MONASH University

Information Technology

FIT5183: Mobile and Distributed Computing Systems (MDCS)

Lecture 11B
Internet Protocol (IP) and Mobile IP

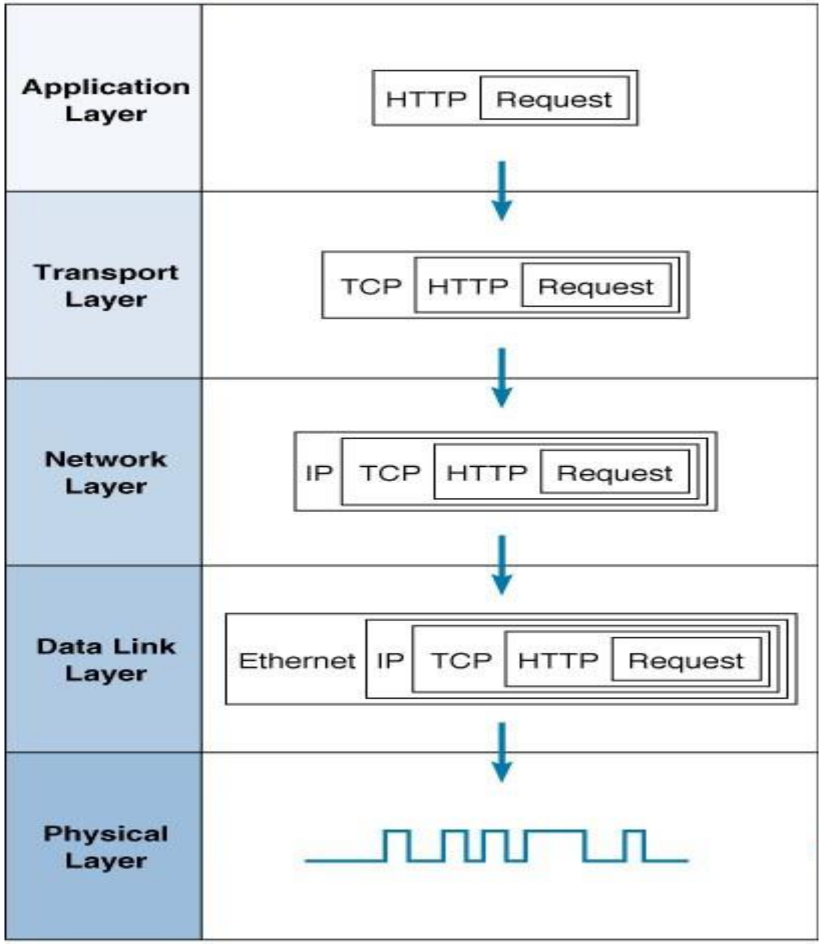
Overview

- Internet Protocol
  - IPv4
  - IPv6
- Mobile IP

Introduction to Internet Protocol

OSI Layers

- Information is passed between the layers via encapsulation
- Header information is attached to data passed down layers

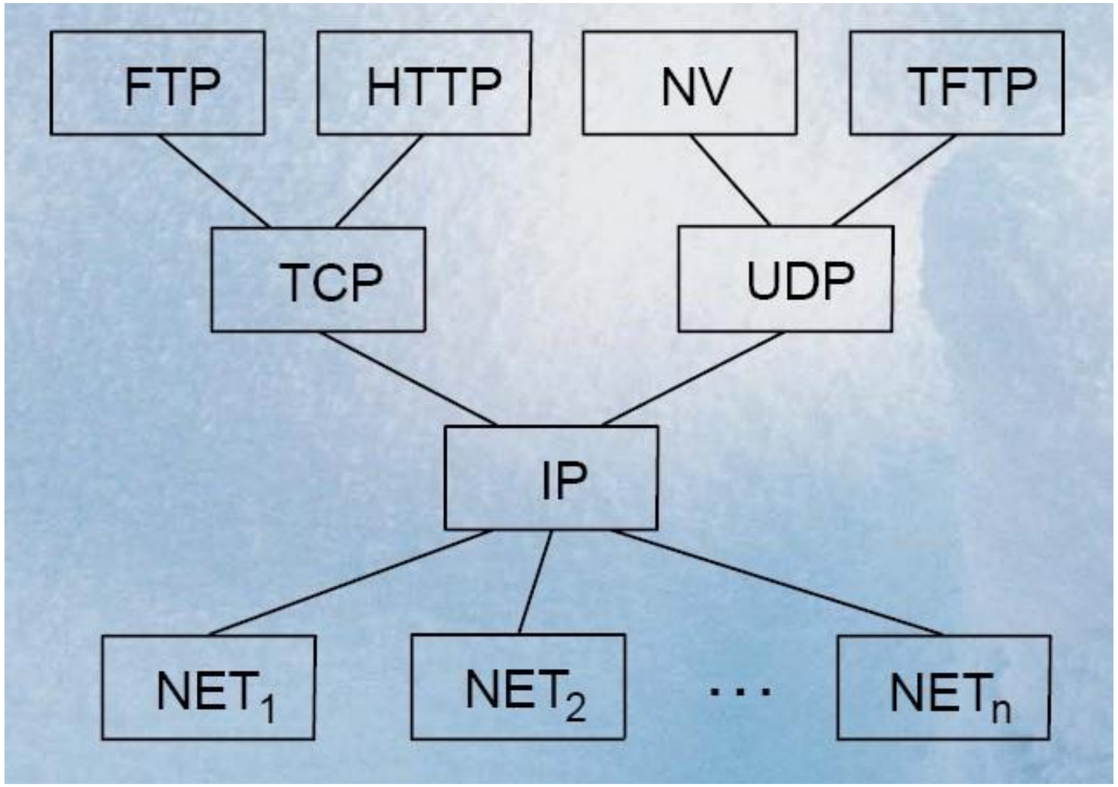


IP (Internet Protocol)

- IP protocol operates at the network layer
- A protocol for networking, addressing and routing
- Data is split into packets and each packet is handled independently of the other packets (may be routed through different paths)
- Supports both connectionless (UDP) and connection-oriented (TCP) protocols:
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)

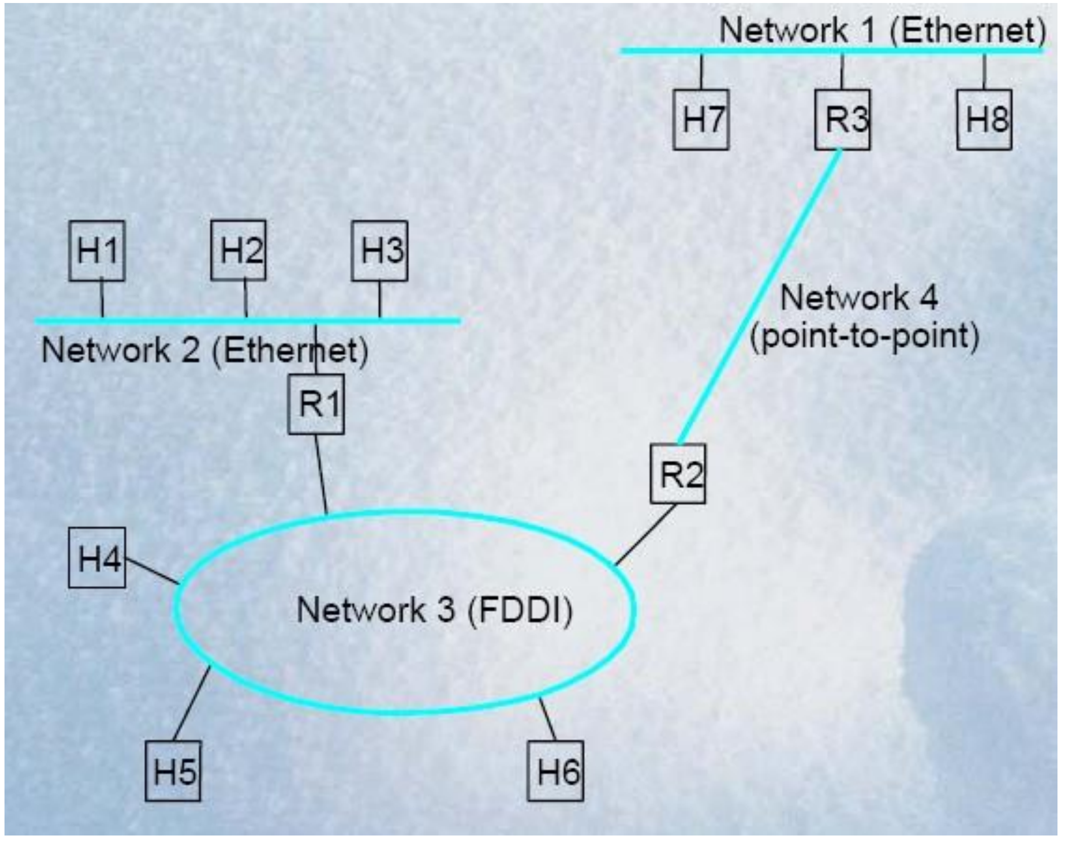
Hourglass Design

- Communication at a specific layer is enabled by a protocol
- Multiple choices at each layer except for IP



Routers

- Internet **Routers** work on IP addresses to determine how to interconnect the sender to the destination
- Connecting networks with different data link and physical layer protocols



