Mobile IP

Mukesh Chinta, Asst Prof, CSE

Introduction

- In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to the fixed address on the envelope. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network.

- The problem occurs when a device roams away from its home network and is no longer reachable using normal IP routing. This results in the active sessions of the device being terminated. Mobile IP was created to enable users to keep the same IP address while traveling to a different network (which may even be on a different wireless operator), thus ensuring that a roaming individual could continue communication without sessions or connections being dropped.

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

Mobile IP

- Mobile IP' signifies that, while a user is connected to applications across the Internet and the user's point of attachment changes dynamically, all connections are maintained despite the change in underlying network properties
- Similar to the handoff/roaming situation in cellular network
- Mobile IP allows the mobile node to use two IP addresses called home address and care of address
- The home address is static and known to everybody as the identity of the host
- The care of address changes at each new point of attachment and can be thought of as the mobile node's location specific address

Mobile IP Terminology

Mobile Node (MN)

system (node) that can change the point of connection to the network without changing its IP address

Home Agent (HA)

router in the home network of the MN, which registers the location of the MN, tunnels IP datagrams to the COA when MN is away from home.

Foreign Agent (FA)

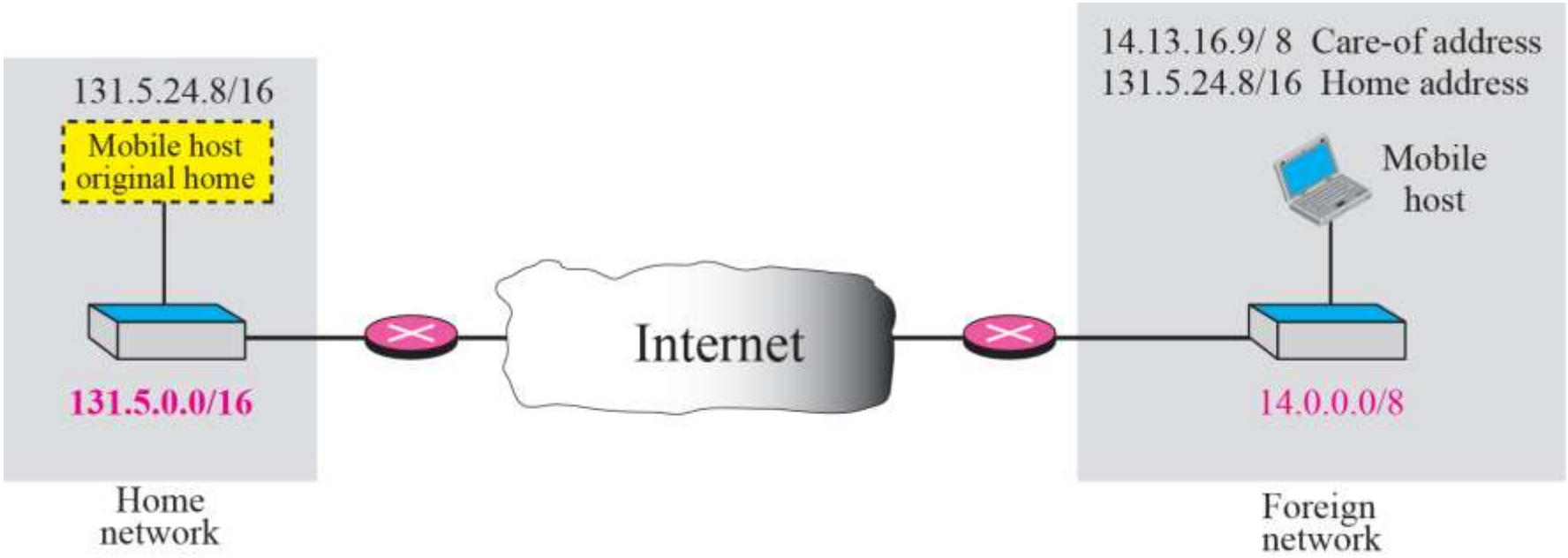
router in the current visited network of the MN, which forwards the tunneled datagrams to the MN, also acts as the default router for the registered MN

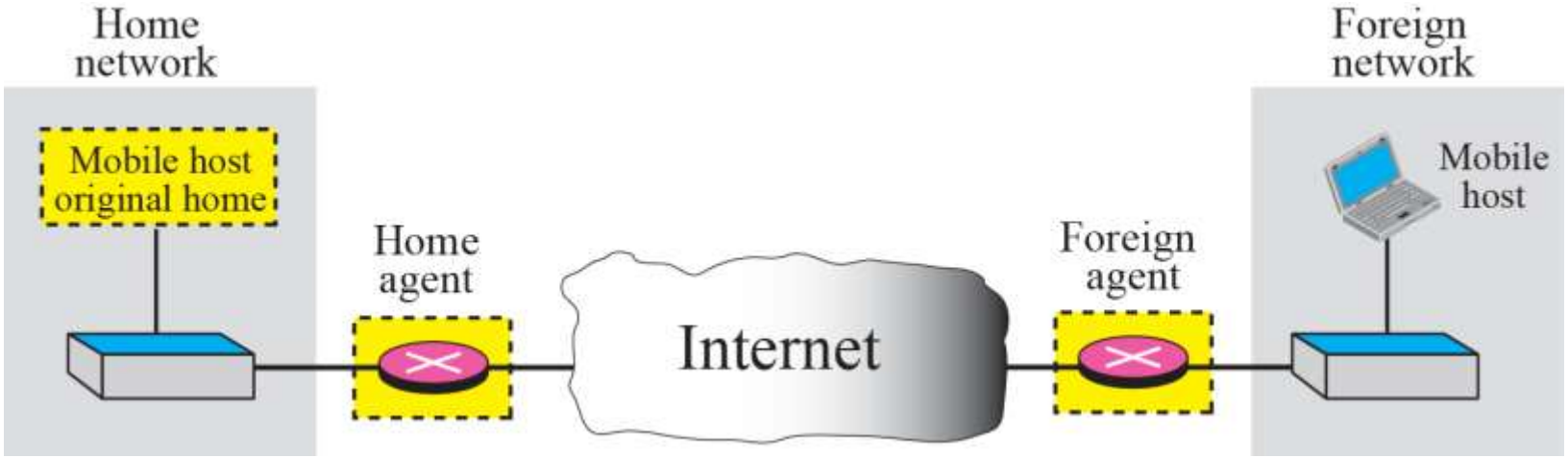
Care-of Address (COA)

