
Mobile Internet Protocol: The Basics



Outline

- The problem
 - **Mobility vs Portability**
- Proposed Solution
 - Terminology
 - Registration & maintenance
 - Security
 - Tunnels
 - Optimizations
 - Mobile IP for IPv6



Levels of Addresses in the Internet

- **Domain name (DNS address)**
 - A location-dependent identifier of a host
cicoria.polito.it
- **Internet address (IP address)**
 - The logical location of a host interface:
(sub)network ID followed by host ID 130.192.9.136
- **Physical address (MAC address)**
 - The hardware address of an interface card 00 a4 24 4a 82 07



Routing in the Internet

- Packets flow from link (subnetwork) to link via routers
- Packets are routed individually based on their IP address (not on DNS name)
- Routing is based on the (sub)network prefix of the IP address



Connections between Internet Computers

- Connections are defined by:
 - Source IP address (L3)
 - Source port number (L4)
 - Destination IP address (L3)
 - Destination port number (L4)
 - Protocol type (e.g., TCP rather than UDP) (L4)



Why Mobile Internet? (1)

- Internet is growing exponentially
 - Many companies use Internet technology for their internal networks (intranets)
 - Increasing support for real-time services, e.g., VoIP
- Internet is the dominant technology for the core network of future mobile networks



Why Mobile Internet? (2)

- Wireless communications technologies suitable for packet data are becoming available
 - IEEE 802.11 is the "wireless ethernet" standard
 - HomeRF is designed for home networking
 - Bluetooth is designed as "cable replacement"
 - Voice-oriented technologies introduce data capabilities (GPRS)
- Laptops, palmtops, PDAs are widely used



7

Why Mobile Internet? (3)

- Wireless medium has different properties than wired medium (packet loss due to bad propagation conditions)
- Communication nodes may move
- Since the cell size decreases, the frequency of cell switch procedures will increase significantly

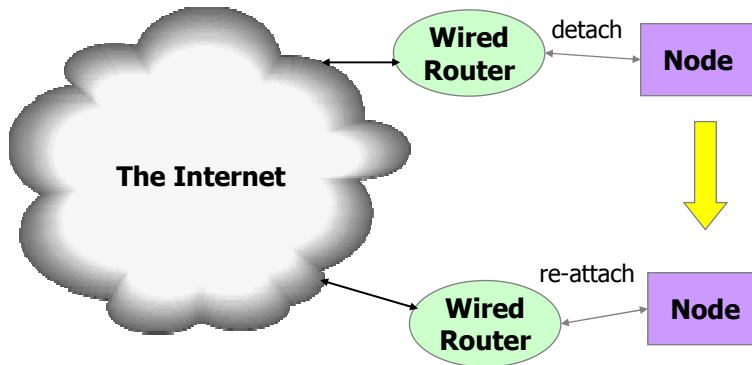


**Need to change point of
attachment to the Internet**



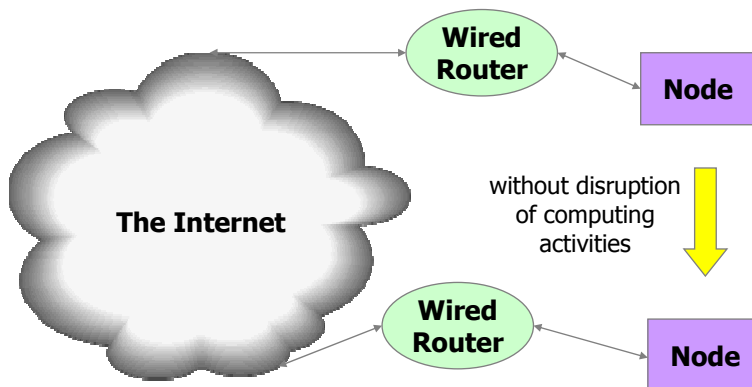
8

Portable Networking



9

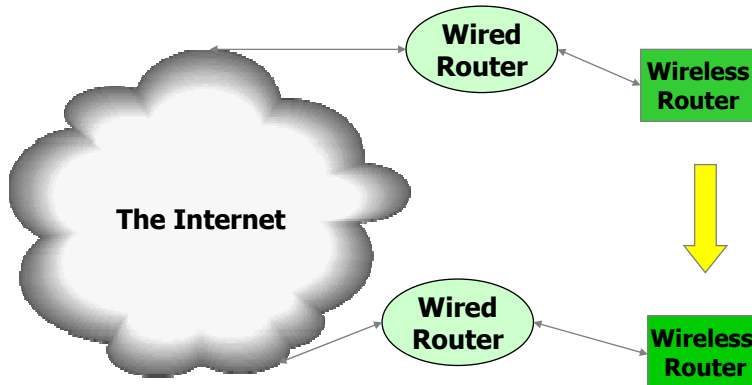
Mobile Networking Node Mobility



10

Mobile Networking

Router Mobility (e.g. Airplane Network)



11

What Are the Problems?

- Nodes in the Internet are identified by a specified IP address
 - Routing is performed using that same IP address
 - This address is associated with a fixed location (network ID)
- In TCP, connections are indexed by a quadruplet containing the IP address and the port numbers of both the connection end-points
 - Changing any of these numbers causes the connection loss



12

Possible Solutions

- The node must change its IP address whenever it changes its attachment point
 - Requires upper-level protocols to handle address changes, thus making transparent mobility impossible
- Host-specific routes must be propagated through the network
 - Requires significant routing table changes and doesn't scale well
- Use another level of indirection...



