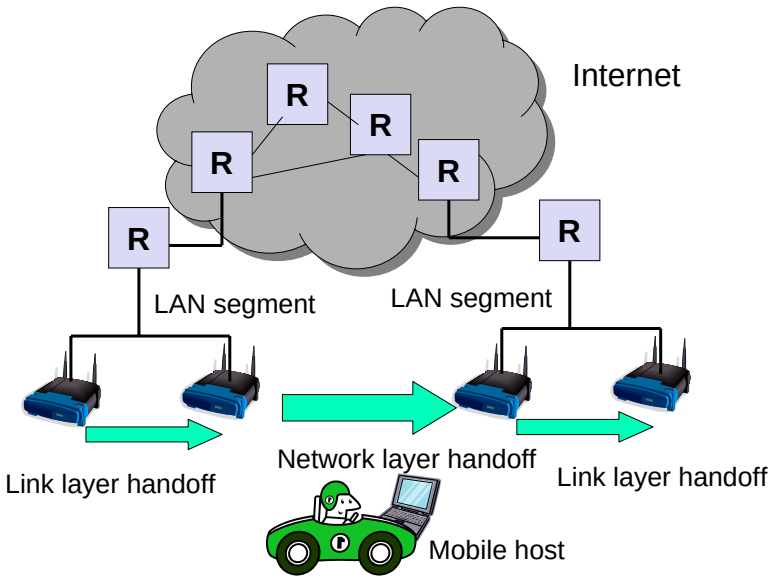
Mobile Routing

Basic Notions of Mobility

- When a host moves, its point of attachment in the network changes. This is called a handoff.
  - The point of attachment is a base station (BS) for cellular network, or an access point (AP) for WLAN.
  - We will assume WLAN in our examples. Problem essentially the same for cellular networks.
- Handoff can be handled completely in the link layer, if both the APs involved are in the same network.
- Otherwise, a route change in the IP layer may be needed. This is called network layer handoff.
- Mobile IP is a standard protocol for handling network layer handoff.

Illustrating Link Layer and Network Layer Handoff



Motivation for Mobile IP

How IP routing works?

- IP addresses are assigned in a topologically significant fashion. All hosts in a network shares the same network address (e.g., 129.13.42).
- Routing is generally based on prefixes. For example, a packet for 129.13.42.12 is forwarded to network 129.13.42 unless there is a different host-specific route.

What if a hosts moves to a different network? Two solutions:

- The host carries the old IP address. Maintain host-specific routes for all mobile hosts on all routers. Not scalable, because of too many individual routes need to be maintained.
- Change IP address of the mobile host to an address in the new network. Upper layer connections (such as TCP) will break. Also, not easy to find IP address for a mobile host that moves frequently.

Mobile IP solution:

- Preserve the original address, but also use a new care-of-address (COA).

Why is Mobile IP Complex?

Need transparency

- Need to be transparent to any upper-layer protocol (such as TCP).
- So, cannot really change the IP address of MH.
- But MH is in a different network after handoff. This new network has a different network address!!

Need compatibility

- Cannot change the Internet addressing scheme just to support Mobile IP!
- Cannot change the routers.
- Mobile hosts must be able to communicate with fixed hosts in the Internet that may not speak mobile IP.

Core Idea of Mobile IP

- Transform the mobility problem into a routing problem.
- Use two IP addresses for the mobile.
- Preserve the original IP address. But borrow a new IP address (COA) in the newly visited network.
- Use forwarding: A specific host (typically the router) in the “home” network forwards IP datagrams to the new COA.
- Mobile IP does not need wireless network. The handoff between two networks may involve physical wireline connection/disconnection.
  - Idea is to simply be able to make the change in network transparent to upper layer.
  - Mobile IP does not dictate how the change might happen.

