Mobile Computing

Chapter 8: Mobile Network Layer

Prof. Sang-Jo Yoo

Contents

- Mobile IP overview
- Agent discovery
- Registration
- Tunneling
- DHCP
- Mobile IP multicasting

Motivation for Mobile IP

- Routing
  - based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
  - To avoid an explosion of routing tables, only prefixes are stored aand further optimizations are applied.
  - 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

Motivation for Mobile IP

- Changing the IP-address?
  - adjust the host IP address depending on the current location
    - Assigning a new IP address (DHCP)
  - Problem: nobody knows about this new address.
  - Almost impossible to find a mobile system, DNS updates take to long time
  - TCP connections break, security problems
    - TCP connection = {source IP, source port, destination IP, destination port}
    - TCP connection cannot survive any address change.

Requirements to Mobile IP

- Transparency
  - Mobility should remain 'invisible' for many higher layer protocols and applications
  - For TCP, mobile computer must keep its IP address.
- 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
  - The minimum requirement: all the messages related to the management of Mobile IP are authenticated.
- Efficiency and scalability
  - Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)

Terminology

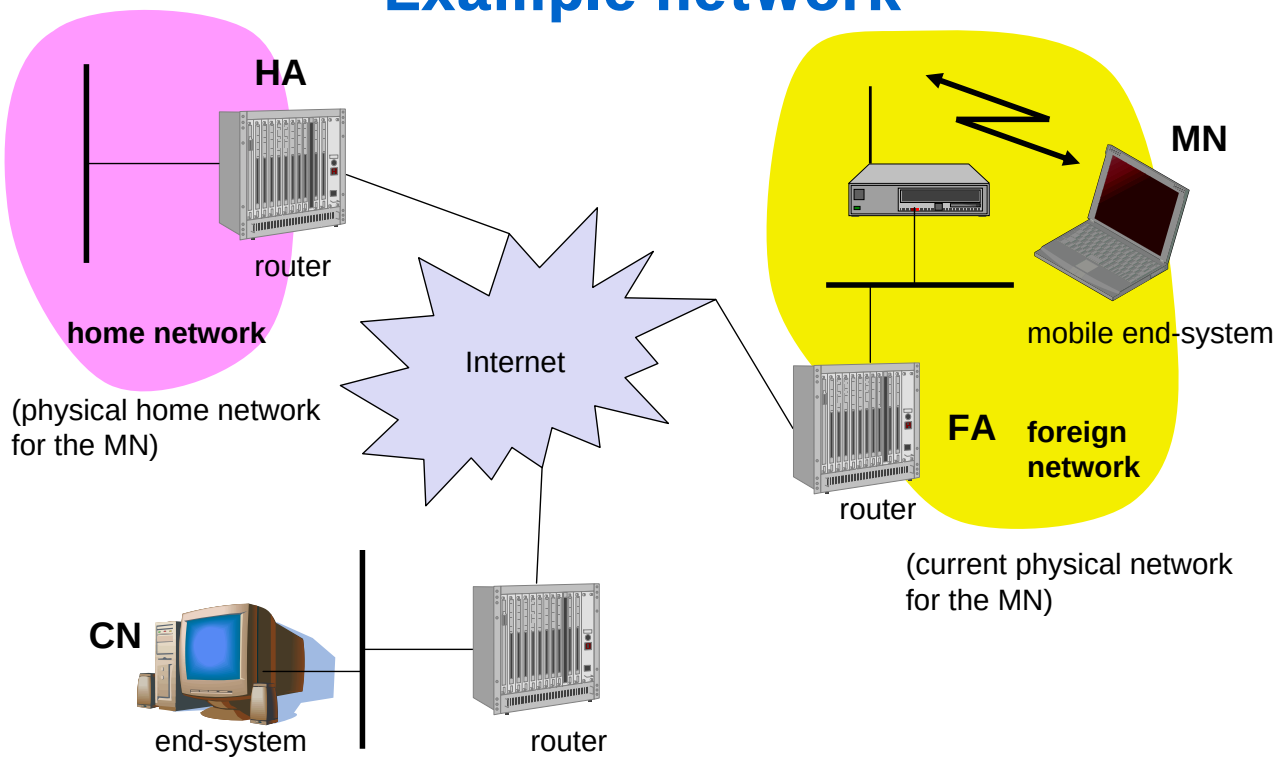
- Mobile Node (MN)
  - system (node) that can change the point of connection to the network without changing its IP address
- Home Agent (HA)
  - system in the home network of the MN, typically a router
  - registers the location of the MN, tunnels IP datagrams to the COA
- Foreign Agent (FA)
  - system 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
- Correspondent Node (CN)
  - communication partner

Terminology

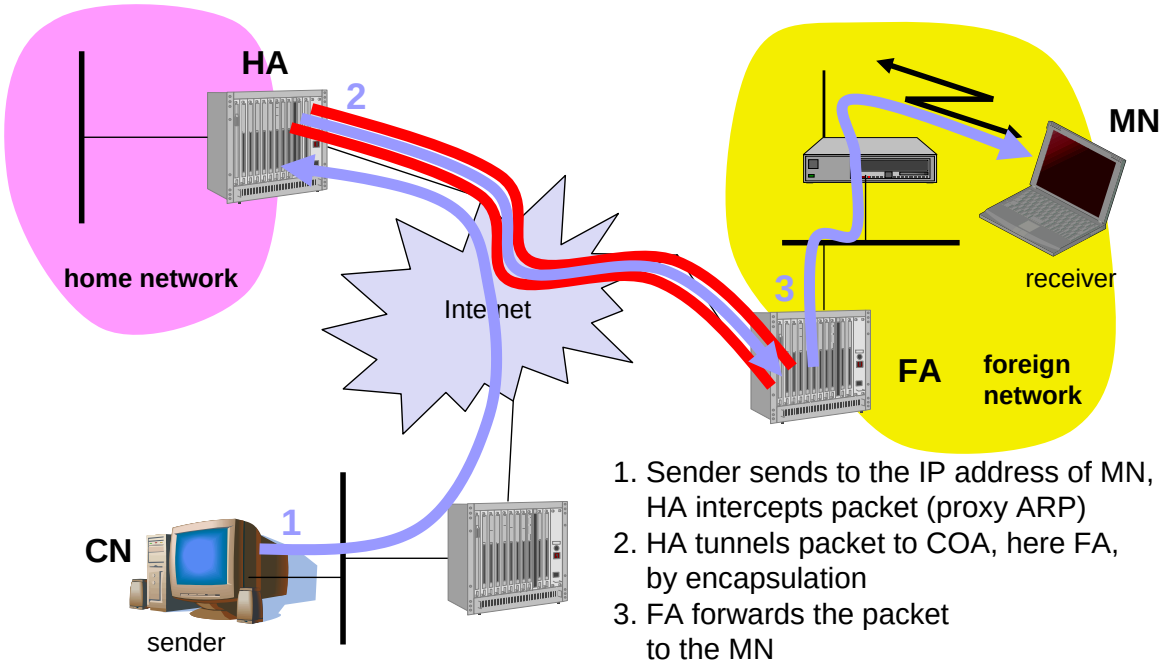
Care-of Address (COA)

- Foreign agent COA
  - The COA could be located at the FA (IP address of FA)
  - The FA is the tunnel end-point and forwards packets to the MN.
  - Many MN using the FA can share this COA.
- Co-located COA
  - MN temporarily acquired an additional IP address which acts as COA.
  - Tunnel end-point is at the MN.
  - Co-located care-of address can be acquired using services such as DHCP

