King Fahd University of Petroleum & Minerals
Computer Engineering Dept

COE 543 – Mobile and Wireless Networks

Term 111

Dr. Ashraf S. Hasan Mahmoud

Rm 22-148-3

Ext. 1724

Email: ashraf@kfupm.edu.sa

Lecture Contents

1.

Main References

this is the one you are responsible for

Charles E. Perkins, "Mobile IP," IEEE Communications Magazine, May 1997, pp. 84-99.

- Notes for Prof. İbrahim Körpeoğlu of Bilkent University - Bilkent / ANKARA
- Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/ MC SS02 – Chapter 8 material
- Charles E. Perkins, "Mobile IP – Design Principles and Practices," Addison-Wesley, 1997

Background Information

- Internet
- TCP/IP
- Subnet-ing
- ICMP
- ARP
- DHCP

Introduction

- Mobility vs. Portability
- DHCP requirements
- Other solutions
  - E.g. TCP connection migration

Motivation for Mobile IP

Routing
- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?
- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?
- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take to long time
- TCP connections break, security problems

Requirements to Mobile IP (RFC 3220, was: 2002)

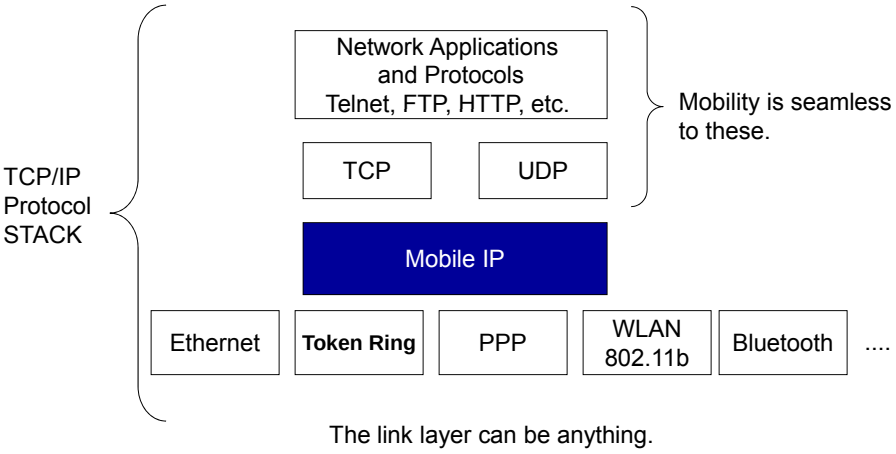
Transparency
- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility
- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security
- authentication of all registration messages

Efficiency and scalability
- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole Internet

Mobile IP



Why we 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.
  - And 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)

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.

Terminology

refer to Perkins's paper for the full list of definitions

Mobile Node (MN)
- system (node) that can change the point of connection to the network without changing its IP address

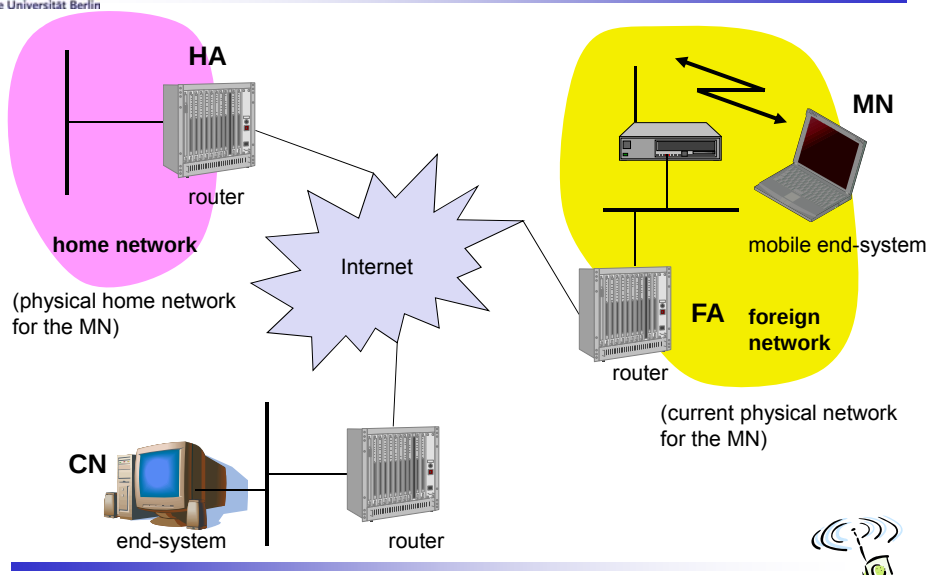
Home Agent (HA)
- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

Foreign Agent (FA)
- system in the current foreign network of the MN, typically a router
- forwards the tunneled datagrams to the MN, typically also the default router for the MN

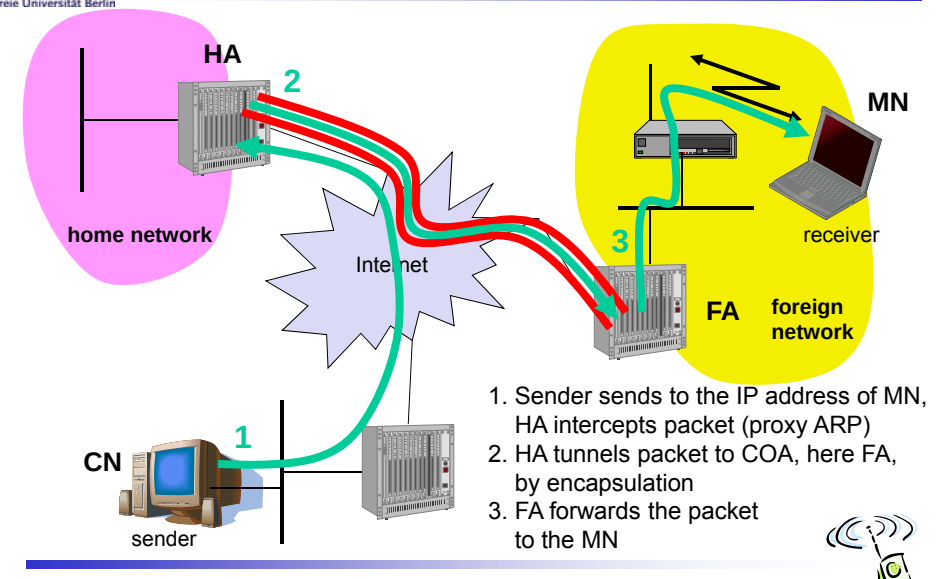
Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

