



HELSINKI UNIVERSITY OF TECHNOLOGY

Mobility in IP networks Mobile IP

Lecture slides for S-38.191

8.2.2001

Mika Ilvesmäki

Tietoverkkolaboratorio – Networking laboratory



Networking laboratory

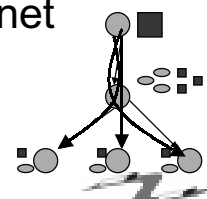


HELSINKI UNIVERSITY OF TECHNOLOGY

Mika Ilvesmäki, M.Sc. (Tech.)

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!





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) ☹



Different users – different mobility

- 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?
 - Solution does not scale, overload of networks with locality information
- We need to restrict the circulation of location and IP address information to a minimum



Mobile IP design objectives

- Limit the size and frequency of route updates
- Simple implementation
- Simple and straightforward use of address space without resorting to assumptions on address availability





Mobile IP standards

- Mobile IP is an IETF working group
- Mobile IP is defined in IETF standards
 - RFC 2002, 2003, 2004, 2006
 - See also, RFC 1701 (GRE) and RFC 1321.
- Standards define
 - Agent discovery
 - Registration procedure
 - Tunneling



Mobile IP basic features

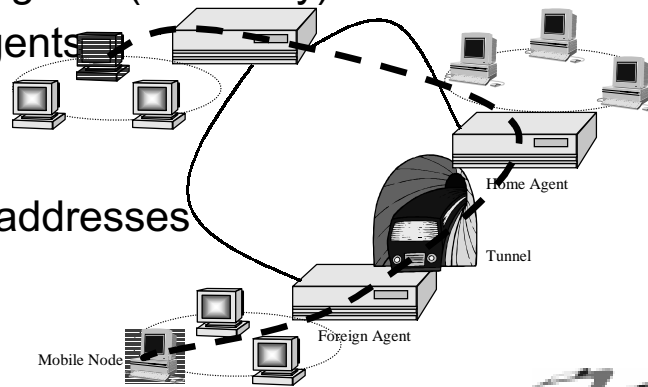
- With tunneling one is able
 - to forward packets from HA to MN
 - And back, if necessary
 - to appear to be in one's home network
- Only the Home Agent knows where you are
 - This solution scales better
- Security is required but not restricted
 - The four building blocks
 - Confidentiality, Authentication, Integrity, Non-repudiation





Mobile IP components

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



Home agent

- 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

- 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, MinIP, GRE etc.





Care of address

- Foreign Agent CoA
- 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 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
 - or solicits for a H/FA presence
 - 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 HA current location of MN
- Re-registerate
- Notify HA when returned to home network
- Registration done over UDP
 - Registration request
 - Registration reply



Traffic forwarding – Internet

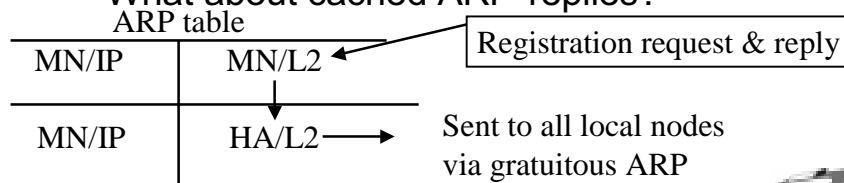
- Home Agent intercepts packets sent to the Mobile Node and sends the packets tunneled to the MN
- ARP requests outside of the home network are answered with HA L2 address
 - proxyARP





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?

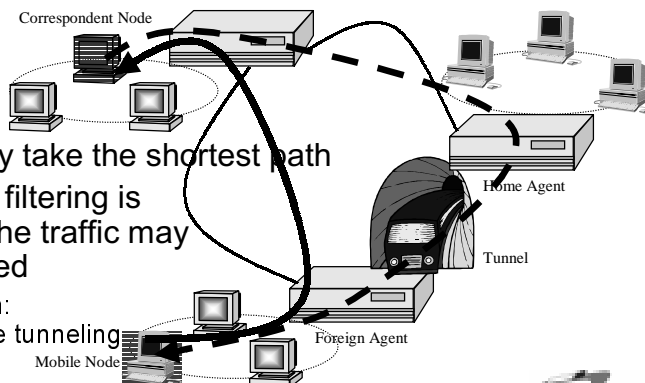


Triangle routing and reverse tunneling

- 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

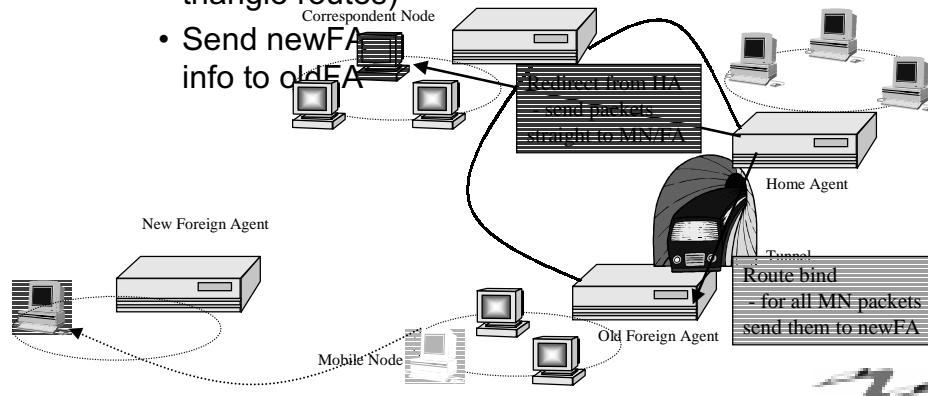




New route advertisements

– Home agent knows the true location of the MN

- Send redirects to correspondent nodes (avoid triangle routes)
- Send newFA info to oldFA