Example network

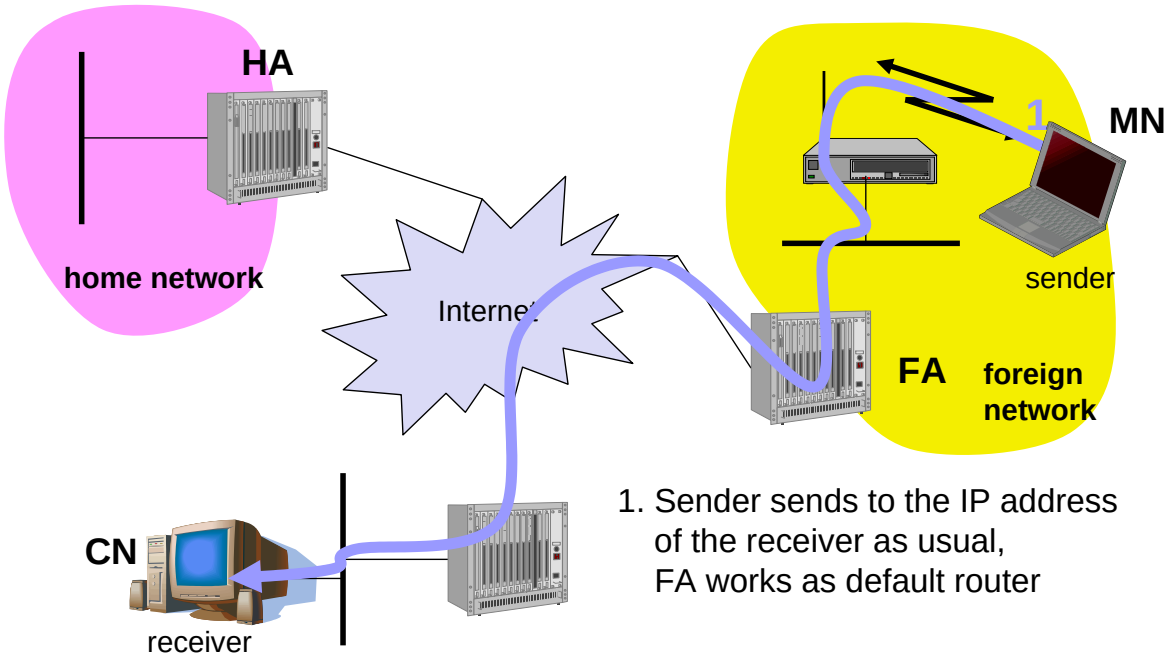


Data transfer to the mobile system



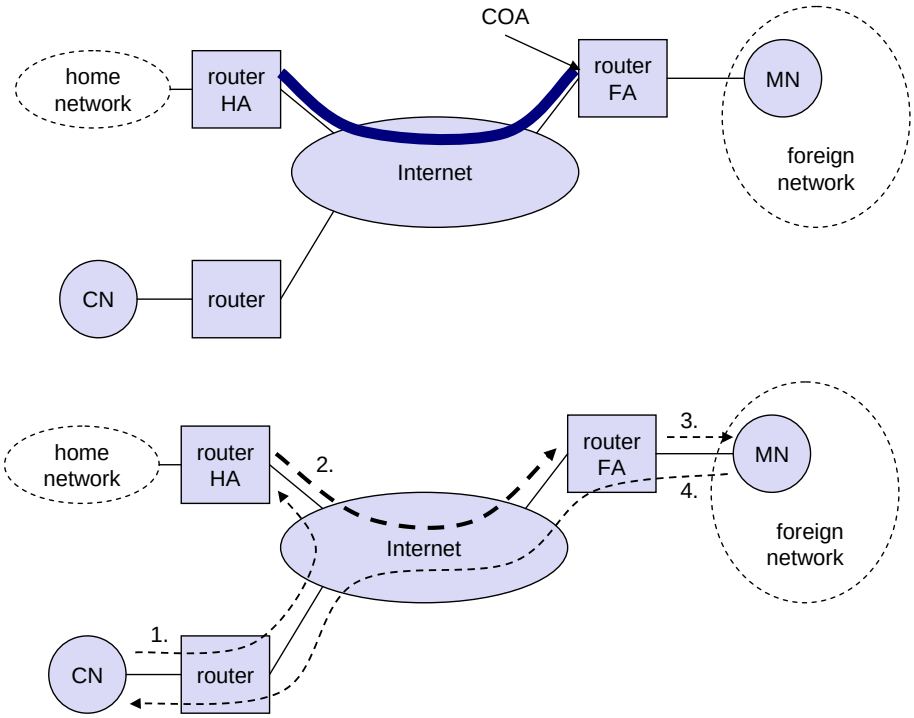
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview



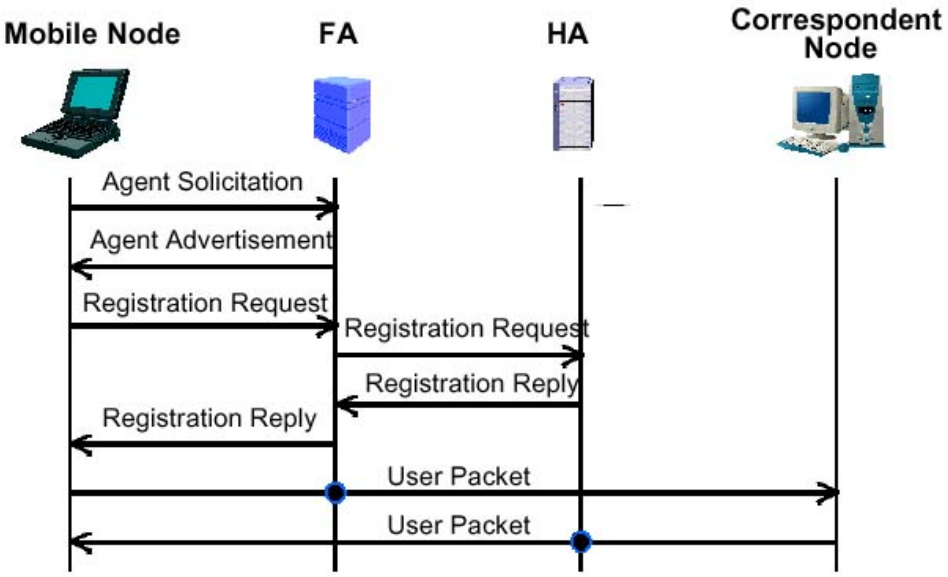
Mobile IP Design Goals

- A mobile node must be able to communicate with other nodes after changing it's link-layer attachment, yet without changing its IP address
- A mobile node must be able to communicate with other nodes that do not implement mobile IP
- Mobile IP must use authentication to offer security against **redirectment attacks**
- The number of administrative messages should be small to save bandwidth & power
- Mobile IP must impose no additional constraints on the assignment of IP addresses

Protocol Overview

- Advertisement
  - HA and FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in the home or a foreign network MN reads a COA from the FA advertisement messages
  - A mobile node can solicit for mobility agents
- Registration - when a mobile node is away from home, it must register its care-of address with it's home agent
  - these actions have to be secured by authentication
- Delivering Datagrams
  - Datagrams must be forwarded by the Home Agent to the Foreign Agent for delivery to the care-of address.
  - The delivery mechanism must handle all packets (including broadcast and multicast)
  - A tunnel is used for this

Overall Behaviors



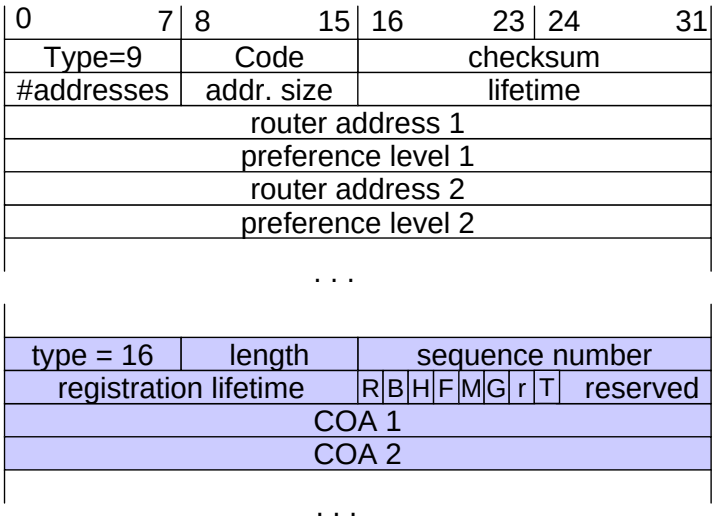
1. Agent Discovery

- Problems:
  - How to find a foreign agent?
  - How does the MN discover that it has moved?
  - → Agent advertisement and Agent solicitation

- Agent advertisement
  - HA and FA advertise their presence periodically using Agent advertisement messages
  - ICMP (Internet Control Message Protocol) message with some mobility extensions : RFC 1256
    - IP header: TTL=1

      destination IP: 224.0.0.1 (multicasting), 255.255.255.255(broadcasting)

Agent advertisement



type = 16
length = 6 + 4 * #COAs
Lifetime: max lifetime in seconds
a node can request
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Agent Solicitation

- MN can send Agent solicitation message
  - If no agent advertisement are present,
  - The inter-arrival time of agent advertisements is too high, or
  - The MN just power on.
  - Based on RFC 1256, ICMP router solicitation message

- **Move detection**
  - Move detection using lifetime
    - If a MN fails to hear an advertisement from the foreign agent (or home agent) with the specified Lifetime.
    - The MN can assume that it has moved to a different link, waits Agent Advertisement or sends Agent Solicitation.
  - Move detection using network-prefixes
    - If the network-prefix of the received Agent Advertisement is different from the that of the previous foreign agent, then registration process should be invoked.

