options are being used. One example of this use is the mobile IP protocol extension when an agent advertises (Section 5.3.1.1).

5.1.2 Mobile Internet Protocol

The mobile Internet protocol (mobile IP) is a protocol developed to allow internetwork mobility for wireless nodes without them having to change their IP addresses. Mobile IP is defined by the Internet Engineering Task Force (IETF) and is described in the IETF RFC 3344. The following subsections explain the requirements for the evolution of the new mobile IP protocol from the existing IP protocol and describe the working of the mobile IP protocol.

5.1.2.1 Evolution of Mobile IP

When a user computer (for example, a laptop) moves from one place to another, it is assigned a new IP address at the new hosting subnet to which the service-providing router provides connectivity to the Internet (Section 5.7). A mobile node can be considered to be a computer on the move from one area to another. The reasons for the use of a new mobile IP protocol instead of the existing IP protocol by the MNs are as follows:

Need for Enhancing IP Network Capacity Use of the existing IP protocol by a large number of MNs will lead to a decrease in the network throughput unless the capacity of existing IP network is scaled up, to cater to such large number of users.

Need for Upgrading Capacity of Routers and Data Link and Physical Layers of IP Networks For mobile nodes to move from one place to another while using the existing IP protocol, new protocols are required at lower layers—the data-link and physical layers. For example, the IP network protocols, as discussed in Section 5.1.1, support 48-bit MAC addresses. But when the number of MNs is large, then other interfaces and lower level protocols have to be added to the existing IP infrastructure. When an MN moves from one service area to another then the use of the existing IP protocol and assignments of new IP addresses is impractical due to the following reasons.

Security needs In Chapter 3, we discussed how a TMSI (temporary mobile subscriber identity) is assigned to a mobile node in a GSM system, when it moves to a new location area. The TMSI is used in place of the IMSI during the connection to secure the identity of the MN from eavesdroppers over the air. The mobility of the called MN is thus hidden from the calling MN. When a new IP address is allocated at the new hosting subnet of the existing IP-based infrastructure, the identity of the mobile node is not hidden from another host. The MN is, thus, exposed and lacks security when using the existing IP protocol.

Need for non-transparency from higher layers The transport layer establishes a connection between a given port at a given IP address (called socket) with another port at another IP address. The connection, established by the transport layers between the sockets, is broken as soon as the new address is assigned. The problems faced in the use of this technique are—(a) re-establishment of the connection takes time which means loss of data during that interval, (b) the re-establishment process must share the same network and the given transmission rate, and (c) any movement of the MN is transparent to the TCP and to L_7 in case the TCP layer re-establishes the connection when the IP protocol is followed by the MN. There is, therefore, a need for non-transparency of the MN to distant ports.

Another problem with the use of IP protocol is that of non-transparency in the routing table. Let us suppose that a distant router is sending data packets for an IP address, presently assigned to a mobile terminal using another router. When the terminal moves from one service area to another, the routing tables on the route need to be updated. Unless this is done, the packets will not reach their new destination. In this case, (a) the reconfiguration messages for updating the routing tables must share the same network and the given transmission rate, (b) re-establishment of the connection takes time and this means loss of data during that interval, and (c) any movement on the part of the MN is transparent and thus, not secure from the distant hosts on the network of distant routers. There is a need for non-transparency of the MN to the distant ports.

5.1.2.2 Working of Mobile IP

Figure 5.2 shows the architecture for a mobile IP network. It shows how a mobile IP network employs home and foreign agents. A mobile node (MN) connects to a mobile services switching centre (MSC) in the radio subsystem (Section 3.1.2.1). An MN can access Internet services using the mobile IP protocol. The MN can change its service router when visiting another location (which is serviced by a different router). A router has a home agent (HA) for a set of home networked MNs as well as a foreign agent (FA) for the visiting MNs. An agent is software employed at a router or the host serviced by a router. The same software can function as both the HA and the FA at different instants of time. An MN can also have software

