4.2 LIMITATIONS OF TRADITIONAL TELEPHONE NETWORK

Nowadays small offices and homes have Internet access (Figure 4.1) based on the public switch telephone network (PSTN). It simply requires the subscriber to take a telephone line, a modem and a computer to set up a connection. The subscriber is to dial an Internet Service Provider (ISP). The ISP owns a number of telephone lines and modems and connects a user to a router. The router finally allows access to the Internet. The dial-up connection is easy to install. However, such an Internet system realized with traditional telephone network has the following limitations:

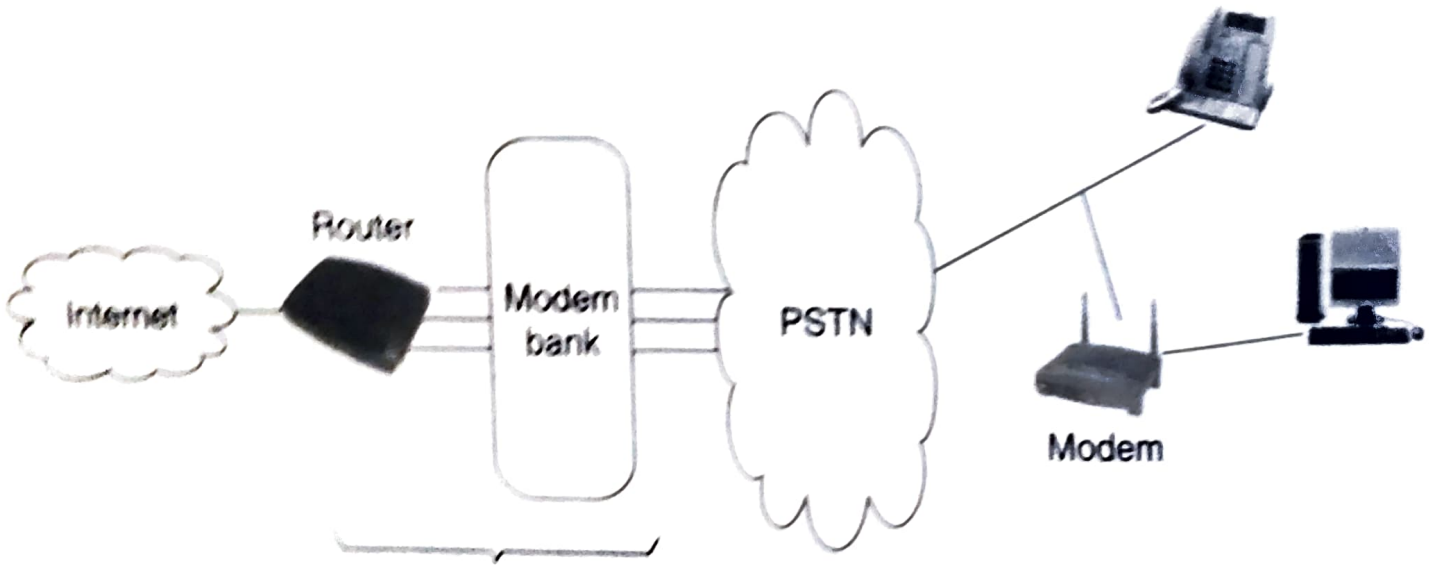


Figure 4.1 Internet access with PSTN.

(i) For every subscriber, the telephone network is designed to handle a limited number of traffic adequate for telephony. On the other hand, Internet sessions desired by a subscriber are usually of long duration. Therefore, for a reasonable number of Internet subscribers, the telecom network cannot be suitable in terms of traffic load handling capacity, and that results in severe congestion.

(ii) The analog modem to modem link between the subscriber and the ISP in such a set-up is unreliable. One does get a 33.6 kbps

connectivity sometimes, but connection could go down to 9.6 kbps and even 4.8 kbps at times. Connection may be dropped as well.

(iii) The volume of services provided by a dial-up Internet connection system is limited by the number of available telephone lines and modems in ISP. An ISP with N telephone lines, N modems and an N port router can serve at most N subscribers at a time.

