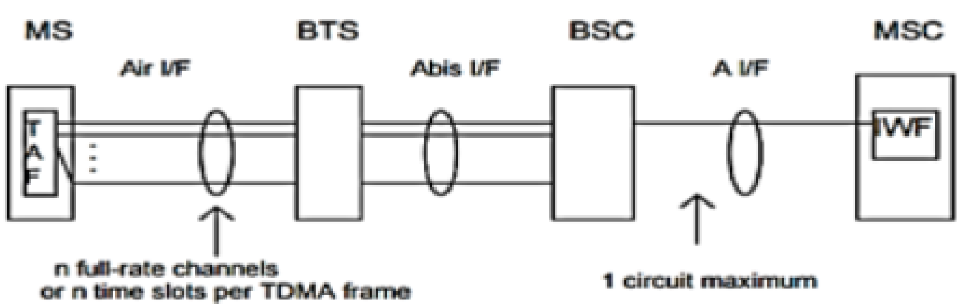
High Speed Circuit Switched Data (HSCSD)

High Speed Circuit Switched Data (HSCSD) is an enhancement in the data rate of circuit switched data in a GSM network. HSCSD uses two techniques to increase the data rate. First, HSCSD makes it possible to use more than one time slot. GSM uses time division multiple access (TDMA). Each radio channel is divided in eight time slots. Each time slot is allocated to a different user. This makes it possible to serve eight customers on one radio channel. HSCSD makes it possible to allocate more than one time slot to a user.

The second technique used by HSCSD is that the error correction can be adapted to the quality of the radio channel. A standard slot can carry 9.6 kbps. HSCSD makes it possible to increase this to 14.4 kbps. The quality of the radio channel must be good enough to do so.

The maximum data rate of a HSCSD configuration with 14.4-kbps channel coding is 115.2 kbps, if all eight time slots are allocated to the same user. In practice, is the number of time slots allocated to a user limited to three, limiting the data rate to 43.2 kbps. Another point is that the core network is based on circuit switched data with data channels of 64 kbps.

The main benefit of HSCSD compared to other data enhancements introduced later is that it is an inexpensive way to implement higher data rates in GSM networks. There modifications to be made are relatively small.



Network Architecture of HSCSD

A new functionality is introduced at the network and MS to provide the functions of combining and splitting the data into separate data streams which will then be transferred via n channels at the radio interface, where n = 1, 2, 3, ... 8. Once split, the data streams shall be carried by the n full rate traffic channels, called HSCSD channels, as if they were independent of each other, for the purpose of data relay and radio interface L1 error control, until to the point in the network where they are combined. However, logically the n full rate traffic channels at the radio interface belong to the same HSCSD configuration, and therefore they shall be controlled as one radio link by the network for the purpose of cellular operations, e.g. handover.

GPRS

General Packet Radio System is also known as **GPRS** is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

Key Features

Following three key features describe wireless packet data

- **The always online feature -** Removes the dial-up process, making applications only one click away.
- **An upgrade to existing systems -** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
- **An integral part of future 3G systems -** GPRS is the packet data core network for 3G systems EDGE and WCDMA.

Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- Open architecture
- Consistent IP services
- Same infrastructure for different air interfaces
- Integrated telephony and Internet infrastructure

- Leverage industry investment in IP
- Service innovation independent of infrastructure

Benefits of GPRS

Higher Data Rate

GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.

Easy Billing

GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent (e.g., when the user reads a Web page).

In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.

