

Mobile IPv4



PRESENTATION

- IPV4
- TERMINOLOGY
- HOME/FOREIGN NETWORK
- TRIANGULAR ROUTING
- SOME PROBLEMS AND THREATS

IPv4 challenges



- IP address identifies the node's point of attachment
- Must be located on the network indicated by the IP address
- 2 mechanisms
 - **Change IP address when changing point of attachment**
 - **Host specific routes**

Mobile IPv4



- Scalable mechanism
- Change point of attachment without changing IP address
- Seamless roaming

SIP

Session

Application Dependent

Transport

Mobile IP

Network

Application & Technology Independent

GSM Mobility

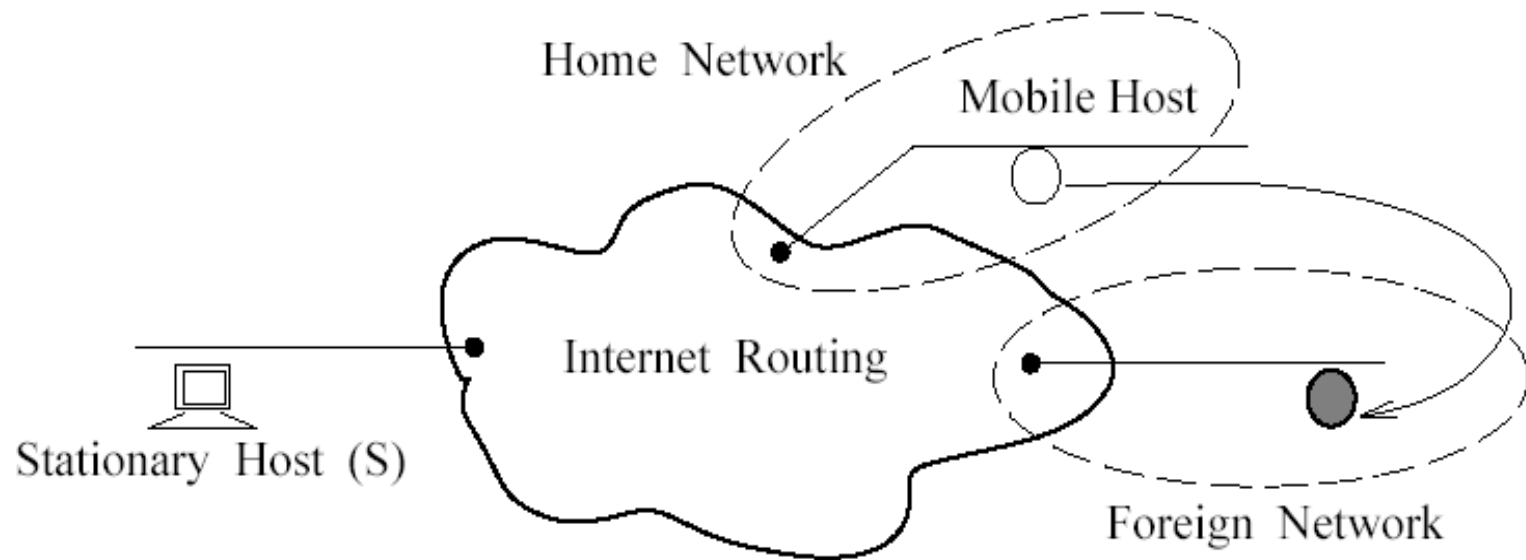
Link

Technology Dependent

Terminology



- Home Network
- Home Address
- Foreign Network
- Care of Address (CoA)
- Home Agent
- Foreign Agent
- Binding

