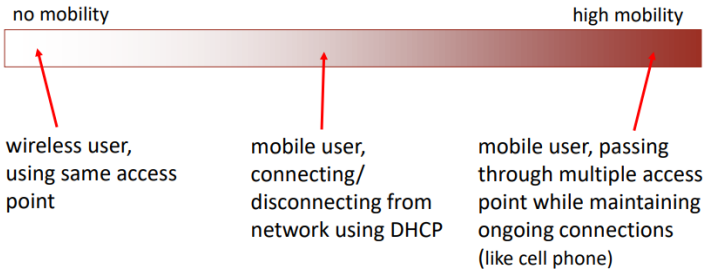
Index

IP Mobility

What is mobility?

- mobile ≠ wireless
- spectrum of mobility, from the network perspective:



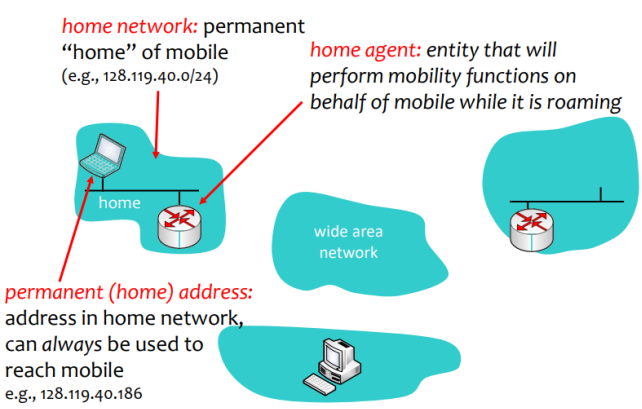
Mobile IP - Motivation

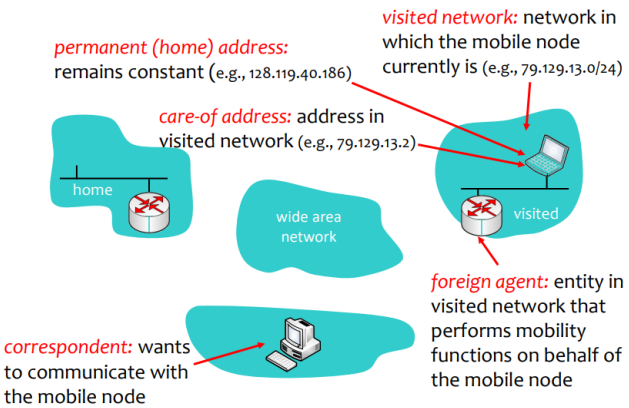
- Traditional Routing is based on destination IP address, with the address prefix determined by the physical network
- Mobility implies changing addresses, routing tables, and introduces security concerns
- A solution requires:
  - Keeping the same address, to support Hand-Over
  - Support for the same level 2 protocols as regular IP
  - Authentication of registration messages

Mobility: approaches

- **Routing handling:** routers advertise permanent address of mobile-nodes-inresidence via usual routing table exchange. Not scalable to milions of mobiles
- **End-systems handling:** indirect routing (via home agent) or direct routing

Mobility: terminology





Mobile IP - Concepts and Functions

- **Mobile Node (MN):** The moving node, changes access network

- **Home Agent (HA):** Node on the home network that registers MN location and uses tunneling to send the MN's packets to the visited network
    - Keeps information about CoA of MN
    - Forwards to the CoA (through a tunnel) packets destined for the home address
- **Home Address:** MN's permanent address
    - MN's address on its home network
    - Used by other nodes to contact MN and as source address on MN's outgoing connections
- **Foreign Agent (FA):** Node on the visited network that assists in routing packets from the tunnel to the MN
    - Provides the CoA to the MN
    - Terminates the tunnel from the HA
    - Default router for the MN's packets
- **Care-of Address (CoA):** Address used to reach the MN at its current (foreign) location
- **Correspondent Node (CN):** Terminal with which the MN has a connection established.