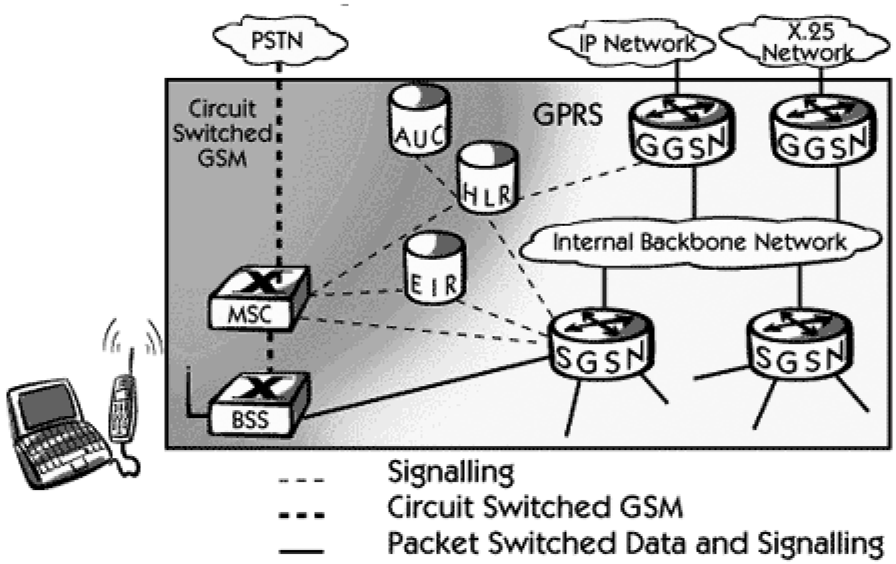
GPRS - Applications

- **Communications -** E-mail, fax, unified messaging and intranet/internet access, etc.
- **Value-added services -** Information services and games, etc.
- **E-commerce -** Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications -** Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- **Vertical applications -** Freight delivery, fleet management and sales-force automation.
- **Advertising -** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

GPRS - Architecture

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is

	required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call

	models and functions introduced by GPRS.

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

GPRS - Quality of Service

The QoS is a vital feature of GPRS services as there are different QoS support requirements for assorted GPRS applications like realtime multimedia, web browsing, and e-mail transfer.

GPRS allows defining QoS profiles using the following parameters :

- Service Precedence
- Reliability
- Delay and
- Throughput

These parameters are described below:

Service Precedence

The preference given to a service when compared to another service is known as **Service Precedence**. This level of priority is classified into three levels called:

- high
- normal
- low

When there is network congestion, the packets of low priority are discarded as compared to high or normal priority packets.

Reliability

This parameter signifies the transmission characteristics required by an application. The reliability classes are defined which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption of packets.

Delay

The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the GI interface to an external packet data network.

This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network. Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

Throughput

The throughput specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the available resources.

The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

Digital Enhanced Cordless Telecommunications(DECT)

DECT stands for Digital Enhanced Cordless Telecommunications. Cordless telephony concept was originally introduced to provide mobility within home or office from main telephone terminal using a device called handset. Handset and main base terminal telephone unit is connected via a analog wireless link.

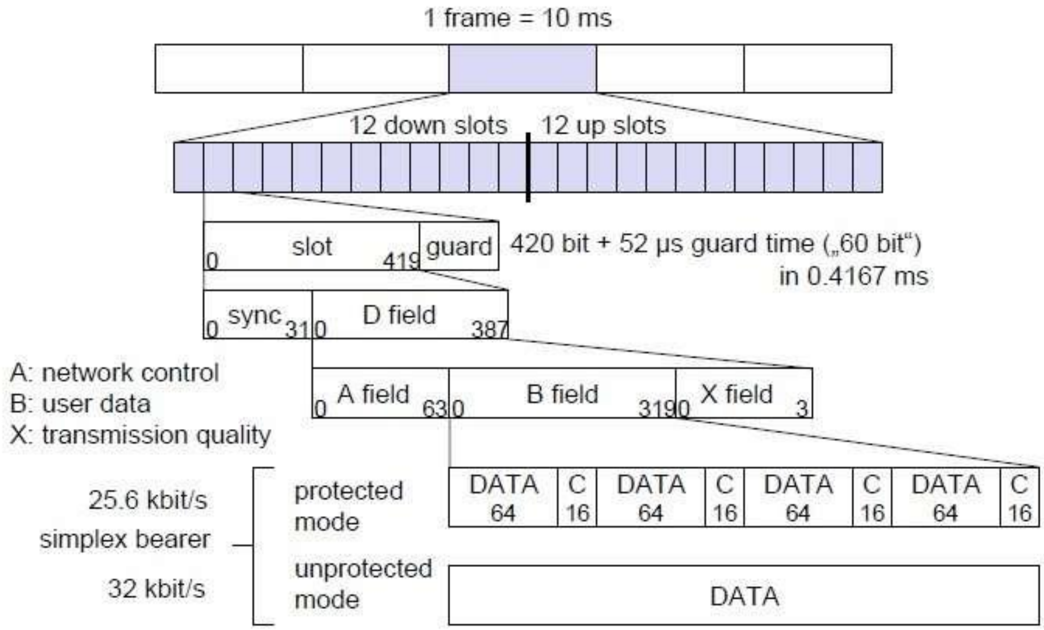
Distance coverage for DECT based system is between about 30-100 meters. It operates at about 1.88GHz to 1.9GHz Radio frequency carrier band, providing a bandwidth of about 20MHz. The access technology for resource allocation here is TDD/TDMA/FDMA. For know more on TDD,TDMA and FDMA refer following links. Data transmission rate of about 1.152 Mbps is achieved.

DECT system specifications or features

Following are the features of DECT system.