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

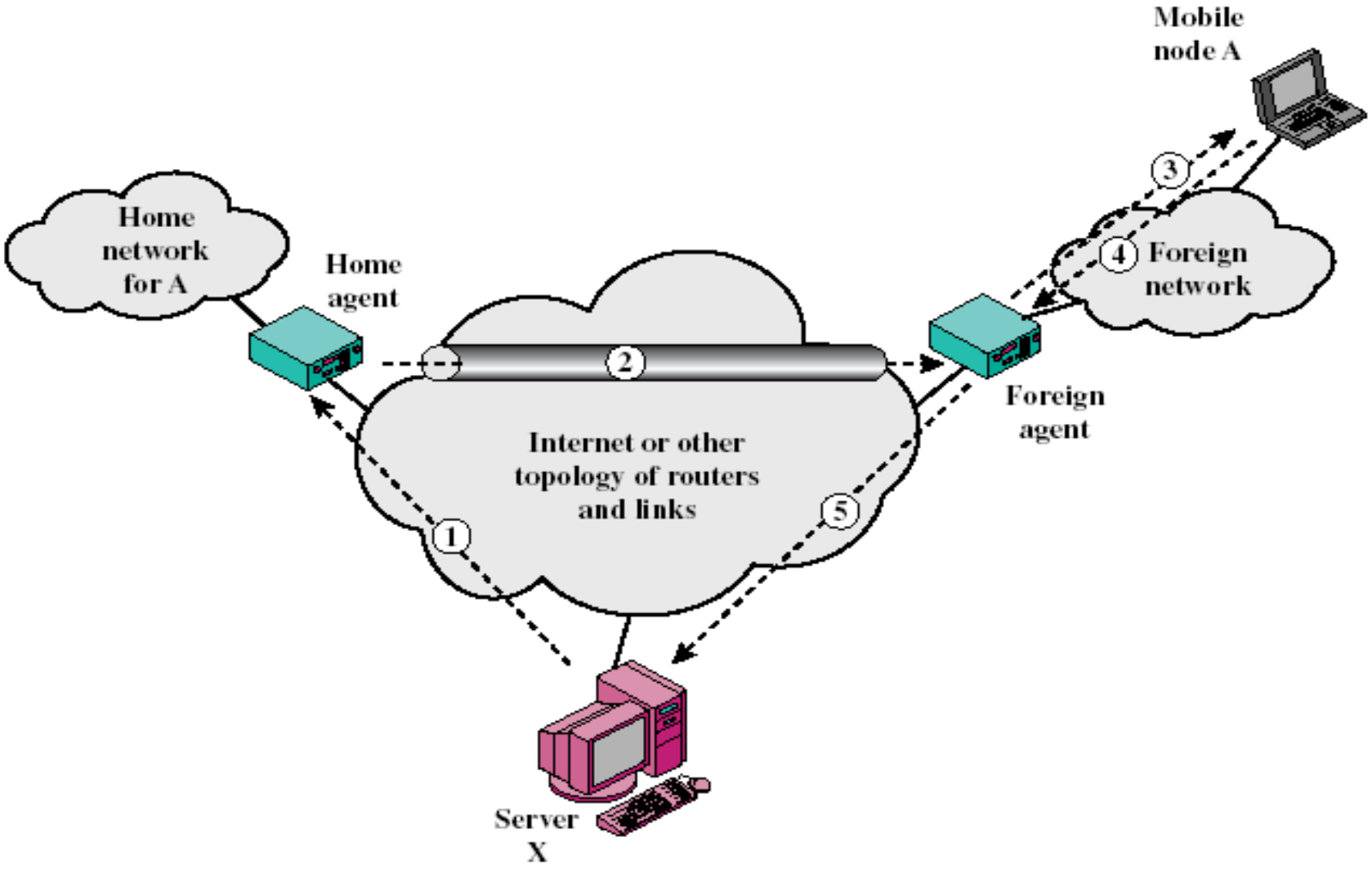
Correspondent Node (CN)

communication partner


131.5.24.8/16
Mobile host original home
131.5.0.0/16
Home network
Internet
14.13.16.9/ 8 Care-of address
131.5.24.8/16 Home address
Mobile host
14.0.0.0/8
Foreign network


Home network
Mobile host original home
Home agent
Internet
Foreign agent
Foreign network
Mobile host

Mobile IP


Mobile
node A
3
Home
network
for A
Home
agent
4
Foreign
network
2
Foreign
agent
Internet or other
topology of routers
and links
1
5
Server
X

Working of Mobile IP

Let's take the case of mobile node (A) and another host (server X). The following steps take place:

- Server X wants to transmit an IP datagram to node A. The home address of A is advertised and known to X. X does not know whether A is in the home network or somewhere else. Therefore, X sends the packet to A with A's home address as the destination IP address in the IP header. The IP datagram is routed to A's home network.
- At the A's home network, the incoming IP datagram is intercepted by the home agent. The home agent discovers that A is in a foreign network. A care of address has been allocated to A by this foreign network and available with the home agent. The home agent encapsulates the entire datagram inside a new IP datagram, with A's care of address in the IP header. This new datagram with the care of address as the destination address is retransmitted by the home agent.
- At the foreign network, the incoming IP datagram is intercepted by the foreign agent. The foreign agent is the counterpart of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to A.

Working of Mobile IP

- A intends to respond to this message and sends traffic to X. In this example, X is not mobile; therefore X has a fixed IP address. For routing A's IP datagram to X, each datagram is sent to some router in the foreign network. Typically, this router is the foreign agent. A uses X's IP static address as the destination address in the IP header.
- The IP datagram from A to X travels directly across the network, using X's IP address as the destination address.

- Discovery - A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- Registration - A mobile node uses a registration procedure to inform its home agent of its care-of address.
- Tunneling - Tunneling procedure is used to forward IP datagrams from a home address to a care of address.

Discovery

- **Extension of ICMP Router Advertisement**
- **Home agents and foreign agents broadcast agent advertisements at regular intervals**
- **Mobile IP uses control messages that are sent to and from UDP port 334.**
  - **Agent advertisement**
    - **Allows for the detection of mobility agents**
    - **Lists one or more available care-of addresses**
    - **Informs the mobile node about special features**
    - **Mobile node selects its care-of address**
    - **Mobile node checks whether the agent is a home agent or foreign agent**
- MNs can solicit for agents if they have not heard an agent advertisement in awhile or use some other mechanism to obtain a COA or temp. IP address (e.g. DHCP).
- MNs know they are home when they recognize their HA

Registration

Registration: used by a MN to inform the FA that it is visiting.

- The new care of address of the MN is sent to the HA.
- Registration expires, duration is negotiated during registration. Mobile must re-register before it expires
- All registrations are authenticated
- The MN sends a registration request in to the FA which passes it along to the home agent. The HA responds to the FA which then informs the MN that all is in order and registration is complete.