An alternative solution is to implement totally shared packet-switched Internet access. In Internet access, packets are transmitted in bursts. During an Internet session, the communication between a subscriber and the service provider remains idle for most of the time. A circuit-switched connection on telephone network cannot utilize the idle slots; it rather occupies resources throughout the session. This causes congestion in the network. In circuit-switched connection a number of new technologies such as ISDN and xDSL are introduced in an attempt to tune the wired technologies to respond with the need of reliable, high-speed access by users connected in fixed lines. However, the data access has been made more realistic providing packet-switched access.

As the local loop is the separate physical line to each subscriber, packet access on such non-sharable resource cannot have additional advantages. More than one subscriber is not allowed to use this resource. Therefore, to get the advantage of packet-switched access, Internet data is separated at a point (P) closest to the subscriber where data from multiple subscribers can be multiplexed. The connection from a subscriber to P is made by shared medium access that is WLL.

4.3 APPLICATION DOMAIN

The WLL is quicker, less expensive and easier to install compared to a conventional landline system. This creates enormous changes in

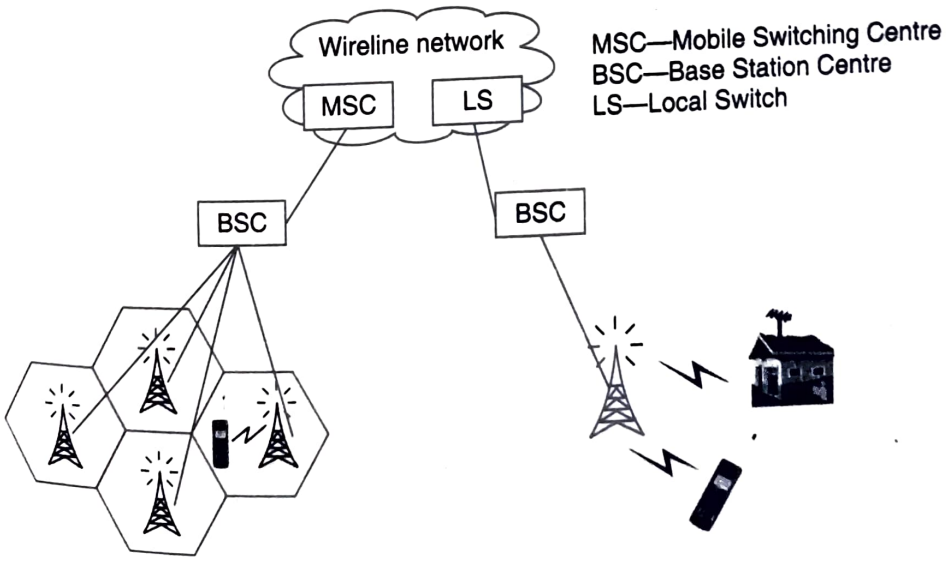


Figure 4.2 Cellular vs WLL system.

communication services in developing countries. It is very much effective where installation of landline system is not even feasible. However, for a developed country, WLL may be used in cordless phone as an extension of house/office telephone or private branch exchange (PBX). This adds convenience in the use of telephonic system (Refer to Figure 4.2).

The WLL can be installed and dismantled quickly (in weeks) and easily, and is ideal also for a temporary solution, instead of waiting for the deployment of copper or fibre cables. Different WLL solutions are introduced to satisfy different needs in terms of service, coverage, frequency spectrum, subscribers' density, etc.

4.3.1 Mobile Cellular System vs WLL System

Although there are similarities between a WLL system and the mobile cellular system as both of these support mobile telephony, the basic difference lies in the planning and design considerations. A WLL system is considered for low-mobility users and designed either as large fixed radio access networks or as the clusters of micro cellular networks. The voice quality in a WLL is comparable with that of a landline telephone system. On the contrary, the cellular system aims at a large coverage area around a base station and can accommodate subscribers with high mobility. However, the voice quality is sacrificed.

