Mobility Support in Internet and Mobile IP

CS 515 - Mobile and Wireless Networking

İbrahim Körpeoğlu
Computer Engineering Department
Bilkent University
Bilkent / ANKARA

Problem

- We have seen that mobile users can change point of attachment
  - In a WLAN, a mobile changes access point.
  - In a cellular network, a mobile changes base station.
  - A mobile user can work at office and at home at different in a day: mobile changes Ethernet subnets.
  - A mobile PDA user may connect to its ISP using a modem and PPP protocol from different telephone lines (telephone jacks) at different places: home, work, a foreign location.
- We want out applications to be not disturbed from mobility
  - We want to continue to talk with our cell-phone when we change base-stations
  - We want to continue to run telnet when we change access points in a Wireless LAN.
  - ....

Two kinds of mobility

1) Mobility is totally transparent to applications
   - This is called seamless mobility

2) Mobility is not transparent to applications when we move, but we can still access the network at a new place.
   - This is called portability

- Some protocols support either one of them
  - Mobile IP can support seamless mobility
  - DHCP can support portability

Mobility Solutions

- Mobile Cellular Telephone Networks and Mobile Internet has different protocols and solutions to support mobile users.
  - Mobile Cellular Telephone Networks Solution
    - GSM has its own registration, handoff, mobility management procedures
  - Mobile Internet Solution
    - Mobile IP has been developed to support IP based hosts and mobile users.
- We will look to Mobile IP first.

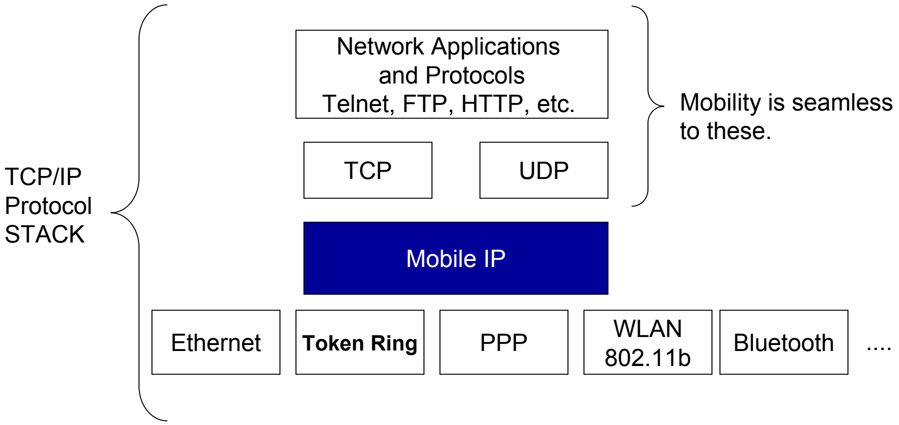
Mobile IP

- Mobile IP is a layer-3 (network layer) mobility solution to support mobile users (laptops, etc) in the Internet in a seamless manner.
- By use of Mobile IP, all TCP/IP applications (applications that use sockets) are unaware of the fact that the users are moving and changing their piont of attachment to the Internet.
  - Only IP protocol and lower layers are aware of mobility
  - Higher protocol layers (TCP, UDP, RTP, etc) and applications are not aware of mobility.

Mobile IP

- We concetrate in how mobility support is done at the network layer.
- We will not be concerned about how mobile stations change physical point of attachments at the Physical layer.
  - This depends on the Physical Media:
    - We have seen how this is achieved in Wireless LAN (802.11b) protocol: re-association with a new access point when the signals get weaker.
    - In Ethernet, we just need to plug out the cable from an old attachment point (jack or HUB) to a new point (a new hub) to change Physical attachment.
    - Other Physical layer may have other procedures to change the point of attachment.
- Mobile IP is a solution that is independent of the physical and data-link layers:
  - It can work for Ethernet, Token Ring, Wireless LANs, PPP over serial cables or phone lines,, etc.

Mobile IP


TCP/IP Protocol STACK

Network Applications and Protocols Telnet, FTP, HTTP, etc.

TCP

UDP

Mobile IP

Ethernet

Token Ring

PPP

WLAN 802.11b

Bluetooth

....

Mobility is seamless to these.

The link layer can be anything.

Why wee need mobile IP

- Current Internet architecture and protocols (without mobile IP support) do not support seamless mobility for mobile users
  - Internet is designed assuming hosts (computer) are static and do not change location frequently.
  - When you move to a new location with your laptop and connect it to a Ethenet cable at the new location, you have re-configure your laptop.
    - Obtain new IP address,
    - Learn the subnet mask.
    - Learn the deafult router IP address
    - Learn the local DNS servers IP addresses
  - When you re-configure your laptop with this information, most of the time you have re-start your laptop.
  - Whether you re-start or not your laptop, previously running network applications will stop working properly when you change the IP address of your laptop.

Why wee need mobile IP

- Initially we had desktops, workstations, main-frames and super-computer all of whic are static and heavy enough so that you can not carry them with you!.
    - Initial design of Internet was for these computers.
- Now, we have
    - Laptop and handheld computers which you carry to new places when you travel
    - Palmtop and Pocket PC computers which you carry in your pocket even if you go to a movie.
    - An these are powerful enough to run a lof interesting network applications like web browsers, etc.
        - Hence you still need Internet access for these highly mobile computers and devices
        - That is why wee need mobility support to be added to the Internet.
        - Mobile IP has been designed for this purpose!

Problems with Internet for Mobility

- In Internet, IP addreses are used for two purposes
    - Identification of hosts
        - Both an IP address or domain name address (FQDN) can be used to identify a host.
        - DNS servers does the mapping between IP addresses and domain names
        - Usually there is one to one mapping.
        - Network protocol in TCP/IP stack usually use IP addresses to identify the end-point
        - Applications may use the domain names so that they are more user friendly to the humans.
    - Locating mobile hosts: for Routing
        - IP addresses are structured and correspond to well-specific locations in Internet.
        - They are used for detemining the routes that packets will follow from a source machine to a destination machine.
        - For static hosts, we can use its IP address for very long times, since the location dependent IP address does not have to be changed, since a static host do not change location.

Problems with Internet for Mobility

- When mobile hosts come into picture in Internet:
  - We need a location-independent identifier for the mobile hosts so that any user who wants to contact to the mobile host should be able to use this identifier to send information to the mobile host without getting bothered with the current location of the mobile.
  - We also need a new location-dependent IP address (all IP addresses are location-dependent) for a mobile host when it moves to a new location in order to route the packets destined for the mobile to the new location so that the mobile can receive them at the new location.
- Hence, a single IP address for the a mobile host can not serve both purposes (*identity* and *location/routing*) at the same time.

Mobile IP Approach

- Use two IP addresses per mobile host
  - One permanent IP address (also called home-address)
    - ❑ Used for *Identification*
  - An other IP address that is changing depending on the current location the mobile host (called care-of-address)
    - ❑ Used for *Routing*
- The binding (association) between these two IP addresses are kept at a well-known location, called home agent.

Why DHCP is not enough

- DHCP: Dynamic Host Configuration Protocol
  - An Internet Protocol that allows host that does not have an IP address to obtain an IP address and other configuration information when it connects to a network at a new location.
    - Network to be connected can be for example an Ethernet link
    - Network to be connected should support DHCP protocol
    - The mobile host should support DHCP protocol
  - The configuration info that can be obtained via DHCP at the new location includes:
    - A registered IP address
    - Subnet mask of the network
    - Local DNS server IP addresses (primary and secondary IP addresses), ...

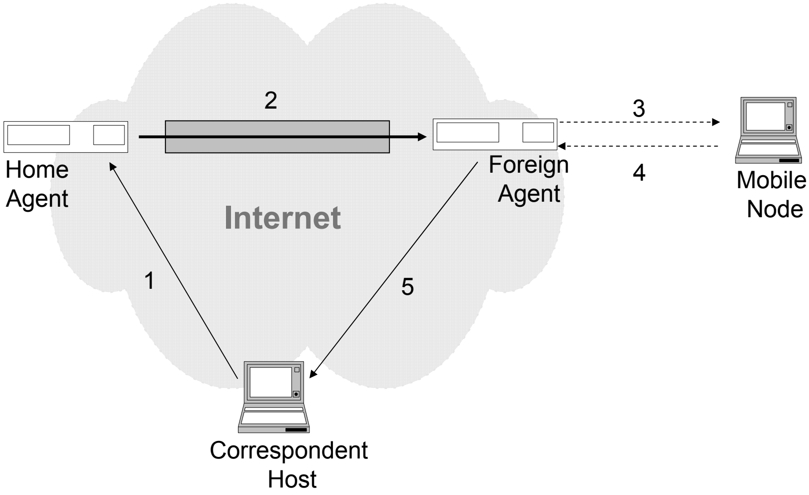
Example

- Assume we have DHCP support in CS department, Math department and dormitories.
  - ❑ Assume you have a laptop that has DHCP support installed.
  - ❑ You don’t need to obtain an IP address from BCC in this case.
  - ❑ You don’t need to bother with network configuration of your laptop.
  - ❑ You will just plug-in your laptop to an Ethernet jack at CS department, at Math department, or at your dormitory and you will be online instantly and easily.
  - ❑ You can move around between CS and Math departments and your dormitory together with your laptop and get connected to the network.
- Disadvantage
  - You have to reboot you computer whenever you connect it to a new network (ethernet jack at a new location). All applcations have to be restarted.
  - You laptop obtains a new IP address at the new location from DHCP server. You can connect to outside world with this new IP address.
    - ❑ However, Your friends wil not able to contact to you.
  - Mobility is not seamless.

DHCP does not provide seamless mobility

- Since you obtain a new IP address a every new location, applications has to be restarted
  - Restart is not problem for web page access
  - Restart is problem for telnet and ftp sessions and some other network and TCP applications.
- Other people can not connect to you when you move to a new location unless they learn your new IP address
  - You have to call them and let your IP address at every move!!!
  - DNS servers are not dynamic enough currently to update the binding between your machine's domain name (host name) and its IP address. This binding will be stale when you move to a new location. Your friend who wants to contact to you and uses your machine's host name, will have the old IP address returned from the DNS server. Hence the packets (messages) he will sent will be routed to your old IP address.

