# LECTURE 8

## Mobile IP

# What is Mobile IP?

- The Internet protocol as it exists does not support mobility
- Mobile IP tries to address this issue by creating an "anchor" for a mobile host that takes care of packet forwarding
- Does not discuss handoff initiation or decision process
- Does not discuss flushing or redirecting packets from an old visited network

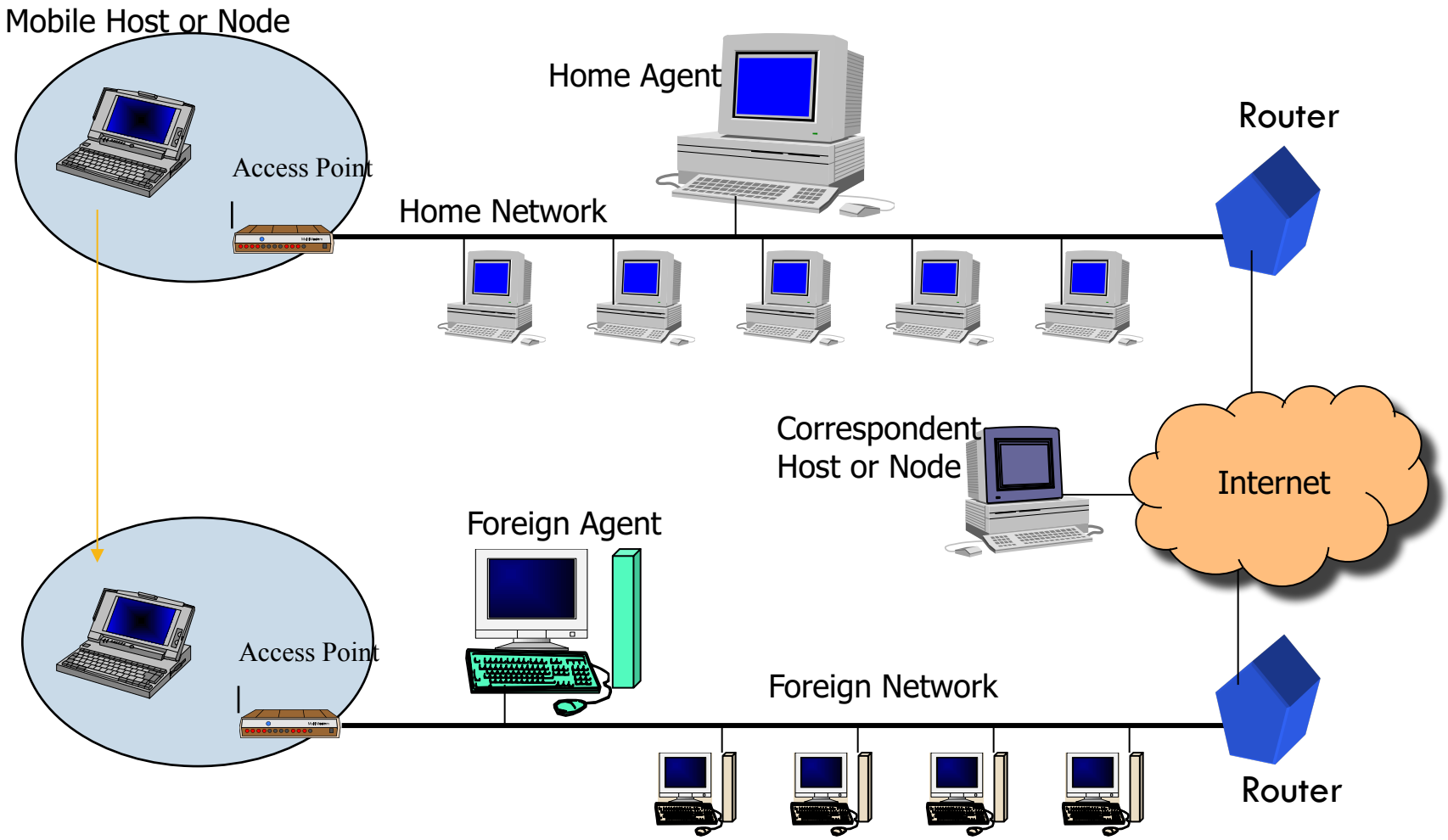
# The Problem!