Correspondent Node (CN)
- communication partner

Example network

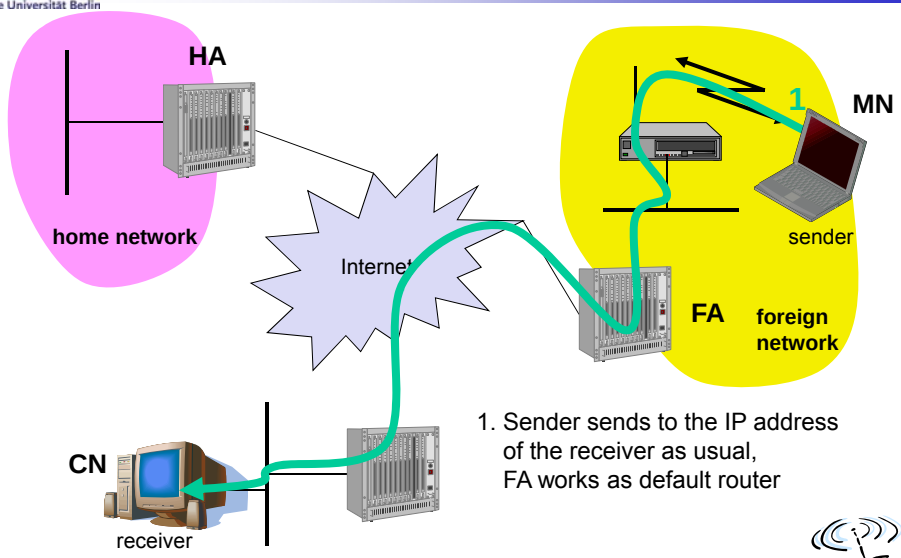


Data transfer to the mobile system

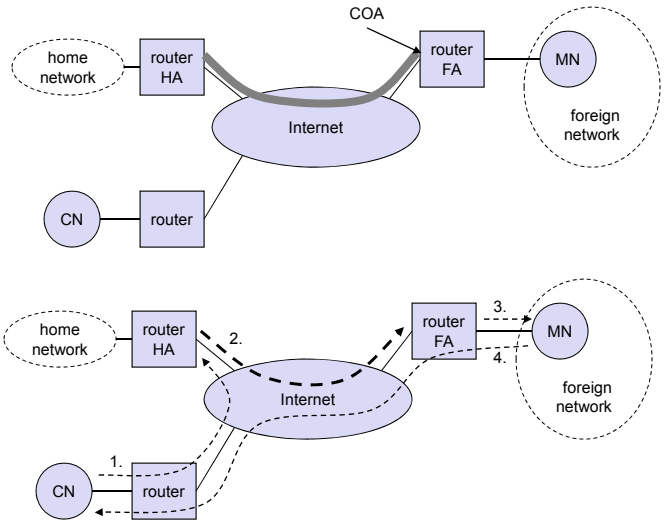


1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



Overview

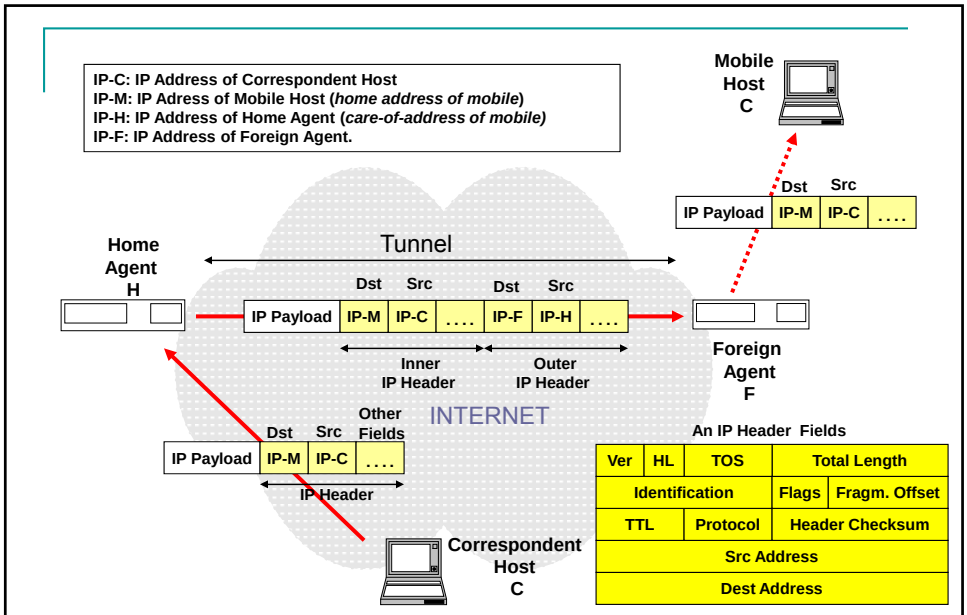


Example

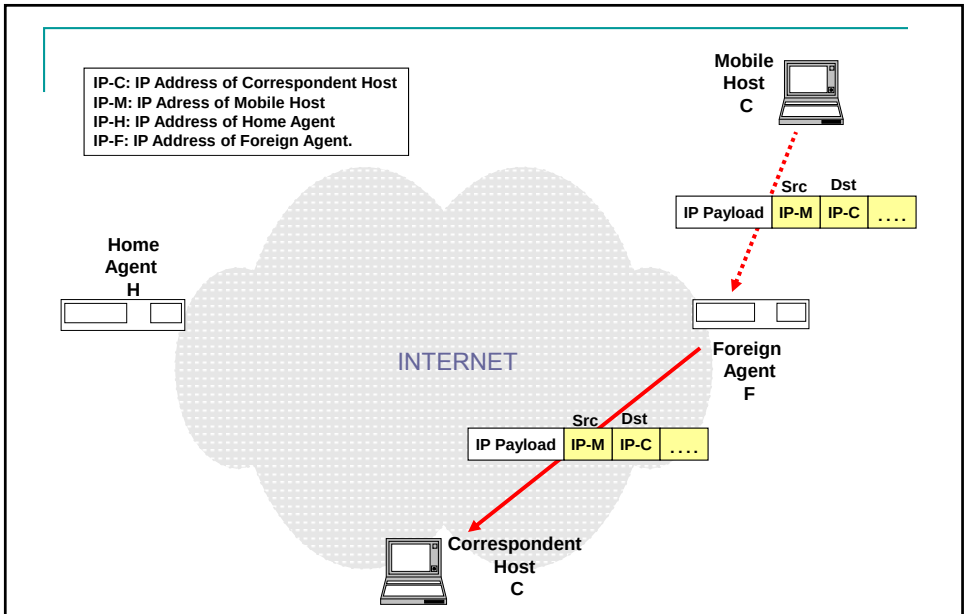
- A correspondent host C wants to send an IP packet to a mobile host M.
  - It generated the IP packet so that the IP packet has destination address equal to mobile's home address
  - The IP packet is send to the mobile's home address
  - Routers forward the packet using normal Internet routing mechanisms 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).



Packet Transport from a Correspondent Host to a Mobile



Packet Transport from a Mobile to a Correspondent Host

Mobile IP Functions

- Agent Discovery – using extension to ICMP
  - 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 – using UDP
  - When a mobile moves to a new network and obtains a new care-of-address there, it 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.

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

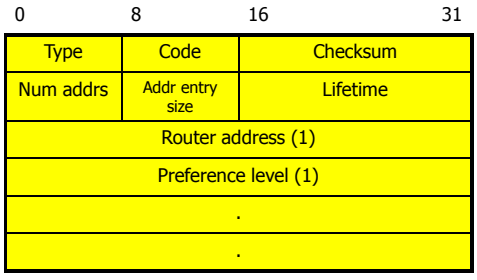
- An agent advertisement message is an ICMP router advertisement message with special extension.
- Original router discovery protocol (ICMP) is specified by RFC 1256
- The special extension is called Mobility Agent Extension.