Mobile IP Protocol Overview



Mobile IP Functions

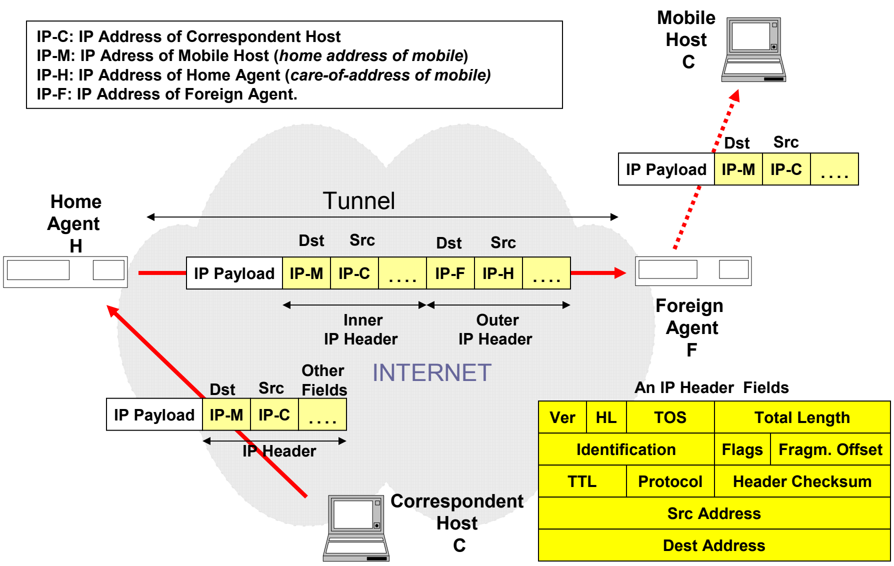
- Agent Discovery
  - When a mobile node moves into a new subnetwork (or network), It has to discover the foreign agent in that network
    - For this, mobile agents (home and foreign) advertise their presence periodically using ICMP messages.
- Registration
  - When a mobive moves to a new network and obtains a new care-of-address there, ıt has to register that address with the home agent (binding), so that home agent knows where to forward the packets aimed for mobile.
    - Registration should be secure
- Tunneling
  - When packet aimed for mobile are intercepted by home agent, they are forward to the current location (care-of-address) of the mobile using a mechanism called Tunneling
    - There are various forms of tunneling: IP-IP, Minimum Encapsulation, GRE, etc.

Example

- A correspondent host C wants to send an IP packet to a mobile host M.
  - It generated the IP packet so that the IP packet has destination address equal to mobile’s home address
  - The IP packet is send to the mobile’s home address
  - Routers forward the packet using normal Internet routing mechanisms to the home network of the mobile.
  - Assume mobile is away from home network and currenty is located in a foreign network. Hence mobile will not be able to receive (capture) the packet that is sent to the mobile’s home network.
  - A home agent located in the mobile’s home network will intercept the packet aimed for mobile
    - This interception is done with the help of proxy ARPing.
  - Home agent will know the whereabouts of the mobile, if the mobile has registered with the home agent previously.

Example – continued.

- Home agent will encapsulate the IP packet using IP-IP encapsulation (tunneling) method and will send the encapsulated IP packet to the new location (care-of-address) of the mobile. The new location is the foreign network that the mobile currently resides in.
- The encapsulated IP packet will be transported to the care-of-address of the mobile using normal Internet routing mechanisms.
  - Care-of-address can be the IP address of a foreign agent or the new IP address of the mobile at thew new location obtained via methods like DHCP, etc. In this case the foreign agent could be co-located at the mobile host.
- The holder of the care-of-address (a foreign agent) will receive the encapsulated IP datagram, wil strip off the outer header (decapsulate) and will forward the original IP packet to the mobile host.
- The mobile host will receive the packet as it is coming from a correspondent host directly without going through the home agent (if foreign agent functionality is not co-located at the mobile host).

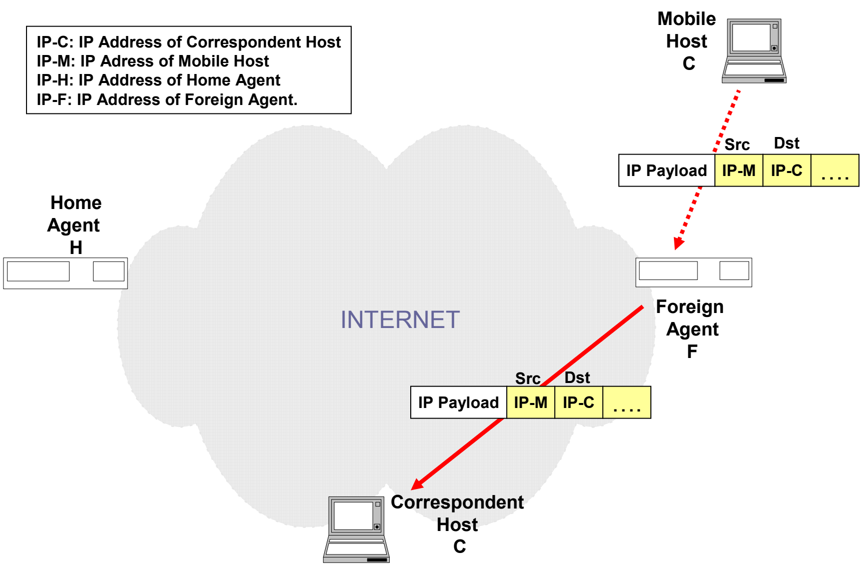


IP-C: IP Address of Correspondent Host
IP-M: IP Adress of Mobile Host (*home address of mobile*)
IP-H: IP Address of Home Agent (*care-of-address of mobile*)
IP-F: IP Address of Foreign Agent.

An IP Header Fields

<table>
<tr><td>Ver</td><td>HL</td><td>TOS</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragm. Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Src Address</td></tr>
<tr><td colspan="5">Dest Address</td></tr>
</table>

Packet Transport from a Correspondent Host to a Mobile



IP-C: IP Address of Correspondent Host
IP-M: IP Adress of Mobile Host
IP-H: IP Address of Home Agent
IP-F: IP Address of Foreign Agent.

Packet Transport from a Mobile to a Correspondent Host

Mobile Agent Discovery

- How a mobile node discovers the home and foreign agents when it travels?
- Agents periodically broadcast their presence (advertisement) on a link (a wireless link – 802.11, or a wired link – ethernet)
    - These broadcasts are agent advertisement messages.
- A mobile node receiving the advertisement understand from the IP addresses included in the advertisement:
    - Whether it is in the home network or not?
    - Whether it has moved to new location or not.
  - This understanding is at the IP level
      - (A mobile already knows that it has moved at the physical link level if has moved).

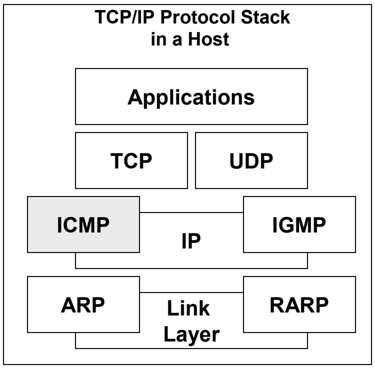
Mobile Agent Discovery

- An agent advertisement message is an ICMP router advertisement message with special extension.
- The special extension is called Mobility Agent Extension.

Agent Advertisement Message

<table>
<tr><th>0</th><th></th><th>8</th><th>16</th><th>31</th><th></th></tr>
<tr><td>Ver</td><td>HL</td><td>TOS</td><td colspan="2">Total Length</td><td rowspan="5">IP Header</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragm. Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Src Address</td></tr>
<tr><td colspan="5">Dest Address</td></tr>
<tr><td colspan="2">Type</td><td>Code</td><td colspan="2">Checksum</td><td rowspan="2">ICMP Router Advertisement Message</td></tr>
<tr><td colspan="2">N_{Addr}=0</td><td>Addr Size</td><td colspan="2">Lifetime</td></tr>
<tr><td colspan="2">Type</td><td>Length</td><td colspan="2">Sequence Number</td><td rowspan="3">Mobility Agent Extension</td></tr>
<tr><td colspan="3">Lifetime</td><td>Flags</td><td>Reserved</td></tr>
<tr><td colspan="5">Zero or more care-of-addresses
..........</td></tr>
</table>

FLAGS
R: Registration requires (with the foreign agent)
B: Foreign agent is busy
H: The agent is home agent.
F: The agent is foreign agent
M: Minimum encapsulation
G: GRE encapsulation
V: Van Jacobson Header Compression



Registration

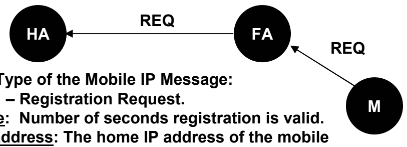
- After a mobile detects at the IP (ICMP) layer that it has moved to a new location, it starts registration procedure with the home agent.
  - The aim of the registration is to let the home agent know mobile's current care-of-address. Mobile obtains this care-of-address ether from the foreign agent or from a server like DHCP server.
- Registration procedure consists of sending a Registration Request Message from mobile to home agent and a Registration Reply Message from home agent to mobile
- Registration messages has to go through Foreign agent.
  - Foreign Agent just forwards these registration messages back and forth
  - Foreign agent is a passive entity in registration. .
- Registration messages sent over UDP to port number 434.

Registration Request

0 8 16 31

Type	Flags	Lifetime
Home address		
Home agent		
Care-of--address		
Identification		
Extensions		

Registration Request Format

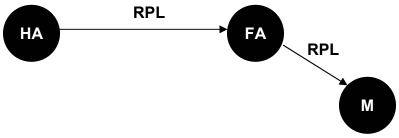


Type: Type of the Mobile IP Message:
1 – Registration Request.
Lifetime: Number of seconds registration is valid.
Home address: The home IP address of the mobile
Home agent: The IP address of the home agent.
Care-of-address: The current IP address of the mobile – this is then end of the tunnel.
Identification: Used for replay protection.
Extensions: Security extensions can be added to protect from malicious people.