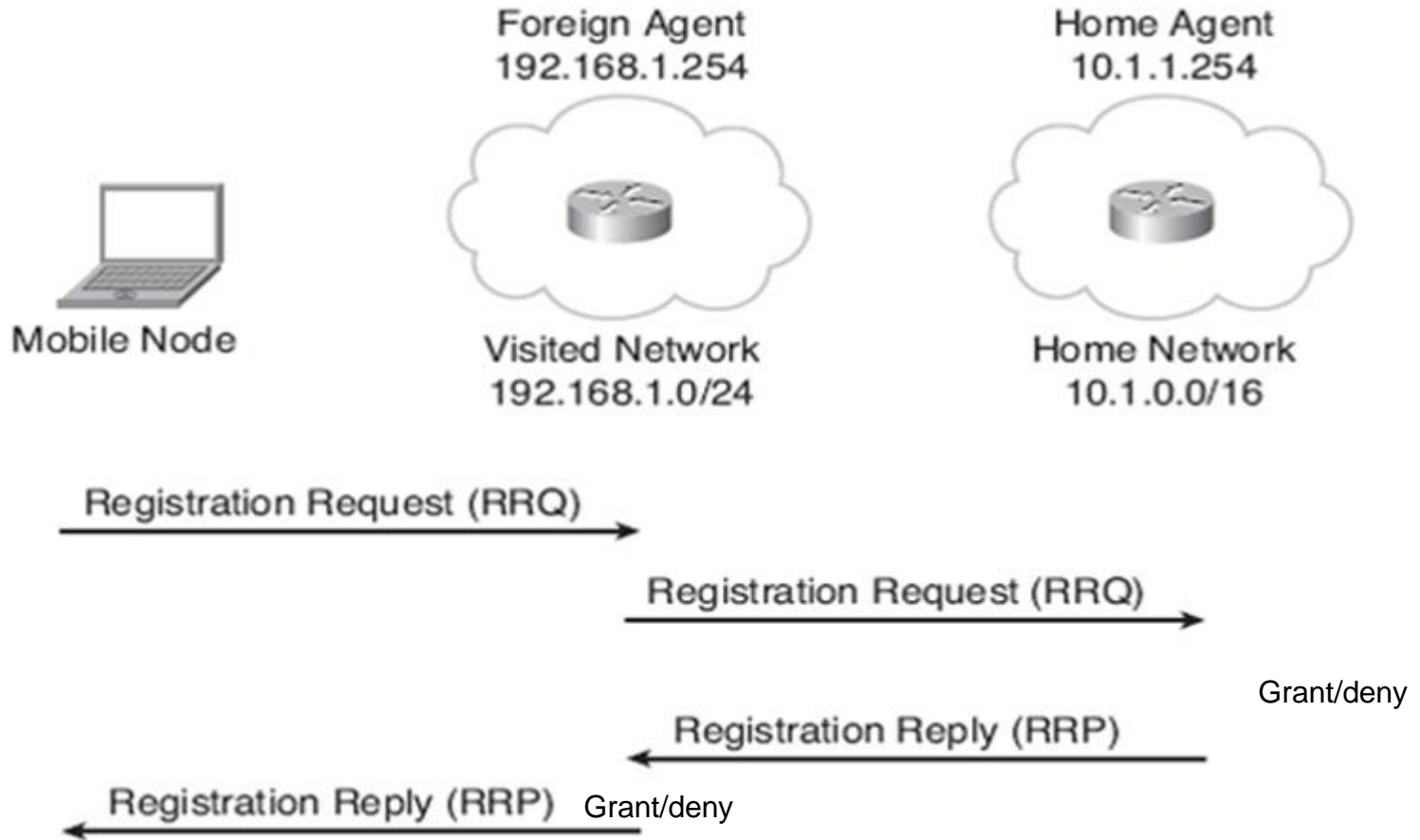


M IPv4 – Home Network



- Home Agent → Agent Advertisements → Mobile Node
- Agent Advertisements contains information
- Mobile Node operates without mobility services on its Home Network
- When returning to its home network from being registered elsewhere, the mobile node deregisters with its home agent, through exchange of a Registration Request and Registration Reply messages

