Mobile Computing
Lecture 20
Protocols for Mobile Computing 1

Contents

- Mobile network layer
- Goals, Assumptions and Requirements
- Motivation for Mobile IP
- Requirements to Mobile IP
- Overview
- Encapsulation
- Problems with mobile IP

Mobile network layer

- In this protocols and mechanisms developed for the network layer to support mobility.
- It provides protocol enhancement that allows transparent routing of IP datagrams to mobile nodes in the internet.
- Mobile IP – Adds mobility support to the internet network layer protocol IP.
- RFC 2002 is a reference document for the complete detail about the mobile IP.

Goals, Assumptions and Requirements

- Receiving of IP datagram after leaving your home network.
- Now nodes needs a so-called topologically correct address.

Quick Solution

- – Assign new IP address when enter into new location.
  - Increase problem with higher layer protocols like TCP , as they rely on IP layer.
  - Routers are built for fast forwarding but not for fast update of routing table.
- – Quick solution not working.

Motivation for Mobile IP

- Routing
  - based on IP destination address,
  - network prefix (e.g. 129.13.42) determines physical subnet
  - change of physical subnet => change of IP address to have a topological correct address (standard IP)
- Solution: Temporarily change routing table entries for mobile host
  - Problem: does not scale if many mobile hosts or frequent location changes
- Solution: Change mobile host IP-address
  - adjust the host IP address depending on the current location
  - DNS updates take to long time
  - Old TCP connections break