Flags:
S: Simultaneous binding.
B: Broadcast – Home agent will tunnel broadcast datagrams to the mobile
D: Mobile node is using *a collocated* care-of-address – that means there is no foreign agent and mobile node will decapsulate the packets itself.
M: Mobile node requests the home agent to encapsulate the packets using Minimal Encapsulation
G: Mobile node requests the home agent to encapsulate the packets using GRE Encapsulation

IP Header	UDP Header	Mobile IP Message	Extensions

Registration Reply



0 8 16 31

Type	Code	Lifetime
Home address		
Home agent		
Identification		
Extensions		

Registration Reply Format

Type: 3 – Registration Reply
Code: Indicates the result of registration
Some code values:

0	registration accepted
66	insufficient resources at foreign agent
70	poorly formed request
130	insufficient resources at home agent
131	mobile node failed authentication

Lifetime: The granted life time by home agent for registration

Care-of-Address Types

- Normal Care-of-address
  - The care-of-address that mobile obtains at a new location is the IP address of a foreign agent serving at that new location.
    - Registration and communication has to go through foreign agent
- Collocated care-of-address
  - There is no separate foreign agent present at the new location
  - Mobile obtains an IP at the new location through some standard mechanisms like DHCP.
  - This IP address is called collocated IP address.
  - The foreign agent functionality is executed at the mobile node itself.
    - The mobile node decapsulates the tunneled packets coming from home agent.
  - Registration and communication is done directly between mobile and home agent.

Securing the registration procedure

- Security problem
  - Fraudulent registrations should be detected.
    - A bad person can send registration packets to home agent as if the packets are coming from a legitimate mobile user.
    - In this way, the bad user can redirect the traffic destined to mobile node to itself and obtain the packets.
    - Hence we need authentication
- There are three authentication extensions defined for Mobile IP
    - The mobile-home authentication extension
    - The mobile-foreign authentication extension
    - The foreign-home authentication extension.

Securing the registration procedure

0	8	16 31
Type	**Length**	**SPI**
SPI….continued		**Authenticator**
Authenticator…..		

Mobile IP Authentication Extension Added to the Registration Request Message

Type: 32 – Mobile-Home authentication extension
33 – Mobile-Foreign authentication extension
34 – Foreign-Home authentication extension
SPI: Security Parameter Index. Defines the security context (algorithm, mode, key) to computer the authenticator.
Authenticator: variable length.

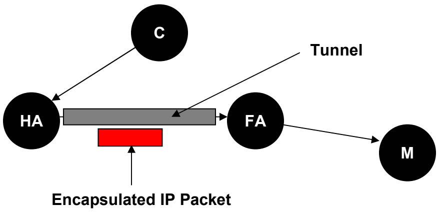
Default Authentication Algorithm:

Keyed-MD5 in prefix-suffix mode
128 bit authenticator: message digest of the registration message.
Computer over:

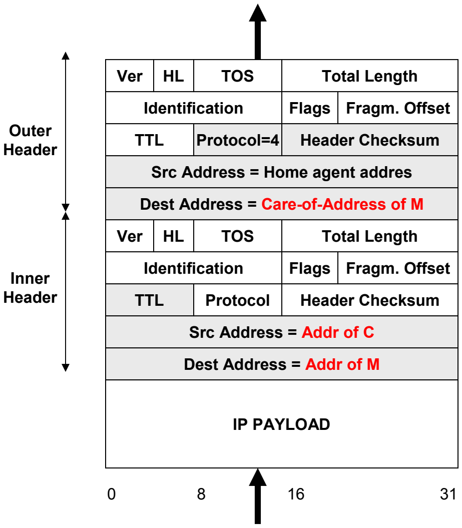
shared secret key,
spi index,
protected fields of registration message,
shared secret again.

Routing and Tunneling

- When a correspondent host sends an IP packet to a mobile (to its home address), packet is routed first to home agent of mobile through normal routing.
- Home agent intercepts the packet and encapsulates it and tunnels it to the care-of-address (tunnel exit point) of the mobile.
  - The encapsulated packet is delivered to the care-of-address using normal routing.
- There are various encapsulation methods:
  - IP-IP Encapsulation
  - Minimal Encapsulation
  - GRE (Generic Routing Encapsulation) Encapsulation.



IP-IP Encapsulation at Home Agent

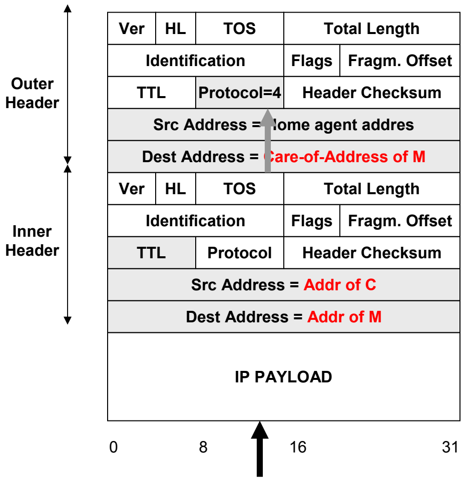


Ver	HL	TOS	Total Length	
Identification			Flags	Fragm. Offset
TTL		Protocol=4	Header Checksum	
Src Address = Home agent addres				
Dest Address = Care-of-Address of M				
Ver	HL	TOS	Total Length	
Identification			Flags	Fragm. Offset
TTL		Protocol	Header Checksum	
Src Address = Addr of C				
Dest Address = Addr of M				
IP PAYLOAD				

Home agent encapsulated the IP Packet inside an other IP header and Sends it to the care-of-address of mobile

An IP packet is received at the Home agent from a correspondent host for a mobile host.

IP-IP Decapsulation at the Care-of-Address



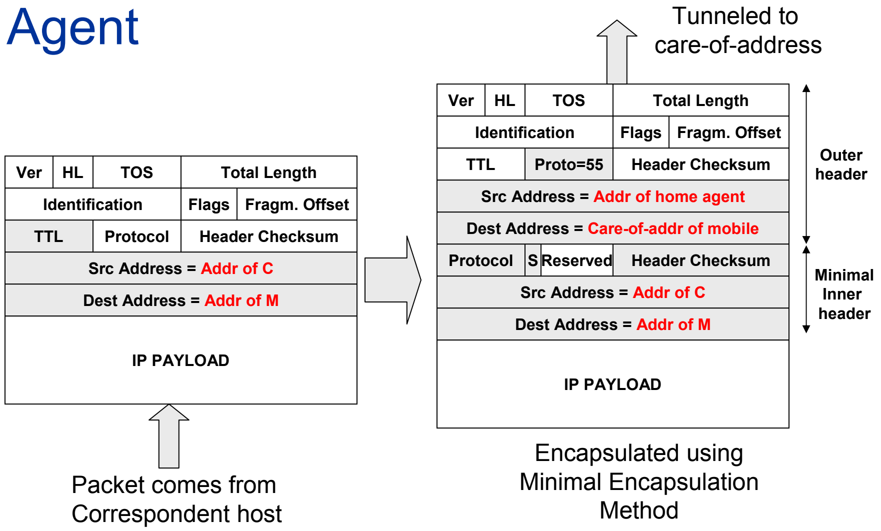
Ver	HL	TOS	Total Length
Identification		Flags	Fragm. Offset
TTL		Protocol=4	Header Checksum
Src Address = Home agent addres			
Dest Address = Care-of-Address of M			
Ver	HL	TOS	Total Length
Identification		Flags	Fragm. Offset
TTL		Protocol	Header Checksum
Src Address = Addr of C			
Dest Address = Addr of M			
IP PAYLOAD			

An encapsulated IP packet is received at the foreign agent (or at the mobile Itself for a collocated care-of-address).

Receiver understands that the packet is IP-IP encapsulated by looking to the protocol field (which is 4).

Receiver forwards (not routes) the decapsulated IP packet to the mobile node using link-level mechanisms!

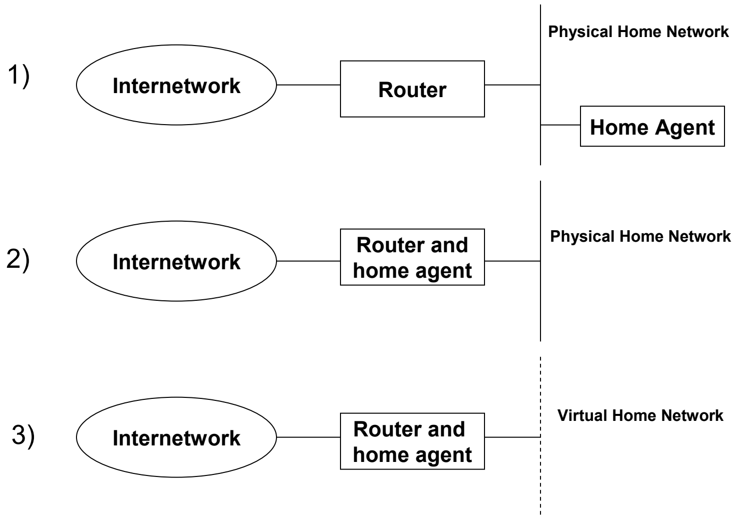
Minimal Encapsulation at Home Agent


Tunneled to care-of-address
Outer header
Minimal Inner header
Packet comes from Correspondent host
Encapsulated using Minimal Encapsulation Method

Ver	HL	TOS	Total Length
Identification		Flags	Fragm. Offset
TTL		Protocol	Header Checksum
Src Address = Addr of C			
Dest Address = Addr of M			
IP PAYLOAD			