2. Registration

- Request forwarding services when visiting a foreign network
  - This allocates a local (foreign) node address
- Inform home agent of their current care-of address
  - This creates a binding of the foreign node address to the home address
- Renew a binding that's about to expire
  - Bindings have lifetimes
- De-register when they return home

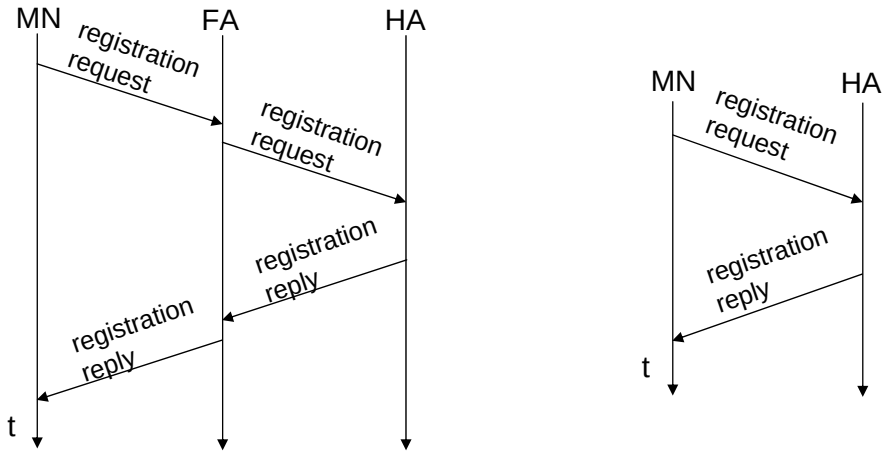
Registration and Security

- The home node and the mobile node have conducted some form of prior key exchange
  - This defines a "secret" between the two nodes
  - The authentication mechanism must defend against replay attacks

- A replay attack occurs when a 3rd party can capture your packets and then "replay" them, fooling you into thinking they are correctly authenticated.
  - E.g., sending an encrypted password over a network leaves you open to a replay attack. Note that attack didn't decrypt.
  - Nonces: Each message from A -> B includes a new random number. When B replies to A, it must include that same random number. Likewise, each B->A message includes a new random number generated by B and echoed by A.

Registration Request

- Registration Request Message
  - The message is sent to FA when foreign agent care-of address is used or R bit of Advertisement is set.
  - The message is directly sent to HA when collocated care-of address is used .



Registration Request

- Both send to UDP port 434. (Registration Reply also)
- IP source address: interface address of the MN
- IP destination address:
  - HA: when co-located care-of address is used
  - FA: when FA care-of address is used

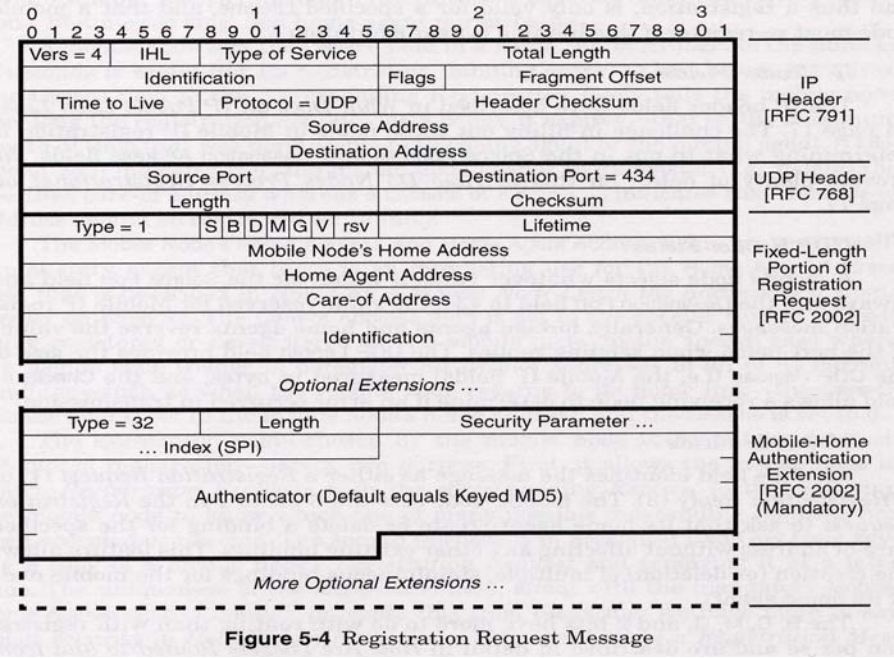


Figure 5-4 Registration Request Message

Registration Request

- Type =1
- S – set to 1 to ask that its HA create or delete a binding for the specified care-of address.
- B – to tell the HA to encapsulate broadcast datagrams from home network to the care-of address.
- D – to inform the HA where the exit-point of the tunnel is located.
- Lifetime – the number of seconds it would like its registration to last before it expires.
- Home address
- Home agent address
- Care-of address
- Identification – 64 bits for replay protection.
- Mobile-home authentication extension – to prevent remote redirect attack.

Registration Request

Fields	Mobile Node Registering with Foreign Agent Care-of Address	Mobile Node Registering with Collocated Care-of Address	Mobile Node deregistering upon Returning to Home Link
Link-Layer Header:			
Source Address	mobile node's link-layer address		
Destination Address	copied from Agent Advertisement	obtained via ARP using care-of address[a]	obtained via ARP using home address
IP Header:			
Source Address	home address	care-of address	home address
Destination Address	foreign agent	home agent[a]	home agent
UDP Header:			
Source Port	*can be anything*		
Destination Port	434		
Registration Request:			
Type	1		
S bit	1, if this registration should not affect existing bindings; 0, otherwise		0
B bit	1, if mobile node wants a copy of broadcasts on the home link; 0, otherwise		0
D bit	0	1	0
M bit	set according to the mobile node's requirements for tunneling and header compression *and* the foreign agent's support for same	set according to the mobile node's requirements and support for tunneling and header compression	0
G bit			0
V bit			0
rsv	0		
Lifetime	copied from Agent Advertisement	whatever the mobile node wants	0
Mobile Node's Home Address	mobile node's IP home address		
Home Agent's Address	home agent's IP address		
Care-of Address	copied from Agent Advertisement	collocated care-of address obtained via DHCP or manually	mobile node's home address
Identification	chosen in accordance with style of replay-protection used between mobile node and home agent		
Extensions:			
	Mobile-Home Authentication Extension is required.		

Table 5-1 Fields in Registration Request as Set by Mobile Node

Registration Reply

- Lifetime:tells the mobile node how long the registration will be honored by the HA.
  - It can be shorter than requested, but never longer.

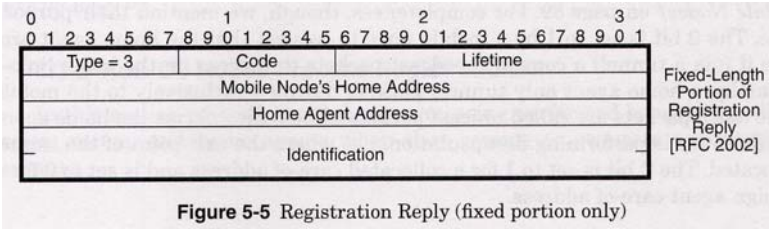


Figure 5-5 Registration Reply (fixed portion only)

