Ch 6. Mobile IP

- What is Mobile IP?
- Mobile IP Requirements and Goals
- IP Overview and the need for Mobile IP
- Mobile IP Entities
- Mobile IP Operation:
  - Agent Discovery
  - Registration
  - Routing/Tunneling/Delivering Packets
- Mobile IP and IPv6
6.1 What is Mobile IP?

- Mobile IP provides network layer mobility
- Provides seamless roaming
- “Extends” the home network over the entire Internet
6.2 Mobile IP Requirements and Goals

Mobile IP cannot:
- make modifications to host OS
- make no modification to IP routing
- support moves more than once per second, must complete registration

Mobile IP must:
- maintain application transparency
- be compatible with Internet addressing
- be scalable to support large numbers of mobile nodes
- be able to operate in a very large Internet
- be secure, all messages must be authenticated
- support any lower layer that IP runs on

Mobile IP will need to add the following functionality to IP:
- location management and handoff support
- authentication
6.3 IP Overview

IP Addressing:

- Dotted Decimal Notation: 32 bits (4x8) used to represent IPv4 addresses - 192.19.241.18

- Network Prefix and Host Portions: p - prefix, h - host, p + h = 32. If p = 24 then h = 32 - 24 = 8. Using above address the network prefix will be 192.19.241 and host will be 18. For those of you familiar with subnet masks, “p” represents the number of 1’s in the subnet mask. If p = 24, subnet mask is 255.255.255.0, if p = 26, subnet mask is 255.255.255.192.

IP Routing:

- Network prefix is used for routing. Routing tables are used to look up next hop and the interface on the router that is to be used.

- In the routing tables we use the following notation: target/prefix length, e.g., 192.19.241.0/24, or 192.19.241.192/26.

- If two subnet masks/prefixes fit the address, the one with the largest prefix is chosen for routing. E.g., a router with the following 3 entries in its table: 7.7.7.99/32 (p=32 host specific) and 7.7.7.0/24 (0<p<32 network prefix) and
0.0.0.0/0 (p=0 default) will use entry 2 for an IP packet with destination 7.7.7.1 and entry 3 for destination 192.33.14.12.

- **Domain Name System (DNS):** used to translate a host name to an IP address. A host sends a query to a server to obtain the IP address of a destination of which it only has the host name.

- **Link Layer Addresses - Address Resolution Protocol (ARP):** Once a host has the IP address of a destination it then needs to finds its layer 2 address or the layer 2 address of the next hop on the path. A broadcast message is sent and the targeted host responds with its layer 2 address. A *proxy ARP* is a response by a node for another node that cannot respond at the time the request is made (e.g. the node is a mobile node and not on its host net at the time, its home agent will respond in its stead). A *gratuitous ARP*, is a reply to no ARP request, used by a node that just joins the network and wants to make its address known. Can be used by a mobile node upon its return to its home net.
6.4 The Need for Mobile IP

IP routing uses network prefixes. In the Internet, the destination address is linked to the location of a host on the network. If a node moves, then all the routing tables in the network must make a special (host specific) entry in their tables to route IP datagrams to the mobile node at its new location. This is impossible to do and will not work if the host is on the move and changing its access/attachment point frequently and if the number of mobile hosts goes up.

A host cannot change its IP address when it changes its location without causing major changes to a different set of tables: all DNS servers must change the entry for host name -> IP address in their tables. The same problems as with the point above arise in addition to another problem related to the transport layer protocols. If a node is truly mobile and it changes network boundaries during a session (i.e., the network prefix has changed) then the node will have to change its IP address. But TCP and UDP use the IP address as part of their identification for a session/connection. If mobility is not needed but only nomadicity then changing the IP address is feasible, it will not intervene with the operation of UDP and TCP, however we still have the DNS problem and scalability issues.
Mobile IP **solves** the following problems:

1) if a node moves without changing its IP address it will be unable to receive its packets,

2) if a node changes its IP address it will have to terminate and restart its ongoing connections everytime it moves to a new network area (new network prefix).

Mobile IP is a routing protocol with a very specific purpose.

Mobile IP is a network layer solution to node mobility in the Internet.

Mobile IP is not a complete solution to mobility, changes to the transport protocols need to be made for a better solution (i.e., the transport layers are unaware of the mobile node’s point of attachment and it might be useful if, e.g., TCP knew that a wireless link was being used!).
### 6.5 Mobile IP Entities

1. **Mobile Node (MN):** a node that can move and implements mobile IP. Each mobile node has a home network and may move and connect to a foreign network.

2. **Home Agent (HA):** supports the mobile on its home network -> maintains the location registry (care of address), and intercepts and tunnels packets to mobile node (at its care of address).