•No Authentication is required!! – Why?
•A mobile node may also solicit a mobile agent discovery message
• Why?
  • Allow detection of mobility agents
  • Lists one or more care-of-address
  • Informs mobile node of special features of that mobility agent

Router Discovery Protocols - background

- Original router discovery protocol (ICMP) is specified by RFC 1256

- **Type**: 9
- **Code**: 0
- **Checksum**:
- **Num addrs**: the number of router addresses advertised in this message
- **Addr entry size**: the number of 32-bit words of info for each router address (typically 2)
- **Lifetime**: the maximum number of seconds that the router addresses may be considered valid
- **Router address(i)**: i=1..num addrs, the sending router's IP addresses on the interface from which this message is sent
- **Preference level(i)**: i=1..num addrs, the preferability of each corresponding router address as a default router address relative to other router addresses on the same subnet

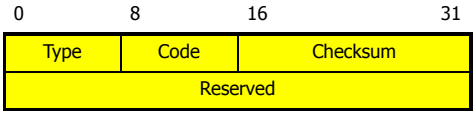


Router Advertisements (From RFC 1256)

Router Discovery Protocols - background

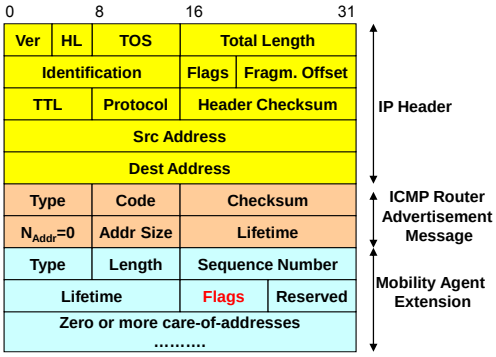
- Router solicitation – when a host needs a timely information

- **Type**: 10
- **Code**: 0
- **Checksum**:
- **Reserved**: sent as 0 – ignored on reception

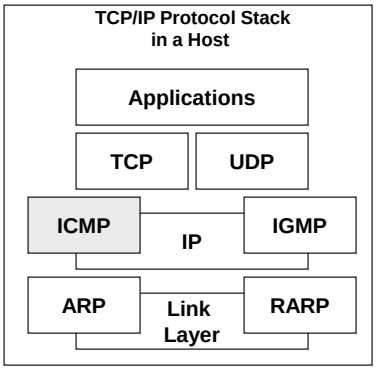


Router Solicitations (From RFC 1256)

Agent Advertisement Message

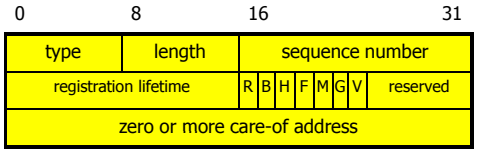


FLAGS
R: Registration required (with the foreign agent)
B: Foreign agent is busy
H: The agent is home agent.
F: The agent is foreign agent
M: Minimum encapsulation
G: GRE encapsulation
V: Van Jacobson Header Compression



Mobility Agent Advertisement Extensions

- **Type**: 16
- **Length**: (6+4*N), where N is the # of care-of addresses advertised
- **Sequence number**: the count of agent advertisement messages sent since the agent was initialized
- **Registration lifetime**: the longest lifetime (measured in seconds) that this agent is willing to access in any registration request; 65535 indicates infinity
- **R, B, H, F, M, G, V**: see previous slide
- **Care-of address**: The advertised foreign agent care-of address provided by this foreign agent. An agent advertisement is required to include at least one care-of address if the F bit is set.



Mobility Agent Advertisement Extension

Registration

Once the mobile node obtains its care-of-address it has to **REGISTER** with the home mobile agent

- 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 Objectives

ALWAYS

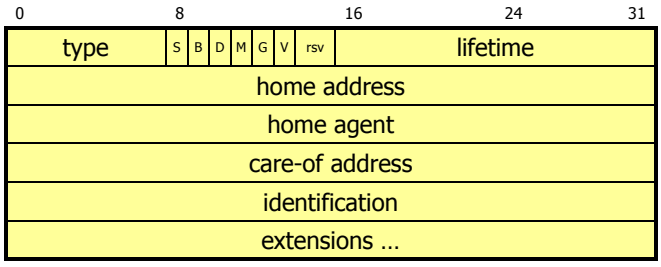
- Request forwarding services when visiting a foreign network
- Inform their home agent of their current COA
- Renew a binding that is due to expire
- De-register when they return home

OPTIONAL

- Discover the address of the home agent if the mobile node is not configured with this info
- Select certain alternative tunneling protocols (minimal encapsulations or GRE) - Required of the use of Van Jacobson header compression
- Maintain multiple simultaneous registration so that a copy of each datagram will be tunneled to each active COA
- De-register certain COAs while retaining others

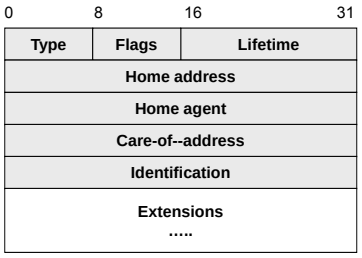
Registration Packet

General Mobile IP Registration Message



Registration request packet format

Registration Request

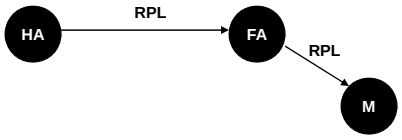


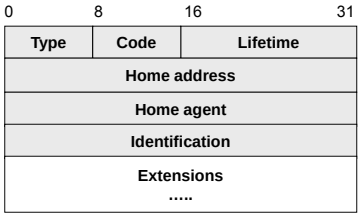
Registration Request Format

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 (retain previous 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

Registration Reply





Registration Reply Format

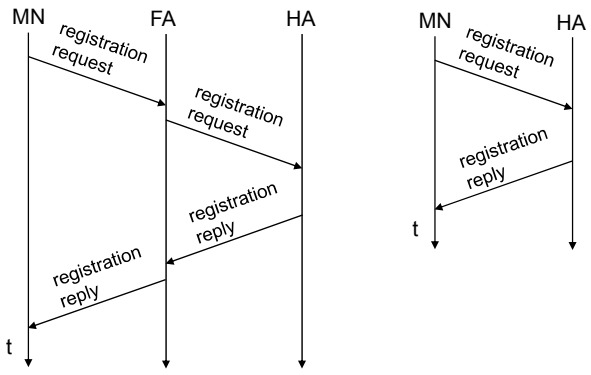
Type: 3 – Registration Reply
Code: Indicates the result of registration
Some code values:
0 registration accepted
66 insufficient resources at foreign agent
70 poorly formed request
130 insufficient resources at home agent
131 mobile node failed authentication
Lifetime: The granted life time by home agent for registration

Identification: depends on the identification in the request

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.

Registration



FA assigned IP as COA

Colocated COA

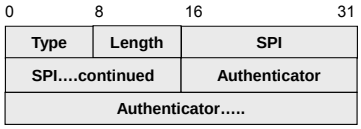
Securing the registration procedure

- 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.

Authentication Overview

- Mobility Security Association = SPI + IP
  - Security Parameter Index (SPI)
  - For mobile node, IP = home address not COA

Securing the registration procedure



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 compute the authenticator.
Authenticator: variable length.

What are the potential dangers?
What are "*replay*" attacks?

Default Authentication Algorithm:

Keyed-MD5 in prefix-suffix mode
128 bit authenticator: message digest of the registration message.
Computed over:
shared secret key,
spi index,
protected fields of registration message,
shared secret again.