The Mobile IP Solution

- RFC 2002: standard proposed by a working group within the Internet Engineering Task Force (IETF)
- Current version of the protocol used in IPv4



Mobile IP

- **Why mobility at the network layer:**
 - Network layer present in all Internet nodes
 - Network layer is responsible for routing traffic to the proper location
 - Mobility across the whole Internet independently of the physical medium
 - Transparent to TCP and higher layers (including the application)



15

Mobile IP Design Goals

1. A mobile node must be able to communicate with other nodes after changing its link-layer attachment, yet without changing its IP address
2. A mobile node must be able to communicate with other nodes that do not implement mobile IP (back compatibility)
3. Leave higher layers unaffected
4. Use of authentication to offer security against **redirection attacks**
5. Small number of administrative messages, to save bandwidth & power (good scalability)
6. No additional constraints on the assignment of IP addresses

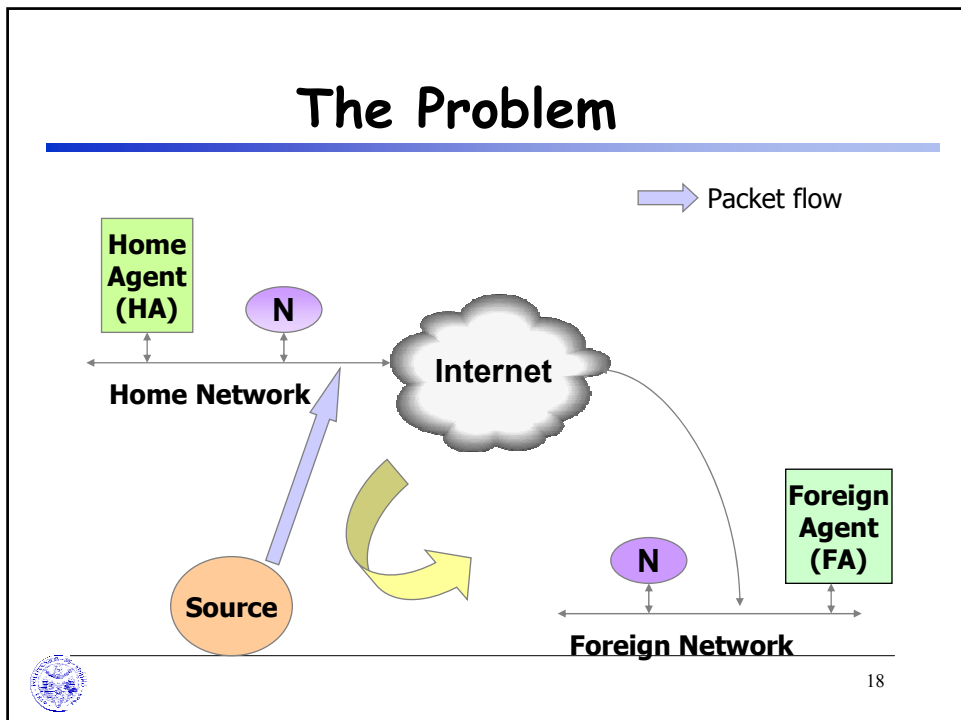


16

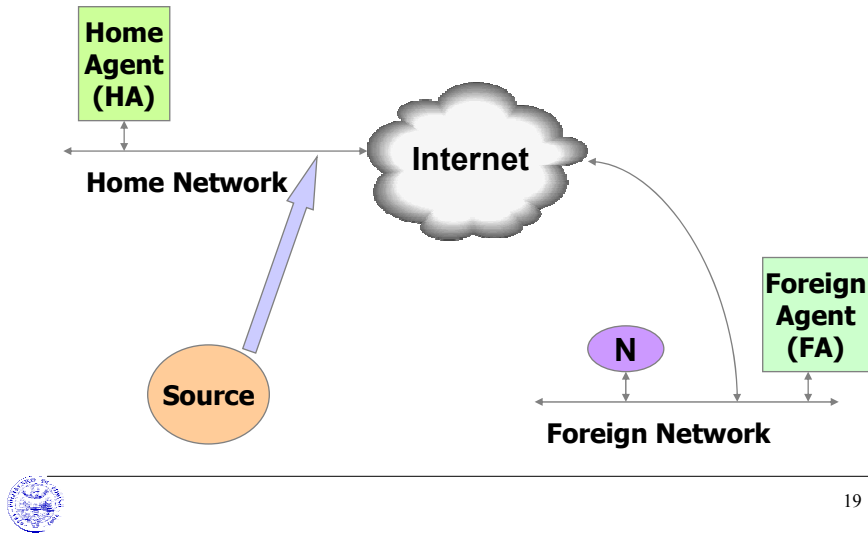
The Mobile IP Solution

- Allows the mobile node to use two IP addresses:
 - The **home address** is static and is used to identify, for instance, the TCP connection end-points. It makes it appear that the mobile node has not moved from its original network
 - The **care-of-address** is assigned on the foreign network, it is used to deliver the datagrams for the mobile node when it has moved out of its home network

