Network-Layer Support for Mobility

Charles E. Perkins

Netcentricity Group

Sun Microsystems, Inc.

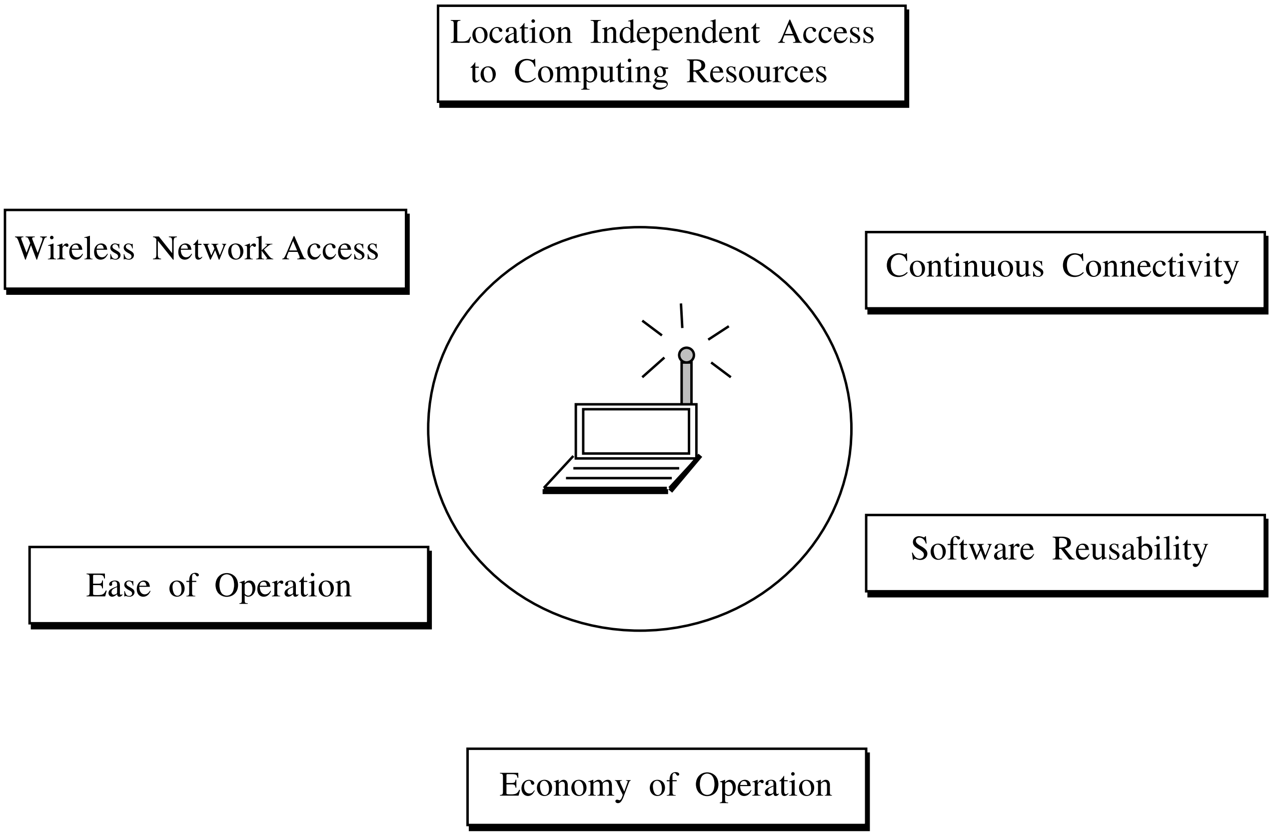
Palo Alto, CA 94303

cperkins@corp.sun.com

Outline of Presentation

- Motivation and Problem Statement
  - Why mobile networking?
  - Why Mobile-IP?
- Terminology and Entity Definition
- Protocol Overview and Detailed Description
- Route Optimization

Why Network-Layer mobility (Mobile-IP)?