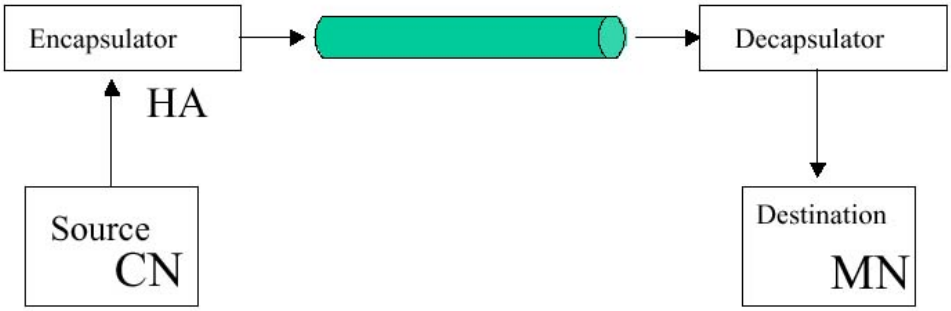
registration successful
- 0 registration accepted
- 1 registration accepted, but simultaneous mobility bindings unsupported

registration denied by FA
- 65 administratively prohibited
- 66 insufficient resources
- 67 mobile node failed authentication
- 68 home agent failed authentication
- 69 requested Lifetime too long

registration denied by HA
- 129 administratively prohibited
- 131 mobile node failed authentication
- 133 registration Identification mismatch
- 135 too many simultaneous mobility bindings

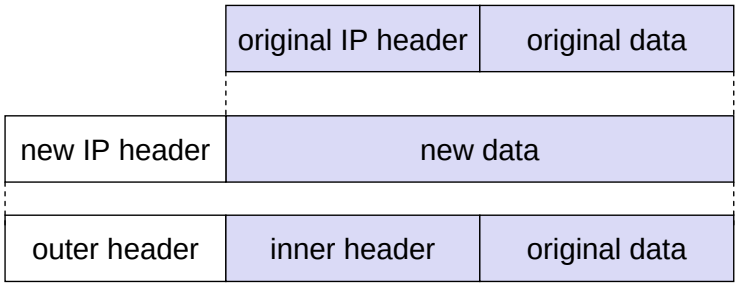
3. Tunneling

- Tunnel
  - Establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.
  - Tunneling is achieved by using encapsulation



Encapsulation

- Encapsulation
  - Mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.
  - Decapsulation: reverse operation
  - Outerheader: the new header
  - IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)



Encapsulation (IP-in-IP)

- IP-in-IP-encapsulation (mandatory, RFC 2003)
  - tunnel between HA and COA

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*	IP checksum	
IP address of HA			
Care-of address COA			
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			

Encapsulation (IP-in-IP)

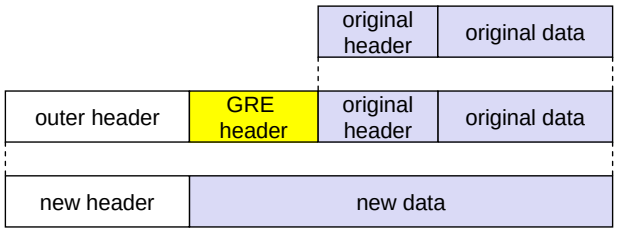
- The outer IP header source & destination address identify the tunnel endpoints (e.g., HA & FA).
- Outer protocol is '4' (IP protocol)
  - Indicates payload is also IP datagram (version 4)
- The inner IP header source address and destination address identify the original sender & recipient
  - Not changed by the encapsulator, except to change TTL
  - TTL is changed to 1 (why?)
- Other headers for authentication might be added to outer header.
- Some outer IP header fields are copied from the inner IP fields (TOS), most are re-computed (TTL, checksum, length) based on new datagram

Encapsulation (Minimal)

- Minimal encapsulation (optional)
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
  - only applicable for unfragmented packets, no space left for fragment identification

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*min. encap.*	IP checksum	
IP address of HA			
care-of address COA			
lay. 4 protoc.	S	reserved	IP checksum
IP address of MN			
original sender IP address (if S=1)			
TCP/UDP/ ... payload			

Generic Routing Encapsulation



RFC 1701

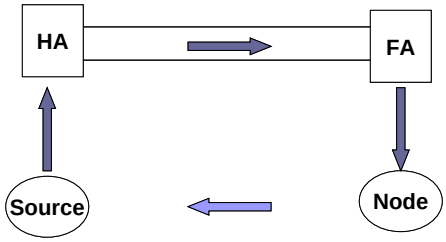
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*GRE*	IP checksum	
IP address of HA			
Care-of address COA			
C R K S s rec.	rsv.	ver.	protocol
checksum (optional)		offset (optional)	
key (optional)			
sequence number (optional)			
routing (optional)			
ver.	IHL	DS (TOS)	length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

RFC 2784

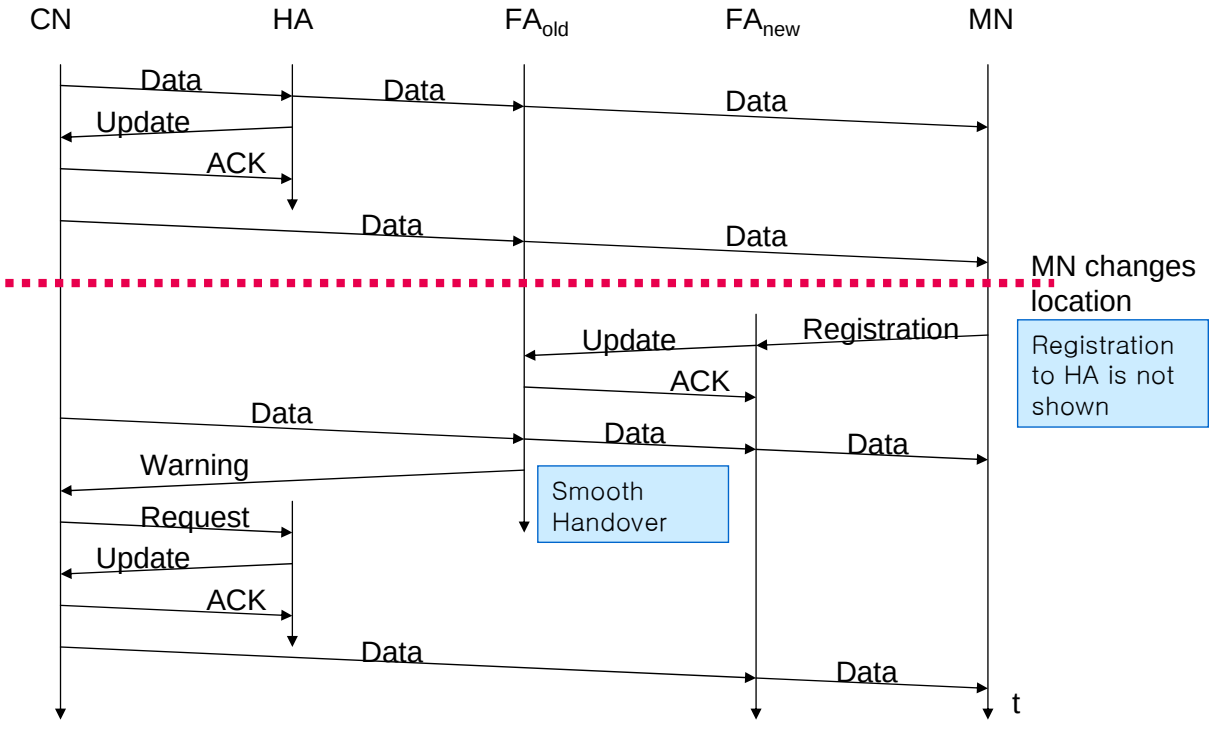
C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