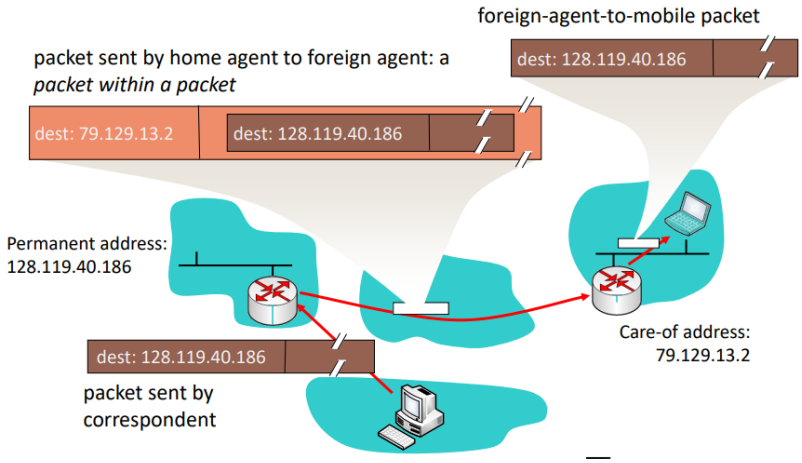
Mobile IP

- **Agent Advertisement**
    - HA and FA send periodic advertisements that enable the MN to know whether it is on its home network
    - Can be solicited explicitly by MN
    - Extension of Router Advertisement message
- **Registration**
    - MN informs HA of its CoA (through the FA)
    - HA acknowledges registration (through the FA)
    - Has a lifetime and must be protected by authentication

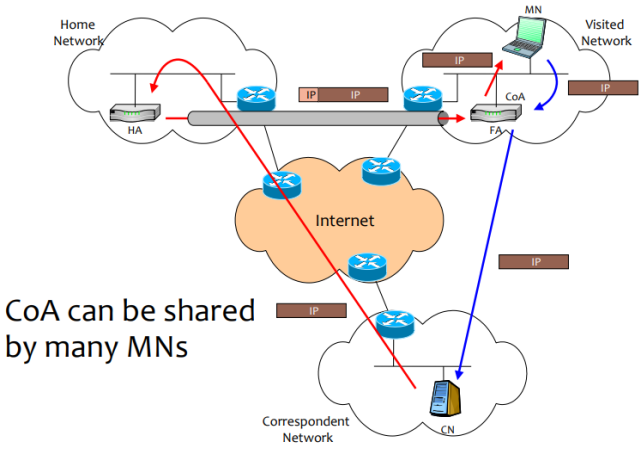
HA registration

- Can be done with or without FA
    - Needs to be through FA if
        - FA supplies CoA (in the advertisement message)
        - FA Advertisement has the R bit set
    - Directly to HA if
        - MN is on home network
        - CoA co-located (CoA obtained through DHCP)
- Re-registration
    - About 3 min. before expiration of lifetime
    - Retransmitted if no answer (> 1 seg.)
- Registration removal
    - Through a registration with lifetime set to zero

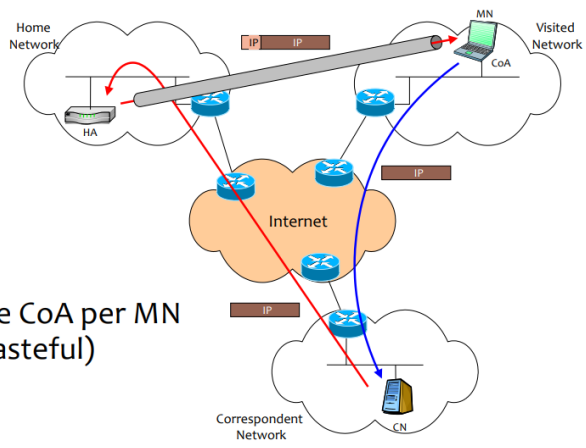
Mobile IP: indirect routing



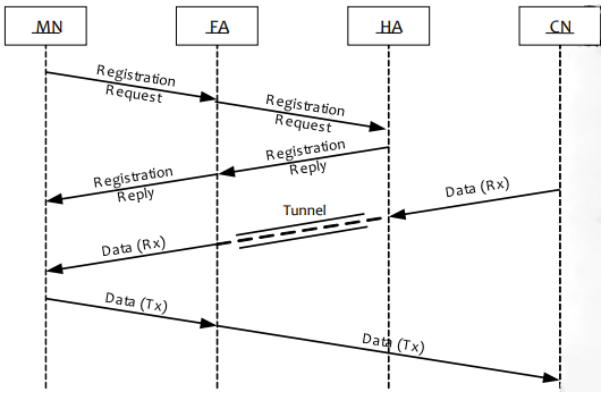
Tunnels (external FA)



