8. Mobile Network Layer
Motivation for Mobile IP

Routing
- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?
- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?
- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take to long time
- TCP connections break, security problems
Requirements to Mobile IP

Transparency
- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility
- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security
- authentication of all registration messages

Efficiency and scalability
- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole Internet
The Goal of a Mobile IP

Supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols
Terminology

Mobile Node (MN)
- system (node) that can change the point of connection to the network without changing its IP address

Home Agent (HA)
- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

Foreign Agent (FA)
- system in the current foreign network of the MN, typically a router
- forwards the tunneled datagrams to the MN, typically also the default router for the MN

Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

Correspondent Node (CN)
- communication partner
Example network

HA

router

home network

(home physical network for the MN)

Internet

mobile end-system

fa

foreign network

(current physical network for the MN)

cn

end-system

router
Data transfer to the mobile system

1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN
Data transfer from the mobile system

1. Sender sends to the IP address of the receiver as usual, FA works as default router.
Overview
Network integration

Agent Advertisement
- HA and FA periodically send advertisement messages into their physical Subnets
- MN listens to these messages and detects, if it is in the home or a foreign network
- MN reads a COA from the FA advertisement messages

Registration (always limited lifetime!)
- MN signals COA to the HA via the FA, HA acknowledges via FA to MN
- these actions have to be secured by authentication

Advertisement
- HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
- routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
- packets to the MN are sent to the HA,
- independent of changes in COA/FA
Agent advertisement

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>23</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>code</td>
<td>checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#addresses</td>
<td>addr. size</td>
<td>lifetime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>router address 1</td>
<td>preference level 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>router address 2</td>
<td>preference level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...  

| type = 16 | length | sequence number |
| registration lifetime | R | B | H | F | M | G | r | T | reserved |
| COA 1 | COA 2 |

...  

type = 16  
length = 6 + 4 * #COAs  
R: registration required  
B: busy, no more registrations  
H: home agent  
F: foreign agent  
M: minimal encapsulation  
G: GRE encapsulation  
r: =0, ignored (former Van Jacobson compression)  
T: FA supports reverse tunneling  
reserved: =0, ignored
Registration

Diagram:
- MN (Mobile Node) sends a registration request to FA (Foreign Agent).
- FA sends a registration reply to MN.
- MN sends a registration request to HA (Home Agent).
- HA sends a registration reply to MN.
- MN sends a registration request to FA.
- FA sends a registration reply to MN.
# Mobile IP registration request

| Bit 31 | Bit 30 | Bit 29 | Bit 28 | Bit 27 | Bit 26 | Bit 25 | Bit 24 | Bit 23 | Bit 22 | Bit 21 | Bit 20 | Bit 19 | Bit 18 | Bit 17 | Bit 16 | Bit 15 | Bit 14 | Bit 13 | Bit 12 | Bit 11 | Bit 10 | Bit 9 | Bit 8 | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
|       | type   | S      | B      | D      | M      | G      | r      | T      | x      | lifetime| home address| home agent| COA | identification| extensions . . . |

- **S**: simultaneous bindings
- **B**: broadcast datagrams
- **D**: decapsulation by MN
- **M**: minimal encapsulation
- **G**: GRE encapsulation
- **r**: =0, ignored
- **T**: reverse tunneling requested
- **x**: =0, ignored
### Mobile IP registration reply

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>8</th>
<th>15</th>
<th>16</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>type = 3</td>
<td>code</td>
<td>lifetime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>home address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>home agent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>extensions . . .</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example codes:**

- registration successful
  - 0 registration accepted
  - 1 registration accepted, but simultaneous mobility bindings unsupported

- registration denied by FA
  - 65 administratively prohibited
  - 66 insufficient resources
  - 67 mobile node failed authentication
  - 68 home agent failed authentication
  - 69 requested Lifetime too long

- registration denied by HA
  - 129 administratively prohibited
  - 131 mobile node failed authentication
  - 133 registration Identification mismatch
  - 135 too many simultaneous mobility bindings
### Encapsulation

