ANNAMACHARYA
INSTITUTE OF TECHNOLOGY AND SCIENCES
(AUTONOMOUS)

Approved by AICTE, New Delhi & Permanent Affiliation to JNTUA, Anantapur.

Three B. Tech Programmes (CSE , ECE & CE) are accredited by NBA, New Delhi,Accredited by NAAC with 'A' Grade , Bangalore.

A-grade awarded by AP Knowledge Mission. Recognized under sections 2(f) & 12(B) of UGC Act 1956.

Venkatapuram Village, Renigunta Mandal, Tirupati, Andhra Pradesh-517520.

Department of CSE(INTERNET OF THINGS AND CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

Academic Year 2023-24

IV. B.Tech I Semster

WIRELESS COMMUNICATIONS
(Common to CIC,AIDS)
(20APE0415)

Prepared By

Mrs. K. Janshi Lakshmi., M.Tech.,(Ph.D).
Assistant Professor
Department of ECE, AITS
janshilakshmi.ece@gmail.com

UNIT - 1
Introduction to Wireless Communication Systems

The ability to communicate with people on the move has evolved remarkably since Guglielmo Marconi first demonstrated radio's ability to provide continuous contact with ships sailing the English Channel in 1897. Since then new wireless communications methods and services have been enthusiastically adopted by people throughout the world. Particularly during the past ten years, the mobile radio communications industry has grown by orders of magnitude, fueled by digital and RF circuit fabrication improvements, new large-scale circuit integration, and other miniaturization technologies which make portable radio equipment smaller, cheaper, and more reliable. Digital switching techniques have facilitated the large scale deployment of affordable, easy-to-use radio communication networks.

Evolution of Mobile Radio Communications

The ability to provide wireless communications to an entire population was not even conceived until Bell Laboratories developed the cellular concept in the 1960s and 1970s. With the development of highly reliable, miniature, solid-state radio frequency hardware in the 1970s, the wireless communications era was born.

The following market penetration data show how wireless communications in the consumer sector has grown in popularity. Figure 1.1 illustrates how mobile telephony has penetrated our daily lives compared with other popular inventions of the 20th century. Figure 1.1 shows that the first 35 years of mobile telephony saw little market penetration due to high cost and the technological challenges involved, but however, in the past decade, wireless communications has been accepted by consumers at rates comparable to television and the video cassette recorder.

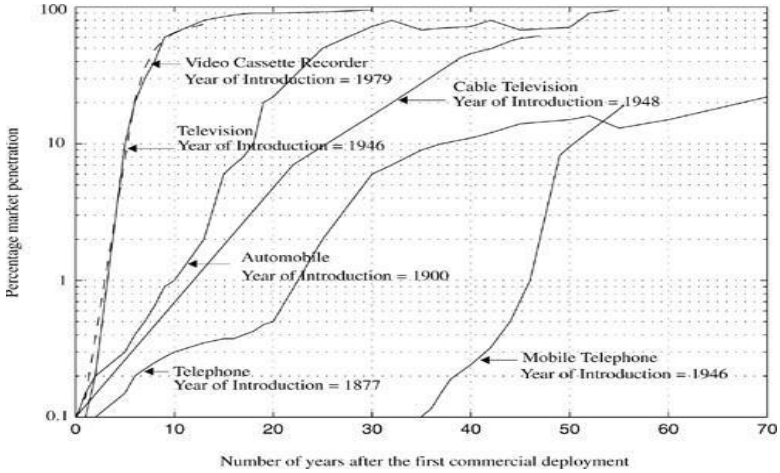


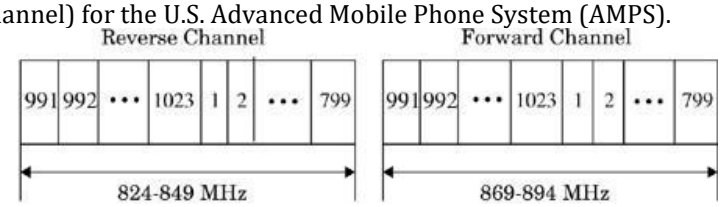
Figure 1.1. The growth of mobile telephony as compared with other popular inventions of the 20th century.

- By 1934, 194 municipal police radio systems and 58 state police stations had adopted amplitude modulation (AM) mobile communication systems for public safety in the U.S.
- In 1935, Edwin Armstrong demonstrated frequency modulation (FM) for the first time, and since the late 1930s, FM has been the primary modulation technique used for mobile communication systems throughout the world.
- With the boom in CB radio and cordless appliances such as garage door openers and telephones, the number of users of mobile and portable radio in 1995 was about 100 million, or 37% of the U.S. population
- The number of worldwide cellular telephone users grew from 25,000 in 1984 to about 25 million in 1993, and since then subscription-based wireless services have been experiencing customer growth rates well in excess of 50% per year. At the beginning of the 21st century, over 1% of the worldwide wireless subscriber population had already abandoned wired telephone service for home use, and had begun to rely solely on their cellular service provider for telephone access.

Mobile Radiotelephony in the U.S.

In 1946, the first public mobile telephone service was introduced in twenty-five major American cities. Each system used a single, high-powered transmitter and large tower in order to cover distances of over 50 km in a particular market. During the 1950s and 1960s, AT&T Bell Laboratories and other telecommunications companies throughout the world developed the theory and techniques of cellular radiotelephony—the concept of breaking a coverage zone (market) into small cells, each of which reuse portions of the spectrum to increase spectrum usage at the expense of greater system infrastructure. AT&T proposed the concept of a cellular mobile system to the FCC in 1968, although technology was not available to implement cellular telephony until the late 1970s. In 1983, the FCC finally allocated 666 duplex channels (40 MHz of spectrum in the 800 MHz band, each channel having a one-way bandwidth of 30 kHz for a total spectrum occupancy of 60

kHz for each duplex channel) for the U.S. Advanced Mobile Phone System (AMPS).



	Channel Number	Center Frequency (MHz)
Reverse Channel	$1 \le N \le 799$	$0.030N + 825.0$
	$991 \le N \le 1023$	$0.030(N - 1023) + 825.0$
Forward Channel	$1 \le N \le 799$	$0.030N + 870.0$
	$991 \le N \le 1023$	$0.030(N - 1023) + 870.0$

(Channels 800–990 are unused)

Figure 1.2. Frequency spectrum allocation for the U.S. cellular radio service

In late 1991, the first US Digital Cellular (USDC) system hardware was installed in major U.S. cities. The USDC standard (Electronic Industry Association Interim Standard IS-54 and later IS-136) allowed cellular operators to replace gracefully some single-user analog channels with digital channels which support three users in the same 30 kHz bandwidth. In this way, U.S. carriers gradually phased out AMPS as more users accepted digital phones

A cellular system based on code division multiple access (CDMA) has been developed by Qualcomm, Inc. and standardized by the Telecommunications Industry Association (TIA) as an Interim Standard (IS-95). This system supports a variable number of users in 1.25 MHz wide channels using direct sequence spread spectrum. CDMA systems can operate at much larger interference levels because of their inherent interference resistance properties. The ability of CDMA to operate with a much smaller signal-to-noise ratio (SNR) than conventional narrowband FM techniques allows CDMA systems to use the same set of frequencies in every cell, which provides a large improvement in capacity.

Personal Communication Service (PCS) licenses in the 1800/1900 MHz band were auctioned by the U.S. Government to wireless providers in early 1995, and these have spawned new wireless services that complement, as well as compete with, cellular and SMR.

Mobile Radio Systems Around the World

Many mobile radio standards have been developed for wireless systems throughout the world, and more standards are likely to emerge. Tables 1.1 through 1.3 list the most common paging, cordless, cellular, and personal communications standards used in North America, Europe, and Japan.

Table 1.1. Major Mobile Radio Standards in North America

Standard	Type	Year Introduction	o Multiple Access	Frequency Band	Modulation	Channel Bandwidth
AMPS	Cellular	1983	FDMA	824-894 MHz	FM	30 kHz
NAMPS	Cellular	1992	FDMA	824-894 MHz	FM	10 kHz
USDC	Cellular	1991	TDMA	824-894 MHz	π/4-DQPSK	30 kHz
CDPD	Cellular	1993	FH/ Packet	824-894 MHz	GMSK	30 kHz
IS-95	Cellular/PCS	1993	CDMA	824-894 MHz 1.8 2.0 GHz	QPSK/BPSK	1.25 MHz
GSC	Paging	1970s	Simplex	Several	FSK	12.5 kHz
POCSAG	Paging	1970s	Simplex	Several	FSK	12.5 kHz
FLEX	Paging	1993	Simplex	Several	4-FSK	15 kHz
DCS-1900 (GSM)	PCS	1994	TDMA	1.85-1.99 GHz	GMSK	200 kHz
PACS	Cordless/PCS	1994	TDMA/FDMA	1.85-1.99 GHz	π/4-DQPSK	300 kHz
MIRS	SMR/PCS	1994	TDMA	Several	16-QAM	25 kHz
iDen	SMR/PCS	1995	TDMA	Several	16-QAM	25 kHz

Table 1.2. Major Mobile Radio Standards in Europe

Standard	Type	Year Introduction	o Multiple Access	Frequency Band	Modulation	Channel Bandwidth
ETACS	Cellular	1985	FDMA	900 MHz	FM	25 kHz

NMT-450	Cellular	1981	FDMA	450-470 MHz	FM	25 kHz
NMT-900	Cellular	1986	FDMA	890-960 MHz	FM	12.5 kHz
GSM	Cellular/PCS	1990	TDMA	890-960 MHz	GMSK	200 kHz
C-450	Cellular	1985	FDMA	450-465 MHz	FM	20 kHz/10 kHz

Standard	**Type**	**Year Introduction**	**o Multiple Access**	**Frequency Band**	**Modulation**	**Channel Bandwidth**
ERMES	Paging	1993	FDMA	Several	4-FSK	25 kHz
CT2	Cordless	1989	FDMA	864-868 MHz	GFSK	100 kHz
DECT	Cordless	1993	TDMA	1880-1900 MHz	GFSK	1.728 MHz
DCS-1800	Cordless/PCS	1993	TDMA	1710-1880 MHz	GMSK	200 kHz

Table 1.3. Major Mobile Radio Standards in Japan

Standard	**Type**	**Year of Introduction**	**Multiple Access**	**Frequency Band**	**Modulation**	**Channel Bandwidth**
JTACS	Cellular	1988	FDMA	860-925 MHz	FM	25 kHz
PDC	Cellular	1993	TDMA	810-1501 MHz	π/4-DQPSK	25 kHz
NTT	Cellular	1979	FDMA	400/800 MHz	FM	25 kHz
NTACS	Cellular	1993	FDMA	843-925 MHz	FM	12.5 kHz
NTT	Paging	1979	FDMA	280 MHz	FSK	12.5 kHz
NEC	Paging	1979	FDMA	Several	FSK	10 kHz
PHS	Cordless	1993	TDMA	1895-1907 MHz	π/4-DQPSK	300 kHz

The world's first cellular system was implemented by the Nippon Telephone and Telegraph company (NTT) in Japan. The system, deployed in 1979, uses 600 FM duplex channels (25 kHz for each one-way link) in the 800 MHz band. In Europe, the Nordic Mobile Telephone system (NMT 450) was developed in 1981 for the 450 MHz band and uses 25 kHz channels. The European Total Access Cellular System (ETACS) was deployed in 1985 and is virtually identical to the U.S. AMPS system, except that the smaller bandwidth channels result in a slight degradation of signal-to-noise ratio (SNR) and coverage range. In Germany, a cellular standard called C-450 was introduced in 1985. The first generation European cellular systems are generally incompatible with one another because of the different frequencies and communication protocols used. These systems are now being replaced by the Pan European digital cellular standard GSM (Global System for Mobile) which was first deployed in 1990 in a new 900 MHz band which all of Europe dedicated for cellular telephone service. The GSM standard has gained worldwide acceptance as the first universal digital cellular system with modern network features extended to each mobile user, and is the leading digital air interface for PCS services above 1800 MHz throughout the world. In Japan, the Pacific Digital Cellular (PDC) standard provides digital cellular coverage using a system similar to North America's USDC.

Examples of Wireless Communication Systems

Most people are familiar with a number of mobile radio communication systems used in everyday life. Garage door openers, remote controllers for home entertainment equipment, cordless telephones, hand-held walkie-talkies, pagers (also called paging receivers or "beepers"), and cellular telephones are all examples of mobile radio communication systems. However, the cost, complexity, performance, and types of services offered by each of these mobile systems are vastly different.

Table 1.4 lists definitions of terms used to describe elements of wireless communication systems.

Table 1.4. Wireless Communications System Definitions

Base Station	A fixed station in a mobile radio system used for radio communication with mobile stations Base stations are located at the center or on the edge of a coverage region and consist o radio channels and transmitter and receiver antennas mounted on a tower.
Control Channel	Radio channel used for transmission of call setup, call request, call initiation, and other beacon or control purposes.
Forward Channel	Radio channel used for transmission of information from the base station to the mobile.
Full Duplex Systems	Communication systems which allow simultaneous two-way communication. Transmissior and reception is typically on two different channels (FDD) although new cordless/PCS systems are using TDD.
Half Duplex Systems	Communication systems which allow two-way communication by using the same radio channel for both transmission and reception. At any given time, the user can only either transmit or receive information.
Handoff	The process of transferring a mobile station from one channel or base station to another.

Mobile Station	A station in the cellular radio service intended for use while in motion at unspecified locations. Mobile stations may be hand-held personal units (portables) or installed in vehicles (mobiles).
Mobile Switching Center	Switching center which coordinates the routing of calls in a large service area. In a cellular radio system, the MSC connects the cellular base stations and the mobiles to the PSTN. An MSC is also called a mobile telephone switching office (MTSO).
Page	A brief message which is broadcast over the entire service area, usually in a simulcast fashion by many base stations at the same time.

Reverse Channel	Radio channel used for transmission of information from the mobile to base station.
Roamer	A mobile station which operates in a service area (market) other than that from which service has been subscribed.
Simplex Systems	Communication systems which provide only one-way communication.
Subscriber	A user who pays subscription charges for using a mobile communications system.
Transceiver	A device capable of simultaneously transmitting and receiving radio signals.

Mobile radio transmission systems may be classified as *simplex, half-duplex* or *full-duplex*. In simplex systems, communication is possible in only one direction. Paging systems, in which messages are received but not acknowledged, are simplex systems. Half-duplex radio systems allow two-way communication, but use the same radio channel for both transmission and reception. This means that at any given time, a user can only transmit or receive information. Constraints like "push-to-talk" and "release-to-listen" are fundamental features of half-duplex systems. Full duplex systems, on the other hand, allow simultaneous radio transmission and reception between a subscriber and a base station, by providing two simultaneous but separate channels (frequency division duplex, or FDD) or adjacent time slots on a single radio channel (time division duplex, or TDD) for communication to and from the user.

In FDD, a pair of simplex channels with a fixed and known frequency separation is used to define a specific radio channel in the system. The channel used to convey traffic to the mobile user from a base station is called the *forward channel*, while the channel used to carry traffic from the mobile user to a base station is called the *reverse channel*. In the U.S. AMPS standard, the reverse channel has a frequency which is exactly 45 MHz lower than that of the forward channel. Full duplex mobile radio systems provide many of the capabilities of the standard telephone, with the added convenience of mobility. Full duplex and half-duplex systems use *transceivers* for radio communication. FDD is used exclusively in analog mobile radio systems.
Time division duplexing (TDD) uses the fact that it is possible to share a single radio channel in time, so that a portion of the time is used to transmit from the base station to the mobile, and the remaining time is used to transmit from the mobile to the base station. If the data transmission rate in the channel is much greater than the end-user's data rate, it is possible to store information bursts and provide the appearance of full duplex operation to a user, even though there are *not* two simultaneous radio transmissions at any instant. TDD is only possible with digital transmission formats and digital modulation, and is very sensitive to timing. It is for this reason that TDD has only recently been used, and only for indoor or small area wireless applications where the physical coverage distances (and thus the radio propagation time delay) are much smaller than the many kilometers used in conventional cellular telephone systems.

Paging Systems
Paging systems are communication systems that send brief messages to a subscriber. Depending on the type of service, the message may be either a numeric message, an alphanumeric message, or a voice message. Paging systems are typically used to notify a subscriber of the need to call a particular telephone number or travel to a known location to receive further instructions. In modern paging systems, news headlines, stock quotations, and faxes may be sent. A message is sent to a paging subscriber via the paging system access number (usually a toll-free telephone number) with a telephone keypad or modem. The issued message is called a *page*. The paging system then transmits the page throughout the service area using base stations which broadcast the page on a radio carrier.

Paging systems vary widely in their complexity and coverage area. While simple paging systems may cover a limited range of 2 to 5 km, or may even be confined to within individual buildings, wide area paging systems can provide worldwide coverage. Though paging receivers are simple and inexpensive, the transmission system required is quite sophisticated. Wide area paging systems consist of a network of telephone lines, many base station transmitters, and large radio towers that simultaneously broadcast a page from each base station (this is called *simulcasting*). Simulcast transmitters may be located within the same service area or in different cities or countries. Paging systems are designed to provide reliable communication to subscribers wherever they are; whether inside a building, driving on a highway, or flying in an airplane. This necessitates large transmitter powers (on the order of kilowatts) and low data rates (a couple of thousand bits per second) for maximum coverage from each base station. Figure 1.3 shows a diagram of a wide area paging system.

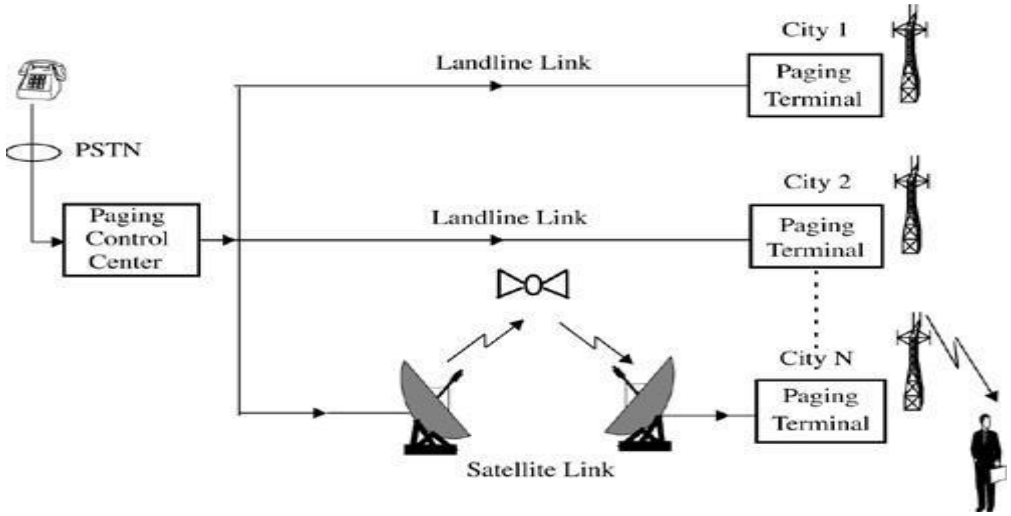


Figure 1.3. A wide area paging system. The paging control center dispatches pages received from the PSTN throughout several cities at the same time.

Paging systems are designed to provide ultra-reliable coverage, even inside buildings. Buildings can attenuate radio signals by 20 or 30 dB, making the choice of base station locations difficult for the paging companies. For this reason, paging transmitters are usually located on tall buildings in the center of a city, and simulcasting is used in conjunction with additional base stations located on the perimeter of the city to flood the entire area. Small RF bandwidths are used to maximize the signal-to-noise ratio at each paging receiver, so low data rates (6400 bps or less) are used.

Cordless Telephone Systems

Cordless telephone systems are full duplex communication systems that use radio to connect a portable handset to a dedicated base station, which is then connected to a dedicated telephone line with a specific telephone number on the public switched telephone network (PSTN). In first generation cordless telephone systems (manufactured in the 1980s), the portable unit communicates only to the dedicated base unit and only over distances of a few tens of meters. Early cordless telephones operate solely as extension telephones to a transceiver connected to a subscriber line on the PSTN and are primarily for in-home use.

Second generation cordless telephones have recently been introduced which allow subscribers to use their handsets at many outdoor locations within urban centers such as London or Hong Kong. Modern cordless telephones are sometimes combined with paging receivers so that a subscriber may first be paged and then respond to the page using the cordless telephone. Cordless telephone systems provide the user with limited range and mobility, as it is usually not possible to maintain a call if the user travels outside the range of the base station. Typical second generation base stations provide coverage ranges up to a few hundred meters. Figure 1.4 illustrates a cordless telephone system.

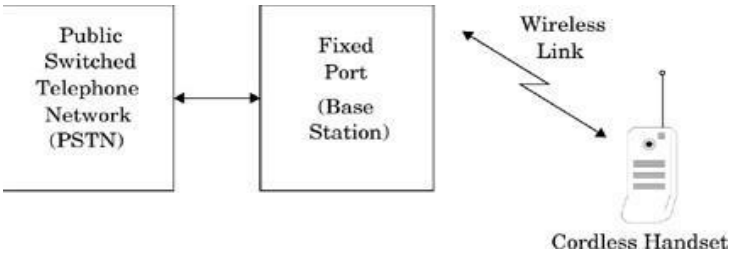


Figure 1.4. A cordless telephone system.

Cellular Telephone Systems

A cellular telephone system provides a wireless connection to the PSTN for any user location within the radio

range of the system. Cellular systems accommodate a large number of users over a large geographic area, within a limited frequency spectrum. Cellular radio systems provide high quality service that is often comparable to that of the landline telephone systems. High capacity is achieved by limiting the coverage of each base station transmitter to a small geographic area called a *cell* so that the same radio channels may be reused by another base station located some distance away. A sophisticated switching technique called a *handoff* enables a call to proceed uninterrupted when the user moves from one cell to another.

Figure 1.5 shows a basic cellular system which consists of *mobile stations, base stations* and a *mobile switching center* (MSC). The mobile switching center is sometimes called a *mobile telephone switching office* (MTSO), since it is responsible for connecting all mobiles to the PSTN in a cellular system. Each mobile communicates via radio with one of the base stations and may be handed-off to any number of base stations throughout the duration of a call. The mobile station contains a transceiver, an antenna, and control circuitry, and may be mounted in a vehicle or used as a portable hand-held unit. The base stations consist of several transmitters and receivers which simultaneously handle full duplex communications and generally have towers which support several transmitting and receiving antennas. The base station serves as a bridge between all mobile users in the cell and connects the simultaneous mobile calls via telephone lines or microwave links to the MSC. The MSC coordinates the activities of all of the base stations and connects the entire cellular system to the PSTN. A typical MSC handles 100,000 cellular subscribers and 5,000 simultaneous conversations at a time, and accommodates all billing and system maintenance functions, as well. In large cities, several MSCs are used by a single carrier.

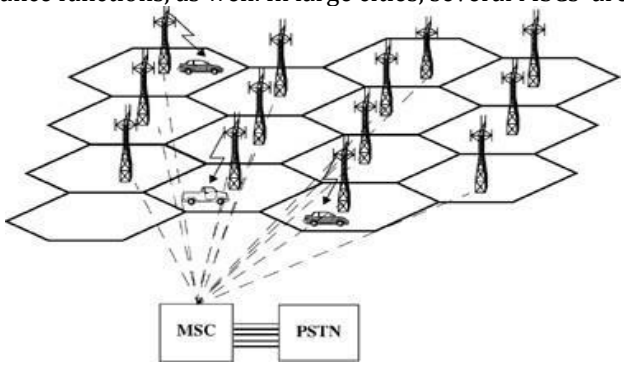


Figure 1.5. A cellular system. The towers represent base stations which provide radio access between mobile users and the mobile switching center (MSC).

Communication between the base station and the mobiles is defined by a standard *common air interface* (CAI) that specifies four different channels. The channels used for voice transmission from the base station to mobiles are called *forward voice channels* (FVC), and the channels used for voice transmission from mobiles to the base station are called *reverse voice channels* (RVC). The two channels responsible for initiating mobile calls are the *forward control channels* (FCC) and *reverse control channels* (RCC). Control channels are often called *setup channels* because they are only involved in setting up a call and moving it to an unused voice channel. Control channels transmit and receive data messages that carry call initiation and service requests, and are monitored by mobiles when they do not have a call in progress. Forward control channels also serve as beacons which continually broadcast all of the traffic requests for all mobiles in the system.

Cellular systems rely on the frequency reuse concept, which requires that the forward control channels (FCCs) in neighboring cells be different. By defining a relatively small number of FCCs as part of the common air interface, cellular phones can be manufactured by many companies which can rapidly scan all of the possible FCCs to determine the strongest channel at any time. Once finding the strongest signal, the cellular phone receiver stays "camped" to the particular FCC. By broadcasting the same setup data on all FCCs at the same time, the MSC is able to signal all subscribers within the cellular system and can be certain that any mobile will be signaled when it receives a call via the PSTN.

How a Cellular Telephone Call is Made

When a cellular phone is turned on, but is not yet engaged in a call, it first scans the group of forward control channels to determine the one with the strongest signal, and then monitors that control channel until the signal

drops below a usable level. At this point, it again scans the control channels in search of the strongest base station signal. When a telephone call is placed to a mobile user, the MSC dispatches the request to all base stations in the cellular system. The *mobile identification number* (MIN), which is the subscriber's telephone number, is then broadcast as a paging message over all of the forward control channels throughout the cellular system. The mobile receives the paging message sent by the base station which it monitors, and responds by identifying itself over the reverse control channel. The base station relays the acknowledgment sent by the mobile and informs the MSC of the handshake. Then, the MSC instructs the base station to move the call to an unused voice channel within the cell (typically, between ten to sixty voice channels and just one control channel are used in each cell's base station). At this point, the base station signals the mobile to change frequencies to an unused forward and reverse voice channel pair, at which point another data message (called an *alert*) is transmitted over the forward voice channel to instruct the mobile telephone to ring, thereby instructing the mobile user to answer the phone. Figure 1.6 shows the sequence of events involved with connecting a call to a mobile user in a cellular telephone system. All of these events occur within a few seconds and are not noticeable by the user.

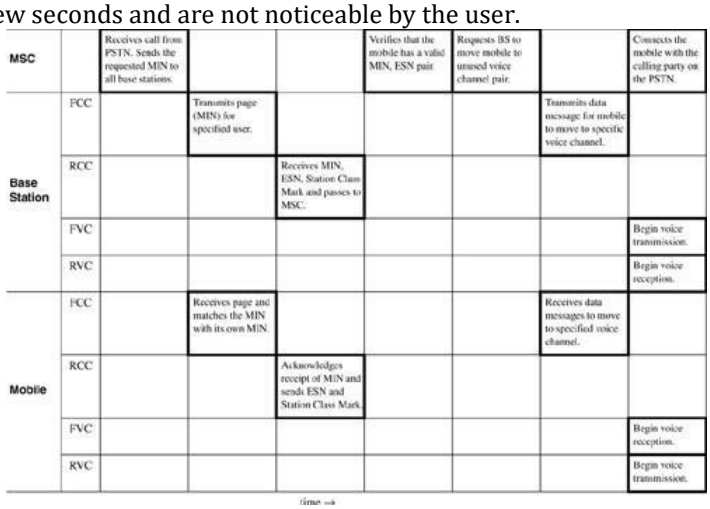


Figure 1.6. Timing diagram illustrating how a call to a mobile user initiated by a landline subscriber is established.

Once a call is in progress, the MSC adjusts the transmitted power of the mobile and changes the channel of the mobile unit and base stations in order to maintain call quality as the subscriber moves in and out of range of each base station. This is called a *handoff*. Special control signaling is applied to the voice channels so that the mobile unit may be controlled by the base station and the MSC while a call is in progress.

When a mobile originates a call, a call initiation request is sent on the reverse control channel. With this request the mobile unit transmits its telephone number (MIN), *electronic serial number* (ESN), and the telephone number of the called party. The mobile also transmits a *station class mark* (SCM) which indicates what the maximum transmitter power level is for the particular user. The cell base station receives this data and sends it to the MSC. The MSC validates the request, makes connection to the called party through the PSTN, and instructs the base station and mobile user to move to an unused forward and reverse voice channel pair to allow the conversation to begin. Figure 1.7 shows the sequence of events involved with connecting a call which is initiated by a mobile user in a cellular system.

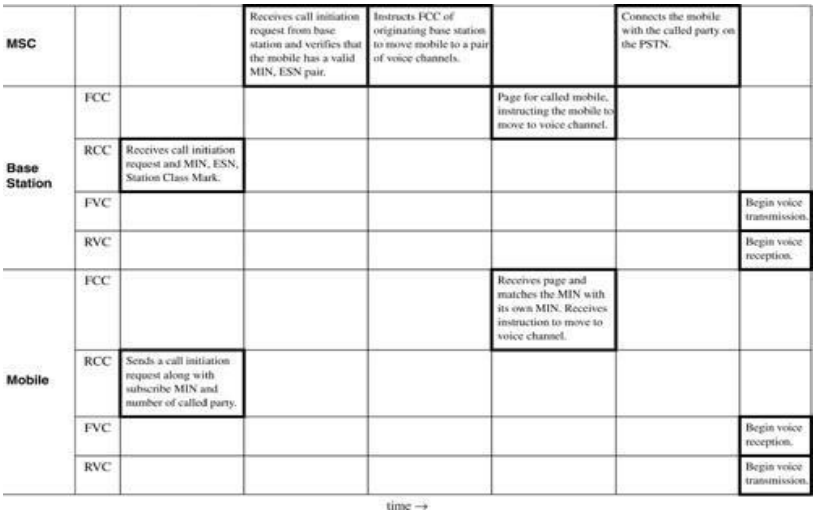


Figure 1.7. Timing diagram illustrating how a call initiated by a mobile is established.

All cellular systems provide a service called *roaming*. This allows subscribers to operate in service areas other than the one from which service is subscribed. When a mobile enters a city or geographic area that is different from its home service area, it is registered as a roamer in the new service area. If a particular roamer has roaming authorization for billing purposes, the MSC registers the subscriber as a valid roamer. Once registered, roaming mobiles are allowed to receive and place calls from that area, and billing is routed automatically to the subscriber's home service provider.

Comparison of Common Wireless Communication Systems

Tables 1.5 and 1.6 illustrate the types of service, level of infrastructure, cost, and complexity required for the subscriber segment and base station segment of each of the five mobile or portable radio systems discussed earlier in this chapter. For comparison purposes, common household wireless remote devices are shown in the table. It is important to note that each of the five mobile radio systems given in Tables 1.5 and 1.6 use a fixed base station, and for good reason. Virtually all mobile radio communication systems strive to connect a moving terminal to a fixed distribution system of some sort and attempt to look invisible to the distribution system.

Table 1.5. Comparison of Mobile Communication Systems—Mobile Station

Service	Coverage Range	Required Infrastructure	Complexity	Hardware Cost	Carrier Frequency	Functionality
TV Remote Control	Low	Low	Low	Low	Infrared	Transmitter
Garage Door Opener	Low	Low	Low	Low	< 100 MHz	Transmitter
Paging System	High	High	Low	Low	< 1 GHz	Receiver
Cordless Phone	Low	Low	Moderate	Low	< 1 GHz	Transceiver
Cellular Phone	High	High	High	Moderate	< 2 GHz	Transceiver

Table 1.6. Comparison of Mobile Communication Systems—Base Station

Service	Coverage Range	Required Infrastructure	Complexity	Hardware Cost	Carrier Frequency	Functionality
TV Remote Control	Low	Low	Low	Low	Infrared	Receiver
Garage Door Opener	Low	Low	Low	Low	< 100 MHz	Receiver
Paging System	High	High	High	High	< 1 GHz	Transmitter
Cordless Phone	Low	Low	Low	Moderate	< 1 GHz	Transceiver

Cellular Phone	High	High	High	High	< 2 GHz	Transceiver

Notice that the expectations vary widely among the services, and the infrastructure costs are dependent upon the required coverage area. For the case of low power, hand-held cellular phones, a large number of base stations are required to insure that any phone is in close range to a base station within a city. If base stations were not within close range, a great deal of transmitter power would be required of the phone, thus limiting the battery life and rendering the service useless for hand-held users.

Trends in Cellular Radio and Personal Communications

Since 1989, there has been enormous activity throughout the world to develop personal wireless systems that combine the network intelligence of today's PSTN with modern digital signal processing and RF technology. The concept, called Personal Communication Services (PCS), originated in the United Kingdom when three companies were given spectrum in the 1800 MHz range to develop Personal Communication Networks (PCN) throughout Great Britain. PCN was seen by the U.K. as a means of improving its international competitiveness in the wireless field while developing new wireless systems and services for citizens.

Indoor wireless networking products are rapidly emerging and promise to become a major part of the telecommunications infrastructure within the next decade. An international standards body, IEEE 802.11, is developing standards for wireless access between computers inside buildings. The European Telecommunications Standard Institute (ETSI) is also developing the 20 Mbps HIPERLAN standard for indoor wireless networks. Products have emerged that allow users to link their phone with their computer within an office environment, as well as in a public setting, such as an airport or train station.