- The IP address is used for dual purposes
  - For routing packets through the Internet
  - As an end-point identifier for applications in end-hosts
    - A socket consists of the following tuple <source IP address, source port, destination IP address, destination port>
    - A TCP connection cannot survive any address change
    - A domain name is converted to an IP address
- If the IP address is stable, packets get routed to the same place always
- If the IP address is changed, the connection breaks!
- How does a sender know the changed IP address?

# Mobile IP Requirements

- Compatibility
  - Must not require changes to existing network protocols
  - Must not require a new LLC/MAC
- Transparency
  - Invisibility to higher layers (TCP through Application)
  - Invisibility to user
- Scalability and Efficiency
  - Not a great deal of additional traffic
  - No great increase in additional network elements
- Security
  - Security concerns due to changing locations of a mobile node

# Mobile IP Architecture and Terminology



# Terminology I

- Mobile Node (MN)
  - Host that can change its point of attachment
- Correspondent Node (CN)
  - The partner for communication (it can be a fixed or mobile node)
- Home Network
  - IP Network where the MN usually resides
- Foreign Network
  - IP network where the MN is visiting

# Terminology II

- Home Address
  - A long term IP address assigned to the MN that is part of the home IP network.
    - It remains unchanged regardless of where the MN is
    - It is used for DNS determination of the MN's IP address
- Care-of Address (COA)
  - IP address in the Foreign Network that is the reference pointer to the MN when it is visiting the Foreign Network
    - This is usually the IP address of the Foreign Agent
    - Sometimes the MN can act as its own Foreign Agent in which case, it is called a co-located COA

# Terminology III

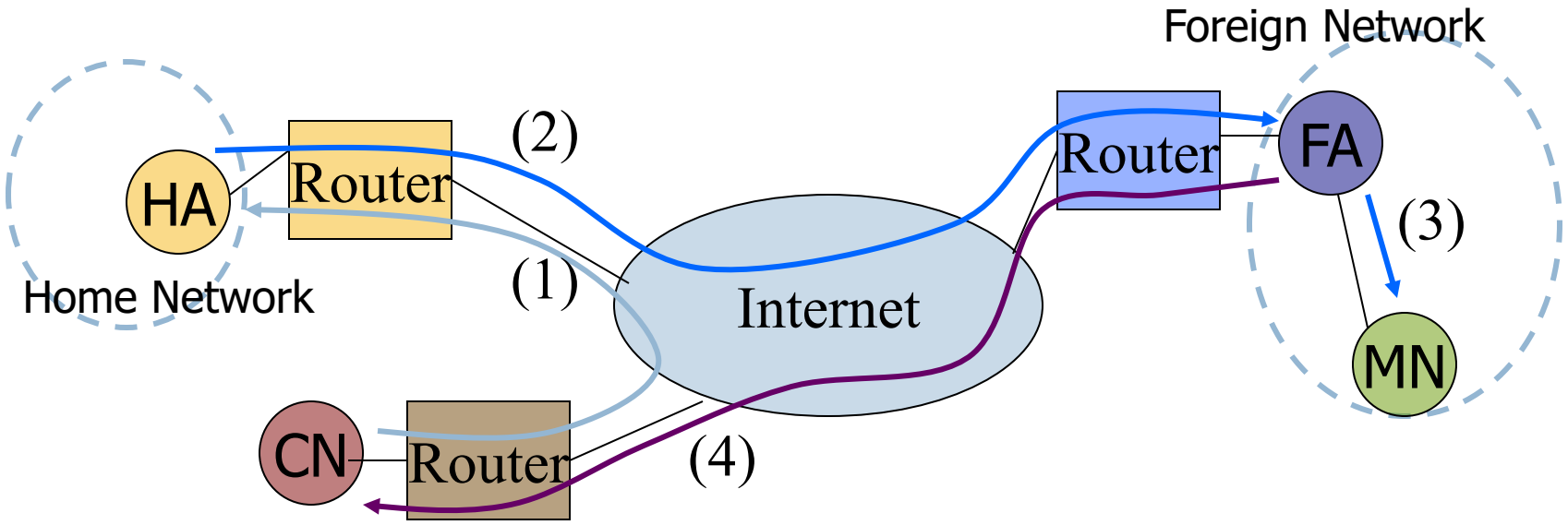
- Home Agent (HA)
  - It is the anchor point for the MN
  - Regardless of where the MN is (except if it is in its home network) packets addressed to it reach the HA
- Foreign Agent (FA)
  - It is the reference IP host for the MN in the Foreign Network

