EEC173B/ECS152C, Spring 2009

Mobile Management in Wireless Networks

- Mobile IP

Acknowledgment: Selected slides from Prof. Mohapatra and Prof. Schiller

IP address problem

- Internet hosts/interfaces are identified by IP address
  - Domain name service translates host name to IP address
  - Based on IP destination address, network prefix (e.g. 129.13.42) locates physical subnet
  - Mixes naming and location
- Moving to another network requires different network address
  => change of IP address
  - But this would change the host's identity
  - How can we still reach that host?

  => or needs special entries in the routing tables

Routing Issues

- 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
- 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

Mobile IP: Introduction

- Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one Internet attachment point to another
- Leaves Internet routing fabric unchanged
- Does not assume "base stations" exist everywhere
- Simple
- Correspondent hosts don't need to know about mobility
- Works both for changing domains and network interfaces
- Although applicable for wired environment, it is particularly suited for wireless environment
- Mobile versus nomadic connectivity
  - Mobile: connection is maintained
  - Nomadic: new connection after every move

Requirements to Mobile IP (RFC 3344)

- 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

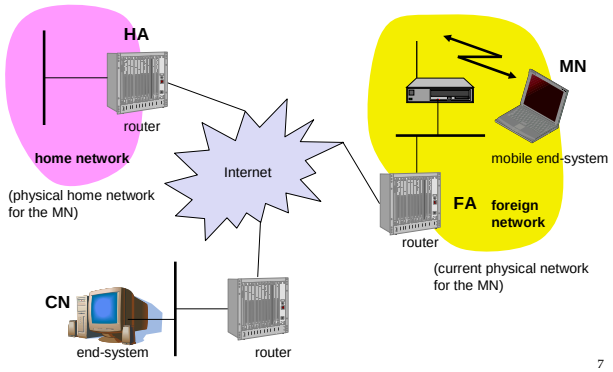
5

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

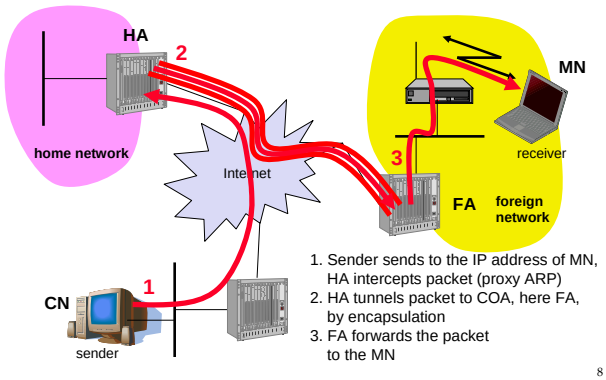
6

Example network



7

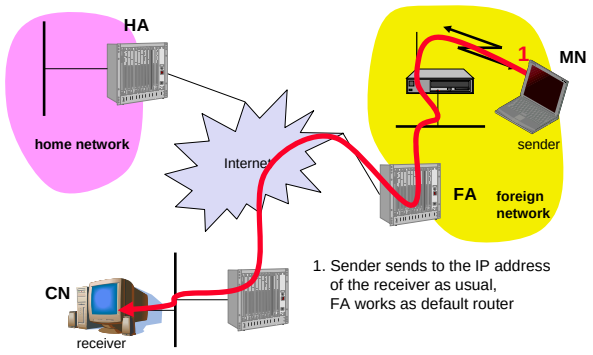
Data transfer to the mobile system



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

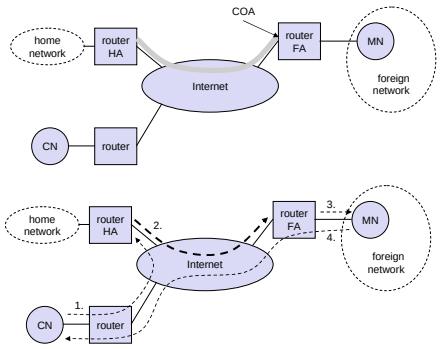
8

Data transfer from the mobile system



9

Overview



10

Basic Capabilities

1. Discovery
   - Uses discovery process to identify prospective home agents and foreign agents
2. Registration
   - Uses an authenticated registration procedure to inform its home agent of its care-off address
3. Tunneling
   - Forwarding IP datagram for a home address to a care-off address

11

1. Discovery

- The discovery process is very similar to the router advertisement process used in ICMP (Internet Control Message Protocol)
- 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 (standard case for home network)
  - MN reads a COA from the FA advertisement messages
- A mobile node listens for these agent advertisement messages. It compares its own network address with that of the router to determine if it is in home or foreign network

12

Agent advertisement

0 – 7	8 – 15	16 – 23	24 – 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			
. . .			