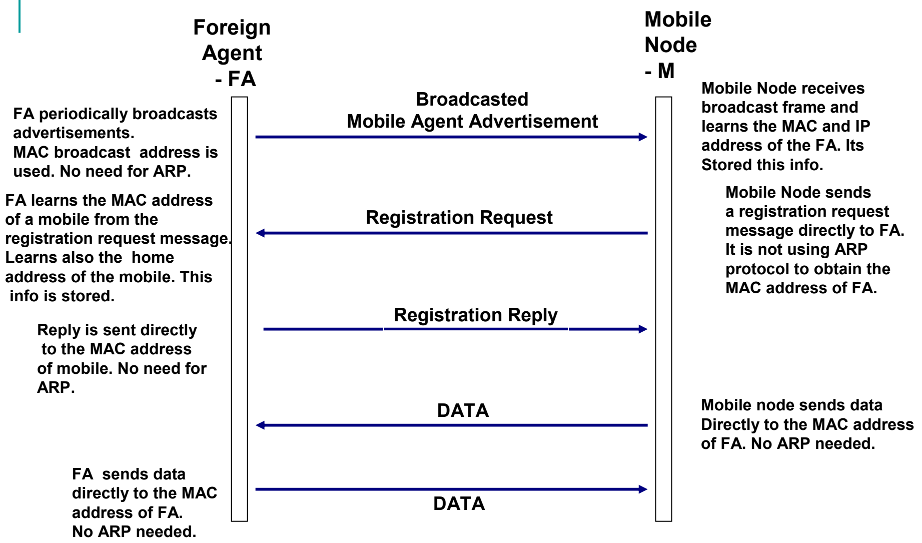
Ver	HL	TOS	Total Length
Identification		Flags	Fragm. Offset
TTL		Proto=55	Header Checksum
Src Address = Addr of home agent			
Dest Address = Care-of-addr of mobile			
Protocol	S	Reserved	Header Checksum
Src Address = Addr of C			
Dest Address = Addr of M			
IP PAYLOAD			

Home Network Configurations



Sending packets between mobile and foreign agent

- When a mobile moves to a new location, a foreign should be broadcasting (IP and link layer broadcast) advertisements on the link (sub-network).
- Mobile will be able to receive this broadcast message and will learn:
  - The IP address of the foreign agent (this will be the care-of-address of the mobile most of the time).
  - The hardware (MAC or link-level address) of the foreign agent.
- When mobile sends a registration packet through this foreign agent, the foreign agent will learn:
  - The home address of the mobile
  - The hardware (MAC or link level) address of the mobile.
    - The registration packet will be sent directly to the foreign agent by using the MAC address of the foreign agent (No need to do ARP request).



FA periodically broadcasts advertisements.
MAC broadcast address is used. No need for ARP.

Mobile Node receives broadcast frame and learns the MAC and IP address of the FA. Its Stored this info.

Mobile Node sends a registration request message directly to FA. It is not using ARP protocol to obtain the MAC address of FA.

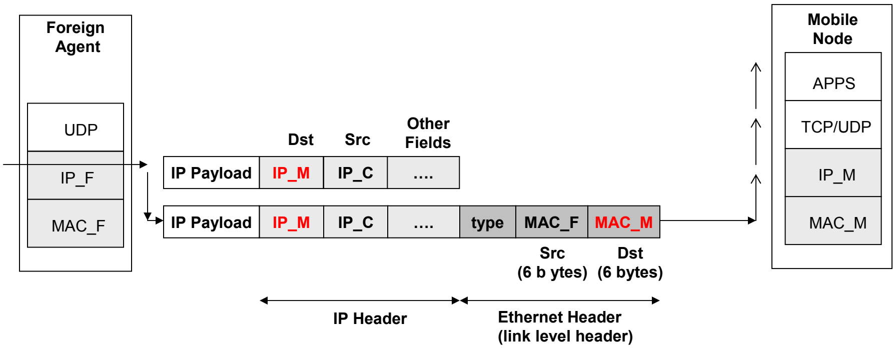
FA learns the MAC address of a mobile from the registration request message. Learns also the home address of the mobile. This info is stored.

Reply is sent directly to the MAC address of mobile. No need for ARP.

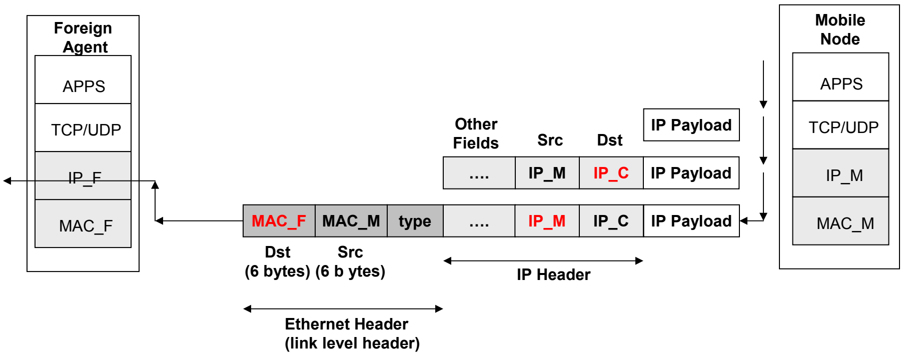
Mobile node sends data Directly to the MAC address of FA. No ARP needed.

FA sends data directly to the MAC address of FA. No ARP needed.

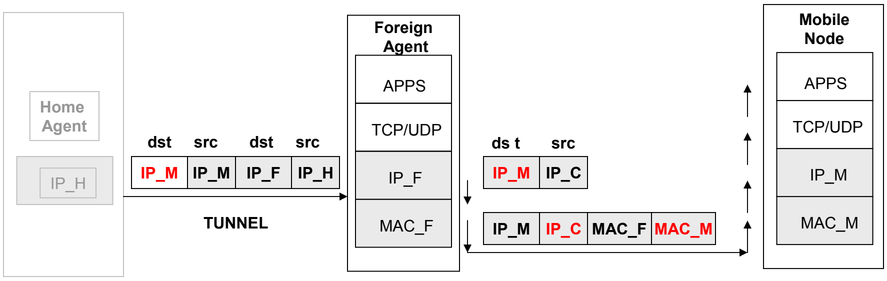
Sending Data from Foreign Agent to Mobile



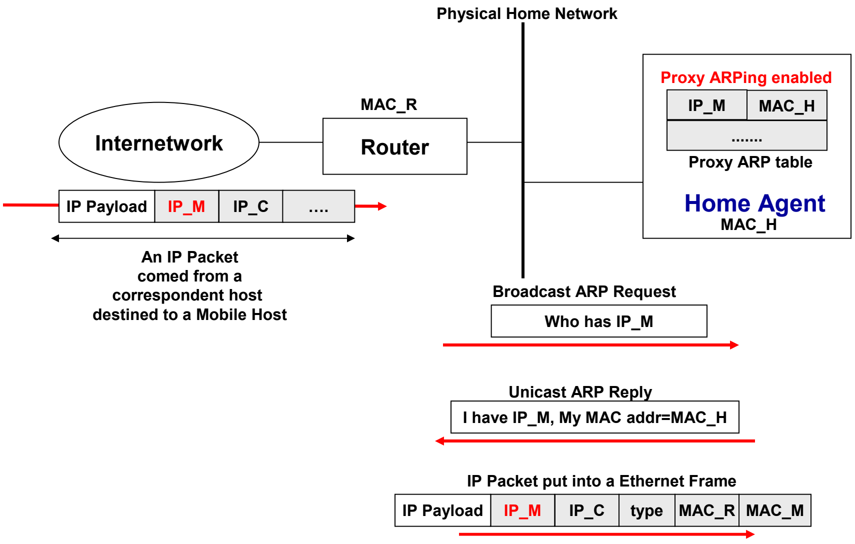
Sending Data from Mobile to Foreign Agent



Decapsulation again



How to attract packets at the Home network



Physical Home Network

Internetwork

MAC_R

Router

Proxy ARPing enabled

IP_M	MAC_H
…….	

Proxy ARP table

Home Agent
MAC_H

IP Payload	IP_M	IP_C	….

An IP Packet
comed from a
correspondent host
destined to a Mobile Host

Broadcast ARP Request

Who has IP_M

Unicast ARP Reply

I have IP_M, My MAC addr=MAC_H

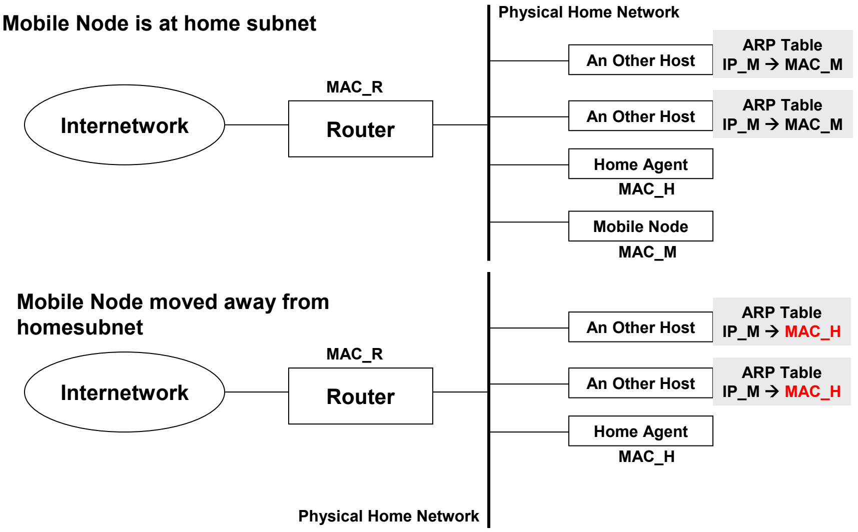
IP Packet put into a Ethernet Frame

IP Payload	IP_M	IP_C	type	MAC_R	MAC_M

Proxy ARPing

- The packet comes to the last router that the home subnetwork is connected to.
- The router will try ro resolve the IP address of Mobile (IP_M) into the corresponding MAC layer address (Hardware address).
- For this pupose, it will broadcasts an ARP request packet
- Since the mobile is not at home subnet, it will not be able to answer ARP request.
- Home agent will answer instead of the Mobile node. İn order to do this, home agent should
- be configured to do proxy ARPing.
- Home agent replies to the ARP request with an ARP reply, including its MAC address (MAC_H) as the MAC level address corresponding to the IP address of the Mobile.
- The router, upon receiving the ARP reply, will send the IP packet to the MAC address of the home agent.
- In this way, the home agent attracts the IP packets that are destined to the mobile node.