Specification or Feature	**DECT system support**
RF Carrier frequency	1.88 to 1.9GHz
Access	TDD/TDMA/FDMA
Cell radius	25 to 100 meters
Channel Spacing	1.728 MHz
No. of carriers	10
No. of channels per carrier	12
Speech codec	ADPCM with 32kbps speech rate
Modulation techniques supported in DECT	Gaussian, FSK, 4PSK, 8PSK, 16-QAM, 64-QAM
Bit rate	32 Kbps
Time slots	2 x 12 (upstream, downstream)
Channel Allocation Method	Dynamic
Traffic density	10000 Erlangs/Km^2

DECT Frame Structure



DECT frame structure

DECT frame duration is about 10ms. It is composed of 24 time slots. 12 time slots are allocated for base terminal to handset direction and 12 logical time slots are allocated for handset to base terminal direction.Each time slot is of duration 0.417ms.

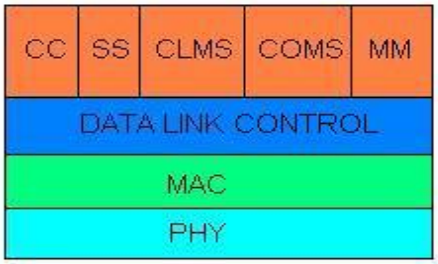
One Time slot = preamble(16bits) + sync(16bits) + A field(64 bits) + B field(320 bits) + X field(4 bits) + Guard bits(60bits)

A filed = Header(8 bits) + Data(40 bits) + CRC(16 bits)

B field= Data(64bits) +CRC(16 bits) +Data + CRC+Data +CRC +Data +CRC

Sync field is used by receiver to synchronize with the start of the frame. A field carries control or management signals. B field carries user data/information. The figure-1 depicts the DECT frame structure as explained.

DECT protocol stack



DECT Protocol Stack-MS/BS

Protocol stack of DECT depicted in figure is used both at Mobile unit and Base Station Unit. It consists of Physical layer, MAC, Data link control layer and different services. Services include CC (Call Control), Supplementary services,C onnection less message service, connection oriented message service and MM(Mobility Management).

DECT MAC layer controls the layer-1(i.e. physical layer). It also provides connection oriented, connectionless and broadcast services to the upper layer in DECT protocol stack. It also provides encryption functionality with the use of Standard cipher protocol.

Push-to-talk (PTT or P2T)

Push-to-talk (PTT or P2T) is a method of telecommunications that normally uses a half duplex system. As the name implies, Push To Talk (PTT) requires the person talking to press a button for the other party at the other end of the line to hear him. Because basic PTT uses half duplex, only one person can talk at a time. Police radios, air traffic controller telecommunications systems, and even some cellular technologies (e.g. iDEN) employ Push To Talk. PTT users communicate bidirectionally but not simultaneously during voice transmission, i.e., callers take turns speaking and listening via push button switching.

Newer PTT systems use voice over Internet Protocol (VoIP) for 3G digital PTT. For example, an air traffic controller communicates with aircraft via one radio frequency, and transmitted voice messages are shared between the controller and each airplane.

The PTT concept has been adopted by cellular systems to offer a service known as Push To Talk over Cellular (PoC), which allows end users to turn their cellphone into a walkie talkie with a much wider range.

With PTT, the caller can simply select a contact or a group/ channel, press the PTT button, speak, and then release the PTT button to get his voice message delivered instantly. There is no need to go through the traditional lengthy voice-call process of dialing, network switching and routing, and waiting for the other party to answer. High-performance PTT solutions can deliver sub-second call set-up and latency to ensure instantaneous communication.

A PTT call is a barge call, allowing the recipient to hear incoming voice right away, through the PTT device's speaker or an accessory in a hands-free, eyes-free manner, without any action. A barge call eliminates the need for the recipient to press the answering button in order to answer a call and hear the caller's voice. To a construction worker, for example, hearing messages burst out of a speaker on their handset is much more convenient than putting down tools and removing gloves to answer a standard phone call. To respond, the recipient can simply push the PTT button and instantly deliver a voice message back.

An addition to one-to-one communication, PTT enables an instant meeting through a group call, which is very useful for team collaboration or delivery of an urgent voice message to multiple people simultaneously. With a PTT group call, there is no need for users to set up and dial into a conference bridge or add additional parties to a phone call one by one manually. Advanced PTT solutions support calls made to a pre-defined group or an ad hoc group that can be created on the fly.