<table>
<thead>
<tr>
<th>original IP header</th>
<th>original data</th>
</tr>
</thead>
<tbody>
<tr>
<td>new IP header</td>
<td>new data</td>
</tr>
<tr>
<td>outer header</td>
<td>inner header</td>
</tr>
</tbody>
</table>
Encapsulation I

Encapsulation of one packet into another as payload
- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE
  (Generic Routing Encapsulation)

**IP-in-IP-encapsulation (mandatory, RFC 2003)**
- tunnel between HA and COA

```
<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>IP-in-IP</td>
<td>IP checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>lay. 4 prot.</td>
<td>IP checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**IP address of HA**

**Care-of address COA**

**IP address of CN**

**IP address of MN**

TCP/UDP/ ... payload
Encapsulation II

Minimal encapsulation (optional)

- avoids repetition of identical fields
- e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
- only applicable for unfragmented packets, no space left for fragment identification

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>min. encaps.</td>
<td>IP checksum</td>
<td></td>
</tr>
</tbody>
</table>

- IP address of HA
- care-of address COA

<table>
<thead>
<tr>
<th>lay. 4 protoc. S</th>
<th>reserved</th>
<th>IP checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of MN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>original sender IP address (if S=1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP/UDP/... payload
Generic Routing Encapsulation

RFC 1701

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>GRE</td>
<td>IP checksum</td>
<td></td>
</tr>
</tbody>
</table>

IP address of HA

Care-of address COA

CRC32 rec. rsv. ver. protocol

checksum (optional) offset (optional)

key (optional)

sequence number (optional)

routing (optional)

RFC 2784

<table>
<thead>
<tr>
<th>C</th>
<th>reserved0</th>
<th>ver.</th>
<th>protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>checksum (optional) reserved1 (=0)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ver.</th>
<th>IHL</th>
<th>DS (TOS)</th>
<th>length</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP identification</td>
<td>flags</td>
<td>fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td>lay. 4 prot.</td>
<td>IP checksum</td>
<td></td>
</tr>
</tbody>
</table>

IP address of CN

IP address of MN

TCP/UDP/... payload
Optimization of packet forwarding

Triangular Routing
- sender sends all packets via HA to MN
- higher latency and network load

“Solutions”
- sender learns the current location of MN
- direct tunneling to this location
- HA informs a sender about the location of MN
- 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 now forwards remaining packets to new FA
- this information also enables the old FA to release resources for the MN
Change of foreign agent
Reverse tunneling (RFC 3024, was: 2344)

1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)
Mobile IP with reverse tunneling

Router accept often only “topological correct“ addresses (firewall!)
  - a packet from the MN encapsulated by the FA is now topological correct
  - furthermore multicast and TTL problems solved (TTL in the home network
    correct, but MN is too far away from the receiver)

Reverse tunneling does not solve
  - problems with *firewalls*, the reverse tunnel can be abused to circumvent security
    mechanisms (tunnel hijacking)
  - optimization of data paths, i.e. packets will be forwarded through the tunnel via
    the HA to a sender (double triangular routing)

The standard is backwards compatible
  - the extensions can be implemented easily and cooperate with current
    implementations without these extensions
  - Agent Advertisements can carry requests for reverse tunneling
Mobile IP and IPv6

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols
- security is integrated and not an add-on, authentication of registration is 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 which can be used instead of the special agent advertisement; addresses are always co-located
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
- **soft hand-over**, i.e. without packet loss, between two subnets is supported
  - MN sends the new COA to its old router
  - the old router encapsulates all incoming packets for the MN and forwards them to the new COA
  - authentication is always granted
Problems with mobile IP

Security
- authentication with FA problematic, for the FA typically belongs to another organization
- no protocol for key management and key distribution has been standardized in the Internet
- patent and export restrictions

Firewalls
- typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)

QoS
- many new reservations in case of RSVP
- tunneling makes it hard to give a flow of packets a special treatment needed for the QoS

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