3. **Foreign Agent (FA):** supports the mobile on the foreign network -> assists with the registration of the mobile node and delivers tunneled packets to visiting mobile.

4. **Care of Address (COA):** address given to a mobile node at the visiting location -> used for tunneling packets. It may be the address of the foreign agent or a temporary local address (e.g., assigned through DHCP).
6.6 Mobile IP Operation: Summary

Consists of 3 steps: 1) Agent discovery, 2) Registration, 3) Routing/Tunneling

- **Agent Discovery**: consists of broadcast messages used by mobiles to detect that they have moved and are required to register with a new FA.
  - FAs send agent advertisements
  - MNs can solicit for agents if they have not heard an agent advertisement in awhile or use some other mechanism to obtain a COA or temp. IP address.
  - MNs know they are home when they recognize their HA.

- **Registration**: used by a MN to inform the FA that it is visiting.
  - The new care of address of the MN is sent to the HA.
  - Registration expires, duration is negotiated during registration
  - Mobile must re-register before it expires
  - All registrations are authenticated
  - The MN sends a registration request in to the FA which passes it along to the home agent. The HA responds to the FA which then informs the MN that all is in order and registration is complete.
- **Routing/Tunneling**: consists of the delivery of the packets to the mobile node at its current care of address.
  - Sender does not need to know that the destination is a MN.
  - HA intercepts all packets for the MN and passes them along to FA using a tunnel (**triangle routing**).
  - Three types of tunneling protocols are specified for Mobile IP:
    - **IP-in-IP encapsulation**: required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.
    - **Minimal encapsulation**: optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.
    - **Generic Routing Encapsulation (GRE)**: optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.

- Type of tunneling supported is indicated in registration.
• **Non Triangle Routing**: tunneling in its simplest form has all packets go to home network (HA) and then sent to MN via a tunnel.

  m This involves two IP routes that need to be set-up, one original and the second the tunnel route.

  m Causes unnecessary network overhead and adds to the latency.

  m **Route optimization** allows the corresponding node to learn the current location of the MN and tunnel its own packets directly. Problems arise with

    k **mobility**: correspondent node has to update/maintain its cache.

    k **authentication**: HA has to communicate with the correspondent node to do authentication, i.e., security association is with HA not with MN.
6.6.1 Nuts and Bolts of Mobile IP

Mobile IP was designed with extensibility in mind. It consists of a short header of fixed length followed by one or more extensions.

Extensions consist of:

- **Type field**: distinguishes the different extensions
- **Length field**: length of data field
- **Data field**: contents of the extension, informations sent from source to destination.
### 6.6.2 Agent Discovery

Agent discovery consists of two ICMP messages:

- **Agent advertisement**: used by nodes to announce their capabilities. Broadcast periodically. It consists of an ICMP router advertisement message with the mobility agent advertisement extension. Each message contains a list of COAs that may be used by visiting MNs. These COAs are called **FA COAs**. Note that the network prefix of the COA may not be the same as the network prefix of the foreign link. It is required however that the FA have an interface on the foreign link to which the MN is attached. For these kinds of attachments, the FA is responsible for receiving all the MNs’ packets and forwarding them. This type of COA is different from the collocated COA described below.

- **Agent solicitation**: used by mobile nodes to discover a FA. This forces a FA to broadcast an agent advertisement message. It consists of an ICMP router solicitation with the time to live set to “1”.

Determining whether a mobile has moved and needs a new FA:

- **Using Lifetimes**: FA will broadcast an advertisement before the lifetime value broadcast in a previous message expires. When a mobile does not
receive an advertisement within the specified time limit, it must try to find another FA to register with. It either assumes there is something wrong or that is has moved out of the range of the previous FA.

- **Using network prefixes**: as a network can have more than one FA, a mobile node receiving an agent advertisement message from a different agent within the specified lifetime, with a different network prefix, knows that it has moved. If the prefix is the same it waits to hear from its FA.

What happens when a mobile node *does not hear advertisements*?

- It assumes it is on its own home network and tries to find the default router. It does so by sending out an **echo request msg**., to which the default router should respond.

- Using Dynamic Host Configuration Protocol (DHCP): if the default router does not respond, it assumes it is connected to a foreign network and tries to find a DHCP server to obtain a temp. IP address. This type of COA is called a **collocated COA**. The network prefix of the COA must correspond to the network prefix of the foreign network link. The MN is responsible for receiving all of its packets. Note that a MN can use a collocated COA even though there is a FA on the foreign link that is offering its services.
Once it has a collocated COA it still has to detect when it has moved. It can do so by either:

1) **listening to each packet** (promiscuous mode) going by on the network and determining from the addresses what local network it is on and if it has moved (different network prefix), or

2) **detect** if any of its ongoing **TCP connections** have had any activity recently. If not then it might conclude that is has moved (i.e., the TCP packets are being sent to the old location and the MN is not receiving them).
6.6.3 Registration

What is registration? It allows the MN to:

- **request routing services** from a FA on a foreign network
- inform its HA of its new COA for packet forwarding (mapping of MN home address onto a COA. This is called a **binding**, each binding has a lifetime!)
- **renew** a registration that is about to expire
- **de-register** when it returns to its home location

After the MN has **obtained a COA** on a foreign network (whether a FA COA or a collocated COA), it **must register** with its HA and FA (if required, note that this may not always be necessary!).