Optimization of packet forwarding

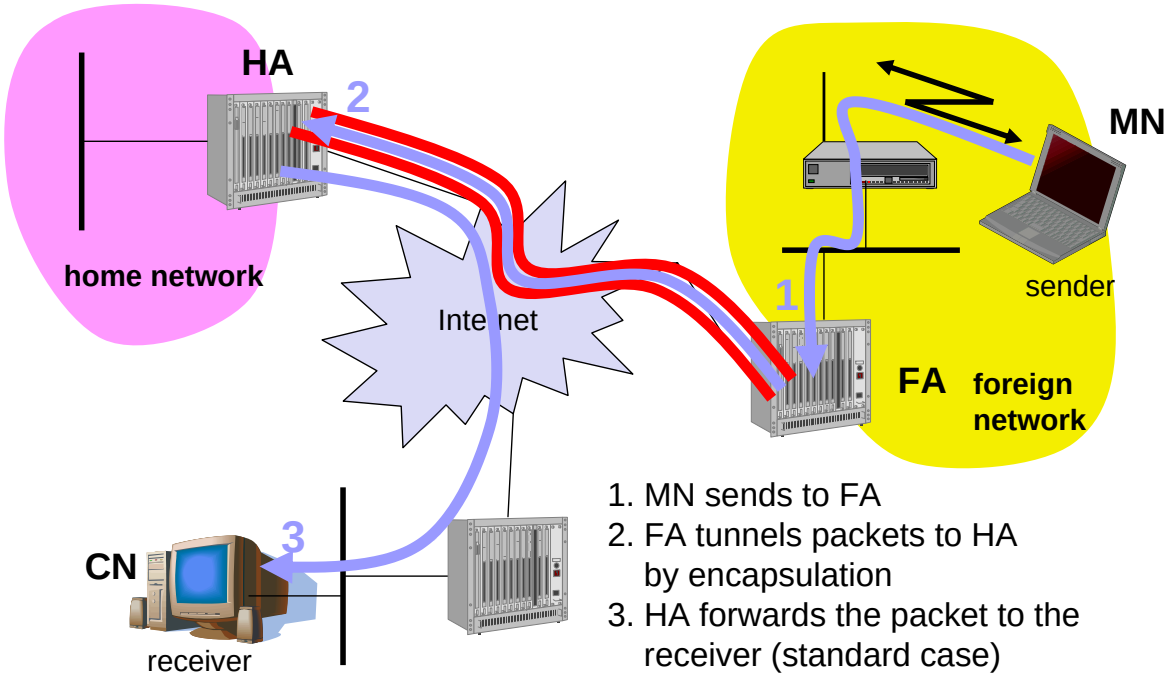
- Triangular Routing
  - sender sends all packets via HA to MN
  - higher latency and network load
- "Solutions"
  - sender learns the current location of MN
  - direct tunneling to this location
  - HA informs a sender about the location of MN
  - big security problems!
- Change of FA
  - packets on-the-fly during the change can be lost
  - new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
  - this information also enables the old FA to release resources for the MN



Change of foreign agent



Reverse tunneling



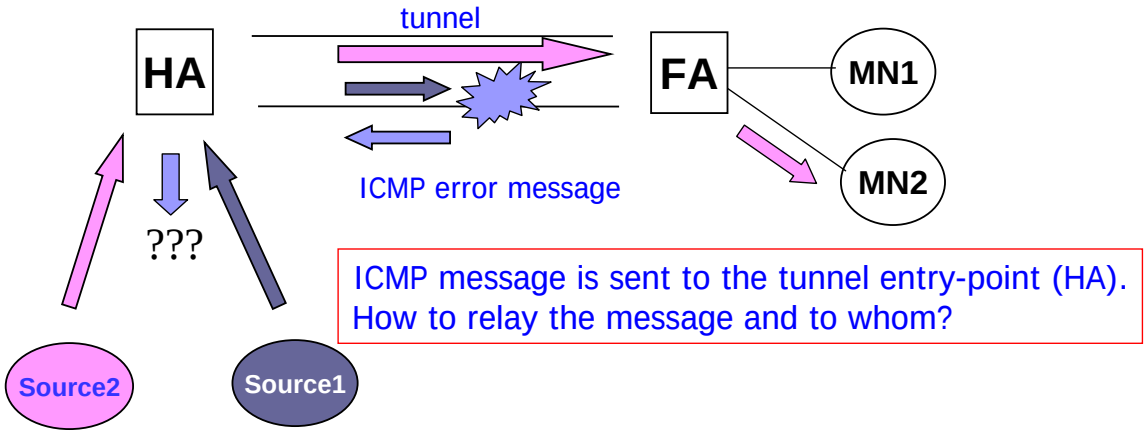
1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)

Mobile IP with reverse tunneling

- Router accept often only “topological correct“ addresses (firewall!)
  - a packet from the MN encapsulated by the FA is now topological correct
  - furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)
- Reverse tunneling does not solve
  - problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
  - optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)
- The standard is backwards compatible
  - the extensions can be implemented easily and cooperate with current implementations without these extensions
  - Agent Advertisements can carry requests for reverse tunneling

Soft Tunnel State

- Relaying ICMP (Internet Control Message Protocol) [RFC 792] Messages



Soft Tunnel State

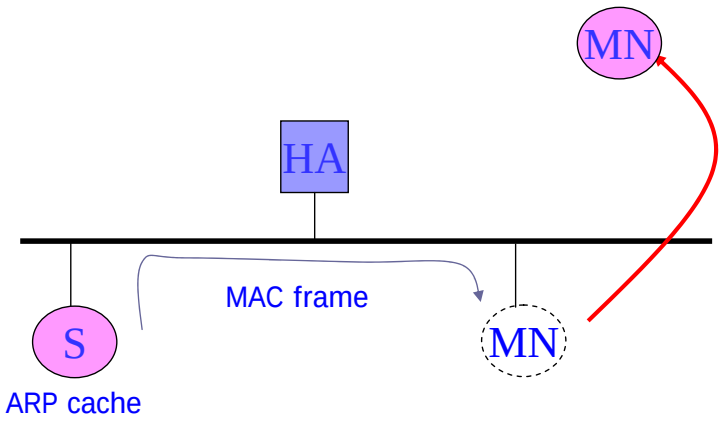
- Tunnel entry-point necessary to relay certain ICMP messages to the original source.
- HA maintains soft state per each tunnel.
  - Path MTU
  - The number of hops
  - Whether or not the end of tunnel is reachable.
- HA updates its soft state based upon ICMP messages received from routers within the tunnel.
  - If the received ICMP message is “fragmentation needed”, then increase path MTU.
  - If HA receives the ICMP “time exceeded”, then increase the length of the tunnel.
  - If HA receives “destination unreachable”, then it knows that the tunnel is now un reachable.

Soft Tunnel State

- When HA receives a IP datagram, check the soft state of the tunnel that will be used.
  - If the tunnel has a problem, then
  - Send a ICMP message to the source without sending the datagram to the destination.
- Why do we call the information as “soft state”?

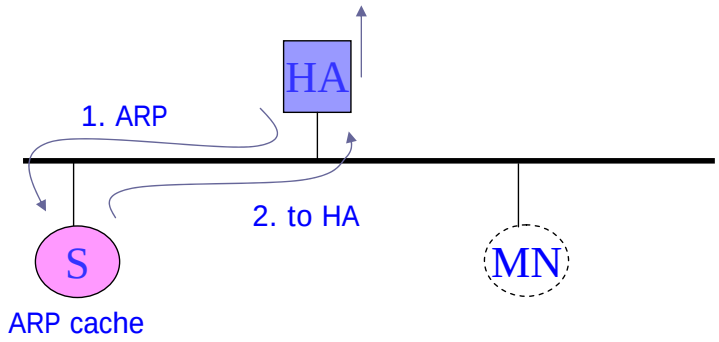
Proxy and Gratuitous ARP

- Hosts remaining on the home network sends IP packets to the link with MN’s MAC address that is stored in ARP cache.
- So, HA must perform proxy ARP for the mobile node.



Proxy and Gratuitous ARP

- HA broadcasts gratuitous ARPs to the hosts on the link as soon as the MN moves away form the home network
  - Every node updates its ARP cache.
    - IP home address of the MN ↔ MAC address of the HA
- When MN returns to the home network, HA broadcast gratuitous ARPs
    - IP home address of the MN ↔ MAC address of the MN



Mobile IP and IPv6

- Mobile IP was developed for IPv4, but IPv6 simplifies the protocols
  - security is integrated and not an add-on, authentication of registration is included
  - COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address autoconfiguration
  - no need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
  - MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
  - “soft“ hand-over, i.e. without packet loss, between two subnets is supported
    - MN sends the new COA to its old router
    - the old router encapsulates all incoming packets for the MN and forwards them to the new COA
    - authentication is always granted

Problems with mobile IP

- Security
  - authentication with FA problematic, for the FA typically belongs to another organization
  - no protocol for key management and key distribution has been standardized in the Internet
- Firewalls
  - typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)
- QoS
  - many new reservations in case of RSVP
  - tunneling makes it hard to give a flow of packets a special treatment needed for the QoS
- Security, firewalls, QoS etc. are topics of current research and discussions!

IP version 6 (Mobile IP)

Mobile IPv4	Mobile IPv6
Mobile node, home agent, home link, foreign link	(same)
Mobile node's home address	Globally routable home address and link-local home address
Foreign agent	A "plain" IPv6 router on the foreign link(foreign agent no longer exists)
Foreign agent care-of address	All care-of addresses are collocated
Collocated care-of address	
Care-of address obtained via Agent Discovery,DHCP, or manually	Care-of address obtained via Stateless Address autoconfiguration, DHCP, or manually
Agent Discovery	Router Discovery
registration with home agent	notification of home agent and other correspondents

4. IP Micro-mobility support

- Limitation of traditional Mobile IP
  - Mobile IP can result in disruption to user traffic during handoff.
  - Mobile IP has high control overhead due to frequent notification to the HA.
  - On every handoff, new QoS reservation would be reestablished from the HA to the FA even though most of the path remains unchanged.
  - Thus,Mobile IP has some limitation when applied to wide-area wireless networks with high mobility users that may require QoS.