A worldwide standard, the Future Public Land Mobile Telephone System (FPLMTS)—renamed International Mobile Telecommunication 2000 (IMT-2000) in mid-1995—has been formulated by the International Telecommunications Union (ITU) which is the standards body for the United Nations, with headquarters in Geneva, Switzerland. FPLMTS (now IMT-2000) is a third generation universal, multi-function, globally compatible digital mobile radio system that will integrate paging, cordless, and cellular systems, as well as low earth orbit (LEO) satellites, into one universal mobile system.

In emerging nations, where existing telephone service is almost nonexistent, fixed cellular telephone systems are being installed at a rapid rate. This is due to the fact that developing nations are finding it is quicker and more affordable to install cellular telephone systems for fixed home use, rather than install wires in neighborhoods which have not yet received telephone connections to the PSTN.

Modern Wireless Communication Systems

Since the mid 1990s, the cellular communications industry has witnessed explosive growth. Wireless communications networks have become much more pervasive than anyone could have imagined when the cellular concept was first developed in the 1960s and 1970s. The widespread adoption of wireless communications was accelerated in the mid 1990s, when governments throughout the world provided increased competition and new radio spectrum licenses for personal communications services (PCS) in the 1800–2000 MHz frequency bands.

Multiple Access Techniques for Wireless Communications

Multiple access schemes are used to allow many mobile users to share simultaneously a finite amount of radio spectrum. The sharing of spectrum is required to achieve high capacity by simultaneously allocating the available bandwidth (or the available amount of channels) to multiple users. For high quality communications, this must be done without severe degradation

in the performance of the system.

Introduction

In wireless communications systems, it is often desirable to allow the subscriber to send simultaneously information to the base station while receiving information from the base station. For example, in conventional telephone systems, it is possible to talk and listen simultaneously, and this effect, called *duplexing*, is generally required in wireless telephone systems.

Duplexing may be done using frequency or time domain techniques. *Frequency division duplexing* (FDD) provides two distinct bands of frequencies for every user. The *forward band* provides traffic from the base station to the mobile, and the *reverse band* provides traffic from the mobile to the base station. In FDD, any *duplex channel*actually consists of two simplex channels (a forward and reverse), and a device called a *duplexer* is used inside each subscriber unit and base station to allow simultaneous bidirectional radio transmission and reception for both the subscriber unit and the base station on the duplex channel pair. The frequency separation between each forward and reverse channel is constant throughout the system, regardless of the particular channel being used.

Time division duplexing (TDD) uses time instead of frequency to provide both a forward and reverse link. In TDD, multiple users share a single radio channel by taking turns in the time domain. Individual users are allowed to access the channel in assigned *time slots*, and each duplex channel has both a forward time slot and a reverse time slot to facilitate bidirectional communication. If the time separation between the forward and reverse time slot is small, then the

transmission and reception of data appears simultaneous to the users at both the subscriber unit and on the base station side. Figure 1 illustrates FDD and TDD techniques. TDD allows communication on a single channel (as opposed to requiring two separate simplex or dedicated channels) and simplifies the subscriber equipment since a duplexer is not required.

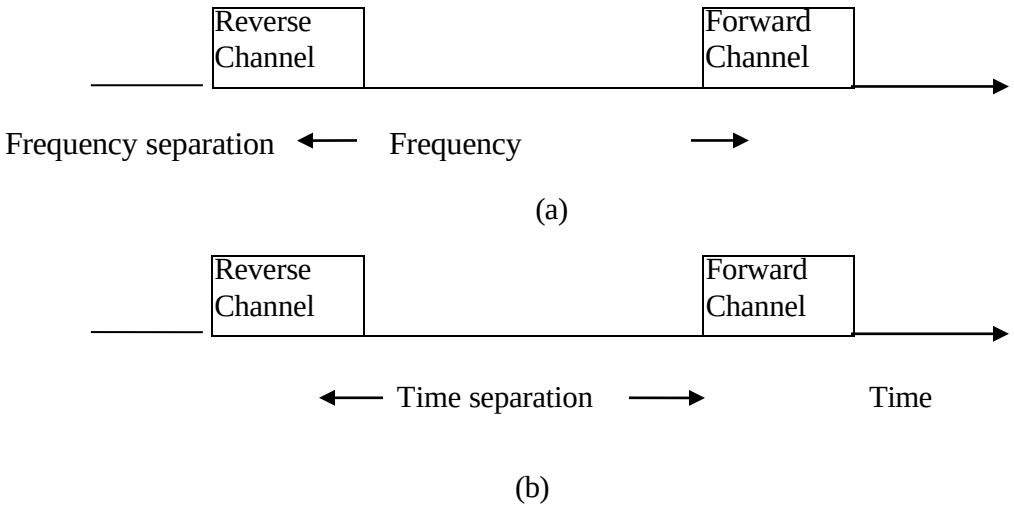


Figure 1 (a) FDD provides two simplex channels at the same time; (b) TDD provides two simplex time slots on the same frequency.

There are several tradeoffs between FDD and TDD approaches. FDD is geared toward radio communications systems that allocate individual radio frequencies for each user. Because each transceiver simultaneously transmits and receives radio signals which can vary by more than 100 dB, the frequency allocation used for the forward and reverse channels must be carefully coordinated within its own system and with out-of-band users that occupy spectrum between these two bands. Furthermore, the frequency separation must be coordinated to permit the use of inexpensive RF and oscillator technology. TDD enables each transceiver to operate as either a transmitter or receiver on the same frequency, and eliminates the need for separate forward and reverse frequency bands. However, there is a time latency created by TDD due to the fact that communications is not full duplex in the truest sense, and this latency creates inherent sensitivities to propagation delays of individual users. Because of the rigid timing required for time slotting, TDD generally is limited to cordless phone or short range portable access. TDD is effective for fixed wireless access when all users are stationary so that propagation delays do not vary in time among the users.

Introduction to Multiple Access

Frequency division multiple access (FDMA), *time division multiple access* (TDMA), and *code division multiple access* (CDMA) are the three major access techniques used to share the available bandwidth in a wireless communication system. These techniques can be grouped as *narrowband* and *wideband* systems, depending upon how the available bandwidth is allocated to the users. The duplexing technique of a multiple access system is usually described along with the particular multiple access scheme, as shown in the examples that follow.

Narrowband Systems — The term *narrowband* is used to relate the bandwidth of a single channel to the expected coherence bandwidth of the channel. In a narrowband multiple access system, the available radio spectrum is divided into a large number of narrowband channels. The channels are usually operated using FDD. To minimize interference between forward and reverse links on each channel, the frequency separation is made as great as possible within the frequency spectrum, while still allowing inexpensive duplexers and a common transceiver antenna to be used in each subscriber unit. In narrowband FDMA, a user is assigned a particular channel which is not shared by other users in the vicinity, and if FDD is used (that is, each duplex channel has a forward and reverse simplex channel), then the system is called FDMA/FDD. Narrowband TDMA, on the other hand, allows users to share the same radio channel but allocates a unique time slot to each user in a cyclical fashion on the channel, thus separating a small number of users in time on a single channel. For narrowband TDMA systems, there generally are a large number of radio channels allocated using either FDD or TDD, and each channel is shared using TDMA. Such systems are called TDMA/FDD or TDMA/TDD access systems.

Wideband systems — In wideband systems, the transmission bandwidth of a single channel is much larger than the coherence bandwidth of the channel. Thus, multipath fading does not greatly vary the received signal power within a wideband channel, and frequency selective fades occur in only a small fraction of the signal bandwidth at any instance of time. In wideband multiple access systems a large number of transmitters are allowed to transmit on the same channel. TDMA allocates time slots to the many transmitters on the same channel and allows only one transmitter to access the channel at any instant of time, whereas spread spectrum

CDMA allows all of the transmitters to access the channel at the same time. TDMA and CDMA systems may use either FDD or TDD multiplexing techniques.

In addition to FDMA, TDMA, and CDMA, two other multiple access schemes will be used for wireless communications. These are *packet radio* (PR) and *space division multiple access* (SDMA).

Frequency Division Multiple Access (FDMA)

Frequency division multiple access (FDMA) assigns individual channels to individual users. It can be seen from Figure 2 that each user is allocated a unique frequency band or channel. These channels are assigned on demand to users who request service. During the period of the call, no other user can share the same channel. In FDD systems, the users are assigned a channel as a pair of frequencies; one frequency is used for the forward channel, while the other frequency is used for the reverse channel. The features of FDMA are as follows:

- The FDMA channel carries only one phone circuit at a time.
- If an FDMA channel is not in use, then it sits idle and cannot be used by other users to increase or share capacity. It is essentially a wasted resource.

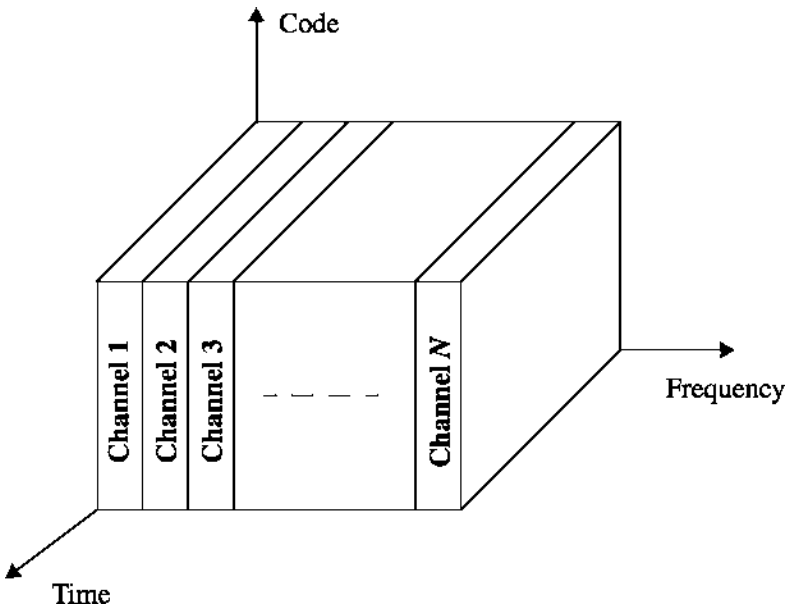


Figure 2 FDMA where different channels are assigned different frequency bands

- After the assignment of a voice channel, the base station and the mobile transmit simultaneously and continuously.
- The bandwidths of FDMA channels are relatively narrow (30 kHz in AMPS) as each channel supports only one circuit per carrier. That is, FDMA is usually implemented in narrowband systems.
- The symbol time of a narrowband signal is large as compared to the average delay spread. This implies that the amount of intersymbol interference is low and, thus, little or no equalization is required in FDMA narrowband systems.
- The complexity of FDMA mobile systems is lower when compared to TDMA systems, though this is changing as digital signal processing methods improve for TDMA.
- Since FDMA is a continuous transmission scheme, fewer bits are needed for overhead purposes (such as synchronization and framing bits) as compared to TDMA.
- FDMA systems have higher cell site system costs as compared to TDMA systems, because of the single channel per carrier design, and the need to use costly bandpass filters to eliminate spurious radiation at the base station.
- The FDMA mobile unit uses duplexers since both the transmitter and receiver operate at the same time. This results in an increase in the cost of FDMA subscriber units and base stations.
- FDMA requires tight RF filtering to minimize adjacent channel interference

Nonlinear Effects in FDMA — In a FDMA system, many channels share the same antenna at the base station. The power amplifiers or the power combiners, when operated at or near saturation for maximum power efficiency, are nonlinear. The nonlinearities cause signal spreading in the frequency domain and generate *intermodulation* (IM) frequencies. IM is undesired RF radiation which can interfere with other channels in the FDMA systems. Spreading of the spectrum results in adjacent-channel interference. Intermodulation is the generation of undesirable harmonics. Harmonics generated outside the mobile radio band cause interference to adjacent services, while those present inside the band cause interference to other users in the wireless system .

The first US analog cellular system, the *Advanced Mobile Phone System* (AMPS), is based on FDMA/FDD. A single user occupies a single channel while the call is in progress, and the single channel is actually two simplex channels which are frequency duplexed with a 45 MHz split. When a call is completed, or when a handoff occurs, the channel is vacated so that another mobile subscriber may use it. Multiple or simultaneous users are accommodated in AMPS by giving each user a unique channel. Voice signals are sent on the forward channel from the base station to mobile unit, and on the reverse channel from the mobile unit to the base station. In AMPS, analog narrowband frequency modulation (NBFM) is used to modulate the carrier. The number of channels that can be simultaneously supported in a FDMA system is given by:

$$N = \frac{B_t - 2B_{guard}}{B_c}$$

where B_t is the total spectrum allocation, B_{guard} is the guard band allocated at the edge of the allocated spectrum band, and B_c is the channel bandwidth. Note that B_t and B_c may be specified in terms of simplex bandwidths where it is understood that there are symmetric frequency allocations for the forward band and reverse band.

Time Division Multiple Access (TDMA)

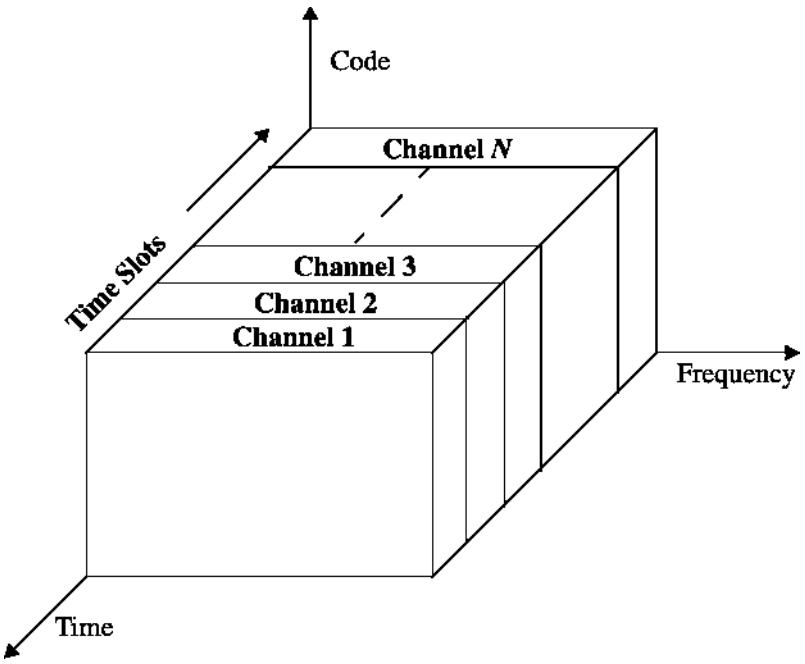


Figure 3 TDMA scheme where each channel occupies a cyclically repeating time slot.

Time division multiple access (TDMA) systems divide the radio spectrum into time slots, and in each slot only one user is allowed to either transmit or receive. It can be seen from Figure 3 that each user occupies a cyclically repeating time slot, so a channel may be thought of as a particular time slot that reoccurs every frame, where *N* time slots comprise a frame. TDMA systems transmit data in a *buffer-and-burst* method, thus the transmission for any user is non-continuous. This implies that, unlike in FDMA systems which accommodate analog FM, digital data and digital modulation must be used with TDMA. The transmission from various users is interlaced into a repeating frame structure as shown in Figure 4. It can be seen that a frame consists of a number of slots. Each frame is made up of a preamble, an information message, and tail bits. In TDMA/ TDD, half of the time slots in the frame information message would be used for the forward link channels and half would be used for reverse link channels. In TDMA/FDD systems, an identical or similar frame structure would be used solely for either forward or reverse transmission, but the carrier frequencies would be different for the forward and reverse links. In general, TDMA/FDD systems intentionally induce several time slots of delay between the forward and reverse time slots for a particular user, so that duplexers are not required in the

subscriber unit.

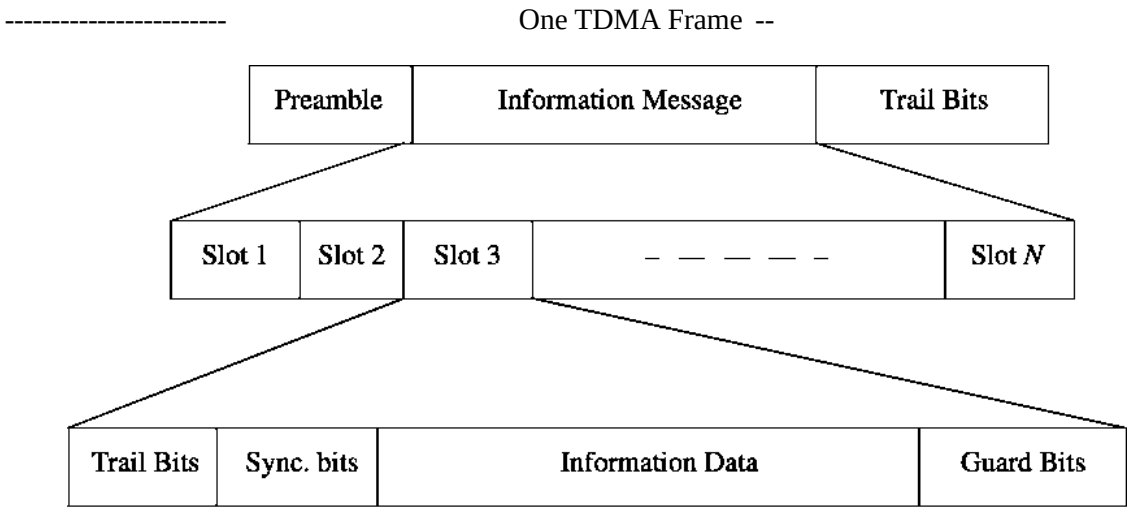


Figure 4 TDMA frame structure. The frame is cyclically repeated over time.

In a TDMA frame, the preamble contains the address and synchronization information that both the base station and the subscribers use to identify each other. Guard times are utilized to allow synchronization of the receivers between different slots and frames. Different TDMA standards have different TDMA frame structures.

The features of TDMA include the following:

- TDMA shares a single carrier frequency with several users, where each user makes use of non-overlapping time slots. The number of time slots per frame depends on several factors, such as modulation technique, available bandwidth, etc.
- Data transmission for users of a TDMA system is not continuous but occurs in bursts. This results in low battery consumption, since the subscriber transmitter can be turned off when not in use (which is most of the time).
- Because of discontinuous transmissions in TDMA, the handoff process is much simpler for a subscriber unit, since it is able to listen for other base stations during idle time slots. An enhanced link control, such as that provided by *mobile assisted handoff* (MAHO) can be carried out by a subscriber by listening on an idle slot in the TDMA frame.
- TDMA uses different time slots for transmission and reception, thus duplexers are not required. Even if FDD is used, a switch rather than a duplexer inside the subscriber unit is

all that is required to switch between transmitter and receiver using TDMA.

- Adaptive equalization is usually necessary in TDMA systems, since the transmission rates are generally very high as compared to FDMA channels.
- In TDMA, the guard time should be minimized. If the transmitted signal at the edges of a time slot are suppressed sharply in order to shorten the guard time, the transmitted spectrum will expand and cause interference to adjacent channels.
- High synchronization overhead is required in TDMA systems because of burst transmissions. TDMA transmissions are slotted, and this requires the receivers to be synchronized for each data burst. In addition, guard slots are necessary to separate users, and this results in the TDMA systems having larger overheads as compared to FDMA.
- TDMA has an advantage in that it is possible to allocate different numbers of time slots per frame to different users. Thus, bandwidth can be supplied on demand to different users by concatenating or reassigning time slots based on priority.

Efficiency of TDMA — The efficiency of a TDMA system is a measure of the percentage of transmitted data that contains information as opposed to providing overhead for the access scheme. The frame efficiency η_f, is the percentage of bits per frame which contain transmitted data. Note that the transmitted data may include source and channel coding bits, so the raw end-user efficiency of a system is generally less than η_f. The frame efficiency can be found as follows.

The number of overhead bits per frame is,

$$\boldsymbol{b_{OH} = N_r b_r + N_t b_p + N_t b_g + N_r b_g}$$

where N_r is the number of reference bursts per frame, N_t is the number of traffic bursts per frame, b_r is the number of overhead bits per reference burst, b_p is the number of overhead bits per preamble in each slot, and b_g is the number of equivalent bits in each guard time interval. The total number of bits per frame, b_T, is

$$b_T = T_f R$$

where T_f- is the frame duration, and R is the channel bit rate. The frame efficiency η_f is thus given as

$$\eta_f = \left(1 - \frac{b_{OH}}{b_T}\right) \times 100\%$$

Number of channels in TDMA system – The number of TDMA channel slots that can be provided in a TDMA system is found by multiplying the number of TDMA slots per channel by the number of channels available and is given by

$$N = \frac{m(B_{tot} - 2B_{guard})}{B_c}$$

where *m* is the maximum number of TDMA users supported on each radio channel. Note that two guard bands, one at the low end of the allocated frequency band and one at the high end, are required to ensure that users at the edge of the band do not "bleed over" into an adjacent radio service.

Spread Spectrum Multiple Access

Spread spectrum multiple access (SSMA) uses signals which have a transmission bandwidth that is several orders of magnitude greater than the minimum required RF bandwidth. A pseudo-noise (PN) sequence converts a narrowband signal to a wideband noise-like signal before transmission. SSMA also provides immunity to multipath interference and robust multiple access capability. SSMA is not very bandwidth efficient when used by a single user. However, since many users can share the same spread spectrum bandwidth without interfering with one another, spread spectrum systems become bandwidth efficient in a multiple user environment. It is exactly this situation that is of interest to wireless system designers. There are two main types of spread spectrum multiple access techniques; *frequency hopped multiple access* (FH) and *direct sequence multiple access* (DS). Direct sequence multiple access is also called *code division multiple access* (CDMA).

Frequency Hopped Multiple Access (FHMA)

Frequency hopped multiple access (FHMA) is a digital multiple access system in which the carrier frequencies of the individual users are varied in a pseudorandom fashion within a wideband channel. Figure 5 illustrates how FHMA allows multiple users to simultaneously occupy the

same spectrum at the same time, where each user dwells at a specific narrowband channel at a particular instance of time, based on the particular PN code of the user. The digital data of each user is broken into uniform sized bursts which are transmitted on different channels within the allocated spectrum band. The instantaneous bandwidth of any one transmission burst is much smaller than the total spread bandwidth. The pseudorandom change of the channel frequencies of the user randomizes the occupancy of a specific channel at any given time, thereby allowing for multiple access over a wide range of frequencies. In the FH receiver, a locally generated PN code is used to synchronize the receiver's instantaneous frequency with that of the transmitter. At any given point in time, a frequency hopped signal only occupies a single, relatively narrow channel since narrowband FM or FSK is used. The difference between FHMA and a traditional FDMA system is that the frequency hopped signal changes channels at rapid intervals. If the rate of change of the carrier frequency is greater than the symbol rate, then the system is referred to as *a fast frequency hopping system.* If the channel changes at a rate less than or equal to the symbol rate, it is called *slow frequency hopping.* A fast frequency hopper may thus be thought of as an FDMA system which employs frequency diversity. FHMA systems often employ energy efficient constant envelope modulation. Inexpensive receivers may be built to provide non-coherent detection of FHMA. This implies that linearity is not an issue, and the power of multiple users at the receiver does not degrade FHMA performance.

A frequency hopped system provides a level of security, especially when a large number of channels are used, since an unintended (or an intercepting) receiver that does not know the pseudorandom sequence of frequency slots must retune rapidly to search for the signal it wishes to intercept. In addition, the FH signal is somewhat immune to fading, since error control coding and interleaving can be used to protect the frequency hopped signal against deep fades which may occasionally occur during the hopping sequence. Error control coding and interleaving can also be combined to guard against *erasures* which can occur when two or more users transmit on the same channel at the same time. Bluetooth and Home RF wireless technologies have adopted FHMA for power efficiency and low cost implementation.

Code Division Multiple Access (CDMA)

In *code division multiple access* (CDMA) systems, the narrowband message signal is multiplied

by a very large bandwidth signal called the *spreading signal.* The spreading signal is a pseudo-noise code sequence that has a chip rate which is orders of magnitudes greater than the data rate of the message. All users in a CDMA system, as seen from Figure 5, use the same carrier frequency and may transmit simultaneously. Each user has its own pseudorandom codeword which is approximately orthogonal to all other codewords. The receiver performs a time correlation operation to detect only the specific desired codeword. All other code words appear as noise due to de-correlation. For detection of the message signal, the receiver needs to know the codeword used by the transmitter. Each user operates independently with no knowledge of the other users.

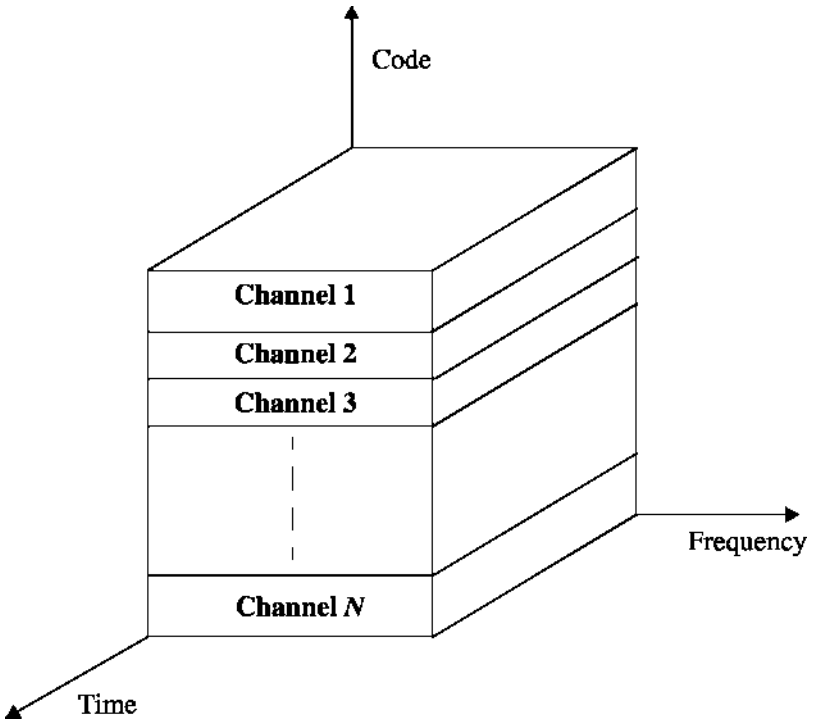


Figure 5 Spread spectrum multiple access in which each channel is assigned a unique PN code which is orthogonal or approximately orthogonal to PN codes used by other users.

In CDMA, the power of multiple users at a receiver determines the noise floor after de-correlation. If the power of each user within a cell is not controlled such that they do not appear equal at the base station receiver, then the *near-far problem* occurs.

The near-far problem occurs when many mobile users share the same channel. In general, the strongest received mobile signal will *capture* the demodulator at a base station. In CDMA,

stronger received signal levels raise the noise floor at the base station demodulators for the weaker signals, thereby decreasing the probability that weaker signals will be received. To combat the near-far problem, *power control* is used in most CDMA implementations. Power control is provided by each base station in a cellular system and assures that each mobile within the base station coverage area provides the same signal level to the base station receiver. This solves the problem of a nearby subscriber overpowering the base station receiver and drowning out the signals of far away subscribers. Power control is implemented at the base station by rapidly sampling the radio signal strength indicator (RSSI) levels of each mobile and then sending a power change command over the forward radio link. Despite the use of power control within each cell, out-of-cell mobiles provide interference which is not under the control of the receiving base station.

The features of CDMA including the following:

- Many users of a CDMA system share the same frequency. Either TDD or FDD may be used.
- Unlike TDMA or FDMA, CDMA has a soft capacity limit. Increasing the number of users in a CDMA system raises the noise floor in a linear manner. Thus, there is no absolute limit on the number of users in CDMA. Rather, the system performance gradually degrades for all users as the number of users is increased, and improves as the number of users is decreased.
- Multipath fading may be substantially reduced because the signal is spread over a large spectrum. If the spread spectrum bandwidth is greater than the coherence bandwidth of the channel, the inherent frequency diversity will mitigate the effects of small-scale fading.
- Channel data rates are very high in CDMA systems. Consequently, the symbol (chip) duration is very short and usually much less than the channel delay spread. Since PN sequences have low autocorrelation, multipath which is delayed by more than a chip will appear as noise. A RAKE receiver can be used to improve reception by collecting time delayed versions of the required signal.
- Since CDMA uses co-channel cells, it can use macroscopic spatial diversity to provide

soft handoff. Soft handoff is performed by the MSC, which can simultaneously monitor a particular user from two or more base stations. The MSC may chose the best version of the signal at any time without switching frequencies.

- Self-jamming is a problem in CDMA system. Self-jamming arises from the fact that the spreading sequences of different users are not exactly orthogonal, hence in the de-spreading of a particular PN code, non-zero contributions to the receiver decision statistic for a desired user arise from the transmissions of other users in the system.
- The near-far problem occurs at a CDMA receiver if an undesired user has a high detected power as compared to the desired user.

Space Division Multiple Access (SDMA)

Space division multiple access (SDMA) controls the radiated energy for each user in space. It can be seen from Figure 8 that SDMA serves different users by using spot beam antennas. These different areas covered by the antenna beam may be served by the same frequency (in a TDMA or CDMA system) or different frequencies (in an FDMA system). Sectorized antennas may be thought of as a primitive application of SDMA. In the future, adaptive antennas will likely be used to simultaneously steer energy in the direction of many users at once and appear to be best suited for TDMA and CDMA base station architectures.

The reverse link presents the most difficulty in cellular systems for several reasons. First, the base station has complete control over the power of all the transmitted signals on the forward link. However, because of different radio propagation paths between each user and the base station, the transmitted power from each subscriber unit must be dynamically controlled to prevent any single user from driving up the interference level for all other users. Second, transmit power is limited by battery consumption at the subscriber unit, therefore there are limits on the degree to which power may be controlled on the reverse link. If the base station antenna is made to spatially filter each desired user so that more energy is detected from each subscriber, then the reverse link for each user is improved and less power is required.

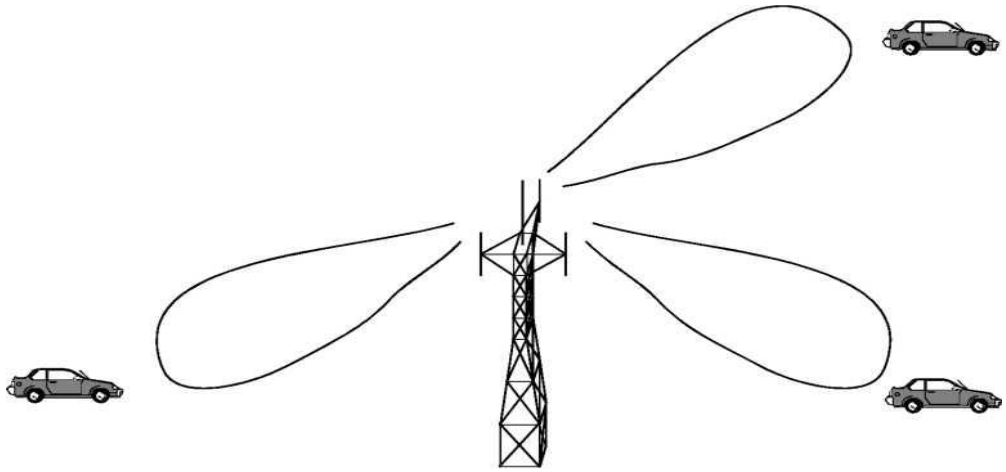


Figure 8 A spatially filtered base station antenna serving different users by using spot beams.

Adaptive antennas used at the base station (and eventually at the subscriber units) promise to mitigate some of the problems on the reverse link. In the limiting case of infinitesimal beam-width and infinitely fast tracking ability, adaptive antennas implement optimal SDMA, thereby providing a unique channel that is free from the interference of all other users in the cell. With SDMA, all users within the system would be able to communicate at the same time using the same channel. In addition, a perfect adaptive antenna system would be able to track individual multipath components for each user and combine them in an optimal manner to collect all of the available signal energy from each user. The perfect adaptive antenna system is not feasible since it requires infinitely large antennas.

OFDM (Orthogonal Frequency Division Multiplexing)

In modulations, information is mapped on to changes in frequency, phase or amplitude (or a combination of them) of a carrier signal. Multiplexing deals with allocation/accommodation of users in a given bandwidth (i.e. it deals with allocation of available resource). OFDM is a combination of modulation and multiplexing. In this technique, the given resource (bandwidth) is shared among individual modulated data sources. Normal modulation techniques (like AM, PM, FM, BPSK, QPSK, etc..,) are single carrier modulation techniques, in which the incoming information is modulated over a single carrier. OFDM is a multicarrier modulation technique, which employs several carriers, within the allocated bandwidth, to convey the information from source to destination. Each carrier may employ one of the several available digital modulation techniques (BPSK, QPSK, QAM etc..,).