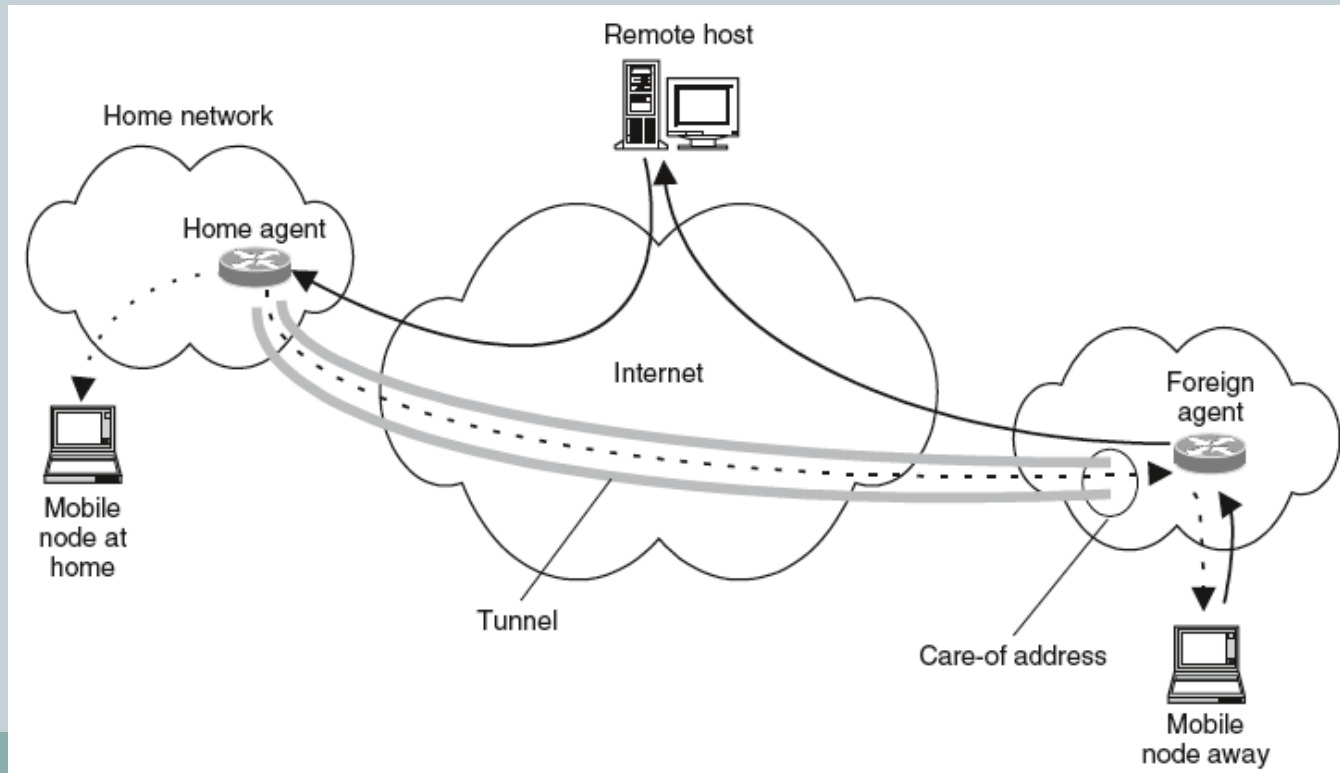
Registration Request Process



M IPv4 – Foreign Network



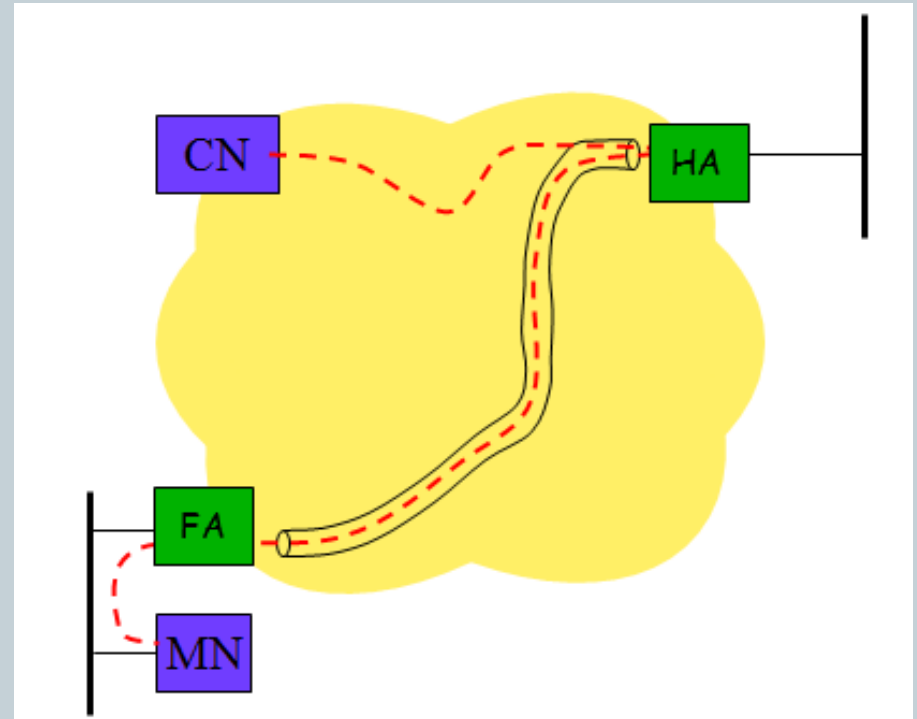
- Care of Address identifies its current location
- Packets sent to permanent address then redirected towards remote address through IP tunnel