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

1. Discovery – other issues

- Agent Solicitation
  - Foreign agents are expected to issue agent advertisement messages periodically
  - If a mobile agent needs agent information immediately, it can issue an ICMP router solicitation message
- Move Detection
  - Use of lifetime field
  - Use of network prefix
- Co-Located Addresses
  - If a mobile node moves to a network which has no foreign agent, it may act as its own foreign agent using a co-located care-of address
  - A co-located care-off address is an IP address obtained by the mobile node that is associated with its network interface

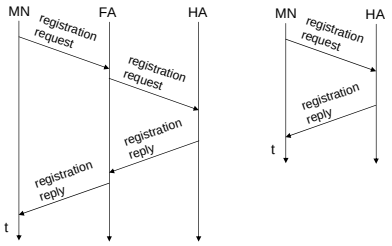
2. Registration

- Always limited lifetime!
- If the mobile node (MN) is using a co-located CoA, then it registers directly with Home Agent (HA)
- Else, MN sends CoA to HA via Foreign Agent (FA)
  - MN requests the forwarding service by sending a registration request to the foreign agent (FA) that it wants to use
  - FA relays this request (with CoA) to the mobile node's home agent (HA)
  - HA either accepts or denies the request and sends a registration reply to the FA
  - FA relays this reply to the MN
- Registration operation uses two types of messages carried in UDP segments:
  - Registration request message
  - Registration reply message

Secure Registration

- Threats:
  - A node may pretend to be a foreign agent and send a registration request to a home agent so as to divert traffic intended for a mobile node to itself
  - A malicious agent may replay old registration messages, effectively isolating the mobile node
- Protection:
  - Message authentication using a code that the sender inserts into the message using a shared key
  - The receiver uses the code to ensure that the message has not been altered

Registration



Mobile IP registration request

0 – 7	8 – 15	16 – 23	24 – 31
type = 1	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 mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

Mobile IP registration reply

0 – 7	8 – 15	16 – 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

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

The Role of Home Agent

- 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

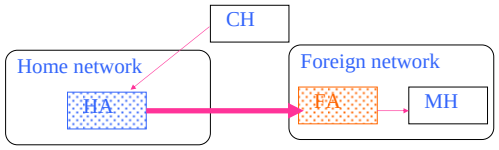
3. Tunneling

- Once a MN is registered with a HA, the HA must be able to intercept IP datagrams sent to the MN's home address so that these data can be sent via tunneling
- The HA needs to inform the other nodes on the same network that IP datagrams with a destination address of the MN in question should be delivered (at the link level) to this agent
- To forward an IP datagram to a care-of address, the HA puts the entire IP datagram into an outer IP datagram – this process is known as a form of encapsulation

Basic Mobile IP – *to* mobile hosts

MH = mobile host (or node)
CH = correspondent host (or node)
HA = home agent
FA = foreign agent

(We'll see later that FA is not necessary or even desirable)



•MH registers new "care-of address" (FA) with HA
•HA tunnels packets to FA
•FA decapsulates packets and delivers them to MH

Packet addressing

Packet from CH to MH

Source address = address of CH
Destination address = home IP address of MH
Payload

Home agent intercepts above packet and tunnels it

Source address = address of HA
Destination address = care-of address of MH
Source address = address of CH
Destination address = home IP address of MH
Original payload

Encapsulation

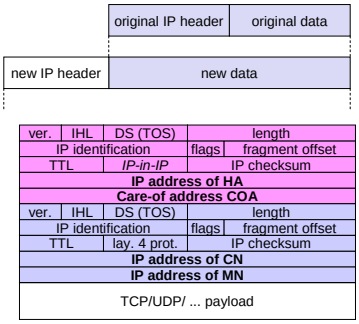
- IP-within-IP Encapsulation
  - The entire IP datagram becomes the payload in a new IP datagram
- Minimal Encapsulation
  - The new header is inserted between the original IP header and the original payload
- Generic Routing Encapsulation (GRE)
  - Generic encapsulation method developed before Mobile IP