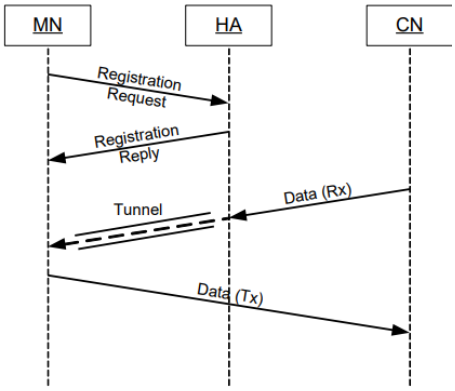
Tunnels (internal FA)



Messages (external FA)



Messages (internal FA)



- Two phases: Registration and Communication
- MN talks with FA
- FA is usually the MN's default router
  - MN may use a different router among those indicated in the Agent Advertisement
- Communication between FA and MN "normal"

- Two phases: Registration and Communication
- FA is internal to MN
  - Co-located CoA tunnel
  - Terminated at MN
  - Communication from MN

Triangular Routing: Problem & Solution

- Triangular routing

    - CN -> MN packets go through HA
    - MN -> CN packets go directly
- Problem: ingress filtering (reverse path filtering)
    - Firewalls only allow topologically correct addresses
    - If source address not related with entry itf ➔ drop packet
- Solution
    - Tunneling also for packets from MN (extension)
    - Bit T on Mobility Agent Advertisement Extension, indicating support for reverse Tunnel
    - Reverse Tunneling: UDP tunneling required if foreign network behind NAT

ARP, Proxy ARP, and Gratuitous ARP

- **Proxy ARP:** sent by HA on behalf of MN to allow nodes on the home network to communicate with the MN when it is abroad
- **Gratuitous ARP:** sent to update caches and used by HA when MN moves to and from foreign network (also by MN when returning home)
- When abroad, MN should not send ARP requests or replies nor send gratuitous ARP for home address
    - It may reply only to ARP requests from the FA

MIPv6

- Adds a new Mobility header to IPv6 for several messages
- New Destination Option header for home address
- New ICMPv6 messages for home agent address discovery
- Security built into the protocol from scratch
- Avoids triangular routing
    - Reverse tunnelling or optimized routing

Mobility Header

- Used to send mobility messages
- Next-header: 135
- Payload Proto: same as IPv6 next header
- MH type: identifies the specific message

Binding update (BU)

- Used to notify HA (or other nodes) of current CoA
- Mobility Header type = 5
- Includes sequence number (used to match BU with Ack) and lifetime fields
- Mobility Option for CoA
    - Not mandatory, can be determined
        - From the Alternate CoA Mobility Option, if present
        - Else from the Source Address of the IPv6 header

Optimization: Binding Update to CN

- **Requires support in CN**
- Binding Cache located at the CN, containing CoAs of MNs
- Packets are sent directly to the MN, bypassing the HA if CoA is known (in Binding Cache)
- Cache updated by Binding Updates with a lifetime

Binding acknowledgement

- MH type = 6
- Includes status field whether the BU is accepted (<128) or rejected (≥128), Lifetime and Sequence number (copied from BU)
- Options:
    - Type-Length-Value (TLV) encoded, similar to BU options
    - Options: Authorization data and Refresh advice

Movement detection

- New prefix appears on link (Router Advert.)
- Unreachability of old router can be detected using NUD
    - Send Router Solicitation to obtain new prefix faster
- Detection through Router Adv./NUD can be slow
- If possible, get notified of link change from lower layers