Authentication

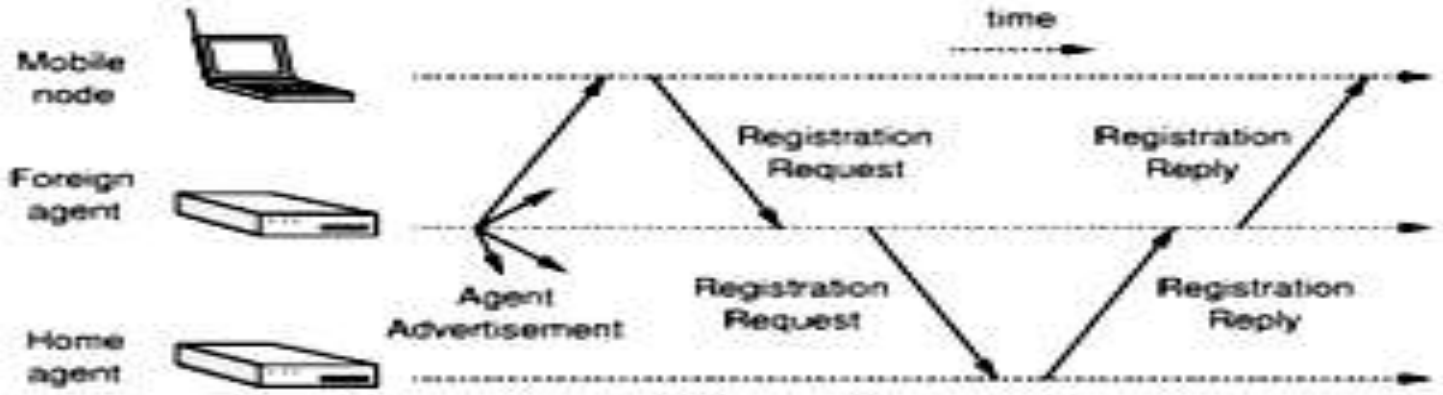
- The MN needs to be authenticated. Each MN, FA & HA support a mobility Security Association (SA) for mobile entities indexed by their Security Parameters Index (SPI) & IP address.
- Registration messages between a MN & its HA must be authenticated with an authorization enabling exchange called Mobile- Home Authentication Extension.
- Using 128-bit secret-key shared between MN & HA and HMAC-MD5 hashing algorithm, a digital signature is generated, which allows the agent to authenticate the MN
- At the end of registration, a triplet containing the HA address, COA & registration life time is maintained in the HA. This is called a binding for the MN. The HA maintains this association until the registration life expires.

Registration

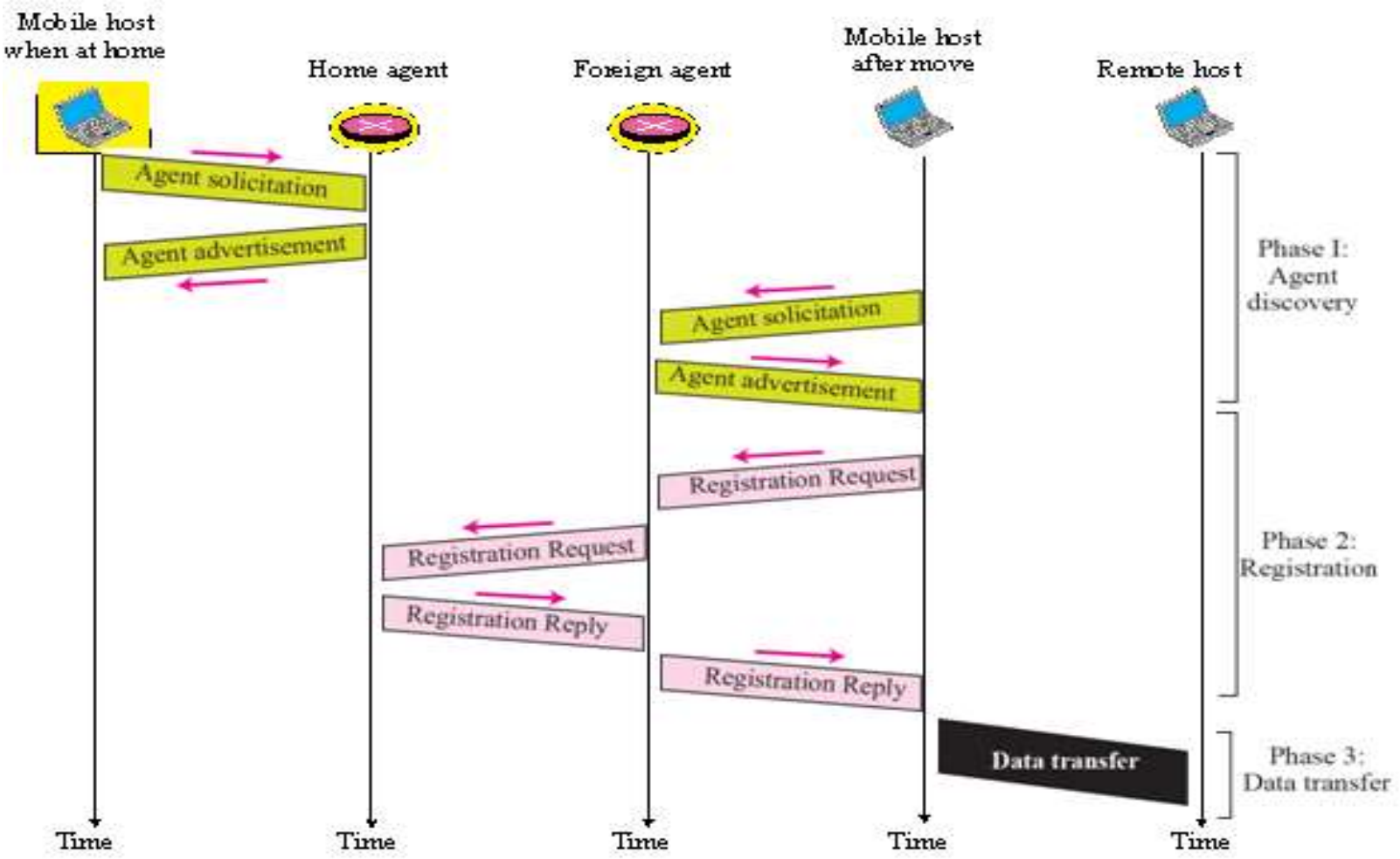
The MN may act as its own FA by using a co-located COA.

A co-located COA is an IP address obtained by the mobile node that is associated with the foreign network.