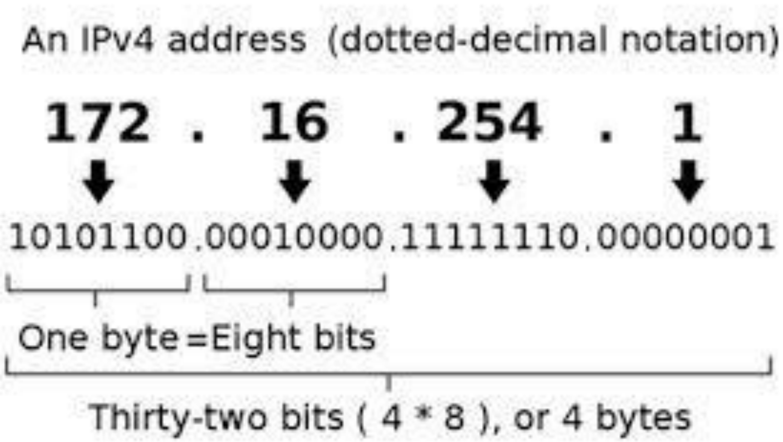
FDDI (Fibre Distributed Data Interface): a standard for data transmission in LAN

IPv4 (Internet Protocol version 4)

- Every device on the Internet must be assigned an IP address in order to communicate with other devices
- A global IP address is a unique identifier
- IPv4 is the version 4 in the development but the first widely IP version used
- IPv4 is a connectionless protocol
- It operates on a best effort delivery model
- But the reliability issues are addressed when it is used with a reliable transport protocol like TCP

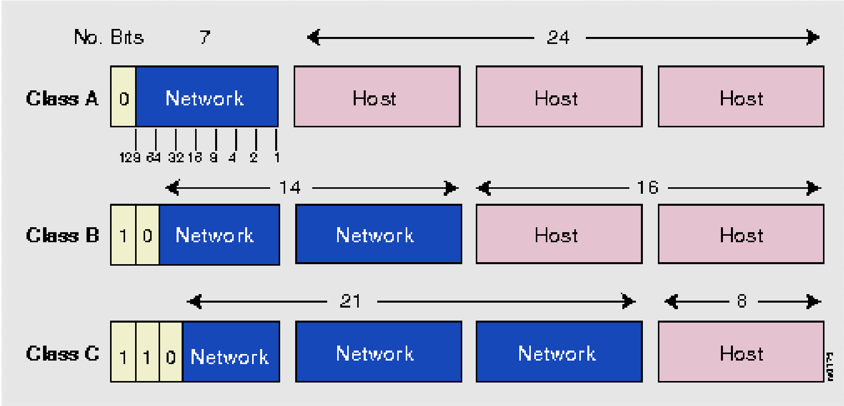
IPv4 - Addressing

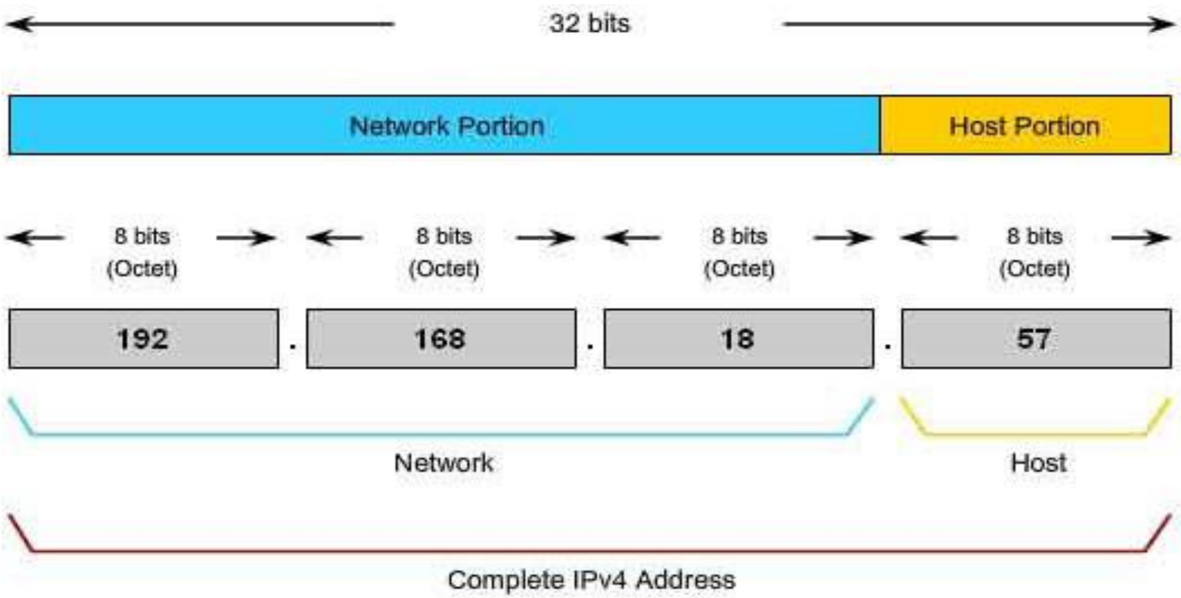
- IP address is 32 bit (4 bytes) in length
- Only **4,294,967,296** (2^{32}) possible unique addresses
- Dot Notation, consisting of 4 decimal numbers, each ranging from 0 to 255
- Global addresses are unique



IPv4 Address Structure

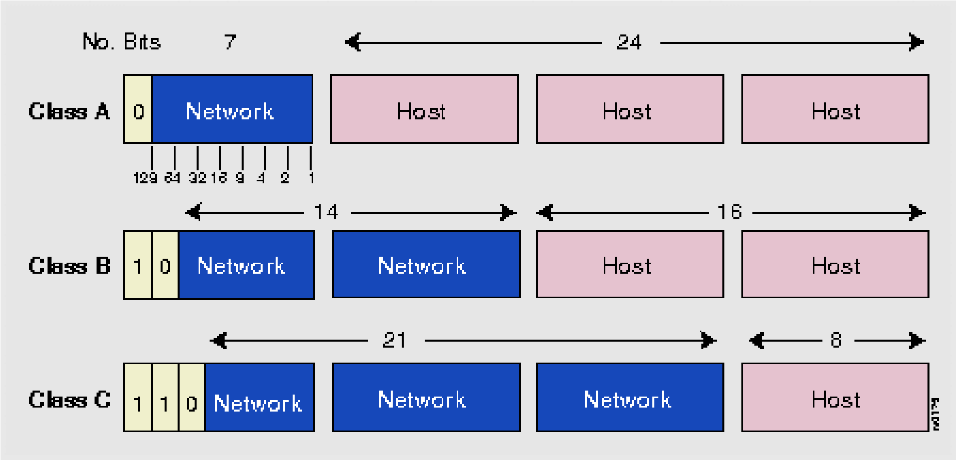
- IP address consists of two parts:
  - Network Identifier (netid)
  - Host Identifier (hostid)





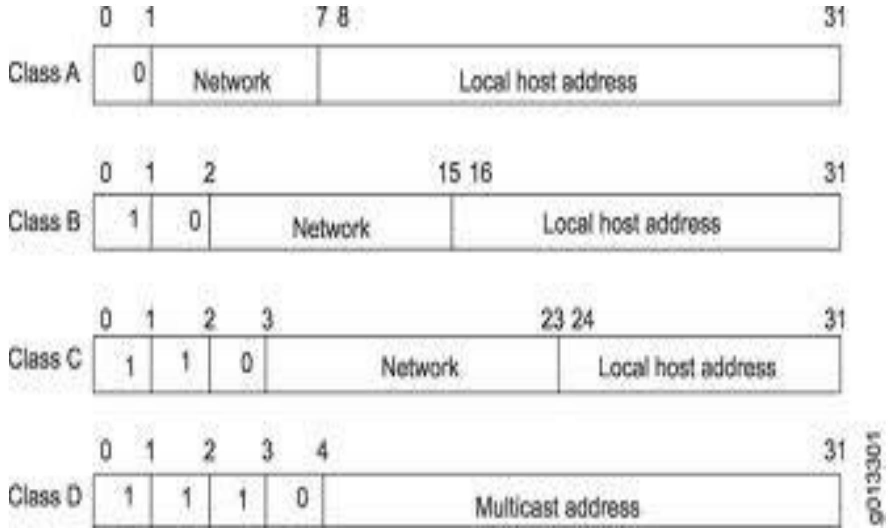
Classful Addressing in IPv4

- Class A for large networks and companies with many hosts
  - Hosts up to 16,777,216
- Class B for medium-sized networks
  - Hosts up to 65, 543
  - Class B at Monash and an example of **130.194**.7.10
- Class C for many but small networks, each with a few hosts
  - Hosts up to 256



Classful Addressing in IPv4

- Class D addresses reserved for multicasting
  - Multicast sending IP messages to a group of defined nodes
- Class E reserved for future use (some research organisations using for experimental purposes)
- Worked well only for early years of the Internet
- But obsolete now, replaced by classless addressing