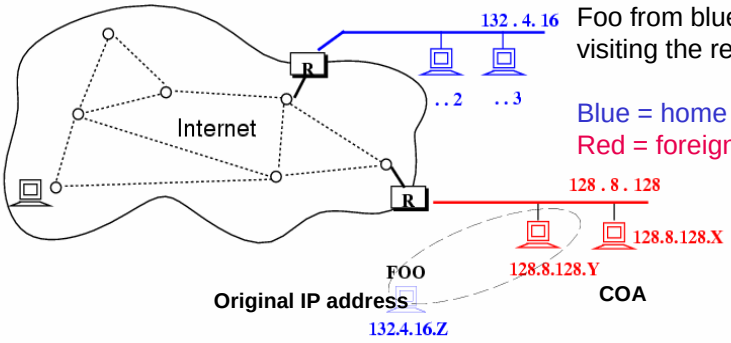
Basic Mechanism: Analogy With Post Office

- Similar to mail forwarding in post office.
- Example: You have moved from your home to Stony Brook for grad studies. What happens to your mail to your home address?
- Solution 1: Notify all your correspondents about your address change. But we need a transparent solution.
- Solution 2: Use the mail forwarding service in the post office. Good idea. Transparent to your correspondents.
- Explore the second solution.
  - You notify the home post office about your address change.
  - Home post office intercepts all your mail. They do this anyway to deliver your mail to you. They now see that you have a forwarding address.
  - Home post office puts your mail in another envelop with your forwarding address. Your real address is still the home address.
  - Home post office mails that envelop again.
  - You get your mail from the Stony Brook post office at your forwarding address.
  - You open the envelop and recover the original mail.
  - The original mail is indistinguishable from the mail you would have gotten at home!

Mobile IP = Mail Forwarding in IP Networks

- Terminology:
  - Home network: Network where the MH got its IP address from.
  - Home Agent: A software entity in the home network that does the encapsulation and forwarding. Typically, runs on an appropriate router.
  - Foreign network: Any network the MH is visiting.
  - Foreign Agent: A software entity in the foreign network that performs the decapsulation. Could run on the MH or on an appropriate router.
- Three basic steps in Mobile IP
  - Agent advertisement (to determine availability of service)
  - Registration (to notify about needed service)
  - Tunneling (to get the actual delivery)

Mobile IP Example



Foo from blue network visiting the red network

Blue = home network
Red = foreign network

- Mobile host retains its original IP address; but borrows the service of a new COA for the network that it is visiting.
- Several mobile hosts can share the same COA. In that case the COA is actually the IP address of a router running the foreign agent. But this does not need to be the case.

[Example due to Charles Perkins]

A Note on IP Routing

- Why do we really need forwarding? Why cannot the MH simply use the original IP address in the foreign network? Why a new COA?
- In the post office analogy, this means that you will continue using your home address while in Stony Brook.
  - This is ridiculous in the post office system.
  - In IP network this is not impossible. But impractical.
- IP routing is hierarchical. IP addresses are assigned in a topologically significant fashion. All hosts in a network share the same network address (e.g., 132.4.16.).
  - Routing is generally based on prefixes. For example, a packet for Foo (132.4.16.Z) is forwarded to network 132.4.16. unless there is a different host-specific route.
  - Providing host specific routes to all mobiles is not scalable, given that such routes must be updated when the move.