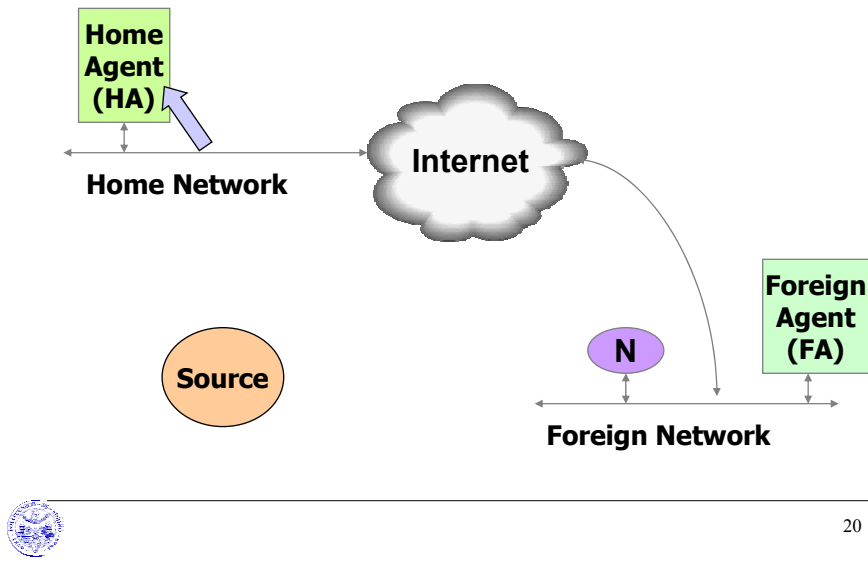
The Problem



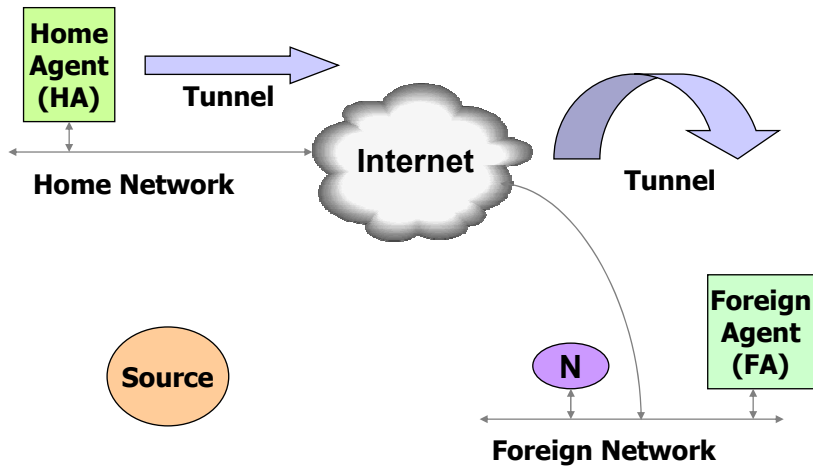
Solution in a Nutshell (1)



Solution in a Nutshell (2)

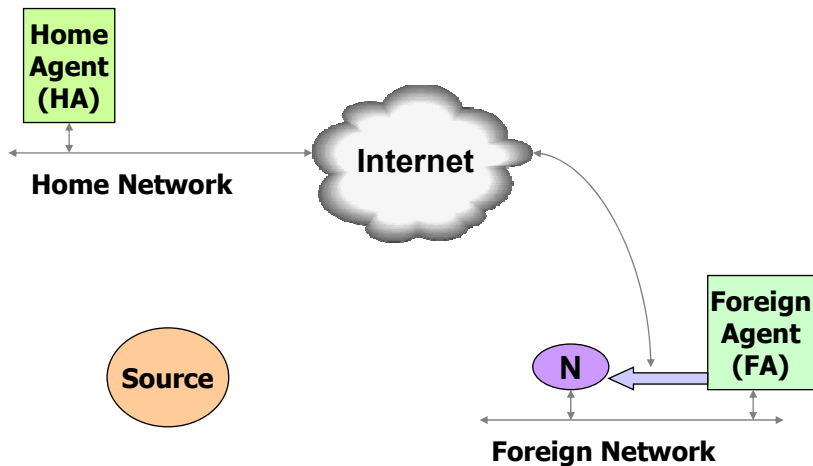


Solution in a Nutshell (3)



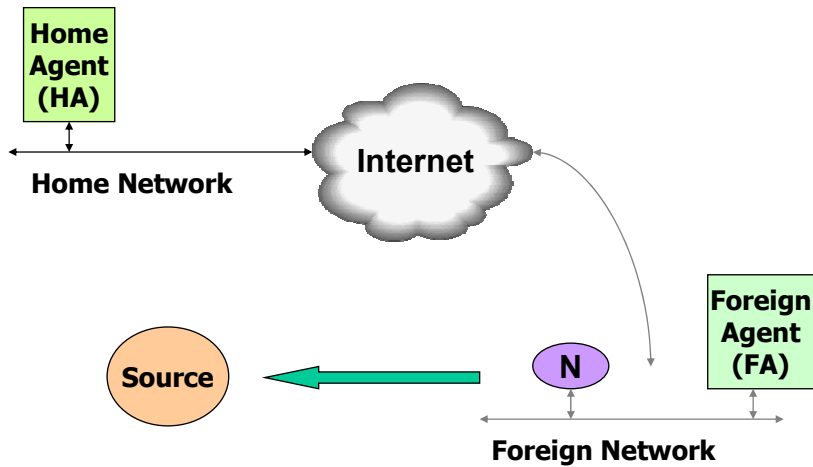
21

Solution in a Nutshell (4)



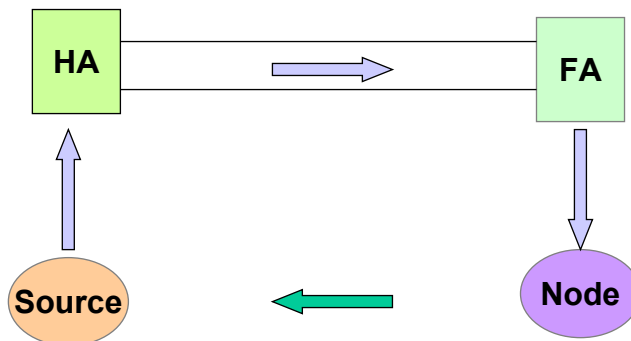
22

Solution in a Nutshell (5)