Packet Radio

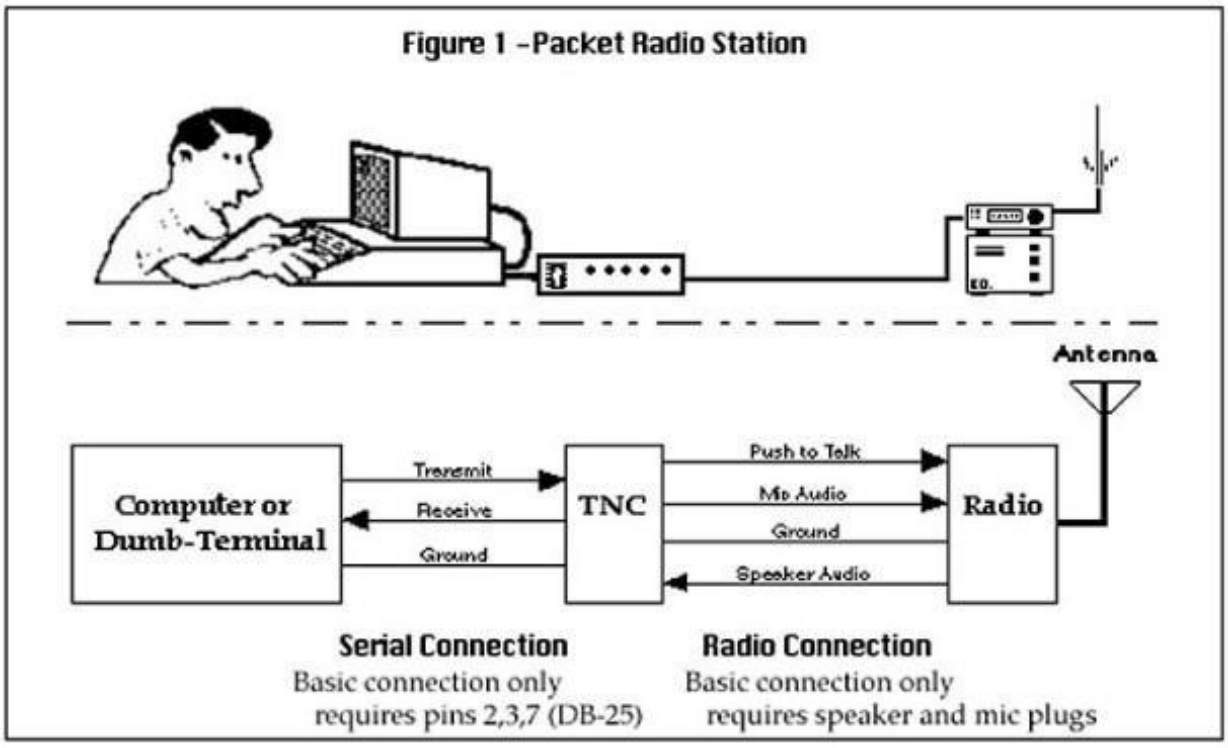
In digital radio, **packet radio** is the application of packet switching techniques to digital radio communications. Packet radio uses a packet switching protocol as opposed to circuit switching or message switching protocols to transmit digital data via a radio communication link. Packet radio is frequently used by amateur radio operators. The AX.25 (Amateur X.25) protocol was derived from the X.25 data link layer protocol and adapted for amateur radio use. Every AX.25 packet includes the sender's amateur radio callsign, which satisfies the US FCC requirements for amateur radio station identification. AX.25 allows other stations to automatically repeat packets to extend the range of transmissions. It is possible for any packet station to act as a digipeater, linking distant stations with each other through ad hoc networks. This makes packet radio especially useful for emergency communications.

Packet radio can be used in mobile communications. Some mobile packet radio stations transmit their location periodically using the Automatic Packet Reporting System (APRS). If the APRS packet is received by an "igate" station, position reports and other messages can be routed to an internet server, and made accessible on a public web page. This allows amateur radio operators to track the locations of vehicles, hikers, high-altitude balloons, etc., along with telemetry and other messages around the world.

Some packet radio implementations also use dedicated point-to-point links such as TARPN. In cases such as this, new protocols have emerged such as Improved Layer 2 Protocol (IL2P) supporting forward error correction for noisy and weak signal links.

Packet radio provides error free communications because of built-in error detection schemes. If a packet is received, it is checked for errors and will be displayed only if it is correct. In addition, any packet TNC can be used as a packet relay station, sometimes called a digipeater. This allows for greater range by stringing several packet stations together.

Below Figure shows an illustration of a typical station setup with a schematic diagram of a station wiring.



Packet radio protocols

- Aloha and PRNET.
- Amateur Packet Radio and the AMPRNet.

Aloha and PRNET:

Since radio circuits inherently possess a broadcast network topology (i.e., many or all nodes are connected to the network simultaneously), one of the first technical challenges faced in the implementation of packet radio networks was a means to control access to a shared communication channel to avoid collisions of signals. Professor Norman Abramson of the University of Hawaii led development of a packet radio network known as ALOHAnet and performed a number of experiments beginning in the 1970s to develop methods to arbitrate access to a shared radio channel by network nodes. This system operated on UHF frequencies at 9,600 baud. From this work the Aloha multiple access protocol was derived. Subsequent enhancements in channel access techniques made by Leonard Kleinrock *et al.* in 1975 would lead Robert Metcalfe to use carrier-sense multiple access (CSMA) protocols in the design of the now commonplace Ethernet local area network (LAN) technology.

Over 1973–76, DARPA created a packet radio network called PRNET in the San Francisco Bay area and conducted a series of experiments with SRI to verify the use of ARPANET (a precursor to the Internet) communications protocols (later known as IP) over packet radio links between mobile and fixed network nodes.[1] This system was quite advanced, as it made use of direct sequence spread spectrum (DSSS) modulation and forward error correction (FEC) techniques to provide 100 kbit/s and 400 kbit/s data channels. These

experiments were generally considered to be successful, and also marked the first demonstration of Internetworking, as in these experiments data was routed between the ARPANET, PRNET, and SATNET (a satellite packet radio network) networks. Throughout the 1970s and 1980s, DARPA operated a number of terrestrial and satellite packet radio networks connected to the ARPANET at various military and government installations.

Amateur Packet Radio and the AMPRNet :

Amateur radio operators began experimenting with packet radio in 1978, when—after obtaining authorization from the Canadian government—Robert Rouleau, VE2PY; Bram Frank, VE2BFH; Norm Pearl, VE2BQS; and Jacques Orsali, VE2EHP[2] of the Montreal Amateur Radio Club Montreal, Quebec, began experimenting with transmitting ASCII encoded data over VHF amateur radio frequencies using homebuilt equipment. In 1980, Doug Lockhart VE7APU, and the Vancouver Area Digital Communications Group (VADCG) in Vancouver, British Columbia began producing standardized equipment (Terminal Node Controllers) in quantity for use in amateur packet radio networks. In 2003, Rouleau was inducted into CQ Amateur Radio magazine's hall of fame for his work on the Montreal Protocol in 1978

Not long after this activity began in Canada, amateurs in the US became interested in packet radio. In 1980, the United States Federal Communications Commission (FCC) granted authorization for United States amateurs to transmit ASCII codes via amateur radio. Repeaters may be designed for amateur packet radio, these are dubbed "digipeaters". The first known amateur packet radio activity in the US occurred in San Francisco during December 1980, when a packet repeater was put into operation on 2 meters by Hank Magnuski KA6M, and the Pacific Packet Radio Society (PPRS). In keeping with the dominance of DARPA and ARPANET at the time, the nascent amateur packet radio network was dubbed the AMPRNet in DARPA style. Magnuski obtained IP address allocations in the *44.0.0.0/8* network for amateur radio use worldwide.

Many groups of amateur radio operators interested in packet radio soon formed throughout the country including the Pacific Packet Radio Society (PPRS) in California, the Tucson Amateur Packet Radio Corporation (TAPR) in Arizona and the Amateur Radio Research and Development Corporation (AMRAD) in Washington, D.C.

By 1983, TAPR was offering the first TNC available in kit form. Packet radio started becoming more and more popular across North America and by 1984 the first packet-based bulletin board systems began to appear. Packet radio proved its value for emergency operations following the crash of an Aeromexico airliner in a neighborhood in Cerritos, California, in August, 1986. Volunteers linked several key sites to pass text traffic via packet radio which kept voice frequencies clear.

Carrier Sense Multiple Access (CSMA) Protocol

In Carrier Sense Multiple Access (CSMA) protocol, the station will sense the channel before the transmission of data. CSMA reduces the chances of collision in the network but it does not eliminate the collision from the channel. 1-Persistent, Non-Persistent, P-Persistent, and O-

Persistent are the three access methods of CSMA.

What is Carrier Sense Multiple Access (CSMA)?

CSMA stands for Carrier Sense Multiple Access (CSMA). CSMA is one of the network protocols which works on the principle of 'carrier sense'. CSMA is a protocol developed to increase the performance of the network and reduce the chance of collision in the network.

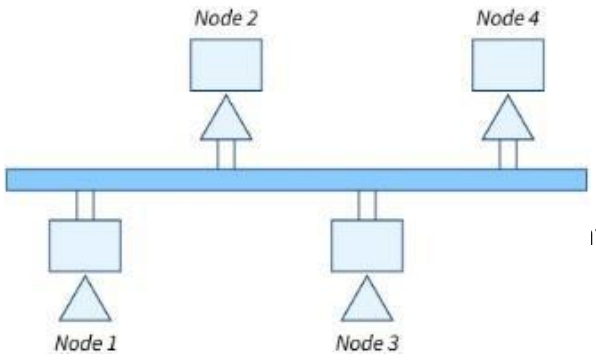
- If any device wants to send data then the device first sense or listens to the network medium to check whether the shared network is free or not. If the channel is found idle then the device will transmit its data.
- This sense reduces the chance of collision in the network but this method is not able to eliminate the collision.
- Carrier Sense Multiple Access (CSMA) is a protocol that senses or listens to the medium before any transmission of data in the medium.
- CSMA is used in Ethernet networks where two or more network devices are connected.

Working Principle of CSMA

- CSMA works on the principle of "Listen before Talking" or "Sense before Transmit". When the device on the shared medium wants to transmit a data frame, then the device first detects the channel to check the presence of any carrier signal from other connected devices on the network.
- In this situation, if the device senses any carrier signal on the shared medium, then this means that there is another transmission on the channel. And the device will wait until the channel becomes idle and the transmission that is in progress currently completes.
- When the channel becomes idle the station starts its transmission. All other stations connected in the network receive the transmission of the station.
- In CSMA, the station sense or detects the channel before the transmission of data so it reduces the chance of collision in the transmission.
- But there may be a situation where two stations detected the channel idle at the same time and they both start data transmission simultaneously so in this there is a chance of collision.
- So CSMA reduces the chance of collision in data transmission but it does not eliminate the collision.

Example: In the network given below in the diagram if node 1 wants to transmit the data in the network then, first of all, it will sense the network if data of any other device is available on the network then it will not send the data. When node 1 finds the channel idle then it will transmit data on the channel.

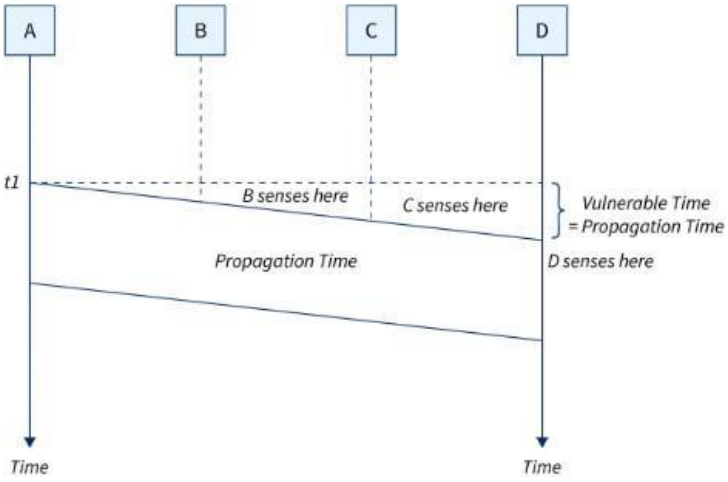
Refer to the below image for an example of CSMA



Vulnerable Time in CSMA

In the CSMA vulnerable time is considered as the propagation time and **Tp** is used to denote it. Generally, it is the time taken by the data frame to reach from one end of the channel to another end. When two stations send the data simultaneously then it will result in a collision in the network. In a situation, if the first bit of the frame sent by the station reaches the end of the shared medium then every station connected in a network hears that bit and every device in the network refrains from sending it.

Refer to the below image for the vulnerable time of CSMA



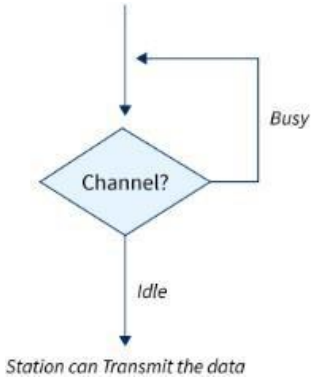
Types of CSMA Access Modes

1-Persistent

This method is considered the straightforward and simplest method of CSMA. In this method, if the station found the medium idle then the station will immediately send the data frame with 1-probability.

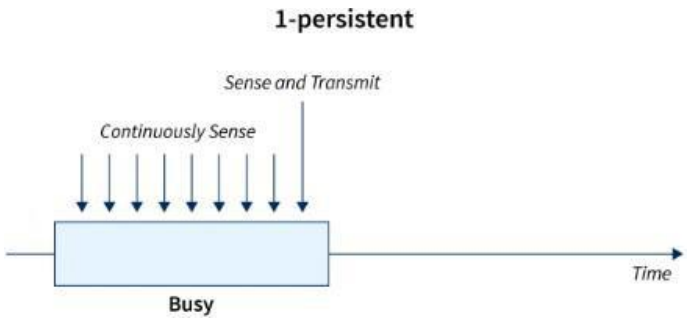
- In this, if the station wants to transmit the data. Then the station first senses the medium.
- If the medium is busy then the station waits until the channel becomes idle. And the station continuously senses the channel until the medium becomes idle.
- If the station detected the channel as idle then the station will immediately send the data frame with 1 probability that's why the name of this method is 1-persistent.

Refer to the below image to show the flow diagram of the 1-persistent method of CSMA


Busy
Channel?
Idle
Station can Transmit the data

In this method there is a high possibility of collision as two or more station sense the channel idle at the same time and transmits data simultaneously which may lead to a collision This is one of the most straightforward methods. In this method, once the station finds that the medium is idle then it immediately sends the frame. By using this method there are higher chances for collision because it is possible that two or more stations find the shared medium idle at the same time and then they send their frames immediately.

Refer to the below image to show the behavior of the 1-persistent method of CSMA

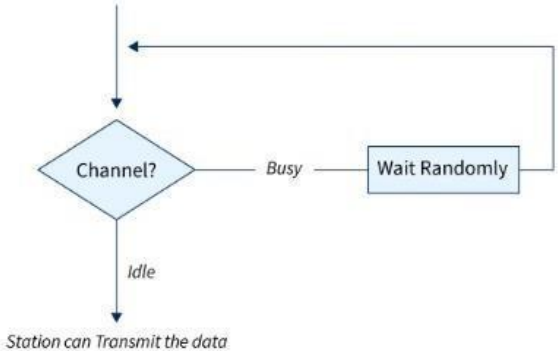


Non-Persistent

In this method of CSMA, if the station founds the channel busy then it will wait for a random amount of time before sensing the channel again.

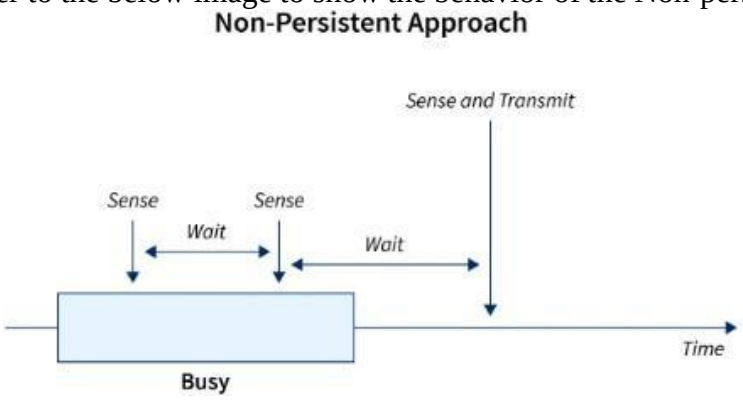
- If the station wants to transmit the data then first of all it will sense the medium.
- If the medium is idle then the station will immediately send the data.
- Otherwise, if the medium is busy then the station waits for a random amount of time and then again senses the channel after waiting for a random amount of time.
- In P-persistent there is less chance of collision in comparison to the 1-persistent method as this station will not continuously sense the channel but since the channel after waiting for a random amount of time.

Refer to the below image to show the flow diagram of the Non-persistent method of CSMA



So the random amount of time is unlikely to be the same for two stations that's why this method reduces the chance of collision.

Refer to the below image to show the behavior of the Non-persistent method of CSMA

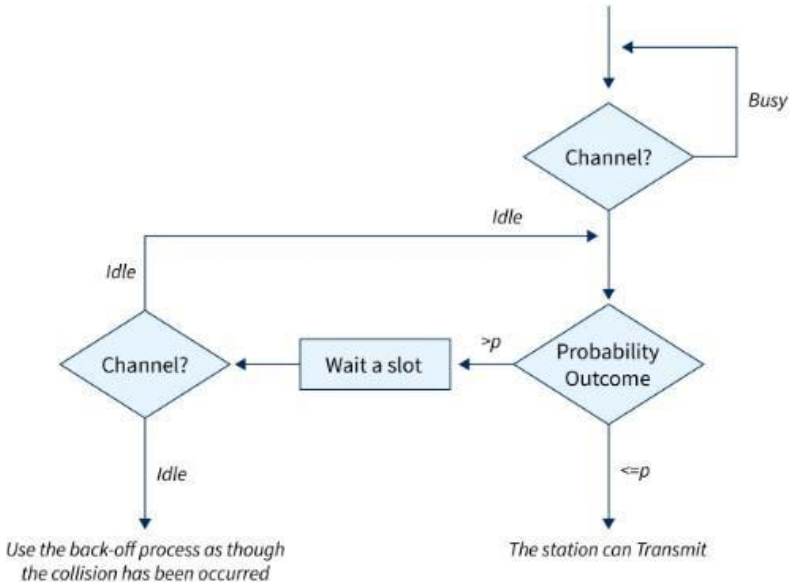


P-Persistent

The p-persistent method of CSMA is used when the channel is divided into multiple time slots and the duration of time slots is greater than or equal to the maximum propagation time. This method is designed as a combination of the advantages of 1-Persistent and Non-Persistent CSMA. The p-persistent method of CSMA reduces the chance of collision in the network and there is an increment in the efficiency of the network. When any station wants to transmit the data firstly it will sense the channel If the channel is busy then the station continuously senses the channel until the channel becomes idle. If the channel is idle then the station does the following steps.

1. The station transmits its data frame in the network by p probability.
2. And the station waits for the start of the next time slot with probability q=1-p and after waiting again senses the channel.
3. If the channel is again idle, then it again performs step1. If the channel is busy, then it thinks that there is a collision in the network and now this station will follow the back-off procedure.

Refer to the below image to show the flow diagram of the P-persistent method of CSMA



O-Persistent

In this method of CSMA supervisory node assign a transmission order to each node in the network. When the channel was idle instead of immediately sending the data channel will wait for its transmission order assigned to them. This mode of CSMA defines the superiority of the station before data transmission in the medium. In this mode, if the channel is inactive then all stations will wait to transmit the data for its turn. Every station in the channel transmits the data in its turn.

Variations of CSMA Protocol

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carrier sense multiple access/ collision detection is one of the network protocols for transmission. CSMA/CD protocol works with the medium access control layer of the network. That's why the station senses the channel before transmission of data and if the station founds the channel idle then the station transmits its data frames to check whether data transmission is successful in the network or not. If the station successfully the data frame sent then it will again send the next frame. If the station detects a collision in the network, then in CSMA/CD the station will send the stop/jam signal to all the stations connected in the network to terminate their transmission of data. Then the station waits for a random amount of time for the transmission of data.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier sense multiple access/collision avoidance is one of the network protocols for data frame transmission. When the station sends the data frame on the channel then it receives the acknowledgment in response to the sent data frame to test whether the channel is idle or not. When the station receives a single signal i.e. its signal this means that there is no collision and data has been successfully received by the receiver. But in case of collision, the station receives two signals: its signal and the second signal sent by the other station. In CSMA/CA collision is avoided by using the following three strategies. Following are the methods used in the CSMA/ CA to avoid the collision:

- Interframe space
- Contention window
- Acknowledgement

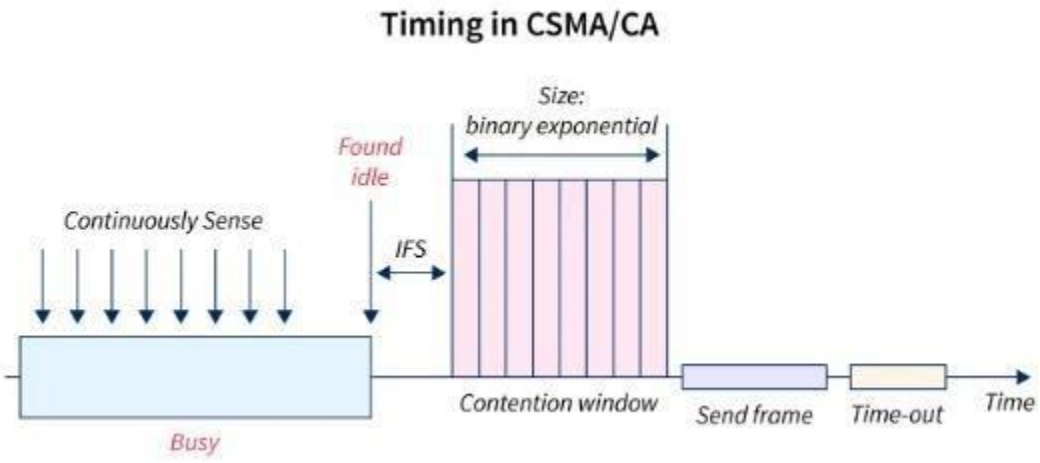
Interframe Space or IFS: If the station wants to transmit the data then it waits until the channel becomes idle and when the channel becomes idle station does not immediately send the data but waits for some time. This period is known as the Interframe Space or IFS. IFS can also define the priority of the frame or station.

Contention window: The contention window is a time that is divided into time slots. When the station is ready for data transmission after waiting for IFS then it chooses the random amount of slots for waiting. After waiting for the random number of slots if the channel is still busy then the station does not initiate the whole process again, the station stops its timer and restarts again when the channel is sensed idle.

Acknowledgement:

There may be a chance of collision or data may be corrupted during the transmission. Positive acknowledgment and time-out are used in addition to ensuring that the receiver has successfully received the data.

Refer to the below image to show the behavior of the CSMA/CA



Conclusion

- Carrier Sense Multiple Access(CSMA) is one of the network protocols in which stations sense the channel before the transmission of data.
- The vulnerable time of the CSMA is referred to as the propagation time denoted by Tp.
- 1-Persistent, Non-Persistent, P-Persistent, and O-Persistent are the three access methods of CSMA.
- In the 1-Persistent method of the CSMA, if the station found the medium idle then the station will immediately send the data frame with 1- probability.
- In the Non-Persistent method of CSMA, if the station founds the channel busy then it will wait for a random amount of time and if the channel is idle it will immediately send the data frame.
- In the P-Persistent method of CSMA, if the station founds the channel idle then it will send the data frame with p probability and for the starting of the next time slot with q=1-p probability.
- CSMA/CA and CSMA/CD are two variations of CSMA.

Reservation protocols

Reservation protocols are the class of protocols in which the stations wishing to transmit data broadcast themselves before actual transmission. These protocols operate in the medium access control (MAC) layer and transport layer of the OSI model.

In these protocols, there is a contention period prior to transmission. In the contention period, each station broadcasts its desire for transmission. Once each station announces itself, one of them gets the desired network resources based upon any agreed criteria. Since each station has complete knowledge whether every other station wants to transmit or not before actual transmission, all possibilities of collisions are eliminated.

Examples of Reservation Protocols

The two prominent reservation protocols are −

- **Bit** – **map Protocol** that operates in the MAC layer
- **Resource Reservation Protocol (RSVP)** that operates in the transport layer

Bit – Map Protocol

In this protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot.

Suppose that there are 10 stations. So the number of contention slots will be 10. If the stations 2, 3, 8 and 9 wish to transmit, they will set the corresponding slots to 1. Generally, the transmission is done in the order of the slot numbers. The process is shown in the following diagram:

Resource Reservation Protocol (RSVP)

RSVP is a transport layer protocol that is used to reserve resources in a computer network to get a different quality of services (QoS) while accessing Internet applications. It operates over Internet protocol (IP) and initiates resource reservations from the receiver's end. It is used both for unicasting (sending data from one source to one destination) and multicasting (sending data simultaneously to a group of destination computers).

Chapter-2

INTRODUCTION TO WIRELESS NETWORKING

DIFFERENCE BETWEEN FIXED AND WIRELESS TELEPHONE NETWORK

Fixed Telephone Network	Wireless Telephone Network
The transmitter and receiver is fixed at one place. Information is carried over cables(fiberoptic/copper) and fixed links(microwave/satellite)	Transmitter and receiver communicate via EM radio waves. They are not always fixed at one place but can movealso.
Network configurations are virtually static and need programming at Local exchange when subscriber changes its location fromone area to the other area.	Network configurations are dynamic and will obtain subscriber information when it moves from one location area or routing area to the other areas.
Takes time for changing the fixed telephone services.	It does not take time and can be done in small interval of time.
A telephone Central office takes care of millions of landline telephone connections.	MSCs take care of cellular telephone connections based on air traffic capacity.
Less overhead data needed.	More overhead data needed as geographical location keeps changing.
No harse channel conditions usually observed with this type of network.	Very harse and random channel conditions can also be observed with this type of network. The system is designed to take care of this channelconditions.

DEVELOPMENT OF WIRELESS NETWORKS

FIST GENERATION (1G):

1G (or 1-G) refers to the first generation wireless telephone technology . These are the analog telecommunications standards that were introduced in the 1980s and continued until being replaced by 2G digital telecommunications. The main difference between the two mobile telephone systems (1G and 2G), is that theradio signals used by 1G networks are analog, while 2G networks are digital.

Although both systems use digital signaling to connect the radio towers (which listen to the handsets) to the rest of the telephone system, the voice itself during a call is encoded to digital signals in 2G whereas 1G is only modulated to higher frequency, typically 150 MHz and up. The inherent advantages of digital technology over that of analog meant that 2G networks eventually replaced them almost everywhere.

One such standard is NMT (Nordic Mobile Telephone), used in Nordic countries, Switzerland, the Netherlands, Eastern Europe and Russia. Others include AMPS (Advanced Mobile Phone System) used in North America & Australia, TACS (Total Access Communications System) in the United Kingdom, C-450 in West Germany, Portugal and South Africa, Radiocom 2000in France, TMA in Spain, and RTMI in Italy. In Japan there were multiple systems. Three standards, TZ-801, TZ-802, and TZ-803 were developed by NTT (Nippon Telegraph and Telephone Corporation), while a competing system operated by DDI (Daini Denden Planning, Inc.) used the JTACS (Japan Total Access Communications System) standard.

SECOND GENERATION (2G):

2G (or 2-G) is short for second-generation wireless telephone technology. Second generation 2G cellular telecom networks were commercially launched onthe GSM standard in Finland by Radiolinja (now part of Elisa Oyj) in 1991. Three primary benefits of 2G networks over their predecessors were that phone conversations were digitally encrypted. 2G systems were significantly more efficient on the spectrum allowing for far greater mobile phone penetration levels and 2G introduced data services for mobile, starting with SMS text messages. 2G technologies enabled the various mobile phone networks to provide the services

such as text messages, picture messages and MMS (multimedia messages). All textmessages sent over 2G are digitally encrypted, allowing for the transfer of data in such a way that only the intended receiver can receive and read it.

After 2G was launched, the previous mobile telephone systems were retroactively dubbed 1G. While radio signals on 1G networks are analog, radio signals on 2G networks are digital. Both systems use digital signaling to connect theradio towers (which listen to the handsets) to the rest of the telephone system. 2G has been superseded by newer technologies such as 2.5G, 2.75G, 3G, and 4G. Howeve 2G networks are still used in many parts of the world.

2.2.2a. 2G technologies

2G technologies can be divided into Time Division Multiple Access (TDMA)-based and Code Division Multiple Access (CDMA)-based standards depending on the type of multiplexing used. The main 2G standards are:

- GSM (TDMA-based), originally from Europe but used in most of the world outside North America. Today accounts for over 80% of all subscribersaround the world. Over 60 GSM operators are also using CDMA2000 in the 450 MHz frequency band (CDMA450).
- IS-95 aka cdmaOne (CDMA-based, commonly referred as simply CDMA in the US), used in the Americas and parts of Asia. Today accounts for about 17%of all subscribers globally. Over a dozen CDMA operators have migrated to GSM including operators in Mexico, India and Australia.
- PDC also known as JDC (Japanese Digital Cellular) (TDMA-based), usedexclusively in Japan
- iDEN (TDMA-based), proprietary network used by Nextel in the United Statesand Telus Mobility in Canada IS-136 a.k.a. D-AMPS (TDMA-based, commonly referred as simply 'TDMA' in the US), was once prevalent in the Americas butmost have migrated to GSM.

2G services are frequently referred as Personal Communications Service, or PCS, in the United States.

b. Capacities, advantages, and disadvantagesCapacity

Using digital signals between the handsets and the towers increases system capacity in two key ways: Digital voice data can be compressed and multiplexed much more effectively than analog voice encodings through the use of various codecs, allowing more calls to be transmitted in same amount of radio bandwidth.

The digital systems were designed to emit less radio power from the handsets. This meant that cells had to be smaller, so more cells had to be placed in the same amount of space. This was possible because cell towers and related equipment had become less expensive.

2G Data Transmission Capacity:

- With GPRS (General Packet Radio Service), you have a theoretical transfer speed of max. 50 kbit/s (40 kbit/s in practice).
- With EDGE (Enhanced Data Rates for GSM Evolution), you have a theoreticaltransfer speed of max. 1 Mbit/s (500 kbit/s in practice).

Disadvantages

In less populous areas, the weaker digital signal transmitted by a cellular phone may not be sufficient to reach a cell tower. This tends to be a particular problem on 2G systems deployed on higher frequencies, but is mostly not a problem on 2G systems deployed on lower frequencies. National regulations differ greatly among countries which dictate where 2G can be deployed.

Analog has a smooth decay curve, but digital has a jagged steppy one. This can be both an advantage and a disadvantage. Under good conditions, digital will sound better. Under slightly worse conditions, analog will experience static, while digital has occasional dropouts. As conditions worsen, though, digital will start to completely fail, by dropping calls or being unintelligible, while analog slowly gets worse, generally holding a call longer and allowing at least some of the audio transmitted to be understood.

Advantage

While digital calls tend to be free of static and background noise, the lossy compression they use reduces their quality, meaning that the range of sound that they convey is reduced. Talking on a digital cell phone, a caller hears less of the tonality of someone's voice.[citation needed]

2.2.2. c. Evolution

2G networks were built mainly for voice services and slow data transmission(defined in IMT-2000 specification documents), but are considered by the general public[who?] to be 2.5G or 2.75G services because they are several times slower than present-day 3G service.

2.5G (GPRS)

2.5G ("second and a half generation") is used to describe 2G-systems that have implemented a packet-switched domain in addition to the circuit-switched domain. It does not necessarily provide faster services because bundling of timeslots is used for circuit-switched data services (HSCSD) as well. The first major step in the evolution of GSM networks to 3G occurred with the introduction of General Packet Radio Service (GPRS). CDMA2000 networks similarly evolved through the introduction of 2.5G

2.75G (EDGE)

GPRS networks evolved to EDGE networks with the introduction of 8PSK encoding. Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC) is a backward-compatible digital mobile phone technology that allows improved data transmission rates, as an extension on top of standard GSM. EDGE was deployed on GSM networks beginning in 2003—initially by AT&T in the United States.

EDGE is standardized by 3GPP as part of the GSM family and it is an upgrade that provides a potential three-fold increase in capacity of GSM/GPRS networks.The 2G digital service provided very useful features, such as caller ID, call forwarding and short messaging.

THIRD GENERATION (3G):

3G short form of third generation is the third generation of mobile telecommunications technology. This is based on a set of standards used for mobile devices and mobile telecommunications use services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.3G finds application in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV.

