with its device access code (DAC). The master after receiving the response from the slave may respond by transmitting the master's real time clock, master's BD_ADDR, the BCH parity bits and the class of the device (FHS packet). After slave has received this FHS packet, both enter into **Connection** state.

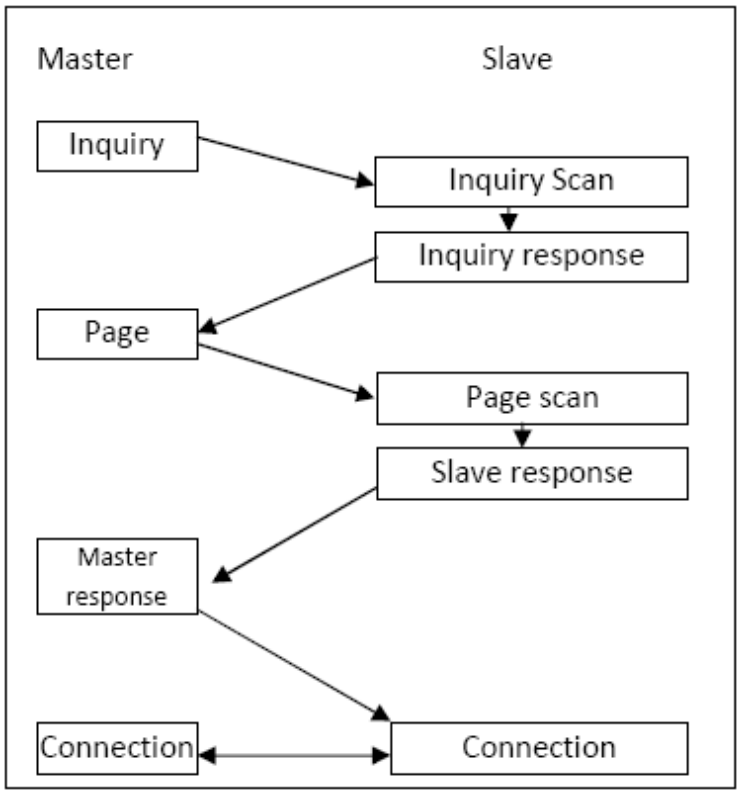


Fig 10.5 Connection setup between master and slave

Link Manager Protocol (LMP): Link Manager is used for managing the security, link set-up and control. It talks to the other link manager to exchange information and control messages through the link controller using some predefined link-level commands. When two Bluetooth devices come within each other's radio range, link managers of either device discover each other. LMP then engages itself in peer-to-peer message

exchange. These messages perform various security functions starting from authentication to encryption. LMP layer performs generation and exchange of encryption keys as well. This layer performs the link setup and negotiation of baseband packet size. LMP also controls the power modes, connection state, and duty cycles of Bluetooth devices in a piconet.

Functions of Link Manager

- Administration and control of all link actions.
- Monitoring state changes
- Monitoring transmission modes
- Monitoring Synchronization
- Device Pairing
- Handling data encryption
- Handling device authentication

The Host Controller Interface (HCI)

The HCI provides a command interface to the base-band controller, link manager and access to the hardware status and control registers. The interface provides a uniform method of accessing the Bluetooth baseband capabilities. The Host control transport layer abstracts away transport dependencies and provides a common device driver interface to various interfaces.