Tunneling



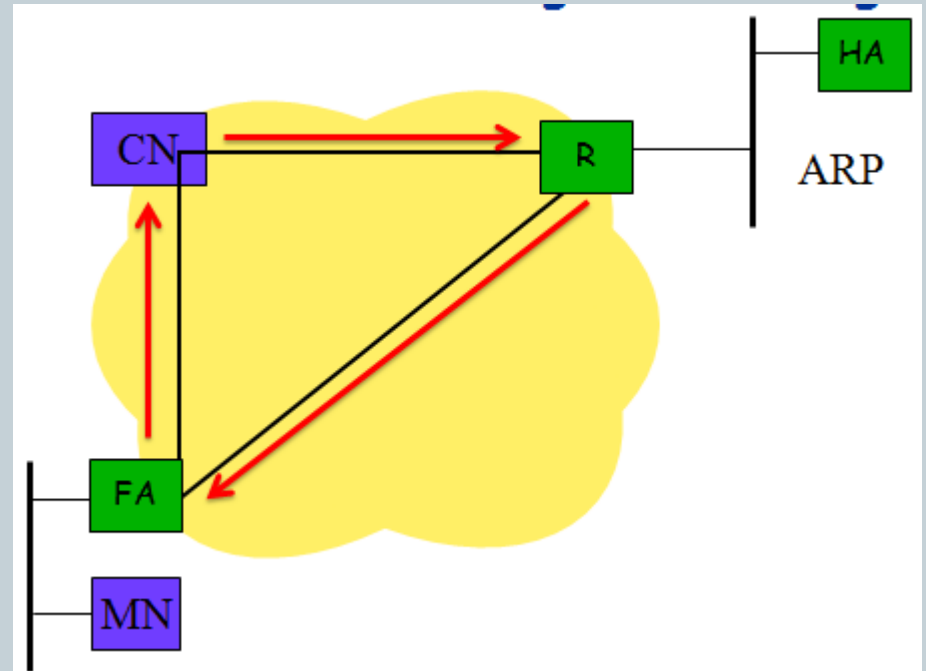
- Used when away from Home Network
- Packet → Home Network (using Home Address) → Home Agent tunnels packet to CoA
- Encapsulation
- Decapsulation



Triangular Routing



- MN : new IP address related to visited network.
- MN → Binding Update (BU) → Correspondent Nodes (CNs)
- If CN received BU - stored in Binding Cache (BC)
- If BC is available, CN can send a packet directly to MN instead of using HA



Problems with Mobile IP

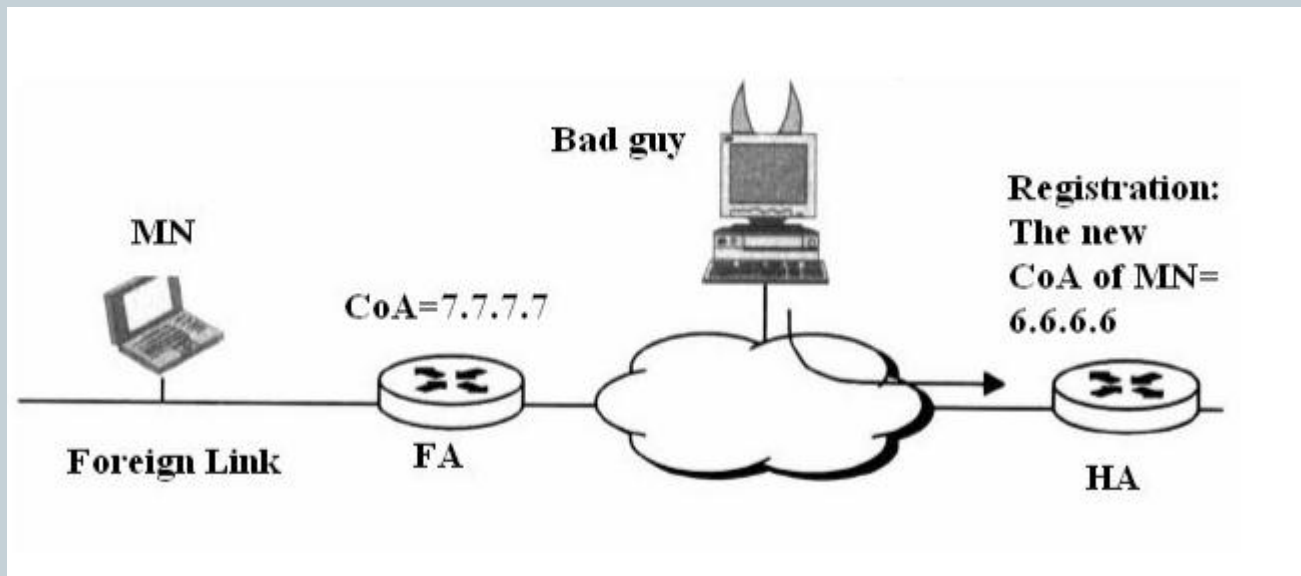


- Sub-optimal routing (triangular routing)
- Security – firewalls cause complexity
- Slow handover
- Latency
- Liability

Some security threats



- Denial of Service (DoS) attack
 - Fake registration request sent to HA
 - Attacker receive all the packets
 - Connection fail





- **Replay attack:**
 - Attacker saves the old valid registration message of the Mobile Node and resend it to Home agent.
 - Home Agent forwards packets to the old care of address (CoA)