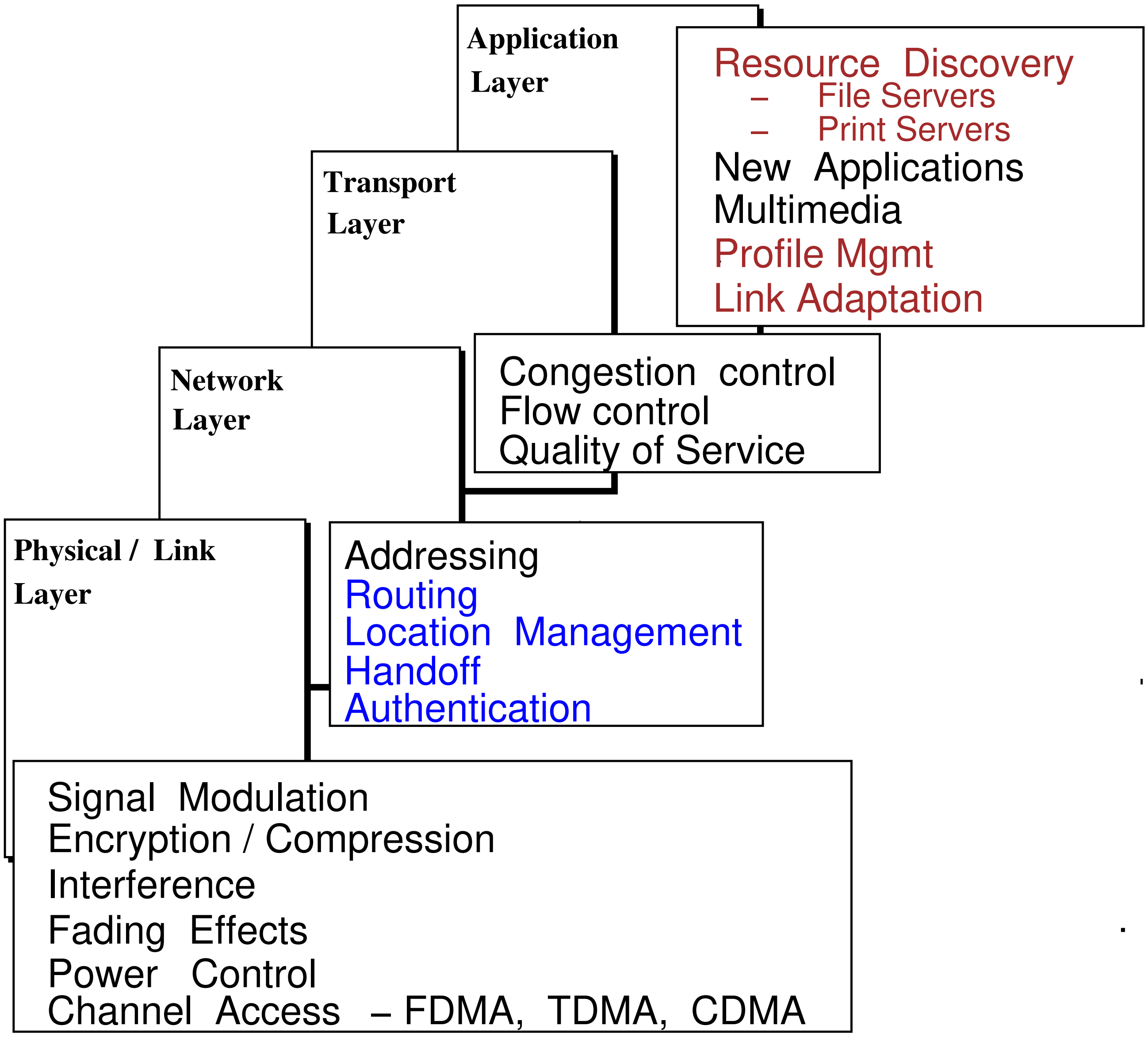


Mobility at the network layer means *application transparency*

Seamless roaming

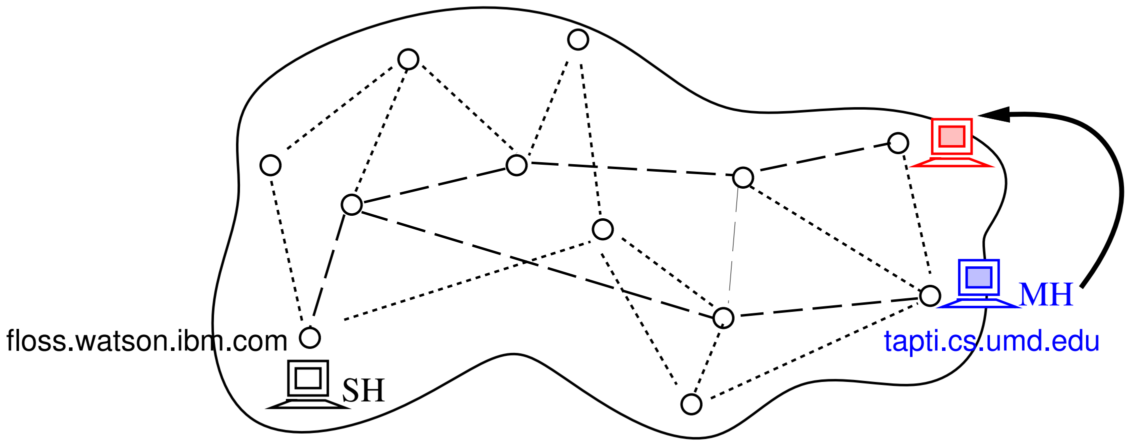
Mobile-IP can make it seem that a (possibly virtual) *home network* extends over the entire Internet.

Network Stacks vs. Nomadicity



We'll only talk about solving a few of the problems posed by nomadic computing

Connections between Internet computers



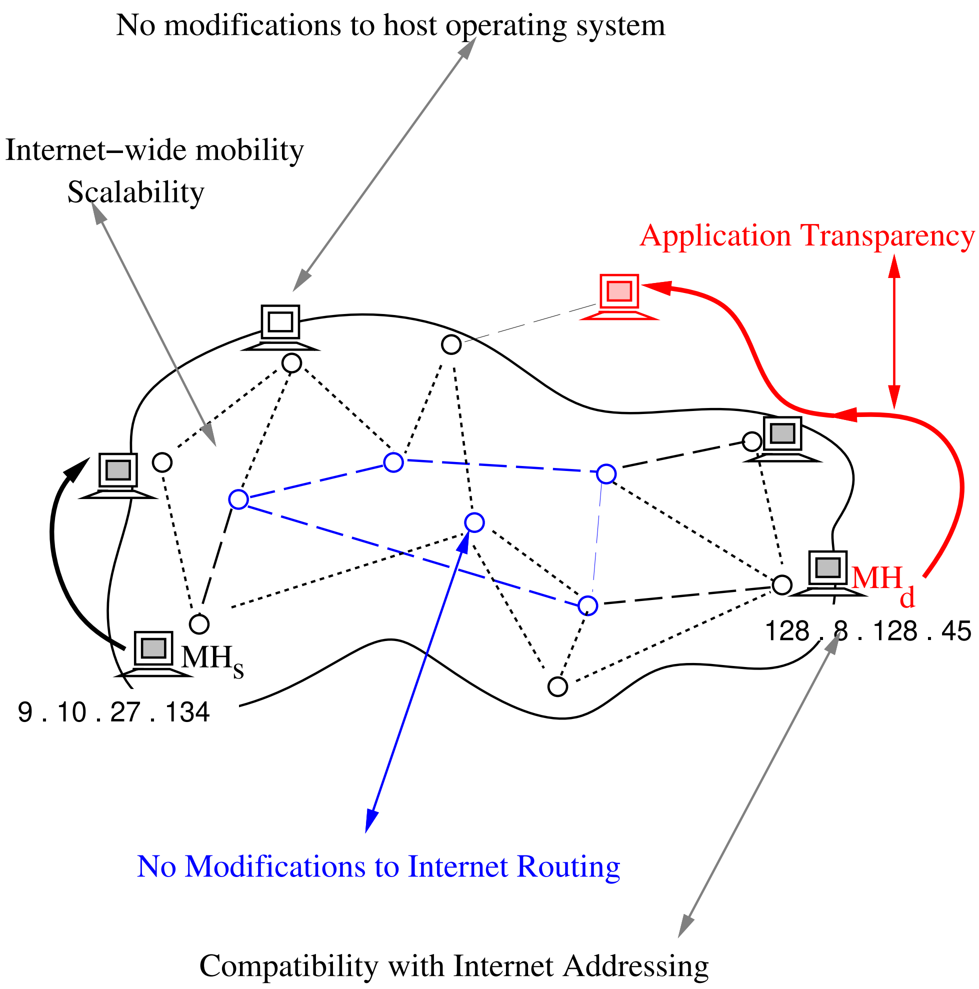
Connection := <129.34.16.43, sh_port #, 128.8.128.45, mh_port #>

,

TCP connections are defined by source and destination IP addresses and port numbers.

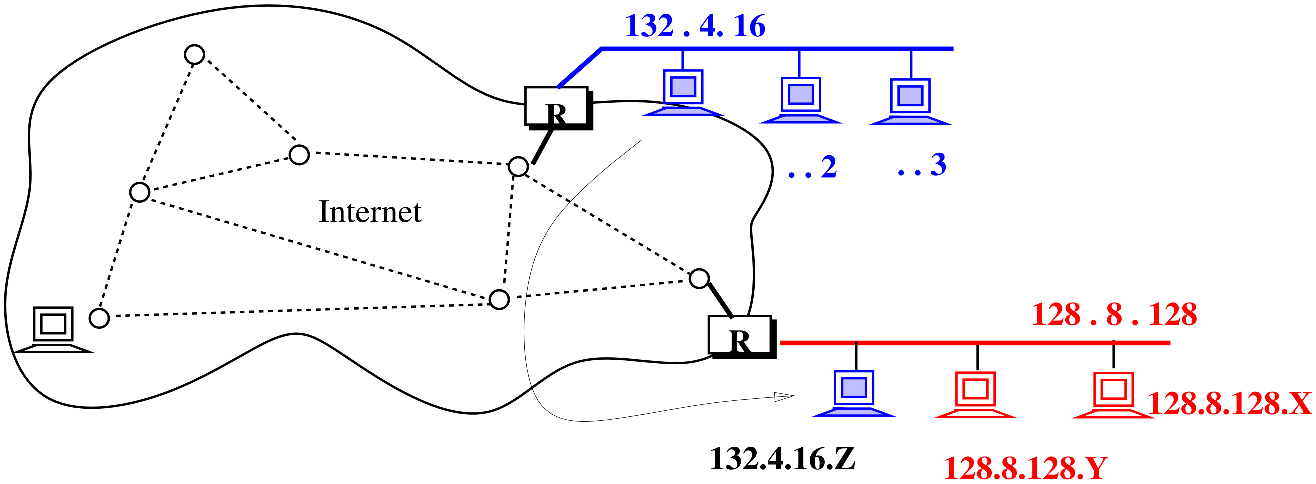
Mobile computers violate the assumption that the IP addresses define the topological relationship of the "connected" computers.