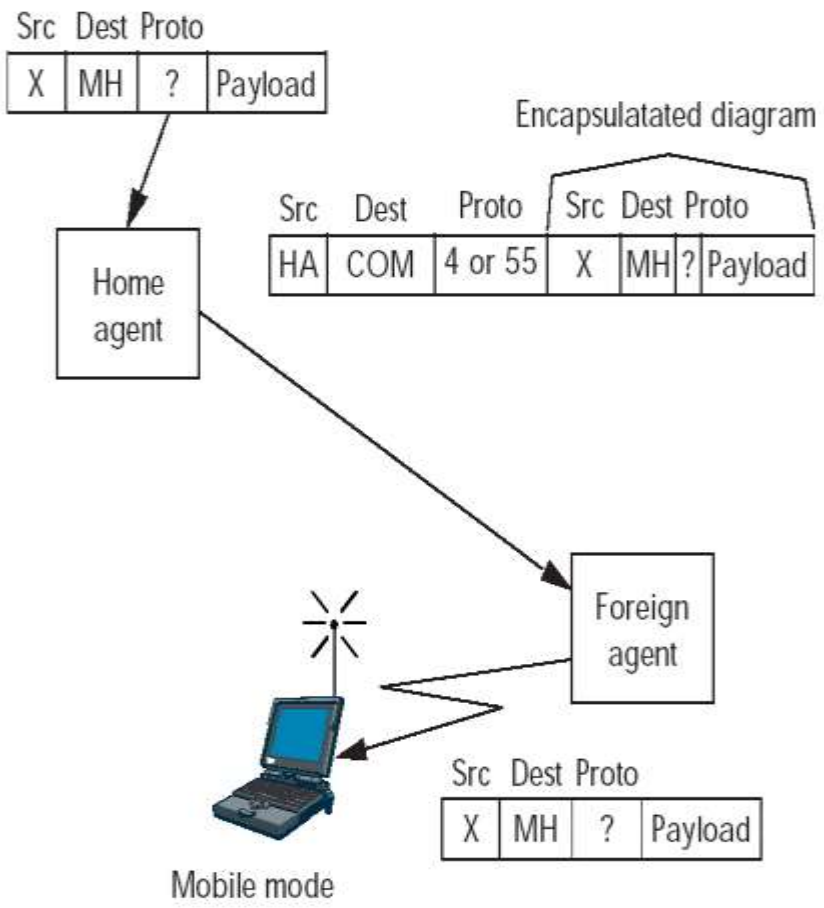
If MN is using a co-located COA, then the registration happens directly with the HA



Remote host and mobile host configuration

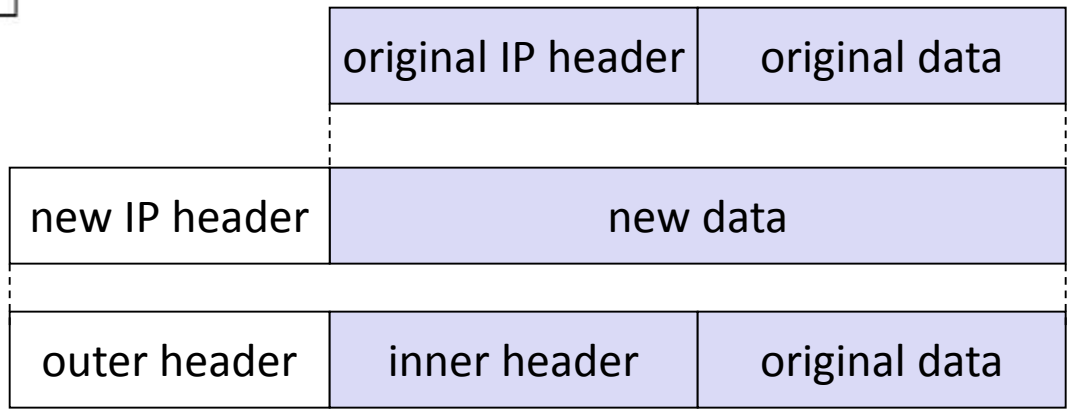


Tunnelling



Routing/Encapsulation/Tunneling: consists of the delivery of the packets to the mobile node at its current care of address.

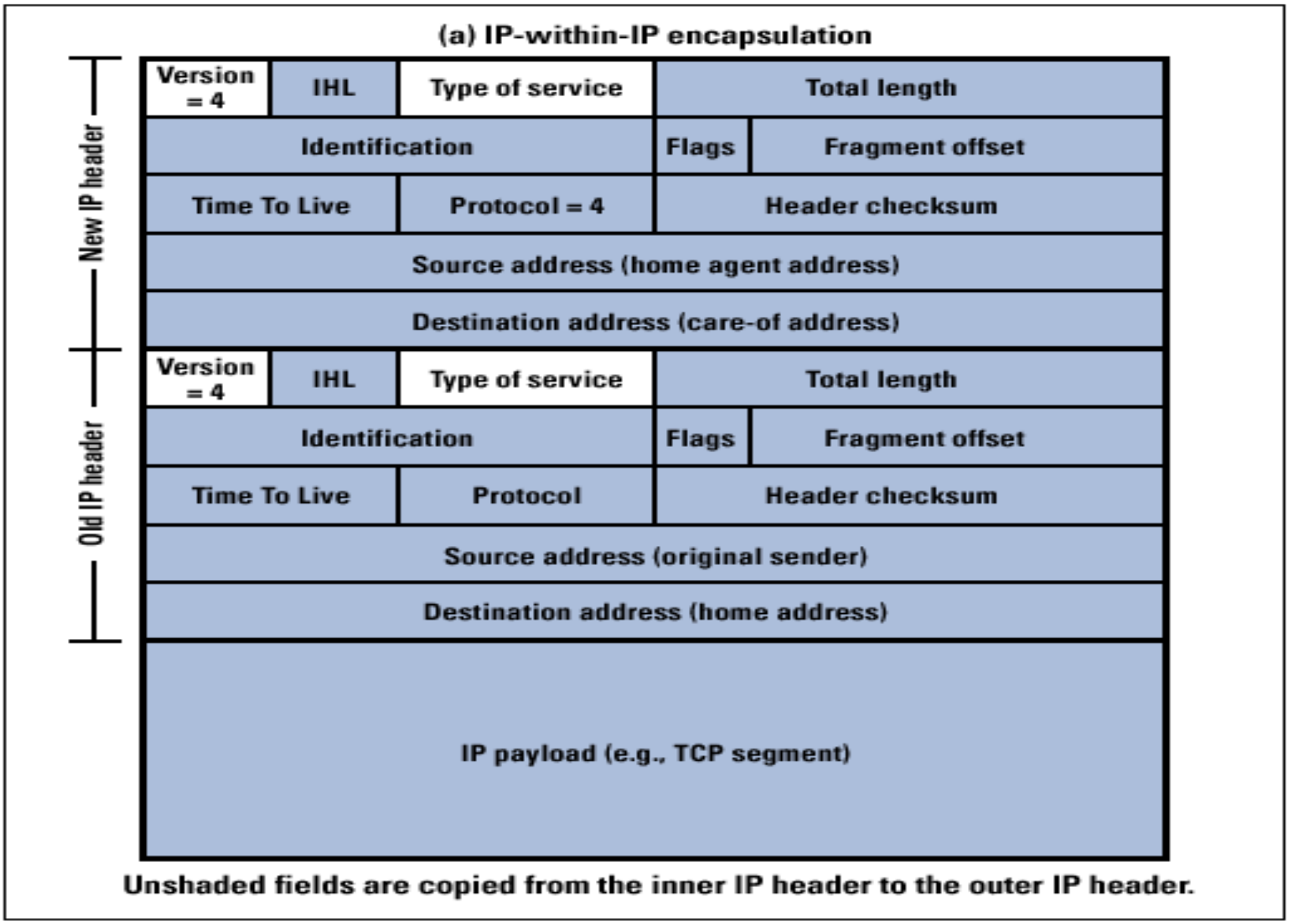
- Sender does not need to know that the destination is a MN.
- HA intercepts all packets for the MN and passes them along to MN using a tunnel.
- MN communicates directly with the CN.
- Referred to as Triangle Routing



Types of Encapsulation

- Three types of encapsulation protocols are specified for Mobile IP:
  - **IP-in-IP encapsulation**: required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.
  - **Minimal encapsulation**: optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.
  - **Generic Routing Encapsulation (GRE):** optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.
- Type of tunneling/encapsulation supported is indicated in registration.