# Protocol Overview

- What does the protocol do?
  - Enables datagrams addressed to the MN at the home address to be delivered wherever the MN is
- Three phases:
  - Delivery to the home network
  - Forwarding to the foreign network
  - Delivery to the mobile node

# Triangle Routing in Mobile IP

- CN transmits a datagram that is routed to MN's home network as usual (1)
- HA intercepts the packet, encapsulates and tunnels it to FA (2)
- FA decapsulates and forwards the packet to MN
- Packets from MN to CN are sent as usual (4)



# Packet Interception by the Home Agent

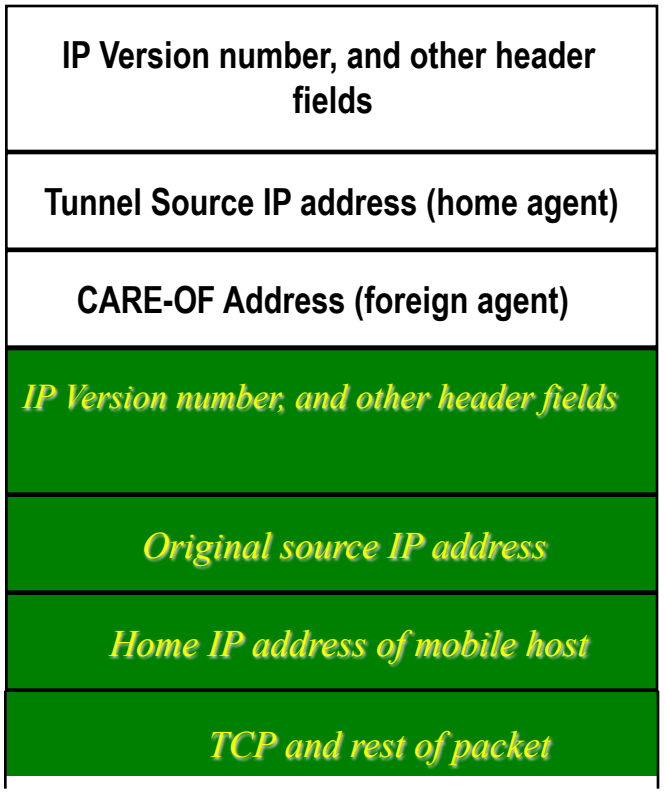
- HA performs a proxy ARP on behalf of the MN when it is away
  - If an ARP request is made to obtain the MAC address of the MN on the home network, the HA responds with its own MAC address
- The MN performs a gratuitous ARP when it returns to the home network
  - Unsolicited ARP reply that is broadcast to each node on the Home Network
  - Some networks do not trigger ARP cache updates based on gratuitous ARP => Mobile IP cannot be implemented correctly

# Packet Encapsulation by HA

- Forwarding packets is achieved by encapsulation (tunneling)
  - Virtual pipe between tunnel entry point (HA) and tunnel termination point (FA)
- The datagram from the CN is made the payload of *another* IP packet
- Three types of encapsulation are provided
  - IP in IP encapsulation
  - Minimal encapsulation
  - Generic routing encapsulation
    - For protocols other than IP

# IP-in-IP Encapsulation

- Mandatory implementation
- The outer header uses IP-in-IP as the protocol type
- The whole tunnel is equivalent to one hop from the original packet's point of view
- Overhead can be reduced since several fields are redundant



# Minimal Encapsulation

- The header in the original packet is stripped of unnecessary information like length, version number, flags, etc.
- The Home Address of the MN and the original source address (of the CN) are retained
- Since the fragment offset field is also removed, it does not work with fragmented IP packets