23

More Abstractly



24

Terminology (1)

- **Mobile node** - a host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address: It may continue to communicate with other Internet nodes at any location using its IP home address (constant address)
- **Home Network** - the network whose network prefix matches that of the mobile node's home address
- **Foreign Network** - the visited network
- **Correspondent node** - a peer with which the mobile node is communicating



25

Terminology (2)

- **Home Agent** - a router on the mobile node's **home network** that tunnels datagrams to the mobile node when it is away from home
- **Foreign Agent** - a router on the mobile node's **foreign network** that provides routing services to the mobile node while registered
- The mobile node is assigned a "**care-of address**" on the foreign network. This address is used to deliver the datagrams for the mobile node when it has moved out of its home network
 - This can either be the **foreign agent** address
 - Or, it can be "**co-located**" with the mobile node



26

Terminology (3)

- **Encapsulation** - The process of incorporating an original IP packet inside another IP packet, making the fields within the original IP header temporarily ineffective
- **Tunneling** - same as encapsulation with additional connotations about packet routing



Protocol Overview

- **Discovering the care-of address**
 - Mobility Agents (FAs and HAs) should **advertise** their services
 - A mobile node can **solicit** for mobility agents
- **Registration** - when a MN is away from home, it gets its **care-of address** on the foreign network that it must register with its HA
- **Datagrams delivery**
 - Datagrams must be forwarded by the home agent to the foreign agent, for delivery, to the care-of address
 - The delivery mechanism must handle all packets (including broadcast and multicast)
 - A **tunnel** (i.e., a **packet re-direction**) is used for this

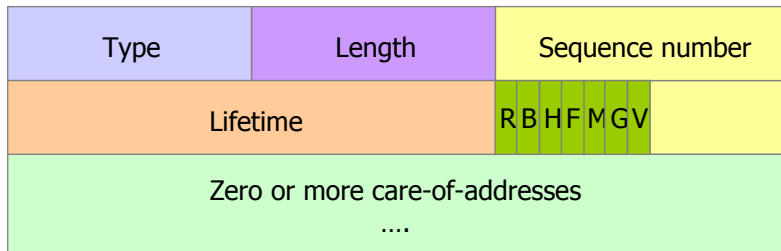
Advertisement & Solicitation

- The router discovery function of ICMP (Internet Control Message Protocol) is adapted for advertisement and solicitation
 - Routers broadcast or multicast advertisements on their directly attached subnetworks periodically (every second or every few seconds)
- MNs also can send out solicitation messages if they do not want to wait for the periodic advertisement. Solicits will cause a router to broadcast or multicast their advertisement
- After receiving an agent advertisement, a MN determines whether it is in its home network or in a foreign network

Agent Advertisement (1)

- Functions:
 1. Allows for detection of mobility agents
 2. Lets the MNs know whether the agent is a HA or a FA, and therefore whether it is on its home network or on a foreign network
 3. Lets MNs determine the network ID (netID) number
 4. If it's an FA:
 - it informs MNs on the special features provided by the FA, e.g., encapsulation techniques
 - Lists one or more care-of addresses

Agent Advertisement (2)



Agent Advertisement (3)

- The **type** field indicates the kind of extension applied to the advertisement (mobility agent extension type=3). (Of course, other extensions may precede or follow)
- The **length** field is the length of this single extension, it depends on the number of **included care-of-address that the FA is advertising** (usually only one care-of-address is advertised)
- The mobility agent usually increments the **sequence number** by 1 for each successive advertisement
- HAs do not have to advertise care-of-addresses, however they must send advertisements so MNs will know when they have returned to their home network

Agent Advertisement (4)

- The **flags** R,B,H,F,M,G, and V inform MNs on special features provided by the mobility agent
- Flags:
 - **R** - Registration is required even if the MN is using a co-located care-of-address
 - **B** - The foreign agent is busy
 - **H** - The agent is a home agent
 - **F** - The agent is a foreign agent
 - **M** - Minimal encapsulation
 - **G** - GRE encapsulation
 - **V** - Van Jacobson header compression



33

Agent Solicitation

- The MNs use agent solicitations to detect any change in the set of mobility agents available at the current point of attachment
- The MN can send one solicitation every second for three consecutive times
- If the MN does not receive any advertisement from the mobility agent, it backoffs until a max time period (which must be 1 minute long at least)



34

Movement Detection

A MN detects that it moved to another network if:

1. It receives an agent advertisement with network prefix different from the current one. When the current registration expires, the MN makes the new registration, or
2. The lifetime of the last received agent advertisement has expired and the MN has not received a new agent advertisement from its current mobility agent



The Registration Procedure



The Registration Procedure

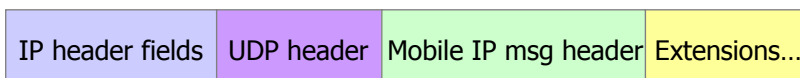
- Through the registration, the MN informs its HA of its current **care-of address**
- The HA creates a **binding** of the mobile node's care-of-address to the mobile node's home address. A binding is defined as the following triplet:
 - MN's home address
 - MN's care-of address
 - Registration lifetime
- Registration is also used to **renew** a binding that's about to expire
- The MN has to **de-register** when it returns home, MN and HA perform a new registration procedure