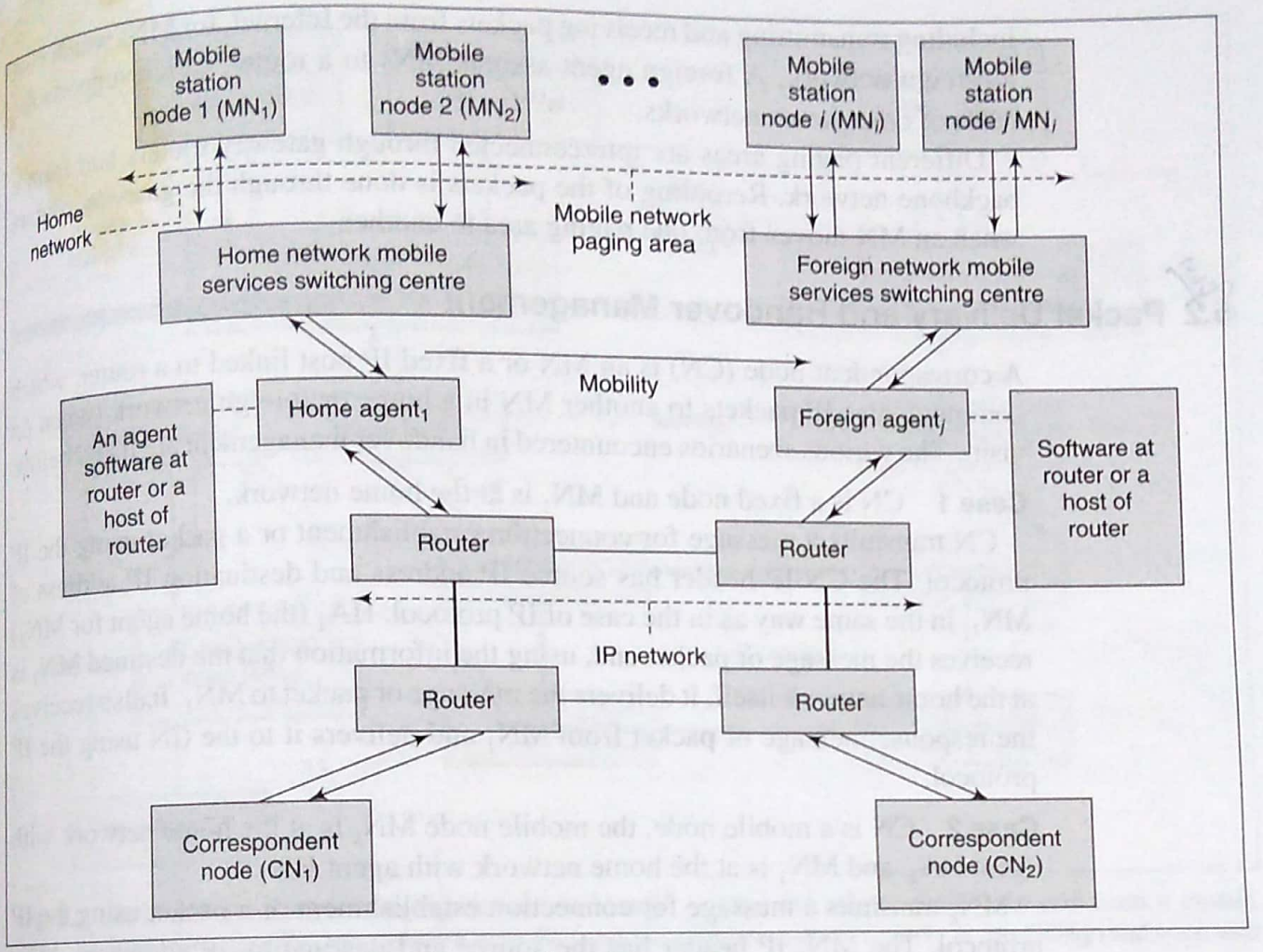

Fig. 5.2 Mobile IP network employing home and foreign agents

which functions as an FA instead of the FA at the router. The HA and the FA play a location management role similar to that of the HLR and the VLR in a GSM system, respectively.

A switching centre has a home agent (HA) in a home network. The home agent provides services to an MN at the registered home network. These services include transmitting and receiving packets from the Internet. A home agent assigns MNs to routers which support the MNs. A home network is a mobile radio subsystem's network within an area known as paging area. The home network is like a subnet. Similar to a subnet, which has a number of IP hosts, a home network has the MNs. The paging area is the area in which the MNs of home as well as foreign networks can be approached through a single MSC or a set of MSCs. Routing of packets through the routers is performed when an MN moves within one paging area. A switching centre has an FA for a foreign network of visiting MNs. Foreign network means another mobile radio subsystem network, which the MNs of home network visit, within the paging area. Foreign agent provides IP address and services,

including transmitting and receiving packets from the Internet, for MNs which visit a foreign network. A foreign agent assigns MNs to a router, which supports the MNs of other home networks.

Different paging areas are interconnected through gateway routers and form a backbone network. Rerouting of the packets is done through the gateway routers when an MN moves from one paging area to another.

5.2 Packet Delivery and Handover Management

A correspondent node (CN) is an MN or a fixed IP host linked to a router, which communicates IP packets to another MN in a home or foreign network (when on visit). The various scenarios encountered in handover management are listed below.

Case 1 CN is a fixed node and MN_1 is at the home network.

CN transmits a message for connection establishment or a packet using the IP protocol. The CN IP header has source IP address and destination IP address of MN_1, in the same way as in the case of IP protocol. HA_1 (the home agent for MN_1) receives the message or packet and, using the information that the destined MN_1 is at the home network itself, it delivers the message or packet to MN_1. It also receives the response message or packet from MN_1 and delivers it to the CN using the IP protocol.

Case 2 CN is a mobile node, the mobile node MN_k is at the home network with agent HA_k, and MN_1 is at the home network with agent HA_1.

MN_k transmits a message for connection establishment or a packet using the IP protocol. The MN_k IP header has the source and destination IP addresses. MN_1 sends the message through HA_k. HA_k uses the same IP address of MN_k as in the IP header and forwards the packet on the Internet in the same way as in the case of the IP protocol and as in case 1. The packet is delivered to HA_1 and then to MN_1. MN_1 transmits back to MN_k like in case 1. Now, HA_k and HA_1 deliver the packets from one end to another and vice versa, instead of the CN directly performing the role of HA_k as in case 1. Both HA_k and HA_1 deliver by just forwarding the packets to their respective MNs using the IP protocol.

The cases when the destined or correspondent MN is visiting a foreign network, and the packets are handed over by the home agent to the foreign agent by tunnelling and encapsulation using the mobile IP protocol, are listed below.

Case 3 CN is a fixed node and MN_1 is at a foreign network.