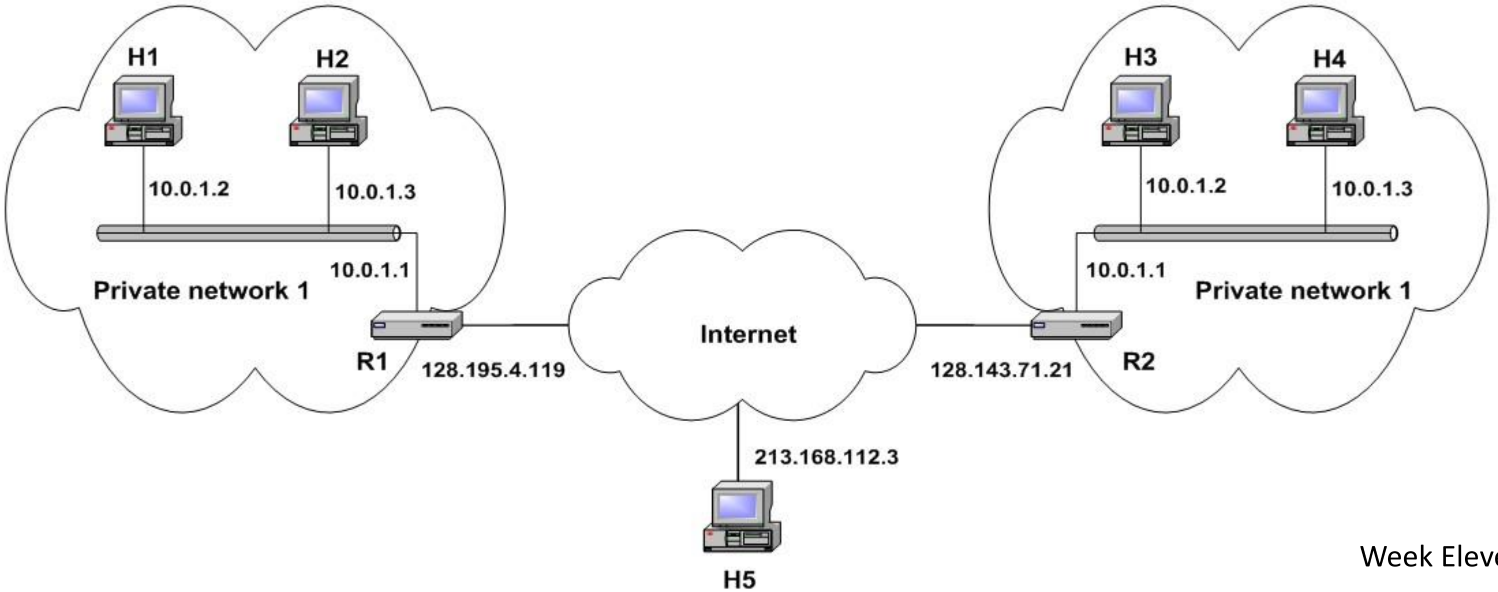
Class	Address	# of Hosts	Netmask (Binary)
CIDR	/4	240,435,456	11110000 00000000 00000000 00000000
CIDR	/5	134,217,728	11111000 00000000 00000000 00000000
CIDR	/6	67,108,864	11111100 00000000 00000000 00000000
CIDR	/7	33,554,432	11111110 00000000 00000000 00000000
A	/8	16,777,216	11111111 00000000 00000000 00000000
CIDR	/9	8,388,608	11111111 10000000 00000000 00000000
CIDR	/10	4,194,304	11111111 11000000 00000000 00000000
CIDR	/11	2,097,152	11111111 11100000 00000000 00000000
CIDR	/12	1,048,576	11111111 11110000 00000000 00000000
CIDR	/13	524,288	11111111 11111000 00000000 00000000
CIDR	/14	262,144	11111111 11111100 00000000 00000000
CIDR	/15	131,072	11111111 11111110 00000000 00000000
B	/16	65,534	11111111 11111111 00000000 00000000
CIDR	/17	32,768	11111111 11111111 10000000 00000000
CIDR	/18	16,384	11111111 11111111 11000000 00000000
CIDR	/19	8,192	11111111 11111111 11100000 00000000
CIDR	/20	4,096	11111111 11111111 11110000 00000000
CIDR	/21	2,048	11111111 11111111 11111000 00000000
CIDR	/22	1,024	11111111 11111111 11111100 00000000
CIDR	/23	512	11111111 11111111 11111110 00000000
C	/24	256	11111111 11111111 11111111 00000000

Classless Addressing

- Classless addressing aimed to eliminate the gaps (inefficient use of addresses) between Class A, B, and C networks
- Use of a new method called **Classless Inter-domain Routing (CIDR)**
- A CIDR IP ends **with a slash followed by a number** (called slash notation)
- Network Prefix specifies how many addresses are covered by the CIDR address
  - E.g. **192.168.100**.0/24 (actually class C) means 24 bits are allocated for the network prefix and remaining 8 bits for host addressing
    (up to 256 addresses) from **192.168.100**.0 to **192.168.100**.255
  - E.g. **192.168.100.0/23** represents the address ranges (up to 512 addresses)

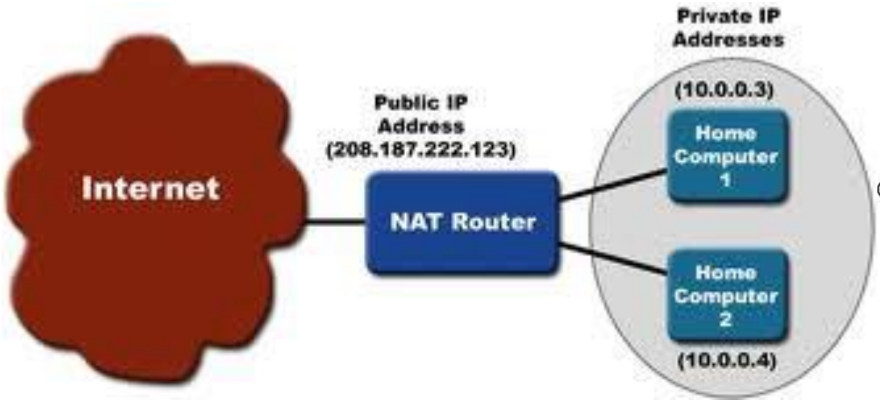
Private Addresses

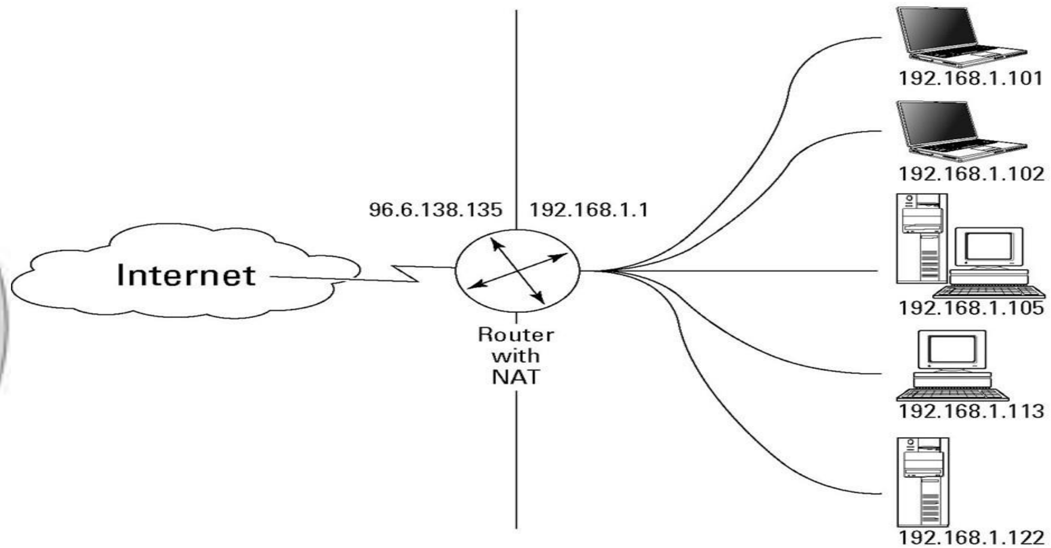
- Most of hosts did not require direct connectivity to other Internet hosts
- For this purpose, private addresses are used (not globally unique)
- Private addresses are reserved by Internet Assigned Numbers Authority (IANA)
- Private addresses are not reachable on the Internet (not routable)
- Private address ranges (e.g. 10.0.0.1, 172.16.0.1,192.168.0.1)
- However, to connect to the Internet, private addresses must be translated into a valid public address



NAT (Network Address Translation)

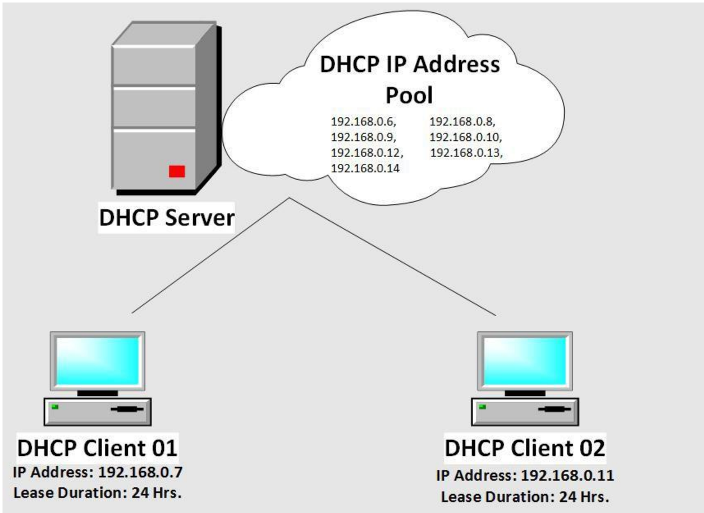
- NAT **maps** one **public IP address** into a number of **private addresses**
- NAT allows multiple devices to share a single IP address using private addresses
- NAT helps with the limitation of IPv4 addresses
- E.g. the routers at home does NAT





DHCP (Dynamic Host Configuration Protocol

- The limited number of IP addresses are addressed by using NAT routers and DHCP for leasing of dynamic IP addresses
- The DHCP server assigns computers unique IP addresses for a specific period of time (Lease obtained … and Lease expires …)
- It will release and renew address as devices leave and join the network
- Most home routers are assigned a globally unique IP address by their ISPs. Within our home network, DHCP assigns a local IP address to devices connected to the local network



Internet and IP Packets

- Video

A Packet's Tale - How does the Internet work?