IP Micro-mobility support

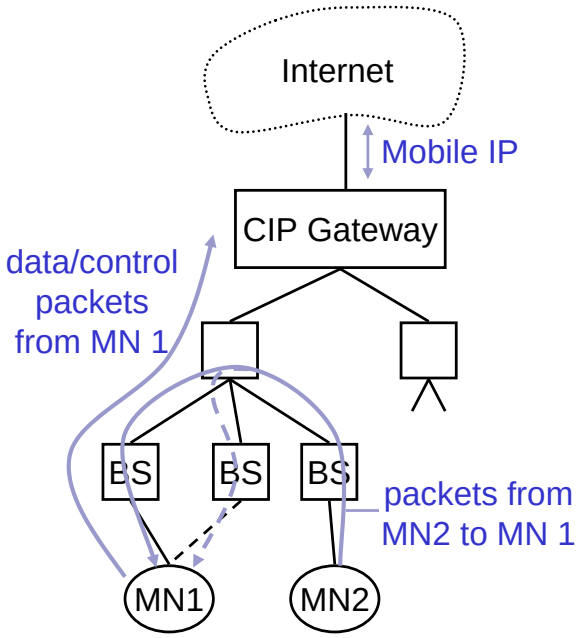
- Micro-mobility support:
  - Efficient local handover inside a foreign domain without involving a home agent
  - Reduces control traffic on backbone
  - Especially needed in case of route optimization
- Example approaches:
  - Cellular IP
  - HAWAII
  - Hierarchical Mobile IP (HMIP)
- Important criteria:
  Security Efficiency, Scalability, Transparency, Manageability

Mobility Classification

- Micro-mobility is the movement of an MN within or across different BSs within a subnet and occurs very rapidly. (local mobility)
- Macro-mobility is the movement of an MN across different subnet within a single domain or region,and occurs relatively less frequently. (intradomain mobility)
- Global Mobility is the movement of an MN among different administrative domains or geographical regions. (interdomain mobility)

Cellular IP

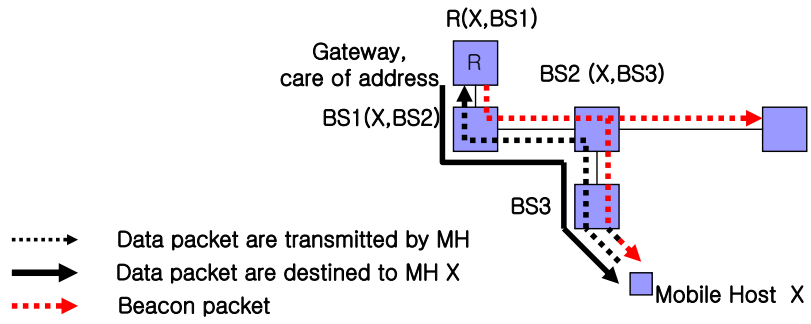
- Operation:
  - "CIP Nodes" maintain routing entries (soft state) for MNs
  - Multiple entries possible
  - Routing entries updated based on packets sent by MN
- CIP Gateway:
  - Mobile IP tunnel endpoint
  - Initial registration processing



Cellular IP(Routing)

- Cellular IP gateway periodically broadcasts a beacon packet that is flooded in the access network.
- Base station records the neighbor they last received this beacon from and use it to route packets toward gateway.
- All packets transmitted by mobile hosts, regardless of their destination address, are routed toward the gateway using these routes.

Cellular IP(Routing)

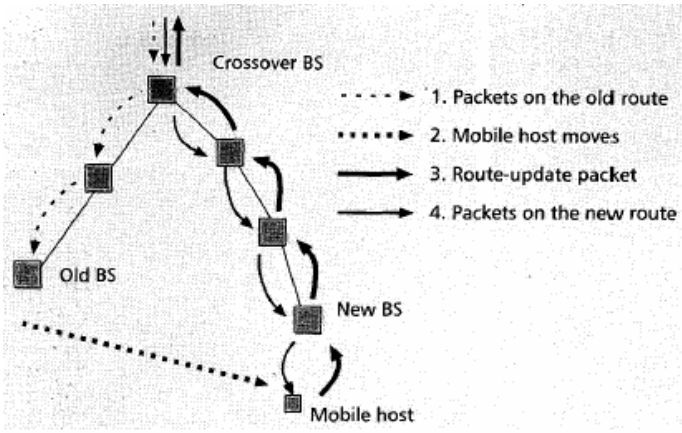


- **As these packets pass each node en route to the gateway,their route information is recorded as follows**
- **Each base station maintains a routing cache.**
- **Soft state mapping remains valid for a system-specific time called route-time-out.**
- **As long as mobile host X regularly sends data packet,base station along the path between Gateway and Mobile Host X**
- **To keep its routing cache mappings valid,the mobile host transmit route-update packets on the uplink at regular intervals called route- updated time**

Cellular IP(Handoff)

- Cellular IP ***hard handoff*** is based on a simple approach that trade off some packet loss for minimizing handoff signaling rather than try to guarantee zero packet loss.
- Cellular IP ***semisoft handoff*** exploits the notion that some mobile hosts can simultaneously receive packets from the new and old base stations during handoff.
- Semisoft handoff minimizes packet loss,providing improved TCP and UDP performance over hard handoff.

Cellular IP(Hard Handoff)



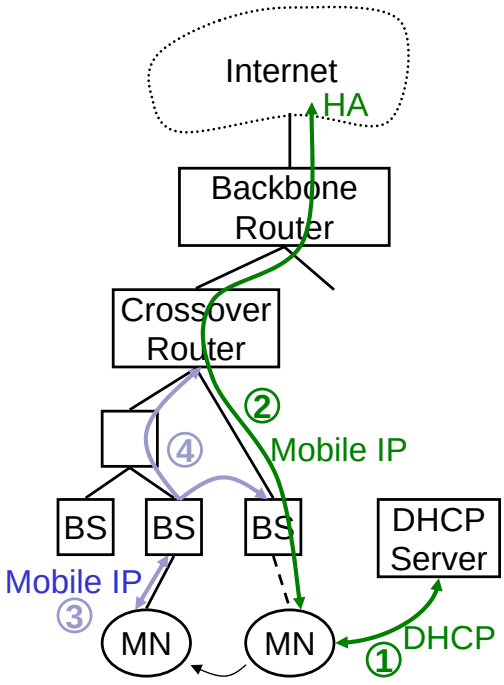
- **To perform handoff,a mobile host tunes its radio to a new base station and sends route-update packet.**
- **In the case of hard handoff handoff latency is equal to the round-trip time between mobile host and crossover BS. (In the worst case the crossover BS is the gateway.**

Cellular IP(Semisoft Handoff)

- Semi-soft handoff scales well for large number of mobile hosts and frequent handoff.
- Semi-soft handoff comprises two architectural components.
  - In order to reduce handoff latency,the routing cache mappings associated with the new base station must be created before the actual handoff takes place.
  - In order to resolve unsynchronized packet,mapping created at crossover points by the reception of semisoft packets include a flag to indicate that downlink packets must pass through a delay device before being forwarded for transmission along the new path.