Example 1: (section 4.11 of book)

Mobile node IP home address	129.34.78.5
Mobile node's home agent	129.34.78.254
Foreign agent's wireless address	137.0.0.11
Foreign agent coa	9.2.20.11
DHCP-allocated coa	9.2.43.94
Mobile node's source port	1094
Foreign agent's source port	1105
coa registration lifetime	60,000 sec
Home agent granted lifetime	35,000 sec

Example 1: (section 4.11 of book)- 2

Agent Advertisement

IP header fields	ICMP header	Router Adv. fields	Mobile Service Extension
S = 137.0.0.11 D = 255.255.255.255 F = 1	Type = 9 Code 16	…	Lifetime = 60,000 COA = 9.2.20.11

Mobile → Foreign Agent

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.5 D = 137.0.0.11 TTL = 1	S = 1094 D = 434	Type = 1 Lifetime = 60,000 COA = 9.2.20.11 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 302

Example 1: (section 4.11 of book)- 3

Foreign Agent → Home

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 9.2.20.11 D = 129.34.78.254 TTL = 64	S = 1105 D = 434	Type = 1 Lifetime = 60,000 COA = 9.2.20.11 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 302

Home → Foreign Agent

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.254 D = 9.2.20.11 TTL = 64	S = 434 D = 1105	Type = 3 Lifetime = 35,000 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 303

Example 1: (section 4.11 of book)- 4

Foreign Agent → Mobile

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 137.0.0.11 D = 129.34.78.5 TTL = 1	S = 434 D = 1094	Type = 3 Lifetime = 35,000 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 303

Example 2: (section 4.11 of book)

Mobile node IP home address	129.34.78.5
Mobile node's home agent	129.34.78.254
DHCP-allocated coa	9.2.43.94
Mobile node's source port	1094
coa registration lifetime	60,000 sec
Home agent granted lifetime	35,000 sec

Mobile enters a foreign network that contains no foreign agents. The mobile obtains an address from a DHCP server for use as a co-located care-of address. The mobile support minimal encapsulation and GRE.

Example 2: (section 4.11 of book)- 2

Mobile → Home Registration Request

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.5 D = 129.34.78.254 TTL = 64	S = 1094 D = 434	Type = 1 Lifetime = 665535 COA = 9.2.43.94 HA = 129.34.78.254 MA = 129.34.78.5 D.M.G.B = 1,1,1,1	SPI = 302

Home → Mobile Registration Reply

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.254 D = 129.34.78.5 TTL = 64	S = 434 D = 1094	Type = 3 Lifetime = 35000 COA = 9.2.43.94 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 303

Example 3: (section 4.11 of book)

Mobile returns home and wishes to de-register all of care-off addresses with its home agent. The care-off address fields are the same as the mobile node's home address, and the requested (and granted) lifetimes are 0.

Example 3: (section 4.11 of book)- 2

Agent Advertisement

IP header fields	ICMP header	Router Adv. fields	Mobile Service Extension
S = 129.34.78.254 D = 255.255.255.255 H = 1	Type = 9 Code 16	…	… no COAs … Lifetime = 35000

Mobile → Home Agent

IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.5 D = 129.34.78.254 TTL = 1	S = 1094 D = 434	Type = 1 Lifetime = 0 COA = 129.34.78.5 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 302

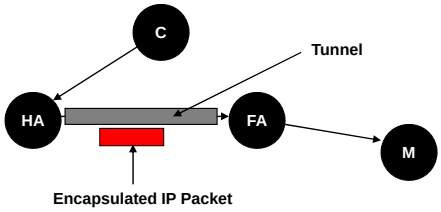
Example 3: (section 4.11 of book)- 2

Home → Mobile

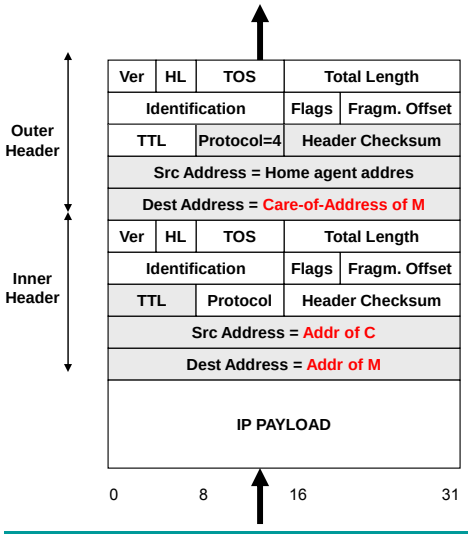
IP header fields	UDP header	Mobile IP msg fields	Authentication Ext.
S = 129.34.78.254 D = 129.34.78.5 TTL = 1	S = 434 D = 1094	Type = 3 Lifetime = 0 COA = 129.34.78.5 HA = 129.34.78.254 MA = 129.34.78.5	SPI = 303

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.



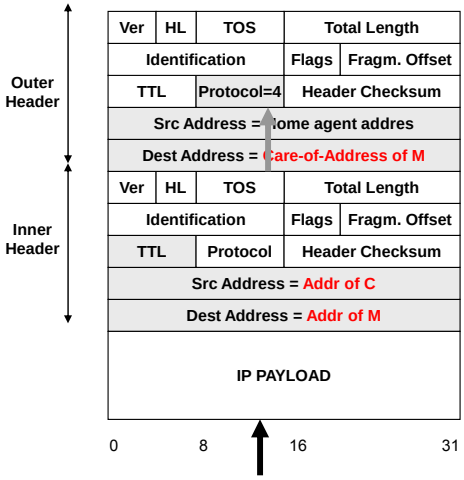
IP-IP Encapsulation at Home Agent



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

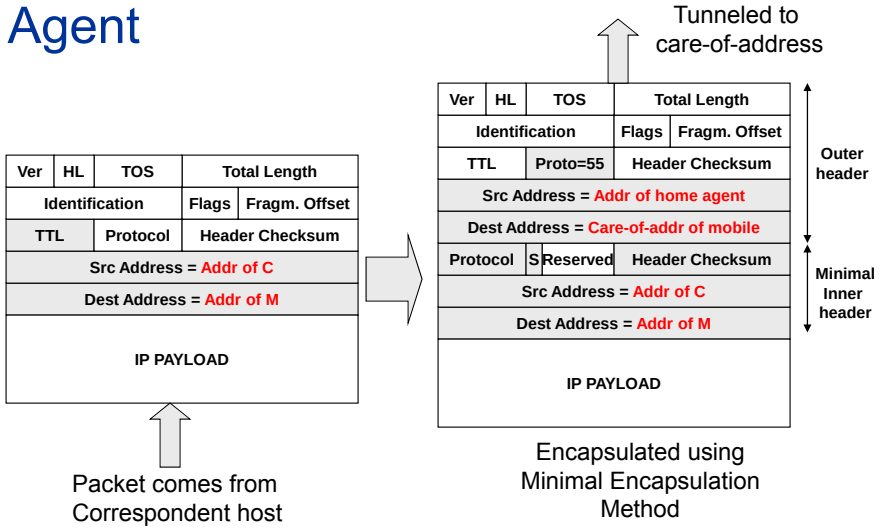


An encapsulated IP packet is received at the foreign agent (or at the mobile Itself for a collocated care-of-address).

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

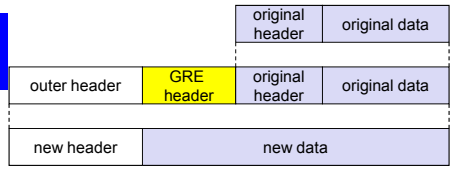
Receiver forwards (not routes) the decapsulated IP packet to the mobile node using link-level mechanisms!