IPv6

- IPv4 Exhausted, started to run out around 1996
- Internet Protocol version 6 (IPv6) was developed by IETF (Internet Engineering Task Force) as an effort to address the IPv4 problems
- Smooth transition path from IPv4
- IPv6 routers and hosts can handle mix traffic because the IPv4 address space can be embedded in the IPv6 space

IPv6 Address Spaces vs IPv4

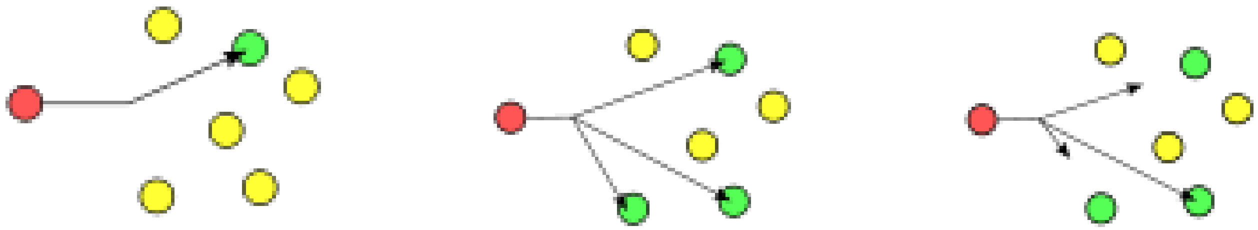
- The exact number of IPv6 addresses available is….
- 340 trillion trillion trillion (one trillion is million million)
- “340,282,366,920,938,463,463,374,607,431,768,211,456”
  - ~ 340 undecillion addresses
- Comparing this to IPv4′s address space of “4,294,967,296”
- Standard representation is set of (128 bits or 16 bytes)
- Separated by colons, eight two-byte words in hexadecimal format
- IPv6 address e.g. 47CD: 1234:3200:0000:0000:4325:B792:0428

Notation

- If there are large numbers of zeros, they can be omitted with series of colons, e.g.
  - **47CD:1234:3200:0000:0000:4325:B792:0428**
  - **47CD:1234:3200::4325:B792:0428**
- Leading zeros can be omitted (**2001:0388:608c:2c58:020f:feff:fef9:05b4**)
  - **2001:388:608c:2c58:20f:feff:fef9:5b4**

IPv6 Address Types

- IPv6 has three types of addresses:
- Unicast addresses: A packet is delivered to one host/ network interface
- Multicast addresses: A packet is delivered to multiple interfaces
  - always begin with FF (e.g. FF00::/8)
- Anycast addresses (reserved addresses): Multiple nodes may be listening but packets will be delivered to only one of these nodes
- IPv6 does not use broadcast messages



IPv6 Unicast Addresses

- **Global Unicast address**
  - Identifies a unique node on the internet, publicly routable addresses
- **Unique-local address**
  - Similar to IPv4's private addresses (not routable) *but still unique*
- **Link-Local Address**
  - Enables nodes on the same link to communicate with each other
  - Link-local addresses have the prefix of FE80
  - A host can generate link-local addresses by extending MAC address, e.g. the MAC address is 00:0E:0C:31:C8:1F

  the Link-local address: FE80::20E:0CFF:FE31:C81F
- **Site-local address** (deprecated)
  - To provide a private addressing for intranet traffic

Autoconfiguration

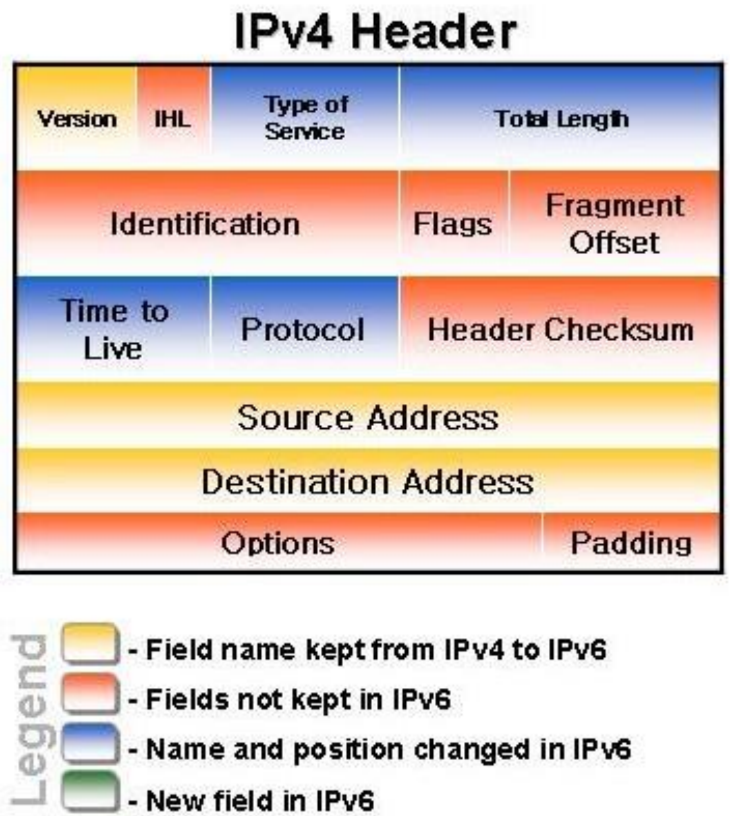
- Stateful autoconfiguration
  - Obtaining IP addresses from a DHCP server
  - DHCPv6 (Dynamic Host Configuration Protocol for IPv6)
- Stateless autoconfiguration
  - Integral to IPv6 protocol
  - Allows a host to generate its own addresses using a combination of *locally available information* + *information advertised by routers*
  - Most likely unique, no need for approving by a server so simpler

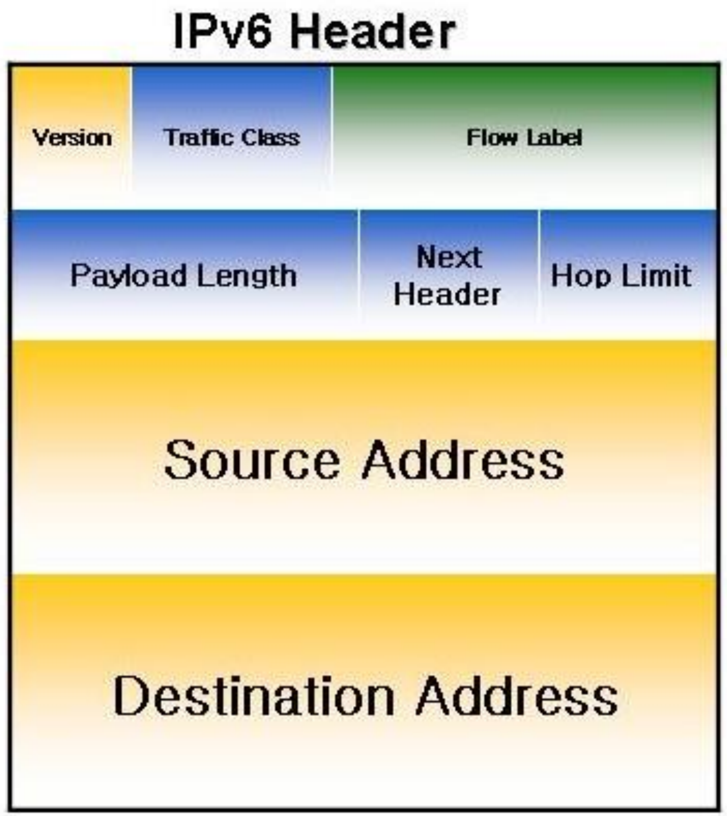
Stateless Autoconfiguration

- The stateless mechanism allows a host to generate its own addresses by combining these two:
  - Routers advertise prefixes (e.g. **2001:690:1:1**) that identify the subnet(s) associated with a link
  - Hosts generate an "interface identifier" that uniquely identifies an interface on a subnet (e.g. IPv6 address: **2001:690:1:1**:20E:0CFF:FE31:C81F)

- In the absence of routers, a host can only generate link-local addresses which only allow communication among nodes attached to the same link