3G telecommunication networks support services that provide an informationtransfer rate of at least 200 kbit/s. Later 3G releases, often denoted 3.5G and 3.75G, also provide mobile broadband access of several Mbit/s to smartphones and mobile modems in laptop computers. This ensures it can be applied to wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV technologies.

A new generation of cellular standards has appeared approximately every tenth year since 1G systems were introduced in 1981/1982. Each generation is characterized by new frequency bands, higher data rates and non–backward- compatible transmission technology. The first 3G networks were introduced in 1998and fourth generation "4G" networks in 2008.

The following standards are typically branded 3G:

- the UMTS system, first offered in 2001, standardized by 3GPP, used primarilyin Europe, Japan, China (however with a different radio interface) and other regions predominated by GSM 2G system infrastructure. The cell phones are typically UMTS and GSM hybrids. Several radio interfaces are offered, sharingthe same infrastructure:
- The original and most widespread radio interface is called W-CDMA.
- The TD-SCDMA radio interface was commercialized in 2009 and is only offered in China.
- The latest UMTS release, HSPA+, can provide peak data rates up to 56 Mbit/s in the downlink in theory (28 Mbit/s in existing services) and 22 Mbit/s in theuplink.

- the CDMA2000 system, first offered in 2002, standardized by 3GPP2, used especially in North America and South Korea, sharing infrastructure withthe IS-95 2G standard. The cell phones are typically CDMA2000 and IS-95 hybrids. The latest release EVDO Rev B offers peak rates of 14.7 Mbit/s downstream.

The above systems and radio interfaces are based on spread spectrum radio transmission technology. While the GSM EDGE standard ("2.9G"), DECT cordless phones and Mobile standards formally also fulfill the IMT-2000 requirements and are approved as 3G standards by ITU, these are typically not branded 3G, and are based on completely different technologies.

The following common standards comply with the IMT2000/3G standard:

- EDGE, a revision by the 3GPP organization to the older 2G GSM based transmission methods, utilizing the same switching nodes, base station sites andfrequencies as GPRS, but new base station and cellphone RF circuits. It is based on the three times as efficient 8PSK modulation scheme as supplement to the original GMSK modulation scheme. EDGE is still used extensively due to its ease of upgrade from existing 2G GSM infrastructure and cell-phones.
  - EDGE combined with the GPRS 2.5G technology is called EGPRS, and allows peak data rates in the order of 200 kbit/s, just as theoriginal UMTS WCDMA versions, and thus formally fulfills the IMT2000 requirements on 3G systems. However, in practice EDGE is seldom marketedas a 3G system, but a 2.9G system. EDGE shows slightly better system spectral efficiency than the original UMTS and CDMA2000 systems, but it is difficult to reach much higher peak data rates due to the limited GSM spectral bandwidth of 200 kHz, and it is thus a dead end.
  - EDGE was also a mode in the IS-135 TDMA system, today ceased.
  - Evolved EDGE, the latest revision, has peaks of 1 Mbit/s downstream and 400 kbit/s upstream, but is not commercially used.
- The Universal Mobile Telecommunications System, created and revised by the 3GPP. The family is a full revision from GSM in terms of encoding methods and hardware, although some GSM sites can be retrofitted to broadcast in the UMTS/W-CDMA format.

- W-CDMA is the most common deployment, commonly operated on the 2,100 MHz band. A few others use the 850, 900 and 1,900 MHz bands.
    - HSPA is an amalgamation of several upgrades to the original W-CDMA standard and offers speeds of 14.4 Mbit/s down and 5.76 Mbit/s up. HSPA is backward-compatible with and uses the same frequencies as W-CDMA.
    - HSPA+, a further revision and upgrade of HSPA, can provide theoretical peak data rates up to 168 Mbit/s in the downlink and 22 Mbit/s in the uplink, using a combination of air interface improvements as well as multi-carrier HSPA and MIMO. Technically though, MIMO and DC-HSPA can be used without the "+" enhancements of HSPA+
- The CDMA2000 system, or IS-2000, including CDMA2000 1x and CDMA2000 High Rate Packet Data (or EVDO), standardized by 3GPP2 (*differing* from the 3GPP), evolving from the original IS-95 CDMA system, is used especially in North America, China, India, Pakistan, Japan, South Korea, Southeast Asia, Europe and Africa.[3]
    - CDMA2000 1x Rev. E has an increased voice capacity (in excess of three times) compared to Rev. 0 EVDO Rev. B offers downstream peak rates of 14.7 Mbit/s while Rev. C enhanced existing and new terminal user experience.

While DECT cordless phones and Mobile WiMAX standards formally also fulfill the IMT-2000 requirements, they are not usually considered due to their rarity and unsuitability for usage with mobile phones.

TRAFFIC ROUTING IN WIRELESS NETWORKS

CIRCUIT SWITCHING:

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

Circuit switching contrasts with packet switching which divides the data to betransmitted into packets transmitted through the network independently. In packet switching, instead of being dedicated to one communication session at a time, network links are shared by packets from multiple competing communication sessions, resulting in the loss of the quality of service guarantees that are provided by circuit switching.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Virtual circuit switching is a packet switching technology that emulates circuitswitching, in the sense that the connection is established before any packets are transferred, and packets are delivered in order.

a. Examples of circuit-switched networks

- Public switched telephone network (PSTN) •

ISDN B-channel

- Circuit Switched Data (CSD) and High-Speed Circuit-Switched Data (HSCSD)service in cellular systems such as GSM
- Datakit
- X.21 (Used in the German DATEX-L and Scandinavian DATEX circuit switcheddata network)
- Optical mesh network

PACKET SWITCHING

- Packet switching is a digital networking communications method that groups alltransmitted

data into suitably sized blocks, called *packets*, which are transmitted

via a medium that may be shared by multiple simultaneous communication sessions. Packet switching increases network efficiency, robustness and enables technological convergence of many applications operating on the same network.

- Packets are composed of a header and payload. Information in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software.
- Starting in the late 1950s, American computer scientist Paul Baran developed the concept *Distributed Adaptive Message Block Switching* with the goal to provide a fault-tolerant, efficient routing method for telecommunication messages as part of a research program at the RAND Corporation, funded bythe US Department of Defense.[1] This concept contrasted and contradicted the theretofore established principles of pre-allocation of network bandwidth, largelyfortified by the development of telecommunications in the Bell System.
- The new concept found little resonance among network implementers until the independent work of Donald Davies at the National Physical Laboratory (United Kingdom)(NPL) in the late 1960s. Davies is credited with coining the modern name *packet switching* and inspiring numerous packet switching networks in Europe in the decade following, including the incorporation of the concept in the early ARPANET in the United States.

2.3.2a. Packet switching in networks

Packet switching is used to optimize the use of the channel capacity available in digital telecommunication networks such as computer networks, to minimize the transmission latency (the time it takes for data to pass across the network), and to increase robustness of communication. The best-known use of packet switching is the Internet and most local area networks. The Internet is implemented by the Internet Protocol Suite using a variety of Layer technologies. For example, Ethernet and Frame Relay are common. Newer mobile phone technologies(e.g., GPRS, I-mode) also use packet switching.

X.25 is a notable use of packet switching in that, despite being based on packet switching methods, it provided virtual circuits to the user. These virtual

circuits carry variable-length packets. In 1978, X.25 provided the first international and commercial packet switching network, the International Packet Switched Service (IPSS). Asynchronous Transfer Mode (ATM) also is a virtual circuittechnology, which uses fixed-length cell relay connection oriented packet switching.

Datagram packet switching is also called connectionless networking because no connections are established. Technologies such as Multiprotocol Label Switching (MPLS) and the resource reservation protocol (RSVP) create virtual circuits on top of datagram networks. Virtual circuits are especially useful in building robust failover mechanisms and allocating bandwidth for delay-sensitive applications.

MPLS and its predecessors, as well as ATM, have been called "fast packet" technologies. MPLS, indeed, has been called "ATM without cells".[12] Modern routers,however, do not require these technologies to be able to forward variable-length packets at multi gigabit speeds across the network.

Circuit Switching	**Packet Switching(Datagram type)**	**Packet Switching(Virtual Circuit type)**
Dedicated path	No Dedicated path	No Dedicated path
Path is established for entire conversation	Route is established for each packet	Route is established for entire conversation
Call setup delay	packet transmission delay	call setup delay as well as packet transmission delay
Overload may block call setup	Overload increases packet delay	Overload may block call setup and increases packet delay
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet

WIRELESS DATA SERVICES

CELLULAR DIGITAL PACKET DATA (CDPD)

Cellular Digital Packet Data (CDPD) was a wide-area mobile data service which used unused bandwidth normally used by AMPS mobile phones between 800 and 900 MHz to transfer data. Speeds up to 19.2 kbit/s were possible. The service was discontinued in conjunction with the retirement of the parent AMPS service; it has been functionally replaced by faster services such as 1xRTT, EV-DO, and UMTS/HSPA.

Developed in the early 1990s, CDPD was large on the horizon as a future technology. However, it had difficulty competing against existing slower but less expensive Mobitex and DataTac systems, and never quite gained widespread acceptance before newer, faster standards such as GPRS became dominant. CDPD had very limited consumer products. AT&T Wireless first sold the technology in the United States under the PocketNet brand.

It was one of the first products of wireless web service. Digital Ocean, Inc. an OEM licensee of the Apple Newton, sold the Seahorse product, which integrated the Newton handheld computer, an AMPS/CDPD handset/modem along with a web browser in 1996, winning the CTIA's hardware product of the year award as a smart phone, arguably the world's first. A company named OmniSky provided service for Palm V devices. Cingular Wireless later sold CDPD under the Wireless Internet brand (not to be confused with Wireless Internet Express, their brand for GPRS/EDGE data). PocketNet was generally considered a failure with competition from 2G services such as Sprint's Wireless Web. AT&T Wireless sold four PocketNet Phone models to the public: the Samsung Duette and the Mitsubishi MobileAccess-120 were AMPS/CDPD PocketNet phones introduced in October 1997; and two IS- 136/CDPD Digital PocketNet phones, the Mitsubishi T-250 and the Ericsson R289LX.

Despite its limited success as a consumer offering, CDPD was adopted in a number of enterprise and government networks. It was particularly popular as a first-generation wireless data solution for telemetry devices (machine to machine communications) and for public safety mobile data terminals. In 2004, major

carriers in the United States announced plans to shut down CDPD service. In July 2005, the AT&T Wireless and Cingular Wireless CDPD networks were shut down. Equipment for this service now has little to no residual value.

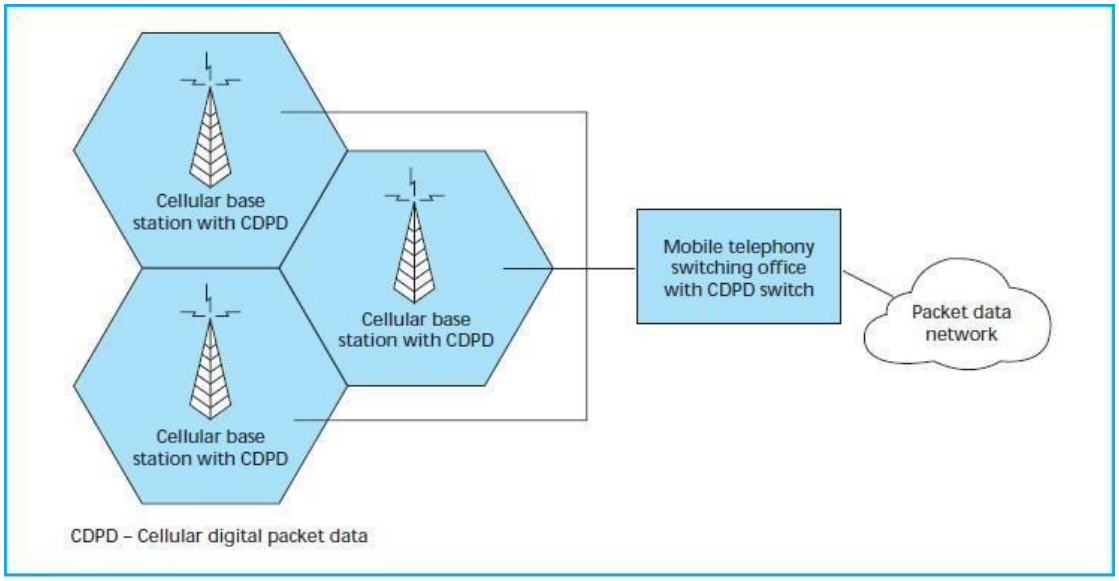


Figure 1.
CDPD as an AMPS network overlay.

Fig.3.1 CDPD

Protocols Used In CDPD:

- MDLP (Mobile Data Link Protocol)
- RRMP (Radio Resource Management Protocol)

MDLP (Mobile Data Link Protocol)

It is used to convey information between Data link layer entities.

Provides Sequence Control to maintain Frame Sequence Order across data linkconnection.

RRMP (Radio Resource Management Protocol)

Used to manage Radio channel Resources. It enables "Mobile End System" to findfree channels in CDPD network.

ADVANCED RADIO DATA INFORMATION SYSTEM (ARDIS):

It is a private network service developed by Motorola & IBM.

2 Protocols are used in ARDIS.

1. MDC 4800(Mobile Data Communication)
2. RD-LAP (Radio Data link-Link Access Protocols)

RAM MOBILE DATA (RMD):

Ram Mobile Data was originally founded by Ram Broadcasting Corporation asAmerican Mobile Data Communications, Inc. in 1988. The name of the companywas changed to Ram Mobile Data in 1989. RAM Mobile Data was the U.S. Operator of the Mobitex network.

Ram Mobile Data was sold and renamed BellSouth Wireless Data in 1995 and later became Cingular Interactive when BellSouth and SBC Communications formed Cingular Wireless. The Mobitex division within CingularWireless was sold to an investment company in 2005 and became Velocita Wireless. Velocita Wireless was purchased by Sprint Nextel and became a Sprint Nextel Company in early 2006. Today Ram Mobile Data is the exclusive operator of Mobitex in the Netherlands. With headquarters in Utrecht (NL) and a daughter in Bruxelles (BE) they are running the entire Mobitex operations throughout the BeNeLux. Furthermore Ram has a business unit Ram track-and-trace and since 2010 a daughter in IT services Ram Info technology.

Navara, a division of Ram Mobile Data, provides mobile device interface solutions for existing applications and databases. Navara is an independent software vendor that produces the Navara Mobility Suite, a software system that allows mobile access to business systems. Navara is utilized to provide mobile access to many different backend systems across many industries. Navara support most major mobile devices and industry-standard integration and communication technologies. Nowadays Navara is no longer a division of Ram and has privatized.

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special

services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface(BRI), Primary Rate Interface (PRI), Narrowband ISDN (N- ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbit/s in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN should not be mistaken for its use with a specific protocol, suchas Q.931 whereas ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In a broad sense ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is designed to provide access to voice and data services simultaneously.

However, common use reduced ISDN to be limited to Q.931 and related protocols, which are a set of protocols for establishing and breaking circuit switchedconnections, and for advanced calling features for the user. They were introduced in1986.In a videoconference, ISDN provides simultaneous voice, video, and texttransmission between individual desktop videoconferencing systems and group(room) videoconferencing systems.

Signaling channel

The signaling channel (D) uses Q.931 for signaling with the other side of the link.

X.25

X.25 can be carried over the B or D channels of a BRI line, and over the B channelsof a PRI line. X.25 over the D channel is used at many point-of-sale (credit card)

terminals because it eliminates the modem setup, and because it connects to the central system over a B channel, thereby eliminating the need for modems and making much better use of the central system's telephone lines. X.25 was also part of an ISDN protocol called "Always On/Dynamic ISDN", or AO/DI. This allowed a user to have a constant multi-link PPP connection to the internet over X.25 on the Dchannel, and brought up one or two B channels as needed.

BROADBAND INTEGRATED SERVICES DIGITAL NETWORK (B-ISDN)

In the 1980s the telecommunications industry expected that digital services would follow much the same pattern as voice services did on the public switched telephone network, and conceived an end-to-end circuit switched services, known as Broadband Integrated Services Digital Network (B-ISDN).

Before B-ISDN, the original ISDN attempted to substitute the analog telephone system with a digital system which was appropriate for both voice and non-voice traffic. Obtaining worldwide agreement on the basic rate interface standard was expected to lead to a large user demand for ISDN equipment, hence leading to mass production and inexpensive ISDN chips. However, the standardization process took years while computer network technology moved rapidly. Once the ISDN standard was finally agreedupon and products were available, it was already obsolete. For home use the largest demand for new services was video and voice transfer, but the ISDN basic rate lacks the necessary channel capacity.

This led to introduction of B-ISDN, by adding the word broadband. Although the term had a meaning in physics and engineering (similar to wideband), the CCITT defined it as: "Qualifying a service or system requiring transmission channels capable of supporting rates greater than the primary rate referring to the primary rate which ranged from about 1.5 to 2 Mbit/s. Services envisioned included video telephone and video conferencing. Technical papers were published in early 1988. Standards were issued by the Comité Consultatif International Téléphonique et Télégraphique (CCITT, now known as ITU-T), and called "Recommendations". They included G.707 to G.709, and I.121 which defined the principal aspects of B- ISDN, with many others following through the 1990s.

The designated technology for B-ISDN was Asynchronous Transfer Mode (ATM), which was intended to carry both synchronous voice and asynchronous data services on the same transport. The B-ISDN vision has beenovertaken by other disruptive technologies used in the Internet. The ATM technology survived as a low-level layer in most Digital subscriber line (DSL) technologies, and as a payload type in some wireless technologies such as WiMAX. The term "broadband" became a marketing term for any digital Internet access service.

SIGNALING SYSTEM NO. 7(SS7)

Signaling System No.7 (SS7) is a set of telephony signaling protocolsdeveloped in 1975, which is used to set up and tear down most of the world's public switched telephone network (PSTN) telephone calls. It also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other mass market services.

In North America it is often referred to as *CCSS7*, abbreviated for *Common Channel Signaling System 7*. In the United Kingdom, it is called *C7* (CCITT number 7), *number 7* and*CCIS7* (Common Channel Interoffice Signaling 7). In Germany it is often called N7 (*Signalisierungs system Nummer 7*).

The only international SS7 protocol is defined by ITU-T's Q.700-series recommendations in 1988. Of the many national variants of the SS7 protocols, most are based on variants of the international protocol as standardized by ANSI and ETSI. National variants with striking characteristics are the Chinese and Japanese (TTC) national variants. The Internet Engineering Task Force (IETF) has defined level 2, 3, and 4 protocols compatible with SS7 which use the Stream Control Transmission Protocol (SCTP) transport mechanism. This suite of protocolsis called SIGTRAN.

SS7 protocol suite

SS7 protocols by OSI layer	
Application	INAP, MAP, IS-41... TCAP, CAP, ISUP, ...
Network	MTP Level 3 + SCCP
Data link	MTP Level 2
Physical	MTP Level 1

The SS7 protocol stack may be partially mapped to the OSI Model of a packetized digital protocol stack. OSI layers 1 to 3 are provided by the Message Transfer Part (MTP) and the Signaling Connection Control Part (SCCP) of the SS7 protocol (together referred to as the Network Service Part (NSP)) for circuit related signaling, such as the BT IUP, Telephone User Part (TUP), or the ISUP, the User Part provides layer 7. Currently there are no protocol components that provide OSI layers 4 through 6. The Transaction (TCAP) is the primary SCCP User in the Core Network, using SCCP in connectionless mode. SCCP in connection oriented mode provides transport layer for air interface protocols such as BSSAP and RANAP. TCAP provides transaction capabilities to its Users (TC-Users), such as the Mobile Application Part, the Intelligent Network Application Part and the CAMEL ApplicationPart.

The Message Transfer Part (MTP) covers a portion of the functions of the OSI network layer including: network interface, information transfer, message handling and routing to the higher levels. Signaling Connection Control Part (SCCP) is at functional Level 4. Together with MTP Level 3 it is called the Network Service Part (NSP). SCCP completes the functions of the OSI network layer: end-to-end addressing and routing, connectionless messages (UDTs), and management services for users of the Network Service Part (NSP).[11] Telephone User Part (TUP) is a link-by-link signaling system used to connect calls. ISUP is the key user part, providing a circuit-based protocol to establish, maintain, and end the connections for calls. Transaction Capabilities Application Part (TCAP) is used to create database

queries and invoke advanced network functionality, or links to Intelligent Network Application Part (INAP) for intelligent networks, or Mobile Application Part (MAP) formobile services.

SS7 Protocol Overview

The number of possible protocol stack combinations is growing. It depends on whether SS7 is used for cellular-specific services or intelligent network services, whether transportation is over IP or is controlling broadband ATM networks instead of time-division multiplexing (TDM) networks, and so forth. This requires coining a new term traditional SS7 to refer to a stack consisting of the protocols widely deployed from the 1980s to the present:

- Message Transfer Parts (MTP 1, 2, and 3) •

Signaling Connection Control Part (SCCP)

- Transaction Capabilities Application Part (TCAP) •

Telephony User Part (TUP)

- ISDN User Part (ISUP)

The following sections provide a brief outline of protocols found in the introductorySS7 protocol stack

MTP

MTP levels 1 through 3 are collectively referred to as the MTP. The MTP comprises the functions to transport information from one SP to another. The MTP transfers the signaling message, in the correct sequence, without loss or duplication, between the SPs that make up the SS7 network. The MTP provides reliable transfer and delivery of signaling messages. The MTP was originally designed to transfer circuit-related signaling because no non circuit-related protocol was defined at the time.

The recommendations refer to MTP1, MTP2, and MTP3 as the physical layer, data link layer, and network layer, respectively. The following sections discuss MTP2 and MTP3. (MTP1 isn't discussed because it refers to the physical network.) For information on the physical aspects of the Public Switched Telephone Network (PSTN), see Chapter 5, "The Public Switched Telephone Network (PSTN)."

MTP2

Signaling links are provided by the combination of MTP1 and MTP2. MTP2 ensures reliable transfer of signaling messages. It encapsulates signaling messages into variable-length SS7 packets. SS7 packets are called signal units (SUs). MTP2 provides delineation of SUs, alignment of SUs, signaling link error monitoring, error correction by retransmission, and flow control. The MTP2 protocol is specific to narrowband links (56 or 64 kbps).

MTP3

MTP3 performs two functions:

- **Signaling Message Handling (SMH)** — Delivers incoming messages to their intended User Part and routes outgoing messages toward their destination. MTP3 uses the PC to identify the correct node for message delivery. Each message has both an Origination Point Code (OPC) and a DPC. The OPC is inserted into messages at the MTP3 level to identify the SP that originated the message. The DPC is inserted to identify the address of the destination SP. Routing tables within an SS7 node are used to route messages.

- **Signaling Network Management (SNM)** — Monitors link sets and route sets, providing status to network nodes so that traffic can be rerouted when necessary. SNM also provides procedures to take corrective action when failures occur, providing a self-healing mechanism for the SS7 network.

TUP and ISUP

TUP and ISUP sit on top of MTP to provide circuit-related signaling to set up, maintain, and tear down calls. TUP has been replaced in most countries because it supports only POTS calls. Its successor, ISUP, supports both POTS and ISDN calls as well as a host of other features and added flexibility. Both TUP and ISUP are used to perform inter switch call signaling. ISUP also has inherent support for supplementary services, such as automatic callback, calling line identification, and so on.

SCCP

The combination of the MTP and the SCCP is called the *Network Service Part (NSP)* in the specifications (but outside the specifications, this term is seldomused). The addition of the SCCP provides a more flexible means of routing and provides mechanisms to transfer data over the SS7 network. Such additional features are used to support non circuit-related signaling, which is mostly used to interact with databases (SCPs). It is also used to connect the radio-related components in cellular networks and for inter-SSP communication supporting CLASS services. SCCP also provides application management functions. Applicationsare mostly SCP database driven and are called subsystems. For example, in cellular networks, SCCP transfers queries and responses between the Visitor Location Register (VLR) and Home Location Register (HLR) databases. Such transfers take place for a number of reasons. The primary reason is to update the subscriber's HLR with the current VLR serving area so that incoming calls can be delivered.

Enhanced routing is called global title (GT) routing. It keeps SPs from having overly large routing tables that would be difficult to provision and maintain. A GT is a directory number that serves as an alias for a physical network address. Aphysical address consists of a point code and an application reference called a subsystem number (SSN). GT routing allows SPs to use alias addressing to save them from having to maintain overly large physical address tables. Centralized STPs are then used to convert the GT address into a physical address; this process is called Global Title Translation (GTT). This provides the mapping of traditional telephony addresses (phone numbers) to SS7 addresses (PC and/or SSN) forenhanced services. GTT is typically performed at STPs.

It is important not to confuse the mapping of telephony numbers using GTT with the translation of telephony numbers done during normal call setup. Voice switches internally map telephony addresses to SS7 addresses during normal call processing using number translation tables. This process does not use GTT. GTT is used only for non circuit-related information, such as network supplementary services (Calling Name Delivery) or database services (toll-free).

In addition to mapping telephony addresses to SS7 addresses, SCCP provides a set of subsystem management functions to monitor and respond to the condition

of subsystems. These management functions are discussed further, along with theother aspects of SCCP, in Chapter 9, "Signaling Connection Control Part (SCCP)."

TCAP

TCAP allows applications (called subsystems) to communicate with each other (over the SS7 network) using agreed-upon data elements. These data elements are called *components*. Components can be viewed as instructions sent between applications. For example, when a subscriber changes VLR location in a global system for mobile communication (GSM) cellular network, his or her HLR is updated with the new VLR location by means of an Update Location component. TCAP also provides transaction management, allowing multiple messages to be associated with a particular communications exchange, known as a transaction.

There are a number of subsystems the most common are

- Toll-free (E800)
- Advanced Intelligent Network (AIN)
- Intelligent Network Application Protocol (INAP)
- Customizable Applications for Mobile Enhanced Logic (CAMEL) •

Mobile Application Part (MAP)

Chapter-3

MOBILE IP AND WIRELESS ACCESS PROTOCOLS

INTRODUCTION TO MOBILE IP

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002 that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

The number of wireless devices for voice or data is projected to surpass the number of fixed devices. Mobile data communication will likely emerge as the technology supporting most communication including voice and video. Mobile data communication will be pervasive in cellular systems such as 3G and in wireless LAN such as 802.11, and will extend into satellite communication. Though mobility may be enabled by link-layer technologies, data crossing networks or different link layers is still a problem. The solution to this problem is a standards-based protocol, Mobile IP.

Mobile IP Overview

In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to the fixed address on the envelope. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network. The problem occurs when a device roams away from its home network and is no longer reachable using normal IP routing. This results in the active sessions of the device being terminated. Mobile IP was created to enable users to keep the same IP address while traveling to a different network (which may even be on a different wireless operator), thus ensuring that a roaming individual could continue communication without sessions or connections being dropped.

Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of

wireless and wire line networks while maintaining connections and ongoing applications. Remote login, remote printing, and file transfers are some examples of applications where it is undesirable to interrupt communications while an individual roams across network boundaries. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses could compromise the network services.

Components of a Mobile IP Network

Mobile IP has the following three components, as shown

- Mobile Node
- Home Agent
- Foreign Agent

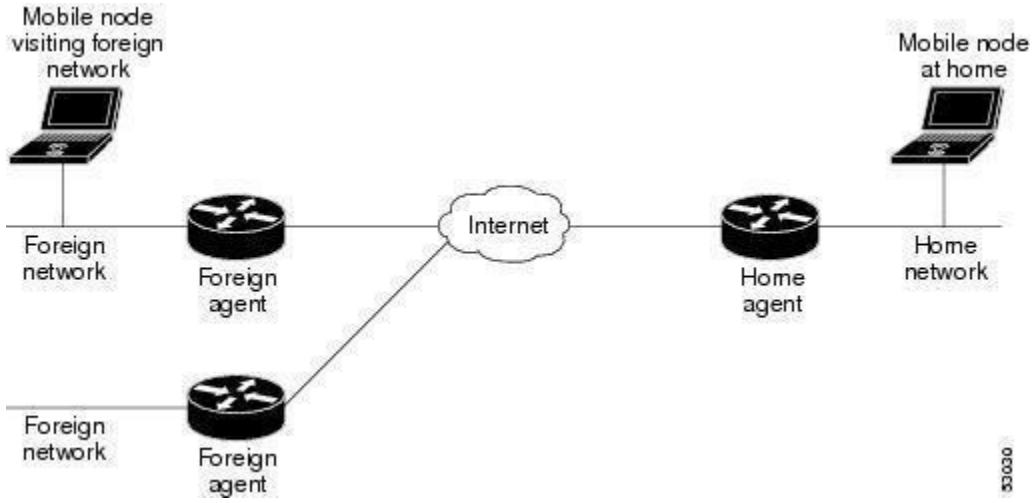


Fig 4.1 Mobile IP Components and Relationships

The Mobile Node is a device such as a cell phone, personal digital assistant, or laptop whose software enables network roaming capabilities. The Home Agent is a router on the home network serving as the anchor point for communication with the Mobile Node; it tunnels packets from a device on the Internet, called a Correspondent Node, to the roaming Mobile Node. (A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network.)

The Foreign Agent is a router that may function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

The care-of address is the termination point of the tunnel toward the Mobile Node when it is on a foreign network. The Home Agent maintains an association between the home IP address of the Mobile Node and its care-of address, which is the current location of the Mobile Node on the foreign or visited network

How Mobile IP Works

This section explains how Mobile IP works. The Mobile IP process has three main phases, which are discussed in the following sections.

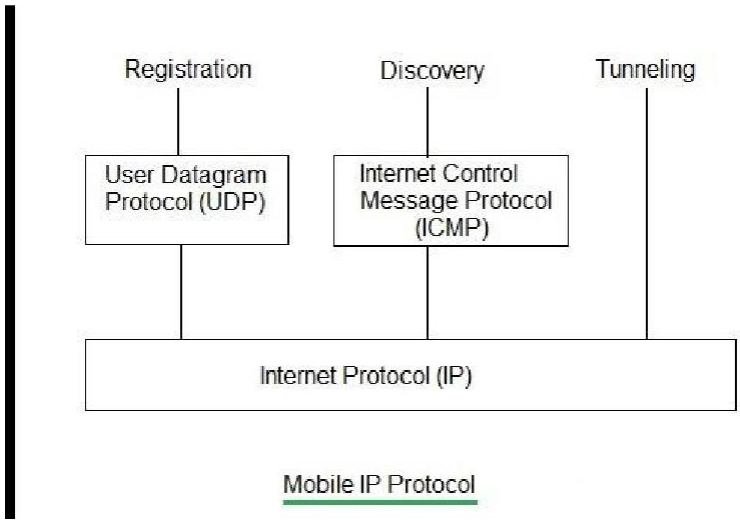


Fig. Mobile IP

- Agent Discovery

  A Mobile Node discovers its Foreign and Home Agents during agent discovery.
- Registration

  The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.
- Tunneling

  A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

a. Agent Discovery

During the agent discovery phase, the Home Agent and Foreign Agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The Mobile Node listens to these advertisements to determine if it is connected to its home network or foreign network.

The IRDP advertisements carry Mobile IP extensions that specify whether an agent is a Home Agent, Foreign Agent, or both; its care-of address; the types of services it will provide such as reverse tunneling and generic routing encapsulation (GRE); and the allowed registration lifetime or roaming period for visiting Mobile Nodes. Rather than waiting for agent advertisements, a Mobile Node can send out an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.

If a Mobile Node determines that it is connected to a foreign network, it acquires a care-of address. Two types of care-of addresses exist:

- Care-of address acquired from a Foreign Agent
- Collocated care-of address

A Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node. A Mobile Node that acquires this type of care-of address can share the address with other Mobile Nodes. A collocated care-of address is an IP address temporarily assigned to the interface of the Mobile Node itself. A collocated care-of address represents the current position of the Mobile Node on the foreign network and can be used by only one Mobile Node at a time. When the Mobile Node hears a Foreign Agent advertisement and detects that it has moved outside of its home network, it begins registration.

Registration

The Mobile Node is configured with the IP address and mobility security association (which includes the shared key) of its Home Agent. In addition, the

Mobile Node is configured with either its home IP address, or another user identifier, such as a Network Access Identifier.

The Mobile Node uses this information along with the information that it learns from the Foreign Agent advertisements to form a Mobile IP registration request. It adds the registration request to its pending list and sends the registration request to its Home Agent either through the Foreign Agent or directly if it is using a collocated care-of address and is not required to register through the Foreign Agent.

If the registration request is sent through the Foreign Agent, the Foreign Agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported. If the registration request is valid, the Foreign Agent adds the visiting Mobile Node to its pending list before relaying the request to the Home Agent. If the registration request is not valid, the Foreign Agent sends a registration reply with appropriate error code to the Mobile Node.