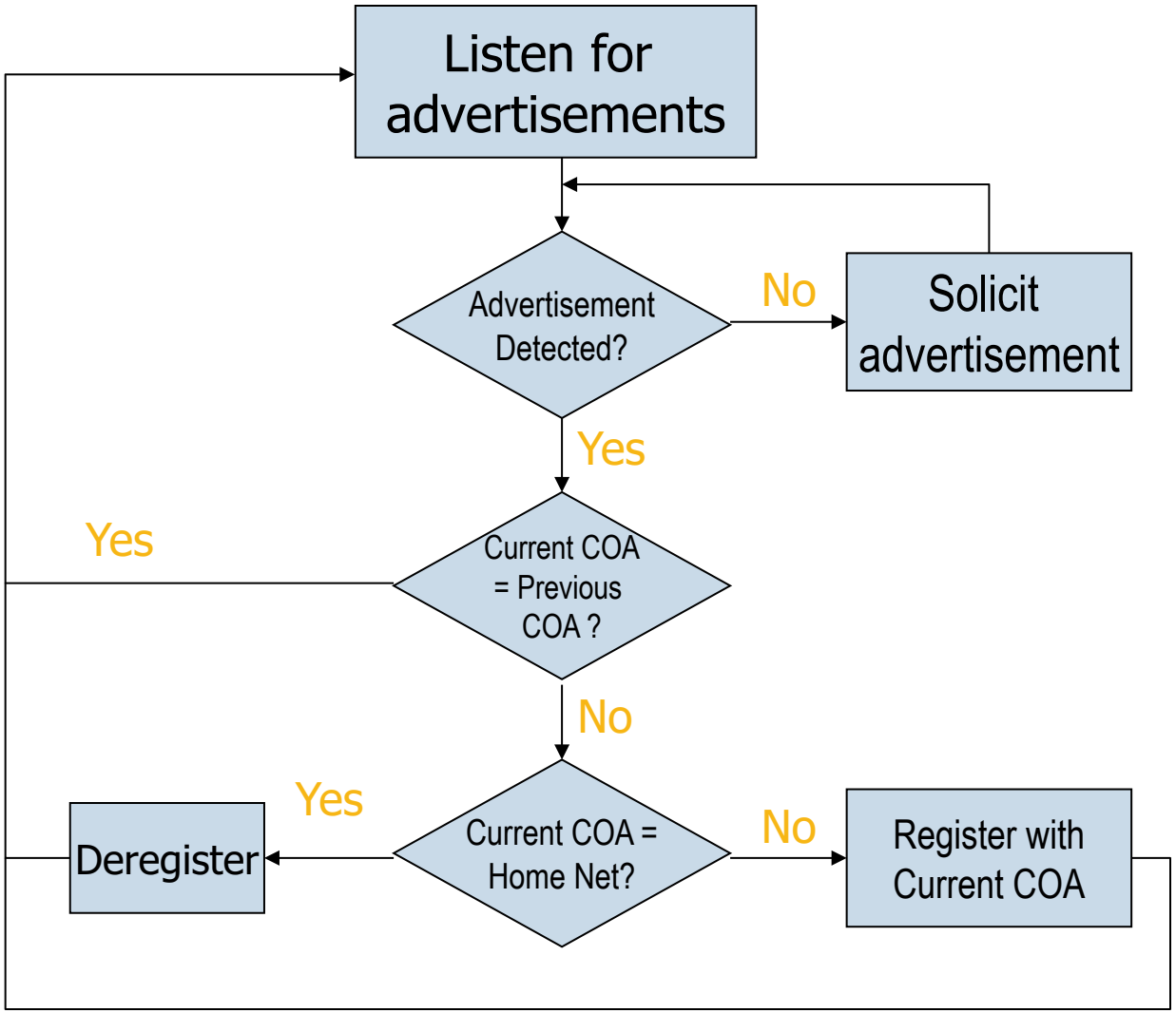
# Agent Advertisement and Discovery

- How does a Mobile Node know that it has moved to another network?
  - In CDPD, the control messages broadcast on the forward channel provide this information
- How does a Mobile Node determine the address of a Home Agent or a Foreign Agent?
- Foreign agents and home agents periodically "advertise" their presence using agent advertisement messages
- This is similar to router advertisement using ICMP