IPv6 Packet Format





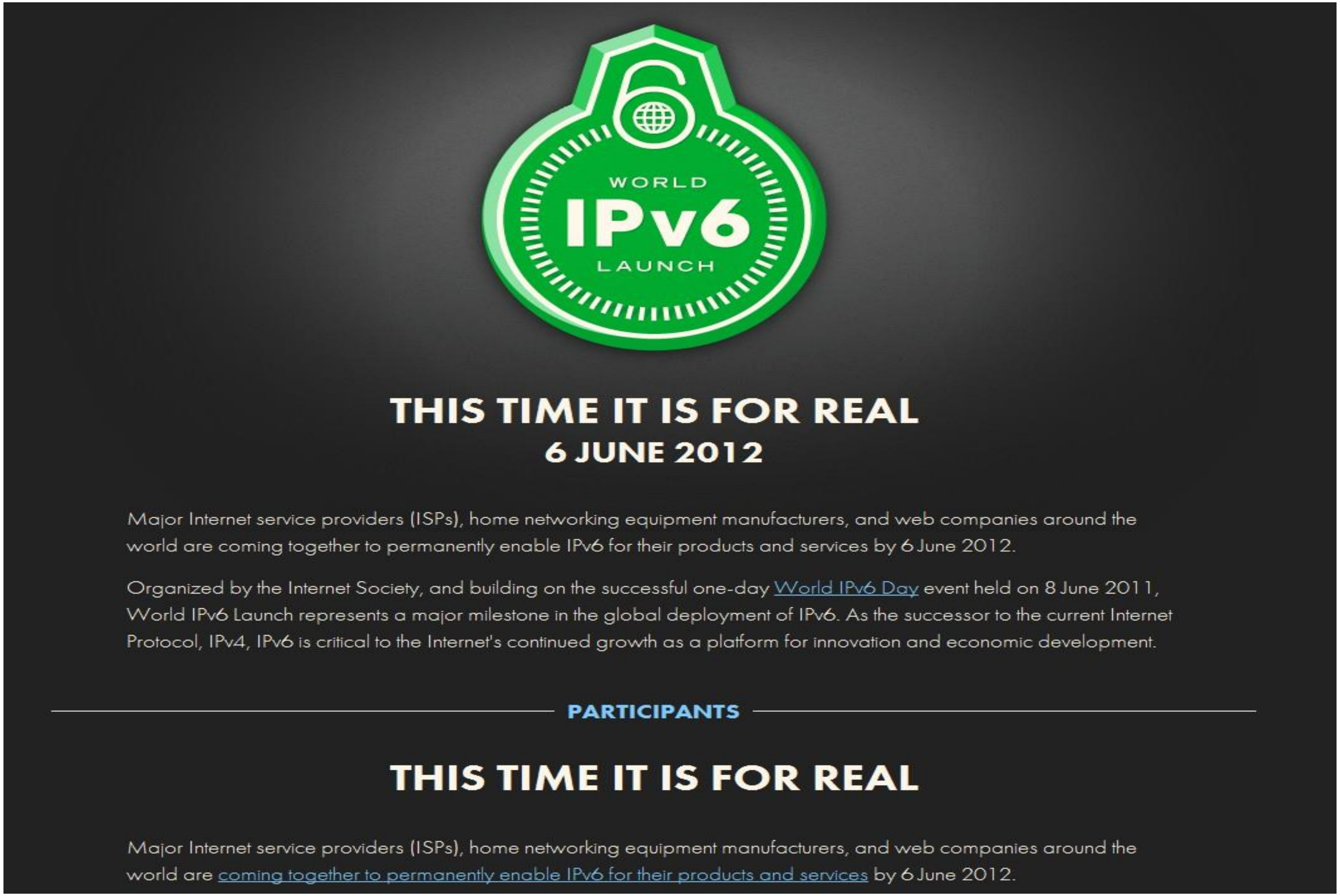
Identification, Flags, and Fragment Offset removal— Fragmentation is done differently in IPv6, no longer by intermediate routers in the networks
Flow Label supporting QoS management

IPv6 vs IPv4

- Large address space
- More efficient routing: no packet fragmentation by the routers
- New header format: more efficient packet processing by simplifying packet header, no IP-level checksum in IPv6
- Stronger and more improved support for mobility (Mobile IP)
- IPSec supports secure exchange of packets, mandatory in IPv6, but optional in IPv4
- Stateless Autoconfiguration
- Neighbour Discovery: find out about neighbouring nodes
  - Router Solicitation, Router Advertisement
    - to request all routers to send Router Advertisement immediately, rather than waiting until the next periodically scheduled advertisement
  - Neighbor Solicitation, Neighbor Advertisement
  - Redirect (informing hosts about a better next-hop address to forward packets)

IPSec

- IPsec is a set of protocols developed by the Internet Engineering Task Force (IETF)
- IPSec provides confidentiality and data integrity
  - Uses SHA1 based algorithms for integrity
  - Uses AES and TripleDES based algorithms for confidentiality
- IPsec supports two encryption modes:
  - Transport
    - Encrypts only the data portion (payload) of each packet, but leaves the header clear
  - Tunnel
    - Encrypts both the header and the payload



IPv6 Video What is IPv6?

Mobile IP

Mobile IP

- In IP networks, routing is based on stationary IP addresses
- 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 moves away from its home network and is no longer reachable
- Mobile IP enables mobile hosts to stay connected and maintain ongoing applications while moving between different networks

Mobile IP

- A standard communications protocol by Internet Engineering Task Force (IETF)
- Mobile IP aims to enable users to keep the same IP address while traveling to a different network
- Mobile IP uses two IP addresses:
  - A fixed home address (the home/original address)
  - And a new address, Care-Of-Address (CoA), that represents its current location in a new network when moving
- Mobile IP for IPv4
- Mobile IP for IPv6

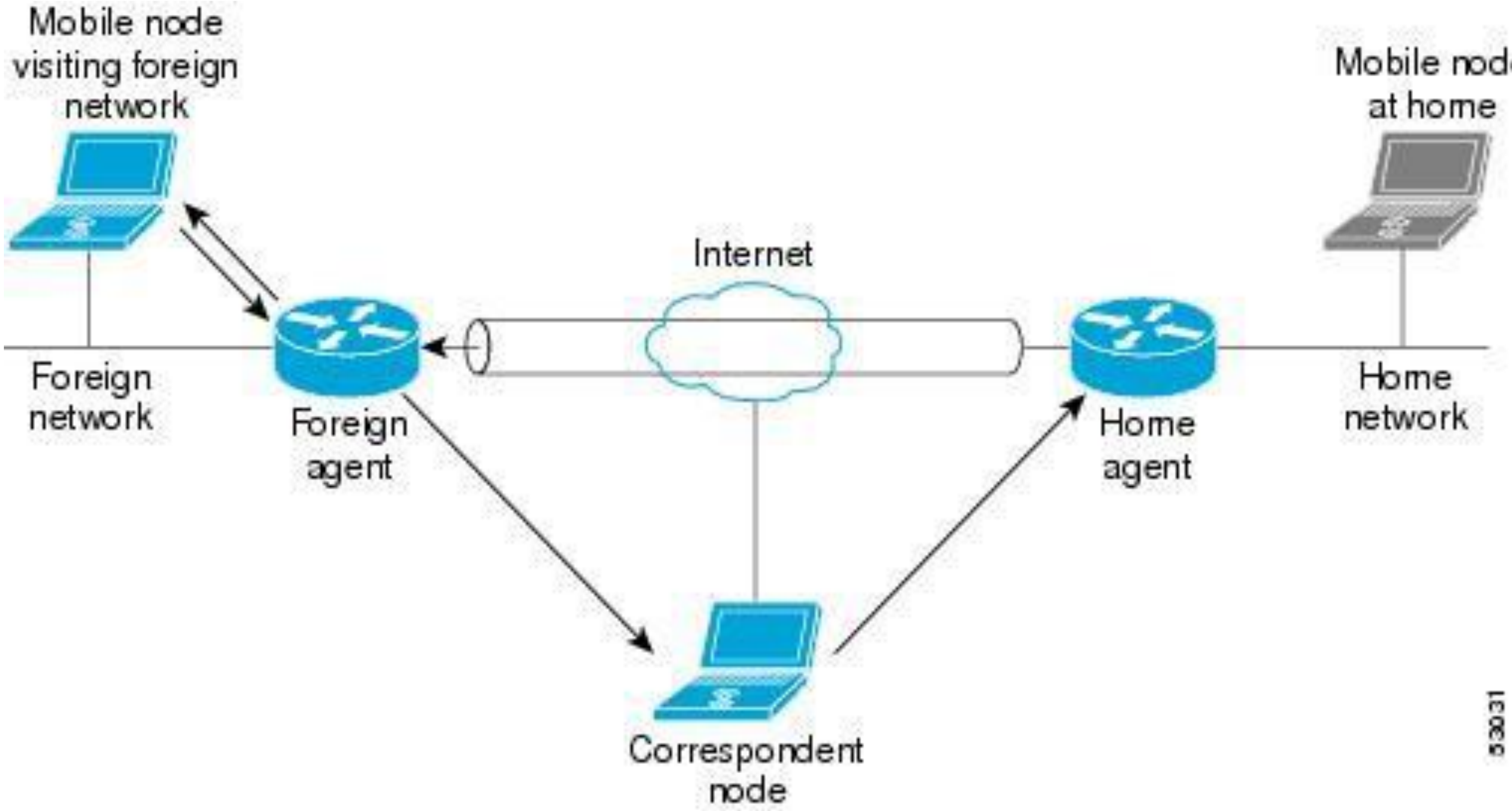
Mobile IP Entities

- **Mobile Node/host (MN):** the entity that may move from one network to network in the Internet
- **Correspondent Node (CN):** the end host to which MN is corresponding
- **Home network:** the network to which the mobile node is originally assigned
  - **Home address**: IP address on the home network which is static
- **Foreign network:** another network to which the mobile node moves
- **Mobility agents:** two agents are involved in routing:
  - Home Agent (HA)
  - Foreign Agent (FA)
    - Supported in IPv4 but removed in IPv6

Mobility Agents in IPv4

- **Home Agent (HA)**
  - Processes running on fixed computers (like a router) at the home site
  - Keeps up-to-date information about the mobile host's current location
- **Foreign Agent (FA)**
  - Processes running on the current location of the mobile host
  - When the mobile host arrives at a new site, it informs the FA at that site
  - FA allocates a 'care-of address' to the mobile host
  - FA contacts HA and passes the 'care-of address' to it
- **Care-of address (CoA)**
  - A temporary IP address which identifies MN's current location in the local subnet
  - FA assigns it to MN and also sends it to HA