37

Registration

- There are two kinds of registration messages
 - Registration request
 - Registration reply
- Overall structure of the registration messages



38

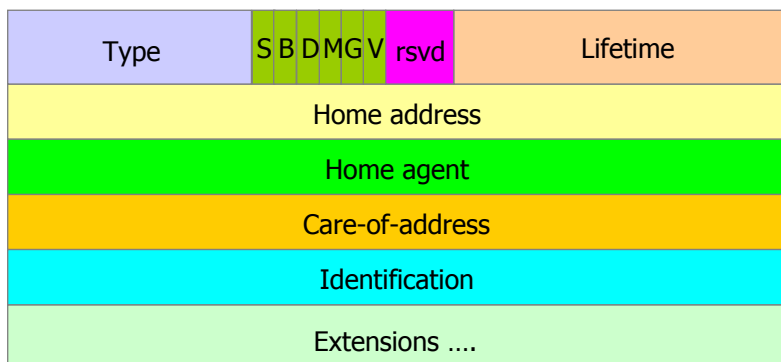
Registration Request

- The registration request allows the MN to inform its HA of its **care-of-address**, of **how long** the MN wants to use its care-of-address, and the special features available from the FA
- The FA acts as a **passive** agent during registration
 - If the MN has derived its care-of-address from the FA, the FA just forwards the registration request to the HA and passes the reply back to the MN
 - If the MN uses a co-located care-of-address, it sends the request directly to the HA using the co-located address as the source IP address of the request



39

Registration Request Format (1)



40

Registration Request Format (2)

- **B** - used to tell the HA to encapsulate broadcast datagrams from the home network to the care-of-address
- **D** - says whether the MN is co-located with the care-of-address
- **Home address**
- **Proposed care-of address**
- **Identification field** - used for reply protection
- **Mobile-home authentication extension** - required in every registration to allow the HA to prevent fraudulent remote redirections

Registration Reply (1)

Type	Code	Lifetime
Home address		
Home agent		
Care-of-address		
Identification		
Extensions		



Registration Reply (2)

- **Lifetime** - tells the MN for how long the registration binding will be considered valid by the HA. It can be shorter than the one included in the registration request, but never longer
- **Code** - describes the status of the registration: accepted or refused, and if refused it indicates the reason
 - Registration denied by the FA:
 - Insufficient resources
 - HA unreachable
 - Registration denied by the HA:
 - Insufficient resources
 - MN failed authentication
 - Need for resynchronization between HA and MN (sync. can be based on timing or the use of nonces)



The Role of the FA

- The FA can limit the binding lifetime to the value that it puts into its agent advertisement
- The FA maintains a visitor list for each pending or current registration and uses it to deliver packets to the MN
- Each visitor list entry includes:
 - Link-layer MN's address
 - MN's home address
 - Care-of-address
 - HA's address
 - Identifier field
 - Lifetime



Securing the Registration Procedure



45

Registration and Security (1)

1. A malicious user could disrupt the communication between the MN and the HA by sending a registration request containing a bogus care-of-address (**redirection attack**)
2. A **replay attack** occurs when a 3rd party can capture your packets and then "replay" them, fooling you into thinking they are correctly delivered and authenticated



To defend the system against these attacks,
an authentication mechanism is performed



46

Registration and Security (2)

- To prevent this, an unforgeable value is included in the identifier field of each registration and changes for every new registration
 - **Timestamps:** the sender includes a timestamp, and receiver must find that the timestamp is close to its local time
 - **Nonces:** Each message from A → B includes a new random number. When B replies to A, it must include that same random number. Likewise, each B → A message includes a new random number generated by B and echoed by A



47

Registration and Security (3)

- We need to use signatures for timestamp-based methods because the time value used to defeat replay attacks is easily predictable
- Nonce-based systems are based on pseudo-random number sequences. As long as the sequence is not predictable (i.e., it's heavily influenced by a secret key), then we may not need to authenticate it
- The default authentication algorithm uses keyed MD5 to compute a 128-bit message digest



48

Digital Signatures: MD5 (1)

- A digital signature is an electronic way of "signing" a document such that
 - Both you and the sender agree that only the sender could send the document
 - Both you and the sender agree the contents haven't been modified
- Notice that the message doesn't need to be encrypted

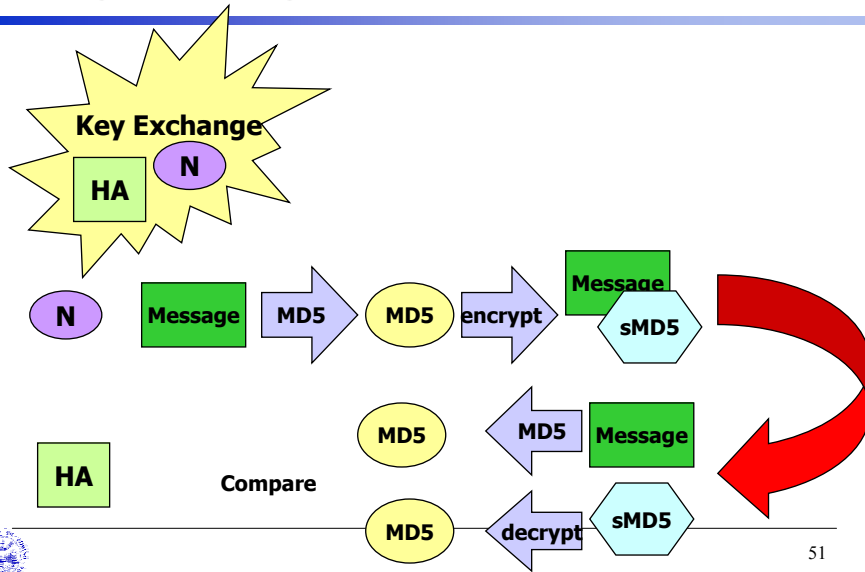


Digital Signatures: MD5 (2)

