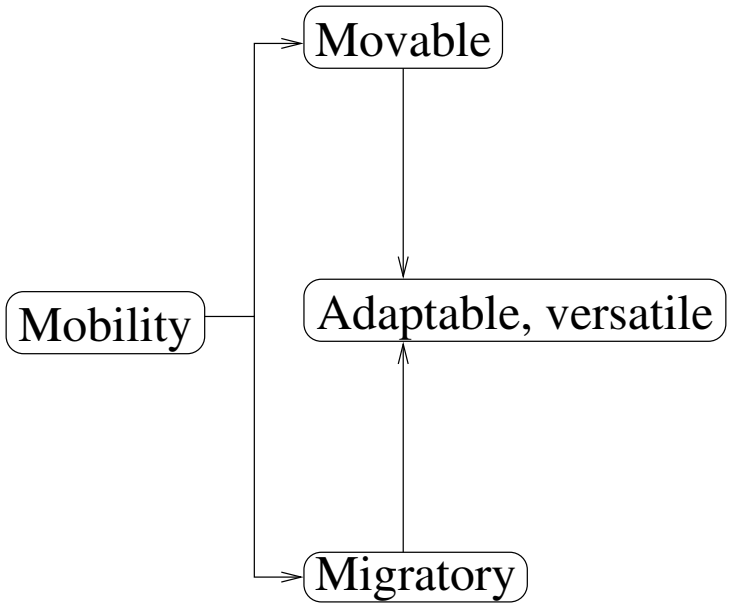
Agenda

The lecture contains: Mobility management of user, terminal and applications.

- Definition of mobility.
- Types of mobility.
- Terminal mobility both macro/micro mobilities.
- Personal mobility or roaming.
- Mobile IP