IP in IP Encapuslation



Routing techniques

- **Triangle Routing:** tunneling in its simplest form has all packets go to home network (HA) and then sent to MN via a tunnel.
  - This involves two IP routes that need to be set-up, one original and the second the tunnel route.
  - Causes unnecessary network overhead and adds to the latency.

- **Route optimization:** allows the correspondent node to learn the current location of the MN and tunnel its own packets directly. Problems arise with
  - **mobility:** correspondent node has to update/maintain its cache.
  - **authentication:** HA has to communicate with the correspondent node to do authentication, i.e., security association is with HA not with MN.

Optimizations of Mobile IP

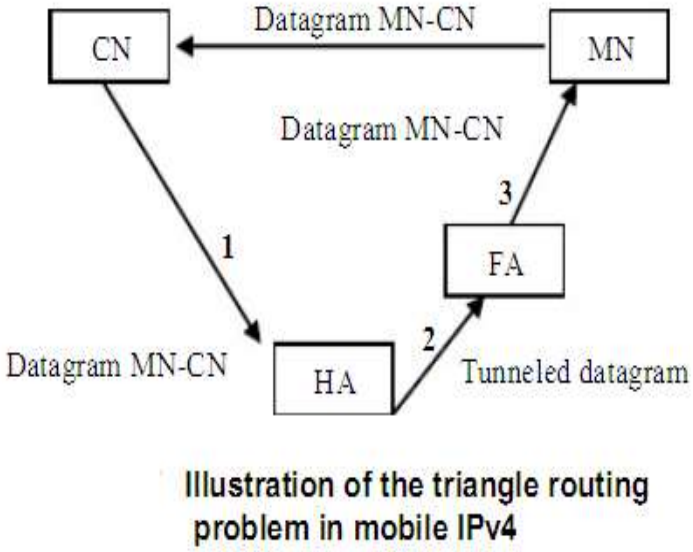
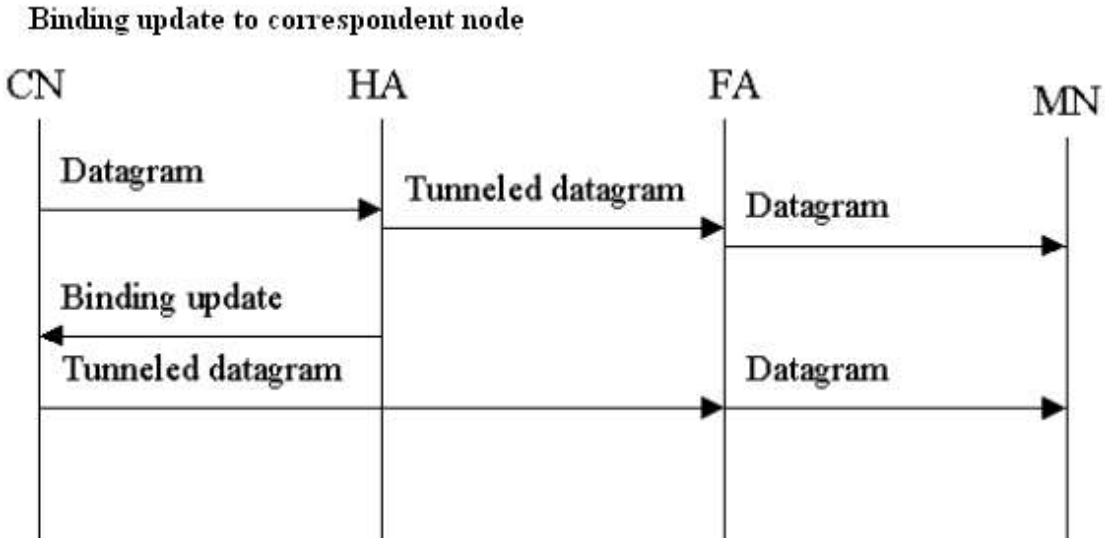


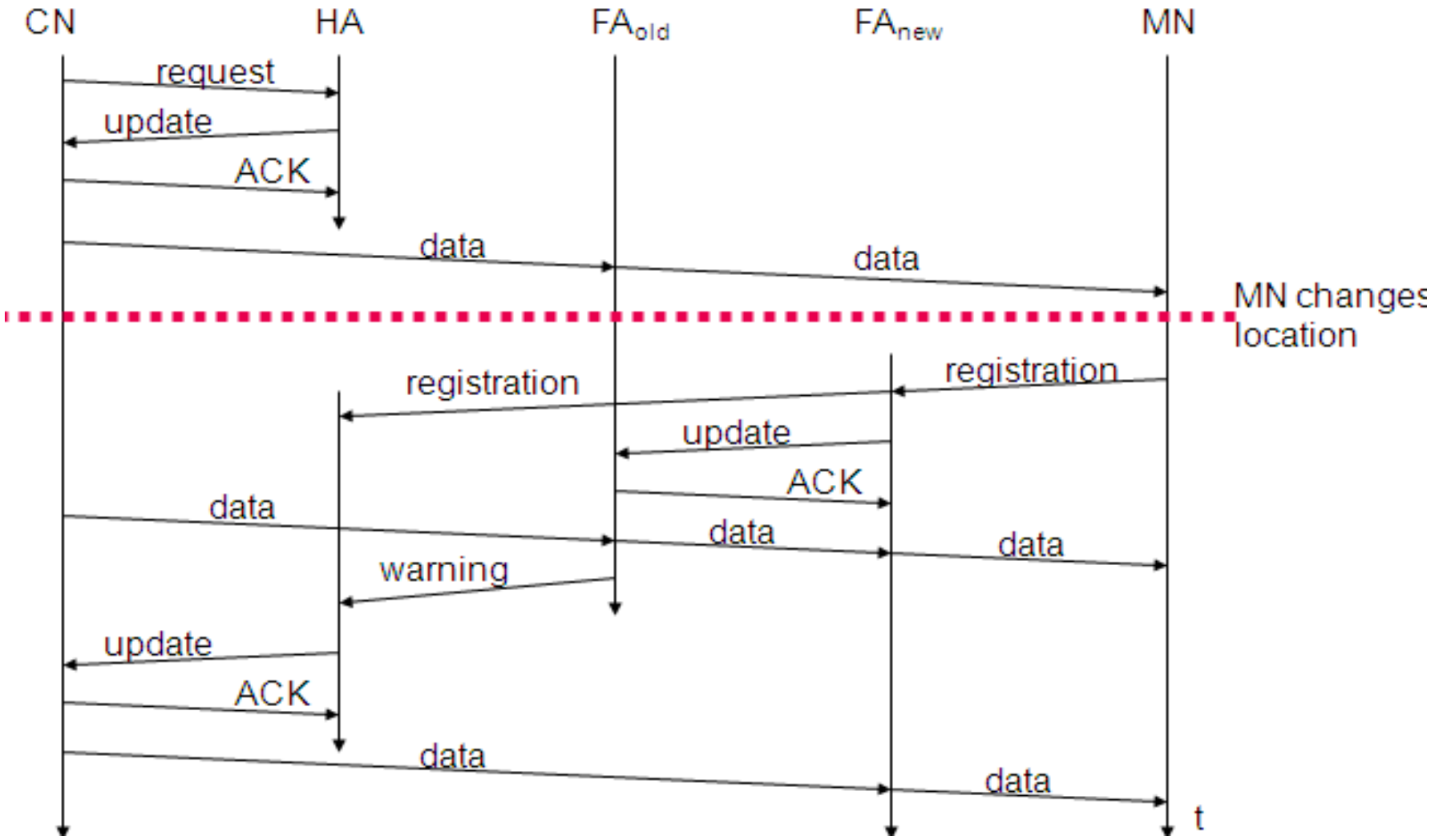
Illustration of the triangle routing problem in mobile IPv4