Minimal Encapsulation at Home Agent



Generic Routing Encapsulation

GRE = A protocol for encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol



RFC 1701

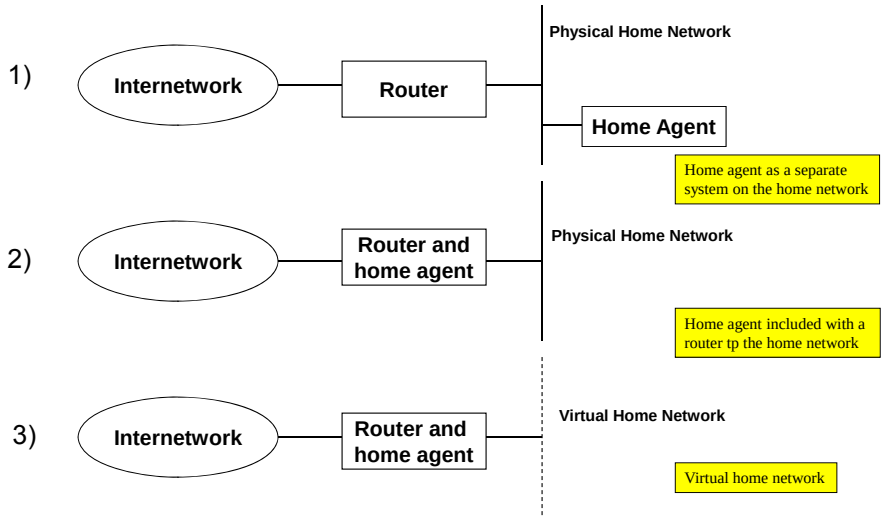
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*GRE*		IP checksum
IP address of HA			
Care-of address COA			
C	R	K	S	s	rec.	rsv.	ver.	protocol
checksum (optional)								offset (optional)
key (optional)								
sequence number (optional)								
routing (optional)								
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.		IP checksum
IP address of CN			
IP address of MN			
TCP/UDP/ ... payload			

RFC 2784

C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

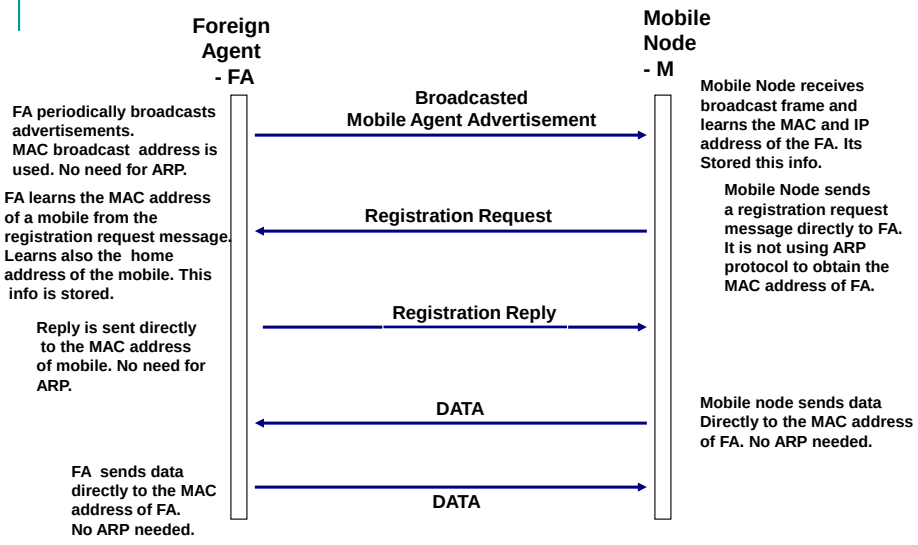
More details about GRE @:
- RFC 2784 (http://www.faqs.org/rfcs/rfc2784.html)
- http://www.networksorcery.com/enp/protocol/gre.htm,

Home Network Configurations

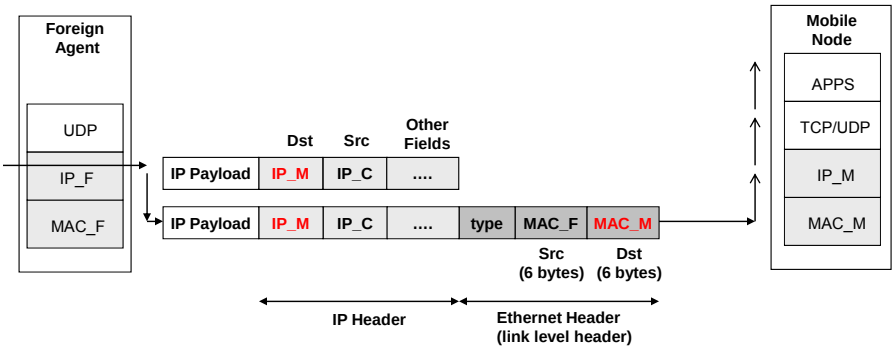


Sending packets between mobile and foreign agent

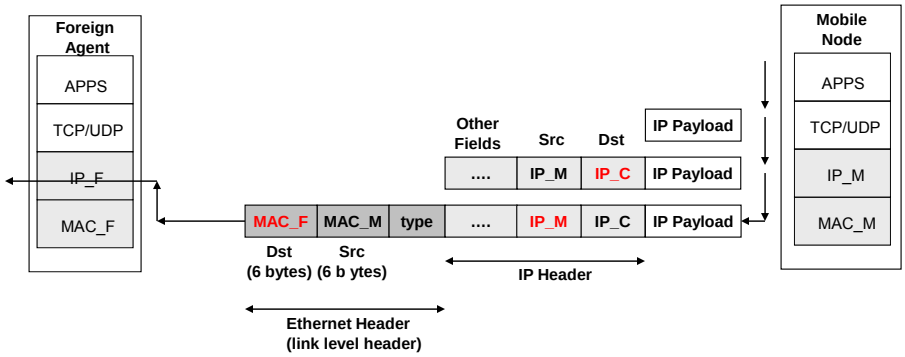
- When a mobile moves to a new location, a foreign should be broadcasting (IP and link layer broadcast) advertisements on the link (sub-network).
- Mobile will be able to receive this broadcast message and will learn:
  - The IP address of the foreign agent (this will be the care-of-address of the mobile 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).



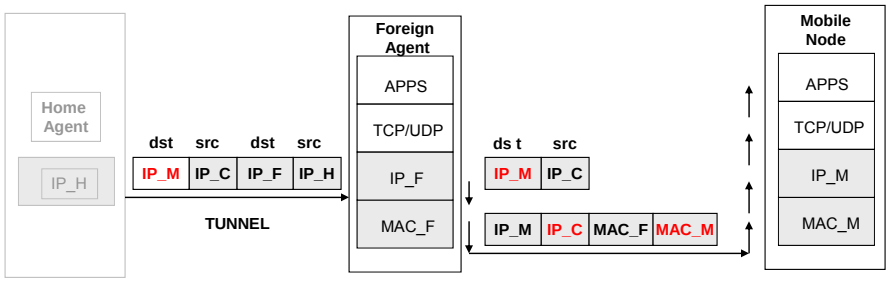
Sending Data from Foreign Agent to Mobile