The following table notes the expectations from a mobile cellular system and the WLL:

Parameter	*Expectations from*	
	Mobile cellular system	*WLL system*
Frequency bands	regulated dedicated bands	no dedicated bands
Radio interfaces	conform to regional and international standard	not standardized
Coverage	wide/universal	limited
Voice quality	a modest voice quality is acceptable	as good as wired phone
Traffic/subscriber	not very high as the user is unlikely to make long calls	high as voice quality is good
Data service	low bit-rate data may be acceptable	medium rate Internet access is a must
Mobility	full mobility including roaming	limited mobility
Cost	air-time charges for some services is acceptable; higher cost to support mobility/roaming	air-time charges are not acceptable; cost should be less than even wired telephone

4.3.2 Merits of Adopting WLL

The WLL systems can be deployed in weeks, and hence it is far easier to implement than the systems designed with copper wire. Faster deployment of WLL leads to realization of revenues sooner as well as fast recovery of the deployment cost. Further, the deployment of WLL involves considerably less costly construction than the laying of copper lines in conventional telephone system. The operations and maintenance in WLL are also easy. The average instances of maintenance per subscriber per year are 3 to 4 times shorter than their wireline implementations.

In WLL, the connection time to accommodate a new subscriber is much lower than that in a wireline or cellular system. This gives satisfaction to a subscriber and significantly reduces the overall cost for each customer.

Moreover, the use of advanced digital radio technology enables the WLL to provide variety of high bandwidth data, multimedia and voice services.

In a wireline telephone network, any form of extension targeting new subscribers in an area/domain demands considerable additional investments. However, in WLL once the WLL infrastructure-network of base stations and interface to the telephone network are in place, adding a new connection (subscriber) involves almost no additional investment. Further, most of the WLL systems are designed to be modular and scalable that allow a network operator to keep pace with the incremental demand, simultaneously ensuring a minimum loss due to investment associated with the underutilized network resources. So a WLL system is very much flexible to meet even the uncertain rates of growth.

In a word, apart from fast deployment and providing high bandwidth services, various costs associated with the WLL such as construction, maintenance and network extension costs are comparatively lower than wireline and cellular systems.

The systems described so far can provide Internet access as long as the portable device is within a network coverage area. The moment it visits another network, it gets disconnected and the session is terminated. However, people on move need to communicate using only its permanent IP address through Internet even after the change in its current point of attachment to the Internet. Hence the support of mobility in the Internet access is a must. Mobile IP gives a solution allowing people to access Internet on the move without a change in IP addresses.

Mobile IP is an open standard defined by the Internet Engineering Task Force (IETF). It allows users to keep the same IP address, stay connected and maintain ongoing applications while roaming between IP networks. The main objective of this technology is to enable users to keep the same IP address while travelling to a different network (may be operated by a different operator) simultaneously ensuring that a roaming individual could continue communication without sessions or connections being dropped. As it is a network layer solution, it is completely independent of the medium on which it runs. For example, it allows a Laptop to disconnect from a wired Ethernet and switch to a WLAN interface without experiencing a disruption in network service.

Whenever a mobile node moves from one network to the other, its network prefix changes and the node cannot be traced by its fixed IP address. The solution of allocating a new IP address, as soon as the node switches to a different network, is not so efficient. It forces the node to terminate any ongoing communications at the old link and then restart them at the new link. The following section describes a solution for the said problem using mobile-IP.

6.4.1 Architecture

Figure 6.11 shows a typical Mobile-IP architecture. The components of Mobile IP are:

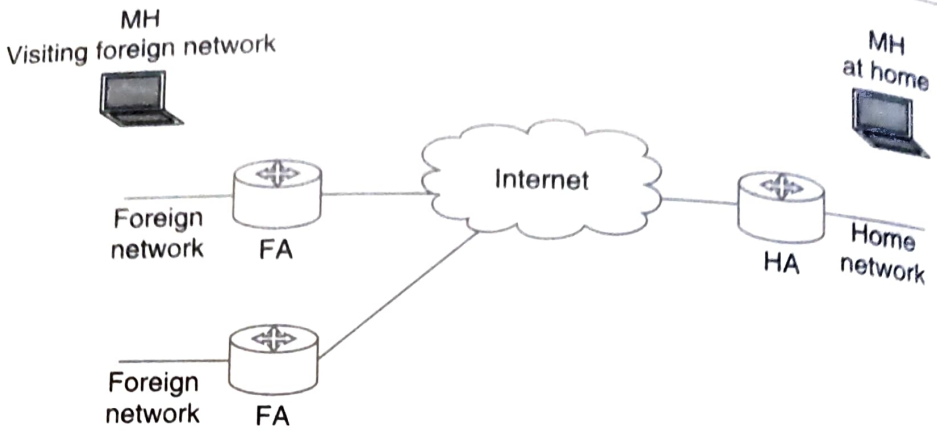


Figure 6.11 Mobile-IP architecture.