A typical PTT call lasts less than a minute, much shorter than a regular voice call, because it eliminates the typical greetings and ending protocol used in regular phone conversations. PTT calling allows users to say no more than necessary, focus on getting the job done, and improve productivity

Mobile Internet Protocol (or Mobile IP)

This is an **IETF (Internet Engineering Task Force)** standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

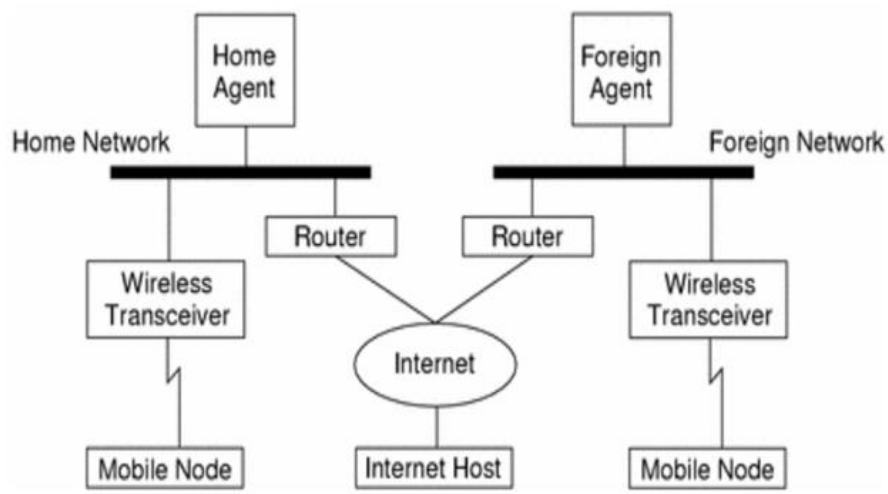


Fig: Mobile IP topology

The following case shows how a datagram moves from one point to another within the Mobile IP framework.

- First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
- If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram.
- If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent.
- The foreign agent (FA) delivers the datagram to the mobile node.

- Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the MN use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address (COA) is used only for communication with mobility agents and is never seen by the Internet host.

Components of Mobile IP

The mobile IP has following three components as follows:

1. Mobile Node (MN)

The mobile node is an end system or device such as a cell phone, PDA (Personal Digital assistant), or laptop whose software enables network roaming capabilities.

2. Home Agent (HA)

The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

- Home agent can be implemented on a **router** that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway.
- If changing the router's software is not possible, the home agent could also be implemented on an **arbitrary node** in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

3. Foreign Agent (FA)

The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.

Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

In short, FA is a router that may function as the point of attachment for the mobile node when it roams to a foreign network delivers packets from the home agent to the mobile node.

4. Care of Address (COA)

The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel. To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.

There are two different possibilities for the location of the care of address:

1. **Foreign Agent COA:** The COA could be located at the foreign agent, i.e. the COA is an IP address of the foreign agent. The foreign agent is the tunnel endpoint and forwards packets to the MN. Many MN using the FA can share this COA as common COA.
2. **Co-located COA:** The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

5. Correspondent Node (CN)

At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node.

6. Home Network

The home network is the subset the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

7. Foreign network

The foreign network is the current subset the MN visits and which is not the home network.

Process of Mobile IP

The mobile IP process has following three main phases, which are:

1. Agent Discovery

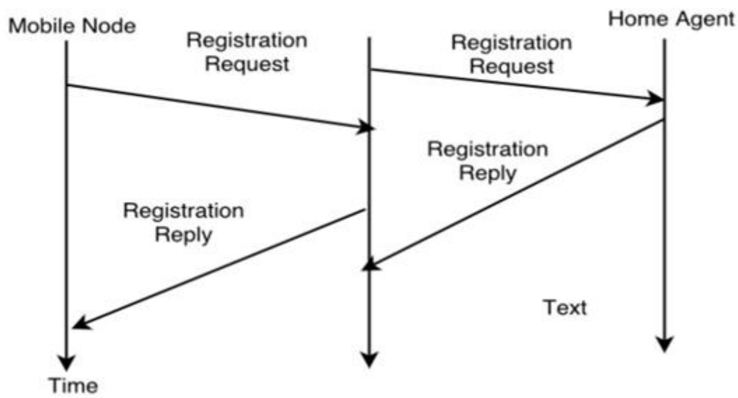
During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

- **Agent advertisement:** For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
- **Agent solicitation:** If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations. These solicitations are again bases on RFC 1256 for router solicitations.

2. Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.



Registration can be done in two ways depending on the location of the COA.

- **If the COA is at the FA**, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a **mobility binding** containing the mobile node's home IP address and the current COA.

Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

- **If the COA is co-located**, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

3. Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

Tunneling is also known as "**port forwarding**" is the transmission and data intended for use only within a private, usually corporate network through a public network.