Characteristics of allowable solutions



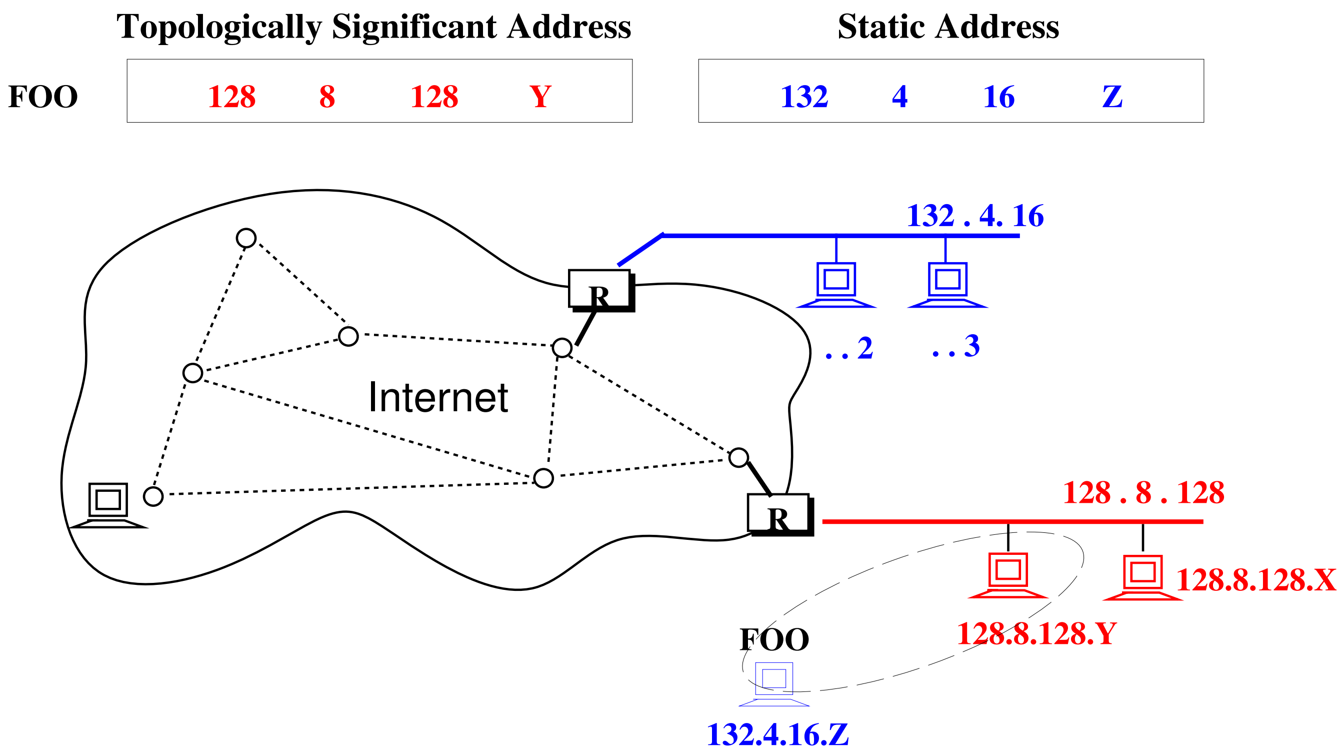
Compatibility (in all respects) with existing Internet computers, applications

IP's subnet model vs. Mobility



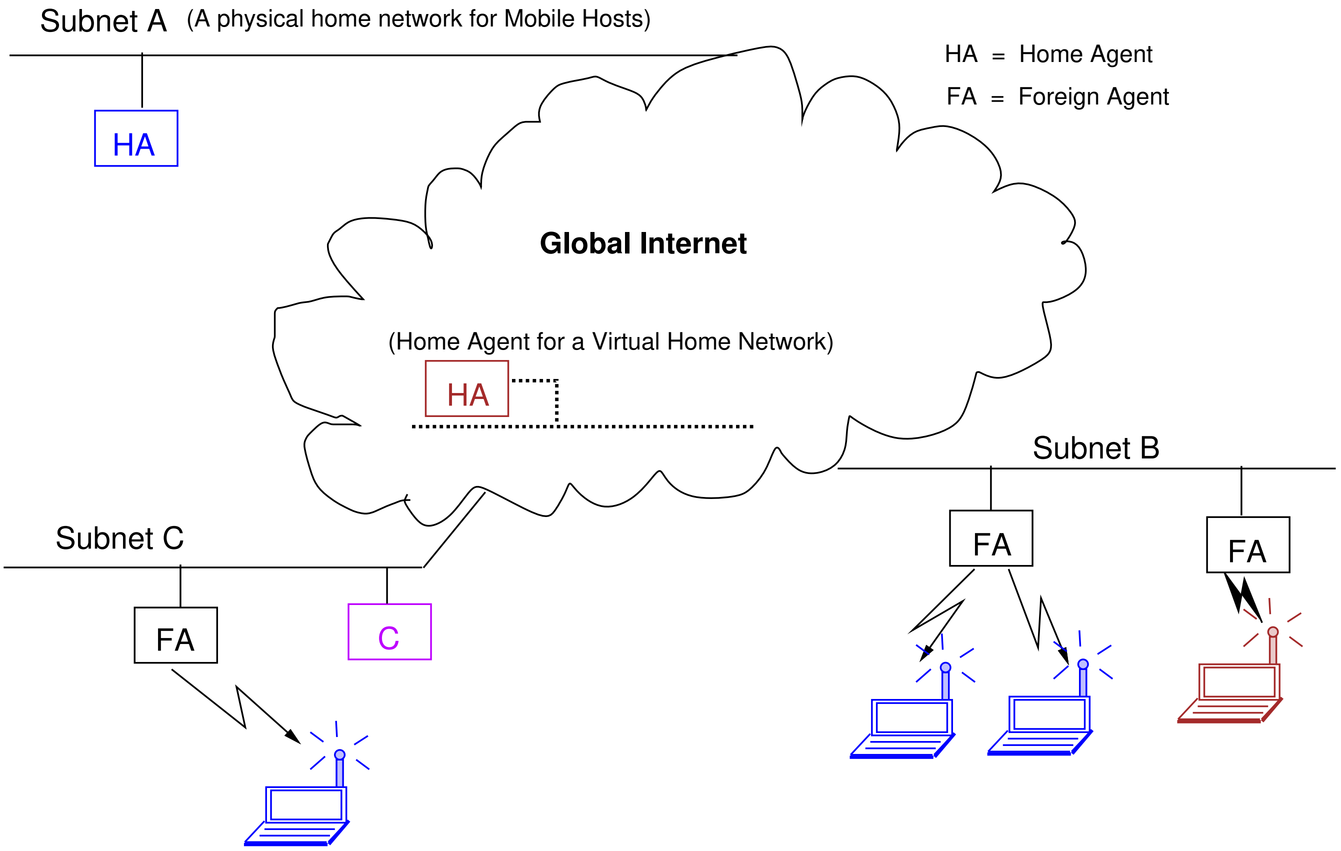
Mobile computers move from one IP subnet to another, but have the wrong "subnet prefix" for the destination subnet.

Solution: two-tier IP addressing



- The mobile computer keeps its static IP address, but borrows the service of a "care-of address" on whatever IP subnet it happens to be visiting
- This care-of address, if offered by a mobility agent at the mobile node's new point of attachment, can be used by many visiting mobile nodes

Overall Picture



The *home agent* is the router for the home network.

The *foreign agent*, located within range of a mobile client, delivers packets to that client after receiving the packets from the home agent.

Mobile-IP transforms the mobility problem into a routing problem.

No special routing is needed to send packets from a mobile client to a conventional, non-mobile node.