Gratuitous ARP Functionality



Mobile Node is at home subnet

Internetwork

MAC_R

Router

Physical Home Network

An Other Host

ARP Table
IP_M → MAC_M

An Other Host

ARP Table
IP_M → MAC_M

Home Agent
MAC_H

Mobile Node
MAC_M

Mobile Node moved away from homesubnet

Internetwork

MAC_R

Router

An Other Host

ARP Table
IP_M → MAC_H

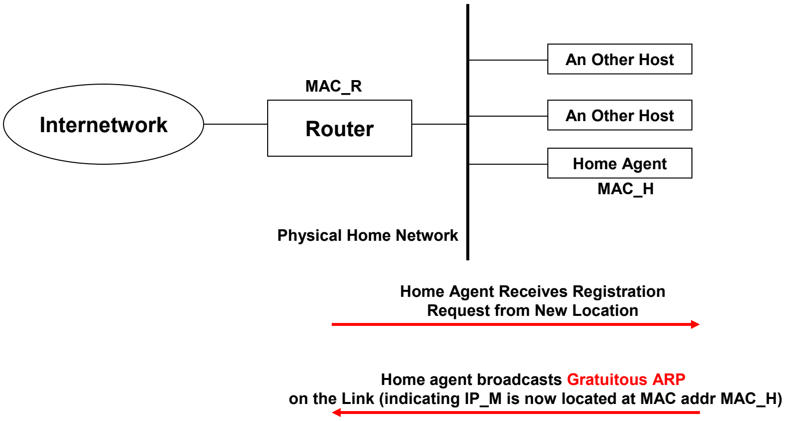
An Other Host

ARP Table
IP_M → MAC_H

Home Agent
MAC_H

Physical Home Network

Gratuitous ARP Operation



Internetwork

MAC_R

Router

An Other Host

An Other Host

Home Agent
MAC_H

Physical Home Network

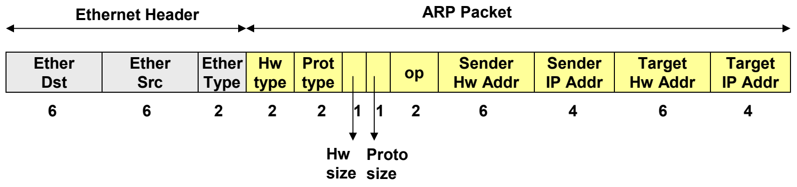
Home Agent Receives Registration
Request from New Location

Home agent broadcasts Gratuitous ARP
on the Link (indicating IP_M is now located at MAC addr MAC_H)

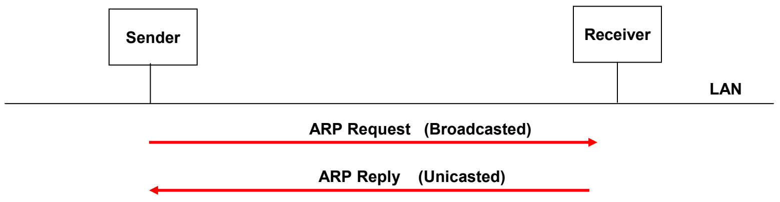
All other hosts on the LAN update their ARP
Caches with binding: IP_M →MAC_H

ARP Packet Format

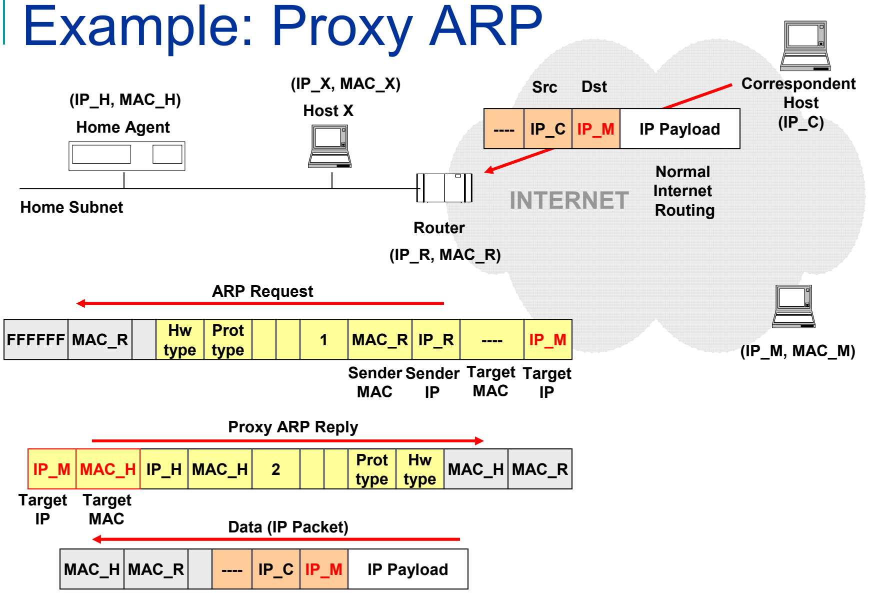
Ether Type: 0x8006 ARP protocol
Op Field: 1 – ARP Request
2 – ARP Reply



Ether Dst	Ether Src	Ether Type	Hw type	Prot type			op	Sender Hw Addr	Sender IP Addr	Target Hw Addr	Target IP Addr
6	6	2	2	2	1	1	2	6	4	6	4



Example: Proxy ARP



----	IP_C	IP_M	IP Payload

ARP Request

FFFFFF	MAC_R		Hw type	Prot type			1	MAC_R	IP_R	----	IP_M
								Sender MAC	Sender IP	Target MAC	Target IP

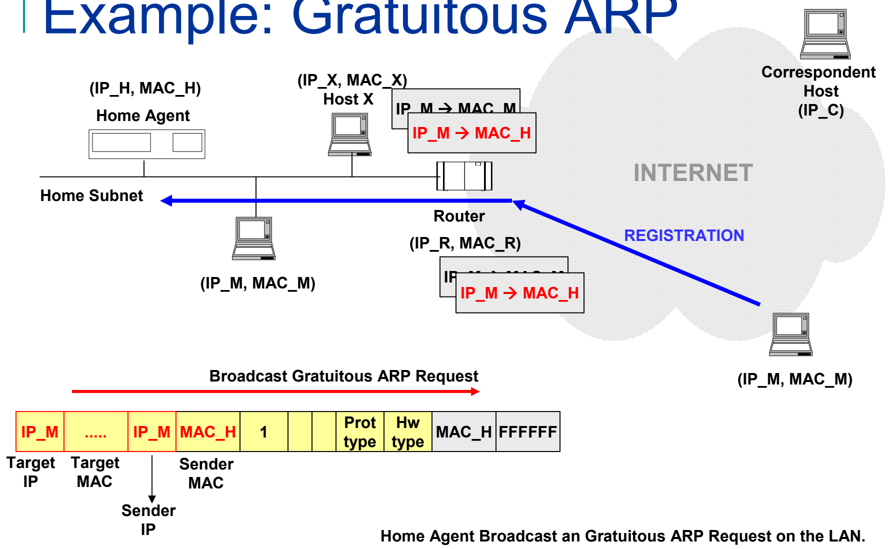
Proxy ARP Reply

IP_M	MAC_H	IP_H	MAC_H	2			Prot type	Hw type	MAC_H	MAC_R
Target IP	Target MAC									

Data (IP Packet)

MAC_H	MAC_R		----	IP_C	IP_M	IP Payload

Example: Gratuitous ARP

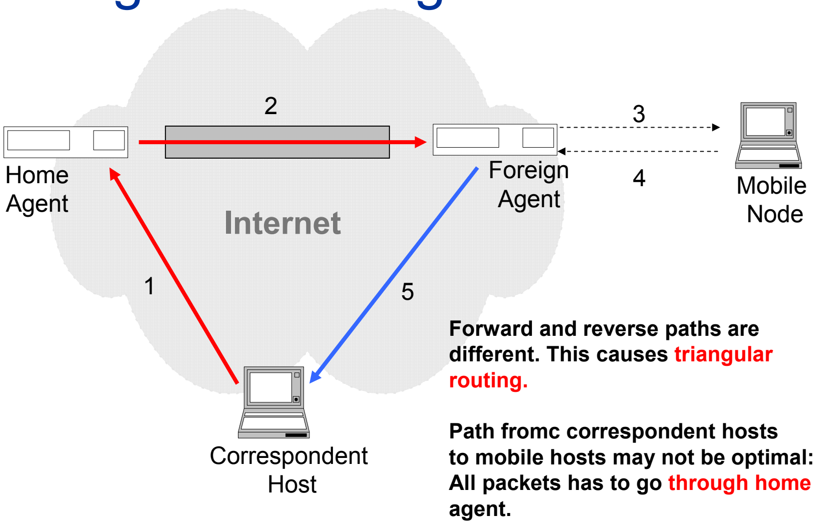


IP_M	.....	IP_M	MAC_H	1			Prot type	Hw type	MAC_H	FFFFFF

Home Agent Broadcast an Gratuitous ARP Request on the LAN.
Any receiveing host will update its ARP cache.

Route Optimization in Mobile IP

Triangular Routing



Forward and reverse paths are different. This causes triangular routing.

Path fromc correspondent hosts to mobile hosts may not be optimal: All packets has to go through home agent.