Mobile Host (MH): A node that can change its point of attachment to the Internet from one link to another while maintaining any ongoing communications and using only its permanent IP address.

Home Agent (HA): Home Agent is a router with an interface to the MH's home link. It serves as the anchor point for communication with the Mobile Host. Home Agent keeps track of MH's movement maintaining a mobility-binding table described at the end of this section.

Foreign Agent (FA): Foreign Agent is also a router but located in the MH's foreign link. It maintains a visitor list that gives a mapping indicating the location where the data destined for the visiting node (mobile host) can be forwarded.

Both HA and FA periodically advertise their presence through the agent advertisement messages.

Home address: The home address of a mobile host is a permanent IP address assigned to the host. It does not change as the mobile node moves from link to link.

Care-of-address: A care-of-address is the IP address associated with a mobile host visiting a foreign link. It generally changes each time the mobile host moves from one foreign link to another. There are two ways for implementing the concept of care-of-address – the foreign agent care-of-address and collocated care-of-address. The foreign agent care-of-address means the IP address of an FA that has an interface with the foreign link the MH is currently visiting. It can be simultaneously shared by many MHs. On the other hand, the collocated care-of-address is an IP address temporarily allocated to an interface of the MH. When no FA is available on a foreign link, the collocated care-of-address is used. A collocated care-of-address is, therefore, used by only one MH at a time. In a word, the care-of-address is either an address of an FA or an address assigned temporarily to an interface of the MH.

The mobility-binding table in HA contains MH_IP (home address of the MH), c_o_addr (care-of-address of MH) and life_time (a parameter to

be discussed later). It maintains an association/mapping between the home/permanent IP address and the care-of-address for routing MH-bound packets. The visitor list in FA contains MH_IP, HA_IP (IP address of HA) and life_time.

6.4.2 How does Mobile IP Work?

The whole process of providing Mobile IP environment is based on three sub-processes, namely Agent discovery, Registration and tunnelling.

Agent discovery

Agent discovery consists of two types of messages—agent advertisement and agent solicitation. To support delivering packets to an MH, the HA and FA periodically broadcast their presence by agent advertisement. All the nodes on the link receive the broadcast. This enables an MH to identify whether it is in home network or it has moved away. If the MH realizes that it is visiting a network other than its home network, it collects care-of-address from agent advertisements.

On the other hand, agent solicitation is sent by an MH which requires agent advertisement instantly and cannot wait for the next periodic agent advertisement. Agent advertisement and agent solicitation are identical to router advertisement and router solicitation of ICMP[3] (Internet Control Message Protocol) Router Discovery Messages. Mobile IP extends ICMP router discovery message to implement agent discovery. In spite of periodic agent advertisements, if a mobile host needs agent information instantly, it can use an ICMP router solicitation message. Any agent receiving this message will then issue an agent advertisement. The event of getting instant agent advertisement is called agent solicitation.

The parameter life_time (lifetime) present in the mobility-binding table and in the visitor list indicates maximum allowable time period between two consecutive advertisements either by an HA or by an FA. Listening the parameter value from an advertisement, an MH realizes how frequently an agent broadcasts its advertisements. In reality during broadcasting, the advertisements may be lost due to the error-prone characteristic of wireless medium. So HA and FA broadcast well before the time period lapses. If an MH is registered with an FA, and fails to listen an agent advertisement within the stipulated lifetime, the MH can realize that either it has moved to a new FA or the desired link is not functioning. In this case, the MH tries to listen advertisement further to take necessary action. If no such advertisement is listened by the MH, it opts for agent solicitation.

[3] ICMP is one of the core protocols of the Internet Protocol suite. ICMP Router Discovery is used by nodes in Internet to detect router running ICMP router discovery.

If for some reasons FAs are busy or no FA is available, the MH itself acts as its own FA by using collocated care-of-address. It can use DHCP[4] (Dynamic Host Configuration Protocol) to contact a service provider in the present network and then obtains the collocated care-of-address. The node sends a request to the DHCP server to lease an address for some period of time.