CN transmits a message for connection establishment or a packet using the IP protocol. The CN IP header has source IP address and destination (MN_1) IP address, in the same way as in case of the IP protocol and as in case 1. HA_1 receives the packets and has the information that the destined mobile node MN_1 is not at the home network and is visiting a foreign network and is reachable via a foreign agent

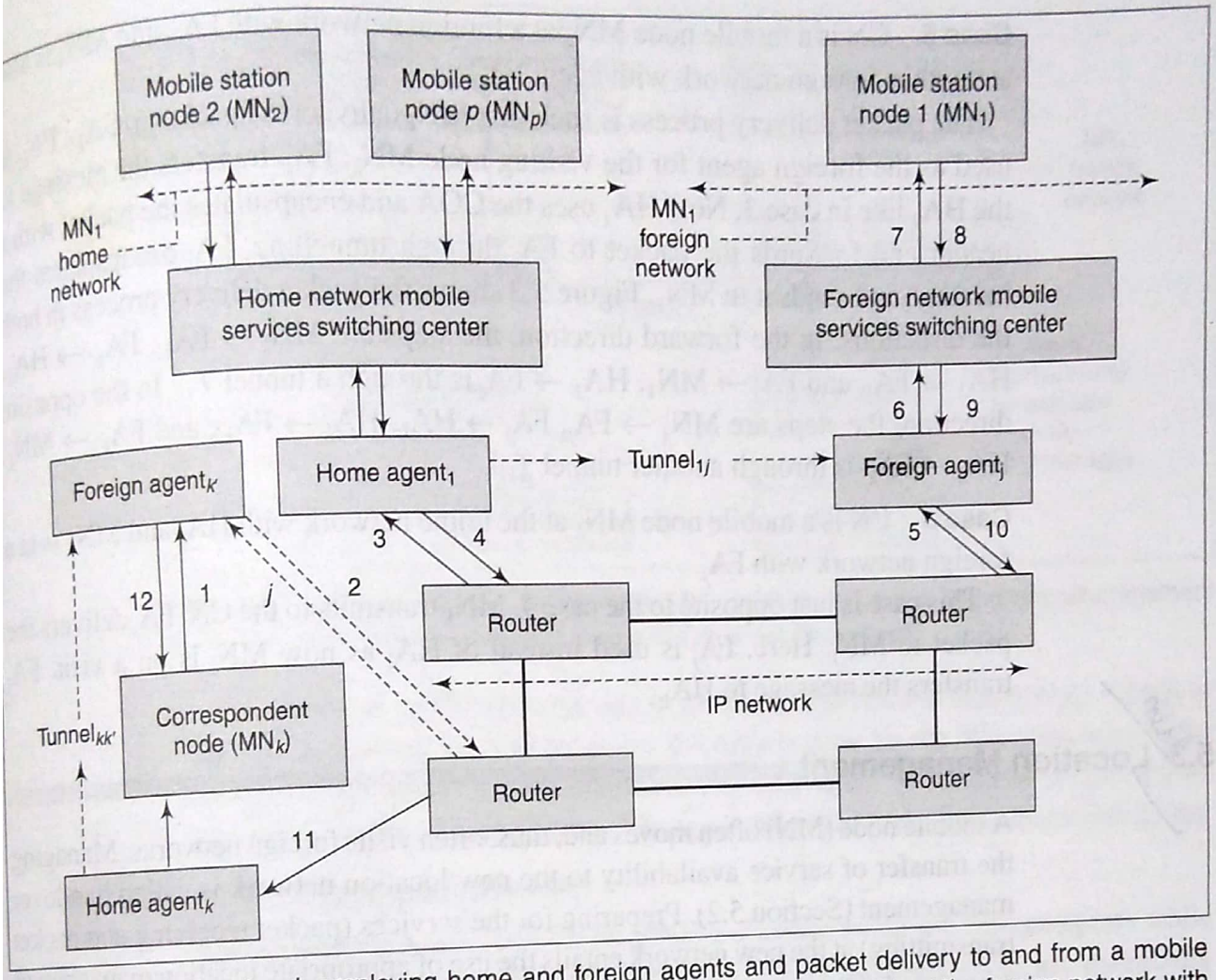

Fig. 5.3 Mobile IP network employing home and foreign agents and packet delivery to and from a mobile node MN_k at a foreign network with FA_k and the other mobile node MN_1 at the foreign network with FA_j

FA_j. It encapsulates the received IP packet using a new header. The new header over the IP packet has a care-of address (COA). The packet encapsulated with the new header is transmitted to FA_j by tunnelling. The FA_j reads the COA and decapsulates the IP packet. It then reads the destination IP address and transfers the packet to MN_1. When MN_1 sends the response message or IP packet with CN as the destination address, FA_j transfers the packet to CN as would have been done by HA_1 had MN_1 been at the home network. The mobility of MN_1 is secure from the CN as any movement on the part of MN_1 is known only to HA_1 and FA_j. Section 5.5 explains the concepts of protocol tunnelling and encapsulation.

Case 4 CN is a mobile node, MN_k, at a foreign network with FA_k and MN_1 is at the home network with agent HA_1.

The packet delivery process is similar to the step in case 3 when MN_1 transmits to CN. MN_k delivers the packet to FA_k. Here, FA_k is used instead of HA_k as now MN_k is on a visit. FA_k transfers the message to HA_1 like in case 1 where CN transfers the message to HA_1.

Case 5 CN is a mobile node MN_k at a foreign network with $FA_{k'}$ and MN_1 is also at another foreign network with agent FA_j.

The packet delivery process is such that MN_k delivers the packet to $FA_{k'}$. $FA_{k'}$ is used as the foreign agent for the visiting node MN_k. $FA_{k'}$ transfers the message to the HA_1 like in case 3. Now HA_1 uses the COA and encapsulates the packet with a header and forwards the packet to FA_j through tunnelling. FA_j decapsulates the message and sends it to MN_1. Figure 5.3 shows the packet delivery process in both the directions. In the forward direction, the steps are $MN_k \rightarrow FA_{k'}$, $FA_{k'} \rightarrow HA_1$, $HA_1 \rightarrow FA_j$, and $FA_j \rightarrow MN_1$. $HA_1 \rightarrow FA_j$ is through a tunnel T_{1j}. In the opposite direction, the steps are $MN_1 \rightarrow FA_j$, $FA_j \rightarrow HA_k$, $HA_k \rightarrow FA_{k'}$, and $FA_{k'} \rightarrow MN_k$. $HA_k \rightarrow FA_{k'}$ is through another tunnel $T_{kk'}$.