- The HA and the mobile node must conduct some form of prior key exchange. This defines a "secret key" between the two nodes, either a shared key or a public/private key pair
- This is not the same as encrypting the communication channel



Digital Signatures: MD5 (3)

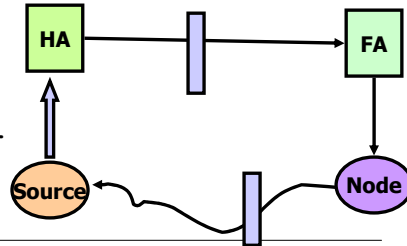


Delivering Datagrams: Tunneling and Route Optimization



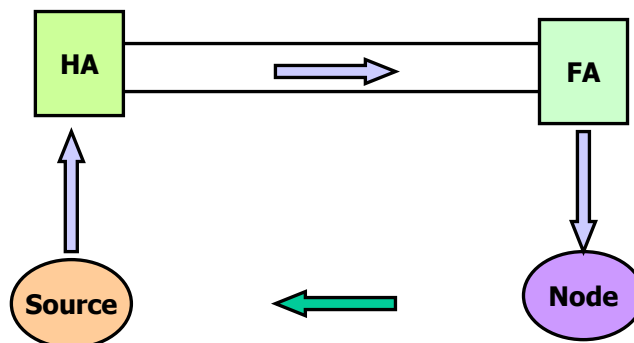
Delivering Datagrams

- Once a MN has registered a care-of address, datagrams must be delivered to that address
- Many options to *get messages there*:
 - Use forward tunnels
 - When the MN gets the care-of address from the FA, it's the FA that decapsulates the tunneled packets
- And other options to *get messages back*:
 - Have node directly contact source
 - Use reverse tunnels



53

Tunneling Basics



54

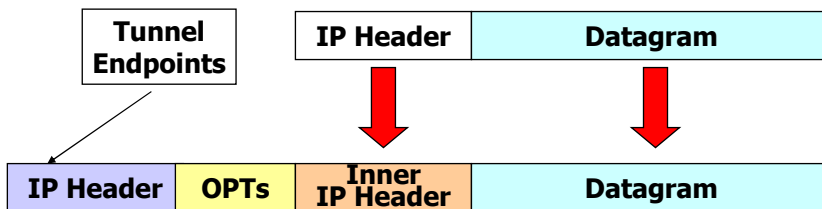
Encapsulation Techniques

- IP-in-IP encapsulation
- Minimal encapsulation
- GRE -- Generic Routing Encapsulation
- PPTP -- Point to Point Tunnel Protocol [RFC2637]
- L2TP -- Layer 2 Tunneling Protocol [RFC2661]



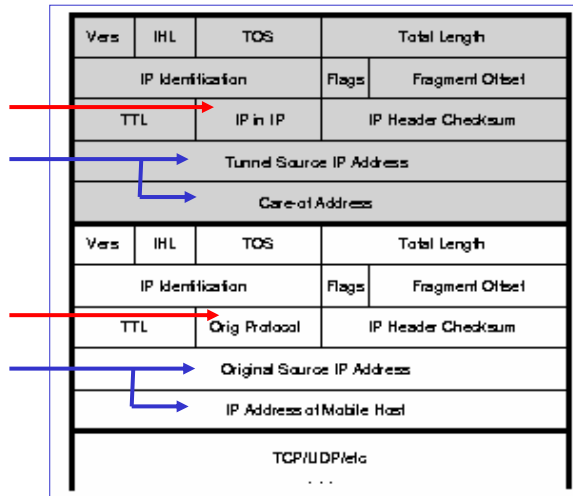
55

IP in IP



56

IP-in-IP Encapsulation



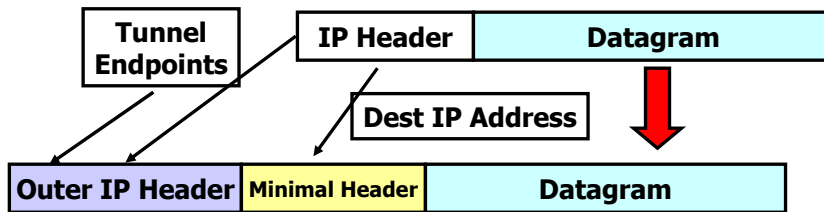
57

IP in IP

- The outer IP header source & destination address identify the **tunnel end-points** (I.e., HA & FA)
- Version: Outer protocol is '4' (IP protocol)
- The inner IP header source address and destination address identify the original sender & recipient
 - Inner IP header not changed by the encapsulator, except for changing TTL which can be decreased by 1
- Other header options used for **authentication** might be added to outer header
- Some outer IP header fields are copied from the inner IP fields (TOS), most are re-computed (checksum, length) based on the new datagram