Terminology

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

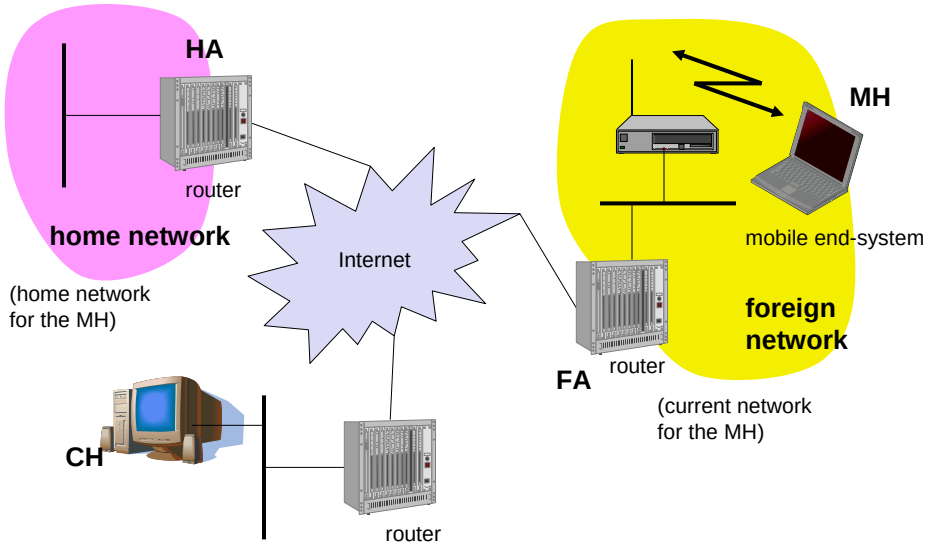
Foreign Agent (FA)

- 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

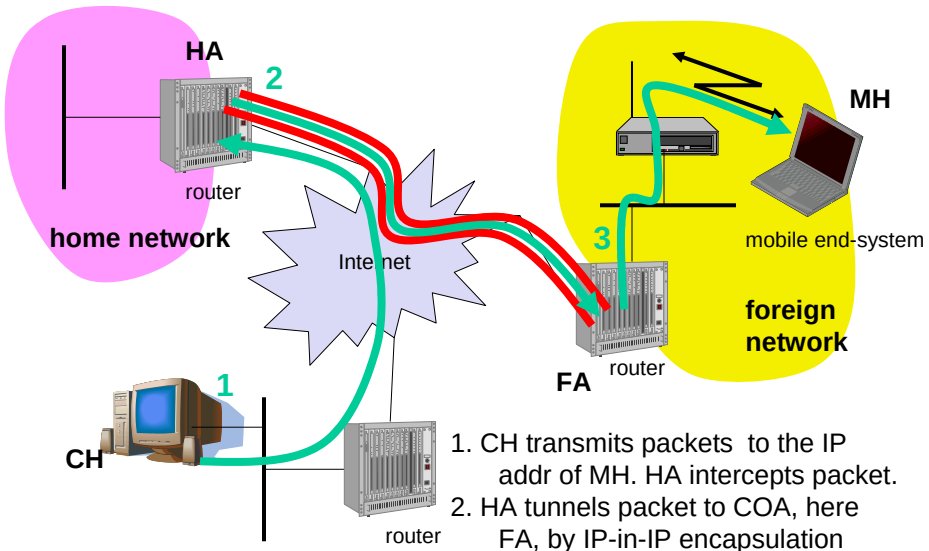
Care-of Address (COA)