Case 6 CN is a mobile node MN_k at the home network with HA_k and MN_1 is at a foreign network with FA_j.

This case is just opposite to the case 4. MN_k transmits to the CN. FA_j delivers the packet to MN_1. Here, FA_j is used instead of HA_1 as now MN_1 is on a visit. FA_j transfers the message to HA_1.

5.3 Location Management

A mobile node (MN) often moves and, thus, often visits foreign networks. Managing the transfer of service availability to the new location network is called handover management (Section 5.2). Preparing for the services (packet receiving and packet transmitting) at the new network entails the use of appropriate location management protocols by the network for management of the MNs location. Agent discovery through agent advertisement and agent solicitation are two protocols used for this.

5.3.1 Agent Discovery

When visiting a foreign network, a mobile node (MN) must discover (find) a foreign agent (FA). Figure 5.4 shows the method of agent discovery by a mobile node MN_1 on receiving the COA during agent advertisement or by agent solicitation in case the COA is not discovered. The steps in the protocol for discovering an agent are as follows:

1. Listen to an advertisement (ICMP message) from an agent.
2. Proceed to step 3 if the advertisement is found, else solicit the agent from the routers. If agent found then proceed to step 3, else repeat the step.
3. If the COA discovered from the message is found to be the same as the previous COA, go back to step 1, else proceed to step 4.
4. If the discovered COA is the same as the home network, de-register at this network and go back to step 1, else if the current COA is a new COA, then register with the new COA.

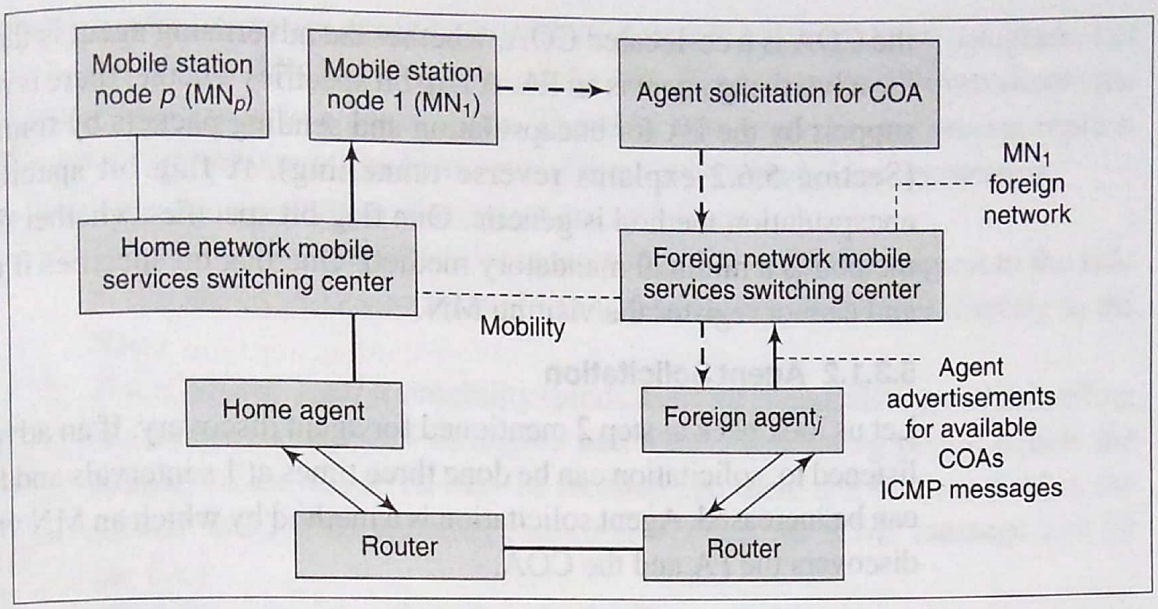

Fig. 5.4 Agent discovery by mobile node MN_1 on receiving COA during agent advertisement or by agent solicitation in case COA is not discovered

Discovery of an FA while on visit to a foreign network and then reverting back to the HA on moving back to the home network is done by the MN using one of the two protocol steps—agent advertisement and agent solicitation (registration) mentioned in steps 1 and 2 above. These are described in the following subsections.

5.3.1.1 Agent Advertisement

Agent advertisements are used by MNs to discover home and foreign agents while moving from one network area to another. Agent advertisements are essentially ICMP messages (Section 5.1.1.10) which are sent to a number of addresses. ICMP message uses the following options and words which are added for the mobility extension of ICMP header.

1. A 32-bit word, with first byte = 00010000 and second byte for length (= 2 words plus number of COAs specified in the extension to which the ICMP message is to be sent) and two bytes for the 16-bit sequence number (for the ICMP message advertised)
2. A 32-bit word has a two-byte specification by the agent for registration lifetime during which the MN can register with the new COA (step 4 in agent discovery). (Lifetime specification is in seconds). It has 8 bits for flags. The remaining byte is not used presently. It is reserved for any future requirements of modifications or specification expansion in ICMP.
3. A set of 32-bit words for the COA addresses for the MN at that agent

Second word has eight flag bits. A COA is said to be a co-located COA if the MN temporarily acquires an additional IP address while on visit to a new network; otherwise the COA is the same IP address for that MN while on visit and when at home. The FA obtains the co-located COA using the dynamic host configuration protocol (DHCP) (Section 5.7). A flag each in the second word specifies whether

the COA is a co-located COA, whether the advertising agent is the HA, or whether the advertising agent is an FA. A flag bit specifies whether there is reverse tunnelling support by the FA for encapsulation and sending packets by tunnelling to the HA (Section 5.6.2 explains reverse tunnelling). A flag bit specifies whether the encapsulation method is generic. One flag bit specifies whether the encapsulation method is a minimal mandatory method. One flag bit specifies if the agent is busy and cannot register the visiting MN.