58

Minimal Encapsulation



59

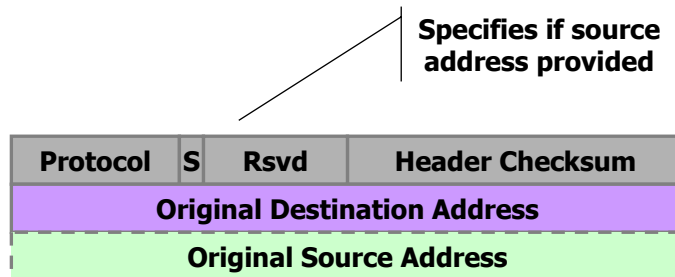
Minimal Encapsulation

- We can save some space by recognizing that much of the inner header can be derived from the outer header
 - Copy inner header
 - Modify protocol field to be 55, for the minimal encapsulation protocol
 - Destination address replaced by tunnel exit
 - If encapsulator isn't originator of message, replace source address with address of encapsulator
 - Increment total length by the size of the additional header (either 12 or 6 octets)
 - Recompute checksum



60

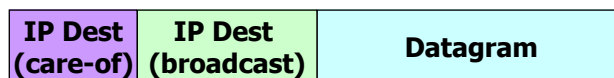
Minimal Encapsulation Header



61

Handling Broadcast & Multicast

- HA should forward everything (but not ARP packets)
- Broadcast packets are either sent directly to co-located nodes or "double encapsulated"



- Mobile nodes can join multicast routes while on the foreign network
 - But, this doesn't handle link-level or administratively scoped multicast



62

Lastly, ARP

- When a MN is on a foreign net, its HA uses proxy ARP to get any messages directed to it
 - When a MN leaves home, the HA uses ARP to update all ARP tables on the subnet
 - When a MN returns home, it uses ARP to recapture its messages
- When a MN is away from home, it can't transmit any broadcast ARP or ARP reply messages
- This means that even "local" traffic destined to the MN on the foreign network goes to the HA and then the FA and then the MN



Route Optimization

- Obviously, all this redirection has a performance penalty
 - Solution: remove the **triangulation!**
- Route optimization provides a means for nodes to **cache the binding** of a MN and then tunnel their own datagrams directly to the care-of address indicated in the binding thus bypassing the HA
- Consists of two main parts:
 - **Updating binding caches**
 - **Smooth handoffs between foreign agents**



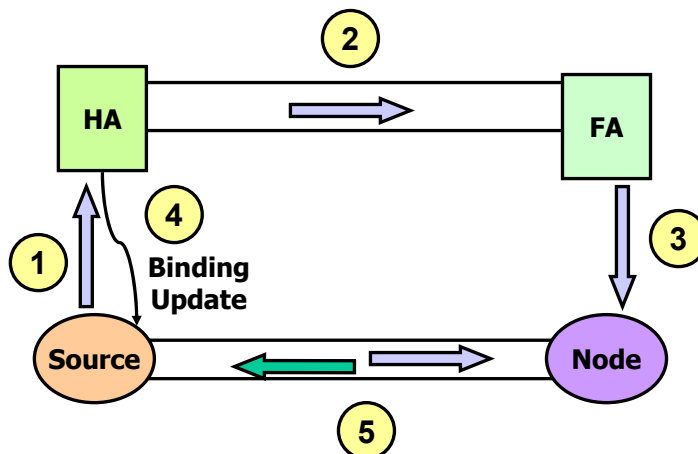
Binding Caches

- Whenever the HA intercepts a datagram for the MN and tunnels it, it understands that the correspondent node has an out-of-date address. Then, the HA sends to the CN a **Binding Update** (which doesn't need to be acked because it is re-sent every time this happens)
- Authentication is required so that the recipient of a binding update can believe it
- The CN can use the binding it's got to tunnel datagrams directly to the MN on the MN's foreign network



65

Binding Update



66

Smooth Handoff (1)

- When a MN moves & registers with a new FA, the basic Mobile IP protocol does not notify the previous FA
 - New messages tunneled to new care-of address
 - In-flight datagrams are lost & upper-level layers (e.g. TCP) should handle that
- Route optimization allows the MN and FA to create a **registration key** for later use in making a smooth transition to a new point of attachment
- As part of registration, the mobile node can have the new FA contact the previous FA



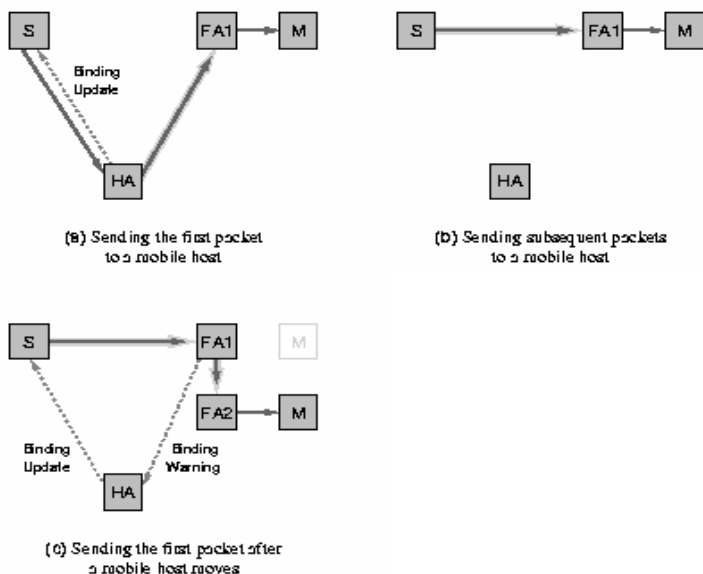
Smooth Handoff (2)

- The MN includes a **Previous Foreign Agent Notification Extension** in its registration request toward the new FA
- The new FA creates a binding update for the previous FA as part of the registration procedure and requests a **Binding Acknowledgment** from the previous FA
- Authentication for the binding update is computed by the MN by using the secret key shared with its previous FA
- The binding update to the previous FA has to be occasionally retransmitted until a binding acknowledgment is received or the MN is sure that its previous FA has expired its binding

