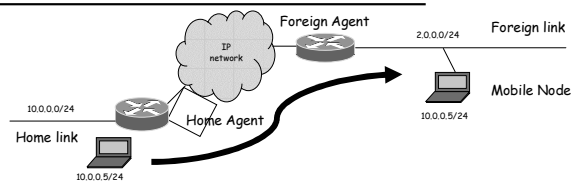
Mobile IP

Jorge García Vidal

Intro

- Mobile IP es una solución para el soporte de movilidad en L3.
- Esto significa que los routers (Agents) tienen un papel activo en el soporte de la movilidad.
- En principio fue pensado para soportar movilidad nomádica.
- Si se consigue optimizar el tiempo de handover, se puede usar para movilidad seamless, con la ventaja de que es independiente de la tecnología de red (802.11, UMTS, etc)

Intro: MIPv4



Mobile Node: A node which can change its point-of-attachment to the network from one link (home link) to another (foreign link), using only its permanent IP home address.
Home Agent: A router with an interface on the MN's home link which:
- the MN keeps informed of its current location (care-of-address)
- Advertises reachibility to the network prefix of MN's home address
- Intercepts packets detined to the MN's home address and tunnels them to the MN's current location, given by its care-of-address.

Foreign Agent: A router on the MN's Foreign link which.
- Assists the MN in informing its HA of its current c-o-a
- Provides a c-o-a and can detunnel packets
- Serves as a default router for packets generated by the MN

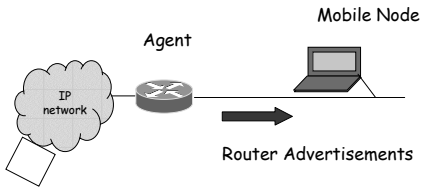
Intro: MIPv4

- Foreign agent care-of address
  - IP address of a foreign agent which has an interface on the foreign link being visited by a mobile node
  - Can be shared by many mobile nodes simultaneously. In MIPv6 does not have much sense as there is no problem with the number of addresses and it is not used anymore.
- Collocated care-of address
  - IP address temporaly assigned to an interface of the mobile node itself
  - Might be used when no foreign agents are available on a foreign link
  - Can be used by only one mobile node at a time. It's the only method used in MIPv6.

General problem of mobility

- Discovery
  - Which is my @H
  - Am I in my Home link?
  - If in a foreign link, which is my @F?
- Registration
  - How the HA can reach me?
- Tunneling
  - How data goes from CN to MN?
  - How data goes from MN to CN?
- Handovers times
- TCP interaction

Review of ICMPv4 Router Discovery…

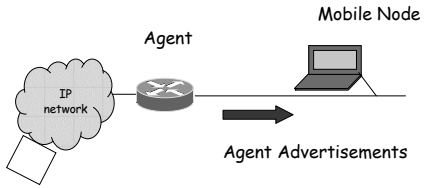


Router Discovery: In ICMPv4, a Router Discovery process, using two ICMP messages (`Router Advertisement` and `Router Solicitation`) has Been defined. In these messages the router specifies:

- Router address (in fact can be many)
- Address entry size: 2 (2x32 per router address)
- Lifetime: seconds the advertised address can be considered valid

Default value: 30 minutes. There is also an ICMP Router Solicitation message…

MIPv4: Discovery



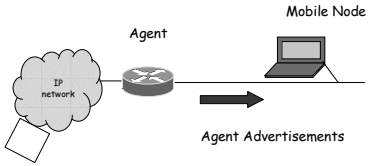
Agent Discovery: Home & foreign agents periodically broadcast ICMP `Agent Advertisements` packets which are received by all nodes on the link (`agent advertisements` are sent as extensions of ICMPv4 `Router Advertisement` messages)

MIPv4: Discovery

- The Agent Advertisement extension consists of the following fields:
  - Type: 16 (i.e. this is an agent advt)
  - Length: 6+4xN (N: # of c-o-@ advertised)
  - Seq. Number: # of messages sent since agent initialization
  - Lifetime: longest lifetime this agent is willing to accept a registration request from a MN
  - R: Registration with this FA is required. Nodes already registered must reregister
  - B: Busy: FA will not accept new registrations
  - H: This agent is a HA; F: This agent is a Foreign Agent
  - M: Use Minimal encapsulation; G: Use GRE
  - Y: The agent support Van Jacobson header compression
  - C-o-@: List of c-o-@ supported by this FA
- Additionaly the prefix length can be included

La información en el recuadro se da como información adicional al tema

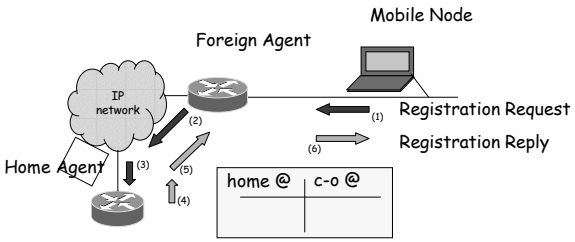
MIPv4: Discovery



Agent Discovery: Mobile nodes examine Agent Advertisements and determine whether they are connected to their home or foreign link. MN connected to a foreign link can obtain care-of-address from the Agent Advertisement. If the MN wants to speed-up the process, it Can send `Agent Solicitation` messages…
A collocated c-o-@ can be obtained either Using DHCP in the foreign link, or can be preassigned, etc.