Service Advertisement

A *mobility agent* is either a foreign agent or a home agent

- Mobility agents send *agent advertisements*
- Care-of Addresses
- Agent solicitation
- Foreign agents can:
  - be too busy for more clients
  - describe what encapsulation they offer
  - require registration via an advertised care-of address

Assume foreign agents for now

Router Advertisement

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Num Addrs   |Addr Entry Size|           Lifetime            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Router Address[1]                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Preference Level[1]                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               .                               |
|                               .                               |
|                               .                               |
```

Type	9
Code	0
Num Addrs	number of router addresses in this message.
Addr Entry Size	2 – or, the number of 32-bit words for each router address.
Lifetime	How long (in seconds) router addresses are valid.

NOTE: the format for *Router Solicitation* (type = 10) is trivial

Advertisement Extension Format

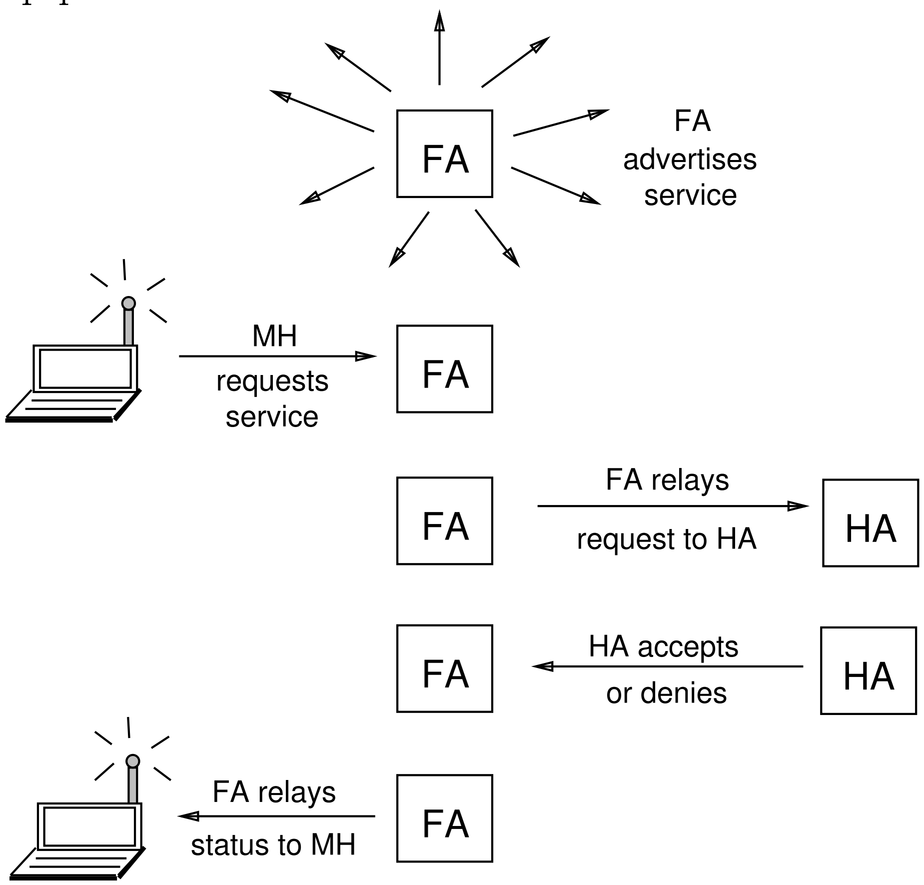
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Lifetime            |R|B|H|F|M|G|V|    reserved     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            zero or more Care-of Addresses                     |
                               ....
```

Type	16
Length	$6 + 4 \times \{$number of care-of addresses$\}$
Sequence number	The number of advertisement messages
Lifetime	
R	Foreign agent registration required
B	Busy bit. Only valid if F=1.
H	Home agent
F	Foreign agent
M	Minimal encapsulation
G	GRE encapsulation
V	Van Jacobson header compression
Care of Address	

Sequence number rollover: 65535 is followed by 256

Registration

A four-step process



A *binding* is the tuple (mobile, care-of address, lifetime)

Registration means updating the binding

Registration is a form of *remote redirect*; authentication required for safety

Choosing UDP for Mobility Messages

UDP (User Datagram Protocol) is the "no frills" choice

- Simpler than ICMP for user processes
- TCP unnecessary
- UDP checksum expected
- Port numbers variable and unauthenticated
- Well-known port 434

Using RFC1256 ICMP Router Advertisement should be reconsidered

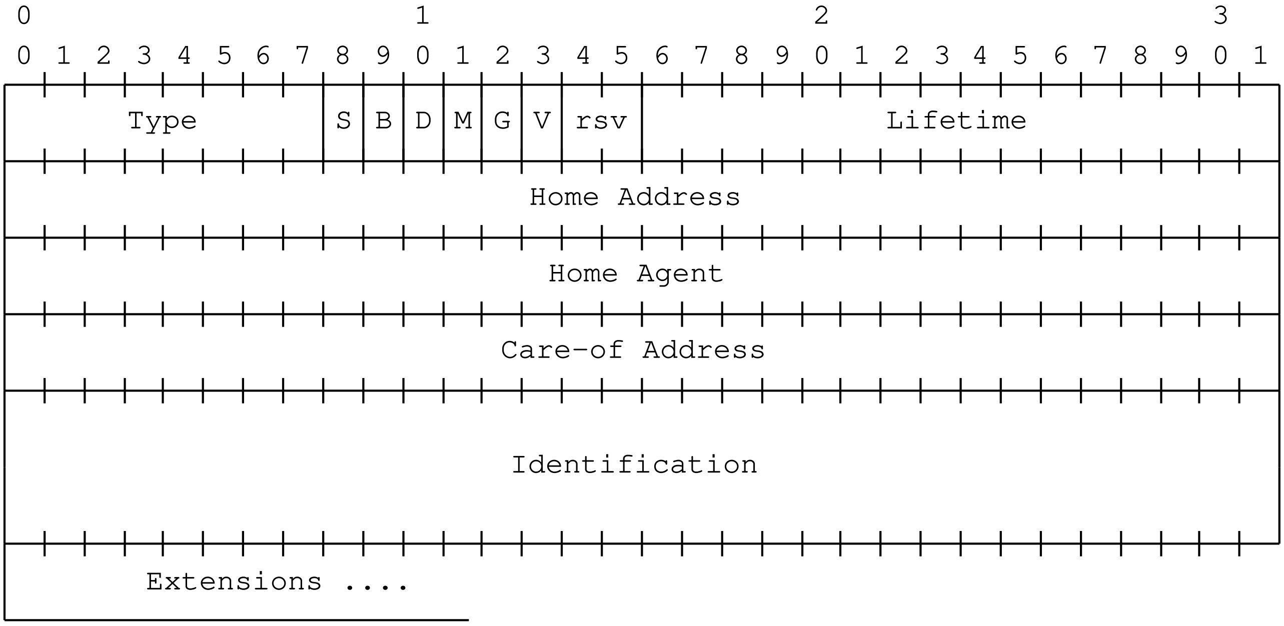
General Mobile IP Registration Message Format

IP header fields	UDP header	Mobile IP message header	Extensions .....

After the IP and UDP header, the registration message header is found, then any necessary extensions, always including an *authentication* extension.