Registration

The primary purpose of registration for a mobile host is to inform its home agent the current care-of-address collected in the agent discovery phase. Immediately after getting care-of-address, the MH prepares registration request. The registration request includes the MH_IP (IP address of the MH), HA_IP (IP address of its Home Agent) and the care-of-address the MH learns from the FA. The MH sends the registration request to its home agent through foreign agent. The FA checks the validity of the registration request. If the request is valid it forwards the request to its HA. Once the HA knows the care-of-address, it can send packets to the care-of-address to deliver the same to the mobile host.

If the MH detects that it has moved to another network, it sends a new registration request through the new FA. In this case, the mobility-binding table of the HA is updated replacing the MH's old care-of-address. Accordingly the HA forwards the data packets to the new care-of-address.

When the MH returns to its home network, it no more requires mobility status and hence sends a deregistration request to the HA to remove care-of-addresses so far assigned to it.

Tunnelling

As soon as a data packet (datagram[5]) destined to an MH reaches the MH's home network, the HA intercepts the packet. It consults the mobility-binding table to know the care-of-address of the MH. Now the HA constructs a new IP datagram[6] setting the care-of-address as destination IP address. The original IP datagram is put or encapsulated in the payload portion of the newly constructed IP datagram. The use of an outer IP datagram with

---

[4] The DHCP is an automatic IP address assigning mechanism. This protocol is used by networked nodes to acquire the essential parameters such as IP addresses, subnet masks, etc. to join and get access of an Internet Protocol (IP) network. The protocol basically automates the joining and accessing of IP network by a node by assigning the said parameters.

[5] A datagram is a formatted unit of data carried by a computer network to exchange data between two network nodes.

[6] An IP [illegible] between two

different destination IP address is known as tunnelling. This outer IP datagram is routed to the FA. The FA in turns decapsulates the same, that is, removes the outer datagram and finds out the MH_IP from the original datagram. The FA then consults the visitor list to find out any such MH_IP in the list. If it is found, the FA delivers the same to the MH. In a word, the HA intercepts IP packets destined to the MH and forwards the same to the MH through the FA. The encapsulation process creates a logical construct called a tunnel between the device that encapsulates and the one that decapsulates. Figure 6.12 shows the encapsulated packet before tunnelling and decapsulated packet at the end of tunnel. The original source and final destination address fields are set to the entry-point and the exit-point of the tunnel respectively.

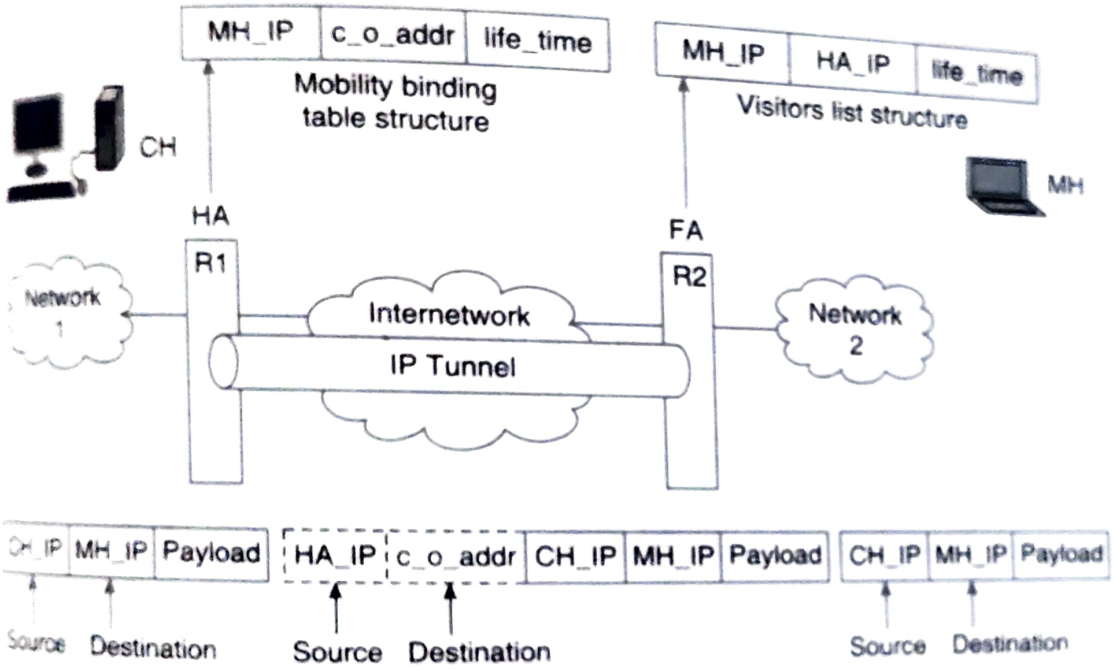


Figure 6.12 Tunnelling.