All **Registration messages**, unlike Agent Discovery messages, use **UDP** (recall Agent Discovery messages use ICMP).

Like Agent Discovery messages, Registration messages consist of a short fixed header and variable length extensions.

Registration consists of the following set of messages: 1) Registration request, and 2) Registration reply.
Three common **scenarios** exist for registration:

- 1) through an FA,
- 2) directly, and
- 3) de-registration.

The registration protocol consists of the MN sending the **Registration Request** message and waiting for a response from the HA.

If the MN does not receive a **Registration Reply** message before a timer expires it sends the request again. It does so a number of times, each time increasing the value of the timer. After a fixed number of attempts it gives up.

Each Registration message must have the **authentication extension**.

The **UDP port numbers** are chosen as follows:

- For the request message the Source Port field can be any value, the Destination Port field must be 434, reserved for Mobile IP registration messages.
- For the reply message the FA and HA usually reverse the port numbers.

The ‘**R**’ bit: if set in the FA advertisement message, enforces a MN that is using a collocated COA to register via the FA and use its address as the destination address (at both the link layer and the IP layer).
6.6.3.1 Processing Registration messages

For a MN

A MN, depending on which registration scenario it is in, will figure what addresses to use in the various fields of the Registration request message.

Link layer addresses are tricky:

- A MN may not use ARP if it is using a FA COA. It needs to use the address of the FA as the destination address.
- If it is using a collocated COA, then it uses ARP to locate the default router using its COA as source. Note that if the ‘R’ bit is set is uses the FA address as the destination address.
- For de-registration is uses ARP to locate the HA link address and it uses its own home address for the ARP message.

For network layer addresses (i.e., IP addresses):

- It uses the FA address as destination address when using the FA COA and its own home address as the source address.
• If using a **collocated COA** it uses its **COA** as **source** address and the **HA address** as **destination** address. Note that if the ‘R’ bit is set then is must use the same addresses as for the FA COA scenario.

• For **de-registration** it uses its own home address as source and the HA address as destination.

The MN sets the appropriate bits for tunneling and header compression and also sets the ‘S’ bit to indicate the purpose/extent of the action to be taken by this message. It chooses a lifetime for the registration. This lifetime should not exceed that indicated by the FA advertisements.

The **identification field** is chosen randomly and is unique for each Registration request message. This allows the MN to **match requests with replies** (replies use the same identification) and it prevents a ‘**malicious**’ user from **replaying** the MN’s request at a later time.

**For a FA:**

A FA may **refuse** a Registration request for a number of reasons: lifetime too long, authentication failed, requested tunneling not supported, cannot handle another MN (current load too high).
If an FA does **not refuse** the request it **relays** it to the HA. Relaying is different from forwarding as the FA is required to process the packet and create new headers.

Some important fields of the request message are **recorded** for use later on: MN link layer address, MN IP address, UDP source port, HA IP address, identification number and requested lifetime.

Regarding a **Registration reply** message, the FA can refuse it and send a decline to the MN if it finds the reply from the HA to be invalid. Otherwise it updates its list of visiting MNs and begins acting on behalf of the MN.

**For a HA**

The HA will **determine**, as the FA did, whether it will accept the request. If it does not it returns a code in the reply message indicating the cause of the failed request.

If the request is **accepted**, the reply is sent back by **reversing** all the IP addresses and UDP port numbers.

The HA **updates** the **binding table** corresponding to that MN dependent upon the nature of the request.
6.6.4 Routing and Tunneling of Packets

Routing a packet to a MN involves the following:

- A router on the home link, possibly the HA, advertises reachability to the network prefix of the MN’s home address.
- All packets are therefore routed to the MN’s home link.
- A HA intercepts the packets for the MN and tunnels a copy to each COA in the binding table.
- At the foreign link either the MN extracts the packet (collocated COA) or the FA extracts the packet and forwards it to the MN.