Registration Request Message Format

The UDP header is followed by the Mobile-IP fields shown below:



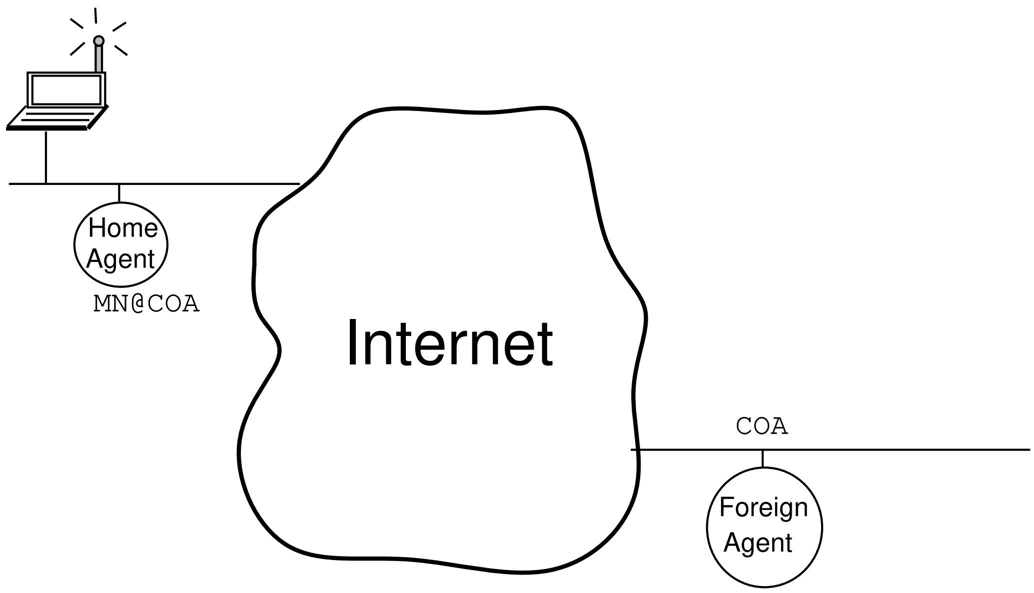
Type	1
Lifetime	
Home Address	The IP address of the mobile node.
Home Agent	The IP address of a home agent.
Care-of Address	The IP address for the end of a tunnel.
Identification	64-bit identification and replay protection

Registration Request Message Flags

Optional registration features can be requested by setting bits in the *flags* field

S	Simultaneous Registrations
B	Broadcasts Requested
D	Dynamic Care-of Address
M	Minimal Encapsulation
G	GRE encapsulation
V	Van Jacobson Header Compression

Deregistration Procedures



- Sends Registration Request with Lifetime = 0, COA = HA
- If authentication fails, HA *MUST NOT* resynchronize
- For safety, when mobile node reboots on home network it *SHOULD* issue gratuitous ARPs.

Authentication Extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |         SPI  .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      .... SPI (continued)      |      Authenticator  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The fields defined as follows:

Type	32 Mobile-Home Authentication extension 33 Mobile-Foreign Authentication extension 34 Foreign-Home Authentication extension
Length	4 plus the number of bytes in the authenticator.
SPI	Security Parameters Index (4 bytes). An opaque identifier
Authenticator	(variable length, depending upon the SPI)