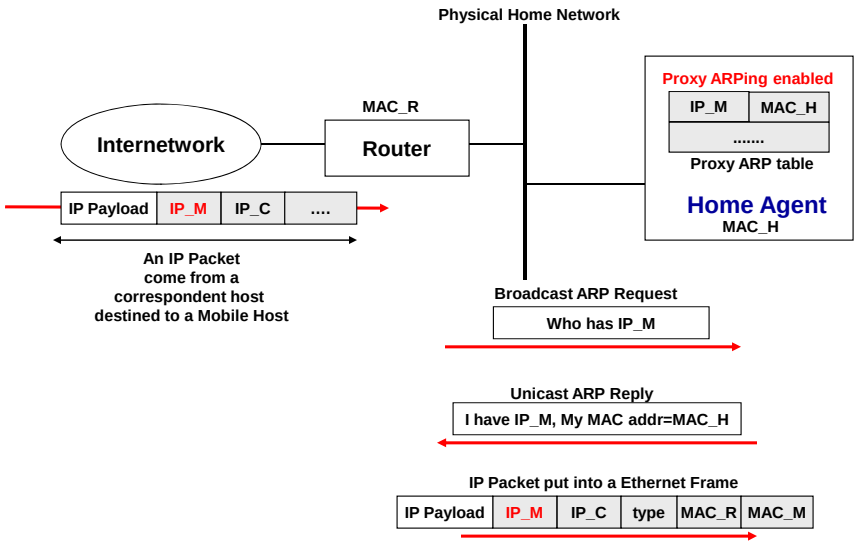
Sending Data from Mobile to Foreign Agent



Decapsulation again



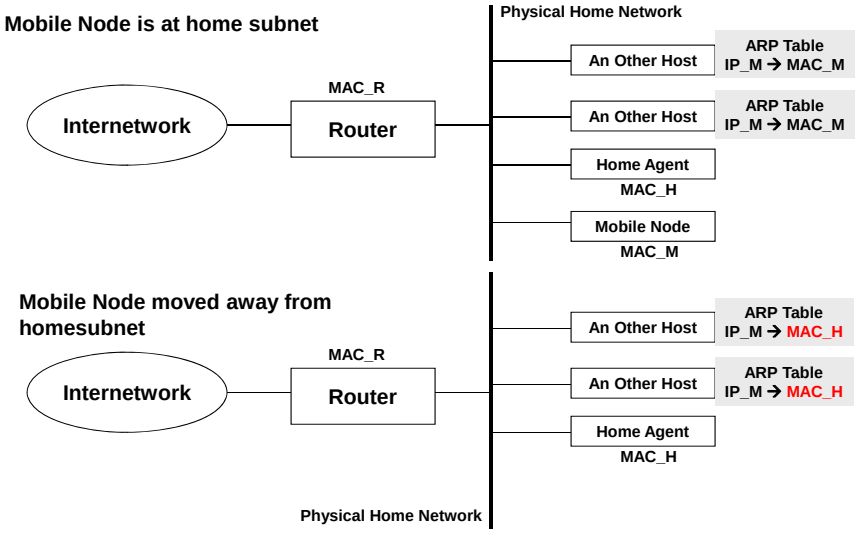
How to attract packets at the Home network



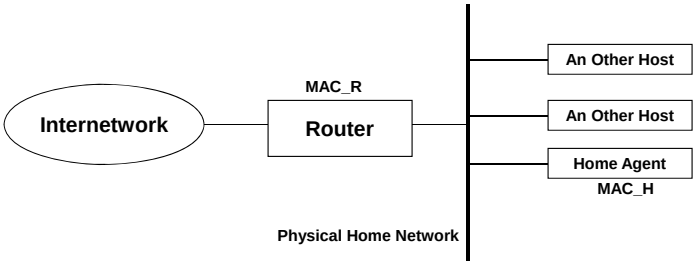
Proxy ARPing

- 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. In 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



Gratuitous ARP Operation



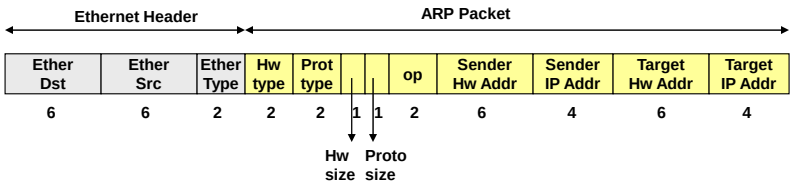
Home Agent Receives Registration Request from New Location

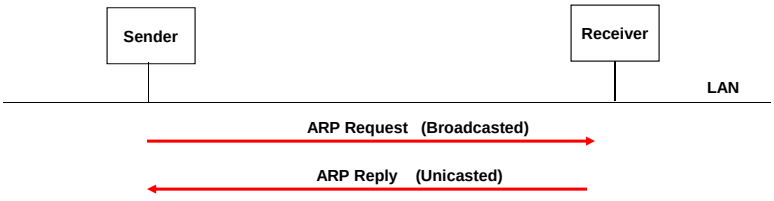
Home agent broadcasts Gratuitous ARP on the Link (indicating IP_M is now located at MAC addr MAC_H)