The route optimization extension adds a conceptual data structure, the binding cache, to the correspondent node and to the foreign agent. The binding cache contains bindings for mobile nodes' home addresses and their current care-of addresses. With the binding the correspondent node can tunnel datagrams directly to the mobile node's care-of address.

Route optimization adds four new UDP-messages to the Mobile IPv4 protocol: Binding update, binding acknowledgement, binding request and binding warning.

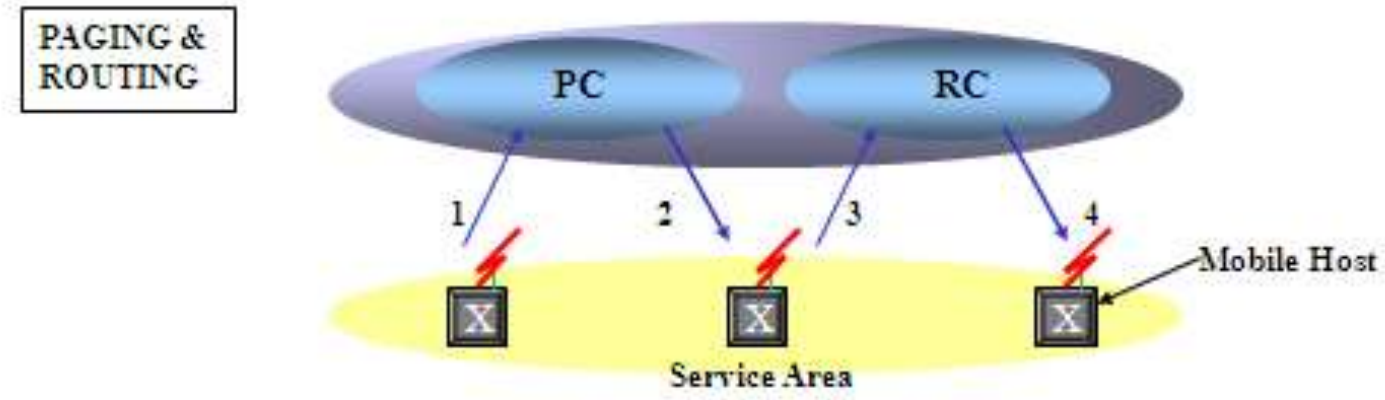
Change of FA


CN
HA
FA_old
FA_new
MN
request
update
ACK
data
data
MN changes location
registration
registration
update
ACK
data
data
data
warning
update
ACK
data
data
t

CELLULAR IP

- Mobile IP represents a simple & scalable global mobility solution, but is not appropriate in support of fast & seamless handoff control.
- Cellular IP is a new robust protocol that is optimized to support local mobility but efficiently interworks with Mobile IP to provide wide area mobility
- Cellular IP shows great benefit in comparison to existing host mobility protocols for environments where mobile hosts migrate frequently. This is very much valid as wireless internet becomes widespread.
- CIP can accommodate large no of users by maintaining distributed Paging and Routing caches
- Also CIP requires no new packet formats, encapsulations, or address space allocations beyond what is present in IP.

Efficient Location Management- CIP



Two parallel structures of mappings (PC &RC)