Registration Reply

The UDP header is followed by the Mobile-IP fields shown below:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Lifetime            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Home Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Home Agent                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Identification                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Extensions .....
+-+-+-+-+-+-+-+-+-+-+
```

Type	3
Code	The status of the registration request
Lifetime	
Home Address	Mobile node's IP address
Home Agent	Home agent's IP address
Identification	As in registration request

Registration Status Codes

0 registration accepted

1 registration accepted; simultaneous mobility bindings unsupported

Service denied by the foreign agent:

64 reason unspecified

65 administratively prohibited

66 insufficient resources

67 mobile node failed authentication

68 home agent failed authentication

69 requested lifetime too long

70 poorly formed request (i.e., reserved bits nonzero)

71 poorly formed reply

80 home network unreachable (ICMP error)

81 home agent host unreachable (ICMP error)

82 home agent port unreachable (ICMP error)

88 home agent unreachable (other ICMP error)

More Registration Status Codes

Service denied by the home agent:

128 reason unspecified

129 administratively prohibited

130 insufficient resources

131 mobile node failed authentication

132 foreign agent failed authentication

133 identification mismatch

134 poorly formed request (i.e., reserved bits nonzero)

135 too many simultaneous mobility bindings

136 unknown home agent address

Rejection messages contain the address of the home agent issuing the rejection.

Up-to-date values of the Code field are specified in the most recent *Assigned Numbers* (RFC 2000).

Tunneling

Home agent *tunnels* (encapsulates) packets to care-of address

Tunnel destination is the care-of address.

Tunnel source is the home agent's address.

Original source and destination placed *after* the tunnel IP header

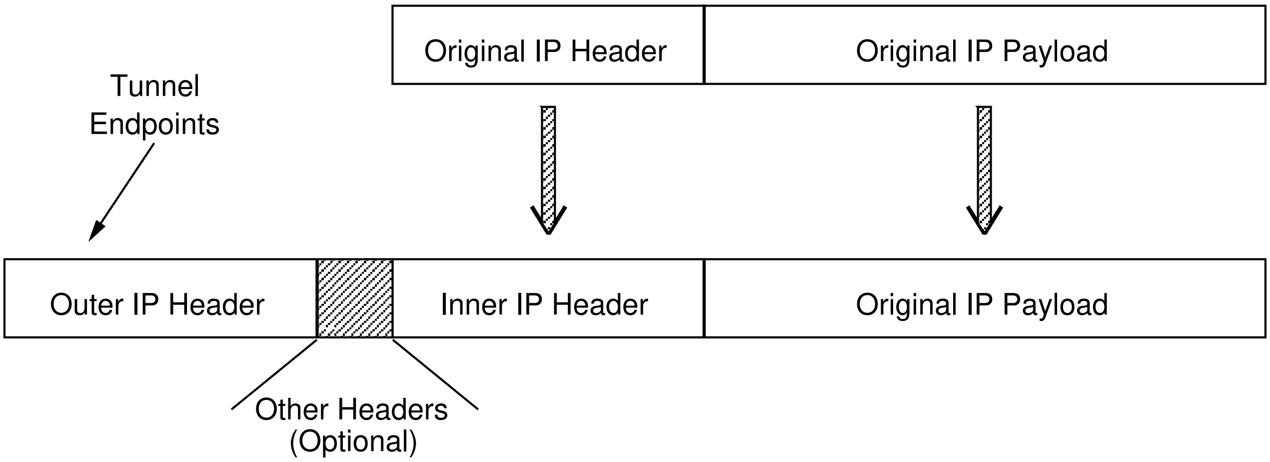
Three methods are available:

- IP-within-IP (default – *must* be supported)
- *minimal* encapsulation
- GRE (type-length-value)

Home agent can maintain tunnel soft state, and return ICMP errors without encapsulating the packet

- MTU of the tunnel
- Hop Limit (path length) of the tunnel
- Reachability of the end of the tunnel

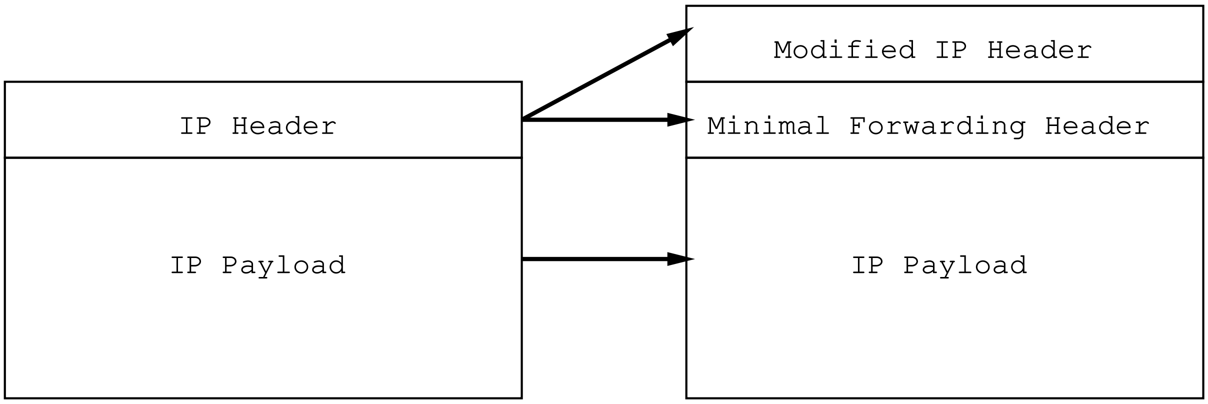
IP within IP



Handles incoming fragmentation

New IP Header uses protocol number 4

Minimal Encapsulation Format



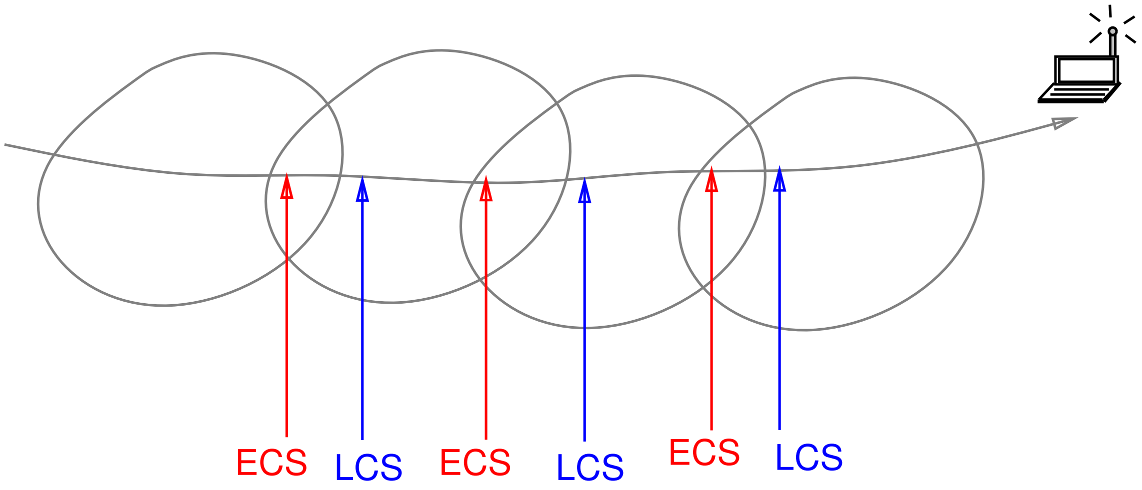
Minimal Encapsulation inserts a minimal forwarding header between the new tunnel IP header and the payload. The minimal forwarding header has the following format:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Protocol   |S|  reserved   |        Header Checksum        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                   Original Source Address                     :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Original Destination Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Protocol	Original IP header protocol number
S	Set if the Original Source Address is present

The new IP Header uses protocol number 55