The tunnelling in Figure 6.12 considers the Correspondent Host (CH) attached to the Network 1 is sending packet {(IP source = CH_IP, IP destination = MH_IP) (IP Payload)} to the MH currently visiting Network 2. The HA intercepts the packet, encapsulates it adding header (IP source = HA_IP, IP Dest = c_o_addr). The c_o_addr is the IP address of FA. Once the packet reaches FA, it decapsulates the packet, i.e. removes the added header and delivers it to the MH.

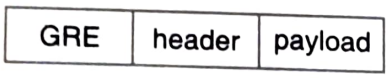
An MH sends packets using its home IP address (HA_IP) effectively maintaining the appearance that it is always in its home network. It forwards packets to the FA that routes those to the correspondent node, the final destination, through HA. In such case, the packets flow through the tunnel established from FA to HA. This is called reverse tunnel.

The default encapsulation process used in mobile-IP is called 'IP encapsulation within IP' or IP-in-IP. In this method an extra IP header is put on the top of the packet to be forwarded. In other words, the original packet (inner packet) to be delivered is encapsulated within the payload

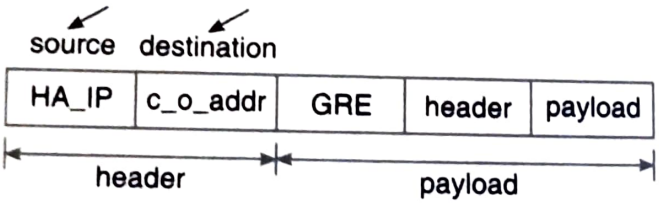
portion of another packet (outer packet). The IP-in-IP encapsulation makes the tunnel appear as a single virtual link to an original packet.

Mobile IP supports two optional encapsulation processes—Minimal Encapsulation and Generic Routing Encapsulation (GRE). Minimum encapsulation also supports only IP network layer protocols. In this encapsulation, some of the redundant fields are discarded from IP-in-IP encapsulation, resulting in less overhead. However, minimal encapsulation works only when an original packet is not fragmented.

In spite of the fact that IP protocols are used as default for mobile IP, many user communities prefer different protocol suites such as Novell Netware or Apple Talk in their organizational network. GRE supports multi-protocol encapsulation. In addition to IP-in-IP encapsulation, the GRE allows encapsulation of packet of one protocol suite into the payload part of a packet of a different protocol suite. For example, consider Network 1 in Figure 6.12 runs on TCP/IP protocol suite where Network 2 runs on Novel Netware. The MH's home network is the Network 1 and visiting network is Network 2. If a packet from Network 2, destined to the MH (MH_IP) arrives at the Network 1, the datagram as shown in Figure 6.13(a) is constructed. It contains a GRE header followed by the original datagram (header, payload) of Novel Netware protocol suite. This will be considered as payload of the outer datagram to be formed. The outer datagram is shown in Figure 6.13(b).



(a) Datagram (Novel Netware protocol suite) preceded by GRE header



(b) Datagram (IP protocol suite) encapsulating datagram in (a)

Figure 6.13 GRE encapsulation.

If tunnel is not set-up perfectly, there is a possibility of formation of a routing-loop[7]. The problem of routing-loop is very serious here as each time the packet reenters the same tunnel, one additional encapsulation occurs causing the packet to grow in size and flow within the network indefinitely. GRE has explicit mechanism for preventing such problem.

[7] The routing loop is a problem arises in network domain. If a link between any two nodes fail and the rest of the nodes in the network are not updated immediately about this failure, the other nodes still try to send packet through the failed link; the node associated with the failed link returns the packet to the sender node intending that the sender would send it via other node and this process will continue making a loop called routing loop.