1 - ***idle MH*** keeps PC upto-date

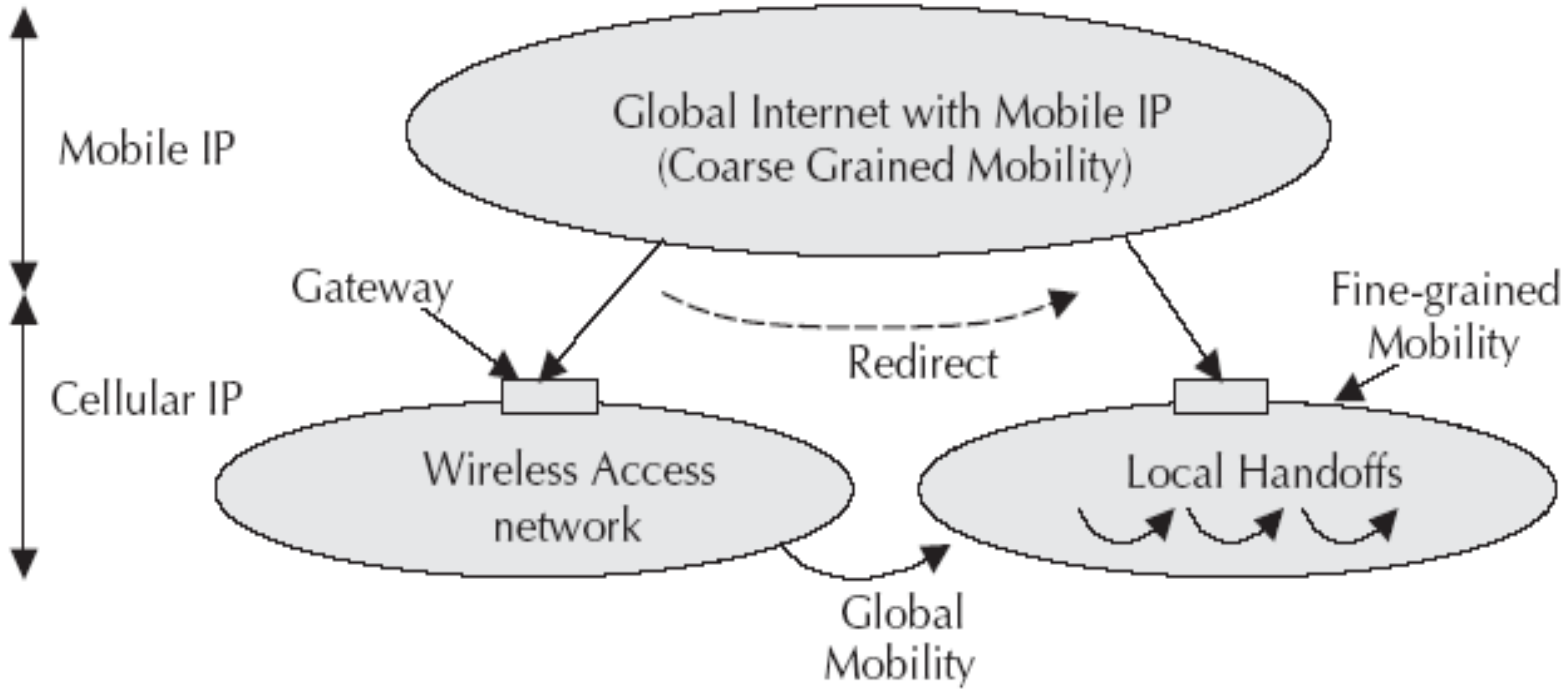
2 - PC mappings used to find the location of ***idle MH***

3 - maintains RC mappings until actively connected

4 - routing of data packets to MH

Paging Caches maintain mappings for stationary & idle hosts; where Routing Caches maintains mappings for mobile hosts. Timeout interval for PC mappings is large, where as for RC it is in Packet timescale.

Relationship between Mobile IP and Cellular IP



Comparison

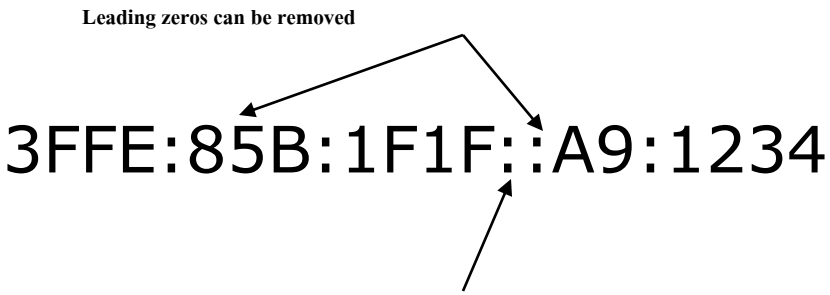
- Overall system must be able to manage
  - The handoff between cells within the same access network
  - The handoff between different access networks
- Mobile IP (MIP)
  - Used as an inter-subnet mobility protocol
  - Macro-mobility
- Cellular IP (CIP)
  - Intra subnet mobility
  - Micro-mobility
  - Paging management

Internet Protocol version 6

- Successor to today's IP version 4 protocol (IPv4)
- Internet Engineering Task Force (IETF) has produced a comprehensive set of specifications (RFC 1287, 1752, 1886, 1971, 1993, 2292, 2373, 2460, 2473, etc.) that define the next-generation IP protocol originally known as 'IPNg'
- Uses 128 bit addresses for each packet creating a virtually infinite number of IP addresses (approximately 3.4*10**38 IP addresses) as opposed to 3758096384 IPv4 addresses

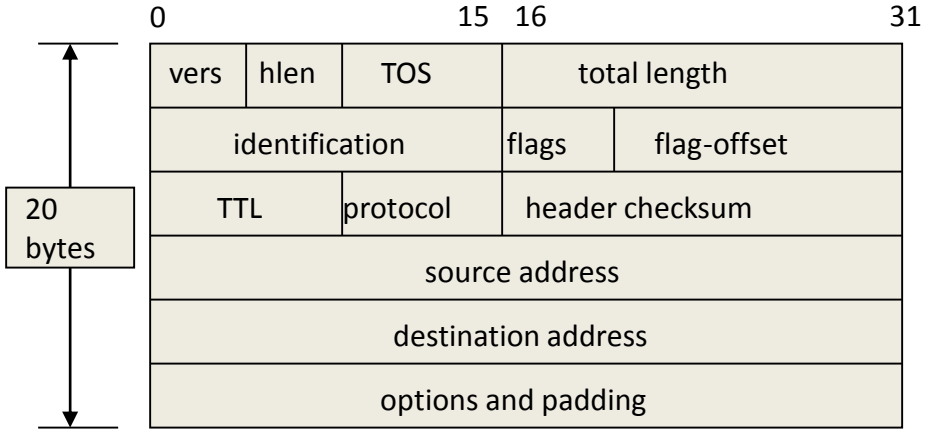
3FFE:085B:1F1F:0000:0000:0000:00A9:1234

8 groups of 16-bit hexadecimal numbers separated by ":"

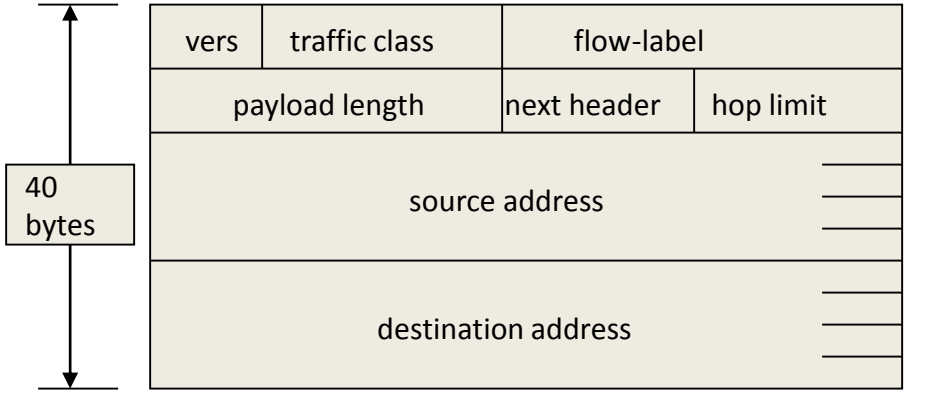


:: = all zeros in one or more group of 16-bit hexadecimal numbers

Header comparison



IPv4



IPv6

Removed (6)

- ID, flags, flag offset
- TOS, hlen
- header checksum

Changed (3)

- total length => payload
- protocol => next header
- TTL => hop limit

Added (2)