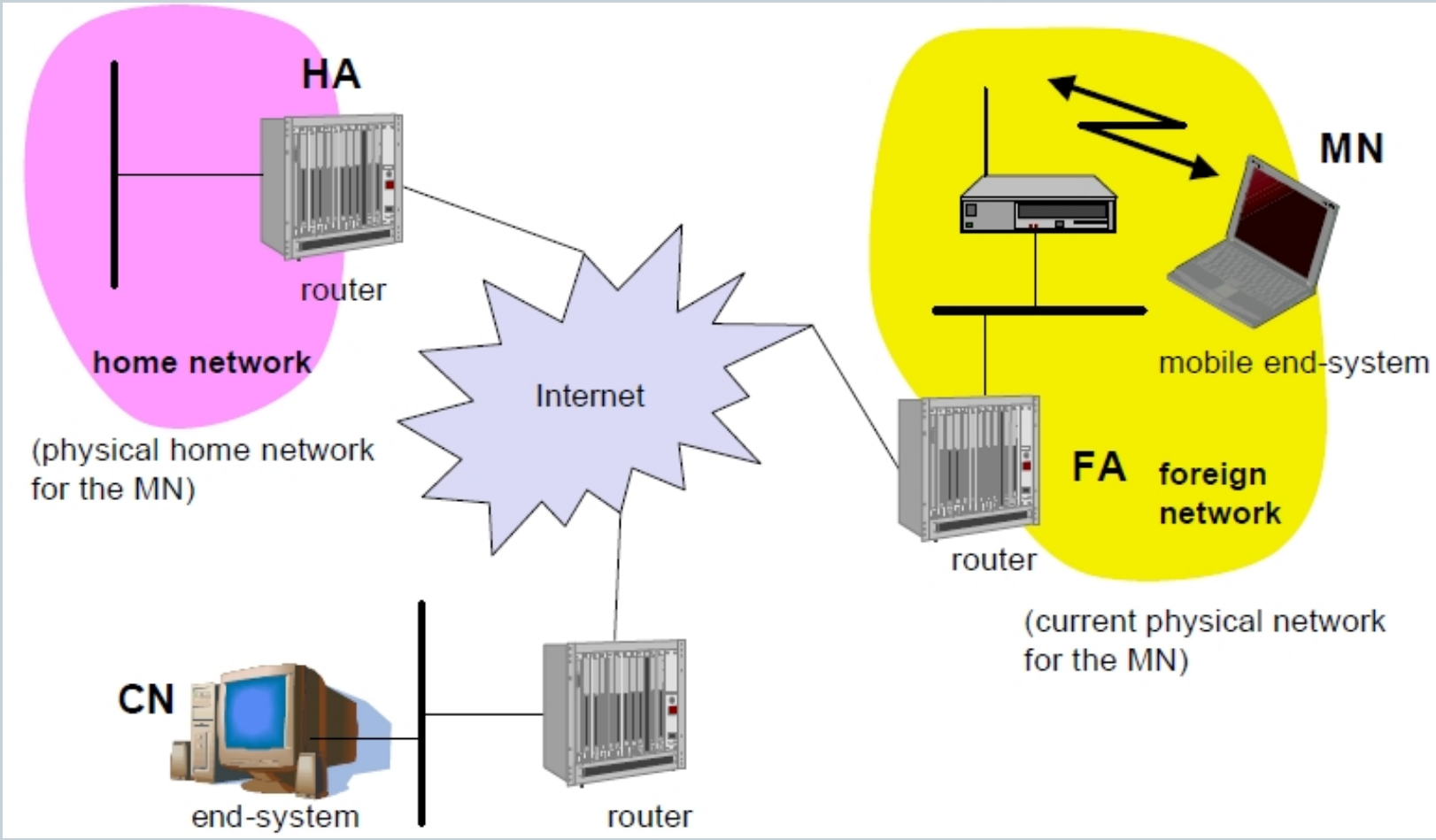
Requirements to Mobile IP

- Transparency
  - mobile end-systems keep IP address
  - Continuous service after link interruption
  - point of connection to the fixed network can be changed
- Compatibility
  - No changes to current hosts, OS, routers
  - mobile end-systems can communicate with fixed systems
- Security
  - authentication of all registration messages
- Efficiency and scalability
  - only few additional messages to mobile system (low bandwidth)
  - Global support for large number of mobile systems