Binding Warning

- Whenever the FA receives a tunneled datagram for a MN for which it has a binding cache entry (not a visitor list entry), it will notify the HA that the CN has an out-of-date address, through a **Binding Warning**
- Upon receiving a binding warning, the HA should send a binding update to the CN
- A binding warning does not need authentication since it does not directly cause any redirection

Binding Warning

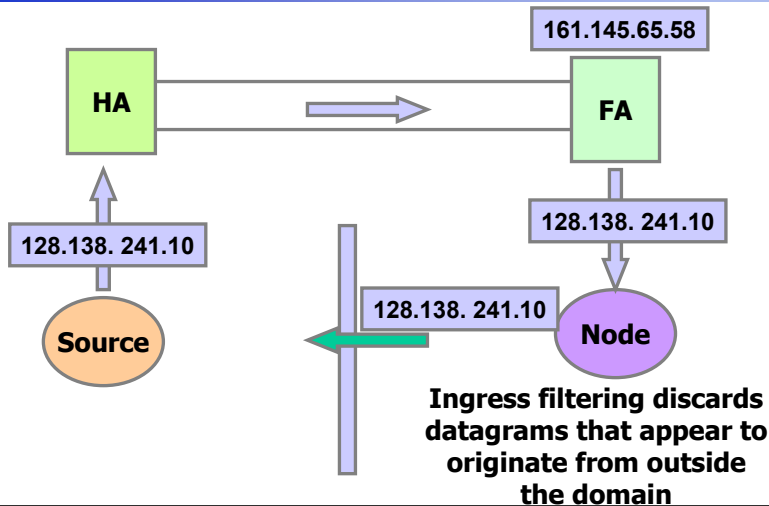


Further Issues



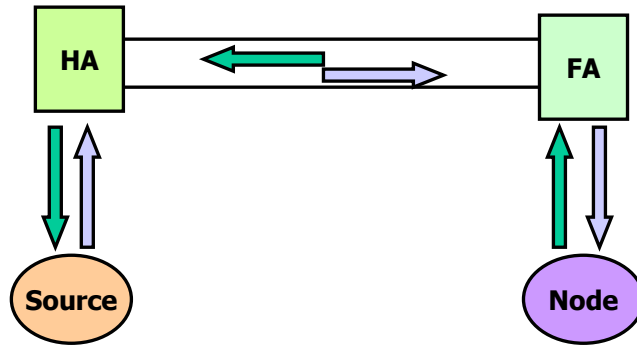
71

The Need for Reverse Tunneling



72

Reverse Tunnel in Action



How Will Mobile IP Change with IPv6?



IPv6: New Features

- IPv6 address configuration protocol forms a good basis for mobility management in wireless networks
 - Neighbors Discovery
 - Stateless Address Configuration



The MN is able to obtain a care-of addresses by using the above-mentioned procedures



75

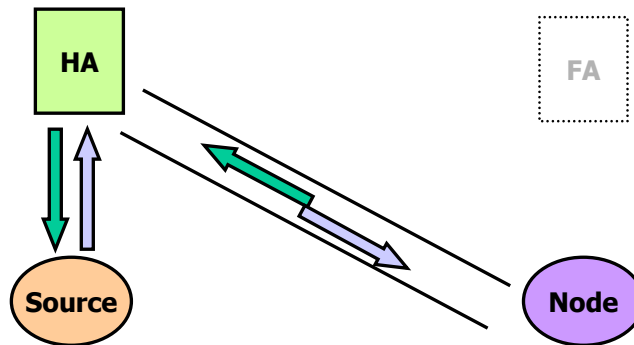
Mobile IP in IPv6

- FAs are not needed anymore, they can be eliminated
- It remains:
 - The concept of the HA sending datagrams from the home network to the MN's care-of address
 - Encapsulation of datagrams to the MN's care-of address



76

Alternate Reverse Tunnel



77

Route Optimization in IPv6

- Binding Updates in route optimization can be easily implemented by using the newly defined destination options in IPv6
- Destination options can be included in any packet that the MN would send to the CN
- Destination options will be read by the destination only, thus it does not cause performance penalty at intermediate routers for using them (in terms of additional delay)



78

Encapsulation and Binding Update in IPv6

- If a packet arrives at the HA, it will be encapsulated and sent to the MN
- When the MN receives an encapsulated IPv6 packet, it infers that the CN should receive a binding update. The MN sends the binding update in a destination option along with the very next packet transmitted to the CN
- This needs authentication. Through the security functions between the MN and the CN specified in IPv6, the MN will be the only one authorized to send binding updates to the CN. The MN would do it as soon as a packet is transmitted to the CN

References

- C. Perkins and A. Myles, "Mobile IP," technical report.
- B. Lancki, A. Dixit, V. Gupta, "Mobile-IP: Supporting Transparent Host Migration on the Internet," Linux Journal, June 1996.
- D. Johnson and D. Maltz. "Protocols for Adaptive Wireless and Mobile Networking", IEEE Personal Communication, 3(1), February 1996
- C. Perkins and D. Johnson. "Mobility Support in IPv6," Proceedings of the Second Annual International Conference on Mobile Computing and Networking (MobiCom'96), November 1996.
- M. Baker, X. Zhao, S. Cheshire, J. Stone, Stanford University, "Supporting Mobility in MosquitoNet", USENIX Winter 1996