Why mobility?

• Need to change physical media without breaking (TCP) connections
• People want Wireless Network Access
  – Ease and economy of operation
• Continuous connectivity
• Home network addressable from the entire Internet

What is mobility?

• A node moving from a location to another location while preserving its original IP address
  – Possibly also changing the layer 2 environment
  – Different layer 2 networks are (usually) separated by routers (or gateways)
• On the border of different layer 2 networks
  the change of IP address has to be notified
  – For instance when moving from WLAN to GPRS
  – This would be YAP (Yet Another Protocol)
  • and most probably it would also break up TCP connection state

What moves? Services or users

• Service mobility
  – User moves and connects to his home network with arbitrary devices
    • VPNs, secure connections, WWW-mail services
• User mobility
  – User and the device moves and connects to his home network
  • Use of all home network services
  • Appearing to be in the home network
Host routes – the easy solution?!

- Why not spread knowledge on the movements to all Internet routers?
  - Assign a new address to the mobile node as it moves
  - This solution does not scale, overload of networks with location information
- We need to restrict the circulation of location and IP address information to a minimum

Network scalability

- Scalability in networks
  - If the number of information elements grows faster or at equal speed in the core of the network the solution does not scale.
  - No sense in distributing information on a single user to all nodes in the network
- All technical solutions in the Internet should be scalable!

Mobility design guidelines

- No modifications to host operating system
- Internet-wide mobility calls for a scalable solution
- Application transparency
- No modifications to Internet routing
- Compatibility with Internet Addressing

Mobile IP design objectives

- Limit the size and frequency of route updates
  - preserve host address regardless of location
- Simple implementation
- Simple and straightforward use of address space without resorting to assumptions on address availability
Mobile IP design plan
- Must detect movement
- Must discover/configure care-of-address
- Must inform the home agent
- Home agent Must forward packets to mobile node

Mobile IP standards
- Mobile IP is an IETF working group
- Mobile IP is defined in IETF standards
  - See also, RFC 1701 (GRE) and RFC 1321.
- Standards define
  - Agent discovery
  - Registration procedure
  - Tunneling

Mobile IP components
- Mobile and correspondent nodes
- Foreign Agents (IPv4 only)
- Home Agents
- Tunnels
- Care-of- addresses

Mobile IP basic features
- With tunneling one is able
  - to forward packets from HomeAgent to MobileNode
  - And back, if necessary
- Only the Home Agent knows where you are
  - This solution scales better
- Security is required but not restricted
  - The four building blocks
    - Confidentiality, Authentication, Integrity, Non-repudiation

Mobile IP transforms the mobility problem into a routing problem!
Home agent

- Router for the home network
- Mobility service providing agent
  - access to the home address of the mobile node without mobile node’s presence.
- Advertise routing info on demand
  - to home network, or to other nodes
- Tunnels packets towards mobile node

Foreign agent (IPv4 only)

- Delivers packets to a mobile node
- Mobility service provider in the foreign network
  - Inform the home agent on FA care-of-address
  - Provide CoA and detunneling for the MN
- Act as the default router for the mobile node in the foreign network

Tunneling

- Tunnel is a path followed by packet that is encapsulated within an another packet’s payload
  - Put (IP) packets inside IP packets
    - avoid standard unicast routing
    - use other protocols in the Internet
  - Tunnels are defined manually
  - Tunnels reduce the MTU
  - Tunnel faults are hard to detect
- Tunneling techniques are several
  - IPinIP (RFC 2003, default), MinIP (RFC 2004), GRE (RFC 1701 & 1702) etc.

Care of address

- Foreign Agent CoA and Co-located CoA
- CoA is the mobile nodes point of attachment
  - changes when the network changes
  - stored together with the permanent (home) IP address
  - not used as the IP source or destination by the other nodes (use the home IP address)
- CoA is the exit point from the tunnel
  - either the Foreign Agent (FA CoA) or mobile node (co-located CoA)
Movement detection

- MN detects Home/Foreign Agent-advertisements (modified RFC 1256)
  - or solicits for a H/FA presence (unmodified RFC 1256)
  - H/FA advertisement = extended ICMP
  - Sequence numbers used to detect need for re-registration
- If no advertisements/solicitations answered
  - send ICMP to home router (check TTL!)
  - assume foreign network and try to obtain an address using DHCP or configure IP address manually
  - then register with Home Agent

Registration

- Request help in routing from the FA
- Inform the HA current location of MN
- Re-register
- Notify HA when returned to home network
- Registration done over UDP
  - Registration request
  - Registration reply

Traffic forwarding – Internet

- Home Agent intercepts packets sent to the Mobile Node and sends the packets tunneled to the MN
- ARP requests outside of the home network are answered with HA L2 address
  - proxyARP aka Gratuitous ARP

Traffic forwarding – home network

- Home Agent intercepts packets sent to the Mobile Node and sends the packets tunneled to the MN
- How about home network ARP requests?
  - What about cached ARP-replies?