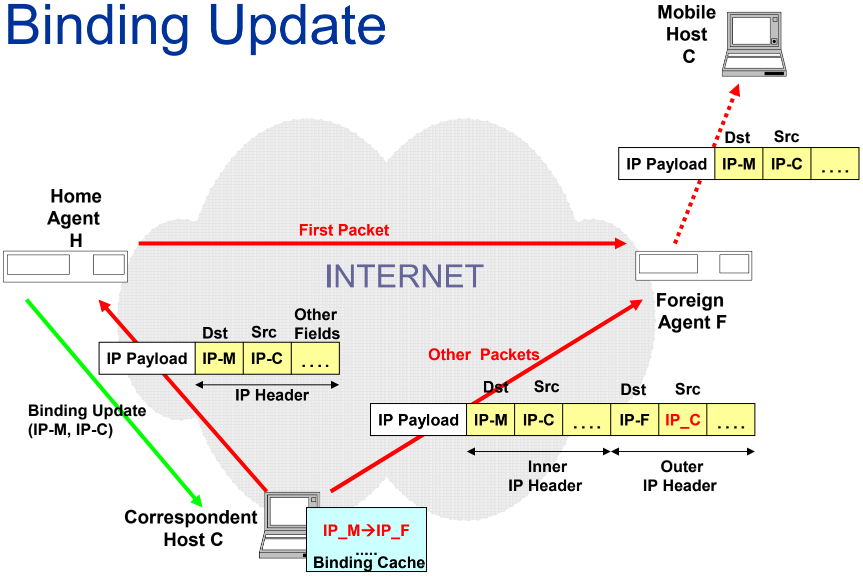
Solution Approach

- Let the correspondent hosts know the current mobility binding or just binding (home address → care-of-address mapping) for mobile hosts.
  - They will store this binding.
  - They will use this binding to directly send the packets to the current location of the mobile.
  - They will again use encapsulation since the care-of-address may not be always collocated at the mobile node (foreign agent should decapsulate).
  - The encapsulated packets will go to the care-of-address directly without going through the home agent.
  - Correspondent hosts should support the binding protocol: Need for modification at correspondent hosts!.

Binding Update

- How does a correspondent host will learn the current binding for the mobile node?
  - Let the mobile node inform the correspondent host!
    - For example when it receives a packet from a correspondent host
  - Let the home agent inform the correspondent host.
    - This is the method chosen, since it is easier to establish security association between a home agent and a correspondent host (Binding update should be secure so the malicious users can not send binding updates to the corresspondent hosts without authenticating themselves).

Binding Update

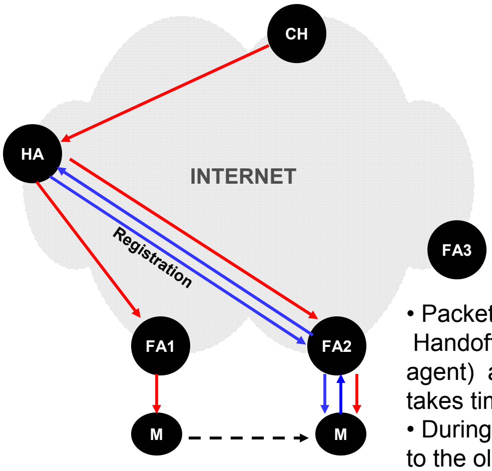


Packet Transport from a Correspondent Host to a Mobile

Binding Warning/Request

- A correspondent host may request a binding Update message from Home agent.
  - Correspondent host sends a Binding Request message and waits for a Binding Update Message.
- A mobile node may warn a Home agent (or some other agent) to send a Binding Update message to a particular host (a correspondent host or to some other host).
  - Mobile node sends a Binding Warning message.
  - Binding warning message include the host IP address (called target address field) to where an Update will be sent.
- A host receiving a Binding Update message should send back a Binding Acknowledgement message.
  - ❑ The sender of Binding Update may retranmit Binding Update if it did not received a Binding Acknowledgement message. The retransmission should occur after a backoff time.
- All binding messages are sent over UDP.

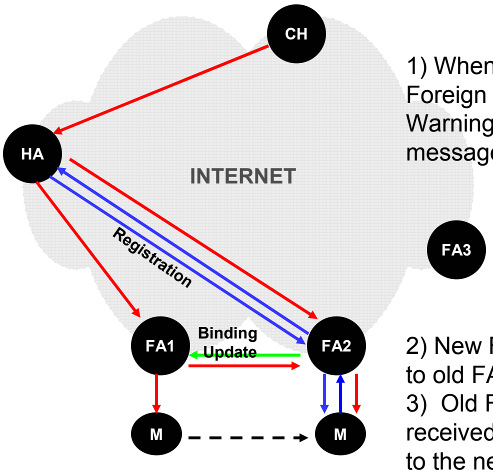
Smooth Handoffs



• Packets may be dropped during handoffs. Handoff to a new base station (or foreign agent) and registration with home agent takes time.

• During this time, packets will be forwarded to the old base station (FA), where the mobile node moved away from.

Smooth Handoffs



1) When M makes handoff, it warns the new Foreign agent (FA2) (by use of a Binding Warning message) to send a Binding Update message to the old FA (FA1).

2) New FA sends a Binding Update message to old FA.

3) Old FA re-encapsulates the Ip packets received from home agent and sends them to the new FA.

Supporting Fast Handoffs in Mobile IP

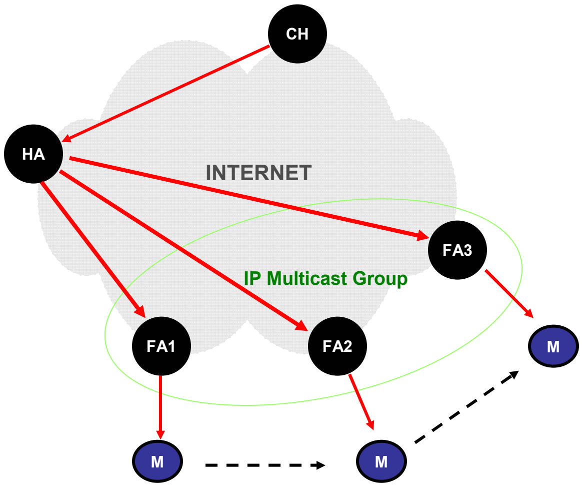
Fast Handoffs

- For highly mobile users, handoffs will be too frequent. Implications of this:
  - Handoffs should be very fast in order to minimize packet delays and packet losses.
  - Registration will be too frequent:
    - Registration causes delay
    - Registration causes extra signaling (control) traffic in the wireless link and infrastructure.
- Two solution approaches to support fast handoffs:
  - Use of IP multicasting
  - Use of hierarchical foreign agents.

Use of IP Multicasting

- A collection of foreign agents in the vicinity of each other join to a multicast group. The group will have a multicast IP address.
- Mobile node will use this multicast IP address as the care-of-address.
- The home agent will send the encapsulated packets for the mobile to this multicast IP address.
- Foreign agents in the multicast group will buffer the received encapsulated IP packets for a while before discarding
  - In this way, when a mobile handoffs from one FA to an other FA (in the same multicast group), it will be able to recover the packets transmitted during handoff from the new FA.

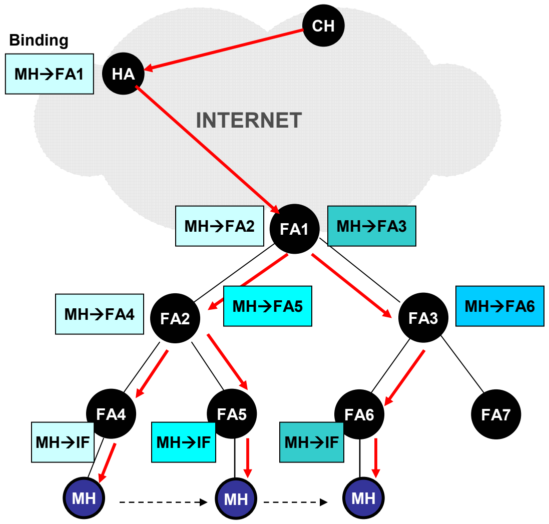
Use of IP Multicasting



Hierarchical Foreign Agents

- Uses a hierarchy of foreign agents between mobile node and home agent.
- Aims is to localize handoffs and registration.
- The hierarchy could be consisting of for example:
  - Base stations (access points) at the lowest level – leaf.
  - <u>Intermediate routers</u> between <u>base stations</u> and <u>campus edge routers</u> in a campus.
  - Campus edge router at the highest level (root) of the foreign agent hierarchy.

Hierarchical Foreign Agents



Hierarchical Foreign Agents

- The following functions of Mobile IP is enhanced:
    - Agent Advertisements
    - Registration
    - Data Forwarding

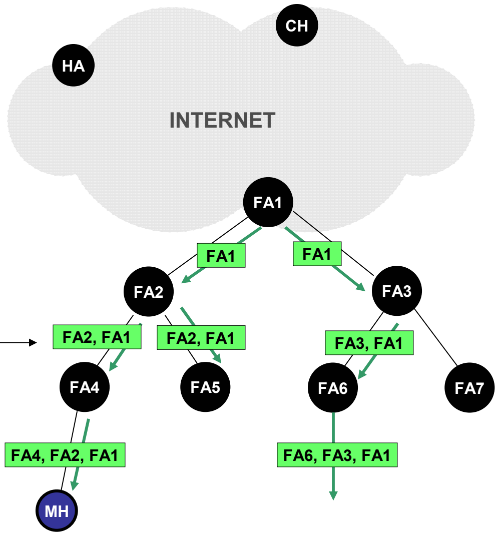
Agent Advertisements

Mobility Agent Extension
to ICMP Router Advertisement

Type	Length	Sequence Number	
Lifetime		Flags	Reserved
Zero or more care-of-addresses ……….			

Agent Advertisement message
Care-of-Address field content

In a message. FAx denotes the IP address
of Foreign Agent X.