Mobile IP Entities in IPv4



Capabilities of Mobile IP

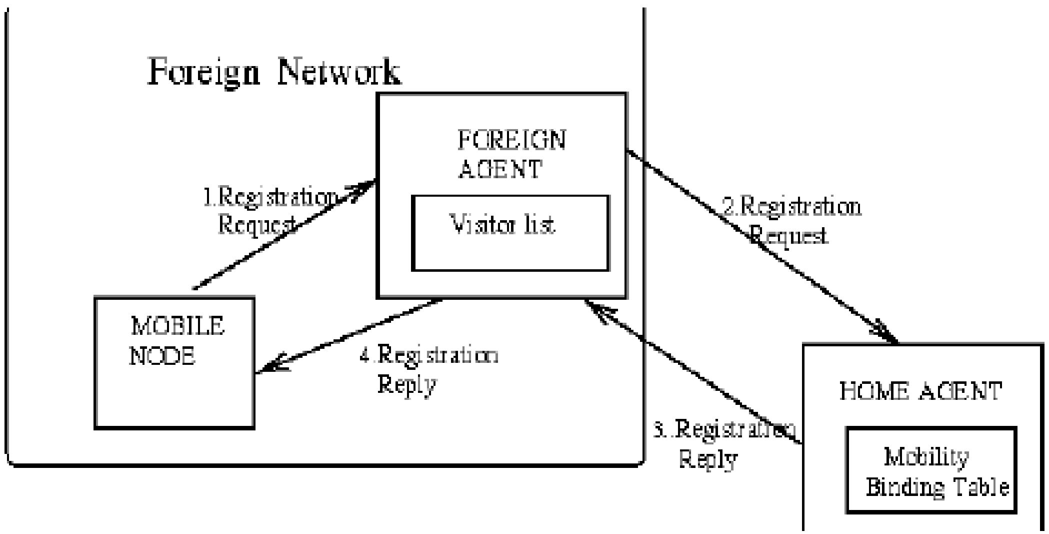
- **Agent Advertisement:** both HA and FA periodically send advertisement messages into their subnets
- **Agent solicitation:** If a mobile node needs agent information immediately (not waiting for the next periodic advertisement), it can send agent solicitation
  - Any agent receiving this message will then issue an agent advertisement
- **Discovery:** mobile node listens to messages to detect HA and FAs
  - MN must determine if it is at the home network or a foreign network
  - **Movement detection:** a mobile node becomes aware that it is on a new network
- **Registration**
- **Tunneling**

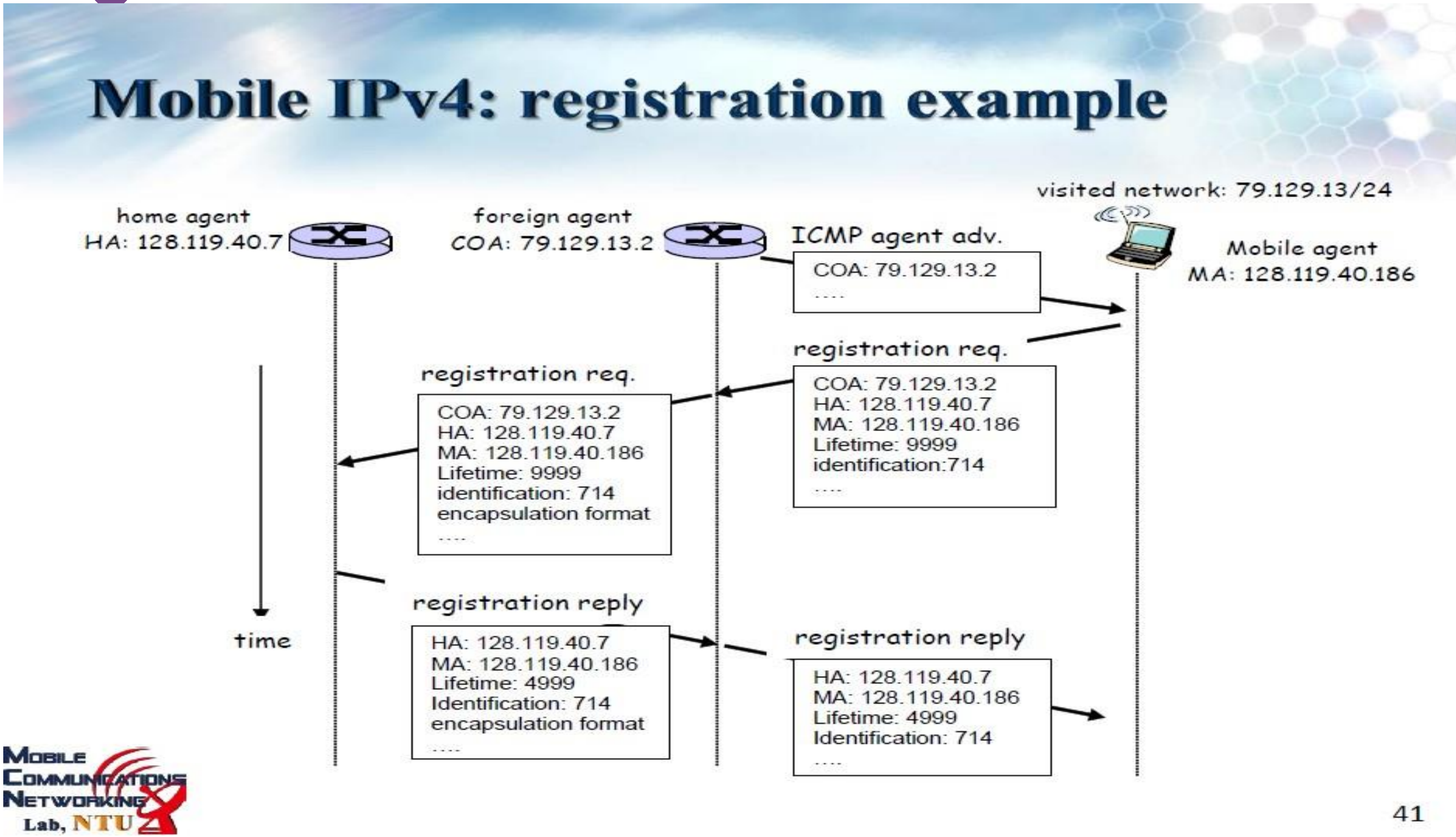
Registration Process

- When the Mobile Node hears a **FA advertisement** and detects that it has moved outside of its home network (**discovery**), it begins registration

  1. Mobile node **sends a mobile IP registration request** to Foreign Agent
  2. Foreign Agent checks its validity and then **relays the request to HA**
  3. HA accepts or denies the request and **sends registration reply to FA**
  4. FA **relays the reply to the mobile node**

- Validation occurs at all three nodes, HA is now aware of MN's location




Mobile IPv4: registration example
visited network: 79.129.13/24
home agent
HA: 128.119.40.7
foreign agent
COA: 79.129.13.2
ICMP agent adv.
COA: 79.129.13.2
....
Mobile agent
MA: 128.119.40.186
registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification:714
....
registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
....
time
registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....
registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
....
Mobile Communications Networking Lab, NTU
41

Tables Maintained on Routers (IPv4)

- Mobility Binding Table

  Maintained by the Home Agent

  Maps MN's home address with its current CoA

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

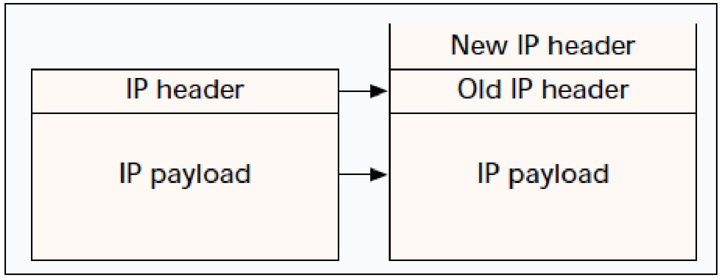
- Visitor List

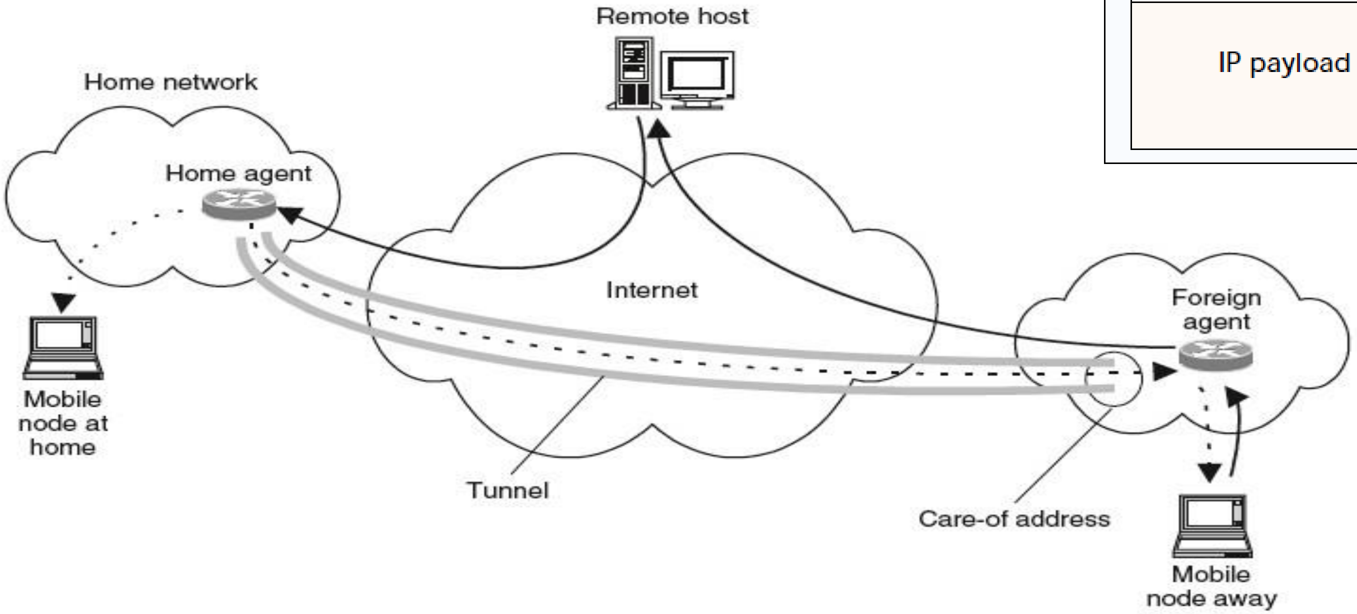
  Maintained by the Foreign Agent serving an MN