The Home Agent checks the validity of the registration request, which includes authentication of the Mobile Node. If the registration request is valid, the Home Agent creates a mobility binding (an association of the Mobile Node with its care-of address), a tunnel to the care-of address, and a routing entry for forwarding packets to the home address through the tunnel.

The Home Agent then sends a registration reply to the Mobile Node through the Foreign Agent (if the registration request was received via the Foreign Agent) or directly to the Mobile Node. If the registration request is not valid, the Home Agent rejects the request by sending a registration reply with an appropriate error code.

The Foreign Agent checks the validity of the registration reply, including ensuring that an associated registration request exists in its pending list. If the registration reply is valid, the Foreign Agent adds the Mobile Node to its visitor list, establishes a tunnel to the Home Agent, and creates a routing entry for forwarding packets to the home address. It then relays the registration reply to the Mobile Node.

Finally, the Mobile Node checks the validity of the registration reply, which includes ensuring an associated request is in its pending list as well as proper authentication of the Home Agent. If the registration reply is not valid, the Mobile Node discards the reply. If a valid registration reply specifies that the registration is accepted, the Mobile Node is confirmed that the mobility agents are aware of its roaming. In the collocated care-of address case, it adds a tunnel to the Home Agent. Subsequently, it sends all packets to the Foreign Agent.

The Mobile Node reregisters before its registration lifetime expires. The Home Agent and Foreign Agent update their mobility binding and visitor entry, respectively, during re registration. In the case where the registration is denied, the Mobile Node makes the necessary adjustments and attempts to register again. For example, if the registration is denied because of time mismatch and the Home Agent sends back its time stamp for synchronization, the Mobile Node adjusts the time stamp in future registration requests. Thus, a successful Mobile IP registration sets up the routing mechanism for transporting packets to and from the Mobile Node as it roams.

c. Tunneling

The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes.

Data packets addressed to the Mobile Node are routed to its home network, where the Home Agent now intercepts and tunnels them to the care-of address toward the Mobile Node. Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The default tunnel mode is IP Encapsulation within IP Encapsulation. Optionally, GRE and minimal encapsulation within IP may be used.

Typically, the Mobile Node sends packets to the Foreign Agent, which routes them to their final destination, the Correspondent Node, as shown in Figure.

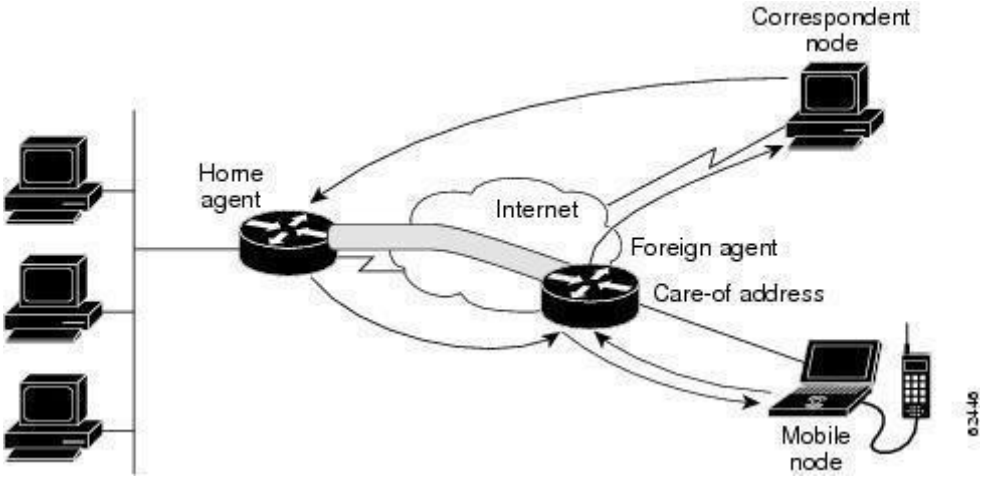


Fig. Packet Forwarding

However, this data path is topologically incorrect because it does not reflect the true IP network source for the data rather; it reflects the home network of the Mobile Node. Because the packets show the home network as their source inside a foreign network, an access control list on routers in the network called ingress filtering drops the packets instead of forwarding them. A feature called reverse tunneling solves this problem by having the Foreign Agent tunnel packets back to the Home Agent when it receives them from the Mobile Node. See Figure.

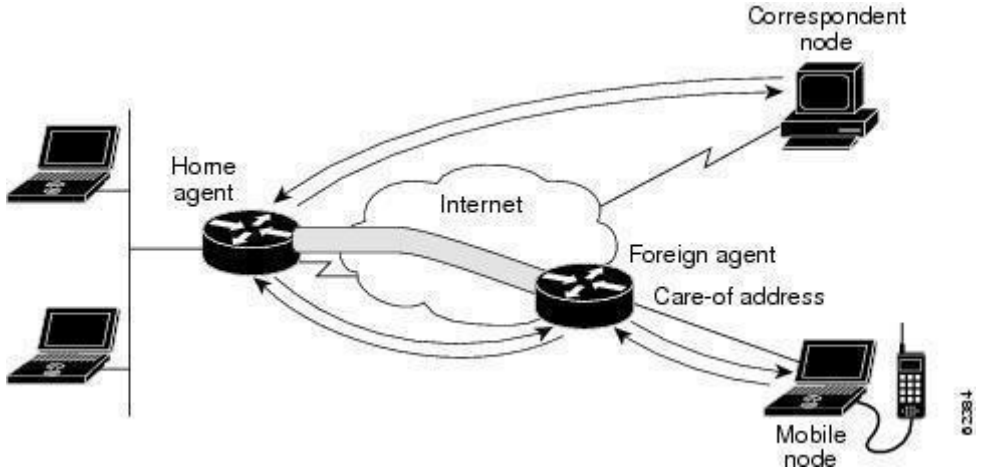


Fig .Reverse Tunnel

Tunnel MTU discovery is a mechanism for a tunnel encapsulator such as the Home Agent to participate in path MTU discovery to avoid any packet fragmentation in the routing path between a Correspondent Node and Mobile Node. For packets destined to the Mobile Node, the Home Agent maintains the MTU of the tunnel to the care-of

address and informs the Correspondent Node of the reduced packet size. This improves routing efficiency by avoiding fragmentation and reassembly at the tunnel endpoints to ensure that packets reach the Mobile Node.

d. Security

Mobile IP uses a strong authentication scheme for security purposes. All registration messages between a Mobile Node and Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE). The integrity of the registration messages is protected by a preshared 128-bit key between a Mobile Node and Home Agent. The keyed message digest algorithm 5 (MD5) in "prefix+suffix" mode is used to compute the authenticator value in the appended MHAE, which is mandatory. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a Mobile Node and Foreign Agent and between a Foreign Agent and Home Agent, respectively. Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The Home Agent returns its time stamp to synchronize the Mobile Node for registration.

Solution to Network Mobility

Network mobility is enabled by Mobile IP, which provides a scalable, transparent, and secure solution. It is scalable because only the participating components need to be Mobile IP aware the Mobile Node and the endpoints of the tunnel. No other routers in the network or any hosts with which the Mobile Node is communicating need to be changed or even aware of the movement of the Mobile Node. It is transparent to any applications while providing mobility. Also, the network layer provides link-layer independence; interlink layer roaming, and link-layer transparency. Finally, it is secure because the set up of packet redirection is authenticated.

WIRELESS ACCESS PROTOCOL (WAP) - ARCHITECTURE

Wireless Access Protocol (WAP) is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers:

- **Application Layer**

  Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WML Script.

- **Session Layer**

  Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

- **Transaction Layer**

  Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

- **Security Layer**

  Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

- **Transport Layer**

  Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

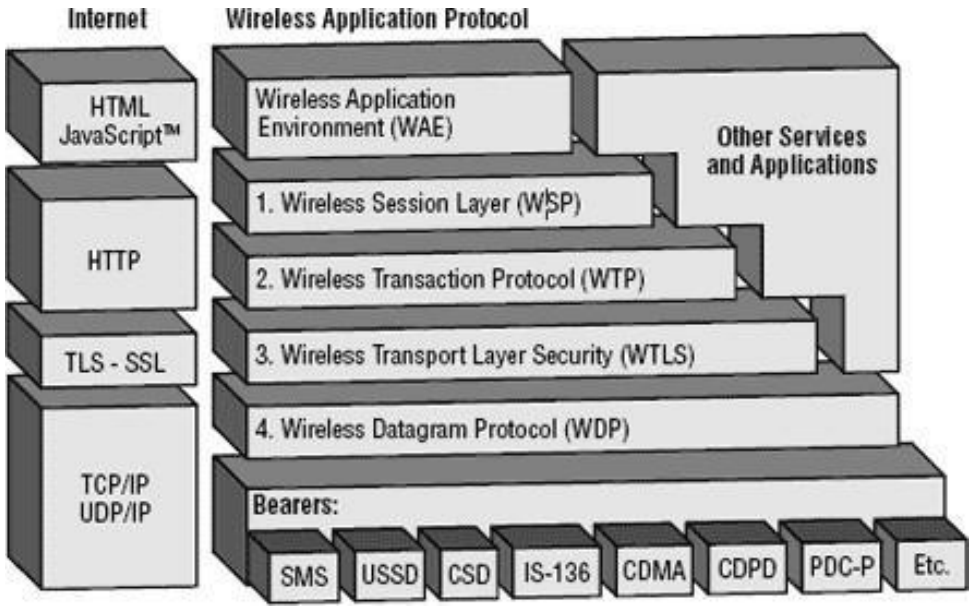


Fig . WAP protocol architecture

Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.

WML (WIRELESS MARKUP LANGUAGE) SCRIPTS

WML Script is a procedural programming language and dialect of JavaScript used for WML pages and is part of the Wireless Application Protocol (WAP). WML Script is a client-side scripting language and is similar to JavaScript. Just like JavaScript WML Script is used for tasks such as user input validation, generation of error message and other Dialog boxes etc.

WML Script is based on ECMA Script (European Computer Manufacturers Association Script), which is JavaScript's standardized version. Thus the syntax of

WML Script is similar to JavaScript but not fully compatible. Despite the syntactical similarities, they are two different languages. WML Script does not have objects or array, which JavaScript has. On the other hand, it allows you to declare and include external functions from other scripts. WML Script is optimized for low power devices, and is a compiled language.

WML Script (Wireless Markup Language Script) is the client-side scripting language of WML (Wireless Markup Language). A scripting language is similar to a programming language, but is of lighter weight. With WML Script, the wireless device can do some of the processing and computation. This reduces the number of requests and responses to/from the server.

Brief descriptions of all the important WML Script components are

WML Script Components:

WML Script is very similar to Java Script. Almost WML Script components have similar meaning as they have in Java Script. A WML Script program component are summarized as follows:

WML Script Operators:

WML Script supports following type of operators.

- Arithmetic Operators
- Comparison Operators
- Logical (or Relational) Operators
- Assignment Operators
- Conditional (or ternary) Operators

WAP SESSION PROTOCOL (WSP):

Wireless Session Protocol is a session-level protocol family for remote operations between a client and proxy or server. WAP protocols and their functions are layered in a style resembling that of the ISO OSI Reference Model [ISO7498]. Layer Management Entities handle protocol initialization, configuration and error conditions (such as loss of connectivity due to the mobile station roaming out of coverage) that are not handled by the protocol itself.

WSP is designed to function on the transaction and datagram services.

Security is assumed to be an optional layer above the transport layer. The security layer preserves the transport service interfaces. The transaction, session or application management entities are assumed to provide the additional support that is required to establish security contexts and secure connections. This support is not provided by the WSP protocols directly. In this regard, the security layer is modular. WSP itself does not require a security layer; however, applications that use WSP may require it.

WSP Features:

WSP provides a means for organized exchange of content between co-operating client/server applications. Specifically, it provides the applications means to:

a) Establish a reliable session from client to server and release that session in an orderly manner;

b) Agree on a common level of protocol functionality using capability negotiation;

c) Exchange content between client and server using compact encoding;

d) Suspend and resume the session.

The currently defined services and protocols (WSP) are most suited for browsing-type applications. WSP defines actually two protocols: one provides connection-mode session services over a transaction service, and another provides non-confirmed, connectionless services over a datagram transport service. The connectionless service is most suitable, when applications do not need reliable delivery of data and do not care about confirmation. It can be used

Without actually having to establish a session.

In addition to the general features, WSP offers means to:

a) Provide HTTP/1.1 functionality:

- Extensible request-reply methods,
- Composite objects,
- Content type negotiation

b) Exchange client and server session headers

c) Interrupt transactions in process

d) Push content from server to client in an unsynchronized manner;

e) Negotiate support for multiple, simultaneous asynchronous transactions.

Basic Functionality:

The core of the WSP design is a binary form of HTTP. Consequently the requests sent to a server and responses going to a client may include both headers (meta-information) and data. All the methods defined by HTTP/1.1 are supported.

In addition, capability negotiation can be used to agree on a set of extended request methods, so that full compatibility to HTTP/1.1 applications can be retained.

WSP provides typed data transfer for the application layer. The HTTP/1.1 content headers are used to define content type, character set encoding, languages, etc, in an extensible manner. However, compact binary encodings are defined for the well-known headers to reduce protocol overhead. WSP also specifies a compact composite data format that provides content headers for each component within the composite data object. This is a semantically equivalent binary form of the MIME "multipart/mixed" format used by HTTP/1.1.

WSP itself does not interpret the header information in requests and replies. As part of the session creation process, request and reply headers that remain constant over the life of the session can be exchanged between service users in the client and the server. These may include acceptable content types, character sets, languages, device capabilities and other static parameters. WSP will pass through client and server session headers as well as request and response headers without additions or removals.

The lifecycle of a WSP session is not tied to the underlying transport. A session can be suspended while the session is idle to free up network resources or save battery. A lightweight session re-establishment protocol allows the session to be resumed without the overhead of full-blown session establishment. A session may be resumed over a different bearer network.

WIRELESS DATAGRAM PROTOCOL (WDP):

The Wireless Datagram Protocol (WDP), a protocol in WAP architecture, covers the Transport Layer Protocols in the Internet model. As a general transport service, WDP offers to the upper layers an invisible interface independent of the underlying network technology used. In consequence of the interface common to transport protocols, the upper layer protocols of the WAP architecture can operate

independent of the underlying wireless network. By letting only the transport layer deal with physical network-dependent issues, global interoperability can be acquired using mediating gateways. The Wireless Datagram Protocol provides a UDP-like service to non-IP bearers. On IP-enabled bearers (like IP or GSM Circuit-Switched Data (CSD) or even GPRS) WDP is identical to UDP, hence people often talk about the "WDP-UDP" protocol.

WDP provides 16-bit port multiplexing and 8-bit data transport in the same way UDP does. Note that WDP is not a real dissector in Wireshark, but some dissectors (like the GSM SMS User Data dissector) will hand off protocol data to WAP dissectors as if it was handed off to a WDP dissector. WDP was added to the WAP specifications as at the time of writing the first WAP specifications there was a plethora of wireless datagram transfer protocols (TETRA, Mobitex, IDEN, GSM SMS and many others) but no-one could be used the same way for offering the WAP services. As a result, WDP provides adaptation to the relevant protocols in order to enable them to convey the WAP protocols.

Protocol dependencies

The WAP transport protocol stack is shown below:

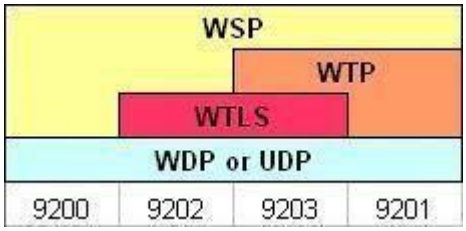


Fig 4.6 WAP transort protocol stack

Depending on the protocol stack, 4 different standard WDP (UDP) ports have been defined: 9200, 9201, 9202 and 9203. WSP can run on other ports too.

Chapter-4
WIRELESS LAN TECHNOLOGY

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11standards, marketed under the Wi-Fi brand name.

Wireless LANs have become popular in the home due to ease of installation and use, and in commercial complexes offering wireless access to their customers; often for free. New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

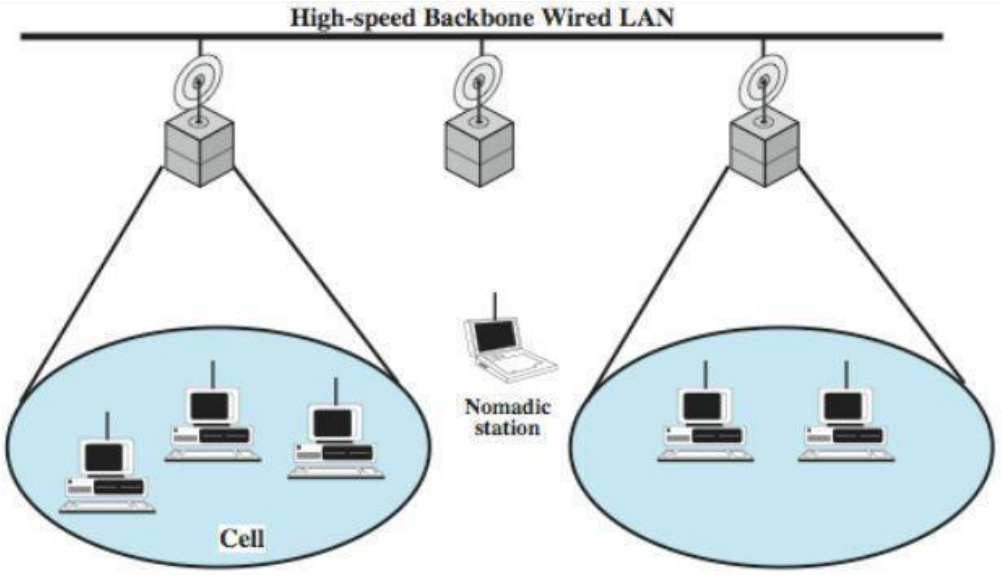


Fig: Infrastructure wireless LAN

WIRELESS LAN APPLICATIONS ARE

- LAN Extension
- Cross-building interconnect
- Nomadic Access
- Ad hoc networking

LAN EXTENSION

Wireless LAN linked into a wired LAN on same premises

Wired LAN

- Backbone
- Support servers and stationary workstations

Wireless LAN

- Stations in large open areas
- Manufacturing plants, stock exchange trading floors, and warehouses

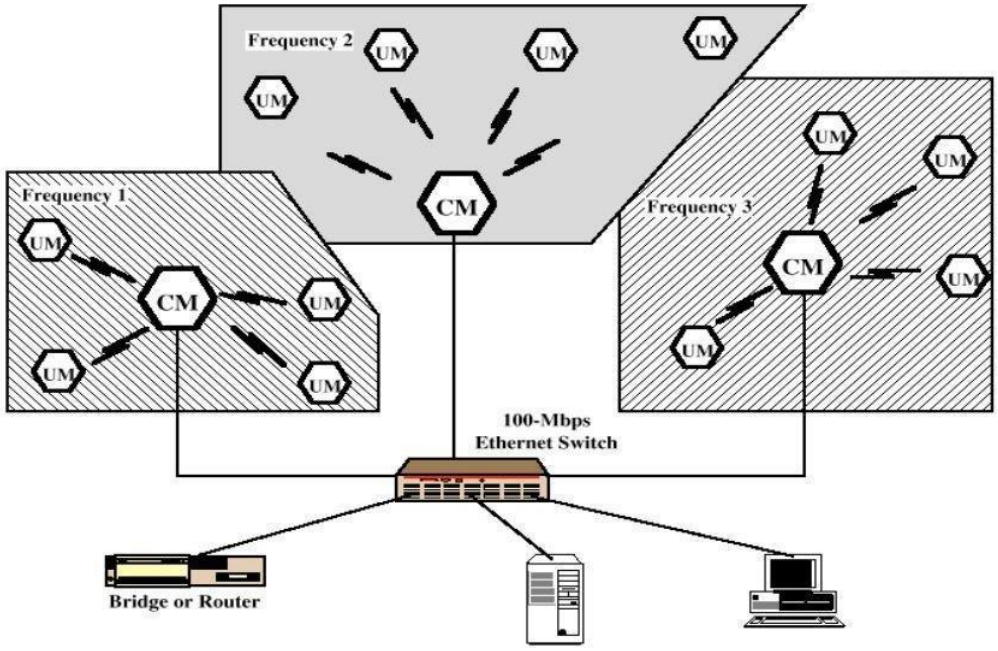


Fig: Multiple cell wireless LAN configuration

CROSS-BUILDING INTERCONNECT

- Connect LANs in nearby buildings wired or wireless LANs
- Point-to-point wireless link is used
- Devices connected are typically bridges or routers

NOMADIC ACCESS

Wireless link between LAN hub and mobile data terminal equipped with antenna

Laptop computer or notepad computer.

Uses:

- Transfer data from portable computer to office server
- Extended environment such as campus

AD HOC NETWORKING

Temporary peer-to-peer network set up to meet immediate need

Example:

Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting

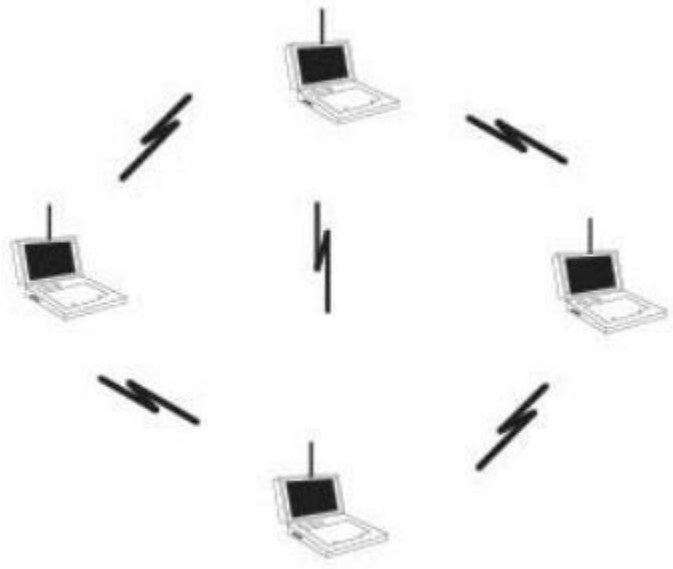


Fig: Ad Hoc LAN

WIRELESS LAN CATEGORIES

Three types of LANs are there they are

- Infrared (IR) LANs
- Spread spectrum LANs
- Narrowband microwave LANs

INFRARED (IR) LANS

Strengths of Infrared Over Microwave Radio are Spectrum for infrared virtually unlimited , Possibility of high data rates , Infrared spectrum is unregulated , Equipment inexpensive and simple , Reflected by light-colored objects , Ceiling reflection for entire room coverage , Doesn't penetrate walls , More easily secured against eavesdropping & Less interference between different rooms

IR Data Transmission Techniques are 3 types they are

1. Directed Beam Infrared IR LANs
2. Omni directional IR LANs
3. Diffused IR LANs

a. Directed Beam Infrared IR LANs

Directed Beam Infrared used to create point-to-point links range depends on emitted power and degree of focusing, focused IR data link can have range of Kilometers example Cross-building interconnect between bridges or routers.

b. Omini directional WLANs

Single base station within line of sight of all other stations on LAN Station typically mounted on ceiling, Base station acts as a multiport repeater.

- Ceiling transmitter broadcasts signal received by IR transceivers
- IR transceivers transmit with directional beam aimed at ceiling base unit

c. Diffused WLANs

All IR transmitters focused and aimed at a point on diffusely reflecting ceiling , IR radiation strikes ceiling

- Reradiated omnidirectionally
- Picked up by all receivers

SPREAD SPECTRUM LAN

Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is deliberately varied. This result in a much greater bandwidth than the signal would have if its frequency were not varied. A conventional wireless signal has a frequency, usually specified in megahertz (MHz) or gigahertz gigahertz), that does not change with time (except for small, rapid fluctuations that occur as a result of modulation).

When you listen to a signal at 103.1 MHz on an FM stereo receiver, for example, the signal stays at 103.1 MHz . It does not go up to 105.1 MHz or down to MHz. The digits on the radio's frequency dial stay the same at all times. The frequency of a conventional wireless signal is kept as constant as the state of the art will permit, so the bandwidth can be kept within certain limits, and so the signal can be easily located by someone who wants to retrieve the information.

- Multiple-cell arrangement
- Within a cell, either peer-to-peer or hub
- Peer-to-peer topology
  - No hub
  - Access controlled with MAC algorithm
    - CSMA
  - Appropriate for ad hoc LANs
- Hub topology
  - Mounted on the ceiling and connected to backbone
  - May control access
  - May act as multiport repeater
  - Automatic handoff of mobile stations
  - Stations in cell either:
    - Transmit to / receive from hub only
    - Broadcast using omnidirectional antenna

NARROWBAND MICROWAVE LANS

Use of a microwave radio frequency band for signal transmission

- Relatively narrow bandwidth
- Licensed Narrowband
  - Controlled by FCC
- Interference free
  - Each geographic area has a radius of 28Km – 5 licenses / 10 frequencies
  - Motorola holds 600 licenses in 18-GHz band!
- Unlicensed
  - Low power / 2-5 GHz

IEEE 802 PROTOCOL ARCHITECTURE

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks. More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells.

Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard.

The number 802 was simply the next free number IEEE could assign, though "802" is sometimes associated with the date the first meeting was held February 1980. The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC), so that the layers can be listed like this:

- Data link layer
  - LLC Sub layer
  - MAC Sub layer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

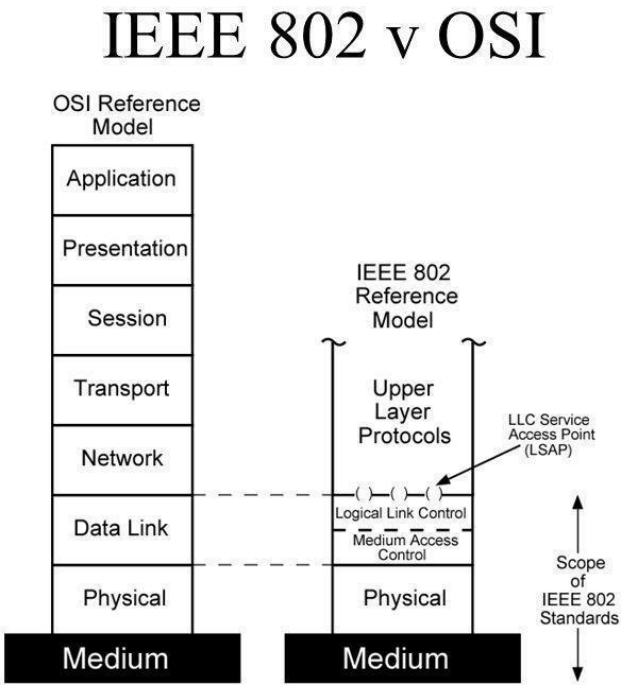


Fig: IEEE 802 Protocols compared to OSI Model

PROTOCOL ARCHITECTURE

- Functions of physical layer:
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium
- Functions of medium access control (MAC) layer:
  - On transmission, assemble data into a frame with address and error detection fields
  - On reception, disassemble frame and perform address recognition and error detection
  - Govern access to the LAN transmission medium
- Functions of logical link control (LLC) Layer:
- Provide an interface to higher layers and perform flow and error control

MAC FRAME FORMAT

MAC control contains MAC protocol information and destination MAC address contains destination physical attachment point where as source MAC address contain source physical attachment point lastly CRC (Cyclic Redundancy heck) for error checking in the frame.

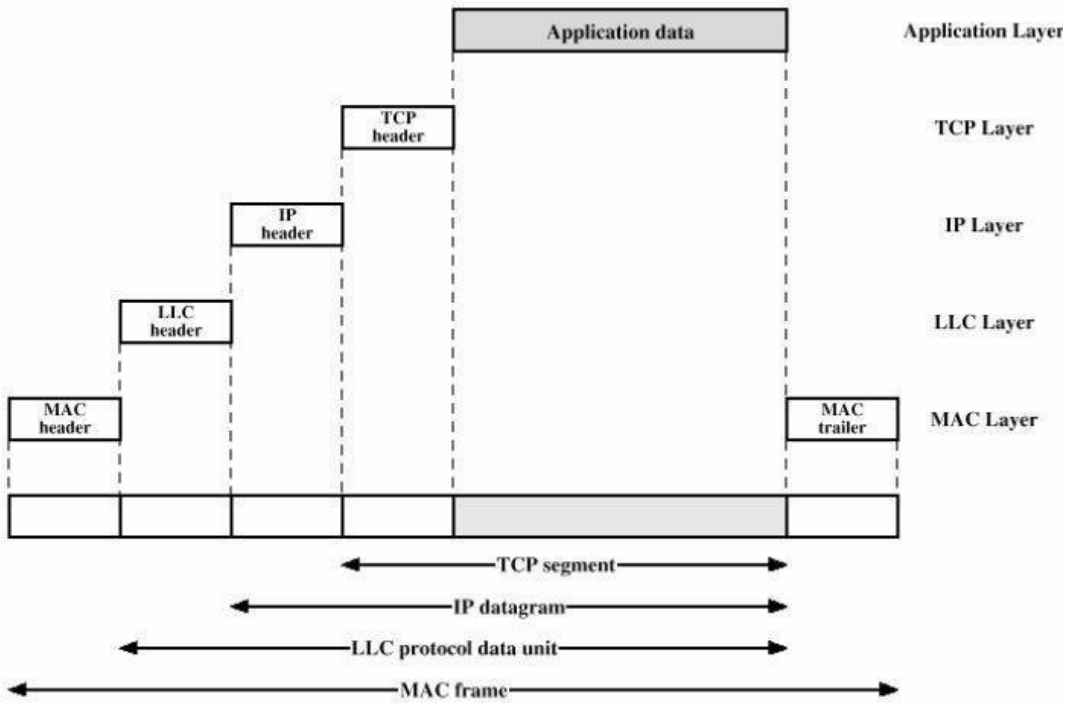


Fig: 5.4 MAC Frame structure

LOGICAL LINK CONTROL (LLC)

„ Characteristics of LLC not shared by other control protocols it must support multi-access, shared-medium nature of the link „ relieved of some details of link access by MAC layer

a. LLC Services „

- Unacknowledged connectionless service: No flow- and error-control mechanisms „ Data delivery not guaranteed. „
- Connection-mode service:„ Logical connection set up between two users „ Flow- and error-control provided „
- Acknowledged connectionless service: Cross between previous two „ Datagram acknowledged „ No prior logical setup

IEEE 802.11 ARCHITECTURE „

Distribution system (DS) „ Access point (AP) „ Basic service set (BSS) „ Stations competing for access to shared wireless medium „ Isolated or connected to backbone DS through AP „ Extended service set (ESS) „ Two or more basic service sets interconnected by DS

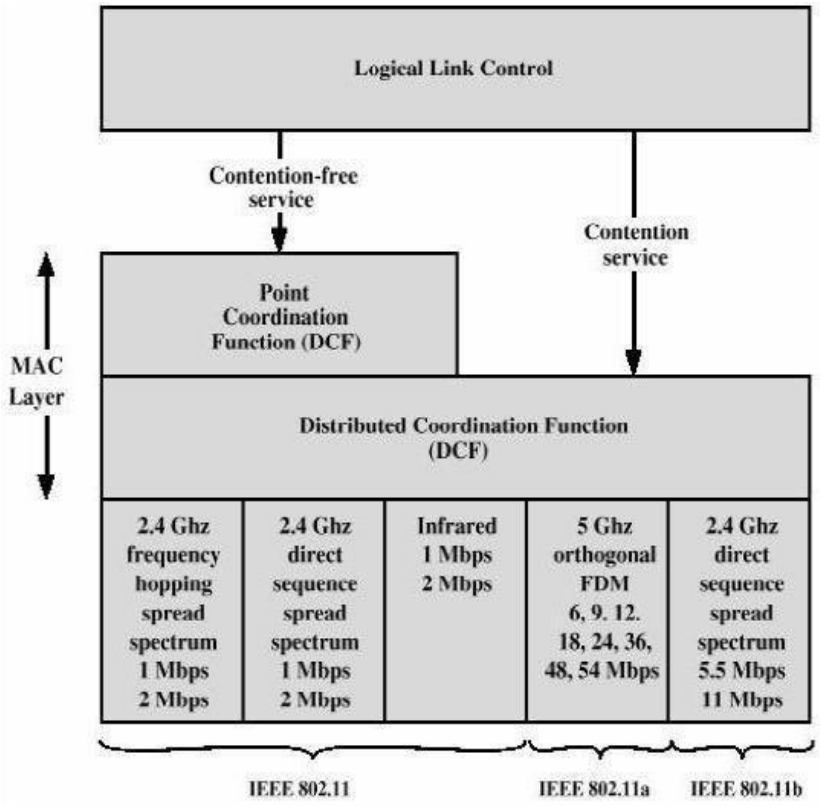


Fig: IEEE 802.11 Protocol Architecture

DISTRIBUTION OF MESSAGES WITHIN A DS

Distribution service „ Used to exchange MAC frames from station in one BSS to station in another BSS „ Integration service „ Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