Back home

- BU with 0 lifetime
- Problem with source address of packet:
    - If at home use Home Address... But HA "uses" Home address...
        - DAD would fail for mobile node
    - => Do not use DAD for the home address configuration
- Must use neighbour solicitation to know HA's link-layer address
    - MN sends Neighbor Solicitation
        - Source IP: unspecified address (::)
        - Dst IP: Solicited-Node multicast address (of the MN's home address)
        - Target: MN's home address
    - HA sends Neighbor Advertisement to multicast address
        - Source IP: address assigned to the interface where advertisement is sent
        - Dst IP: all-nodes multicast address
        - Target: MN's home address
    - MN knows HA link layer address from the advertisement and can now send the BU

Route optimization

- MN sends BU to CN, and CN keeps a binding cache
- CN can use CoA of MN as destination address, and MN can use the CoA as source address without suspicion of forgery
- How to ensure authenticity of BU?
    - Security Association established on the fly using the Return Routability procedure

CN → MN

- CN sends packets to the CoA
- Adds a Routing header with Home Address
    - Type 2 routing header (not deprecated)
        - Carries a single address, therefore is safe
- MN replaces CoA in dst address with Home Address

MN → CN

- Problem with source address (HA is topologically incorrect)
- MN sends packets with
    - CoA as Src address
    - Home Address option containing the HA
        - Carried in an IPv6 Destination Option extension header and processed at the CN
- MN adds the destination Home Address option to every packet that has the Home Address as source address

Some notes

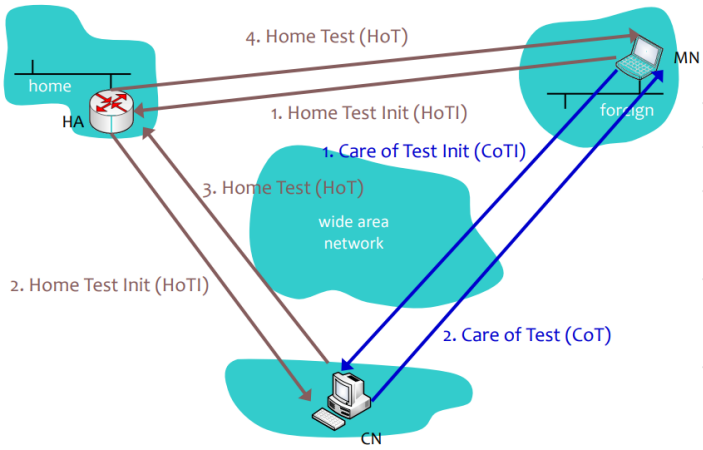
- Should use CoA directly for short lived connections
- Dynamic Home Agent Address Discovery (DHAAD): Home Agent option added to Router Advertisement
- Discovering Home Address dynamically

Security

- **BU to HA**
    - Uses IPsec security association (SA) between HA and MN
    - MUST support and SHOULD use Encapsulating Security Payload (ESP) in transport mode
    - SAs have policies for receiving only for specific home address
        - Prevent a MN from sending BU on behalf of another MN
- **BU to CN**
    - Cannot have a preconfigured SA with every possible CN!
    - Use the return routability procedure
        - MN proves that it is reachable both through the HA and the CoA
    - Key is derived in this procedure

    - BU contains
        - Home address (in Home Address destination option if different from the Source Address)
        - Sequence number (in the Binding Update message header)
        - Home nonce index (in the Nonce Indices option)
        - Care-of nonce index (in the Nonce Indices option)
        - First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BU)))
    - This information can reassure the CN that the BU is legit

Return routability



Security tokens used

- HoTI (Home init cookie)
- CoTI (Care-of init cookie)
- HoT (home init cookie; home keygen token; home nonce index)
- CoT (care-of init cookie; care-of keygen token; care-of nonce index)
- Use of nonces to protect against Binding Update replay attacks

Security generation

- home keygen token :=
  - First (64, HMAC_SHA1 (Kcn, (home address | home nonce | 0)))
- care-of keygen token :=
  - First (64, HMAC_SHA1 (Kcn, (care-of address | care-of nonce | 1)))
- Kcn: key on CN (not shared)
- Key on MN derived from material
  - Kbm = SHA-1 (home keygen token | care-of keygen token)
  - For revocation is only SHA-1 (home keygen token)