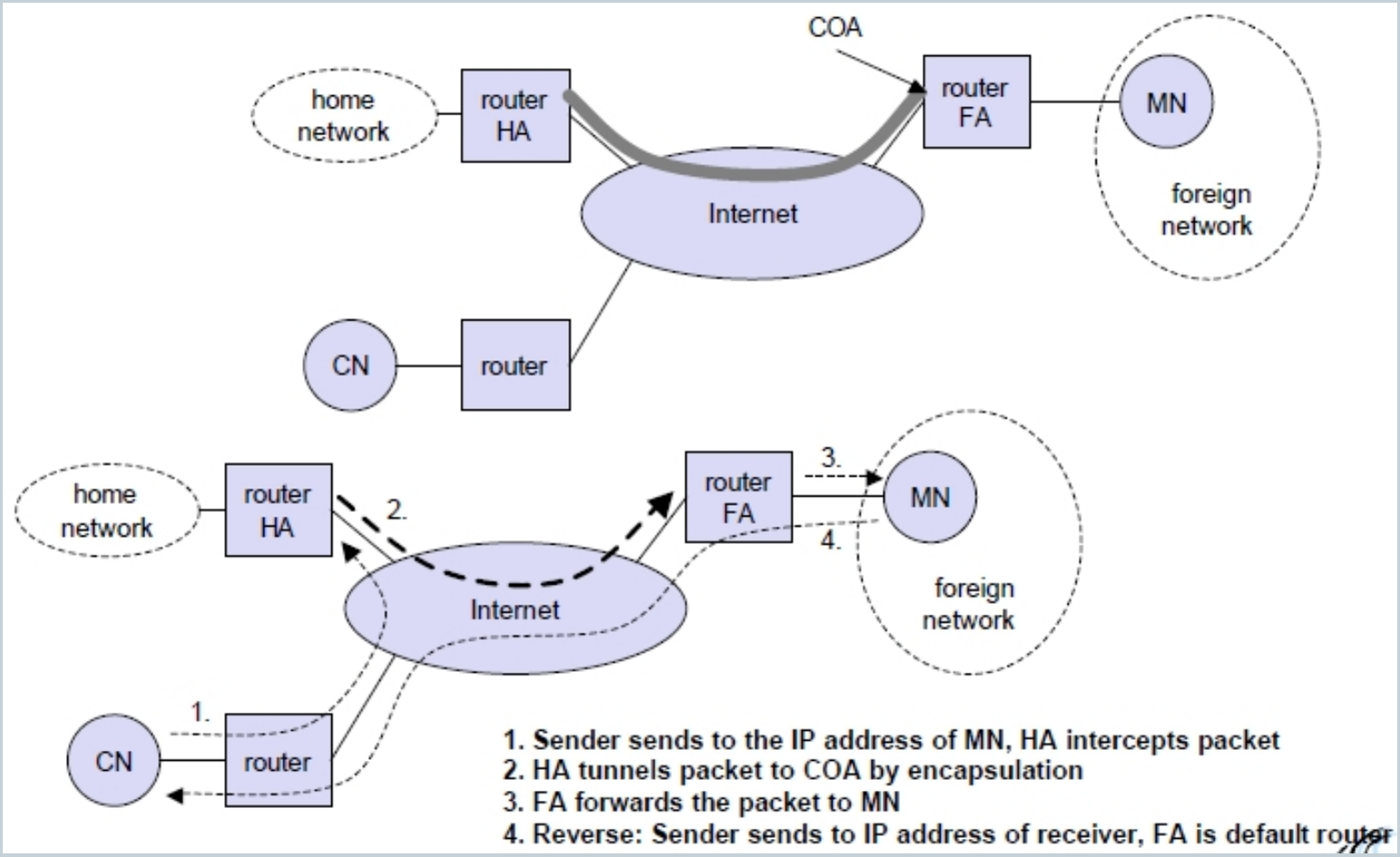
Terminology

- Mobile Node (MN)
  - Laptop, PDA, etc.. that may move about
- Home Agent (HA)
  - Router in home network of the MN, helps in forwarding
  - registers current MN location, tunnels IP datagrams to COA
- Foreign Agent (FA)
  - Router in current foreign network of MN
  - forwards tunneled datagrams to the MN
- Care-of Address (COA)
  - address of the current tunnel end-point for the MN (at FA or MN)
  - can be chosen, e.g., via DHCP
- Correspondent Node (CN)
  - Node that wants to communicate with MN

Example network



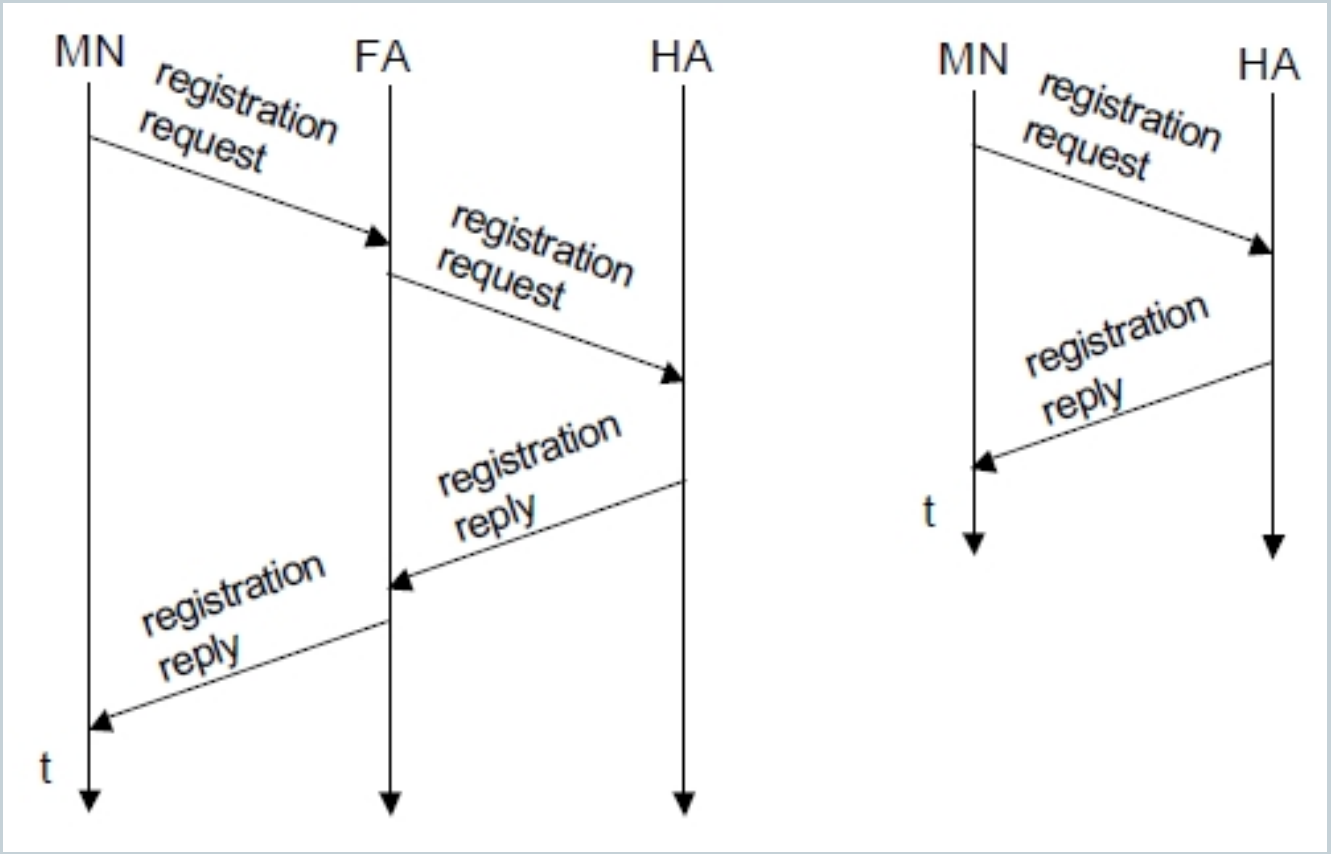
Overview


COA
home network
router HA
router FA
MN
foreign network
Internet
CN
router
home network
router HA
2.
router FA
3.
MN
4.
foreign network
Internet
1.
CN
router
1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA by encapsulation
3. FA forwards the packet to MN
4. Reverse: Sender sends to IP address of receiver, FA is default router