# Agent Advertisement II

- A "mobility extension" to ICMP contains the relevant information
  - Is it a Home Agent or a Foreign Agent?
  - COA associated with the FA
  - Busy or not
  - Whether minimal encapsulation is permitted
  - Whether reverse tunneling is permitted (later)
  - Whether registration is mandatory
- The Agent Advertisement packet must be a broadcast message on the link
- The same agent may act as both a HA and a FA
- If the MN gets an advertisement from its HA, it must deregister its COA's and enable a gratuitous ARP
- If a MN does not "hear" any advertisement, it must solicit an agent advertisement using ICMP

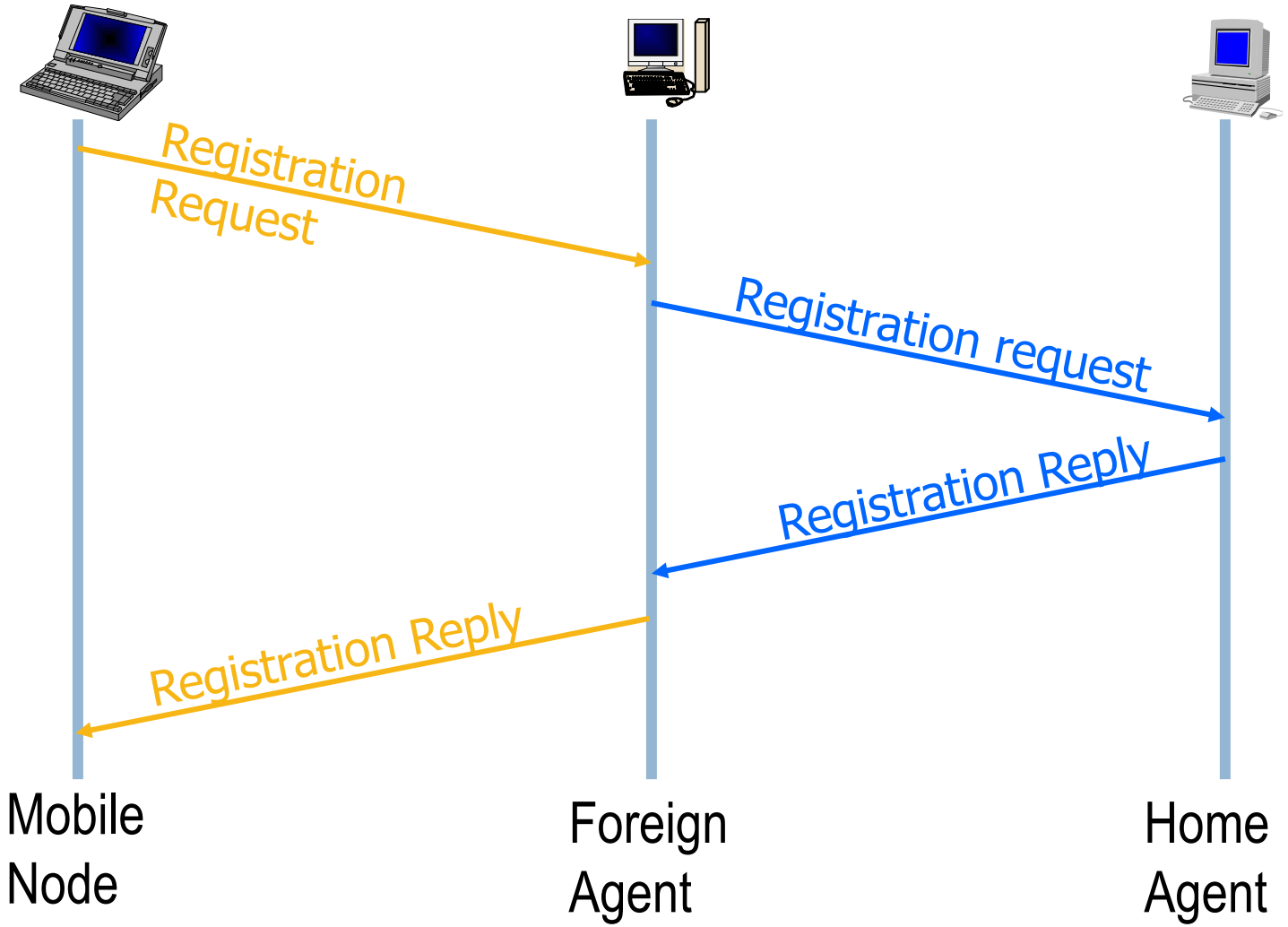
# Connection Search Flow Chart



# Registration

- Purpose:
  - Inform the HA about the COA
  - FA can obtain approval from the HA to provide service to the MN
  - Authenticated to prevent malicious attacks

# Registration in Mobile IP II



# Registration III

- UDP packets are used for registration (port 454 in the HA)
- A nonce called an identification field is used in the request and another in the reply to prevent replay attacks
- If the COA is the FA
  - MN sends registration request to FA
  - FA forwards it to the HA
  - Else
  - MN directly sends the request to the HA
- HA creates a binding between the MN's home address and the current COA
  - This binding has a fixed lifetime
  - MN should re-register before the expiration of the binding

# Registration IV

- The Home Agent may maintain multiple COA for a mobile node upon request
  - Most implementations do not support this
- Broadcast datagrams are NOT tunneled unless explicitly requested by the MN
- Deregistration involves “registering” the home address with the HA
- Deregistering one of the multiple COAs is done by registering it with zero lifetime
- If multiple COAs are not explicitly requested, each new registration request wipes out the previous binding.

# Registration V

- Registration reply indicates whether the registration is successful or not
- Rejection is possible by either HA or FA
  - Insufficient resources
  - Header compression not supported
  - HA unreachable
  - Too many simultaneous bindings
  - Failed authentication
- Directed broadcast
  - If a MN cannot reach its HA, it will send a broadcast registration request to its home network
  - This is rejected by every (other) valid HA on its home network
  - The MN uses one of the HA addresses in the reject message to make a valid registration request (with proper authentication credentials)