Algorithms for Motion Detection

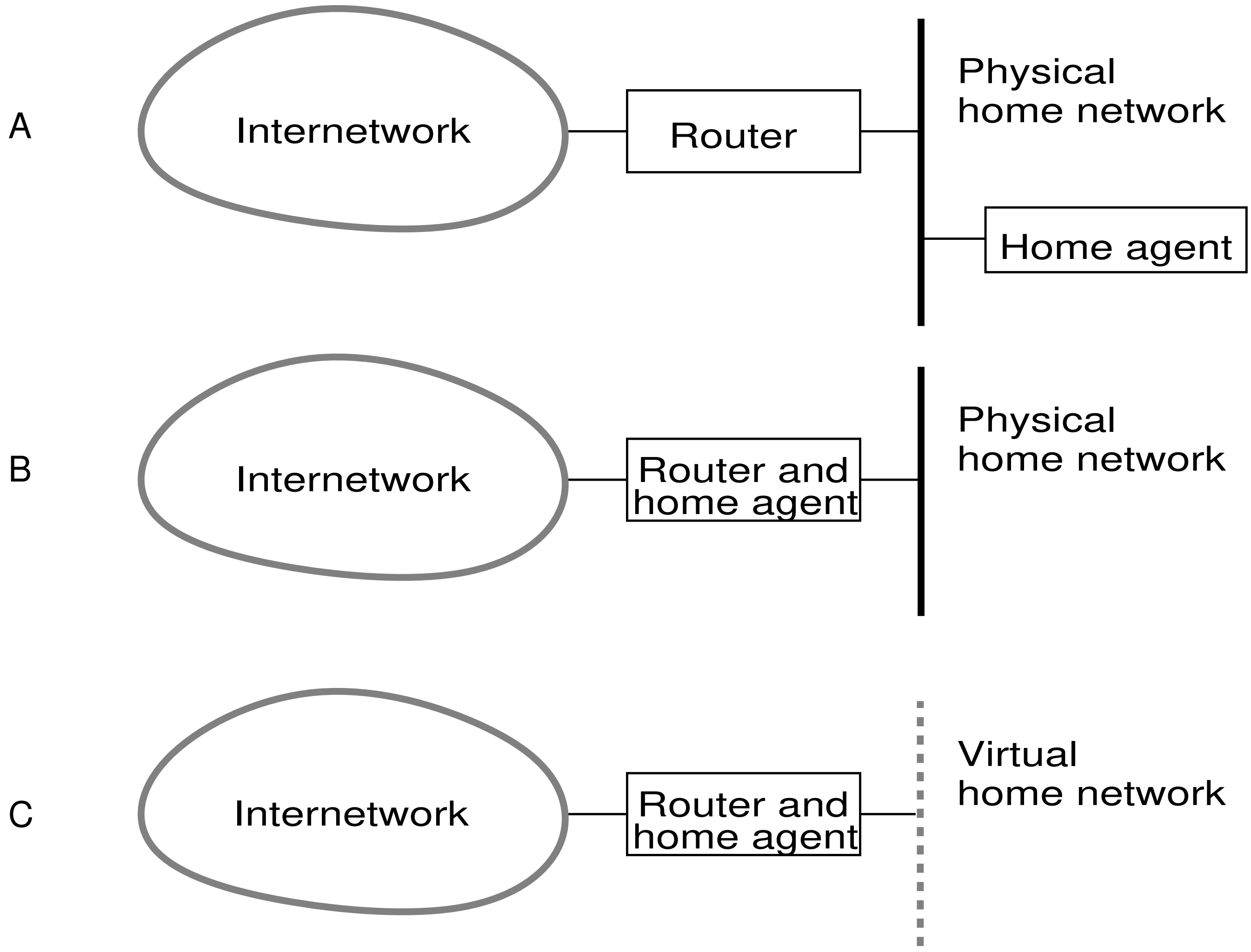


- Lazy Cell Switching (LCS) (switch on BLUE)
- Eager Cell Switching (ECS) (switch on RED)
- Prefix Comparison (switch on RED) (requires more subnets)
- Link-Layer notification (can include signal-strength, etc.)

Performance depends upon pattern of user mobility, frequency of advertisement, and whether mobile node can respond to multiple IP addresses

LCS can outperform ECS if used in conjunction with signal strength measurement

Home Networks



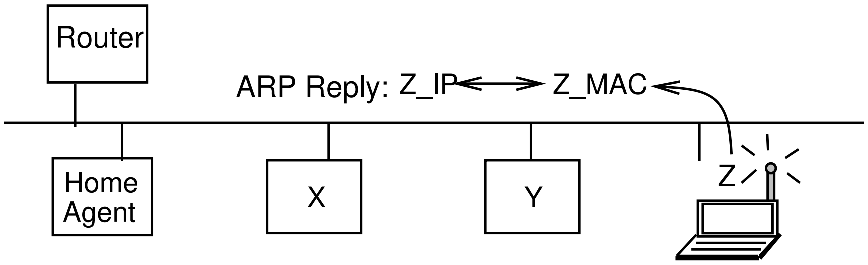
A. Home Agent as a separate system on Home Network

B. Home Agent included with a router to the Home Network

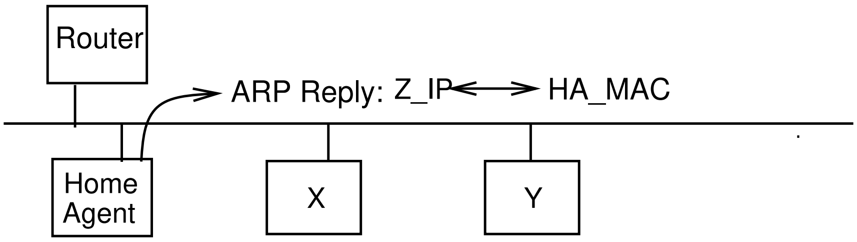
C. A *virtual* Home Network

Real Home Networks need to use *Gratuitous ARP*

Effect of Gratuitous ARP



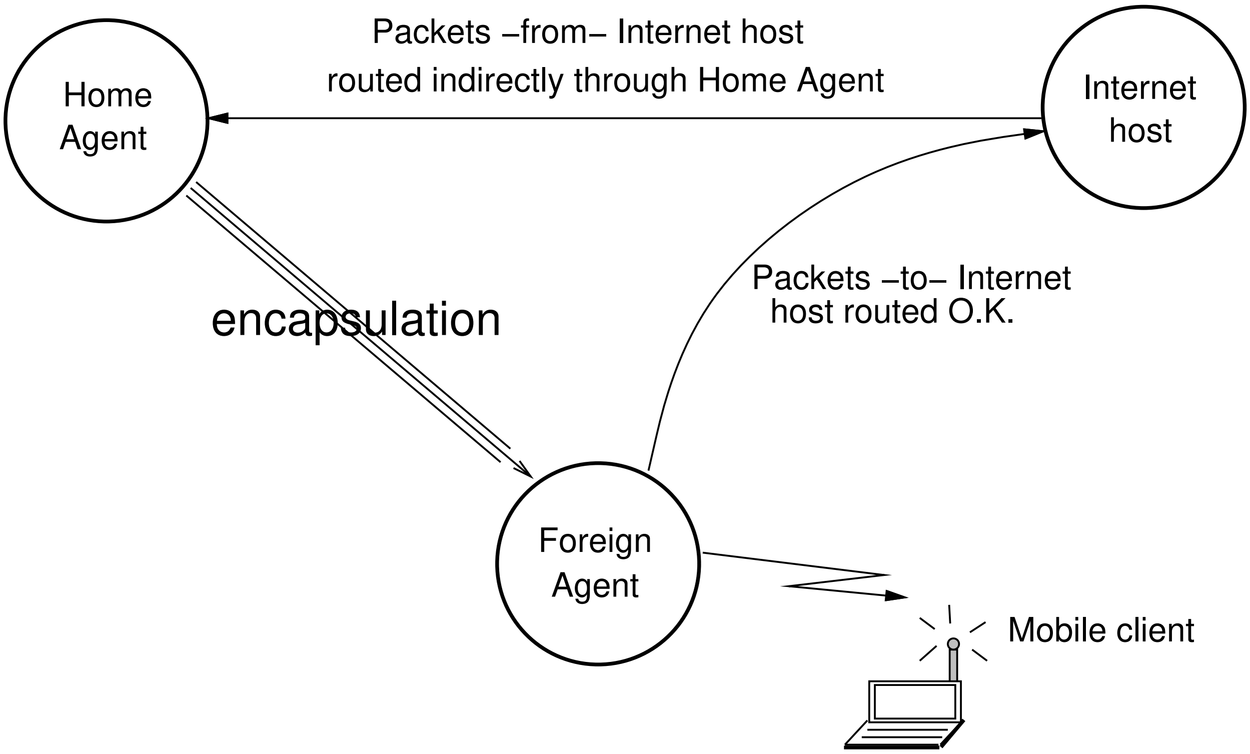
(a)



(b)

- In figure (a), mobile node Z is attached to its home network, and naturally answers ARP Requests. The router, home agent, and nodes X and Y all associate Z's IP address with its MAC address `Z_MAC`.
- In figure (b), mobile node Z is roaming, and the Home Agent has broadcast an ARP Reply indicated that Z's MAC address is `HA_MAC`. Until Z returns home, the home agent will continue to *proxy ARP* for Z.

Triangle (Non-Optimal) Routing



Triangle routing is undesirable:

- Home Agent bottleneck
- Increased network utilization
- Increased sensitivity to network partition

Route Optimization

Current solution requires modified correspondent, and security associations with home agents

Idea: Allow correspondent hosts to know the care-of address of the mobile node – i.e, to get a *binding update*.

Location cache, part of route table

Main ideas:

- Get *bindings* to the correspondent nodes that need them
- Allow *smooth updates* from one foreign agent to another
- Provide *registration keys* for the latter operation
- Define *special tunnels* for additional robustness

Binding Cache Maintenance

Four UDP message types:

- Binding Warning
- Binding Request
- Binding Update
- Binding Acknowledge

When a mobility agent sees that a correspondent host has a stale location cache, it issues a *Binding Warning*. The correspondent then makes a *Binding Request*, which elicits a *Binding Update*. The update may be acknowledged with a *Binding Acknowledge*.

Binding Update

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |A|I|M|G|Reserved|           Lifetime            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Mobile Node Home Address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Care-of Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Identification                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	18
A	requests a Binding Acknowledge message
I	indicates whether Identification is present
M, G	identify allowable encapsulation
Lifetime	
Home Address	
Care-of Address	
Identification	

- *MUST* be authenticated with *route optimization authentication* extension
- Set care-of address equal to the home address to delete mobile node's existing location cache entry and/or visitor list entry

Route Optimization Extensions

Route Optimization defines the following Mobile IP message extensions:

35 = Route Optimization Authentication Extension