- 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

Mobile IP Illustration

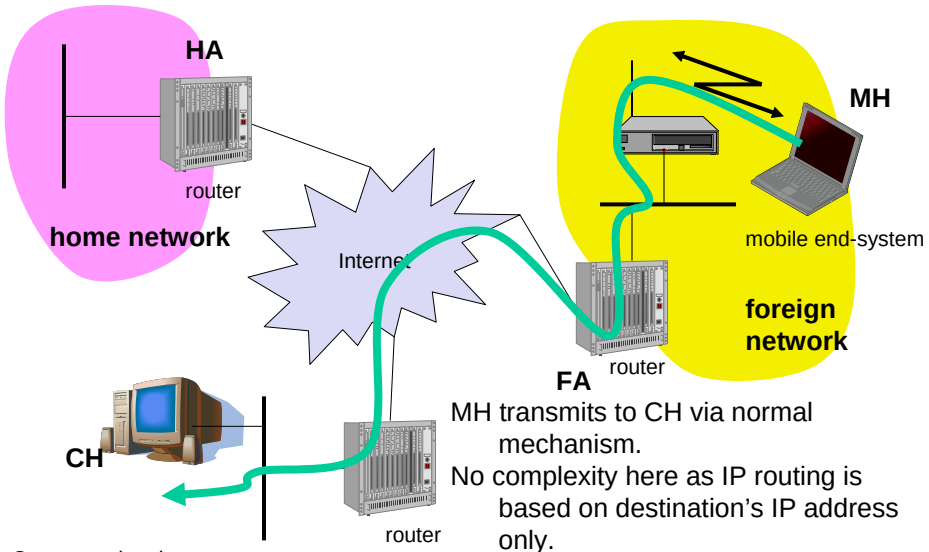


Transfer to the Mobile Host



1. CH transmits packets to the IP addr of MH. HA intercepts packet.
2. HA tunnels packet to COA, here FA, by IP-in-IP encapsulation
3. FA decapsulates and forwards the packet to the MH.

Transfer from the Mobile Host

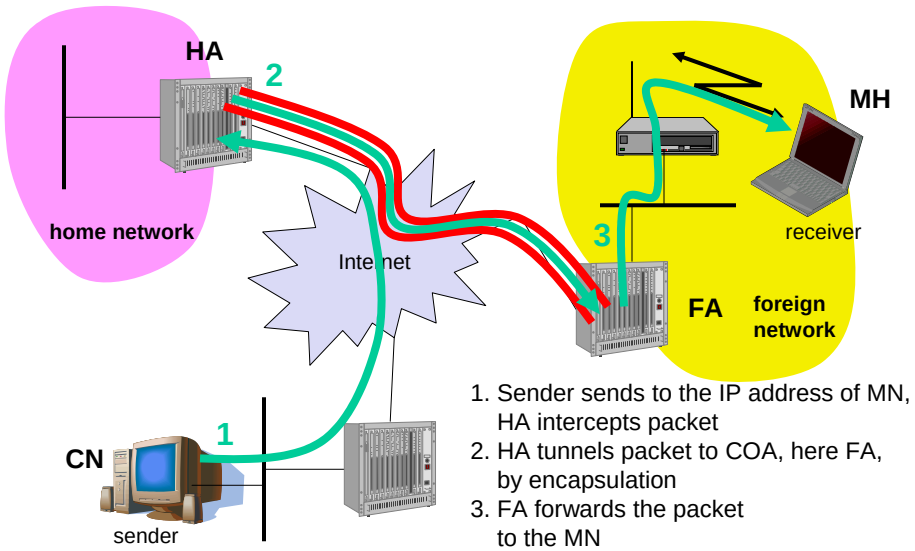


MH transmits to CH via normal mechanism.

No complexity here as IP routing is based on destination's IP address only.

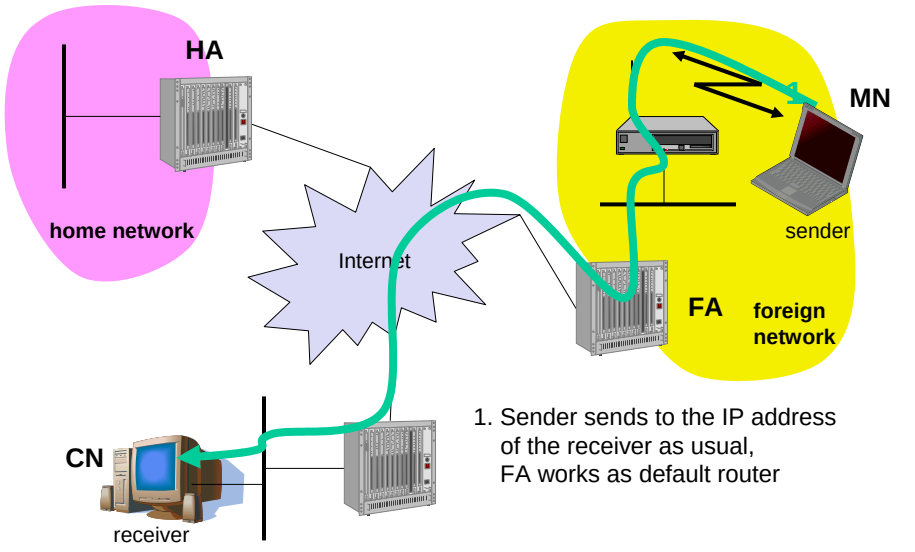
FA acts as the default router in this example.