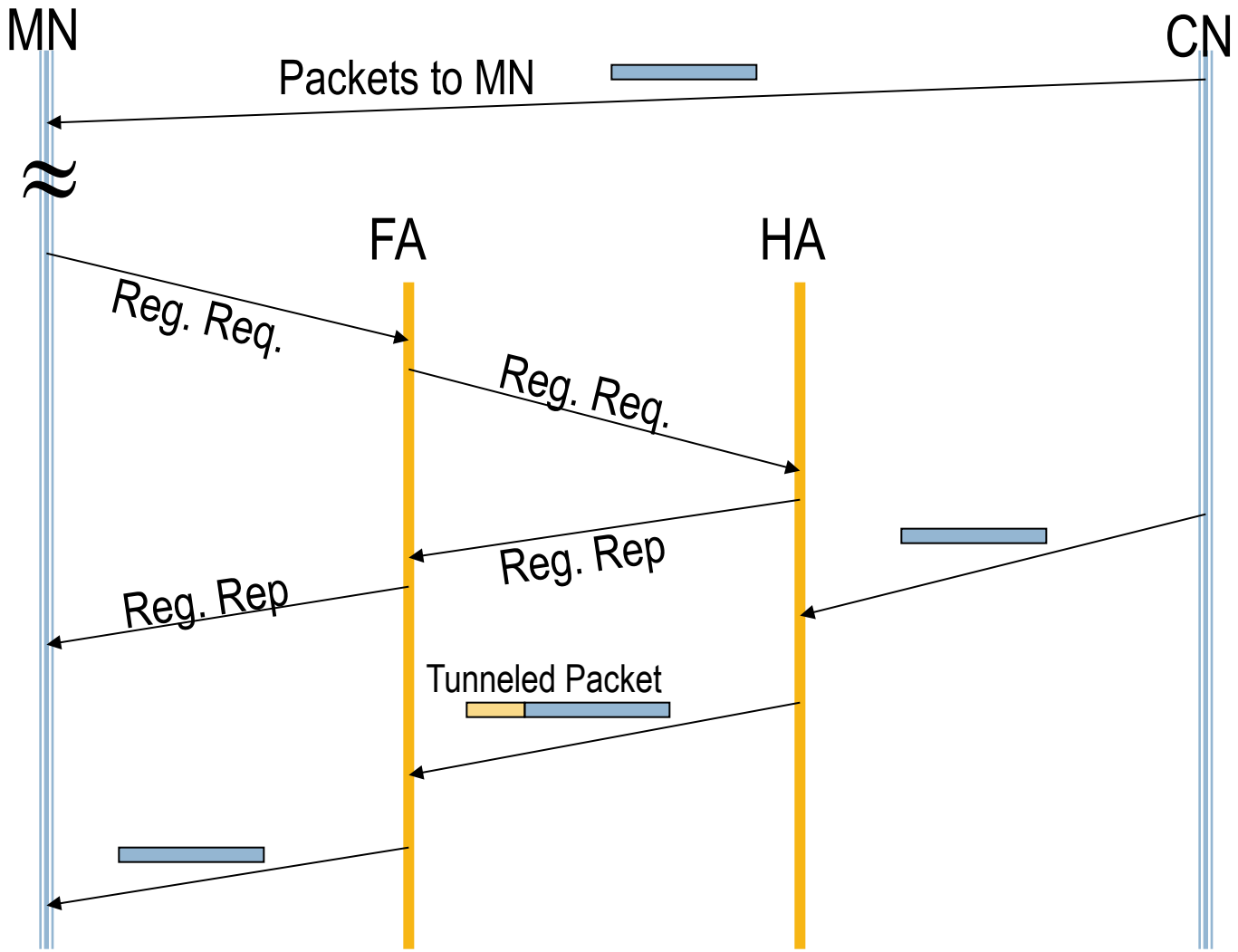
# Mobility Binding List at the HA (CF: Location Directory)

- Upon a valid registration, the HA should create an entry for a mobile node that has:
  - Mobile node's care of address
  - Identification field
  - Remaining lifetime of registration

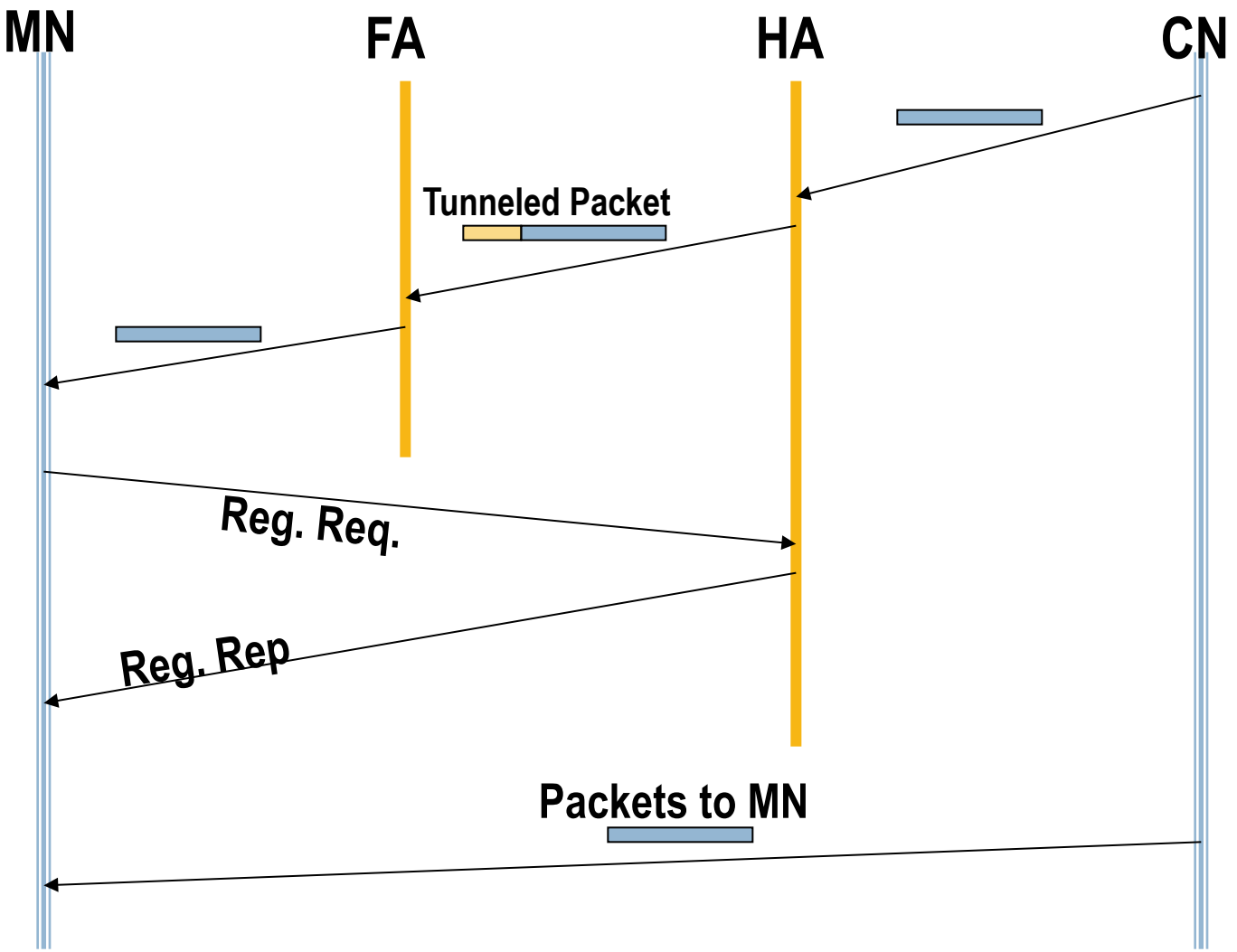
# Visitor List at FA: CF Registration Directory