96 = Previous Foreign Agent Notification extension

113 = Foreign Agent Key Request Extension

114 = Mobile Node Public Key Extension

115 = Foreign Agent Public Key Extension

116 = Registration Key Request Extension

120 = Home-Mobile Key Reply Extension

121 = Foreign Agent Key Reply Extension

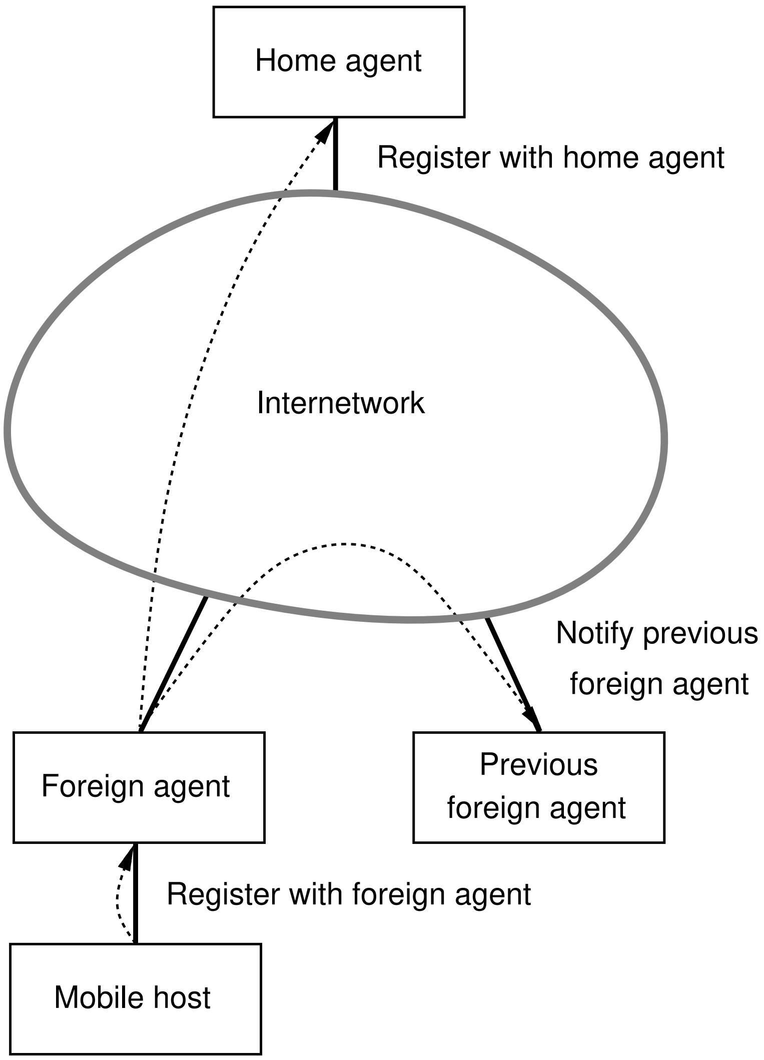
122 = Mobile Node Public Key Reply Extension

123 = Foreign Agent Public Key Reply Extension

124 = Diffie-Hellman Key Reply Extension

128 = Key Establishment Failure Extension

Smooth Handoffs



Smooth handoffs use binding updates, too.

- Mobile uses the *Previous Foreign Agent Notification Extension* to ask the new foreign agent to *relay* its binding update to its previous foreign agent

Previous Foreign Agent Notification Extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |        Cache Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Previous Foreign Agent Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     New Care-of Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             SPI                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Authenticator ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- The new foreign agent uses the information to create a *binding update* for the previous foreign agent.
- In this case, the binding update does *not* have to contain the identification field.

Special Tunnels

- Suppose a foreign agent decapsulates but cannot forward a datagram
- It *MAY* then *tunnel* the datagram back to the destination address.
- The outer (*encapsulating*) source IP address is set to its *care-of address*
- A home agent receiving the special tunnel *MAY* decapsulate.
- A home agent receiving the special tunnel *MUST* check to make sure that the binding for the mobile node does NOT show a care-of address equal to the tunnel source before forwarding.

Miscellaneous Topics

Multiple Home Agents

Security Parameter Index

MD5 (Message Digest 5: RFC 1321)

Nonces vs. Timestamps in Authentication

TCP congestion control vs. error-prone media

Discovering Home Agent addresses

Simultaneous Registrations

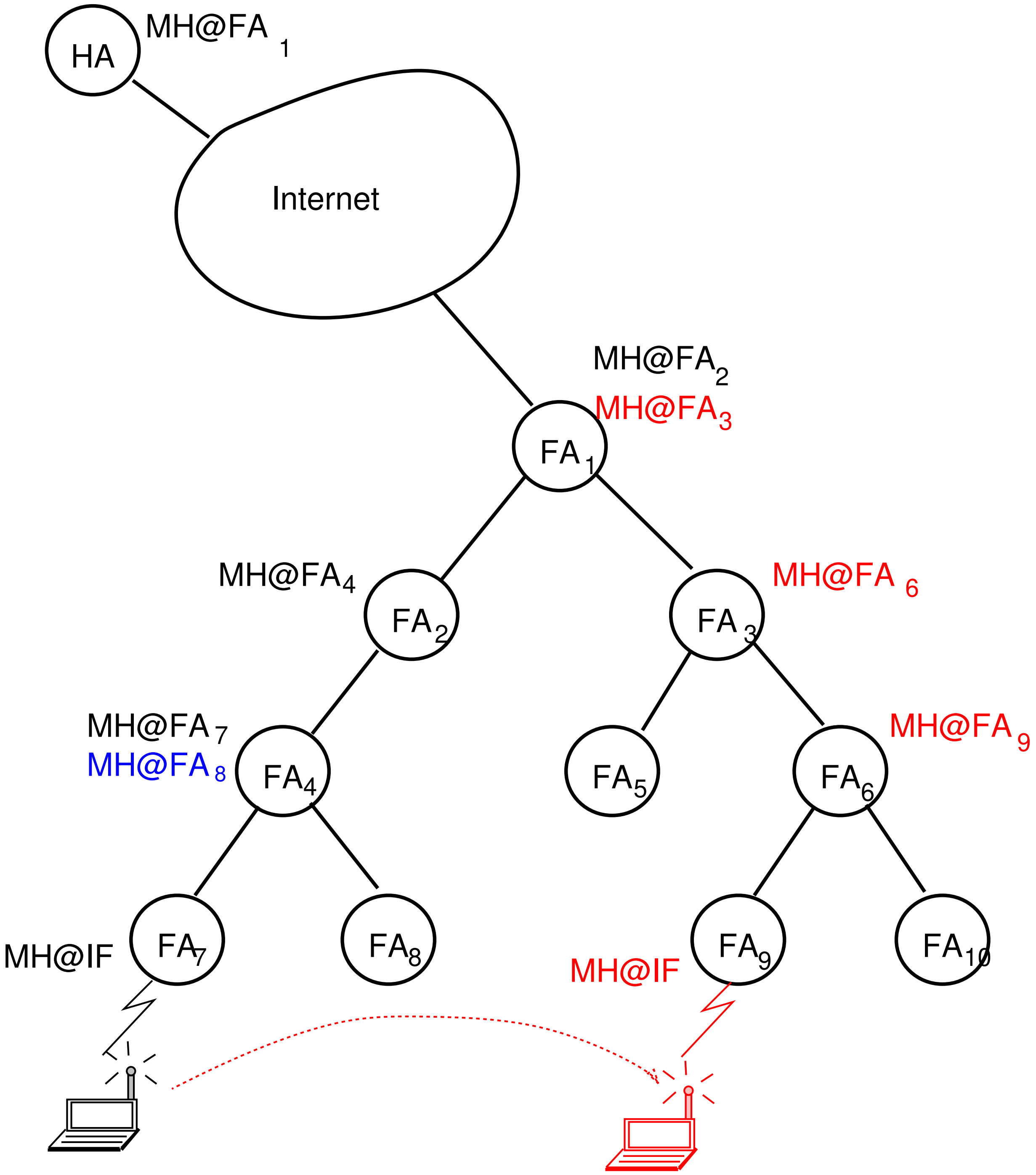
Broadcast and Multicast preferences

Foreign Agent hierarchies

New PPP extension

Firewalls and *ingress filtering*

Hierarchical Foreign Agents/Regional Registration



Idea: make Registration Requests go only as far as needed up a hierarchy of Foreign Agents

- Security needs careful attention
  - Establish session key, as outlined in Route Optimization
- Each ancestral foreign agent considers the mobile node to be registered at foreign agent just below it in the hierarchy
- Registration Requests passed from level to level
- Likewise for Registration Replies
- Agent Advertisements show complete regional hierarchy of foreign agents that are cooperating
- Can even allow use of "co-located" care-of addresses, once a cooperating foreign agent has been found

Freeware

- http://anchor.cs.binhampton.edu/ mobileip (Linux MH and "agent")
- http://kth.edu.se/it.kth.se/ klemets ("MINT")
- University of Singapore
- http://cs.columbia.edu/ ji
- http://cs.cmu.edu/ dbj ("MONARCH")

Mobile IP mailing list:

to join:	`mobile-ip-request@SmallWorks.com`
to contribute:	`mobile-ip@SmallWorks.com`