Mobility and types of mobility

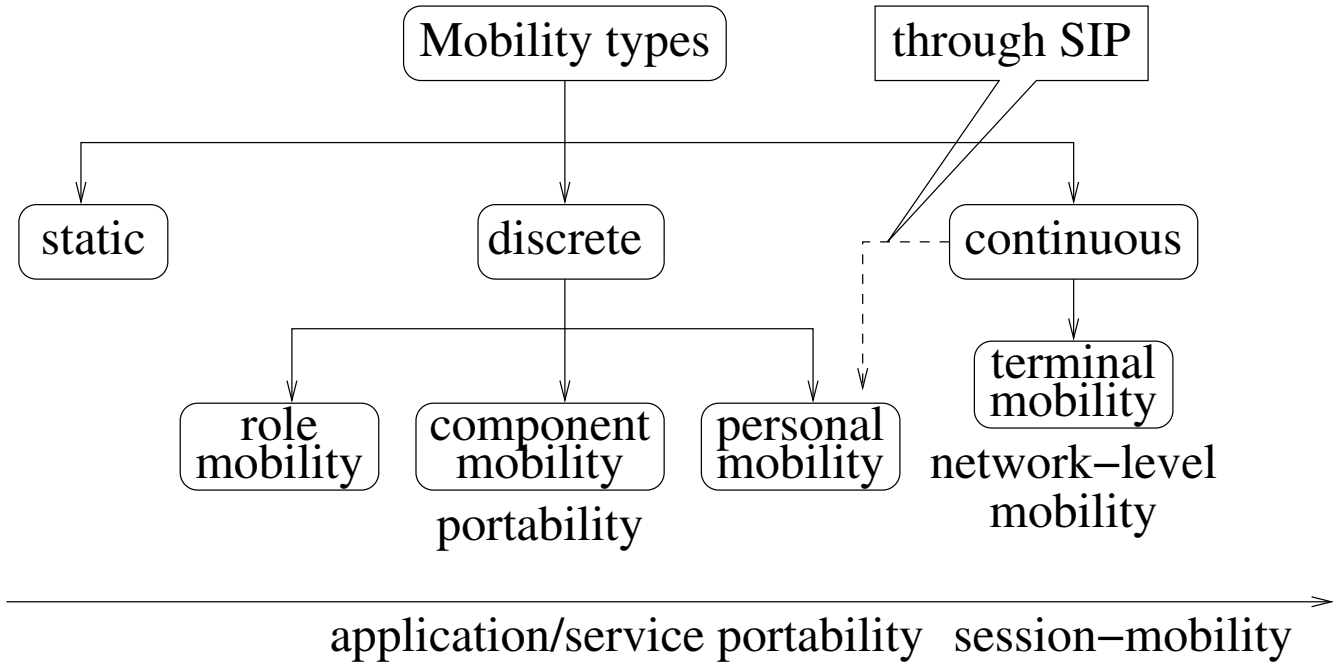
Mobility



- Wired and wireless networks both offer mobility.
- Wireless may not always mean mobility.
- Mobility enhances availability of service.
- Mobility without accompanied services is meaningless.

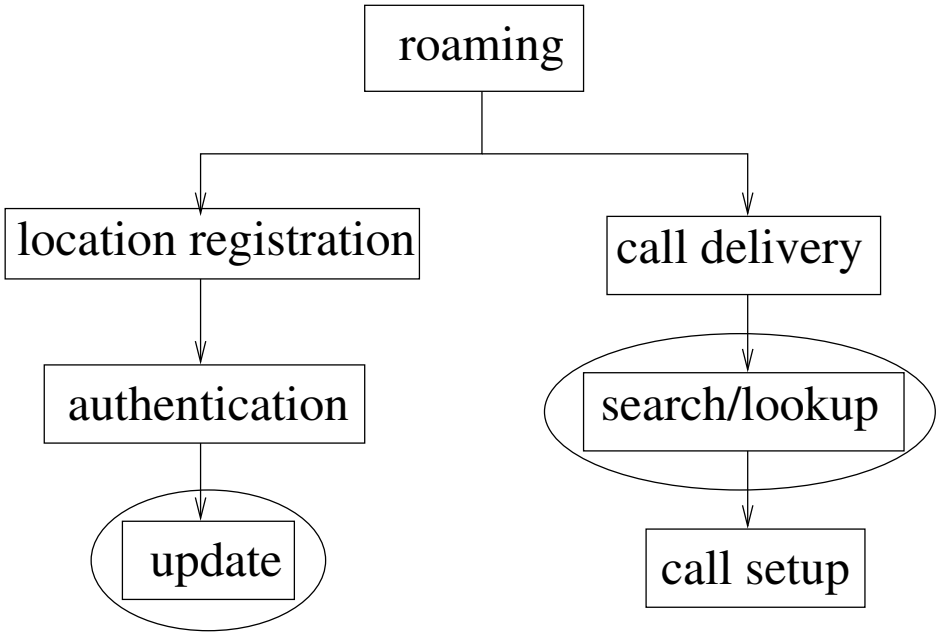
Mobility and types of mobility

Types of mobility



Mobility and types of mobility

Roaming



Search and **update** are basic.

Mobility and types of mobility

Terminal mobility

- Moving terminal to new location while maintaining services.
- Terminal mobility can be provided in network layer.
  - **Mobile IP:** IP addressed does not change.
  - **DHCP:** IP address changes.

Mobility and types of mobility

Application mobility

- **Session mobility:** active session not disrupted while terminal or person relocates: eg., call transfer, handover.
- **Role mobility:** each person may have several roles.

Mobility and types of mobility

Summary of mobility service types

Mobility type	Continuous	Discrete
Personal	SIP (not implemented)	Login
Terminal	Mobile IP (not implemented)	LAN
Application	Mobile agent (not implemented)	Applet/servlet

Mobility and types of mobility

Terminal mobility at different layers of network

- Most common way of implementing mobility (discrete mobility or IP roaming service) is simple **PPP** dial-up.
- Utilizes public telephone network.
- Another way is **DHCP**: offers topologically correct IP address.
- Both provide **nomadicity** but not mobility.