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

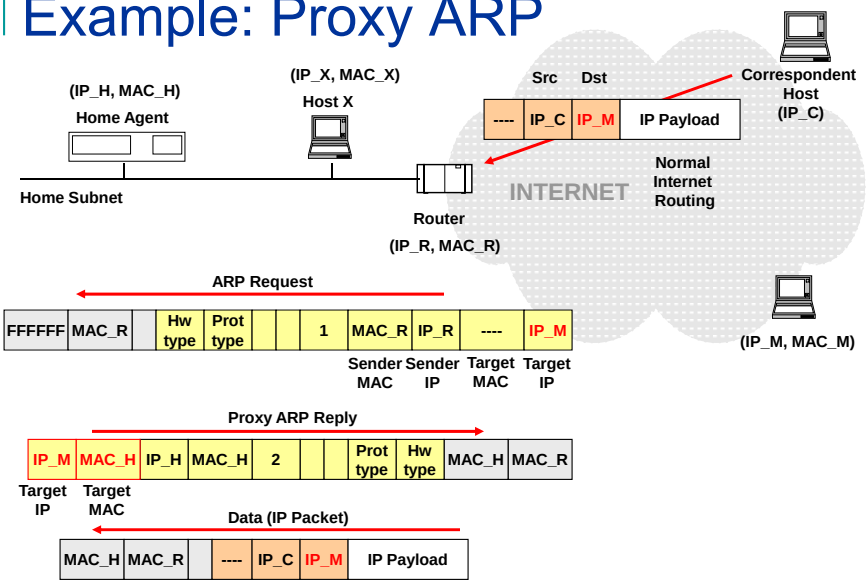
ARP Packet Format

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

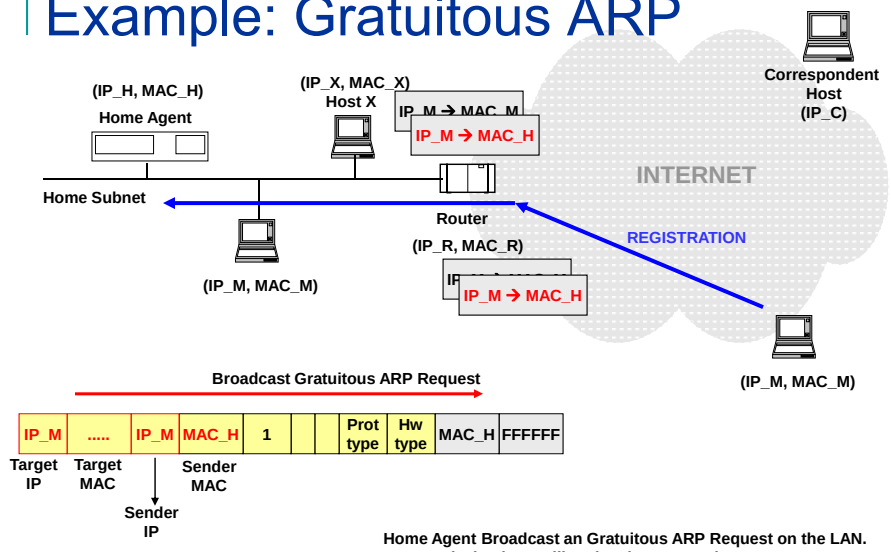




Example: Proxy ARP



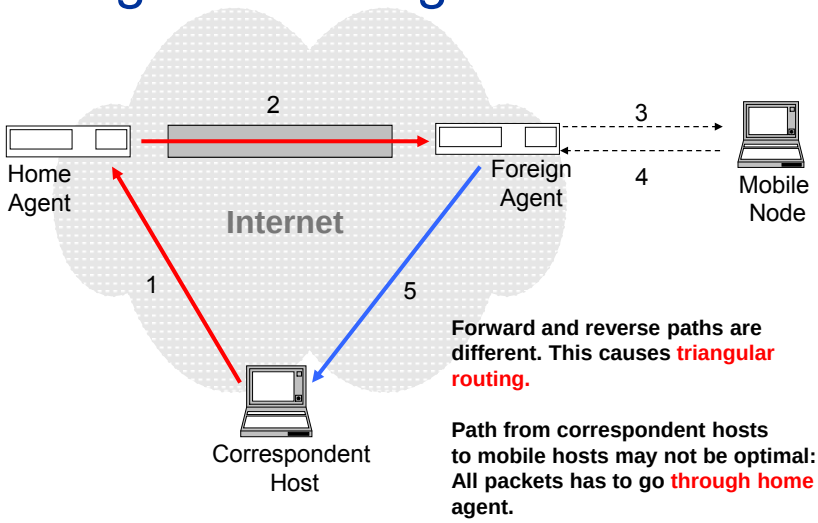
Example: Gratuitous ARP



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

Solution Approach

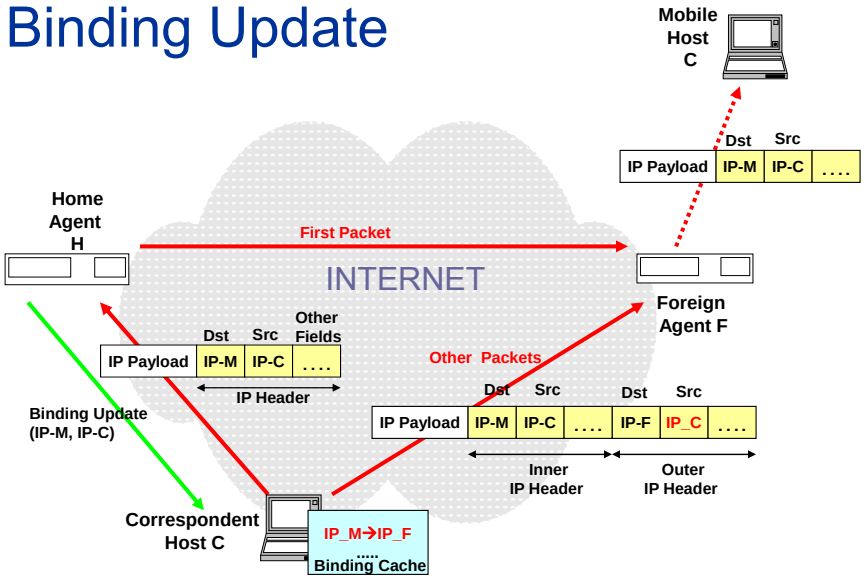
If the COA is a colocated address, the CN sends directly to the mobile host (no FA intervention)
Else
The en/de-capsulation are used and the tunnel ends at the FA

- 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



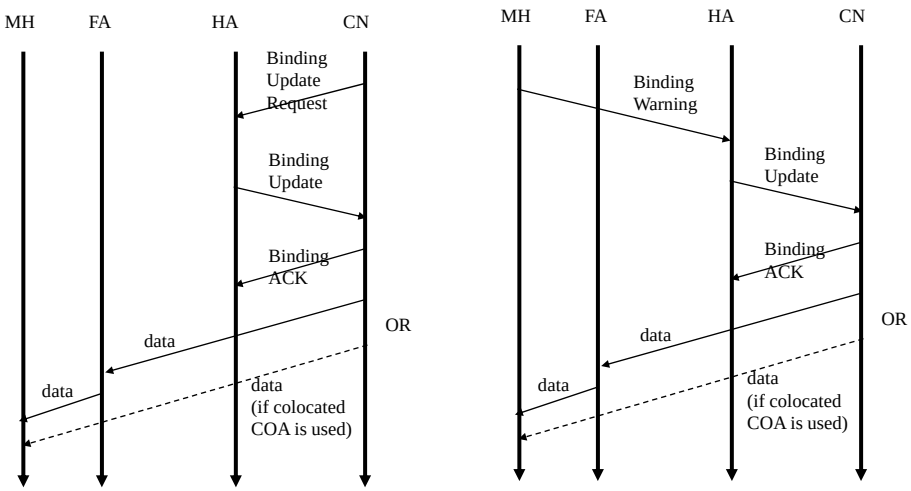
Packet Transport from a Correspondent Host to a Mobile

Binding Warning/Request

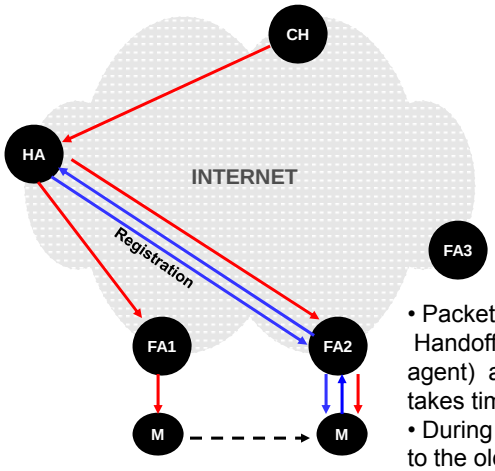
- A correspondent host may request a binding Update message from Home agent.
  - Correspondent host sends a Binding Request message and waits for a Binding Update Message.
- A mobile node may warn a Home agent (or some other agent) to send a Binding Update message to a particular host (a correspondent 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.

Questions:
1. Why should CN continue to do IP encapsulation?
2. What are the modifications at the CN required for this Binding update method to work?