Encapsulation: IP within IP

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

25

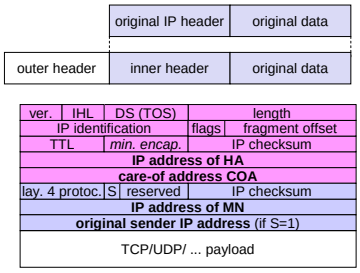
Encapsulation: IP within IP (Cont'd)



26

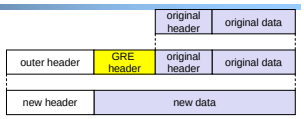
Minimal Encapsulation

- 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

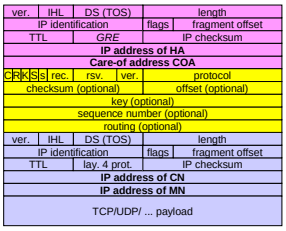


27

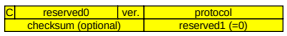
Generic Routing Encapsulation



RFC 1701



RFC 2784

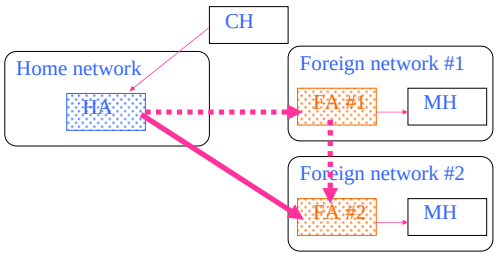


28

Optimization of Packet Forwarding

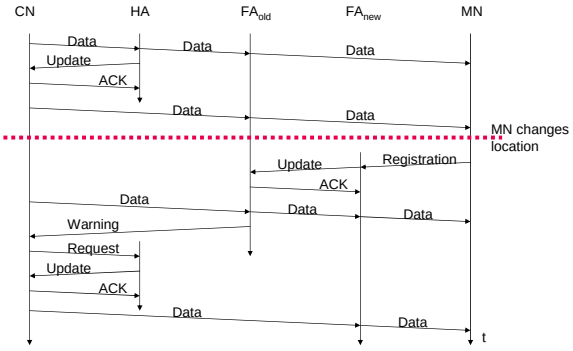
- Triangular Routing
  - Sender sends all packets via HA to MN
  - Higher latency and network load
- "Solutions"
  - Sender learns the current location of MN
  - Direct tunneling to this location
  - HA informs a sender about the location of MN
  - Big security problems!
- Change of FA
  - Packets on-the-fly 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

When mobile host moves again



•MH registers new address (FA #2) with HA & FA #1
•HA tunnels packets to FA #2, which delivers them to MH
•Packets in flight can be forwarded from FA #1 to FA #2

Change of Foreign Agent

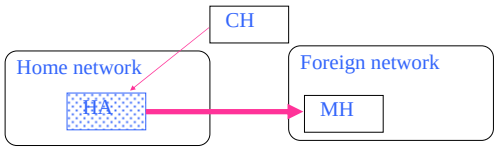


Problems with Foreign Agents

- Assumption of support from foreign networks
  - A foreign agent exists in all networks you visit?
  - The foreign agent is robust and up and running?
  - The foreign agent is trustworthy?
- Correctness in security-conscious networks
  - We'll see that "triangle route" has problems
  - MH under its own control can eliminate this problem
- Other undesirable features
  - Some performance improvements are harder with FAs
- We want end-to-end solution that allows flexibility

Solution

•Mobile host is responsible for itself
- -(With help from infrastructure in its home network)
- -Mobile host decapsulates packets
- -Mobile host sends its own packets
- -"Co-located" FA on MH



⇒MH must acquire its own IP address in foreign network
This address is its new "care-of" address
Mobile IP spec allows for this option

Obtaining a Foreign IP Address

- Can we expect to obtain an IP address?
  - DHCP becoming more common
  - Dynamic IP address binding like some dial-up services
  - Your friend can reserve an IP address for you
  - Various other tricks
  - More support for dynamic IP address binding in IPv6
- This assumes less than getting others to run a FA

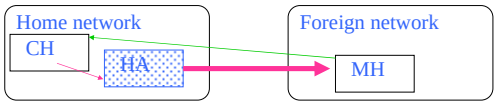
Design implications

- New issues: the mobile host now has two roles:
  - Home role
  - Local role

- More complex mobile host
- Loss of in-flight packets? (This can happen anyway.)