5.3.1.2 Agent Solicitation

Let us look back at step 2 mentioned for agent discovery. If an advertisement is not listened to, solicitation can be done three times at 1 s intervals and later this interval can be increased. Agent solicitation is a method by which an MN visiting a network discovers the FA and the COA.

5.4 Registration

When an MN discovers an agent for service and finds a COA from it, then the MN needs to register itself (for the service of receiving and transmitting of IP packets) with the new agent FA. The MN must also de-register (for the service of receiving and transmitting of IP packets) with the HA (step 4 of agent discovery in the protocol). The function of HA now is to encapsulate the IP packets and transmit them to the discovered FA (through tunnelling), whenever a CN communicates with the MN. Figure 5.5 shows a mobile node MN_k at a foreign network, after agent discovery of FA_j, seeking registration for creating a tunnel between HA_1 and FA_j

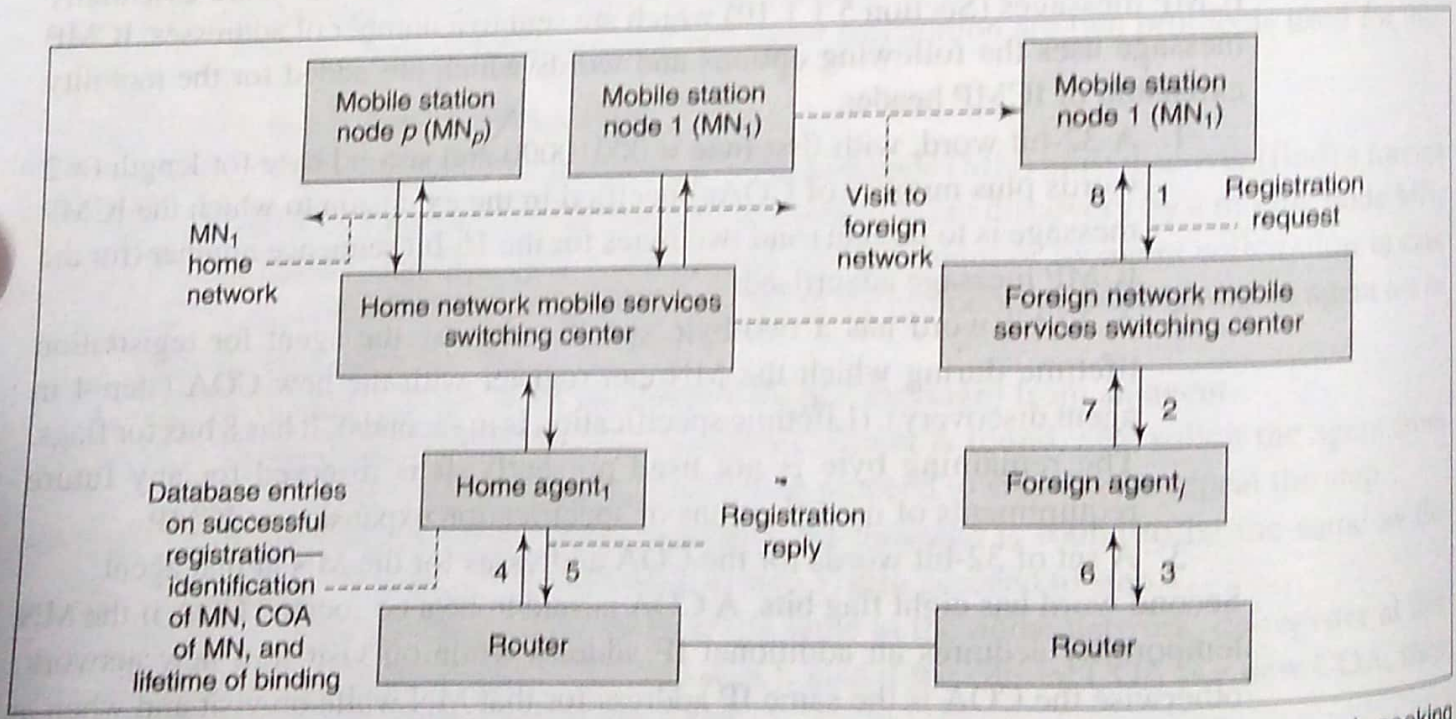

Fig. 5.5 Mobile node MN_k at a foreign network after agent discovery of FA_j in a mobile IP network seeking registration for creating tunnel between HA_1 and FA_j

Requests and replies are made by the MN, FA, and HA using a UDP datagram. Let us assume that the MN has IP address of the HA. If not, then the MN broadcasts the registration request to a paging area. The HAs then send the registration replies. The MN requests one of the HAs (out of those which reply) for registration.

The steps for registration at an agent are as follows:

1. The MN sends a registration request to FA. FA sends that request to the HA. When the COA is a co-located COA, then the request is sent directly to the HA.
2. The HA binds itself for mobility (binds itself for encapsulating and tunnelling the packets to the MN through a new FA). The binding period equals the lifetime of the COA. (It may be recalled that there is a lifetime field in the second word of the mobility extension words in the ICMP message sent by the FA.)
3. The MN registers again before the binding period expires, when it moves to another foreign network, or when it returns back to the home network.
4. The HA sends a registration reply to the FA and the FA to the MN. The MN checks whether the reply shows successful registration. This means that mobility binding now exists from the HA to the FA. It is possible that the reply shows that the registration was not successful. This is when there are too many tunnels created at the HA and the HA does not have the resources to handle new requests or there is an authentication failure or the HA is not reachable to the FA.