A HA can use one of two methods to intercept a MN’s packets:

- The HA is a router with multiple network interfaces. In that case it advertises reachability to the MN’s home network prefix.
- The HA is not a router with multiple interfaces. It must use ARP to receive the MN’s packets. It either responds to ARP requests on behalf of the MN (proxy ARP) or uses gratuitous ARPs to inform the home network that it is receiving the MN’s IP packets. This is to update any ARP caches that hosts and other devices might have.
1. How to ‘fool’ the routing table into handling tunneled packets at the HA?
   - A virtual interface is used.
   - A packet destined for the MN is handled by the routing routine as all received IP packets are.
   - The routing table has a host specific entry for the MN. This host specific entry is used to route the packet to a virtual interface that basically consists of a process that does encapsulation.
   - Once encapsulation has been performed the packet is sent to be processed by the routing routine again. This time the destination address is the COA and it is routed normally.

2. How to ‘fool’ the routing table into handling tunneled packets at the FA?
   - The same procedure is used as above.
   - A packet coming in with a COA that is one of the FA addresses’ is handled by the routing routine.
   - A host specific address (its own address) in the routing table points to the higher layers and the packet is passed on to a virtual interface.
- The **virtual interface** consists of a process that **decapsulates** the packet and re-routes it to the routing routine.

- The routing routine routes the packet **normally** based upon a **host specific** entry that is the MN’s home address (for which it has the link layer address!).

**How does a MN route its packets?**

- It needs to **find** a router to send all its packets to.

- It can **select** a router in one of a number of ways dependent upon whether it has a FA COA or a collocated COA.

- Having a FA COA does not imply that the MN needs to use it as its default router for sending packets. It can use **any router** that sends advertisements or that is advertised in the Agent Advertisement message.

- If the MN is using a collocated COA it needs to listen for router advertisements or is it hears none, use **DHCP** to find the default router.

- Determining the **link layer address** is another issue. Collocated COA MNs can use ARP. FA COA must note the link layer address when they receive router advertisements or agent advertisements.
### 6.6.5 Different types of Tunneling

1. **Fragmentation** is used in IP networks to break large packets up into smaller ones. In the IP header a fragment offset will indicate the location of the fragment within the larger packet when reassembly occurs at the destination.

2. **IP in IP encapsulation** does not violate any fragmentation rules. It consists of taking an IP packet and adding to it another full IP header with different IP source and destination addresses. It also does not decrement the time to live field, treating a tunnel as a single hop. This encapsulation technique is supported by all HAs and FAs.

3. **Minimal Encapsulation** on the other hand does lose any fragmentation data. It basically removes redundant information carried by both the encapsulating IP header and the encapsulated IP header. So a minimally encapsulated packet can be fragmented, but a fragmented packet cannot be minimally encapsulated. In addition, the time to live field is decremented by every router so a packet may not make it to its destination if the tunnel is long. This encapsulation technique need not be supported by all FAs and HAs, it is optional.

4. **Generic Routing Encapsulation (GRE)** was designed to encapsulate a packet from one protocol into a network layer of a second protocol. It can be used for IP to IP, its advantage is that it includes a **Recur** field that protects against recur-
sive encapsulation (i.e., a packet going through several tunnels). This field is set
to a certain value, and every time encapsulation occurs it is decremented until it
reaches zero when the packet is discarded. Like minimal encapsulation, this
encapsulation technique need not be supported by all FAs and HAs, it is
optional.
6.6.6 Tunneling versus Source Routing

When Mobile IP was first proposed, source routing was suggested as a mechanism for routing packets to MNs.

Source routing involves defining the path that an IP packet must follow through the network. **Loose source routing** means that routers that are specified in the packet must be passed through. **Strict source routing** means that only those routers specified in the packet must be used.

It was suggested that MNs use Loose source routing to reach a correspondent node and by specifying **Record Route Option** in the packet force the correspondent node (i.e., the destination) to use the same return path using Loose source routing.

Why was it not adopted? For three reasons:

- Not all hosts implement the source routing option and so drop packets that require that option.

- Source routing packets require more processing, each router must look into the extension headers to make sure whether or not it must carry out some special function.
Finally security was another issue, and unless authentication is used, bad
guys can intercept the IP packets by using a bogus intermediate address
specified in the source routing extension.
6.7 Mobile IP and IPv6

- No triangle routing:
  - MN may notify its correspondents when it moves
  - Correspondents put care of address in routing headers
- HA will encapsulate packets when it gets them, i.e., if correspondent does not have care of address.
- MNs create their own care of address using some local automatic address configuration scheme such as DHCP.
- RFC for further reading can be ftped from:

Title : Mobility Support in IPv6
Author(s) : David B. Johnson, Charles Perkins
Filename : draft-ietf-mobileip-ipv6-05.txt
Pages : 72
Date : 13-Mar-98
Summary:
This document specifies the operation of mobile computers using IPv6. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address.