NOW, LET US ASUME WE ARE IN A FOREIGN LINK…

MIPv4: Registration

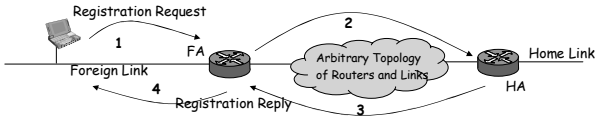


Registration: As the MN is in a foreign link, it must register its care-of-address with its home agent, using UDP Registration Request/Reply messages

The HA maintains a binding table that maps MN's home @ with MN's c-o @

MIPv4: Registration

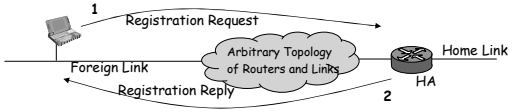
An MN registers on a foreign link using a FA´s c-o @.



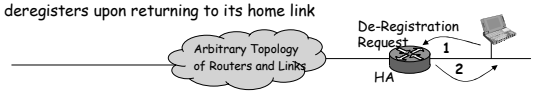
(1) The MN requests the forwarding service by sending a registration request to the FA
(2) The FA relays this request to the HA of that MN
(3) The HA either accept or denies the request and sends a registration reply to the FA
(4) The FA relays this reply to the MN

MIPv4: Registration

A MN registers on a foreign link using a collocated c-o @ (perhaps because no FA is present on the foreign link)



A MN deregisters upon returning to its home link



MIPv4: Registration

- The `registration request` message is carried in UDP messages and consists of the following fields:
  - Type: 1 (i.e. registration request)
  - S: Simultaneous binding (i.e. request for the HA to retain its prior mobility bindings)
  - B: Broadcast: The MN would like to receive a copy of IP broadcast from the Home Link
  - D: MN decapsulates data, i.e. uses a collocated c-o @.
  - M: Use Minimal encapsulation, G: Use GRE
  - V: HA should use Van Jacobson compression.
  - Lifetime: Seconds before the registration expires
  - H@: Home IP@ of the MN; C-o@: Foreign IP@ of the MN.
  - Identifier: 64-bit generated MN for matching registration requests and for security purposes
  - Extensions: So far, only authentication extension

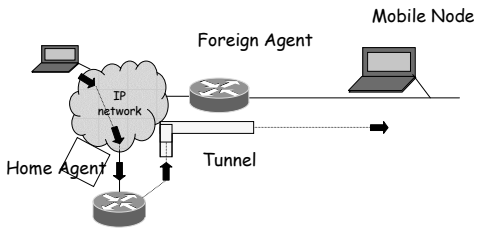
La información en el recuadro se da como información adicional al tema

MIPv4: Registration

- The `registration reply` message is carried in UDP messages and consists of the following fields:
  - Type: 3 (i.e. registration request)
  - Code: Indicates the result of the registration request
  - Lifetime: Seconds before the registration expires
  - H@: Home IP@ of the MN;
  - Home Agent: HA IP@.
  - Identifier: 64-bit generated MN for matching registration requests and for security purposes

La información en el recuadro se da como información adicional al tema

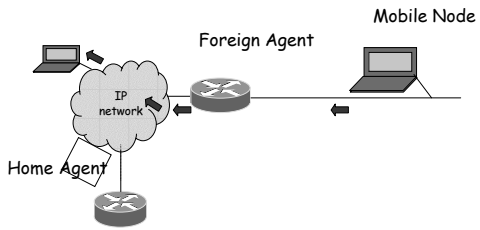
MIPv4: Tunneling



The HA intercepts the packet addressed to the MN's home address and tunnels It to the MN's care-of-address.
The FA removes the packet from the tunnel and delivers the packet to the MN.

NOTE: in case of collocated c-o-@, the tunnel ends in the MN

MIPv4: triangular routing



In the reverse direction, packets are sent directly to their destination (Triangular routing)

MIPv4: Tunneling & triangular routing

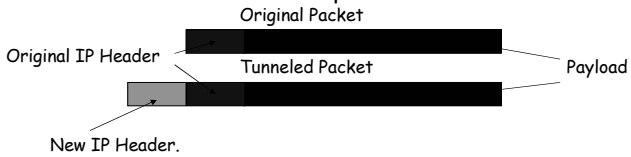
Tunneling

Types of tunneling:

- IP in IP Encapsulation (RFC 2003)
- Minimal Encapsulation (RFC 2004)
- Generic Routing Encapsulation (GRE, RFC 1701)

MIPv4: Tunneling & triangular routing

IP in IP Encapsulation



(i) Change source and destination addresses,

(ii) set the protocol = 4, and

(iii) update the Header length, total length, checksum and fragmentation.

(iV) if the inner header has D=1, in the outer header D=1.