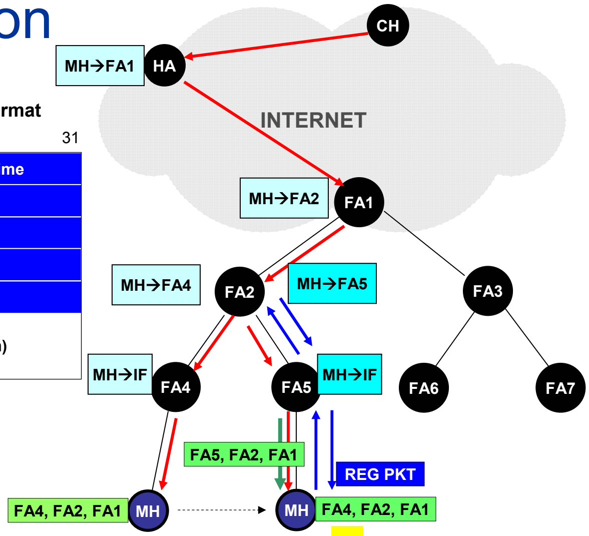


Registration

Registration Request Format

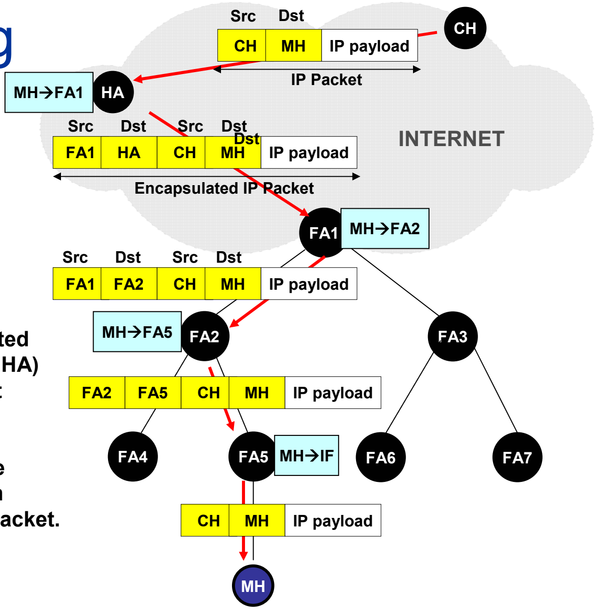
0 8 16 31

Type	Flags	Lifetime
Home address=MH		
Home agent=FA2		
Care-of—address=FA5		
Identification		
Extensions (Authentication Extension) …..		



Compare FA4, FA2, FA1
With FA5, FA2, FA1

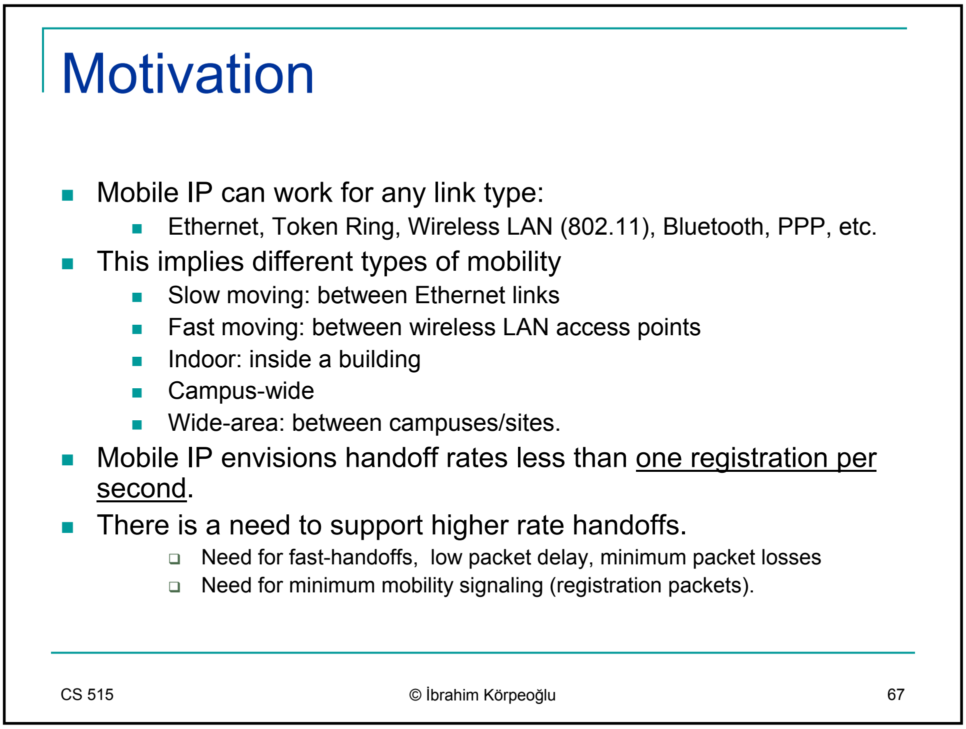
Forwarding



Each FA takes an encapsulated packet from previous FA (or HA) and recapsulates the packet to be sent to the next FA.

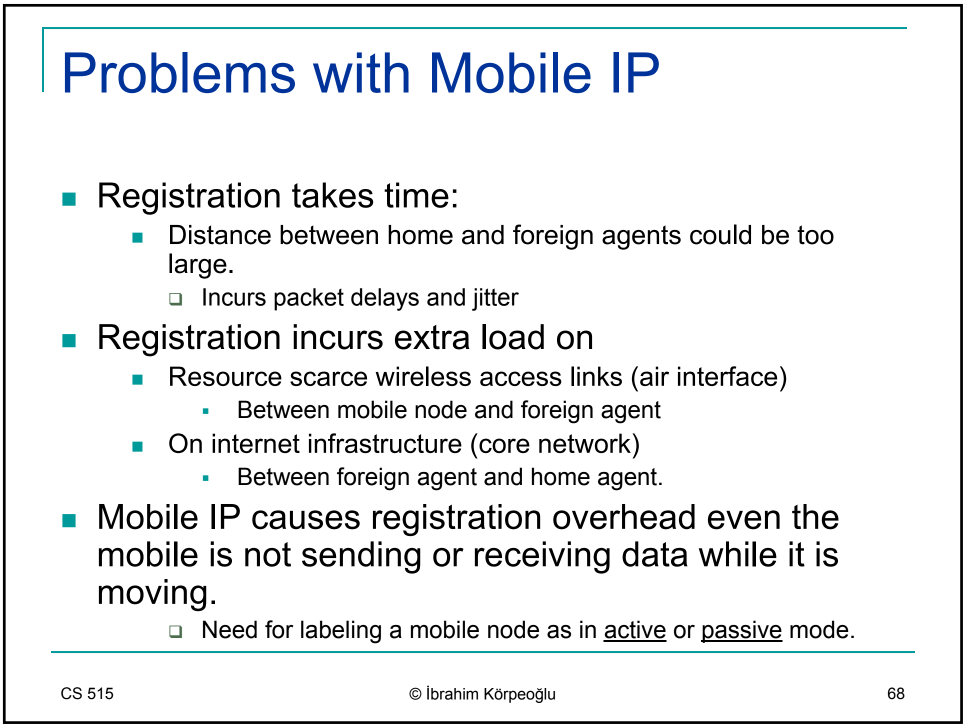
If an FA is the final FA on the way to the mobile node, then it does not recapsulate the packet.

Cellular IP



Motivation

- Mobile IP can work for any link type:
  - Ethernet, Token Ring, Wireless LAN (802.11), Bluetooth, PPP, etc.
- This implies different types of mobility
  - Slow moving: between Ethernet links
  - Fast moving: between wireless LAN access points
  - Indoor: inside a building
  - Campus-wide
  - Wide-area: between campuses/sites.
- Mobile IP envisions handoff rates less than one registration per second.
- There is a need to support higher rate handoffs.
    - Need for fast-handoffs, low packet delay, minimum packet losses
    - Need for minimum mobility signaling (registration packets).



Problems with Mobile IP

- Registration takes time:
  - Distance between home and foreign agents could be too large.
    - Incurs packet delays and jitter
- Registration incurs extra load on
  - Resource scarce wireless access links (air interface)
    - Between mobile node and foreign agent
  - On internet infrastructure (core network)
    - Between foreign agent and home agent.
- Mobile IP causes registration overhead even the mobile is not sending or receiving data while it is moving.
    - Need for labeling a mobile node as in active or passive mode.

Cellular IP Approach

- Use the concept of cellular mobile telephone networks for
  - Handoff management
    - Efficient handoffs with low delay, minimum packet losses.
  - Location tracking
    - *Exact location* is known for active mobiles
    - *Approximate location* is known for passive mobiles
      - Paging is used to learn the exact location for a passive mobile.
  - Passive connectivity
- Based on IP principles: The underlying network is IP.
  - No new packet formats
  - No encapsulation
  - No new address space.

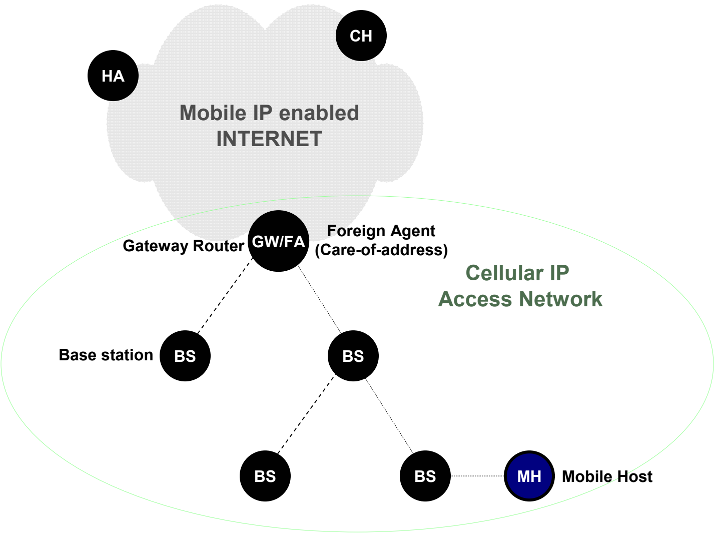
Cellular IP

- Cellular IP can support micro-mobility in
  - Pico-cellular or micro-cellular networks (Personal Area Networks or Wireless LANs)
  - Campus wide networks
  - Multi-cell wireless access networks.
- Can be integrated with Mobile IP to support macro-mobility
  - Mobility between campuses and different administrative domains.