Binding Update/Request/Warning

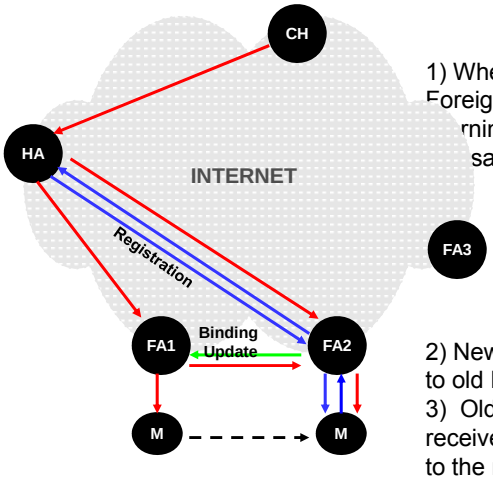


Smooth Handoffs



- 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 ...rning message) to send a Binding Update ...sage 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

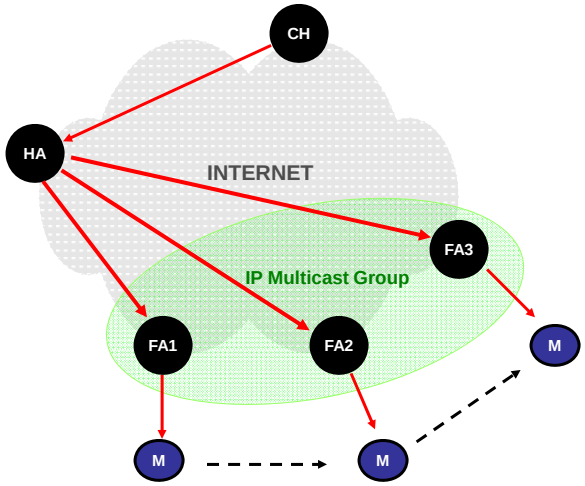
Fast Handoffs

- 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.

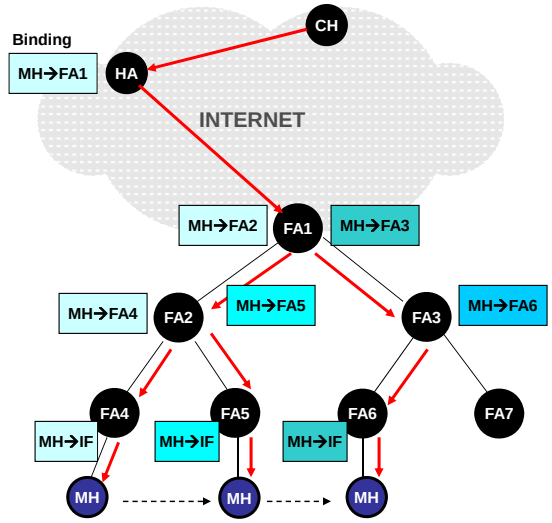
Use of IP Multicasting



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.
  - Intermediate routers between base stations and campus edge routers 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

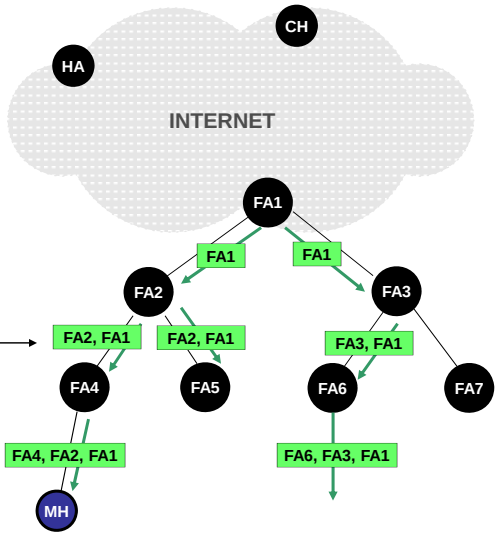
Agent Advertisements

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.

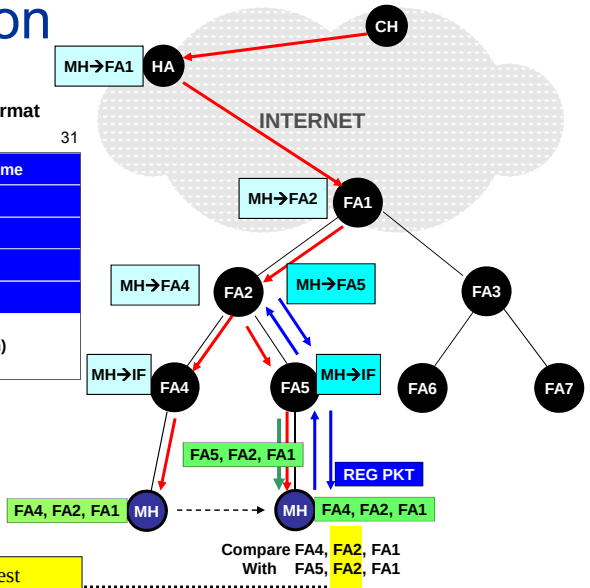


ICMP extension
-I bit (flag) – indicates a hierarchy of COAs

Registration

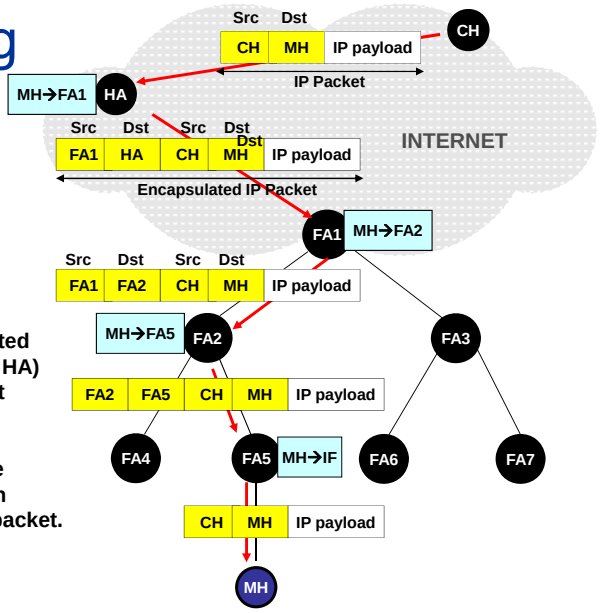
Registration Request Format

0	8	16	31
Type	Flags	Lifetime	
Home address=MH			
Home agent=FA2			
Care-of—address=FA5			
Identification			
Extensions (Authentication Extension)			



REGIONAL Registration Request
- Sequence of tunnels
- Home agent: closest common ancestor

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.

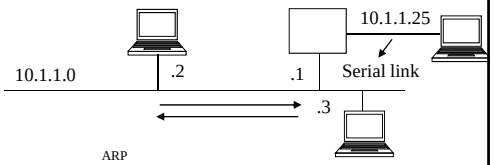
BACKUP SLIDES

ARP

6	6	2	2	2	1	1	2	6	4	6	4
Ethernet DA	Ethernet SA	Frame Type	Hard type	Prot type	Hard size	Prot size	Op	Sender Ethernet Add	Sender IP Add	Target Ethernet Add	Target IP Add

Ethernet DA: 255.255.255.255
Ethernet SA:
Sender Ethernet Add:
Sender IP Add:
Target Ethernet Add:
Target IP Add:
Frame Type: 0x0800 IP
0x0806 ARP
0x8035 RARP

Hardware Type: 1 Ethernet
Protocol Type: 0x0800 IP
Hardware size: 6 Ethernet MAC address length
Protocol size: 4 IP address length
OP: 1 ARP REQ
2 ARP REP
3 RARP REQ
4 RARP REP



ARP
10.1.1.2 broadcasts ARP REQ towards 10.1.1.3
10.1.1.3 sends ARP REP to 10.1.1.2

ARP Proxy
10.1.1.2 braodcasts ARP REQ for 10.1.1.25
The router 10.1.1.1 does proxy ARP for the candidate 10.1.1.25, and returns its own ethernet MAC address.

Gratuitous ARP
10.1.1.2 broadcasts ARP REQ for 10.1.1.2
All nodes on the subnet updates their ARP cache with the new Target ethernet address

ARP Cache
Expires after 20 minutes in BSD

Reverse ARP
Diskless systems use RARP to get its IP address from RARP server on the network during bootstrap time