Data transfer to the mobile system



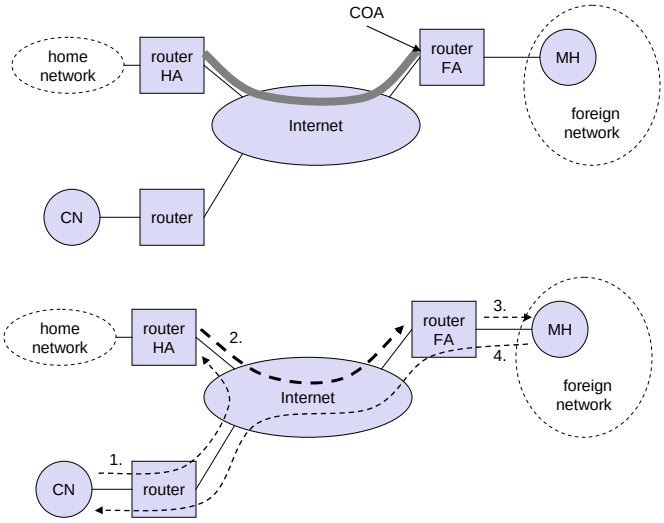
1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



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

Overview Picture



Agent Advertisement and Registration

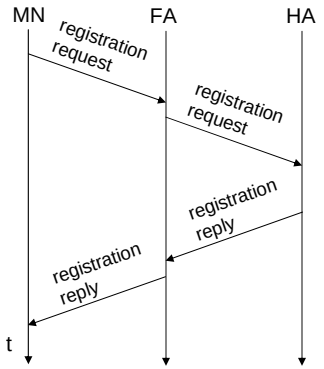
Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets.
- MH listens to these messages and detects, if it is in the home or a foreign network.
- MH reads a COA from the FA advertisement messages.

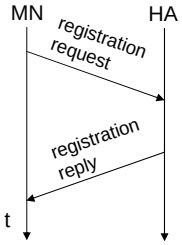
Registration (always limited lifetime!)

- MH signals COA to the HA via the FA, HA acknowledges via FA to MH.

Registration

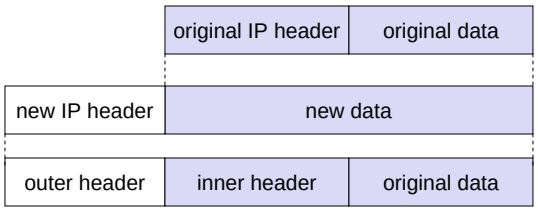


Registration via FA



Registration via collocated COA (No FA involved, MH itself performs the FA actions. Collocated COA can be gotten via DHCP)

Tunneling (IP-in-IP Encapsulation)



- All packets to MH is intercepted at HA and tunneled to the COA.
- Uses IP tunneling (IP-in-IP encapsulation), similar to MBone.
- Outer IP packet has COA as the destination and HA and the source.

Encapsulation I

Encapsulation of one packet into another as payload

- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation

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 II

Minimal encapsulation (optional)

- avoids repetition of identical fields
- e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
- only applicable for unfragmented packets.

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			

Some More Details

Communication from CH to MH:

- Source IP address: CH, Dest IP address: MN
- Goes to the home network. HA intercepts.
- HA encapsulates and tunnels packet to foreign network. Addresses on the outer packet: Source: HA, Dest: COA

If COA is on FA, FA decapsulates packet and delivers to MH via a local mechanism.

- This local mechanism is not a part of mobile-IP specs. Note here MH uses its home network address.
- Local mechanism could be as simple transmitting on a Ethernet segment.

If COA is on MH (collocated COA)

- Packet is directly delivered to MH.
- MN itself decapsulates packet.