Registration Request Fields for Sending Mobile IP registration is by a UDP datagram, which sends the request using the following words after the UDP header (Section 5.1.1):

1. A 32-bit word with first byte = 00000001, eight bits for flags, and two bytes for the lifetime (in seconds)
2. A 32-bit word for the home IP address of the MN
3. A 32-bit word for the home agent IP address of the MN
4. A 32-bit word for the COA of the MN at the new agent
5. A 32-bit word for the identification of the MN
6. A set of words for extensions

The first word has eight flag bits. A flag each in first word specifies whether the COA is a co-located COA, whether the advertising agent is the HA, and whether the advertising agent is the FA. One flag bit specifies whether the MN requests previous mobility binding to be retained. This permits both new as well as the previous mobility bindings. A flag bit specifies whether the encapsulation method is generic, whether the encapsulation method is a minimal mandatory method, and whether the MN wishes to receive broadcast (multicast) messages, which the HA receives for tunnelling to the new FA. If not, then the broadcast messages are filtered at the HA. A flag bit is used to specify if there is reverse tunnelling support from the FA.

Registration Reply Fields for Sending UDP datagram sends the reply using the following words after the header:

1. A 32-bit word with first byte = 00000011, eight bits for a code specifying the result of registration, and two bytes for the lifetime (in seconds)
2. A 32-bit word for the home IP address of the MN
3. A 32-bit word for the home agent IP address of the MN
4. A 32-bit word for identification of the MN
5. A set of words for extensions

The result of registration (at the code sent in the first word of the reply) indicates (a) successful registration and whether the previous mobility binding still exists, (b) FA's rejection with one of the five reasons for it, or (c) HA's rejection with one of six reasons for it.

New Database Entry Fields after Registration at the HA The new database entry fields after registration at the HA consist of the following—*identification* of MN, COA of the MN, and *lifetime* of binding to tunnel the packets to the MN's COA. Figure 5.5 shows the entry fields for the MN registered at HA_i. The COA defined at the COA field facilitates the tunnelling of the packets to the registered new COA (of the MN on a foreign network) after identifying that MN using the identification field. The lifetime field specifies how long the tunnel binds and can be used by the HA for forwarding the packets to the new COA (at FA). (When the binding life expires, the tunnel is not forwarded from the HA to the FA using the COA.)

Database Entries in the Fields at the FA after Registration at the HA Following are the entries for the MNs visiting at the FA: (a) MN identification field, (b) home IP address of the MN, (c) IP address of the HA, (d) MN-link layer address for sending and receiving packets and messages to and from the MN, (e) UDP source port of the registration request, (f) received identification of the MN, (g) COA of the MN and lifetime of binding to tunnel the packets to the MN's COA (The binding of lifetime field specifies how long the tunnel can deliver the forwarded messages to new MN after registration at the FA. When the binding life expires the tunnel does not deliver to the FA using the COA), and (h) remaining lifetime.

5.5 Tunnelling and Encapsulation

When a mobile node (MN) is visiting a foreign network supported by a foreign agent (FA), then the FA has the COA (care-of address) of the MN. The FA receives the IP packets that were received at the HA through a tunnel from the HA to the FA (from HA IP address to the COA IP address at the FA). Tunnelling refers to establishing of a pipe. Pipe is a term used to specify a data stream between two connected ends. The data stream is inserted from one end and is retrieved as FIFO (first in first out) words from the other end. Packets received at the HA are transmitted through the tunnel after encapsulation.