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

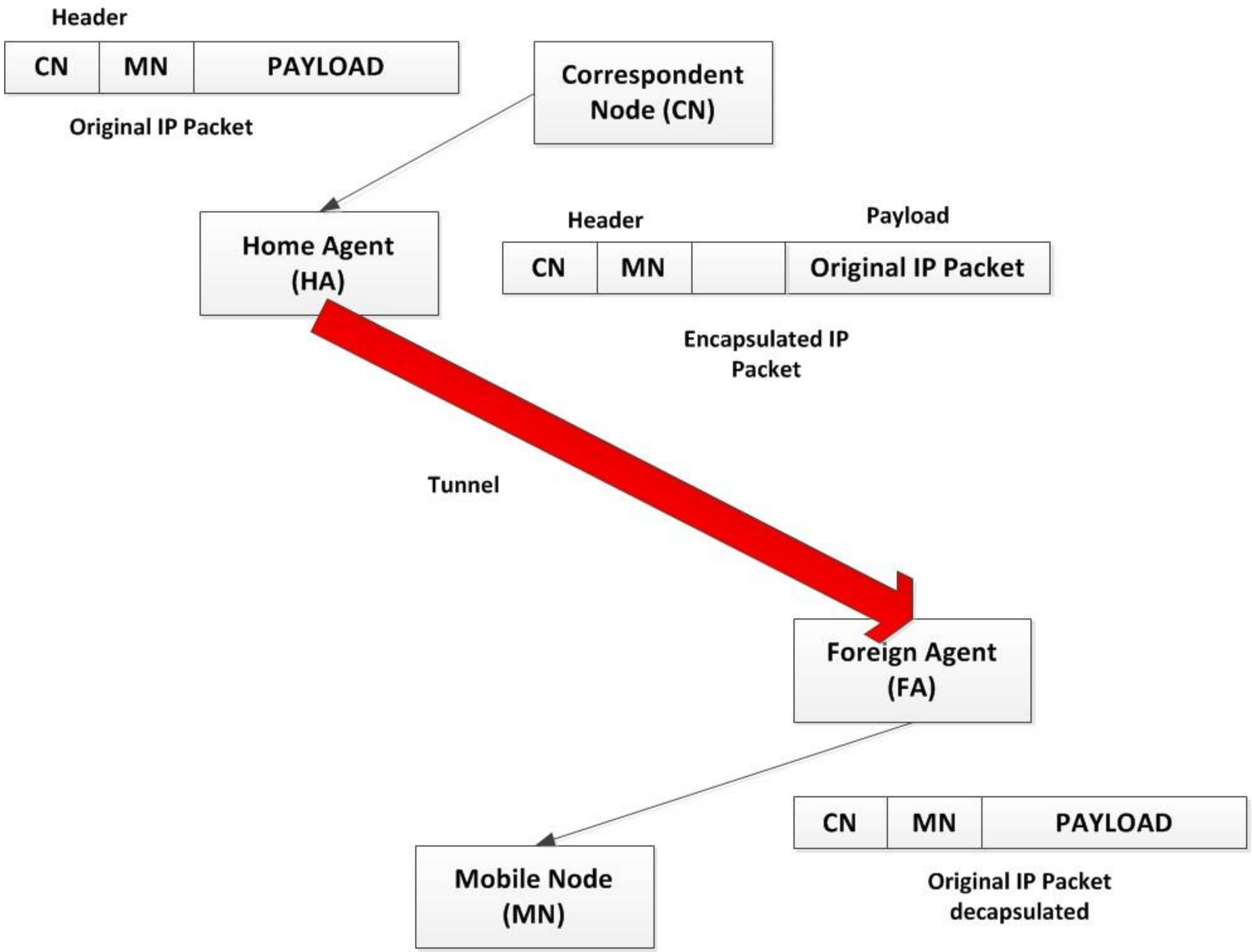
Tunneling

- HA receives IP packets sent to the mobile node's home address
- Home agent forwards and reroutes the packets to the care-of address via **tunneling**
- Tunneling involves **encapsulation of the IP packets**
- FA unpacks the packet and delivers it to the mobile host





Tunneling and Encapsulation

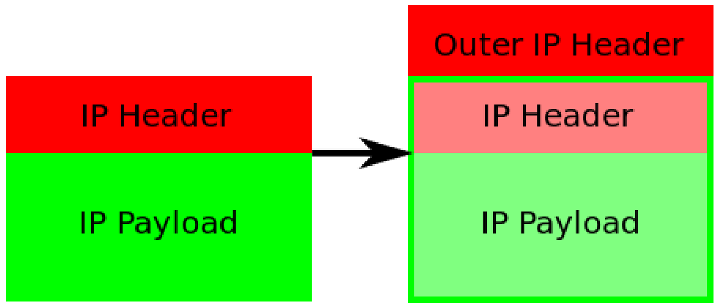


Mobile IP Encapsulation Options

- IP Encapsulation within IP

  (IP-in-IP)

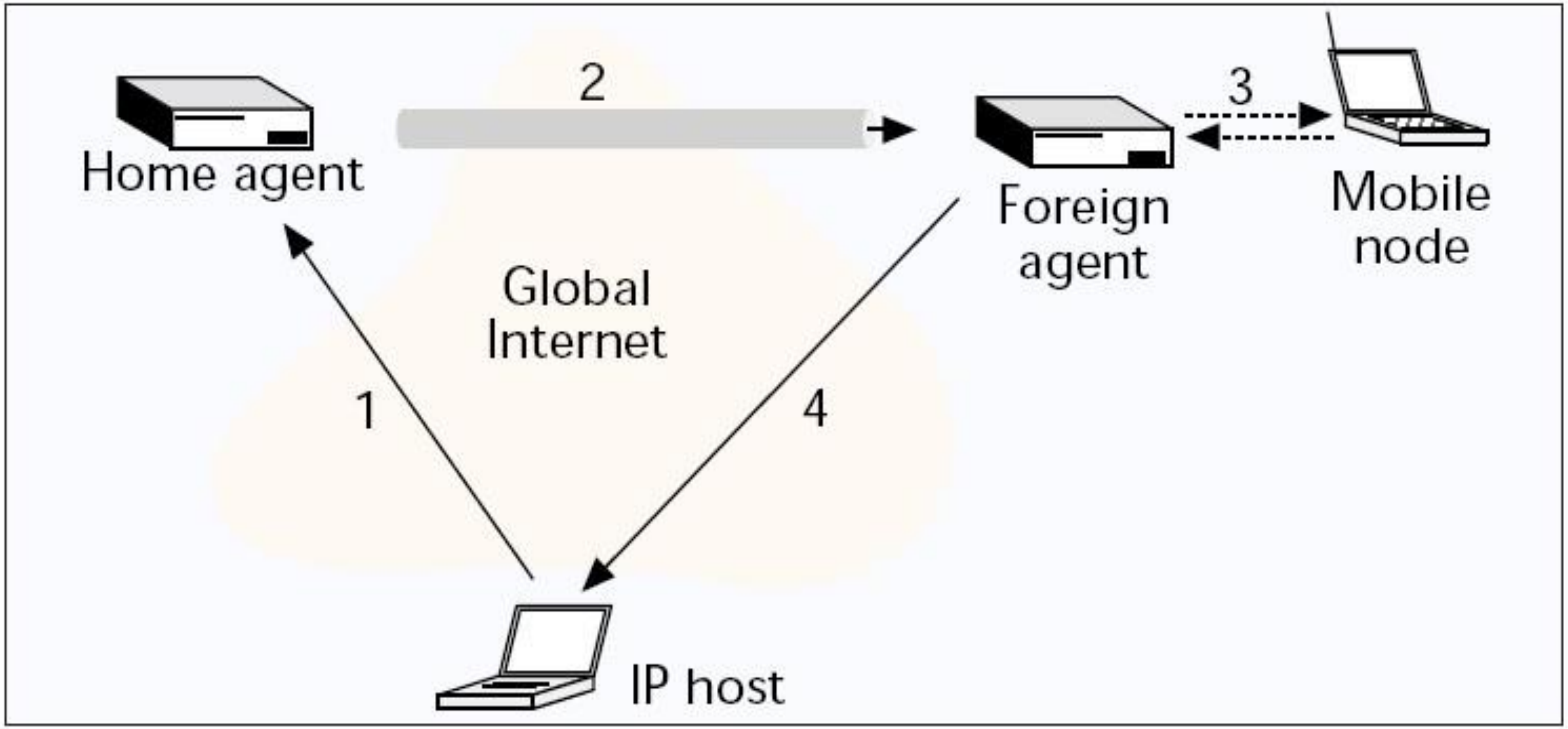
  – to take an IP packets and make it the payload of another IP packet
  – The new header specifies how to send the encapsulated packet to the mobile node's care-of address



- Minimal encapsulation (optional)