Transition Types Based On Mobility:

- No transition
  - Stationary or moves only within BSS
- BSS transition
  - „ Station moving from one BSS to another BSS in same ESS
- „ ESS transition
  - „ Station moving from BSS in one ESS to BSS within another ESS

a. Association-Related Services „

Association „ Establishes initial association between station and AP „ Re-association „ Enables transfer of association from one AP to another, allowing station to move from one BSS to another „ Disassociation „ Association termination notice from station or AP

IEEE 802.11 MEDIUM ACCESS CONTROL

MAC layer covers three functional areas:

- Reliable data delivery „
- Access control „
- Security

Reliable Data Delivery

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- Frame exchange protocol
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn't receive ACK, it retransmits frame
- Four frame exchange
  - Source issues request to send (RTS)

- Destination responds with clear to send (CTS)
- Source transmits data
- Destination responds with ACK

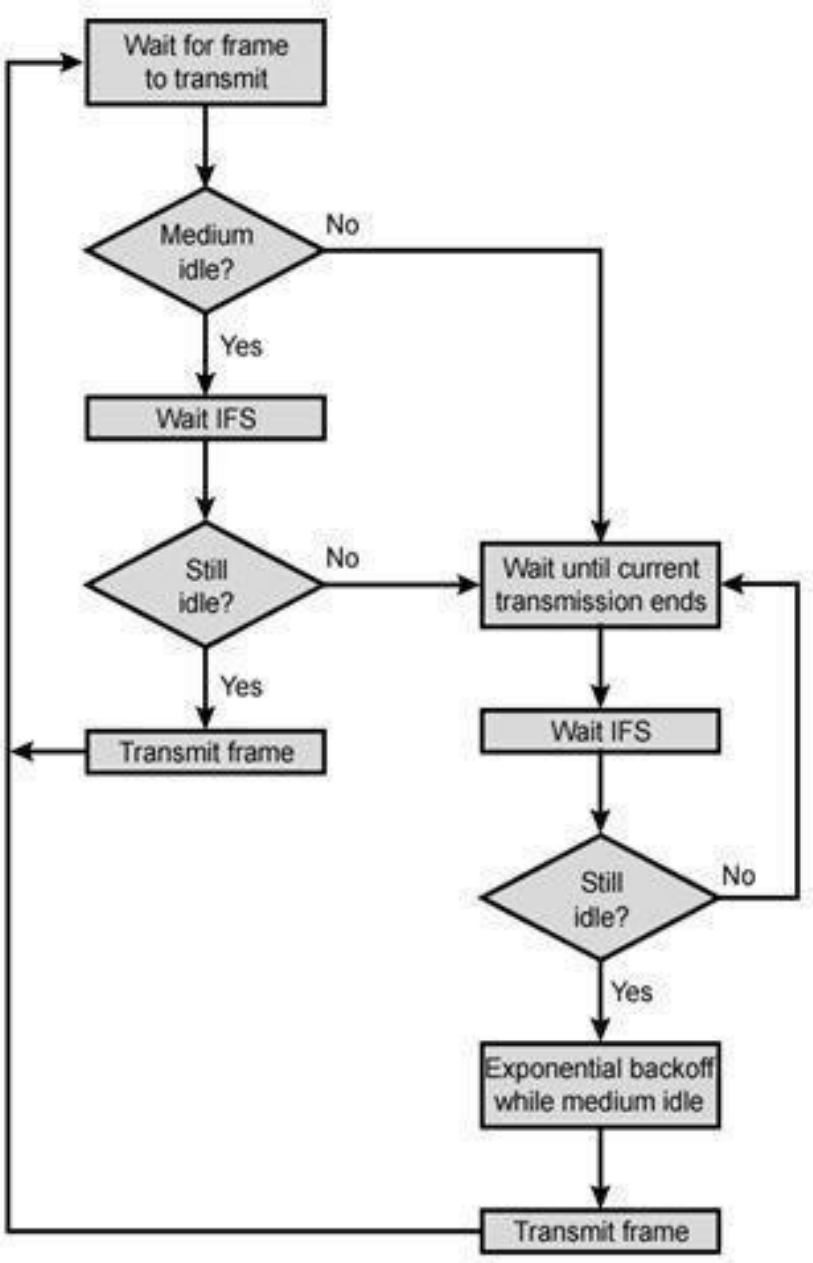


Fig: IEEE 802.11 Medium Access Control Logic

a Interframe Space (IFS) Values

- Short IFS (SIFS)„used for immediate response actions „
- Point coordination function IFS (PIFS) „used by centralized controller in PCF scheme when using polls „
- Distributed coordination function IFS (DIFS) „ Longest IFS „ Used as minimum delay of asynchronous frames contending for access

b. IFS Usage

- SIFS used for Acknowledgment (ACK) , Clear to send (CTS) &„ Poll response „
- PIFS used by centralized controller in issuing polls Takes precedence over normal contention traffic „
- DIFS used for all ordinary asynchronous traffic

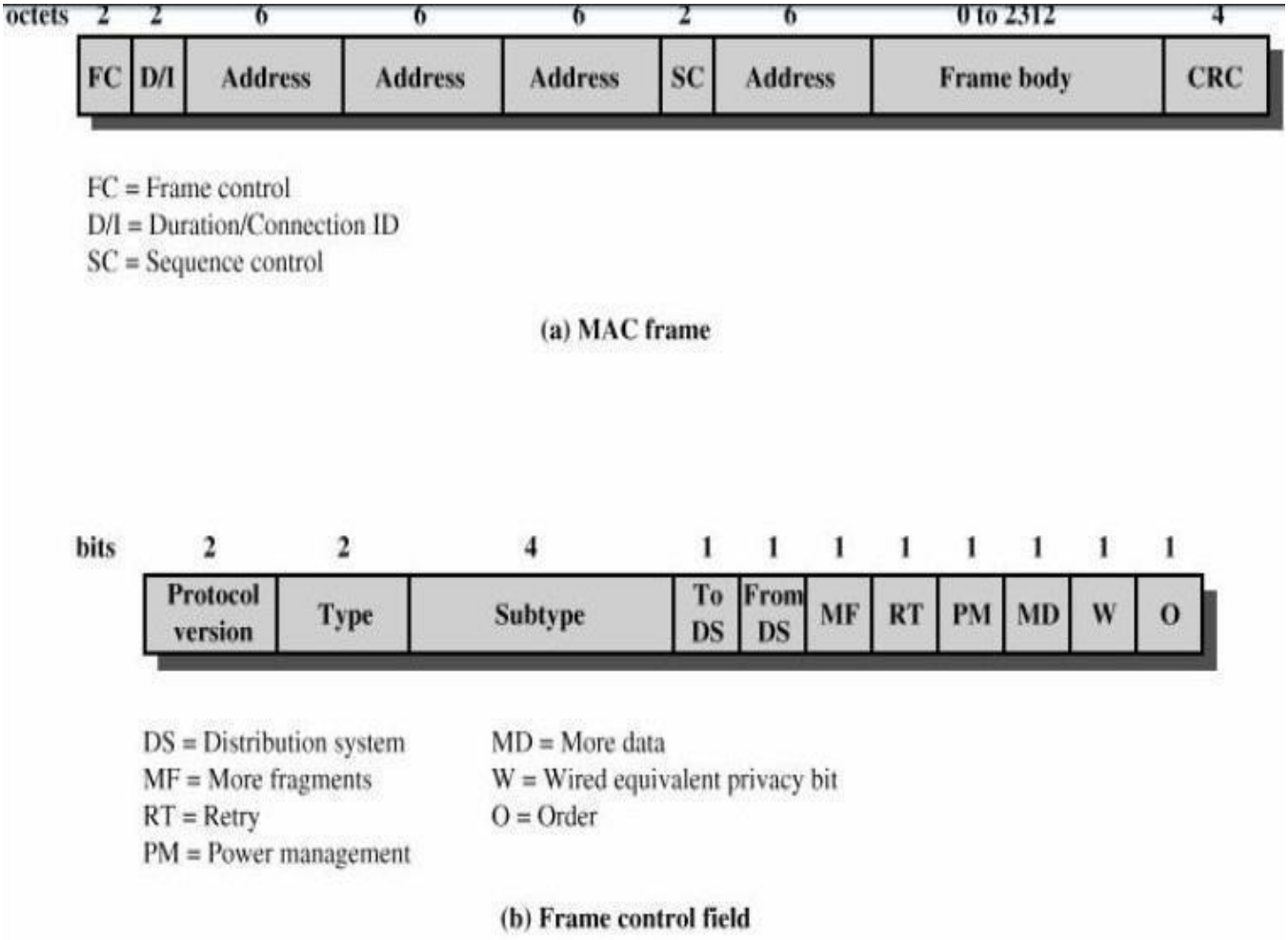


Fig: IEEE 802.11 Medium Access Control Frame Format

c. MAC Frame Fields

Following are the Frame fields in MAC Frame

- **Frame Control** – frame type, control information
- **Duration/connection ID** – channel allocation time
- **Addresses** – context dependant, types include source and destination
- **Sequence control** – numbering and reassembly
- **Frame body** – MSDU or fragment of MSDU
- **Frame check sequence** – 32-bit CRC

PHYSICAL LAYER ARCHITECTURE

This section focuses on operation of items specified by the 802.11 series of standards for the physical layer. These items will include the PLCP and PMD sublayers, management layer entities, and generic management primitives. An in-depth understanding of how the physical layer operates and how it interfaces with the MAC layer is vitally important to the analyst's understanding of information gathered by a wireless protocol analyzer.

PLCP Sublayer:

The MAC layer communicates with the Physical Layer Convergence Protocol (PLCP) sublayer via primitives (a set of "instructive commands" or "fundamental instructions") through a service access point (SAP). When the MAC layer instructs it to do so, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP minimizes the dependence of the MAC layer on the PMD sublayer by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer. The PLCP sublayer is illustrated in Figure.

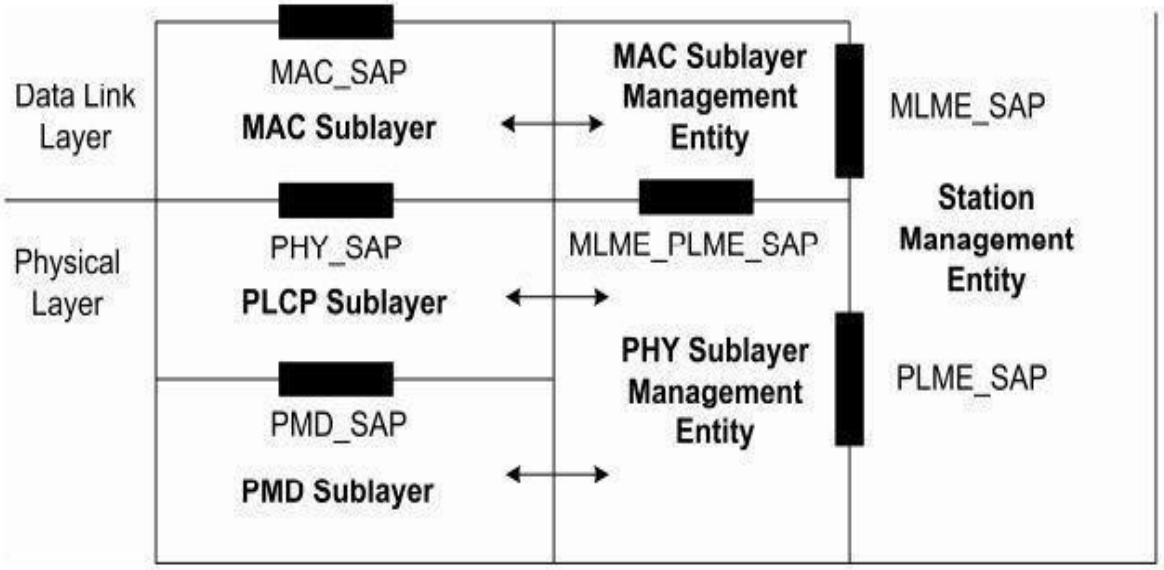


Fig: 802.11 Physical and MAC Layer Architecture

The PLCP appends a PHY-specific preamble and header fields to the MPDU that contain information needed by the Physical layer transmitters and receivers. The 802.11 standard refers to this composite frame (the MPDU with an additional PLCP preamble and header) as a PLCP protocol data unit (PPDU). The MPDU is also called the PLCP Service Data Unit (PSDU), and is typically referred to as such when referencing physical layer operations. The frame structure of a PPDU provides for asynchronous transfer of PSDUs between stations. As a result, the receiving station's Physical layer must synchronize its circuitry to each individual incoming frame.

a. Physical Layer Operations

The general operation of the various Physical layers is very similar. To perform PLCP functions, the 802.11 standard specifies the use of state machines. Each state machine performs one of the following functions: ƒ Carrier Sense/Clear Channel Assessment (CS/CCA) ƒ Transmit (Tx) ƒ Receive (Rx) Carrier Sense/Clear Channel Assessment (CS/CCA) Carrier Sense/Clear Channel Assessment is used to determine the state of the medium. The CS/CCA procedure is executed while the receiver is turned on and the station is not

currently receiving or transmitting a packet. The CS/CCA procedure is used for two specific purposes: to detect the start of a network signal that can be received (CS) and to determine whether the channel is clear prior to transmitting a packet (CCA). Transmit (Tx) Transmit (Tx) is used to send individual octets of the data frame. The transmit procedure is invoked by the CS/CCA procedure immediately upon receiving a PHY-TXSTART.request (TXVECTOR) from the MAC sublayer.

The CSMA/CA protocol is performed by the MAC with the PHY PLCP in the CS/CCA procedure prior to executing the transmit procedure. Receive (Rx) Receive (Rx) is used to receive individual octets of the data frame. The receive procedure is invoked by the PLCP CS/CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. Although counter-intuitive, the preamble and PLCP header are not "received". Only the MAC frame is "received". 218 802.11 PHY Layers The following sections describe how each of the PLCP functions is used for transferring data between the MAC and Physical layers. Carrier Sense Function The Physical layer implements the carrier sense operation by directing the PMD to check to see whether the medium is busy or idle.

The PLCP performs the following sensing operations if the station is not transmitting or receiving a frame: ƒ Detection of incoming signals - The PLCP within the station will sense the medium continually. When the medium becomes busy, the PLCP will read in the PLCP preamble and header of the frame to attempt synchronization of the receiver to the data rate of the signal. ƒ Clear channel assessment - The clear channel assessment operation determines whether the wireless medium is busy or idle. If the medium is idle, the PLCP will send a PHYCCA.indicate primitive (with its status field indicating idle) to the MAC layer. If the medium is busy, the PLCP will send a PHYCCA.indicate primitive (with its status field indicating busy) to the MAC layer.

The MAC layer can then make a decision on whether to send a frame. Stations and access points that are 802.11-compliant store the clear channel

assessment operating mode in the Physical layer MIB attribute aCCAModeSuprt. A developer can set this mode through station initialization procedures. Figure 5.8 shows an example of configuring the different CCA operating modes.

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5 GHz	1 Mb/s	2 Mb/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11b	1999	2.4-2.5 GHz	5.5 Mb/s	11 Mb/s	~35 meters	~100 meters
802.11g	2003	2.4-2.5 GHz	25 Mb/s	54 Mb/s	~25 meters	~75 meters
802.11n	2007 (unapproved draft)	2.4 GHz or 5 GHz bands	200 Mb/s	540 Mb/s	~50 meters	~126 meters

Fig: IEEE 802.11 Standards

BLUETOOTH

Introduction

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks. A manufacturer must make a device meet Bluetooth SIG standards to market it as a Bluetooth device. A network of patents apply to the technology, which are licensed to individual qualifying devices.

The main aim is to develop a short range, low power, and inexpensive wireless radio communication standard. Project is named after a king who tried to unite the Denmark and Norway. There are some IEEE standards, which resembles with Bluetooth but the main thing about Bluetooth is that its specification is for complete system, from physical layer to the application layer. But for example the specification of IEEE 802.15 standardize only physical and the data link layer: and the rest of the protocol stack is not under consideration

The Bluetooth Special Interest Group (SIG) is a trade association comprised of leaders in the telecommunications, computing, automotive, industrial automation and network industries that is driving the development of *Bluetooth* wireless technology The Special Interest Group was founded in September 1998.

SPECIFICATION OF BLUETOOTH

- Operates in the 2.4 GHZ band which is globally available
- It has 79 channels
- Uses FHSS ,GFSK modulation
- 1600 hops per second
- Can support up to 8 devices in a piconet
- Omni-directional, non line of sight transmission through walls
- 10m to 100m range
- Low cost, $20
- 1mW power
- Extended range with external power amplifier (100 meters)

BLUETOOTH BASEBAND SPECIFICATION

The part of the Bluetooth system that specifies or implements the medium access and physical layer procedures to support the exchange of real-time voice, data information streams, and ad hoc networking between Bluetooth Devices. Bluetooth Baseband is the physical layer of the Bluetooth. It manages physical channels and links apart from other services like error correction, data whitening, hop selection and Bluetooth security.

The Baseband layer lies on top of the Bluetooth radio layer in the bluetooth stack. The baseband protocol is implemented as a Link Controller, which works with the link manager for carrying out link level routines like link connection and power control. The baseband also manages asynchronous and synchronous links, handles packets and does paging and inquiry to access and inquire Bluetooth devices in the area. The baseband transceiver applies a time-division duplex (TDD) scheme. (Alternate transmits and receives). Therefore apart from different hopping frequency (frequency division), the time is also slotted.

PHYSICAL CHARACTERISTICS

Physical Channel

Bluetooth operates in the **2.4 GHz ISM band**. In the US and Europe, a band of 83.5 MHz width is available; in this band, 79 RF channels spaced 1 MHz apart are defined. In France, a smaller band is available; in this band, 23 RF channels spaced 1 MHz apart are defined.

The channel is represented by a **pseudo-random hopping sequence** hopping through the 79 or 23 RF channels. Two or more Bluetooth devices using the same channel form a **piconet**. There is one **master**and one or more **slave**(s) in each piconet. The hopping sequence is unique for the piconet and is determined by the Bluetooth device address (BD_ADDR) of the master; the phase in the hopping sequence is determined by the Bluetooth clock of the master. The channel is divided into time slots where each slot corresponds to an RF hop frequency. Consecutive hops correspond to different RF hop frequencies.

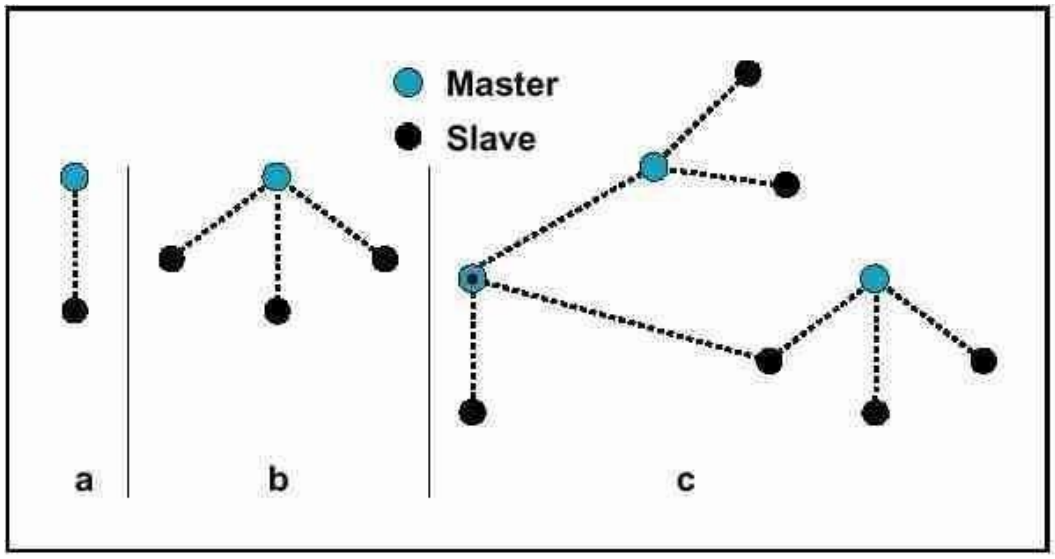


Fig: Piconet

The channel is divided into time slots, each 625 us in length. The time slots are numbered according to the Bluetooth clock of the piconet master.

A TDD scheme is used where master and slave alternatively transmit. The

master shall start its transmission in even-numbered time slots only, and the slave shall start its transmission in odd-numbered time slots only. The packet start shall be aligned with the slot start.

Physical Links

The 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, is synchronous and synchronous user information.

Device Addressing

4 possible types of addresses can be assigned to bluetooth units, BD_ADDR, AM_ADDR, PM_ADDR & AR_ADDR

BD_ADDR: Bluetooth Device Address.	Each Bluetooth transceiver is allocated a unique 48-bit device address. It is divided into a 24-bit LAP field, a 16-bit NAP field and a 8-bit UAP field.

AM_ADDR: Active Member Address	It is a 3-bit number. It is only valid as long as the slave is active on the channel. It is also sometimes called the MAC address of a Bluetooth unit.
PM_ADDR: Parked Member Address	It is a 8-bit member (master-local) address that separates the parked slaves. The PM_ADDR is only valid as long as the slave is parked.
AR_ADDR: Access Request Address	This is used by the parked slave to determine the slave-to-master half slot in the access window it is allowed to send access request messages in. It is only valid as long as the slave is parked and is not necessarily unique.

PACKETS

All data on the piconet channel is conveyed in packets.

Packet Types

13 different packet types are defined for the baseband layer of the Bluetooth system. All higher layers use these packets to compose higher level PDU's. The packets are ID, NULL, POLL, FHS , DM1 ; these packets are defined for both SCO and ACL links. DH1, AUX1, DM3, DH3, DM5, DH5 are defined for ACL links only. HV1, HV2, HV3 , DV are defined for SCO links only.

PACKET FORMAT

Each packet consists of 3 entities, the **access code** (68/72 bits),the **header** (54 bits) , and the **payload** (0-2745 bits).

- **Access Code**: 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 unique piconet while the DAC is used for paging and its responses. IAC is used for inquiry purpose.

- **Header**: The header contains information for packet acknowledgement, packet numbering for out-of-order packet reordering, flow control, slave address and error check for header.
- **Payload**: The packet payload can contain either voice field, data field or both. It has a data field; the payload will also contain a payload header.

CHANNEL CONTROL

Controller States

Bluetooth controller operates in two major states: Standby and Connection. There are seven substates 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 packet, using the channel (master) access code and the master Bluetooth clock. The hopping scheme used is the channel hopping scheme. The other states (page, inquiry etc are described below)

Connection Setup (Inquiry/Paging)

Step 1:

The **inquiry procedure** enables a device to discover which devices are in range, and determine the addresses and clocks for the devices.

1.1:	The inquiry procedure involve a unit (the source) sending out inquiry packets (**inquiry** state) and then receiving the inquiry reply
1.2:	The unit that receives the inquiry packets (the destination), will hopefully be in the **inquiry scan** state to receive the inquiry packets.
1.3:	The destination will then enter the **inquiry response** state and send an inquiry reply to the source.

After the inquiry procedure has completed, a connection can be established using the paging procedure.

Step 2:

With the **paging procedure**, an actual connection can be established. The paging procedure typically follows the inquiry procedure. Only the Bluetooth device address is required to set up a connection. Knowledge about the clock (clock estimate) will accelerate the setup procedure. A unit that establishes a connection will carry out a page procedure and will automatically be the master of the connection. The procedure occurs as follows:

2.1:	A device (the source) pages another device (the destination).	**Page** state
2.2:	The destination receives the page.	**Page Scan** state
2.3:	The destination sends a reply to the source.	**Slave Response** state : (Step 1)
2.4:	The source sends an FHS packet to the destination.	**Master Response** state : (Step 1)
2.5:	The destination sends it's second reply to the	**Slave Response** state : (Step

	source.	2)
2.6:	The destination & source then switch to the source channel parameters.	**Master Response** state: Step 2 **& Slave Response** state: Step 3

The **Connection** state starts with a POLL packet sent by the master to verify that slave has switched to the master's timing and channel frequency hopping. The slave can respond with any type of packet.

Connection Modes

A Bluetooth device in the **Connection** state can be in any of the four following modes: **Active, Hold, Sniff** and **Park** mode.

- **Active Mode:** In the active mode, the Bluetooth unit actively participates on the channel. The master schedules the transmission based on traffic demands to and from the different slaves. In addition, it supports regular transmissions to keep slaves synchronized to the channel. Active slaves listen in the master-to-slave slots for packets. If an active slave is not addressed, it may sleep until the next new master transmission.
- **Sniff Mode:** Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. In the SNIFF mode, a slave device listens to the piconet at reduced rate, thus reducing its duty cycle. The SNIFF interval is programmable and depends on the application. It has the highest duty cycle (least power efficient) of all 3 power saving modes (sniff, hold & park).
- **Hold Mode**: Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. The master unit can put slave units into HOLD mode, where only an internal timer is running. Slave units can also demand to be put into HOLD mode. Data transfer restarts instantly when units transition out of HOLD mode. It has an intermediate duty cycle (medium power efficient) of the 3 power saving modes (sniff, hold & park).
- **Park Mode:** In the PARK mode, a device is still synchronized to the piconet but does not participate in the traffic. Parked devices have given up their MAC (AM_ADDR) address and occasional listen to the traffic of the master to re-synchronize and check on broadcast messages. It has the

lowest duty cycle (power efficiency) of all 3 power saving modes (sniff, hold & park).

SCATTERNET

Multiple piconets may cover the same area. Since each piconet has a different master, the piconets hop independently, each with their own channel hopping sequence and phase as determined by the respective master. In addition, the packets carried on the channels are preceded by different channel access codes as determined by the master device addresses. As more piconets are added, the probability of collisions increases; a graceful degradation of performance results as is common in frequency-hopping spread spectrum systems.

If multiple piconets cover the same area, a unit can participate in two or more overlaying piconets by applying time multiplexing. To participate on the proper channel, it should use the associated master device address and proper clock offset to obtain the correct phase. A Bluetooth unit can act as a slave in several piconets, but only as a master in a single piconet. A group of piconets in which connections consists between different piconets is called a **scatternet**. Sometimes an existing master or slave may wish to swap roles (i.e. a **master-slave switch**); this can take place in two steps:

1. First a TDD switches of the considered master and slave, followed by a piconet switch of the both participants.
2. Then, if so desired, other slaves of the old piconet can be transferred to the new piconet.

When a unit has acknowledged the reception of the FHS packet, this unit uses the new piconet parameters defined by the new master and the piconet switch is completed.

Other Baseband Functions Error Correction

There are three kinds of error correction schemes used in the baseband protocol: 1/3 rate FEC, 2/3 rate FEC and ARQ scheme.

- In **1/3 rate FEC** every bit is repeated three times for redundancy,

- In **2/3 rate FEC** a generator polynomial is used to encode 10 bit code to a 15 bit code,
- In the **ARQ scheme**, **DM, DH** and the data field of **DV** packets are retransmitted till an acknowledgement is received (or timeout is exceeded). Bluetooth uses fast, unnumbered acknowledgement in which it uses positive and negative acknowledgements by setting appropriate ARQN values. If the timeout value is exceeded, Bluetooth flushes the packet and proceeds with the next.

Flow Control

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

If these RX 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.

Synchronization

The Bluetooth transceiver uses a time-division duplex (TDD) scheme, meaning that it alternately transmits and receives in a synchronous manner. The average timing of master packet transmission should not drift faster than 20 ppm relative to the ideal slot timing of 625 us. Jitter from average timing should be less than 1 microsecond. The piconet is synchronized by the master. To transmit on the piconet channel you need 3 pieces of information, The (channel) hopping sequence, the phase of the sequence, and the CAC to place on the packets.

Channel Hopping Sequence	The Bluetooth Device Address (BD_ADDR) of the master is used to derive this frequency hopping sequence.
Phase	The system clock of the master determines the phase in the hopping sequence.
Channel Access Code	This is derived from the Bluetooth Device Address (BD_ADDR) of the master.

The slaves adapt their native clocks with a timing offset in order to match the master clock, giving then an estimated clock value. The offset is zero for the master as its native clock **is** the master clock. The Bluetooth clocks should have the LSB ticking in units of 312.5us, giving a clock rate of 3.2 kHz.

A 20us uncertainty window is allowed around the exact receive time in order for the access correlator for the receiver to search for the correct channel access code and get synchronized with the transmitter. When a slave returns from the hold mode, it can correlate over a bigger uncertainty window till they don't overlap slots. A parked slave periodically wakes up to listen to beacons from the master and re-synchronizes its clock offset.

Bluetooth Security

At the link layer, security is maintained by authentication of the peers and encryption of the information. For this basic security we need a public address which is unique for each device (BD_ADDR), two secret keys (authentication keys and encryption key) and a random number generator. First a device does the authentication by issuing a challenge and the other device has to then send a response to that challenge which is based on the challenge, it's BD_ADDR and a link key shared between them. After authentication, encryption may be used to communicate. See our Bluetooth Security page and Bluetooth article(s) for more details

BLUETOOTH PROTOCOL STACK

The Bluetooth protocol stack is defined as a series of layers, though there are some features which cross several layers. A Bluetooth device can be made up of two parts: a host implementing the higher layers of the protocol stack, and a module implementing the lower layers. This separation of the layers can be useful for several reasons. For example, hosts such as PCs have spare capacity to handle higher layers, allowing the Bluetooth device to have less memory and a less powerful processor, which leads to cost reduction.

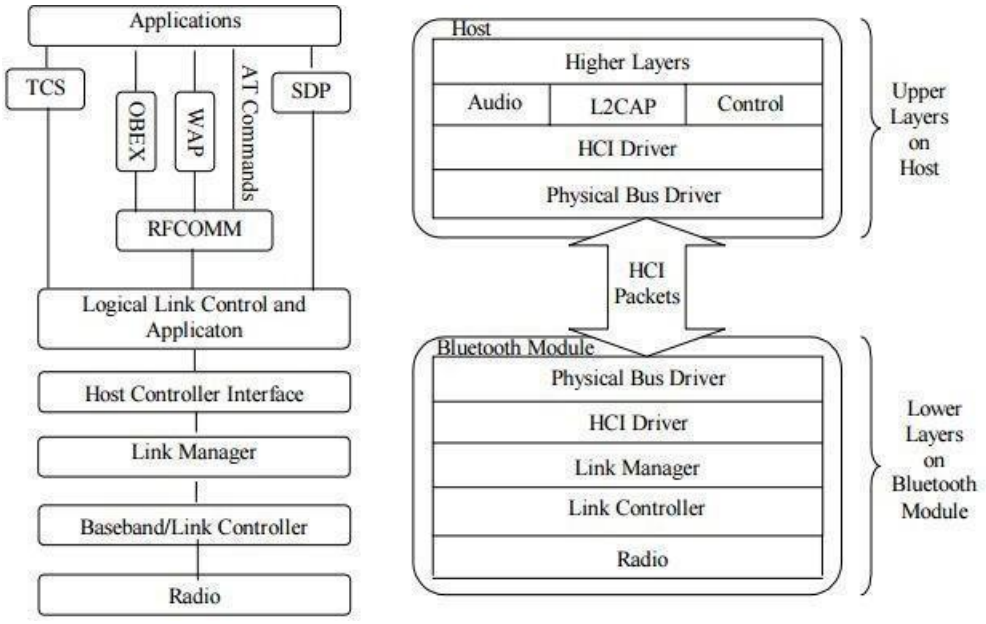


Fig .Typical Bluetooth Protocol Stack

Also, the host device can sleep and be awoken by an incoming Bluetooth connection. Of course, an interface is needed between the higher and lower layers, and for that purpose the Bluetooth defines the Host Controller Interface (HCI). But for some small and simple systems, it is still possible to have all layers of the protocol stack run on one processor. An example of such a system is a headset

BLUETOOTH MODULE

Baseband - There are two basic types of physical links that can be established between a master and a slave: • Synchronous Connection Oriented (SCO) • Asynchronous Connection-Less (ACL) An SCO link provides a symmetric link between the master and the slave, with regular periodic exchange of data in the form of reserved slots. Thus, the SCO link provides a circuit-switched connection where data are regularly exchanged, and as such it is intended for use with time-bounded information as audio. A master can support up to three SCO links to the same or to different slaves. A slave can support up to three SCO links from the same master. An ACI link is a point-to-multipoint link between the master and all the slaves on the piconet.

It can use all of the remaining slots on the channel not used for SCO links. The ACL link provides a packet-switched connection where data are exchanged

sporadically, as they become available from higher layers of the stack. The traffic over the ACL link is completely scheduled by the master. Each Bluetooth device has a 48 bit IEEE MAC address that is used for the derivation of the access code. The access code has pseudo-random properties and includes the identity of the piconet master. All the packets exchanged on the channel are identified by this master identity. That prevents packets sent in one piconet to be falsely accepted by devices in another piconet that happens to use the same hopping frequency in the certain time slot. . All packets have the same format, starting with an access code, followed by a packet header and ending with the user payload.