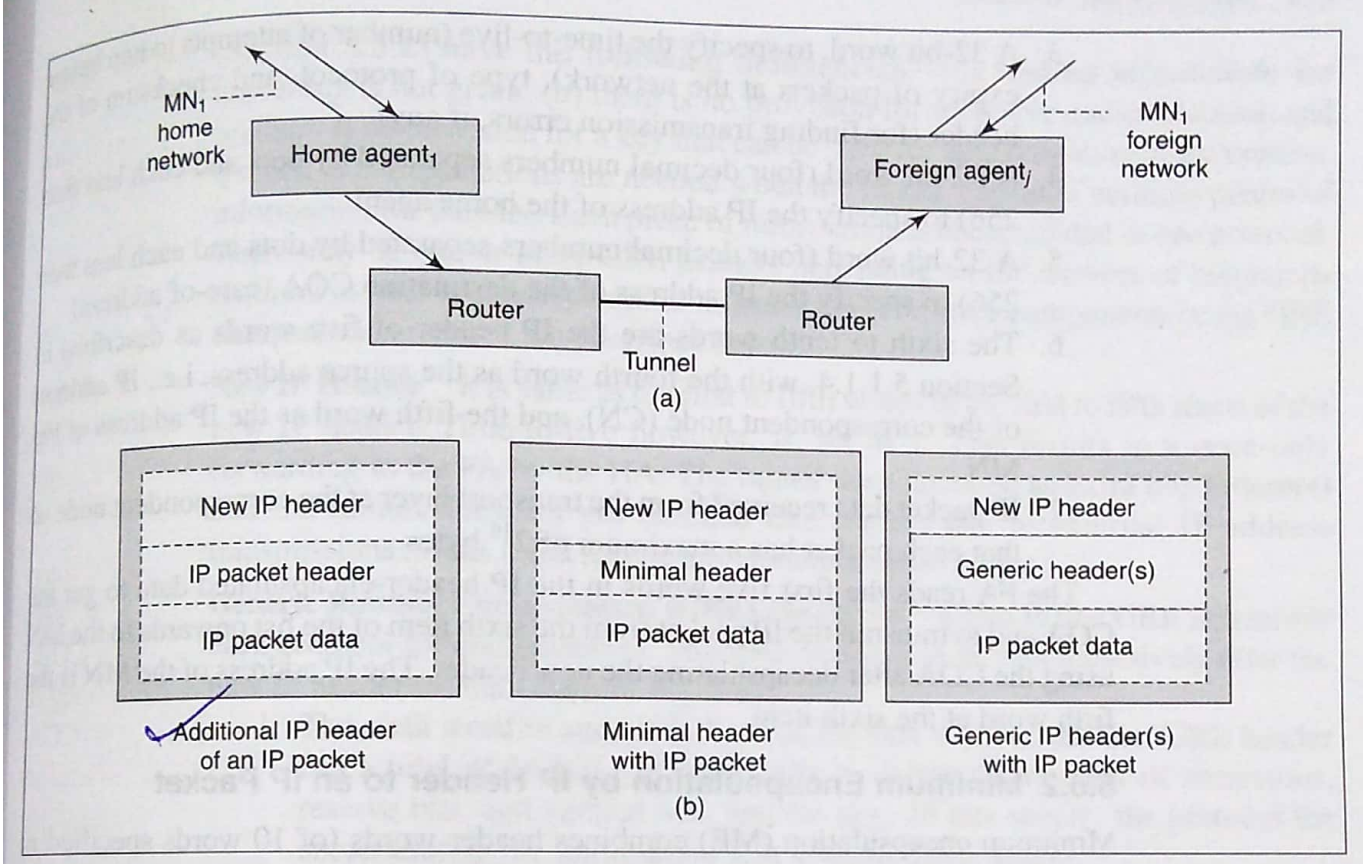

Fig. 5.6 Mobile node MN_k at a foreign network after agent discovery of FA_j in a mobile IP network seeking registration for creating a tunnel between HA_1 and FA_j

Figure 5.3 shows two tunnels (T_{1j} and $T_{kk'}$). Figure 5.6(a) shows a tunnel between the HA and the FA to carry the encapsulated packet. Figure 5.6(b) shows three ways of encapsulation. These ways are described in the following subsections.

5.5.1 Encapsulation by Additional IP Header of an IP Packet

Section 5.1.1 describes the packet formation in IP protocol and IP header fields. One way of encapsulating is as follows—the IP packet received at the HA has an IP header and data with a maximum 2^{16}-byte IP packet. Another IP header (new IP header) is placed over this IP packet. Now, the new IP header has the IP address of the HA as the source and the IP address of the FA as the destination. The data encapsulated with the new IP header has the following fields:

1. A 32-bit word, to specify the IP version (IPv4 or IPv6 for Internet or broadband Internet), length of the IP header (five words), precedence of the IP packet, and total packet length (which is now five words more than that of IP packet received at the HA)
2. A 32-bit word, to specify the ID for the packet, flags, and fragment offset for the same packet ID (a packet can be transmitted in fragments.)

3. A 32-bit word, to specify the time-to-live (number of attempts to hop before expiry of packets at the network), type of protocol, and checksum of the header (for finding transmission errors, if any)
4. A 32-bit word (four decimal numbers separated by dots and each less than 256) to specify the IP address of the home agent
5. A 32-bit word (four decimal numbers separated by dots and each less than 256) to specify the IP address of the destination COA (care-of address)
6. The sixth to tenth words are the IP header of five words as described in Section 5.1.1.4, with the fourth word as the source address, i.e., IP address of the correspondent node (CN), and the fifth word as the IP address of the MN
7. IP packet data received from the transport layer at the correspondent node so that each packet has a maximum of 2^{16} bytes

The FA reads the first five words in the IP header-encapsulated data to get the COA and to transmit the IP packet from the sixth item of the list onwards to the MN using the COA after decapsulating the new header. The IP address of the MN is the fifth word at the sixth item.

5.5.2 Minimum Encapsulation by IP Header to an IP Packet

Minimum encapsulation (ME) combines header words (of 10 words specified in Section 5.5.1) into seven or eight words in the following manner—the first words in the new IP header (of five words) and the IP packet header (of five words) are the same and are duplicating in case of IP-in-IP encapsulation (see Fig. 5.6).

1. The sixth and seventh words in the sixth item of the new IP header are not present in minimum encapsulation (ME) as both words are mere repetitions.
2. The eighth word in the sixth item is changed and now specifies the type of protocol, a one-bit flag, seven reserved bits, and a 16-bit checksum of the modified three-word IP header (from the original five) for finding transmission error, if any.
3. The ninth word in the sixth item is changed and now specifies (instead of the CN IP address) the MN IP address (which was earlier specified by the tenth word).
4. The tenth word in the sixth item is changed and now specifies (instead of the MN IP address) the CN IP address in case the flag bit is set to 1, and the tenth word in the sixth item is removed in case the flag bit is set to 0.

The FA reads the first five words in ME and transmits the packet to the MN using the COA. The MN IP address is specified by the seventh or the eighth word, depending upon the flag bit.

5.5.3 Generic Routing Encapsulation by IP Header to IP Packet

IP header-in-IP header encapsulation (Section 5.5.1) and minimal encapsulation

(Section 5.5.2) have the following deficiencies—(a) routing information for tunnelling is not given, (b) there is no provision for recursive encapsulations, and (c) there is no provision for a key that can be used for authentication or encryption. Recursive encapsulations are needed when the tunnel transmits multiple pieces of information for the MN. Each piece of information is encapsulated in one protocol. There may be one or more GRE headers depending on the number of recursions required to send multiple pieces of information. The three components in the GRE encapsulation method are described below.

New IP Header It is same as the first to fifth words in the first to fifth items of the new IP header. Time-to-live however, is, set as 1. This results in a once-only forwarding to the FA by the HA. The tunnel does not need an extra hop (attempt) and the tunnel does not get blocked like routers due to external IP address transmissions. It has fixed source and destination end points.