- traffic class
- flow label

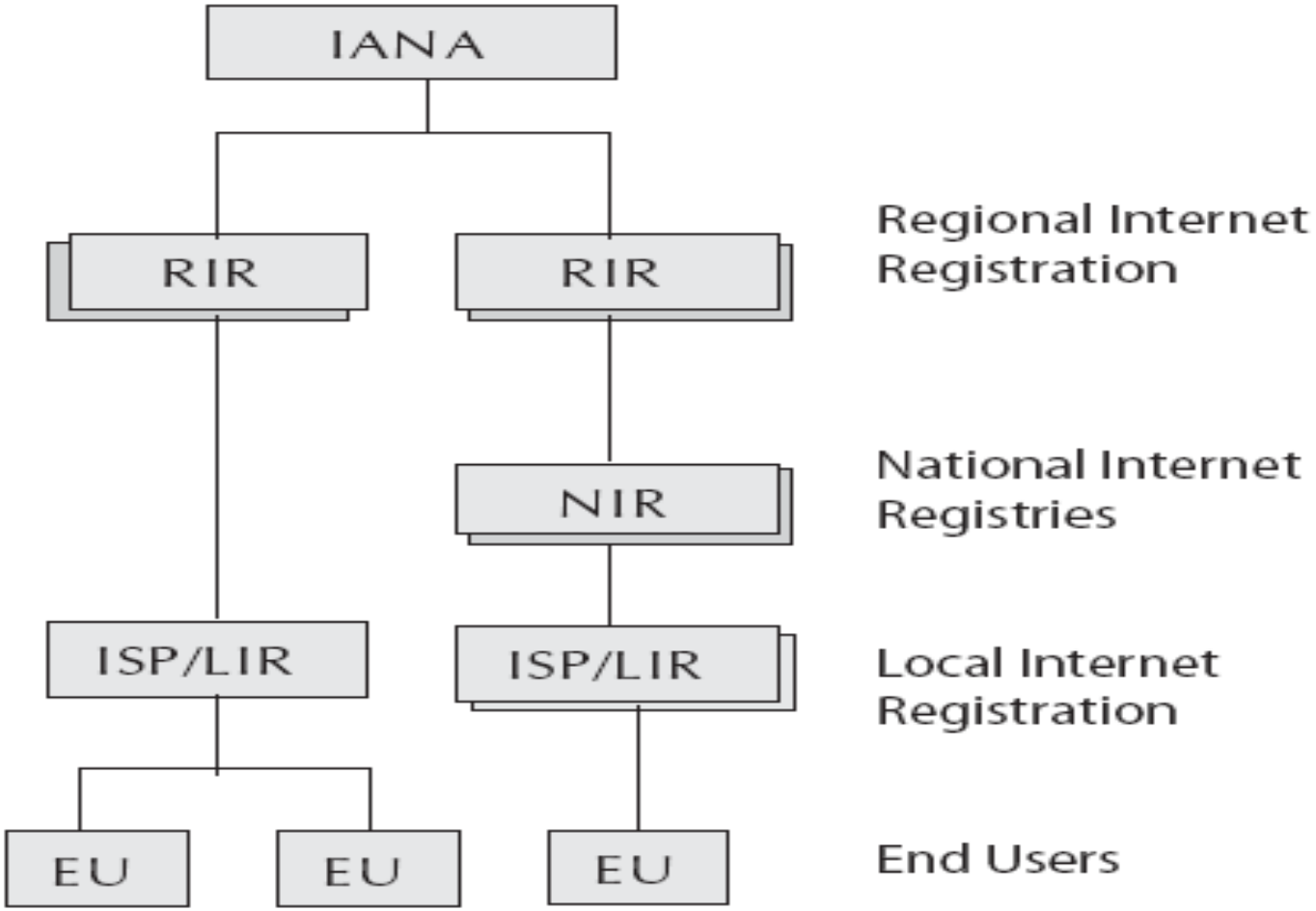
Expanded

- address 32 to 128 bits

IPv6

- There are global addresses and local addresses
- Global addresses are used for routing of global Internet
- Link local addresses are available within a subnet
- IPv6 uses hierarchical addressing with three level of addresses
- Includes a Public Topology (the 48 bit external routing prefix)
- Site Topology (typically a 16 bit subnet number)
- Interface Identifier (typically an automatically generated 64 bit number unique on the local LAN segment)

Hierarchical addressing of IPv6



Features of IPSec

- IPv6 Comes native with a security protocol called IP Security (IPSec), which is a standards-based method of providing privacy, integrity and authenticity to information transferred across IP networks
- Diffie-Hellman key exchange mechanism for deriving key between peers on a public network
- Public key cryptography to guarantee the identity of the two parties and avoid man-in-the-middle attacks
- Bulk encryption algorithms, such as 3DES, for encrypting the data
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication
- Digital certificates signed by a certificate authority to act as digital ID cards
- IPSec provides IP network layer encryption

Migrating from IPv4 to IPv6

- Migration of the **network components** to be able to support IPv6 packets. Using IP tunneling, IPv6 packets can propagate over an IPv4 envelope. Existing routers can support IP tunneling.
- Migration of the **computing nodes** in the network. This will need the operating system upgrades so that they support IPv6 along with IPv4. Upgraded systems will have both IPv4 and IPv6 stacks.
- Migration of **networking applications** in both client and server systems. This requires porting of the applications from IPv4 to IPv6 environment.

Interconnecting IPv6 networks

- Tunneling is one of the key deployment strategies for both service providers as well as enterprises during the period of IPv4 and IPv6 coexistence.
- Tunneling service providers can offer an end-to-end IPv6 service without major upgrades to the infrastructure and without impacting current IPv4 services.

Tunneling Mechanisms

- Manually created tunnels such as IPv6 manually configured tunnels (RFC 2893)
- IPv6 over IPv4 tunnels
- Semiautomatic tunnel mechanisms such as that employed by tunnel broker services
- Fully automatic tunnel mechanisms such as IPv4 compatible

Mobile IP with IPv6

- IPv6 with hierarchical addressing scheme can manage IP mobility much efficiently.
- IPv6 also attempts to simplify the process of renumbering which could be critical to the future routing of the Internet traffic.
- Mobility Support in IPv6, as proposed by the Mobile IP working group, follows the design for Mobile IPv4. It retains the ideas of a home network, home agent and the use of encapsulation to deliver packets from the home network to the mobile node's current point of attachment.
- While discovery of a care of address is still required, a mobile node can configure its care of address by using Stateless Address Auto-configuration and Neighbor Discovery. Thus, foreign agents are not required to support mobility in IPv6.

1. There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.

2. Support for route optimization is a fundamental part of the Mobile IPV6.

3.Mobile IPv6 route optimization can operate securely even without pre-arranged security associations.

4. Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering".

5. The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location.

6. Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.

7. Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.

8. The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".

9. The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.