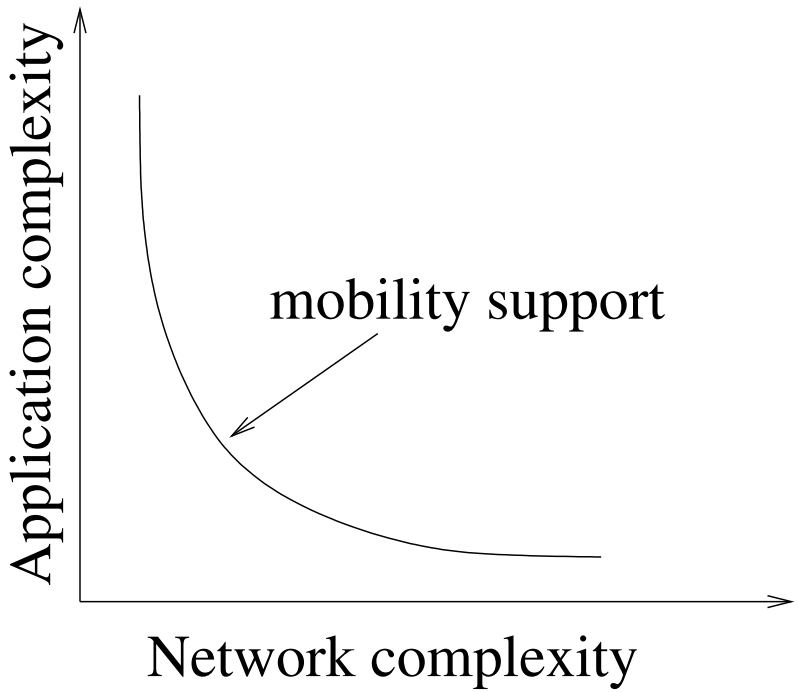
Mobility and types of mobility

Terminal mobility at different layers of network

- Possible to implement mobility at **application** or **transport** layer.
- Conceptually the approach in either case is the same because
  - Network layer should be identified with new IP address (IP address to be **released** & **renewed**)
  - Terminal's application as well as corresponding servers in home network have to be updated.
  - But it simplifies routing (no **tunneling** is required).

Mobility and types of mobility

Terminal mobility at different layers of network



- Accessing home network independent of access technology is not possible,
- Change in IP address causes transport level connection to break.
  - session continuity can not be maintained.
- Two-way information exchange such as VoIP connection or video conferencing not possible.

Mobile IP

Communication invariants

- A protocol for seamless macro mobility with diverse access technologies.
- Relies on link layer technology for radio specific mobility issues.
- Allows users to keep same IP address, stay connected, and maintain ongoing application while roaming.
- Maintains the following communication invariants.
  <src IP address, src port no., dest IP address, dest port no.>

Mobile IP

Importance of IP address

- Interruption in remote login, remote printing and file transfers undesirable while roaming across n/w boundaries.
- Access privileges, software licensing are also based on IP addresses.
- IP address universal for most applications.
- N/W layer is present at all internet nodes, and responsible for routing packets to proper locations.
- Mobility across internet is possible even if physical medium (wired/wireless interfaces) has been changed.

Mobile IP

User view of IP Mobility

- MN must be able to communicate with other nodes by changing point of attachment but keeping same IP address.
- MN should be able to communicate with nodes not implementing mobile IP.

Mobile IP

Implementer's view of IP mobility

- Location update messages of a node on another node should be authenticated to prevent remote re-direction attacks.
- Should support wireless link (number and length of control messages should be minimized)
- No extra constraints on IP address assignment policies (like IP address range restriction).
- Should support frequent moves (could be 1 per second).
- No extra support from link layer operation of MN
  - Link-layer may provide link layer handoff (in same subnet).

Mobile IP

A top level overview

- Mobile IP associate **two IP addresses** with each mobile node:
  - a static **home address**, and
  - a dynamic **care-of address**.
- Messages to a mobile node can be delivered by tagging them with care of address when it is outside home network.

Mobile IP

Involved entities

- Home agent (HA)
- Foreign agent (FA)
- Care of Address (COA)
- Correspondent Node (CN)

Mobile IP

Component services

- Agent discovery
  - Beacon messages broadcast via ICMP router discovery at regular intervals from FA and HA.
  - MN listens to beacons and sends registration request.
- Registration or binding: binding request from MN sent to HA via FA.
- Encapsulation: done by HA to send CN's messages to MN through COA.
- Decapsulation: done by FA for delivering to MN within its own network.