Generic Routing Encapsulation (GRE) Header(s) There is one GRE header for each protocol for encapsulation. The GRE header can be sent recursively after the new IP header (bottom right in Fig. 5.6).

1. The sixth word in encapsulation and the first word of the first GRE header has a total of 16 bits for flags—bits to define the number of recursions, reserve bits, and version bits, and the next 16 bits specify the protocol for encapsulating the information sent with the GRE header.
2. The seventh word specifies a 16-bit checksum and a 16-bit offset. Both are optional as indicated by the flag bits used to define these options. (Checksum of the GRE header enables locating of transmission errors, if any, at the receiver).
3. The eighth word specifies a 32-bit key. It is optional as indicated by the flag bit to used define the key option. (The key at the GRE header enables authentication or encryption at the FA.)
4. The ninth word specifies a 32-bit sequence number information. It is optional as indicated by the flag bit used to define the sequencing option. (Sequencing at the GRE header enables the FA to rearrange the packets sent by the HA.)
5. The tenth word specifies a 32-bit routing information. It is optional as indicated by the flag bit used to define the routing option. (Routing at the GRE header enables authentication or encryption at the FA.)
6. From the eleventh word, if number of recursions are defined in the first word of the GRE header, then the next GRE header is inserted before the IP header and IP data sent by the HA. There will be eleventh and twelfth words in case of one recursion. If the number of recursions specified in the eleventh word in the GRE header is two, then the next two GRE headers are also inserted before the IP header and IP data sent by the HA (Fig. 5.6).

IP Header and IP Packet Data This part remains the same as that in the un-encapsulated IP header and the data received from the CN (correspondent node) IP

packet at the HA. The first word has five flag bits and three recursion-number-defining bits. The five flag bits are—checksum option flag, sequence number field option flag, key option flag, and source-routing option flag. Source routing is a method in which the source of a packet provides the route information also. Source-routing-method-based routers use the routing information word for routing a packet.

5.6 Route Optimization

Consider Fig. 5.3. Let us assume that MN_1 is visiting a foreign network which happens to be the home network of CN_2 and CN_2 is very close to CN_1 (Fig. 5.2). Consider the mobile IP network employing home and foreign agents and packet delivery to and from a mobile node MN_k at a foreign network with FA_k and MN_1 at the foreign network with FA_j. Figure 5.7 shows a mobile IP network employing a triangular route without mobility binding between COA_j and CN_k. It marks the path numbered in sequence as 1, 2, 3, 4, and 5 to MN_1. Packets make a triangular trip to reach from CN_k to MN_1. It is also possible that FA_k and FA_j are identical. Optimization of the triangular route can be carried out in case the MN_1 opts to make its mobility known. Section 5.6.1 explains how the route is optimized.

expiries.

5.7 Dynamic Host Configuration Protocol

When a mobile node visits a foreign network then it gets a new IP address known as care-of address (COA) by agent discovery process and advertisement of the COAs by the foreign agent (Section 5.3.1). Also, a co-located COA is obtained by the dynamic host configuration protocol (DHCP). Let us assume that a mobile computer (laptop or other) visits another network (which has a separate domain name server identity on the network and functions as a subnet on the Internet). The computer gets a new IP address in this case too. The server provides a dynamic IP address, subnet mask, and ARP and RARP caches to enable the computer to transmit and receive the IP packets at the new IP address from the Internet via the subnet. The server (subnet) has its own IP address to provide connectivity to the Internet. Dynamic host configuration protocol (DHCP) is a protocol to dynamically provide new IP addresses and set subnet masks for the visiting computer so that it can use the server and subnet router at the place being visited.

Any software in an agent (e.g., a foreign agent visiting a mobile node) or device software for connecting to the network can have a software component called the

DHCP client. The DHCP client protocol communicates with a server. The steps in the DHCP protocol for dynamically configuring the IP address and other networks are as follows:

1. The DHCP client in an agent, device, or computer broadcasts a discover request known as DHCPDISCOVER directly or through a DHCP relay agent to the servers. A subnet may have a number of DHCP servers. For this reason, the request is broadcasted to several servers. (A DHCP server may be part of the operating system of the computer seeking connection to the network. The server has software for allocation of network addresses to the computer.)
2. Each server listening to the discover request finds the configuration, which can be offered to the client. Server(s) send(s) the configuration parameters, including an IP address not presently in use, at the subnet. The configuration parameters are in the DHCPOFFER for the offered configuration.
3. The DHCP client can reject the offer from a server or servers. When DHCP offers from all the servers are rejected, the client repeats the steps from step 1, else it proceeds to step 4.
4. The client replies to the servers through a DHCPREQUEST to each server. The option 'reject' is set in each reply to those DHCP servers to which the client reply is 'reject'. The option 'select' is set for those servers to which the client reply is 'select'.
5. The selected DHCP server creates and manages bindings. (A binding is a collection of configuration parameters, including at least one IP address, which is associated with and binds to the DHCP client.) DHCP server also sets a time interval during which the offered IP address will be valid for the DHCP client computer. The required interval can vary depending upon the likely Internet connection interval at a particular Internet-serving network. The binding may periodically provide new IP addresses.
6. The DHCP server confirms the binding through a message. It sends DHCPACK after creating the binding.
7. When the DHCP client computer leaves the subnet, it sends DHCPRELEASE message. In case the client does not send DHCPRELEASE within a specified time interval, the server frees the created binding.
8. The server and client also use the authentication protocols before considering the DHCPDISCOVER from a client and before accepting a DHCPOFFER, respectively.

The DHCP protocol guarantees that any assigned network address, at a given instant, is in use by either one DHCP client or none.