- Each Foreign Agent maintains a visitor list containing the following information:
  - Link layer address of the mobile node
  - Mobile node's home IP address
  - UDP registration request source port
  - HA IP address
  - Identification field
  - Registration lifetime
  - Remaining lifetime of pending or current registration

# MN moves from Home Network to Foreign Network



# MN moves from Foreign Network to Home Network



# Route Optimization

- Triangle routing is inefficient
  - German and Japanese in Boston
  - Vulnerability
  - Congestion
  - Bottleneck in the home agent
- In the future, intermediate routers and CNs can be expected to cache COA bindings and tunnel packets
  - Authentication?
  - Changes to the existing Internet entities?

# Smooth Handoffs

- Suppose a MN changes its foreign network
- While a new registration request is in progress, data is being tunneled to the old FA
  - This data has to be resent by the CN!
  - The retransmitted data has to be tunneled again!
- If the old FA can tunnel packets it receives to the new FA, this can reduce delay and congestion
- If the old FA re-tunnels the packet back to the HA, it is called a "special tunnel"
  - Enables HA to detect a "loop" if a new registration request has not been enabled

# Reverse Tunneling

- Sometimes packets will have to be tunneled through the HA
  - Firewalls drop outgoing packets that have an IP address that corresponds to another network
  - TTL considerations
    - Packets addressed to hosts on the home network with small TTL need to sense the internet as one hop

# Mobility Support in IPv6

- Addresses “macro”-mobility (movement from one subnetwork to another). “Micro”-mobility to be handled by link-level mobility management (like WLANs)
- Every IPv6 node implements functions for mobility support (including corresponding hosts => no FA is needed)
- Mobile hosts have one home address and one or more care-of addresses
- There exists what is called “binding” between the home address and the primary care-of address

# Mobility Support in IPv6 (Continued)

- Secure binding updates, binding acknowledgements and binding requests
  - enable packets to reach the MH through the HA
    - Extremely small role for the HA
  - enable the CH find out the current care-of address of the MH
  - enable intermediate routers find out the current care-of address of the MH
- The following advantages are perceived:
  - Congestion at the home agent will be reduced
  - Optimal routing of packets will be enabled

# Optimized Mobile IP?