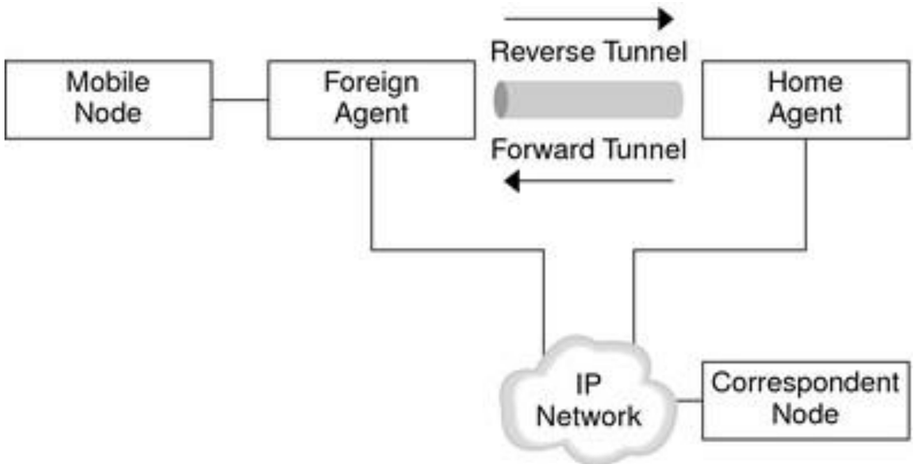
  – Avoids repetition of identical fields

Triangular Routing in IPv4



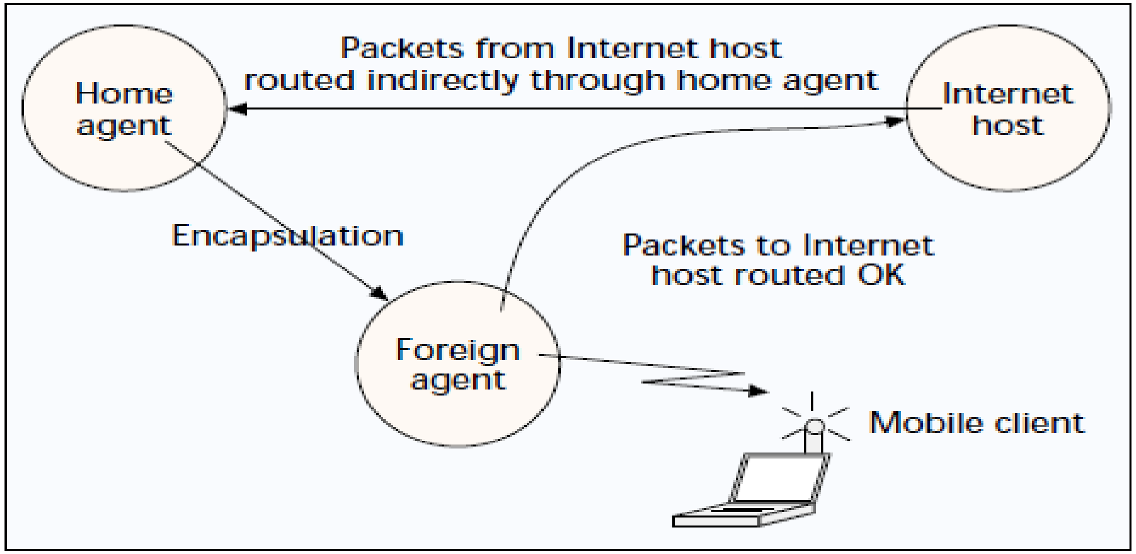
Reverse Tunneling

- **Ingress Filtering** is a security technique to ensure that incoming packets are from the networks they claim to be from
- Ingress filtering would force routers to drop packets from a mobile node which was communicating through a foreign network
  – Because packets would include the home address as the IP source
- To avoid this, **reverse tunneling** can be used
- FA will reverse tunnel packets to HA



Triangular Routing: Problem

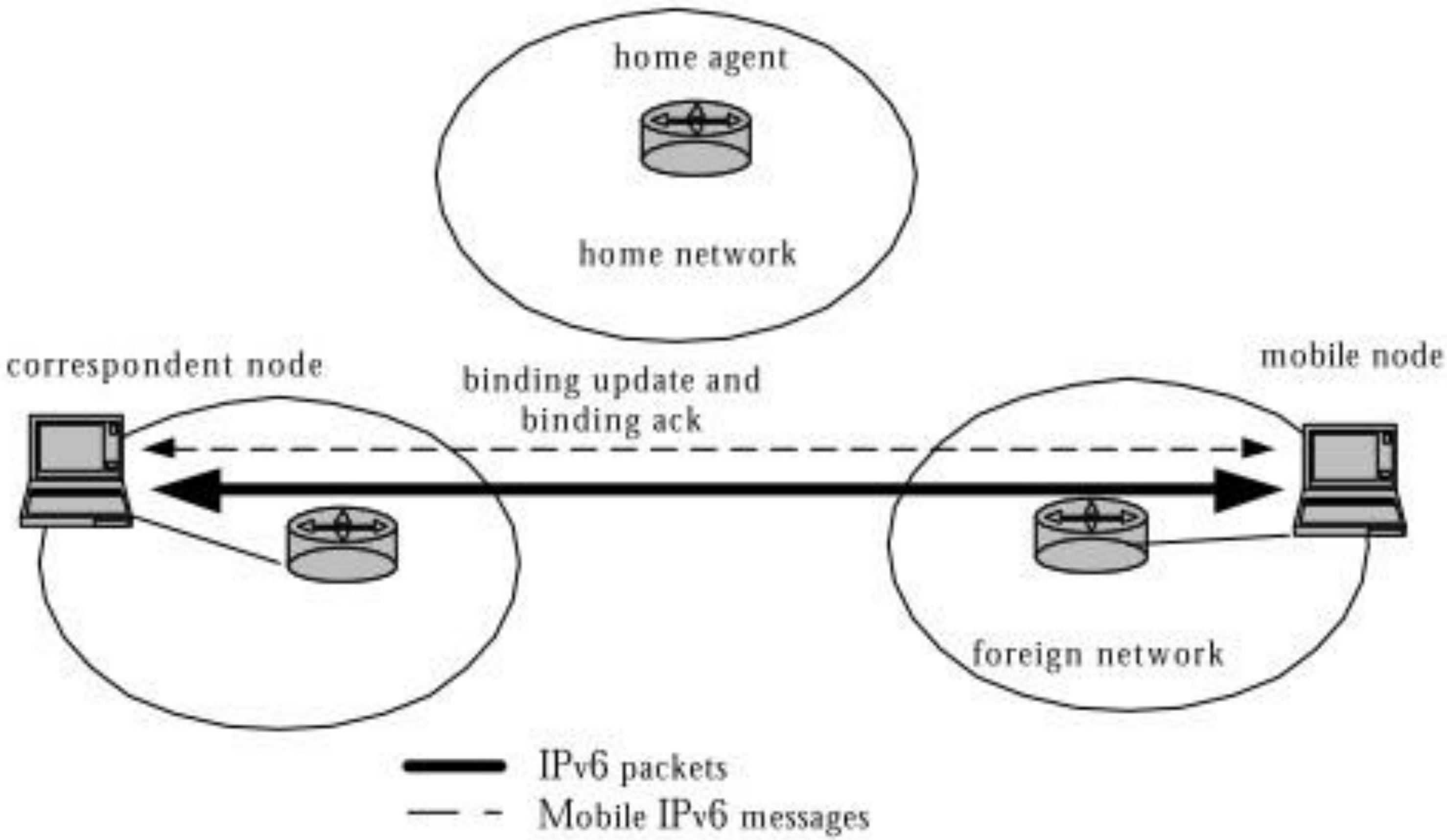
- Datagrams going to the mobile node have to travel through HA but datagrams from the mobile node to CNs can be routed directly to their destinations
- Increase response time
- Ingress Filtering
- How to eliminate triangular routing?



Route Optimization: Solution

- MN sends CN its **CoA** and **binding information**
  - Binding - the association between a mobile node’s home address and its care-of address, along with the remaining lifetime of that association
- **CN** performs binding of addresses (CoA and home address) and **directly communicates with MN** to avoid triangular routing and Ingress filtering issues
  - It allows the shortest communications path to be used
  - It also eliminates congestion at the mobile node's home agent
- Whenever **CoA changes**, MN sends CN a Binding Update message to update the CN’s binding cache
- **Fully supported in IPv6**

Using Route Optimization



Mobility in IPv6

- Route Optimization is a fundamental part of Mobile IPv6
  - MN communicating directly with CN, avoiding triangular routing
- Foreign Agents are not used in Mobile IPv6
- Care-of address is obtained via Stateless Auto-Configuration or DHCPv6
- Movement Detection
  - The primary movement detection mechanism for Mobile IPv6 uses the IPv6 Neighbor Discovery protocol
- Binding updates and Binding Caches
  - Binding is an integral part of IPv6
  - Binding update sent by HA and MN to CN’s
- IPSec is mandatory in IPv6

References

- Acknowledgement: some of the materials are borrowed from Week 7 lecture on Internet Mobility by Christer Åhlund from Lulea University of Technology
- Charles E. Perkins and David B. Johnson, Route Optimization for Mobile IP Understanding IP Addressing: Everything You Ever Wanted To Know, 3com
- Andrew Hines, Neighbour Discovery in IPv6
- George Coulouris, Jean Dollimore, and Tim Kindberg, Distributed Systems: Concepts and Design, 2011
- IPv6 http://www.ipv6.com/articles/general/ipv6-the-next-generation-internet.htm
- Oracle http://docs.oracle.com/cd/E18752_01/html/816-4554/mipoverview-5.htm
- Microsoft http://technet.microsoft.com/en-us/library/cc757359(v=ws.10).aspx
- Cisco http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html
- http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/mobile_ip/mobil_ip.html
- MobileIPv6 http://www.cu.ipv6tf.org/literatura/0201788977_ch03.pdf
- Wikipedia