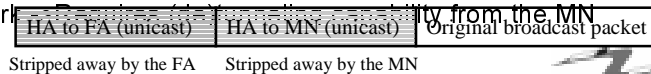
Receiving home network

broadcast in foreign network

- Co-located address
 - Broadcast packets encapsulated and tunneled to the Mobile Node (tunnel exit point)



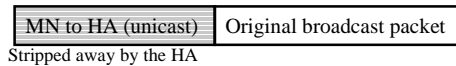
- Foreign Agent address
 - Tunneled to the FA (tunnel exit point)
 - If link level broadcast then packets have to be recursively encapsulated otherwise broadcasted in the foreign network





Sending broadcasts

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



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

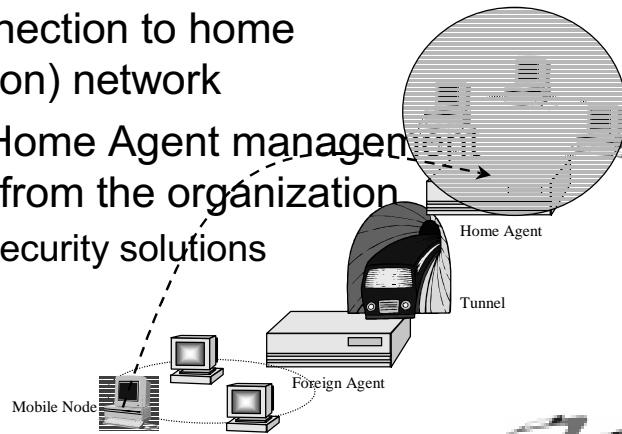


- Multicast is received
 - normally as a group member (co-located address)
 - via HA as encapsulated/tunneled packets
 - may require recursive encapsulation



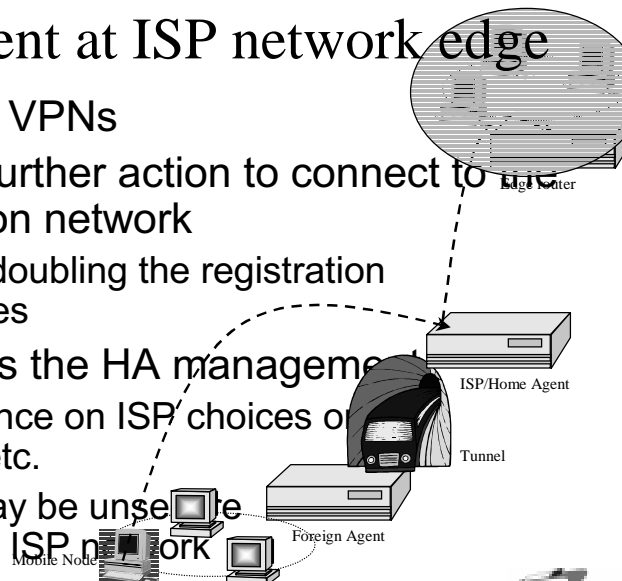
Home agent at home network edge

- 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

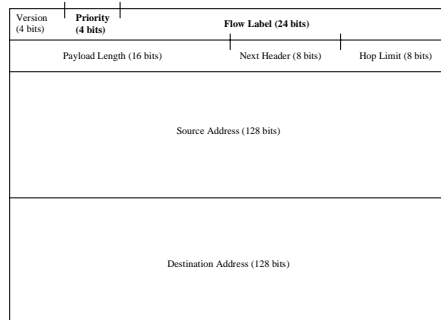
- ISP based VPNs
- Requires further action to connect to organization network
 - possibly doubling the registration procedures
- Outsources the HA management
 - Dependence on ISP choices of security etc.
 - Traffic may be unsecured within the ISP network





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



IPv6 vs. IPv4 and mobility

- | | |
|---|--|
| <p>IPv4</p> <ol style="list-style-type: none">1. MN, HA2. MN home address3. Foreign Agent4. FA CoA/CoCoA5. Address from<ol style="list-style-type: none">1. Agent discovery2. DHCP3. Manually6. Agent discovery7. Tunneling8. Routes optimized by a separate protocol | <p>IPv6</p> <ol style="list-style-type: none">1. MN, HA2. Global home address and link-local address3. Plain IPv6 router4. All colocated CoAs5. Address from<ol style="list-style-type: none">1. Auto-configuration2. DHCPv63. Manually6. Router discovery (ICMPv6)7. Source routing (option) or tunneling8. Integrated route optimization |
|---|--|



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)
- Useful also in IPv6