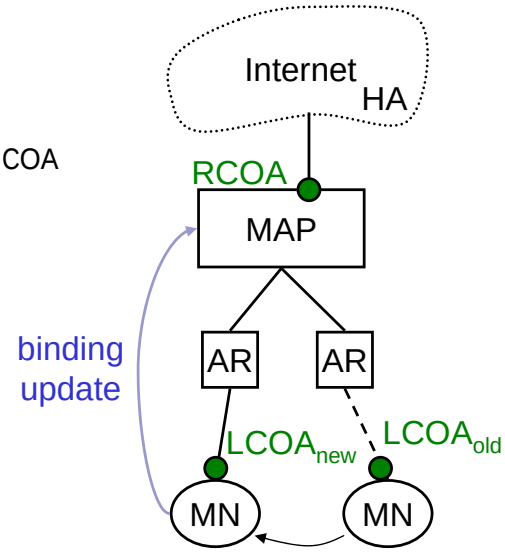
HAWAII

- Handoff-Aware Wireless Access Internet Infrastructure
- Operation:
  - MN obtains co-located COA ① and registers with HA ②
  - Handover: MN keeps COA, new BS answers Reg. Request ③ and updates routers ④
  - MN views BS as foreign agent
- Security provisions:
  - MN-FA authentication mandatory
  - Challenge/Response Extensions mandatory



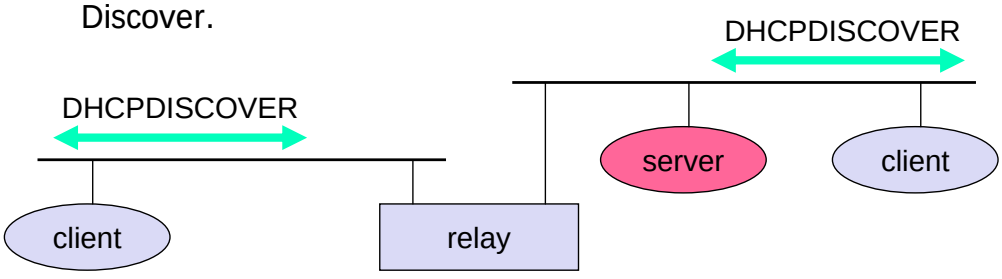
Hierarchical Mobile IPv6 (HMIPv6)

- Operation:
  - Network contains mobility anchor point (MAP)
    - mapping of regional COA (RCOA) to link COA (LCOA)
  - Upon handover, MN informs MAP only
    - gets new LCOA, keeps RCOA
  - HA is only contacted if MAP changes

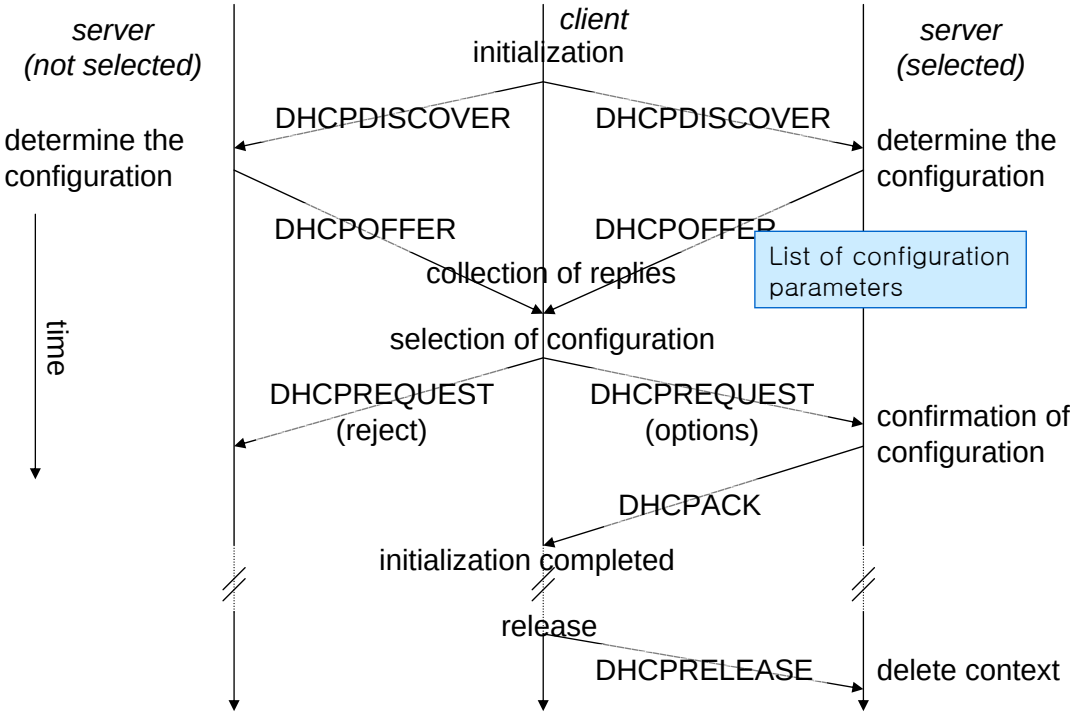


5. DHCP: Dynamic Host Configuration Protocol

- Application
  - If a new computer is connected to a network, DHCP provide it with all necessary information for full system integration into the network.
  - supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  - enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP
- Client/Server-Model
  - the client sends via a MAC broadcast a request to the DHCP server: DHCP Discover.



DHCP - protocol mechanisms



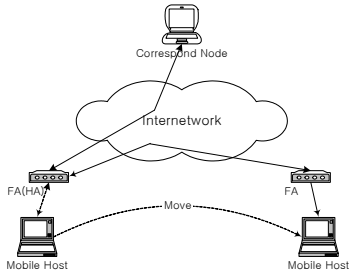
DHCP characteristics

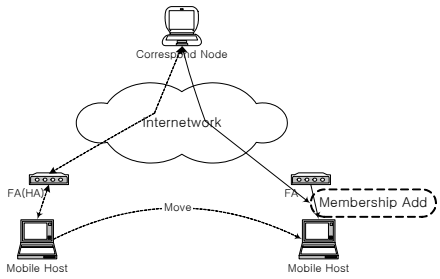
- Server
  - several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)
- Renewal of configurations
  - IP addresses have to be requested periodically, simplified protocol
- Options
  - available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)
- Big security problems!
  - no authentication of DHCP information specified

6. Mobile IP multicasting problem definition

IETF Standards

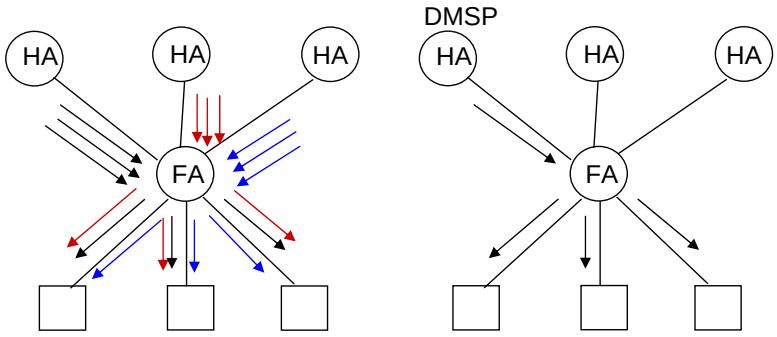
- Remote-subscription
  - Optimal routing (con)
  - Frequent multicasting tree updating (pro)
  - Join delay (pro)
  - Out-of-synch problem (pro)
- Bidirectional-tunneling
  - No out-of-synch problem (con)
  - No tree updating and join procedure (con)
  - Multiple unicast tunnels from a HA to a FA (pro)
  - Multiple tunnels from different HAs to a FA (pro)
  - No optimal routing (pro)
  - Registration delay





Mobile IP Multicasting

- MOM (ACM Mobicom'97)
  - Use bidirectional tunneling
  - Solve tunneling convergence problem
  - Select one HA from multiple HAs in FA for a group: DMSP



- DMSP selection methods
  - Age-based, count-based
- DMSP handoff events
  - MHs of DMSP movement
  - New MH comes in

- Problems of MOM
  - No optimal routing (still exists)
  - Out-of-synch problem (newly generated)
  - Registration delay for tunneling (still exists)
  - Losses during DMSP handoff (newly generated)

- RBMOM (IEICE Trans. on Comm. 2001)
  - Hybrid: bidirectional tunneling & remote subscription
  - Method
    - D=distance between FA and MHA
    - Dh=distance between FA and HA
    - MHA: multicast agent for a MH (HA or FA)
    - R=predetermined threshold distance (hop count)

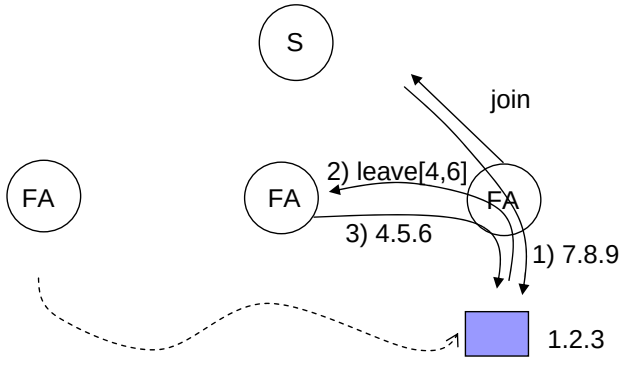
```
When a MH moves to a new FA
If (D > R)
   if (Dh<=R)
        if(FA is on the multicast tree)
              MHA=FA
        else  MHA=HA
  else
        MHA=FA
        if FA is not on the tree, then join the tree
        inform to HA that FA is now MHA for the MH
        inform to the previous MHA that it does not need to send data.
Else
  inform to the MHA the location of the new FA
  (RBMOM can use DMSP approach on selecting MHA)
```

- Problems of RBMOM
  - It does not consider reliable multicasting
  - Data structure and operational procedures for all agent types are not perfect.
  - Distance between FA and MHA is not only thing to decide for joining the tree.
  - HA is receiving the multicasting data (as a member of the tree) even though there is no MH that is receiving data from the HA.