Cellular IP

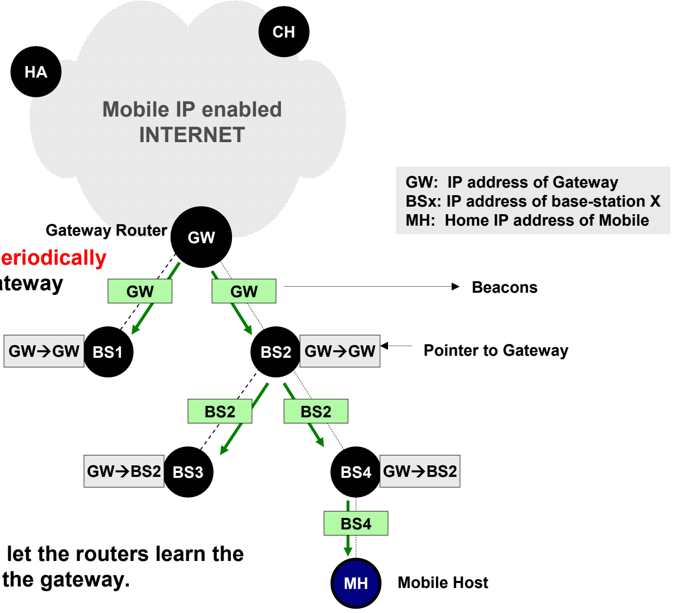
- In a cellular IP network
  - All routing for mobile hosts is done by Cellular IP routing
    - Route distribution and update is done according to Cellular IP protocol.
  - No need to modify the IP packet format or IP forwarding mechanism.
  - Per-host location information is stored in cellular IP network routers for mobile hosts.
- Related Work:
  - Hierarchical Foreign Agents for Mobile IP proposed by IETF
  - Hawaii Project at Lucent/Bell Labs
  - Learning features of Ethernet switches
    - A switch learns the location of traffic sources while its is forwarding the frames.

Cellular IP Network Model


CH
HA
Mobile IP enabled INTERNET
Gateway Router
GW/FA
Foreign Agent (Care-of-address)
Cellular IP Access Network
Base station
BS
BS
BS
BS
MH
Mobile Host

Beacons

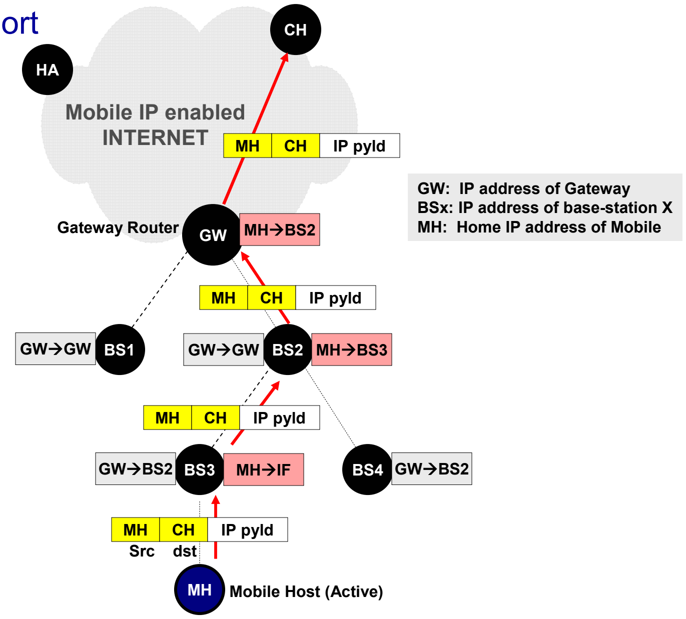
Beacons are sent periodically originating from Gateway



GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Beacons are use to let the routers learn the path to the gateway.

Data Transport From MH To CH

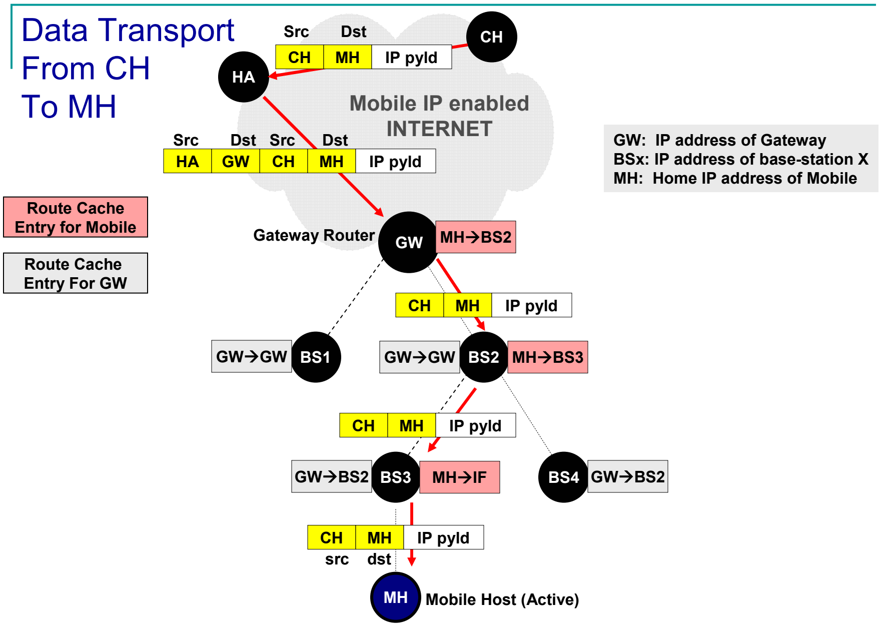


🟥 Route Cache Entry for Mobile

□ Route Cache Entry For GW

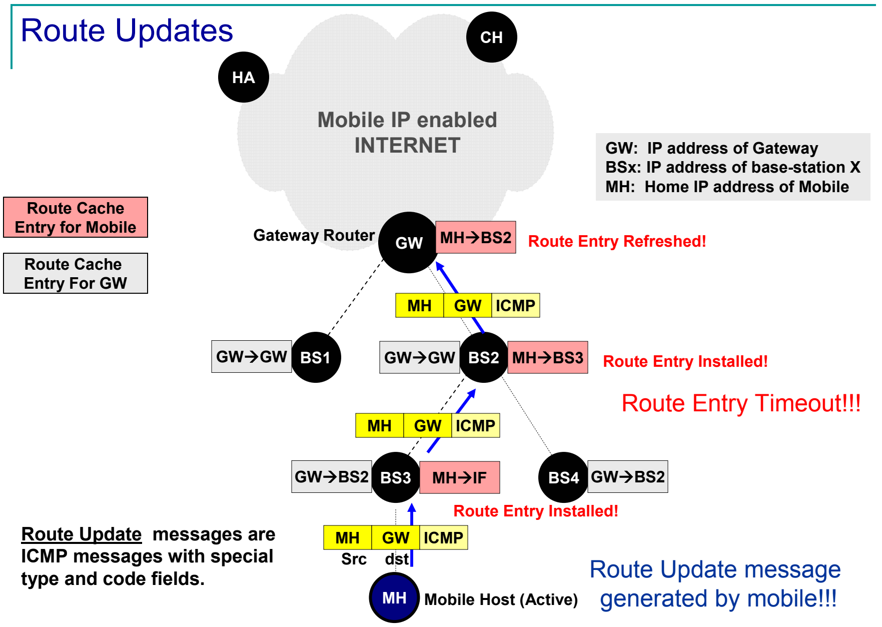
GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Data Transport From CH To MH



GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Route Updates



GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Route Entry Refreshed!

Route Entry Installed!

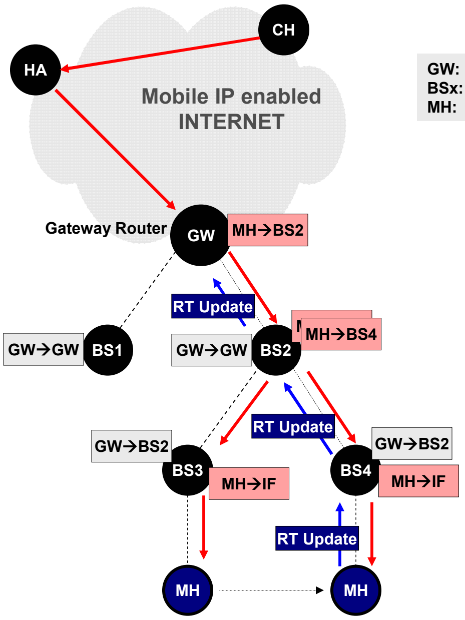
Route Entry Timeout!!!

Route Entry Installed!

Route Update message generated by mobile!!!

__Route Update__ messages are ICMP messages with special type and code fields.

Handoff



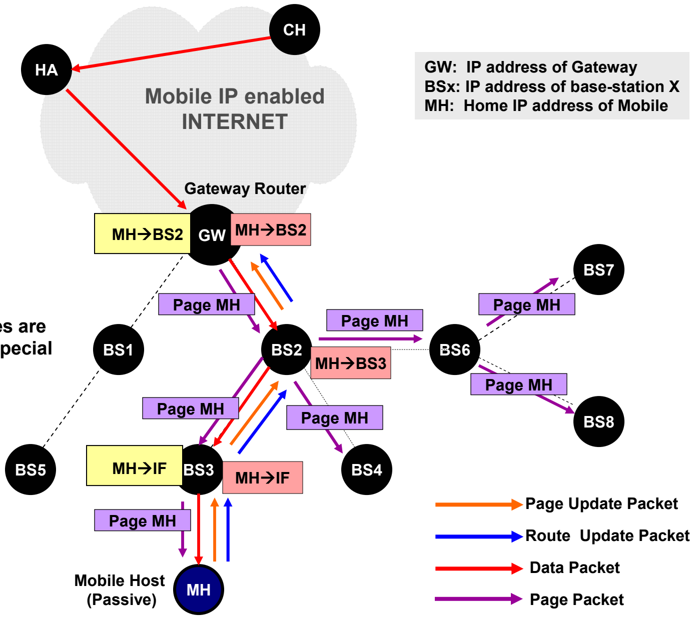
GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Route Cache Entry for Mobile

Route Cache Entry For GW

Route Update Packet
RT Update

Paging



GW: IP address of Gateway
BSx: IP address of base-station X
MH: Home IP address of Mobile

Route Cache Entry for Mobile

Paging Cache

<u>Page Update</u> messages are ICMP messages with special type and code fields.

Page Update Packet
Route Update Packet
Data Packet
Page Packet