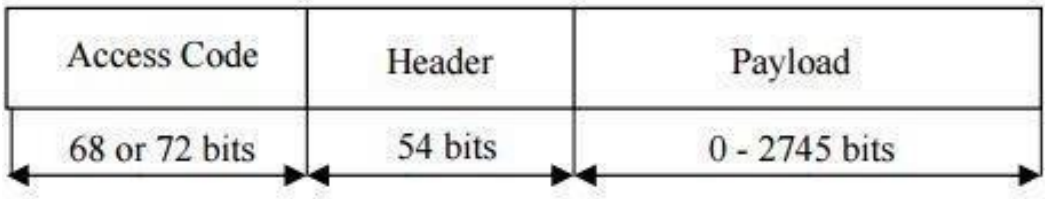


Fig. Bluetooth Packet Structure

The access code is used to address the packet to a specific device. The header contains all the control information associated with the packet and the link. The payload contains the actual message information. The Bluetooth packets can be 1, 3, or 5 slots long, but the multislot packets are always sent on a single-hop carrier. The Link Controller - The link control layer is responsible for managing device discoverability, establishing connections and maintaining them. In Bluetooth, three elements have been defined to support connection establishment: scan, page and inquiry. Inquiry is a process in which a device attempts to discover all the Bluetooth enabled devices in its local area.

A unit that wants to make a connection broadcasts an inquiry message that induces the recipients to return their addresses. Units that receive the inquiry message return an FHS (FH synchronization) packet which includes, among other things, their identity and clock information. The identity of the recipient is required to determine the page message and wake-up sequence. For the return of FHS packets, a random backoff mechanism is used to prevent collisions.

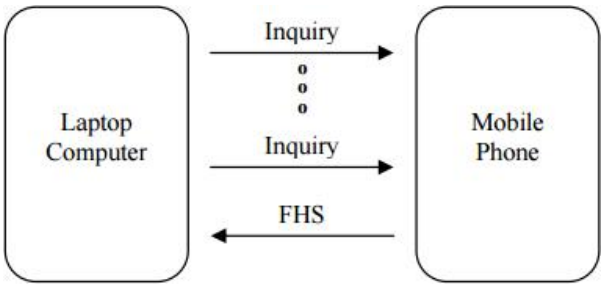


Fig: Discovering a Bluetooth device

a. The Link Manager

The host drives a Bluetooth device through Host Controller Interface (HCI) commands, but it is the link manager that translates those commands into operations at the baseband level. Its main functions are to control piconet management (establishing and destruction of the links and role change), link configuration, and security and QoS functions. Link manager communicates with its peers on other devices using the Link Management Protocol (LMP). Every LMP message begins with a flag bit which is 0 if a master initiated the transaction and 1 if the slave initiated the transaction. That bit is followed by a 7-bit Operation Code, and by the message's parameters.

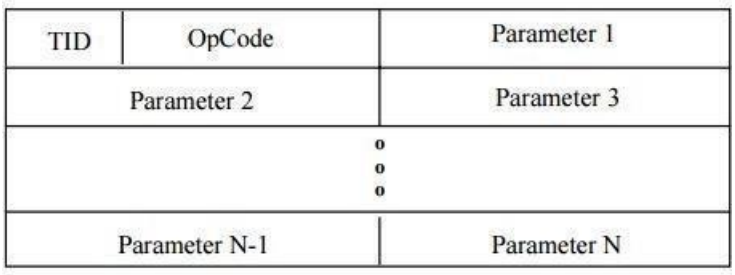


Fig: LMP PDU payload body

When a link is first set up, it uses single-slot packets by default. Multi-slot packets make more efficient use of the band, but there are some occasions when they can't be used, for example on noisy links or if SCO links don't leave sufficient space between their slots for multi-slot packets. LMP also provides a mechanism for negotiating encryption modes and coordinating encryption keys used by devices on both ends of the link. In addition, LMP supports messages for configuration of the quality of service on a connection. Packet types can automatically change according to the channel quality, so that the data can be transferred at a higher rate when

the channel quality is good, and on lower rates with more error protection if the channel quality deteriorates.

b. Bluetooth Logical Link Control & Adaptation Protocol (L2CAP)

Logical Link Control and Adaptation Protocols take data from higher layers of the Bluetooth stack and from applications and send them over the lower layers of the stack. It passes packets either to the HCI, or in a host-less system directly to the Link Manager. The major functions of the L2CAP are

- Multiplexing between different higher layer protocols to allow several higher layer links to share a single ACL connection. L2CAP uses channel numbers to label packets so that, when they are received, they can be routed to the correct place.
- Segmentation and reassembly to allow transfer of larger packets than lower layers support.
- Quality of service management for higher layer protocols.

All applications must use L2CAP to send data. It is also used by Bluetooth's higher layers such as RFCOMM and SDP, so L2CAP is a compulsory part of every Bluetooth system.

RFCOMM

RFCOMM is a simple, reliable transport protocol that provides emulation of the serial cable line settings and status of an RS-232 serial port. It provides connections to multiple devices by relying on L2CAP to handle multiplexing over single connection. RFCOMM supports two types of devices:

- Type 1 - Internal emulated serial port. These devices usually are the end of a communication path, for example a PC or printer.
- Type 2 - Intermediate device with physical serial port. These are devices that sit in the middle of a communication path, for example a modem.

Up to 30 data channels can be set up, so RFCOMM can theoretically support 30 different services at once. RFCOMM is based on GSM TS 07.10 standard, which is an asymmetric protocol used by GSM cellular phones to multiplex several streams of data onto one physical serial cable.

WLL TECHNOLOGY

Wireless local loop (WLL), is the use of a wireless communications link as the "last mile / first mile" connection for delivering plain old telephone service (POTS) or Internet access (marketed under the term "broadband") to telecommunications customers. Various types of WLL systems and technologies exist. Other terms for this type of access include Broadband Wireless Access (BWA), Radio In The Loop (RITL), Fixed-Radio Access(FRA), Fixed Wireless Access (FWA) and Metro Wireless (MW).

Wireless local loop technology Wireless local loop, often called WLL, uses cellular or personal communications services (PCS) spectrum but subtracts the mobility factor, creating a fixed service, like regular telephone service without any wires. It is considered a solution in areas where there are few or no wired facilities, such as undeveloped countries or areas of rugged terrain, but had also been touted as a potential local service alternative in the U.S. The network is built around a number of radio base stations, each connected by microwave, coax or fiber optic back-hauls to one or more central office switches.

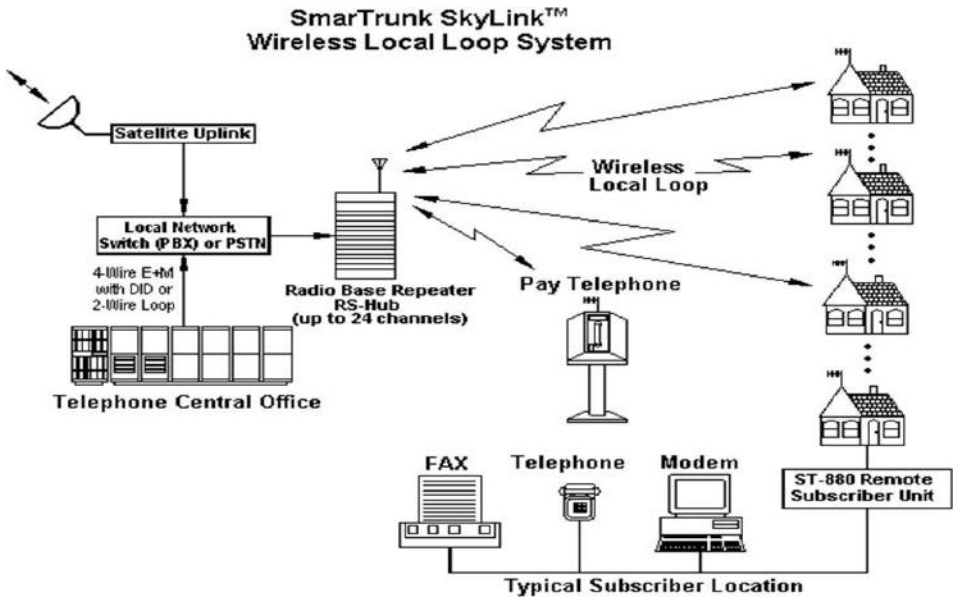


Fig: A general WLL Setup

The Radio Base Station is connected to a customer unit attached to the residential or office by a radio link. The Residential unit has a directional antenna aimed at the base station and is fitted outside the served building in order to provide a high quality link with wire line quality of service. The telephone handset is

connected to it via a standard phone jack inside the building. At the Network Operations Centre the Element Manager provides information on the base station and customer site traffic and equipment, whilst also supplying facilities to activate and deactivate lines and services. This definition of WiLL is becoming most common It is a wireless means of providing local loop access, replacing the copper pair into a home or business, often providing zero mobility unless combined with a cordless phone/device. Typically used for broadband applications Wireless in Local Loop is meant to serve subscribers at homes or offices. The telephone provided must be at least as good as wired phone. Its voice quality must be high – a subscriber carrying out long conversation must not be irritated with quality.

Chapter 5

MOBILE DATA NETWORKS

INTRODUCTION

In studying the principles of data communications, the wireless spectrum is generally treated as part of communications media only. This may give the impression that the remaining components of a wireless data network were the same as those of a fixed, wired network. The reality, however, is quite different, thanks to a number of factors with varying degree of roles in wireless and fixed, wired networks. There are network components that exist in only one network type and not the other. There are also network components existing in both types, but playing a less significant role in one or the other.

There are many sub-systems, such as antenna radiation and mobility management that do not surface in the fixed, wired networks. Wall connectors are not usually part of transmission systems in wireless networks. There are systems that do make an essential part of both network types, but with much less significance in one than the other.

Examples of such systems are power consumption systems, data security, and privacy, by containing signal, signal detection techniques and error-control techniques. Lastly, there are certainly many components that play equally important roles in both types of networks, such as switching and routing techniques, flow and congestion control mechanisms and call-control procedures. Thus a study of wireless data networks has its own scope, different from networking systems in general.

DATA ORIENTED CDPD NETWORKS

Cellular Digital Packet Data (CDPD) was a wide-area mobile data service which used unused bandwidth normally used by AMPS mobile phones between 800 and 900 MHz to transfer data. Speeds up to 19.2 kbit/s were possible. The service was discontinued in conjunction with the retirement of the parent AMPS service; it has been functionally replaced by faster services such as 1xRTT, EV-DO, and UMTS/HSPA.

Developed in the early 1990s, CDPD was large on the horizon as a future technology. However, it had difficulty competing against existing slower but less expensive Mobitex and DataTac systems, and never quite gained widespread acceptance before newer, faster standards such as GPRS became dominant.

CDPD had very limited consumer products. AT&T Wireless first sold the technology in the United States under the PocketNet brand. It was one of the first products of wireless web service. Digital Ocean, Inc. an OEM licensee of the Apple Newton, sold the Seahorse product, which integrated the Newton handheld computer, an AMPS/CDPD handset/modem along with a web browser in 1996, winning the CTIA's hardware product of the year award as a smart phone, arguably the world's first. A company named OmniSky provided service for Palm V devices.

Cingular Wireless later sold CDPD under the Wireless Internet brand (not to be confused with Wireless Internet Express, their brand for GPRS/EDGE data). PocketNet was generally considered a failure with competition from 2G services such as Sprint's Wireless Web. AT&T Wireless sold four PocketNet Phone models to the public: the Samsung Duette and the Mitsubishi MobileAccess-120 were AMPS/CDPD PocketNet phones introduced in October 1997; and two IS-136/CDPD Digital PocketNet phones, the Mitsubishi T-250 and the Ericsson R289LX.

Despite its limited success as a consumer offering, CDPD was adopted in a number of enterprise and government networks. It was particularly popular as a first-generation wireless data solution for telemetry devices (machine to machine communications) and for public safety mobile data terminals. In 2004, major carriers in the United States announced plans to shut down CDPD service. In July 2005, the AT&T Wireless and Cingular Wireless CDPD networks were shut down. Equipment for this service now has little to no residual value.

CDPD NETWORK AND SYSTEM

Primary elements of a CDPD network are:

End systems: physical & logical end systems that exchange information

Intermediate systems: CDPD infrastructure elements that store, forward & route the information.

There are 2 kinds of End systems

1. Mobile end system: subscriber unit to access CDPD network over a wireless interface.
2. Fixed end system: common host/server that is connected to the CDPD backbone and providing access to specific application and data.

There are 2 kinds of Intermediate systems

1. Generic intermediate system: simple router with no knowledge of mobility issues
2.mobile data intermediate system: specialized intermediate system that routes data based on its knowledge of the current location of Mobile end system. It is a set of hardware and software functions that provide switching, accounting, registration, authentication, encryption, and so on.

The design of CDPD was based on several design objectives that are often repeated in designing overlay networks or new networks. A lot of emphasis was laid on open architectures and reusing as much of the existing RF infrastructure as possible. The design goal of CDPD included location independence and independence from, service provider, so that coverage could be maximized ; application transparency and multiprotocol support, interoperability between products from multiple vendors.

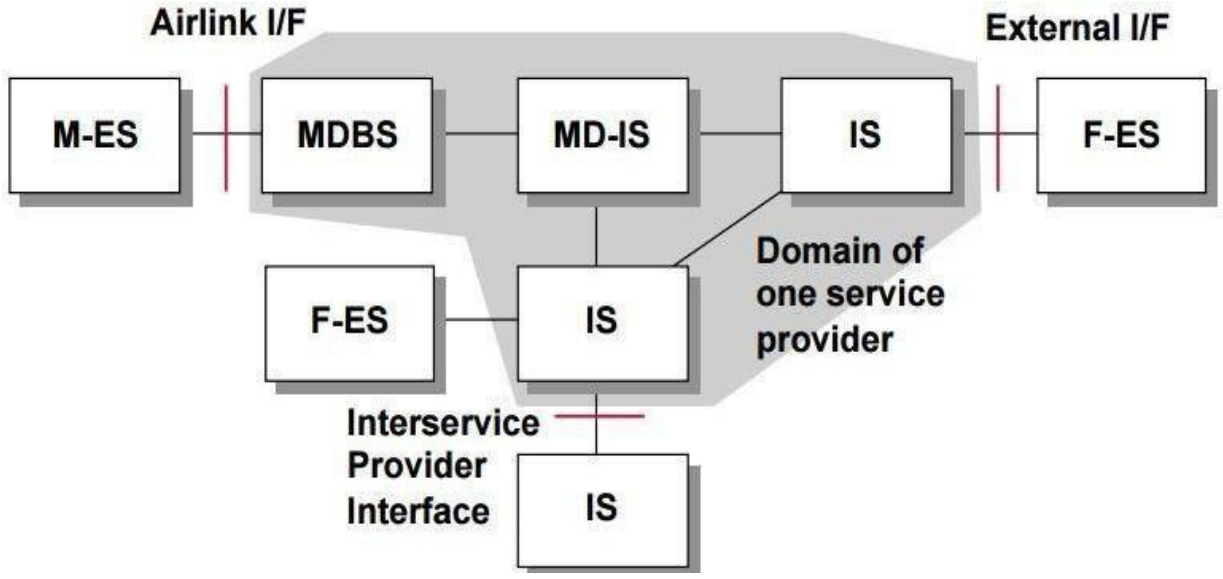


Fig: CDPD Network Architecture

a CDPD Entities:

M-ES (Mobile End Systems):

- CDPD network trackes location of ES and routes them network datagram's
- ES address does NOT imply location; current sub network "point of attachment" determines this.
- ES' are associated with the CDPD network's routing domain, not the user's corporate home network
- Mobility support functions:
  - » Mobility management: tracking MDES and routing
  - » Radio resource management: connectivity to subnet work "point of attachment"

F-ES (Fixed End Systems):

- Fixed location, traditional routing can be used.
- Internal F-ES: provided by service provider, considered to be inside the security firewall.
  - » For authentication, authorization, network mgmt, accounting
  - » For domain name services, location services, etc.
- External F-ES: external to CDPD, must operate over the external network interface.

IS, MD-IS (Intermediate Systems):

- IS provides routing (can be off-the-shelf.
- MD-IS provides MOBILE routing: MNLP (Mobile Network Location Protocol)
  - »Mobile Home Function: like home agent processing in Mobile IP or HLR function in cellular networks; uses encapsulation to forward packets to MD-IS in the visited region
  - » Mobile Serving Function: like foreign agent processing in Mobile IP or VLR function in cellular networks

MD-BS (Mobile Data Base Station):

- Controls radio interface, responsible for radio channel allocation, radio media access
  - » RF Channel Pair: Forward link from BS to multiple ESs Reverse link from multiple ESs to BS
- Co located with cellular voice equipment

- CDPD channels must be able to hop to new frequencies as demanded by the voice services

CDPD PROTOCOLS

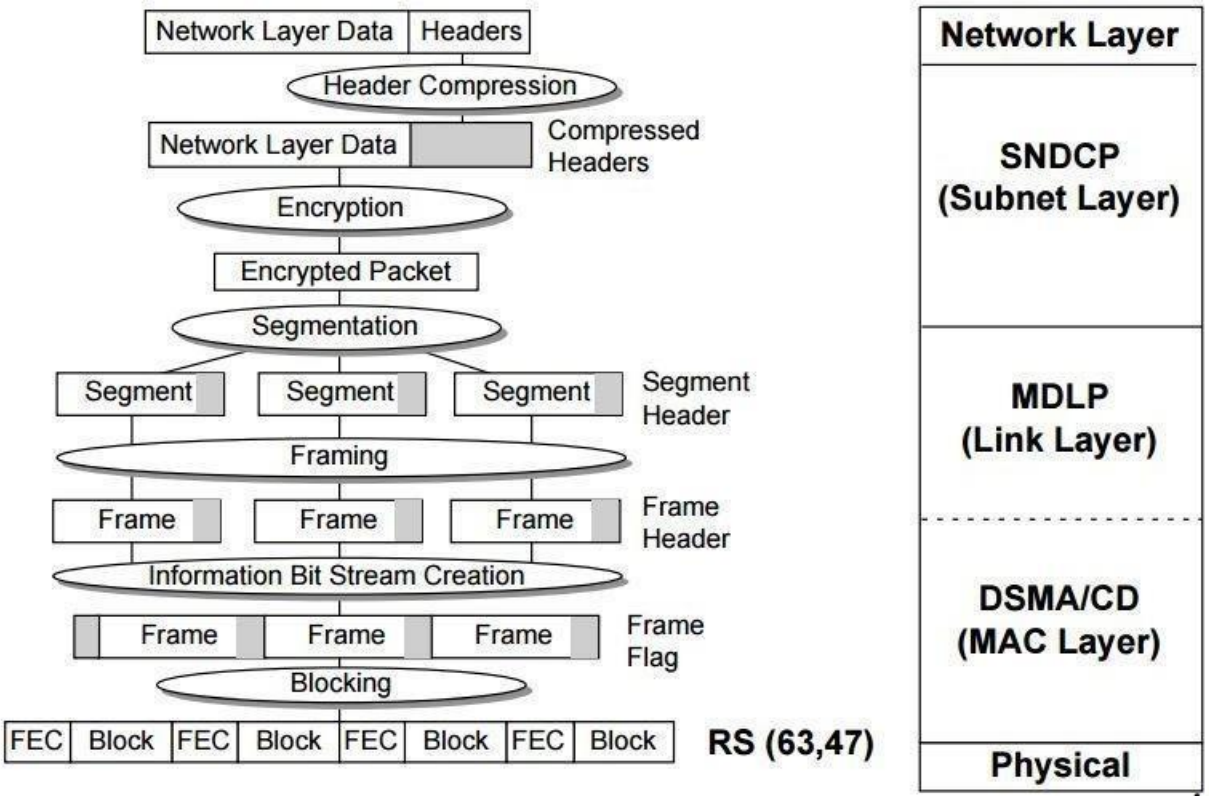


Fig: CDPD Protocol Stack

a PHYSICAL LAYER

- Uses GMSK modulation, raw data rate is 19.2 Kbps.
- Restricted to using pair of analog or digital TDMA cellular voice frequency pairs for each physical CDPD channel
- Physical layer services:
  - » Tune to specified pair of RF channels
  - » Transmit/receive bits
  - » Set power levels
  - » Measure signal strengths
  - » Suspend/resume monitoring of RF channels in M-ES to conserve battery power

MAC LAYER

- Arbitrate access to shared medium between M-ES and MD-BS and Frame recognition, frame delimiting, error detection/ correction

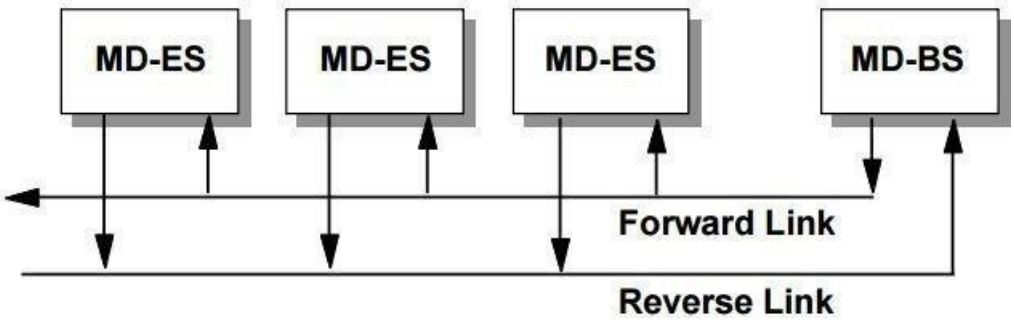


Fig: 7.3 Medium Access Control Layer

- Forward link is scheduled by BS, signals channel idle/busy & Reverse link Contention access with back-off.
- Forward channel:

  » Data packets "broadcast" from BS to ES HDLC, zero insertion, frames segmented into 274 bit (+8 bit color code) blocks, extended with ECC to 378 bits

  » Forward channel sync word, reverse channel busy/idle flag, decode failure flags, 378 RS (63, 47) block
- Reverse channel:

  » DSMA/CD access strategy

  » 378 bit blocks/up to 64 of these per burst

  » M-ES will back off and retry whenever it senses decode failure flag on the forward channel.

MOBILE DATA LINK PROTOCOL (MDLP)

- Point (MDIS) to multipoint (M-ES), connection-oriented, fully sequenced, acknowledged transfers.
- Functions provided include:

  » One or more logical data link connections on a channel stream

  » Sequence control

  » Transmission/format/operational error detection and recovery retransmits missing blocks

  » Flow control

  » Sleep function for power conservation

» Dynamic address assignment (Temporary Equipment ID--TEI)

SUB NETWORK DEPENDENT CONVERGENCE PROTOCOL (SNDCP)

- Connectionless mode subnet work service
- Provides the following functions:
  - » Mapping of data primitives
  - » Segmentation/reassembly of NPDUs
  - » Compression/elimination of redundant protocol control information
  - » Encryption/decryption
  - » Network layer to data link layer multiplexing to support multiple network layer protocols on top of the data link

GPRS (GENERAL PACKET RADIO SERVICE)

The introduction of second generation cellular mobile systems witnessed an impressive growth in the number of mobile subscribers. The most popular second generation systems are GSM and IS-95. The GSM system is based on FDMA-TDMA technology and is widely used in Europe, many parts of Asia and Africa. The IS-95 system is based on CDMA technology and is used in North America. With the increasing popularity of these systems there was an increasing demand for the data services over the wireless.

In future it is expected that the wireless systems would be able to provide various kind of services like Internet access over wireless, streaming audio and video, text and multimedia messaging services. Existing cellular systems do not fulfill the current data needs. The data rates are slow, the connection setup time is long and the services are too expensive. The reason for this is that these systems are designed primarily to handle circuit switched voice data and a channel is dedicated to a single user for the entire duration of the call. This leads to inefficient channel utilization for the packet switched data since it is bursty in nature and many calls could utilize same channel.

If packet switched bearer service is provided, the channels can be allocated to the users when needed, leading to sharing of the physical channel (Statistical multiplexing) and thus efficient channel utilization. The General Packet Radio Service (GPRS) has been developed to address the above inefficiencies and to

simplify the wireless access to packet data network. It applies packet radio principles to efficiently transfer data between GSM mobile stations and external packet data network. GPRS supports both X.25 and IP (IPv4 as well as IPv6) networks. GPRS offers session establishment time below one second and data rates up to several tens kbit/s.

It also provides for user friendly billing since the billing is based on the amount of transmitted data as against GSM where user is billed based on the duration of the call. This is suitable for applications with bursty traffic (e.g. web browsing) where user can be "online" for longer period of time but will be billed based on transmitted data volume.

SYSTEM ARCHITECTURE

In GSM system the mobile handset is called Mobile Station (MS). A cell is formed by the coverage area of a Base Transceiver Station (BTS) which serves the MS in its coverage area. Several BTS together are controlled by one Base Station Controller (BSC). The BTS and BSC together form Base Station Subsystem (BSS). The combined traffic of the mobile stations in their respective cells is routed through a switch called Mobile Switching Center (MSC). Connection originating or terminating from external telephone (PSTN) are handled by a dedicated gateway Gateway Mobile Switching Center (GMSC). The architecture of a GSM system is shown in the figure 7.4 below.

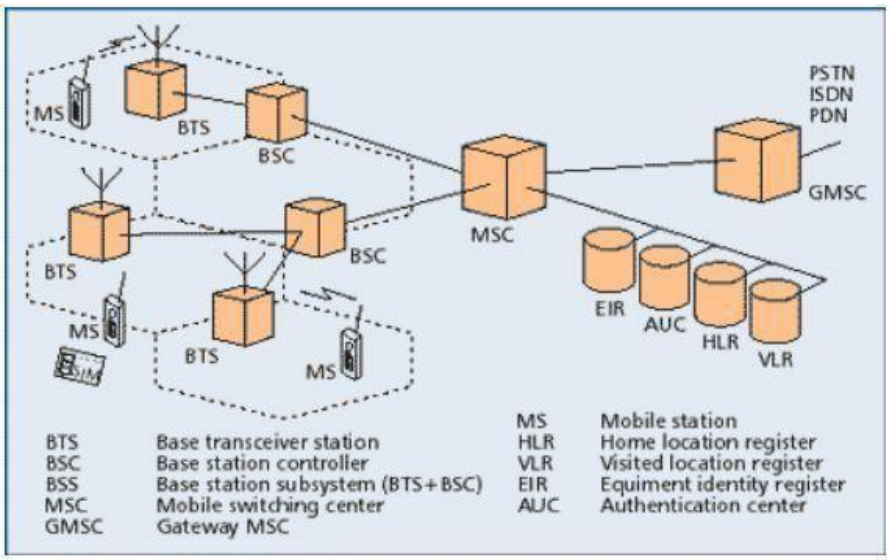


Fig: GPRS Architecture

In addition to the above entities several databases are used for the purpose of call control and network management. These databases are Home Location Register (HLR), Visitor Location Register (VLR), the Authentication Center (AUC), and Equipment Identity Register (EIR). Home Location Register (HLR) stores the permanent (such as user profile) as well as temporary (such as current location) information about all the users registered with the network. A VLR stores the data about the users who are being serviced currently. It includes the data stored in HLR for faster access as well as the temporary data like location of the user.

The AUC stores the authentication information of the user such as the keys for encryption. The EIR stores stores data about the equipments and can be used to prevent calls from a stolen equipments. All the mobile equipments in GSM system are assigned unique id called IMSI (International Mobile Equipment Identity) and is allocated by equipment manufacturer and registered by the service provider. This number is stored in the EIR. The users are identified by the IMSI (International Module Subscriber Identity) which is stored in the Subscriber Identity Module (SIM) of the user. A mobile station can be used only if a valid SIM is inserted into an equipment with valid IMSI. The "real" telephone number is different from the above ids and is stored in SIM. The most important network nodes added to the existing GSM networks are:

- SGSN (Serving GPRS Support Node)
- GGSN (Gateway GPRS Support Node)

The Serving GPRS Support Node (SGSN) is responsible for routing the packet switched data to and from the mobile stations (MS) within its area of responsibility. The main functions of SGSN are packet routing and transfer, mobile attach and detach procedure (Mobility Management (MM)), location management, assigning channels and time slots (Logical Link Management (LLM)), authentication and charging for calls. It stores the location information of the user (like the current location, current VLR) and user profile (like IMSI addresses used in packet data networks) of registered users in its location register.

The Gateway GPRS Support Node (GGSN) acts as interface between the GPRS backbone and the external packet data network (PDN). It converts the GPRS packet

coming from the SGSN into proper packet data protocol (PDP) format (i.e. X.25 or IP) before sending to the outside data network. Similarly it converts the external PDP addresses to the GSM address of the destination user. It sends these packets to proper SGSN. For this purpose the GGSN stores the current SGSN address of the user and his profile in its location register.The GGSN also performs the authentication and charging functions. In general there may be a many to many relationship between the SGSN and GGSN. However a service provider may have only one GGSN and few SGSNs due to cost constraints. A GGSN proved the interface to several SGSNs to the external PDN.

GPRS SERVICES

The bearer services of GPRS offer end-to-end packet switched data transfer. Of the two types of bearer services offered by GPRS only the point-to-point (PTP) service is available now and the point-to-multipoint (PTM) service will be made available in future releases of GPRS. The PTP service offers transfer of data packets between two users. It is offered in both connectionless mode (PTP connectionless network service (PTP-CLNS), e.g., for IP) and connectionoriented mode (PTP connection-oriented network service (PTP-CONS), e.g., for X.25).

The PTM service offers transfer of data packets from one user to multiple users. There exist two kinds of PTM services:

- Using the multicast service PTM-M, data packets are broadcast in a certain geographical area. A group identifier indicates whether the packets are intended for all users or for a group of users.
- Using the group call service PTM-G, data packets are addressed to a group of users (PTM group) and are sent out in geographical areas where the group members are currently located.
- It is also possible to send SMS over GPRS. In fact the 160 character limit in GPRS is not applicable in GPRS as in GSM. It is also planned to have other supplementary services like call forwarding unconditional (CFU), call forwarding on mobile subscriber not reachable (CFNRc), and closed user group (CUG).

ENHANCED DATA RATES FOR GSM EVOLUTION (**EDGE**):

EDGE is a digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM. EDGE is considered a pre-3G radio technology and is part of ITU's 3G definition. EDGE was deployed on GSM networks beginning in 2003 – initially by Cingular (now AT&T) in the United States. EDGE is standardized also by 3GPP as part of the GSM family. A variant, so called Compact-EDGE, was developed for use in a portion of Digital AMPS network spectrum.

Through the introduction of sophisticated methods of coding and transmitting data, EDGE delivers higher bit-rates per radio channel, resulting in a threefold increase in capacity and performance compared with an ordinary GSM/GPRS connection. EDGE can be used for any packet switched application, such as an Internet connection. Evolved EDGE continues in Release 7 of the 3GPP standard providing reduced latency and more than doubled performance e.g. to complement High-Speed Packet Access (HSPA). Peak bit-rates of up to 1 Mbit/s and typical bit-rates of 400 kbit/s can be expected.

SHORT MESSAGING SERVICE IN GSM

Short Message Service (**SMS**) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.SMS was the most widely used data application, with an estimated 3.5 billion active users, or about 80% of all mobile phone subscribers at the end of 2010. The term "SMS" is used for both the user activity and all types of short text messaging in many parts of the world.

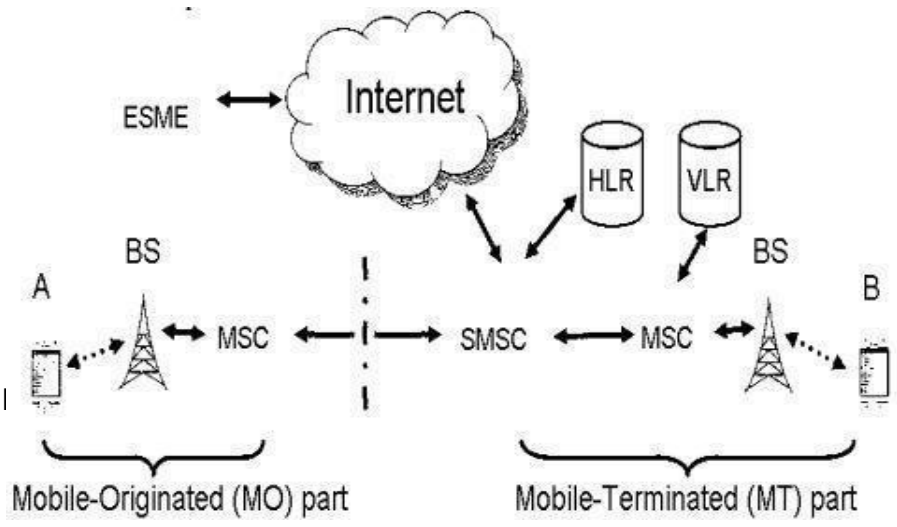


Fig: 7.5 Typical Network Architecture for SMS

SMS is also employed indirect marketing, known as SMS marketing. As of September 2014, global SMS messaging business is said to be worth over USD 100 billion, and SMS accounts for almost 50 percent of all the revenue generated by mobile messaging.SMS as used on modern handsets originated from radio telegraphy in radio memo pagers using standardized phone protocols.