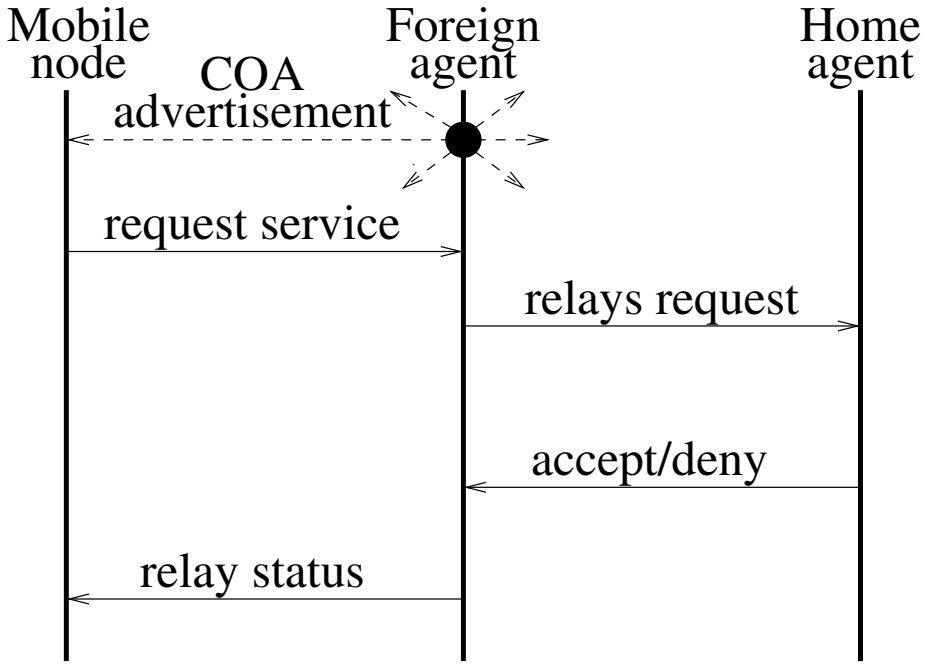
Discovery of care-of address

Router advertisements

- MN ability to discovers new mobility agent is based on ICMP router advertisement.
- RAs are extended to include additional mobility information.
- RAs allows MN to
  - Detect its movement.
  - Get network number and status of their link to the Internet
  - Determine if the agent is a FA or HA and if MN is in the domain of HN or FN.
- MN also can seek a COA by broadcasting a **solicitation** message to agents.

Registering a care-of address

Binding



- When MN moves (acquires a new COA) the current binding changes.
- Registration process updates existing binding.

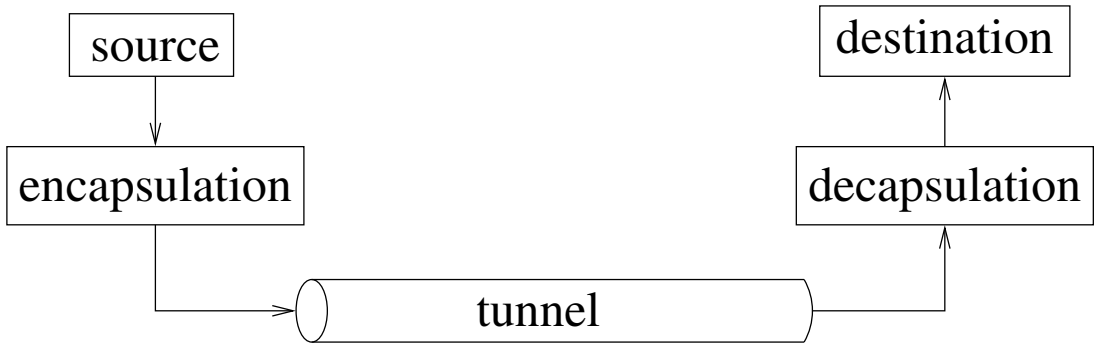
Registering a care-of address

Authenticity of binding request

- Security association (SA) between a MN with its HA is required.
- With SA, a MD5 can be used create a digital signature that accompanies binding updates.
- Replay attacks can be prevented if a unique **nonce** also accompanies binding update.