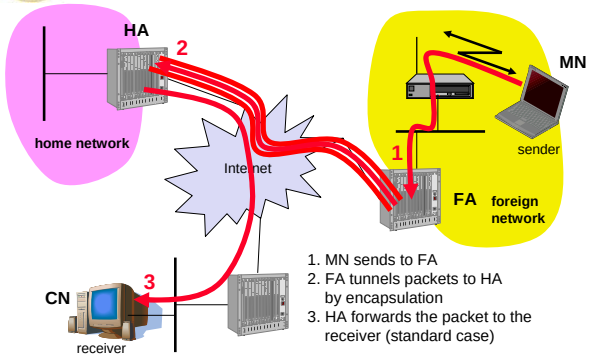
+ Can visit networks without a foreign agent
+ Can join local multicast groups, etc.
+ More control over packet routing = more flexibility

Problems with ingress filtering

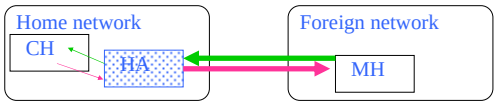


- Mobile host uses its home IP address as source address
- Security-conscious boundary routers will drop this packet
  - Router accept often only "topological correct" addresses

Solution: Reverse tunneling (RFC 3024)



Bi-directional Tunnel



- Provide choice of "safe" route through home agent both ways
  - 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 to far away from the receiver)
- This is the slowest but most conservative option

More about Reverse Tunneling

- 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

Mobile IP and IPv6 (Cont'd)

- 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

41

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!

42

Security in Mobile IP

- Security requirements (Security Architecture for the Internet Protocol, RFC 1825)
  - Integrity: any changes to data between sender and receiver can be detected by the receiver
  - Authentication: sender address is really the address of the sender and all data received is really data sent by this sender
  - Confidentiality: only sender and receiver can read the data
  - Non-Repudiation
    sender cannot deny sending of data
  - Traffic Analysis
    creation of traffic and user profiles should not be possible
  - Replay Protection
    receivers can detect replay of messages

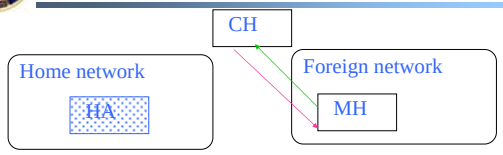
43

Problem: performance

- Example: short-lived communication
  - When accessing a web server, why pay for mobility?
  - Do without location-transparency
  - Unlikely to move during transfer; can reload page
  - Works when CH keeps no state about MH

44

Solution: yet more flexibility



•Use current care-of address and send packet directly
-This is regular IP!

•More generally:
-MH should have flexibility to adapt to circumstances
-A range of options: from slow-but-safe to regular IP
-Should be an end-to-end packet delivery decision (no FA)

45

Routing options

- Allow MH to choose from among all routing options
- Options:
  - Encapsulate packet or not?
  - Use home address or care-of address as source address?
  - Tunnel packet through home agent or send directly?
- Choice determined by:
  - Performance
  - Desire for transparent mobility
  - Mobile-awareness of correspondent host
  - Security concerns of networks traversed
- Equivalent choices for CH sending packets to MH

46

Mobility 4x4

	Outgoing Indirect, Encapsulated	Outgoing Direct, Encapsulated	Outgoing Direct, Home Address	Outgoing Direct, Temp. Address
Incoming Indirect, Encapsulated	Most reliable, least efficient	Requires decapsulation on CH	No security-conscious routers on path	
Incoming Direct, Encapsulated		Requires fully mobile-aware CH	No security-conscious routers on path	
Incoming Direct, Home Address			Requires both hosts to be on same net. seg.	
Incoming Direct, Temp. Address				Most efficient, no mobility support

47