Communication from MH to CH:

- Source IP address: MH, Dest: CH

Optimizations

"Triangular Routing"

- CH sends all packets via HA to MH.
- higher latency and network load.

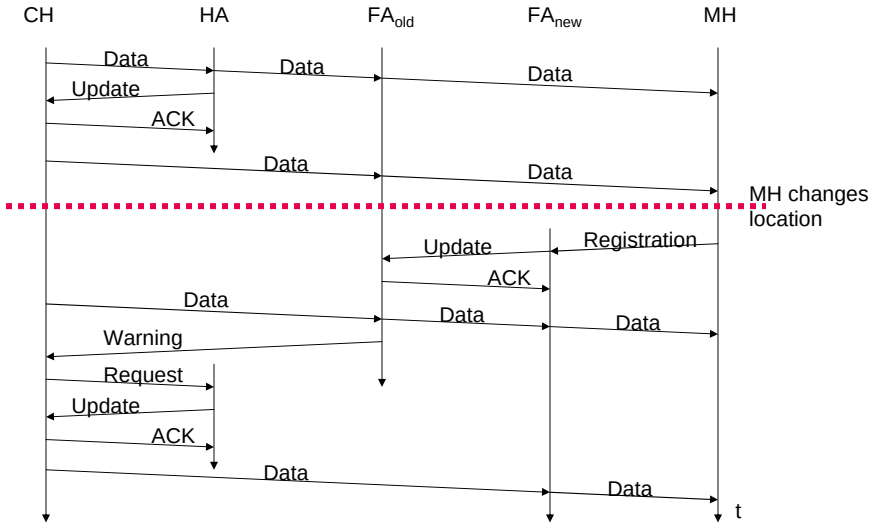
Solution

- CH can learn the current location (COA) of MH from the HA.
- Then CH can directly tunnel the packet to the COA.
- However, this requires that CH also speaks Mobile IP.

Change of FA

- Packets in transit 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 MH.

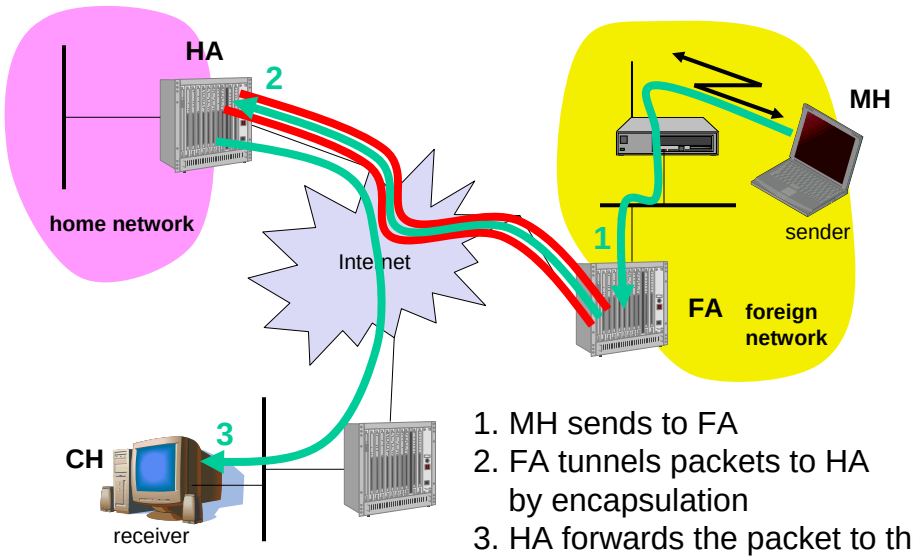
Illustration: Change of foreign agent



Reverse Tunneling

- The packets originating from MH in the foreign network has the source address from the MH's home network.
- Often a firewall in the foreign network will filter such packets for security reasons, as the source addresses are not "topologically correct."
- To avoid this, FA can "reverse tunnel" packets to home agent.

Reverse Tunneling



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