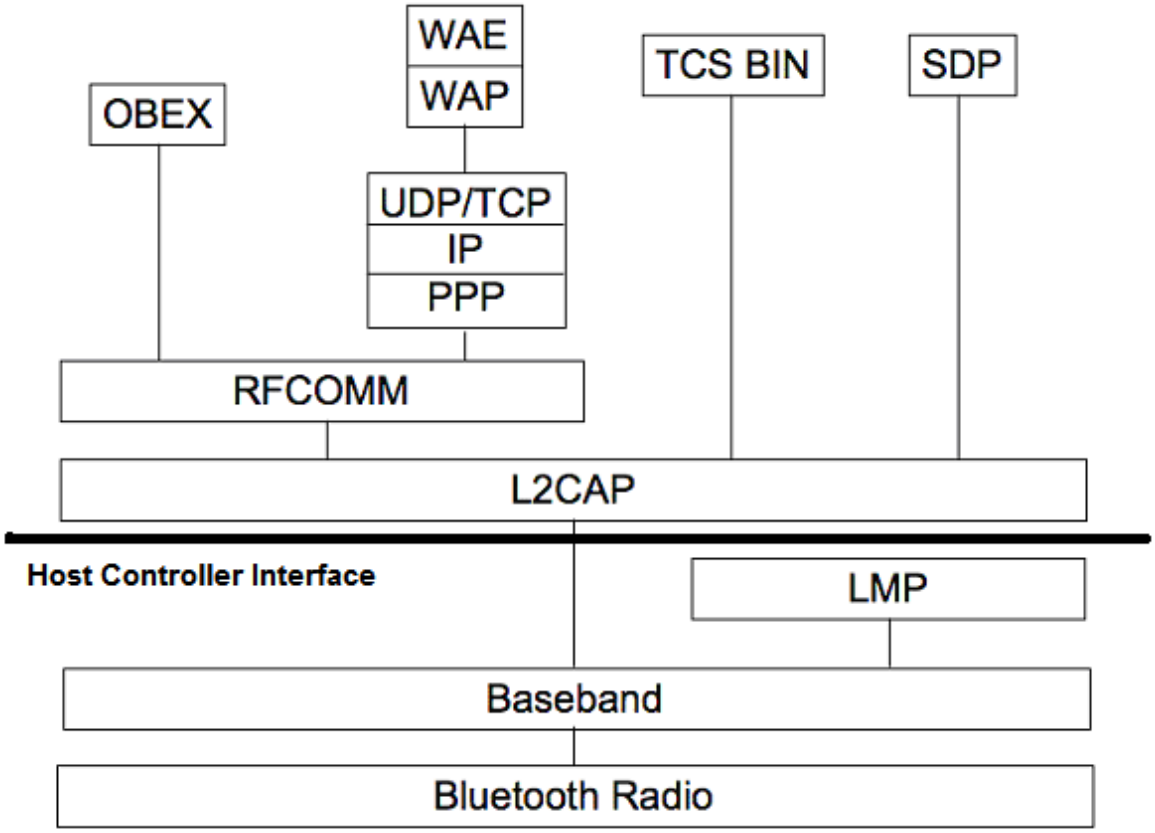


Figure 10.6 Bluetooth Protocol stack

Information Exchange and Request

A Bluetooth link manager can request from other link manager the clock offset (master requesting the slave to tell it the current clock offset stored by it which slave itself got from master during some packet exchange), slot offset (slot offset is the time in microseconds between the start of the master's transmission slot in the piconet where the PDU is transmitted and the start of the master's transmission slot where the BD_ADDR device in the PDU is master. It is useful in master-slave switch and inter-piconet communications), timing accuracy (clock drift and jitter), link manager version and information about supported features like support for authentication, SCO packets etc.

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher level protocols and applications to transmit and receive L2CAP packets up to 64 Kilobytes in length. L2CAP only supports ACL links. L2CAP uses the concept of channels to establish different pathways between different applications on Bluetooth devices. These channels are identified by Channel IDentifiers (CIDs) which represent a logical end point of a connection for each application on a device.

Segmentation and Reassembly

Segmentation and Reassembly (SAR) operations are used to improve efficiency by supporting a maximum transmission unit (MTU) size larger than the largest Baseband packet. This reduces the overhead by spreading the network and transport packets used by higher layer protocols over several baseband packets. L2CAP segments higher layer packets into `chunks' that can be passed to the Link Manager for transmission and reassembles those chunks into L2CAP packets using information provided through HCI and from packet header

Service Discovery Protocol (SDP)

The Service Discovery Protocol (SDP) enables a Bluetooth device to join a piconet. Using SDP a device inquires .what services are available in a piconet and how to access them. SDP uses a client-server model where the server has a list of services defined through service records. One service record in a server describes the characteristics of one service. In a Bluetooth device there can be only one SDP server. If a device provides multiple services, one SDP server acts on behalf of all of them. Similarly multiple applications in a device may use a single SDP client to query servers for service records.

Cable Replacement Protocol

This protocol stack has only one member viz., Radio Frequency Communication (RFCOMM).

RFCOMM: This is a serial line communication protocol and is based on ETSI 07.10 specification. The "cable replacement" protocol emulates RS-232 control and data signals over Bluetooth baseband protocol. It provides a reliable data stream, multiple concurrent connections, flow control and serial cable line settings.

Telephony Control Protocol

This comprises of two protocol stacks viz., Telephony Control Specification Binary (TCS BIN), and the AT-Commands.

Telephony Control protocol Binary: TCS Binary or TCS BIN is a bit-oriented protocol. TCS BIN defines the call control signaling protocol for set up of speech and data calls between Bluetooth devices. It also defines mobility management procedures for handling groups of Bluetooth TCS devices.

AT-Commands: **T**his protocol defines a set of AT-commands by which a mobile phone can be used and controlled as a modem for fax and data transfers. AT (short form of attention) commands are used from a computer or DTE (Data Terminal Equipment) to "control a modem or DCE (Data Circuit terminating Equipment). AT-commands in Bluetooth are based on ITU-T Recommendation.

Adopted Protocols

PPP, TCP/IP: These are standard Internet protocols defined by IETF. These are used as the lower layer protocols of the WAP stack.

OBEX: It is a session protocol defined by IrDA. This protocol is also utilized by bluetooth thus enabling the possibility for application to use either the Bluetooth radio or IrDA technologies.

WAP/WAE: Bluetooth may be used as a bearer technology for transporting between a WAP client and a nearby WAP server. WAP operates on top of the bluetooth stack using PPP and the TCP/IP protocol suite.

REFERENCES

1. Mobile Cellular Telecommunications – William C.Y.Lee (Mc Graw Hill)
2. Mobile and Personal Communication System – Raj Pandya (PHI)
3. Mobile Computing—Raj Kamal(Oxford)
4. Mobile Computing—Asoke Talukdar(TMH)
5. Mobile Communication – J.Schiller(Pearson)
6. Wireless Communication & Network—William Stallings (PEARSON)
7. Wireless Communication—Rappaport(PHI)
8. The Wireless Application Protocol – Sandeep Singhal(PHI)
9. Data Communication and networking—Forouzan(TMH)
10. Wireless and Mobile Systems—Agrawal(Thomson)
11. Wireless and Mobile Network Architecture—Lin (WILEY)
12. High speed Networks and Internets – Stallings (Pearson)
13. Wireless Communication and Networking—Garg (Elsevier)
14. Wireless Networking – Kumar (Elsevier)
15. IS-95, CDMA and CDMA 2000 – Garg (Pearson)
16. Computer Networks – Tanenbaum (PHI)
17. Professional WAP – Charles Arehart (Wrox Press)
18. Data and computer communications-Stalling (Pearson)