ARP table

<table>
<thead>
<tr>
<th>MN/IP</th>
<th>MN/L2</th>
<th>Registration request &amp; reply</th>
</tr>
</thead>
<tbody>
<tr>
<td>MN/IP</td>
<td>HA/L2</td>
<td>Sent to all local nodes via gratuitous ARP</td>
</tr>
</tbody>
</table>

Sent to all local nodes via gratuitous ARP
Triangle routing and reverse tunneling

- CN sends to MN
  - Traffic flows via HA
- MN to CN
  - Traffic may take the shortest path
  - If ingress filtering is in effect the traffic may be dropped
  - Solution: Reverse tunneling

Foreign Agent
Home Agent
Tunnel
Mobile Node
Correspondent Node

- CN sends to MN
  - Traffic flows via HA
- MN to CN
  - Traffic may take the shortest path
  - If ingress filtering is in effect the traffic may be dropped

Solution: Reverse tunneling

New route advertisements

- Home agent knows the true location of the MN
  - Send redirects to correspondent nodes (avoid triangle routes)
  - Send new FA info to old FA

Old Foreign Agent
Home Agent
Tunnel
Mobile Node
Correspondent Node
New Foreign Agent

- HA to FA (unicast)
- HA to MN (unicast)
- Original broadcast packet

Receiving home network broadcast in foreign network

- Co-located address
  - Broadcast packets encapsulated and tunneled to the Mobile Node (tunnel exit point)
  - Requires (de)tunneling capability from the MN

- Foreign Agent address
  - Tunneled to the FA (tunnel exit point)
  - If link level broadcast, then packets have to be recursively encapsulated otherwise broadcasted in the foreign network

Original broadcast packet
Redirect from HA
-sends packets straight to MN/FA
Route bind
-for all MN packets send them to new FA

Sending broadcasts

- Directed broadcasts sent as such
  - If allowed by the Home Agent
- Link layer broadcasts tunneled to the HA

HA to FA (unicast)
HA to MN (unicast)
Original broadcast packet

MN to FA (unicast)
Original broadcast packet

**Multicast**

- Multicasts are sent to the
  - Multicast router
    - No encapsulation/tunneling needed
  - HA that should have the multicast routing capability
    - encapsulated and tunneled to the HA

- Multicast is received
  - normally as a group member (co-located address)
  - via HA as encapsulated/tunneled packets
    - may require recursive encapsulation

---

**Home agent at home network edge**

- Client based VPNs
- Direct connection to home (organization) network
- Requires Home Agent management resources from the organization
  - Flexible security solutions

---

**Home agent at ISP network edge**

- ISP based VPNs
- Requires further action to connect to the organization network
  - possibly doubling the registration procedures
- Outsources the HA management
  - Dependence on ISP choices on security etc.
  - Traffic may be unsecure within the ISP network

---

**IPv6 fundamentals**

- New header
- Addressing space increased from 32 bits to 128 bits
  - by some estimates IPv4 addresses are depleted by 2005-2015
  - IPv6 addresses, realistically applied, can cover at least 1564 addresses/m² (oceans included), optimistic calculations give up to 3911873538269506102 addresses/m²
IPv6 – new features

- New anycast – sending mode added to broadcast, multicast and unicast
  - same address for several nodes
  - packet is sent to nearest node having the anycast address
- Multicast sendings controlled with scope – field
- Flow labels to cache forwarding information
- Priority field to support QoS
- Stateless autoconfiguration
  - no more DHCP or BOOTP

IPv6 - repercussions

- Simpler, though longer header
  - Arbitrary amount of option headers that are not examined in all routers
    - routing
    - fragmentation (only at the source)
    - authentication (for data integrity)
    - security (for data confidentiality)
    - hop-by-hop (to be examined at every hop)
    - destination (to be examined by the destination router)
  - there will be difficulties of keeping up with new headers
  - GOLDEN RULE for LARGE SCALE NETWORKS: Extended would be better than extensible

- TCP has to be updated
  - checksum counted with IP address fields

IPv4 vs. IPv6 and mobility

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. MN, HA</td>
<td>1. MN, HA</td>
</tr>
<tr>
<td>2. MN home address</td>
<td>2. Global home address and link-local address</td>
</tr>
<tr>
<td>3. Foreign Agent</td>
<td>3. Plain IPv6 router</td>
</tr>
<tr>
<td>4. FA CoA/CoCoA</td>
<td>4. All colocated CoAs</td>
</tr>
</tbody>
</table>
| 5. Address from
  - Agent discovery
  - DHCP |
| 6. Manually |
| 7. Tunneling |
| 8. Routes optimized by a separate protocol |
| 1. Auto-configuration |
| 2. DHCPv6 |
| 3. Manually |
| 6. Router discovery (ICMPv6) |
| 7. Source routing (option) or tunneling |
| 8. Integrated route optimization |

Mobile IPv6

- MN creates its own CoA with automatic address configuration
  - Stateful: DHCPv6
  - Stateless: Local subnet prefix as in Neighbor Discovery (RFC 2461, IPv6 ARP)+own hardware address
- MN may notify its correspondents when it moves (no more triangular routing)
- Correspondents put CoA in routing headers
- HA encapsulates packets if it gets them
- Binding updates carried in Destination Option
Mobile IP summary

- Method to ensure packet forwarding to the mobile node
  - Home Agent, Mobile node, encapsulation and tunneling
  - possibly also Foreign Agent
- Requires registration (although not covered in these slides)
- Works also in IPv6