These were defined in 1985 as part of the Global System for Mobile Communications (GSM) series of standards as a means of sending messages of up to 160 characters to and from GSM mobile handsets. Though most SMS messages are mobile-to-mobile text messages, support for the service has expanded to include other mobile technologies, such as ANSI CDMA networks and Digital AMPS, as well as satellite and landline networks

WIRELESS ATM & HIPER LAN

WIRELESS ATM

The increasing importance of portable computing/telecommunications applications has motivated the studies on broadband wireless network technologies such as wireless ATM (Asynchronous Transfer Mode) or WATM. Wireless ATM technology has been studied over the last couple of years by research and development groups as well as standards organizations worldwide. Several research and development efforts concerning validations and refining handover and location management protocols have been performed.

A number of system-level prototypes for WATM have been developed by these R&D labs in different parts of the world. WATM is now being actively considered as a potential framework for next-generation wireless communication networks capable of supporting integrated, quality-of-service (QoS) based multimedia services. Although ATM technology is very complex and its wireless adoption is more complicated, many technical issues are being solved. The strength of the wireless ATM technology will be its ability to support different protocols like ISDN and Internet protocols.

In this paper, we briefly outlined the concepts of ATM with its applications and services to present the basis for wireless ATM. We provide a system-level explanation of main technical issues in the specification of a wireless ATM network and its protocol architecture with data link control, medium access control, wireless control, mobility management issues. Technology development status with the standards activities are also mentioned and a brief summary is given.

ATM AND WIRELESS ATM Asynchronous Transfer Mode (ATM) technology combines the performance of high speed switching systems developed by the telecommunications industry and the flexibility of Local Area Networks (LANs) developed by the computer industry. ATM networks consist of fast packet switching systems linked by means of point-to-point links to each other and to their terminal nodes [6]. All data are packaged into cells of 53 bytes with each cell carrying 5

bytes of control information (header). The header part allows the switch to process cells according to service requirements of the source and to route cells to the target. Terminals set up a connection, i.e. a route through the network, to the destination terminal before they start transferring cells over it. Besides advertising their destination, they also negotiate a quality-of-service (QoS), specifying, for example, the tolerable cell delay and cell loss probability. ATM's high data rates, its negotiated connection set-up as well as its flexibility allow it to carry any type of traffic between any number of network nodes.

Wireless ATM is to add nomadic access capability to ATM based networks by supporting mobility as well as native ATM transport capability. ATM is a transport technology characterized by its flexibility to accommodate any type of service as well as high-speed transport capability. As mentioned before, it is capable of carrying any kind of traffic, from circuit-switched voice to burst data traffic at any speed by changing the transmission rate of 53-byte-long ATM cells and wireless version is intended to provide broadband services to a variety of mobile terminals via a standard ATM network API 3. This means that the network should support the full range of ATM services such as UBR, ABR, VBR and CBR. While these services would be qualitatively identical to those available at a wired ATM interface, the maximum bit rate may be numerically constrained by access radio link speed. Based on an analysis made in, for the current and near-future applications, service bit rates in the region of 1-10Mb/s are viewed as the typical design goal.

WIRELESS ATM ARCHITECTURE

Wireless ATM architecture is obtained by incorporating new wireless protocols at the access level and extensions into the standard ATM protocol stack which is shown in Figure 8.1 . At the access level, new protocols are needed for:

- Physical layer radio channels between the mobile terminals and base stations,
- Medium access control (MAC) to arbitrate the shared use of the radio channels by the mobile terminals
- Data/logical link control (DLC/LLC) to detect and/or correct the radio channel errors and maintain end-to-end QoS.

- Wireless control to support such functions as radio resource management at the physical, MAC and DLC layers, as well as mobility management.

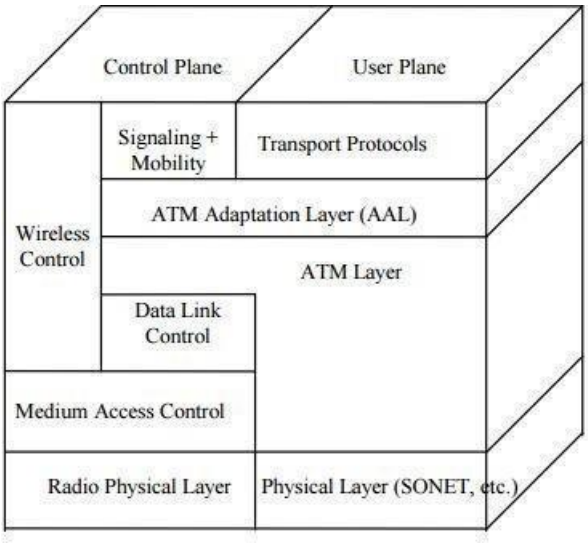


Fig: 8.1. Protocol Architecture for Wireless ATM

WATM protocol architecture is based on integration of radio access and mobility features as "first class" capabilities within the standard ATM protocol stack. The general philosophy for adding mobility and broadband radio access to ATM is outlined in, as in Figure 8.2, showing that a WATM system may be partitioned into two relatively independent parts: a mobile ATM infrastructure and a radio access segment, each of which can be designed and specified separately.

This facilitates standardization by multiple organizations and allows for gradual evolution of radio access technologies without having to modify the core mobile ATM network specification.

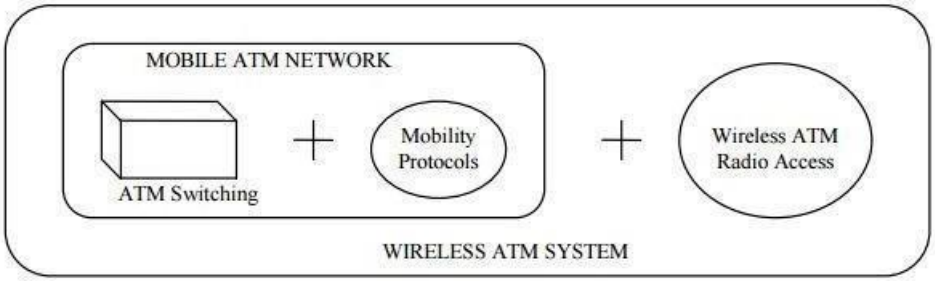


Fig: 8.2. Modular protocol architecture of WATM system

The WATM radio access structure consists of Radio Physical Layer (PHY), Medium Access Control (MAC), Data Link Control (DLC) and wireless control. The WATM DLC layer interfaces each ATM virtual circuit (both service data and

signaling) with the ATM network layer above. An additional wireless control interface is provided within the control plane to deal with radio link specific control functions such as initial registration, resource allocation, and power control. Regular ATM signaling (with mobility extensions) is used for ATM layer connection control functions such as call establishment, QoS control, and handover.

Service data, ATM signaling, and wireless control are multiplexed and scheduled onto the shared radio channel through the MAC layer. The MAC layer in turn, interfaces with the radio transport convergence (RTC) sublayer, which supports required framing and synchronization. The physical media dependent (PMD) sublayer below defines the actual modulation method used to transmit/receive data. Both RTC and PMD are in the radio physical layer at the very low level of the hierarchy.

To support interaction between the radio-dependent access point and radio independent ATM switch, the Access Point Control Protocol (APCP) layer is defined. The main use of the protocol is to reserve and release resources in the access point and assist the access point with setting up connections with terminals. APCP may run on a virtual channel between each access point and the switch. To complete the APCP specification, efforts by the ATM Forum and ETSI are said to be on their way.

DATA LINK CONTROL

The Data Link Control (DLC) protocol is needed to improve the cell error rate caused by the physical wireless channel and the MAC protocol, thus insulating the ATM layer above it from these errors. The noisy wireless channel is expected to suffer from relatively high bit error rates. Thus, a robust DLC layer is required for detecting these transmission bit errors and recovering from them either by bit correction (forward error 12 control, or FEC) or packet retransmission (automatic repeat request, or ARQ) . In addition, the MAC layer is prone to packet loss because of buffer overflow or blocking. Hence, the DLC must also recover from this MAC-level packet loss by retransmission.

Whether employing ARQ or FEC, the bit error and fading impairments of the wireless channel makes it challenging for the candidate DLC protocol to support the standard ATM services (i.e. CBR, real-time VBR, non real-time VBR, ABR and UBR).

Bit errors cause frequent cell retransmission which, in turn, may cause excessive cell access delay. Fluctuations in channel characteristics will create large cell delay variation. This delay variation is a serious problem for real-time applications which require real-time VBR. In addition, signals received on the radio channel are prone to variable fading. This increase the probability of a cell to be received in error at the base station, hence increasing the cell access delay.

The DLC layer exchanges 53-byte ATM cells (as data service units) with the ATM layer. The DLC protocol data unit may be a packet consisting of one or more cells. This packet is then transmitted by the MAC protocol as a single data unit. The use of a multi-cell DLC packet may reduce overhead but will require significant processing to convert between the ATM cell formats to the DLC packet format.

MEDIUM ACCESS CONTROL

The wireless access channel must be shared by multiple users. Bandwidth demands on the channel are generated by active local users, new local users requesting access, and users coming from neighboring base stations via handover. Unlike traditional multi-access data or voice networks which deal with only one type of traffic, WATM networks must handle multimedia traffic with various characteristics and QoS requirements. Thus, the MAC protocol for wireless ATM must be selected to provide QoS levels of these services while maintaining an acceptable radio channel efficiency.

PHYSICAL LAYER

Frequency spectrum in the 5 to 6GHz band has been requested from the respective agencies in the US and Europe, FCC and CEPT, respectively. ETSI has specified 5GHz for short range access at 25 Mbps data rate. An operating frequency at the same data is also under consideration at ETSI for ATM remote access. In the US, similar spectrum allocations are underway at the FCC. A transmit power range of 100-200mW and a bit error of 10 -4 at 99.5% availability have also been specified.

WIRELESS CONTROL

The wireless control sublayer is needed for the allocation of wireless radio

resources to mobile terminals during connection setup and their management during handover. Wireless control messages are exchanged between base stations and mobile terminals and between base stations themselves to handle such functions as terminal registration and authentication, handover, disconnection, and connection state transfer during handover. The content of DLC/MAC buffers at a radio port is an example of connection state which must be transferred to the new radio port after handover. Using the MAC protocol, base stations exchange wireless control messages with mobile terminals using short signaling packets.

HIPERLAN (High Performance Radio Local Area Networks)

HIPERLAN is a Wireless LAN standard. It is a European alternative for the IEEE 802.11 standards (the IEEE is an international organization). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the BRAN project (Broadband Radio Access Networks). The HiperLAN standard family has four different versions.

HiperLAN/1

Planning for the first version of the standard, called HiperLAN/1, started 1991, when planning of 802.11 was already going on. The goal of the HiperLAN was the high data rate, higher than 802.11. The standard was approved in 1996. The functional specification is EN300652, the rest is in ETS300836.

The standard covers the Physical layer and the Media Access Control part of the Data link layer like 802.11. There is a new sublayer called Channel Access and Control sublayer (CAC). This sublayer deals with the access requests to the channels. The accomplishing of the request is dependent on the usage of the channel and the priority of the request.

CAC layer provides hierarchical independence with Elimination-Yield Non-Preemptive Multiple Access mechanism (EY-NPMA). EY-NPMA codes priority choices and other functions into one variable length radio pulse preceding the packet data. EY-NPMA enables thenetwork to function with few collisions even though there would be a large number of users. Multimedia applications work in HiperLAN because of EY-NPMA priority mechanism. MAC layer defines protocols for routing, security and power saving and provides naturally data transfer to the upper layers.

On the physical layer FSK and GMSK modulations are used in HiperLAN/1.

HiperLAN features:

- range 50 m
- slow mobility (1.4 m/s)
- supports asynchronous and synchronous traffic
- Bit rate - 23.2 Mbit/s
- Description- Wireless Ethernet
- Frequency range- 5 GHz[*citation needed*]

HiperLAN does not conflict with microwave and other kitchen appliances, which are on 2.4 GHz. An innovative feature of HIPERLAN 1, which may other wireless networks do not offer, is its ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range. For power conservation, a node may set up a specific wake up pattern. This pattern determines at what time the node is ready to receive, so that at other times, the node can turn off its receiver and save energy. These nodes are called p-savers and need so called p-supporters that contain information about wake up patterns of all the p-savers they are responsible for. A p-supporter only forwards data to a p-saver at the moment p-saver is awake. This action also requires buffering mechanisms for packets on p-supporting forwaders.

HiperLAN/2

HiperLAN/2 functional specification was accomplished February 2000. Version 2 is designed as a fast wireless connection for many kinds of networks. Those are UMTS back bone network, ATM and IP networks. Also it works as a network at home like HiperLAN/1. HiperLAN/2 uses the 5 GHz band and up to 54 Mbit/s data rate. The physical layer of HiperLAN/2 is very similar to IEEE 802.11a wireless local area networks. However, the media access control (the multiple access protocol) is Dynamic TDMA in HiperLAN/2, while CSMA/CA is used in 802.11a/n.

Basic services in HiperLAN/2 are data, sound, and video transmission. The emphasis is in the quality of these services (QoS).The standard covers Physical, Data Link Control and Convergence layers. Convergence layer takes care of service dependent functionality between DLC and Network layer (OSI 3). Convergence sublayers can be used also on the physical layer to connect IP, ATM or UMTS networks. This feature makes HiperLAN/2 suitable for the wireless connection of

various networks.

On the physical layer BPSK, QPSK, 16QAM or 64QAM modulations are used. HiperLAN/2 offers security measures. The data are secured with DES or Triple DES algorithms.Most important worldwide manufacturers of HiperLAN/2 are Alvarion (Israel), Freescale (USA), Panasonic (Japan).

ADHOC NETWORKING

A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" – anywhere, anytime A wireless ad-hoc network, also known as IBSS - Independent Basic Service Set, is a computer network in which the communication links are wireless.

The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts.

PROTOCOL STACK

A major limitation with mobile nodes is that they have high mobility, causing links to be frequently broken and reestablished. Moreover, the bandwidth of a

wireless channel is also limited, and nodes operate on limited battery power, which will eventually be exhausted. Therefore, the design of a mobile ad hoc network is highly challenging, but this technology has high prospects to be able to manage communication protocols of the future. The cross-layer design deviates from the traditional network design approach in which each layer of the stack would be made to operate independently. The modified transmission power will help that node to dynamically vary its propagation range at the physical layer. This is because the propagation distance is always directionally proportional to transmission power. This information is passed from the physical layer to the network layer so that it can take optimal decisions in routing protocols. A major advantage of this protocol is that it allows access of information between physical layer and top layers (MAC and network layer).

ROUTING

Proactive routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

Example: "Optimized Link State Routing Protocol" OLSR

Distance vector routing

As in a fix net nodes maintain routing tables. Distance-vector protocols are based on calculating the direction and distance to any link in a network. "Direction" usually means the next hop address and the exit interface. "Distance" is a measure of the cost to reach a certain node. The least cost route between any two nodes is the route with minimum distance. Each node maintains a vector (table) of minimum distance to every node. The cost of reaching a destination is calculated using various route metrics. RIP uses the hop count of the destination whereas IGRP takes into account other information such as node delay and available bandwidth.

Reactive routing

This type of protocol finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

- High latency time in route finding.
- Excessive flooding can lead to network clogging.
- Example: "Ad hoc On-Demand Distance Vector" (AODV)

Flooding

Is a simple routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on. Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP, and those used in wireless ad hoc networks.

Hybrid routing

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

- Advantage depends on number of other nodes activated.
- Reaction to traffic demand depends on gradient of traffic volume.

Example: "Zone Routing Protocol" (ZRP)

Position-based routing

Position-based routing methods use information on the exact locations of the nodes. This information is obtained for example via a GPS receiver. Based on the exact location the best path between source and destination nodes can be determined. Example: "Location-Aided Routing in mobile ad hoc networks" (LAR)

APPLICATION

The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly. Wireless ad-hoc networks can be further classified by their application:

1. Mobile ad hoc networks (MANETs**):** A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.

2. Vehicular ad hoc networks (VANETs): VANETs are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

3. Smartphone ad hoc networks (SPANs): SPANs leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smartphones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure.

4. Internet-based mobile ad hoc networks (iMANETs) :iMANETs are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. One implementation of this is Persistent System's CloudRelay.

5. Military / Tactical MANETs : Military/Tactical MANETs are used by military units with

PROS AND CONS

Pros:

- No expensive infrastructure must be installed
- Use of unlicensed frequency spectrum
- Quick distribution of information around sender

Cons:

- All network entities may be mobile ⇒ very dynamic topology
- Network functions must have high degree of adaptability
- No central entities ⇒ operation in completely distributed manner

WPAN (WIRELESS PERSONAL AREA NETWORK)

The market for wireless personal area networks is expanding rapidly. As people use more electronic devices at home and in the office, and with the proliferation of peripherals, a clear need for wireless connectivity between these devices has emerged. Examples of the devices that need to be networked are desktop computers, handheld computers, printers, microphones, speakers, pagers, mobile phones, bar code readers, and sensors. Using cables to connect these devices with a PC and with each other can be a difficult task in a stationary location. When you add mobility into the mix, the challenge becomes daunting.

If the setup and administration of a WPAN becomes simple and intuitive in the future for the end user, then the most concrete scenario for WPAN technology is cable replacement. This provides a compelling reason to use WPAN technology, and will open the door for more advanced applications in the future. Here are the main characteristics of a WPAN:

- Short-range communication
- Low power consumption
- Low cost
- Small personal networks
- Communication of devices within a personal space

While providing these features, a WPAN has to achieve two main goals: broad market applicability and device interoperability. It is important that the WPAN specification addresses the leading device categories that require wireless connectivity in a way that is both easy to implement and affordable. The price point to make a technology attractive is $5 (U.S.) or less. At this level, device manufacturers are willing to incorporate a technology into a broad range of devices for both the consumer and business markets. Interoperability is also imperative.

Three wireless standards are leading the way for WPANs:

- IrDA
- Bluetooth
- IEEE 802.15.

Each of these standards enables users to connect a variety of devices without having to buy, carry, or connect cables. They also provide a way to establish ad hoc networks among the abundance of mobile devices on the market. Each of these standards is discussed in the following subsections.

WPAN STANDARDS

Many standards are available for personal area networks. Each standard has strengths and weaknesses, making it suitable for specific application scenarios. In some cases, more than one technology will be able to perform a required task, hence nontechnical factors such as cost and availability will factor into the decision as to which technology is more appropriate. Here we take a look at the leading standards in this space. The information provided will give you a solid understanding about where each standard is being used and for what purposes.

IrDA

IrDA, the acronym for Infrared Data Association, is an international organization that creates and promotes interoperable, low-cost infrared data connection standards. IrDA has a set of protocols to support a broad range of appliances, computing, and communication devices. These protocols are typically aimed at providing high-speed, short-range, line-of-sight, and point-to-point wireless data transfer. IrDA protocols use IrDA DATA as the data delivery mechanism, and IrDA CONTROL as the controlling mechanism.

Chances are that you currently own a device that has support for infrared communication. The Infrared Data Association estimates that more than 300 million IrDA enabled devices have been shipped, making it one of the most pervasive wireless technologies in existence. The original goal of IrDA was to provide a cable replacement technology, much like the other PAN standards. The idea was that two computers could communicate simply by pointing them at each other. For example, to print a document, you would simply point the infrared (IR) port at the printer and be able to send the data. No cables would be required.

Technically, infrared technology is well suited for such tasks. The following are some of infrared's features:

- Communication range of up to 1 meter, although a distance of 2 meters can often be reached.
- A low-power option for communication up to 20 centimeters. This requires 10 times less power than the full-power implementation.
- Bidirectional communication.
- Data transmission from 9600 bps to a maximum speed of 4 Mbps.

In theory, using IR for data transfer is a great idea. Unfortunately, even with such ubiquity it is rarely used for its original intent. This may be due to technical challenges in many early implementations, or more plausibly, to the line-of-sight restriction. For IR to work, the communicating devices have to maintain line of sight. This means that they have to situated within the operating range (typically up to 2 meters apart), point at each other, and have no physical impediments. In most office environments, this limitation is not practical for many peripherals such as printers or scanners. Using infrared to transfer data between two devices is more realistic. Two device users can use infrared to transfer information, such as electronic business cards, between one another. Users with Palm devices call this type of transfer *beaming*, as in, "Can you beam me your contact information?" Beyond user-to-user data transfer, infrared is not commonly used for information transfer, since most users do not use two devices with IR ports. While nearly all portable devices have one, the majority of desktops do not. Once again, this limits the effectiveness of IR as a mass-market data transfer protocol.

That said, there are some areas where infrared is frequently used. The IrDA CONTROL standard allows wireless peripherals such as keyboards, mice, game pads, joysticks, and pointing units to interact wirelessly with a host device, very often a desktop PC or gaming unit. A host device can communicate with up to eight peripherals simultaneously. The data transmission rate for IrDA CONTROL typically reaches a maximum at 75 Kbps, which is easily fast enough for the type of data being transferred by these types of devices.

One of the major advantages of IrDA from a device manufacturer's perspective is cost. IR ports can be incorporated into a device for as low as $1 (U.S.). This is a very low cost for implementing wireless communication into a device compared to

other WPAN standards.

BLUETOOTH

Bluetooth is a standard for enabling wireless communication between mobile computers, mobile phones, and portable handheld devices. Unlike IR, Bluetooth does not require a line of sight between devices to be effective. It is able to communicate through physical barriers, typically with a range of 10 meters, although with power amplifiers, 100 meters is possible. Bluetooth uses the unlicensed 2.4-GHz spectrum for communication, with a peak throughput of 720 Kbps. It is expected that this throughput will increase to around 10 Mbps with future Bluetooth specifications.

The origins of Bluetooth date back to 1994 when Ericsson was researching ways to enable mobile phones to communicate with peripherals. Four years later, in 1998, Ericsson, along with Nokia, Intel, Toshiba, and IBM, formed the Bluetooth Special Interest Group (SIG) to define a specification for small form-factor, low-cost wireless communication. Since then, 3COM, Lucent, Microsoft, and Motorola have joined the Bluetooth SIG as Bluetooth promoters. In addition, well over 2,000 companies have joined the SIG as Bluetooth Adopter/Associate members. This all happened before a single Bluetooth product was commercially available, leading to unprecedented market excitement.

People were excited about the futuristic products that would soon be available, expecting that every device, from portable computers to home appliances, would soon incorporate Bluetooth technology. These devices would then interact with one another, transferring data files, contact information, security credentials, and even perform financial transactions. All of this would happen seamlessly without any technical knowledge required from the user.

Needless to say, the hype once again surpassed the technology. While Bluetooth will indeed enable those scenarios someday, right now it is most effective as a cable replacement technology. Since a line of sight is not required for communication, getting Bluetooth devices to interact with one another is trivial. Bluetooth provides an auto discovery mode, whereby Bluetooth devices will automatically discover other devices that are within range. Once they are detected, they can start communicating. There is some concern that this will overload the 2.4-GHz spectrum

as more Bluetooth devices become available. To address this issue, the Bluetooth specification defines three device modes:

- **Generally discoverable mode.** This allows a Bluetooth device to be detected by any other Bluetooth device within its proximity.
- **Limited discoverable mode.** Only well-defined devices will be able to detect a device in this mode. This mode will be used when a user has many Bluetooth devices and wants them to discover each other automatically.
- **Non discoverable mode.** This makes the device invisible to other devices soit cannot be detected.

When two or more devices connect, they form a piconet, an ad hoc network that can consist of a maximum of eight devices. Every device in a piconet can communicate directly with the other devices. It is also possible to have networks with more than eight devices. In this case, several piconets can be combined together into a scatternet. In a scatternet configuration, not all devices can see each other; only the devices within each piconet are able to communicate. Figure 8.3 helps to illustrate how this works. In this figure there is one scatternet consisting of five piconets; the hands-free mobile phone is a member of three different piconets and is able to communicate directly with the headset, the Bluetooth pen, and the access point, but is not able to communicate directly with the laptops, printer, or fax machine.

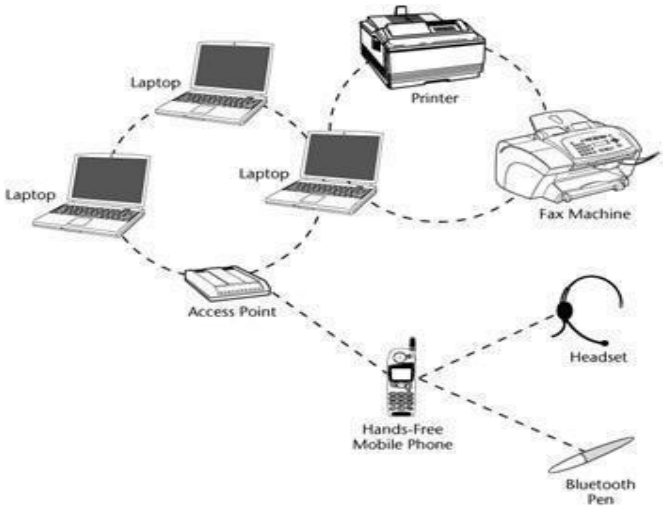


Figure . Bluetooth scatternet with five piconets.

The number of Bluetooth devices on the market is growing every day. It is common for mobile phones, PDAs, laptops, and peripherals to come equipped with Bluetooth chips. This has been made possible by the lowered cost of Bluetooth chipsets [currently around $20 (U.S.), with a targeted range of $5 to $10 (U.S.)] in conjunction with increased market demand. Users are now aware of the many compelling features that Bluetooth offers. The leading ones include:

- Cable replacement
- Mobile device networking
- Global ad hoc networking
- Support for both voice and data communication
- Worldwide vendor and product support

Bluetooth Profiles

In order for Bluetooth to realize true ubiquity, interoperability is a key. Bluetooth devices from different vendors have to be able to communicate seamlessly. In order to promote this level of interoperability, the Bluetooth SIG has defined 13 profiles that device manufacturers can use when implementing their products. These profiles help ensure that Bluetooth products are built on a single foundation, allowing for true interoperability.

The entire second volume of the Bluetooth v1.1 specification is dedicated to profile definitions. Each profile is designed for a specific task. Four profiles are foundation profiles, providing the building blocks upon which other profiles are constructed. The other nine profiles are usage profiles. These describe actual usage cases where Bluetooth technology excels. Bluetooth profiles are not meant to be the definitive way to use Bluetooth technology but rather are aimed at providing standards for implementers to build upon.

Device manufacturers will base their Bluetooth offerings on these profiles, ensuring that all Bluetooth devices will be able to communicate with one another. Detailed summaries of each profile are provided in the Bluetooth profile definition book, which is over 450 pages long. If you are interested in obtaining this information, visit the Bluetooth Web site at www.bluetooth.com.

Bluetooth Security

Because cable replacement is one of Bluetooth's primary uses, the overall goal of Bluetooth security is to make the wireless connection at least as secure as cables would be. The Bluetooth specification defines security at the link level. Application-level security is not specified, leaving the developer to choose the security mechanism that is most appropriate for each particular application.

The Bluetooth specification defines several security measures that can be employed in various situations. Additionally, each profile definition outlines when security should be implemented for particular usage scenarios. Bluetooth communication can be encrypted for over-the-air communication and has built-in device authentication. The level of encryption is user-defined and can have a key size between 8 and 128 bits.

This allows the user to determine what level of security is required. Note that a tradeoff exists between speed and security: Greater key lengths lead to slow communication. For authentication, each Bluetooth device has a unique address so the user can have some faith in the device with which they are communicating. (For an overview of mobile and wireless security, see Chapter 6, "Mobile and Wireless Security.")

IEEE 802.15

802.15 is a specification driven by the Institute of Electrical and Electronics Engineers (IEEE) to develop consensus standards for short-range wireless networks or wireless personal area networks. It has similar goals to Bluetooth in that it looks to address wireless networking of portable and mobile computing devices such as PCs, PDAs, mobile phones, peripherals, and consumer electronics. The 802.15 WPAN Working Group was established in 1999 as part of the Local and Metropolitan Area Networks Standards Committee of the IEEE.

At the time of establishment, the 802.15 WPAN Working Group was aware of the Bluetooth specification and used parts of it as the foundation for the 802.15 standard. The 802.15 WPAN specification is aimed at standardizing the Media Access Control (MAC) and Physical (PHY) layers of Bluetooth, in the attempt to accommodate wider adoption of short-range wireless technology. 802.15 also deals

with issues such as coexistence and interoperability within the networks. To accomplish this goal, four task groups have been established, each working on specific components of the 802.15 specification. They are:

- **802.15 WPAN Task Group 1: WPAN/Bluetooth.** The WPAN Task Group 1 (TG1) has created the WPAN 802.15.1 standard based on the Bluetooth v1.1 specification. To accomplish this, the IEEE licensed technology from the Bluetooth SIG. Specifically, 802.15.1 defines the MAC and PHY specifications for wireless connectivity of devices that are either fixed or portable within the personal computing space. The spec also takes into consideration coexistence requirements with 802.11 wireless local area network (WLAN) devices.
- **802.15 WPAN Task Group 2: Coexistence Mechanisms.** The 802.15 WPAN Task Group 2 (TG2) is developing the recommended practices to facilitate the coexistence of WPAN (802.15) and WLAN (802.11) technologies. Part of this task involves developing a coexistence model to quantify the mutual interference of a WPAN and a WLAN. Once approved, this outcome of TG2's work will become the IEEE 802.15.2 specification.
- **802.15 WPAN Task Group 3: High Rate WPAN.** The 802.15 WPAN Task Group 3 (TG3) is chartered to publish a new standard for high-rate (20 Mbps or higher) WPANs. In addition to high data rates, 802.15.3 also has to provide a means for low-power and low-cost solutions to address the needs of portable consumer electronics, digital imaging, and multimedia applications.
- **802.15 WPAN Task Group 4: Low Rate-Long Battery Life.** The 802.15 WPAN Task Group 4 (TG4) is chartered to establish a low-data-rate (200 Kbps maximum) solution with long battery life (many months to many years) and low complexity. It is intended to operate in an unlicensed international frequency band and is targeted at sensors, interactive toys, smart badges, home automation, and remote controls.

WPAN COMPARISON

Of the three WPAN standards, IrDA, Bluetooth, and 802.15, IrDA has been around the longest, and has the highest market penetration, with more than 300

million enabled devices shipped. At the same time, infrared also is the most limiting, as the range is up to 2 meters, and it requires a line of site between communicating devices. The Bluetooth specification addresses these issues by using unlicensed 2.4-GHz spectrum for communication. This allows for communication through physical barriers, as well as larger ranges, typically up to about 10 meters. Bluetooth has also garnered a lot of industry attention, with more than 2,000 companies joining the Bluetooth SIG. In order to provide further standardization for WPAN technology, the IEEE 802.15 specification was developed. The 802.15 specification uses Bluetooth v1.1 as a foundation for providing standardized short-range wireless communication between portable and mobile computing devices. Table 8.1 provides a summary of the leading WPAN technologies.

STANDARD	FREQUENCY	BANDWIDTH	OPTIMUM OPERATING RANGE	POINTS OF INTEREST
IrDA	875nm wavelength	9600 bps to 4 Mbps. Future of 15 Mbps	1-2 meters (3–6 feet)	Requires line of site for communication.
Bluetooth	2.4 GHz	v1.1: 720 Kbps; v2.0: 10 Mbps	10 meters (30 feet) to 100 meters (300 feet)	Automatic device discovery; communicates through physical barriers.
IEEE 802.15	2.4 GHz	802.15.1: 1 Mbps 802.15.3: 20-plus Mbps	10 meters (30 feet) to 100 meters (300 feet)	Uses Bluetooth as the foundation; coexistence with 802.11 devices.

Table: Comparison of WPAN Technologies

There is no clear leader, as we are still in the early stages of WPAN technology development. Bluetooth has generated the most industry attention so

far, but 802.15 is just as exciting. Since 802.15 is interoperable with both Bluetooth and 802.11, it will have a solid future in the WPAN space. In many ways, IR is not a competing technology to either Bluetooth or 802.15 since it addresses a separate market need. IrDA is included in nearly all mobile devices, providing a quick and easy way for reliable short-range data transfer. With its low implementation costs, many low-end devices will continue to support IrDA, while more advanced devices with more robust wireless needs will implement Bluetooth or 802.15.

Another area of interest is the increasing range that these technologies can address. Initially, Bluetooth was aimed at a personal operating space of 10 meters. Now, with power-amplified Bluetooth access points, the range has extended to 100 meters. 802.15 is in the same situation. The increased range for these technologies blurs the line between wireless personal area networks and wireless local area networks.