Network integration

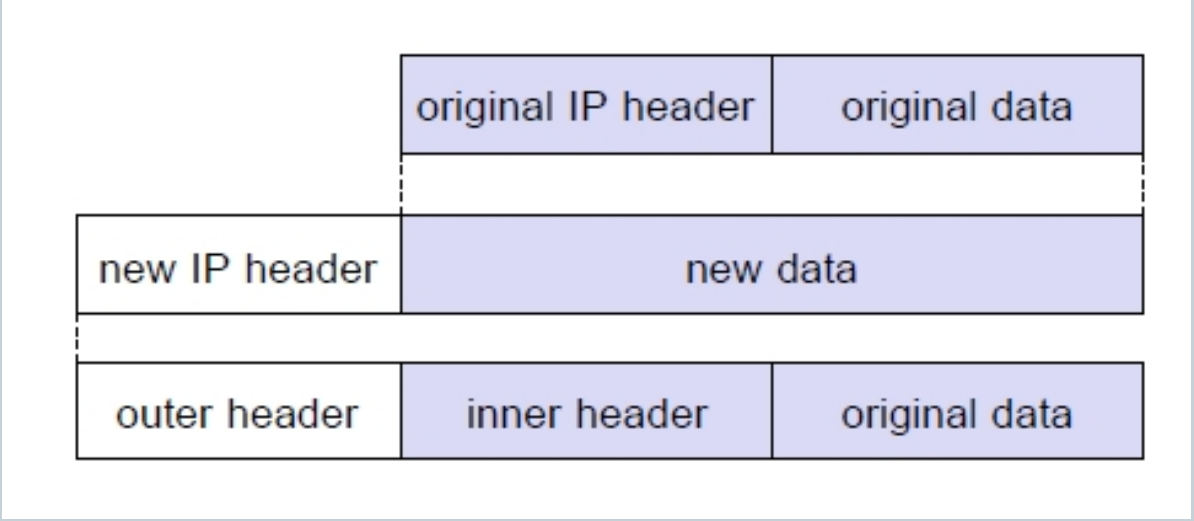
- Agent Advertisement
  - HA and FA periodically send advertisement messages into their subnets
  - MN reads a COA from the FA advertisement messages
- Registration (always limited lifetime!)
  - MN signals COA to the HA via the FA, HA acknowledges
  - Messeges need to be secured by authentication
- Advertisement
  - HA advertises the MN IP address (as for fixed systems)
  - routers adjust their entries, (HA responsible for a long time)
  - All packets to MN are sent to HA

Registration



Encapsulation

- Encapsulation of one packet into another as payload
  - e.g. IP-in-IP-encapsulation (mandatory, RFC 2003)
  - tunnel between HA and COA



Optimization of packet forwarding

- Triangular Routing
  - sender sends all packets via HA to MN
  - Triangular routes longer, higher latency and network load
- “Solutions”
  - HA informs a sender about the location of MN
  - sender learns current location of MN
  - direct tunneling to this location
  - 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 forwards remaining packets to new FA
  - Update also enables old FA to release resources for MN

Mobile IP and IPv6

- Mobile IP was developed for IPv4, but IPv6 simplifies the protocols
  - security is integrated, not add-on, authentication of registration 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**
  - MN can signal a sender directly the COA, without HA
  - “soft“ hand-over, i.e. without packet loss supported
    - MN sends the new COA to its old router
    - old router encapsulates all packets for MN, forwards them to new COA
    - authentication is always granted

Problems with mobile IP

- Security
  - FA typically belongs to another organization
  - authentication with FA problematic
  - patent and export restrictions
- Firewalls
  - Firewalls filter based on IP addresses
  - FA encapsulates packets from MN
  - Home firewalls rejects packet from MN (unless reverse tunneling)
  - MN can no longer send packets back to home network
- QoS

- Security, firewalls, QoS etc. are topics of current research and discussions!