(v) Set a TTL so that the packet can leave the tunnel

When the packet leaves the tunnel, the TTL of its inner header has been decremented twice, i.e. the tunnel between two routers behaves as a sinlge link connecting these two routers

MIPv4: Tunneling & triangular routing

- When an ICMP message is generated in the tunnel, it is sent back to the encapsulating router, and not to the originating node.
- It is only required that the ICMP payload has the first 8 bytes of the original message, and it is thus not possible in general to determine who was the originating node.
- However, by maintaining information called soft-state, a tunnel entry-point can make determination of the orginating node upon receipt of an ICMP message

MIPv4: Tunneling & triangular routing

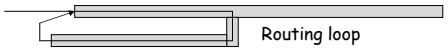
- The soft-state is a set of variables that describe the current characteristics of the tunnel. These variables include:
  - Path MTU of the tunnel
  - Length of the tunnel measured in hops
  - Whether or not the tunnel is reachable.
- The soft-state is maintained from the ICMP messages received from the tunnel

MIPv4: Tunneling & triangular routing

- The soft-state is used to generate ICMP message addressed to the originating node, at the time the packet enters the tunnel (i.e. in some way it anticipates that if the packet is sent, an ICMP message will be received…)
- E.g: If a too large packet is received with D=1, the entry-point of the tunnel can use the MTU path variable of the soft state to generate an ICMP "Fragmentation needed but D=1" back to the originating node, and discard the original packet.

MIPv4: Tunneling & triangular routing

- Recursive encapsulation is the process by which a routing loop causes that the packet reenters the same tunnel before exiting.



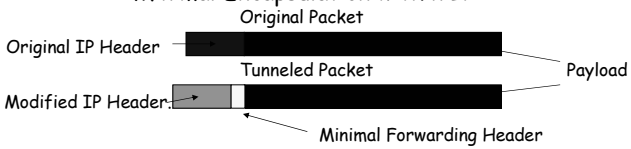
Additional headers with "fresh" TTL fields would be added, and the Packet would be captured (and fragmented as the packet size Grows) forever.

MIPv4: Tunneling & triangular routing

- Recursive encapsulation is avoided using the following tests:
  - If the tunnel entry-point is itself the source IP@ of the inner header, then there is recursive encapsulation. This test is only applied to packet which are not generated in the entry-point itself.
  - If the tunnel exit-point is itself the source IP@ of the inner header, then there is recursive encapsulation.

MIPv4: Tunneling & triangular routing

Minimal Encapsulation within IP



The original IP header is modified

(i) Change source and destination addresses, (ii) set the protocol = 55,

(iii) update the Header length, total length, checksum (for new header and payload) and fragment.

(iV) if the entry-point is not the origin of the packet, decrement TTL.

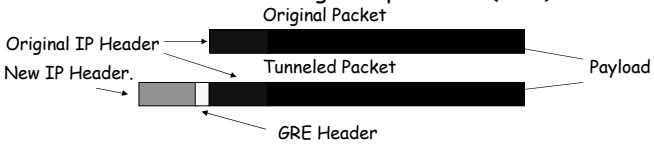
The Minimal Forwarding Header is filled as (i) Copy original Protocol field, (ii) set bit S if the packet is originated in the tunnel entry-point (iii) compute a header cheksum including MFH, (iv) copy original destination IP@, and (v) if S=0, copy original original source IP@

MIPv4: Tunneling & triangular routing

- It cannot be used for already fragmented packets (fragmentation info of the original header is lost)
- TTL is decremented by each router in the tunnel.
- Soft state must still be maintained
- Same procedure as before for preventing recursive encapsulation.

MIPv4: Tunneling & triangular routing

Generic Routing Encapsulation (GRE)



GRE supports encapsulation of multiprotocol packets.

Incorporates a field recur which is decremented by one everytime the packet is encapsulated, controlling thus the recursive encapsulation problems.

MIPv4: Security issues

- In order to prevent security attacks in which:
  - A node may pretend to be a FA and send a registration request so as to divert traffic intended for a MN itself
  - A malicious agent replay old registration messages, curring the MN from the network

registration request/reply messages as authenticated using authentication extensions which incorporate message digests based on MD5 digest algorithm.

MIPv6: Main differences with MIPv4

Comparison between IPv6 and IPv4 mobility

Mobile IPv4 Concept	Equivalent Mobile IPv6 Concept
MN, HA, home link, foreign link	same
Mn´s home address	Globally routable home address and link-local home address
Foreign agent	A "plain" IPv6 router on the foreign link (foreign agent no longer exists)
Foreign agent care-of address	All care-of addresses are collocated
Collocated care-of address	
Care-of address obtained via Agent Discovery, DHCP or manually	Care-of address obtained via Stateless Address Autoconfiguration, DHCP, or manually
Agent Discovery	Route Discovery
Authenticated registration with home agent	Authenticated notification of home agent and other correspondent nodes
Routing to MNs via tunneling	Routing to MNs via tunnelling
Route optimization via separate protocol specification	Integrated support for route optimization

Bibliography

- W. Stallings "Mobile IP", IPJ Vol4, No2, June 2001 (see www.cisco.com/ipj)
- J. D. Solomon, "Mobile IP, The Internet Unplugged", Prentice-Hall 1998