- RBMOM modification (IEE Electronics Letters, 2002)
  - Service range R (distance from MHA to the new FA) is dynamically decided by MHA
    - So, tunneling or joining the tree is decided by MHA not FA
    - R*(1hop delay)+TDs-mha+Ttunnel<=maxDelay
      TDs-mha=(hops from S to MHA)*(1hop delay)
      Ttunnel= tunneling process delay

- MMROP (IEEE Trans. on Consumer Electronics, 2001)
  - Basically, use IETF-RS method
  - To solve out-of-synch problem, missing sequence packets are transmitted by tunnel between new FA and old FA.

  - Problems
    - It still has many problems of RS



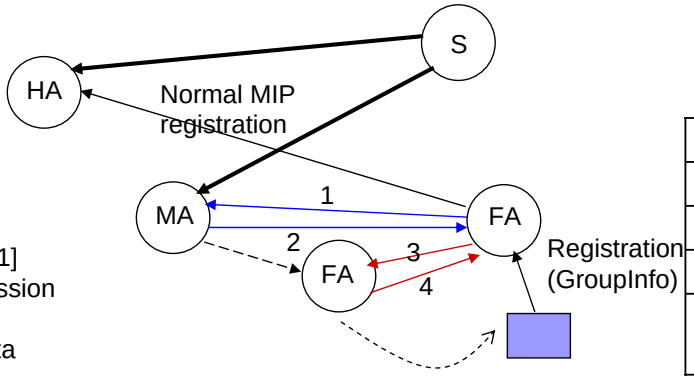
REMMIP

- Objectives
  - Tunneling from MA (multicast agent, HA or FA) instead of HA.
    - FA can be a MA for the MH that visited before.
    - Reduce path length from source to MH.
    - Reduce packet loss and out-of-synch problem
  - Eliminate HAs from multicasting tree
    - If it does not have any MHs in its home network and it does not act as MA for other FAs.
  - Reliable and efficient mobile IP multicasting mechanism.

- MA
  - HA maintains the MH's location.
  - MA is the agent that has a responsibility to send multicast data to a certain FA.
  - MA should join the multicast tree.

1. MH moves to new FA

- MH sends the GroupInfo when it initiates normal mobile IP registration procedure.
- IF the new FA does not receives data of the group.
  - The MH is the first host of the group.
  - FA sends TUNNELING REQUEST[SEQmh+1] to the MA of the MH
  - FA sets the MH's MA to the FA's MA
  - IF there is out-of-synch problem, FA requests RECOVERY REQUEST [SEQmh+1, SEQma-1] to the MH's prev agent.
  - Optionally, MH can send MOVE message to the MH's prev agent.

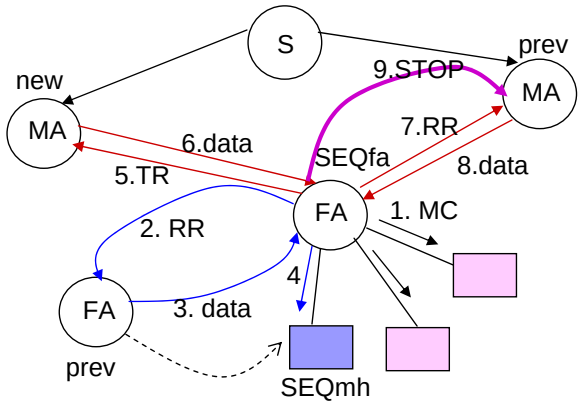


1. TR[SEQmh+1]
2. Data transmission
3. RR[a,b]
4. Recovery data

GroupInfo

Group ID
MA Address
Prev Agent Address
HA Address
Sequence Number SEQmh

- IF the new FA has already received data from other MA.
  - FA selects a MA from the possible MA candidates (current and new).
    - MA changes cause out-of-synch problem for the existing MHs, so it is not recommended.
    - MA selection events
      - When a new MA candidate is added.
    - Many MA selection methods can be considered.
  - IF the MA of the FA is not changed.
    - Notify (MA CHANGE) to the new MH.
    - IF FA cannot send all data [SEQmh+1,SEQfa] to the new MH, FA requests RR [SEQmh+1, SEQfalast-1] to the MH's prev Agent.
      - After FA received the data, it forwards them to the new MH.
    - Optionally, the new MH can send MOVE message to the MH's prev agent.

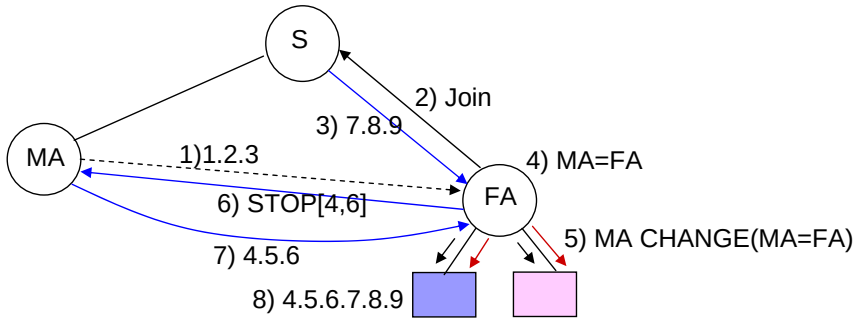


  - IF FA selects a new MA(MH's MA).
    - Notify (MA CHANGE) to all MHs except the new MH in FA network that MA has been changed.
    - FA sets the new MA as its MA.
    - IF FA cannot send all data [SEQmh+1,SEQfa] to the new MH, FA requests RR [SEQmh+1, SEQfalast-1] to the MH's prev Agent.
      - After FA received the data, it forwards them to the new MH.
    - FA sends TUNNELING REQUEST[SEQfa+1] to the new MA.
    - IF there is out-of-synch problem, FA sends RR[SEQfa+1, SEQma-1] to the FA's prev MA.
    - FA sends STOP to the FA's prev MA.
    - FA sends reordered data to all MHs in the network..
    - Optionally, the new MH can send MOVE message to the MH's prev agent.

2. BT to RS by FA

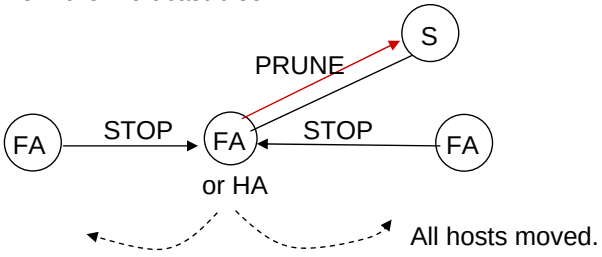
- When FA is not on the tree and uses BT, if one of the following conditions is satisfied, then join the multicasting tree.

1) #MH > Th(N)
   If the number of MHs is greater than threshold value – many customers: optimal routing
2) min(MHt)>Th(T)
   If the minimum staying time of MHs is greater than threshold value – slow mobility
3) Hop(DMSP-FA)>Th(H)
   If the number of hops from DMSP to FA is greater than threshold value – reduce hop count



3. IF agent(HA, FA) recognizes MH's leaving.

- All agents can know MH's leaving
  - Soft state: MH and/or agent periodically transmits membership message.
  - Explicit MOVE message is sent by MH.
- IF there exists no MH of a multicast group.
- TEHN
- Case 1: MA of the agent = Agent (the agent joined tree)
  - Check there is any FA that is served by the agent.
  - IF no, wait a moment (because of RECOVERY REQUEST)
    - Leave from the multicast tree.



- Case 2: MA of the agent! =Agent (the agent is served by other agent)
  - Wait a moment (because of RECOVERY REQUEST)
  - Send STOP to the agent's MA to finish tunneling.