Tunneling

IP-in-IP encapsulation



- Original packet is becomes payload to new packet
- An outer IP header is created for delivering packet from entry point to exit point of the tunnel.

Tunneling

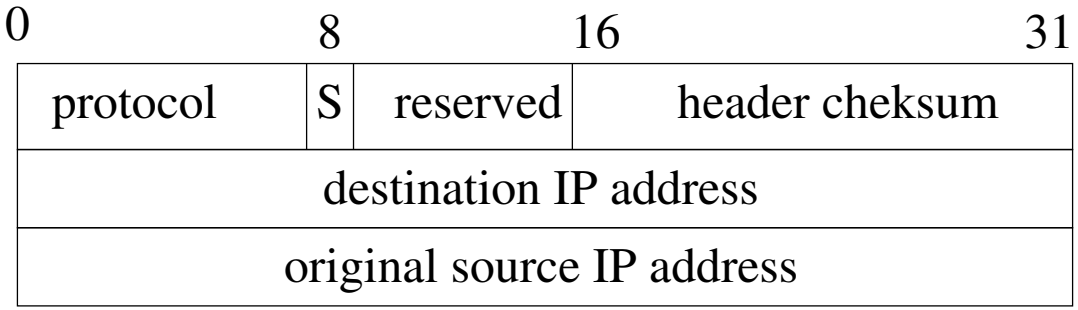
Minimal encapsulation

- Can not store fragmentation information.
- Includes IP header + Minimal encapsulation header.

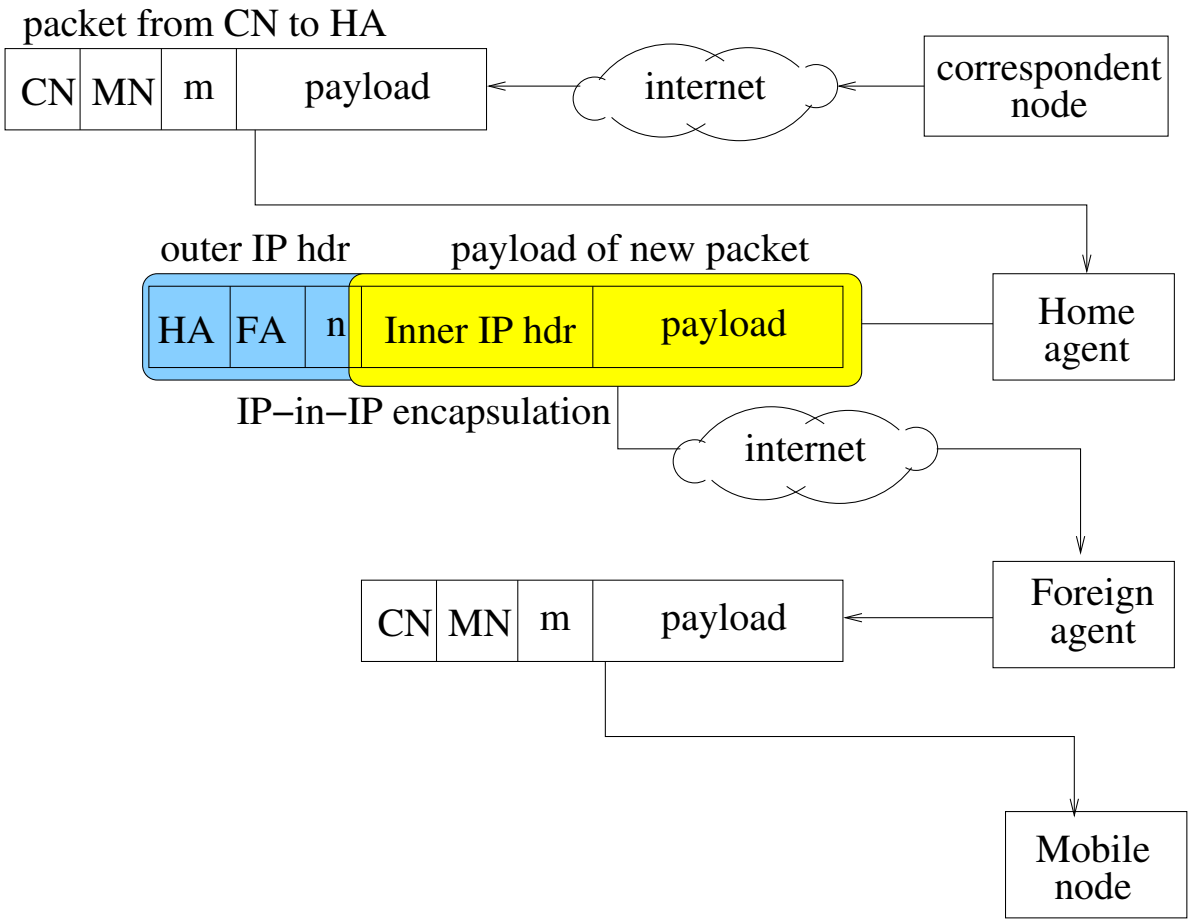
IP header modified as follows:

1. Destination address: IP address of tunnel exit point (COA).
2. Source address: IP address of encapsulator (HA).

Minimal encapsulation header:



Mobile IP


packet from CN to HA
CN
MN
m
payload
internet
correspondent node
outer IP hdr
payload of new packet
HA
FA
n
Inner IP hdr
payload
Home agent
IP–in–IP encapsulation
internet
CN
MN
m
payload
Foreign agent
Mobile node

Handoffs in mobile IP

- Essentially, MIP provides handoff at IP layer.
- When MN leaves a n/w and enter another it has to perform IP layer handoff.
- IP handoff is supported by three steps:
  1. Link-layer handoff:
  2. Mobile IP movement detection.
  3. Mobile IP registration.

Handoffs in mobile IP

Link layer handoff

- There are two modes of operations: BSS and ESS.
- In ESS mode AP acts as bridge forwarding traffice over DS.
- An ESS assigns an identifier (ESSID).
- When MN moves away from AP its SNR decreases: LL handoff initiated.
- MN scans (passive/active) for potential APs with ESSID (monitoring for a beacon message): takes $\approx$ 90% of time.
- MN is authenticated (may be by WEP)
- MN then gets associated with AP.

Handoffs in mobile IP

Movement detection

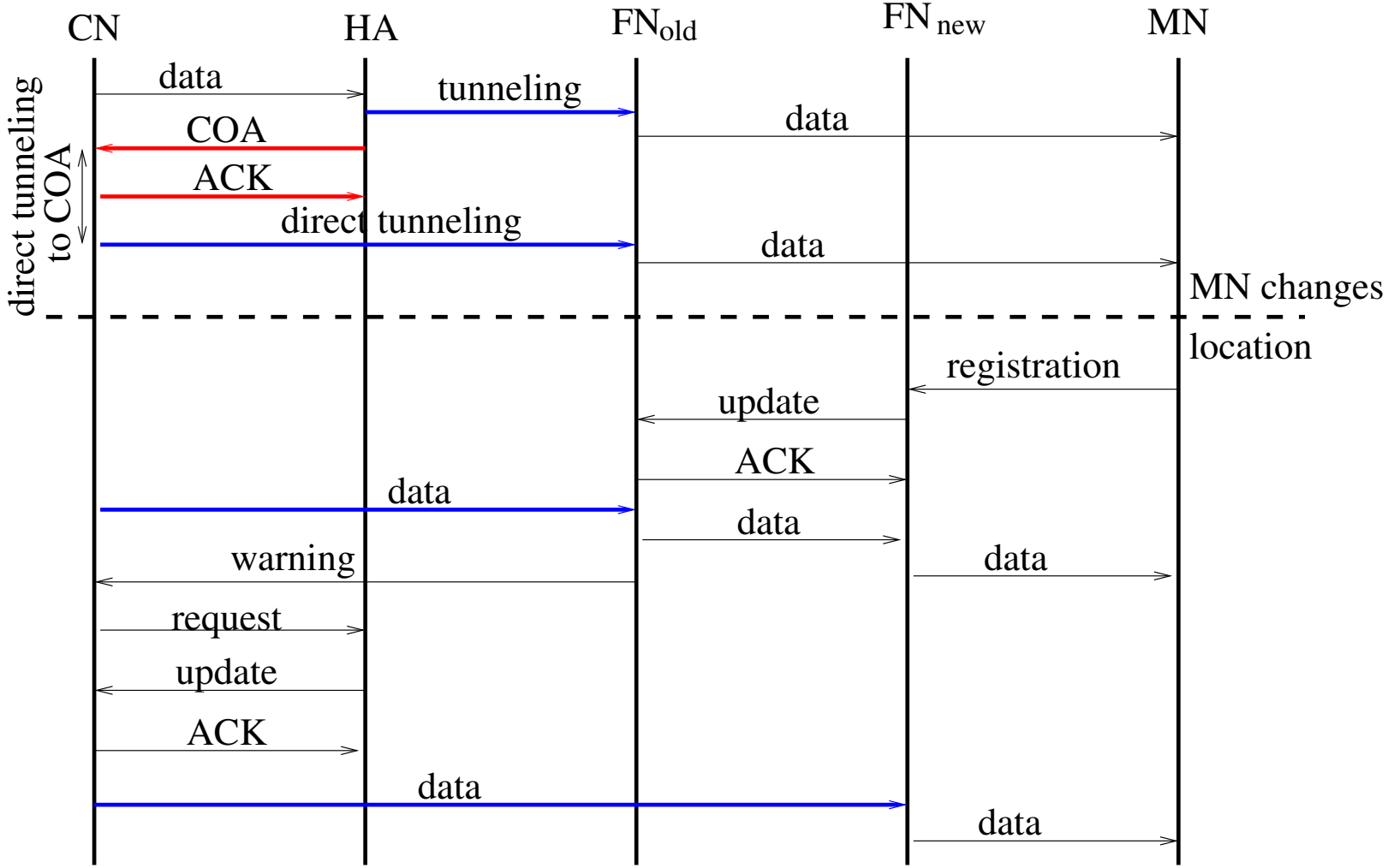
- Due to layer independence, detection of movement can not be communicated from LL.
- Alternative mechanism required at IP layer.
- If MN discovers agent from RA, the movement is detected
  1. If MN receives a previously undiscovered RA.
  2. Loss of contact with discovered agent.

Handoffs in mobile IP

Cell switching

1. Lazy cell switching: handoff delayed until current RA becomes unavailable.
   - Non-availability is determined by a timeout (3 seconds).
2. Eager cell switching: handoff initiated as soon as new RA is received.
   - Usually preferred as MN should be attached to only one node.

Overall component interactions



Reverse Tunneling

- Data from MN to CN can sent directly (bypassing HA) - assumes that CN has a public routable address (no private address).
- Some network may also prevent packets from source IP not belonging to its domain.
- So reverse tunneling will be required. This tunnel is from foreign agent to home agent of MN.
- It essentially provides functionality of a NAT.

ARP Proxy

- What happens when a local node (unaware of Mobile IP) from Home N/W send messages?
- It will know that mobile node belongs to same subnet, so tries to send data directly.
- So it uses ARP to find data link layer address of MN. It may first look into ARP cache, if no cache entry found than CN will send an ARP request.
- There will be no answer to these requests.

ARP Proxy

- To solve this problem HA intervenes in following way.
  - **ARP proxying:** HA listen to all ARP requests concerning mobile nodes currently registered with it. HA answers these requests on behalf of these MN nodes providing its own h/w address.
  - **Gratuitous ARP:** To tackle stale ARP cache cache entries, HA informs all devices in the N/W to associate H/W addresses of all these MNs to its own h/w address. The message is sent more than once to ensure every device get it.

Summary

- In this module, we learnt about various types of mobilities.
- We found a set of protocols already in place to provide restricted form of discrete personal mobility and terminal mobility.
- It is also possible to realize mobilities at different network layers.
- Mobile IP is a technology which is meant for continuous macro mobility.
- We examined mobile IP protocol in details.