Session 6D

Mobile IP and IPv6

Mouli Sankaran

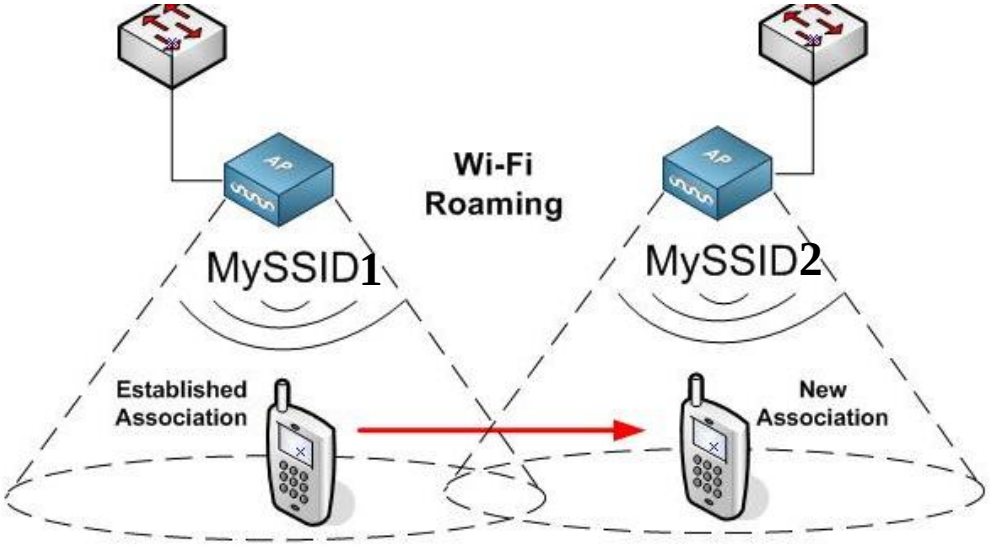
Session 6D: Focus

- Mobile IP
  - Mobile Hosts and Home Addresses
  - Home Agents and Foreign Agents
  - Routing to Mobile Hosts
  - IP Tunneling
  - Proxy ARP
- IPv6
  - Motivation and Design Goals
  - Addressing Conventions and Scheme
  - Header
  - Features

Course page where the course materials will be posted as the course progresses:

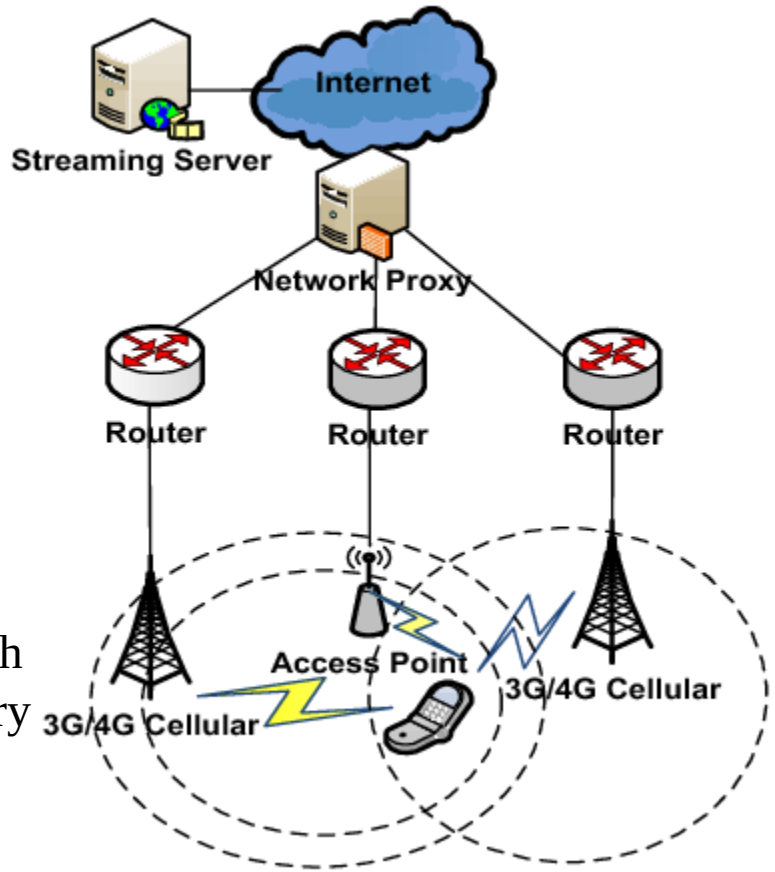
Mobile IP

Roaming Mobile Devices on Internet



Mobile devices moving from one hotspot to another.

Mobile devices moving from one BTS to another in 3G/4G Networks.



Note: It is not that only mobile devices transit through different networks, even laptops are also not stationary like desktops. In the college, your laptops connect to different WiFi routers on different subnets as you move across buildings or departments.

BTS: Base Transceiver Station

Routing among Mobile Devices

- It is very obvious that mobile devices present some challenges for the Internet architecture.
- The Internet was designed in an era when computers were large, immobile devices
- While the Internet's designers probably had some notion that mobile devices might appear in the future, it's fair to assume it was not a top priority to accommodate them.
- Today, of course, mobile computers are everywhere, notably in the forms of laptops and IP-enabled mobile phones, and increasingly in other forms such as sensors and IoT devices.
- Let us now look at some of the challenges posed by mobile devices connecting to Internet and some of the current approaches to accommodating them.

Mobile Devices on Internet

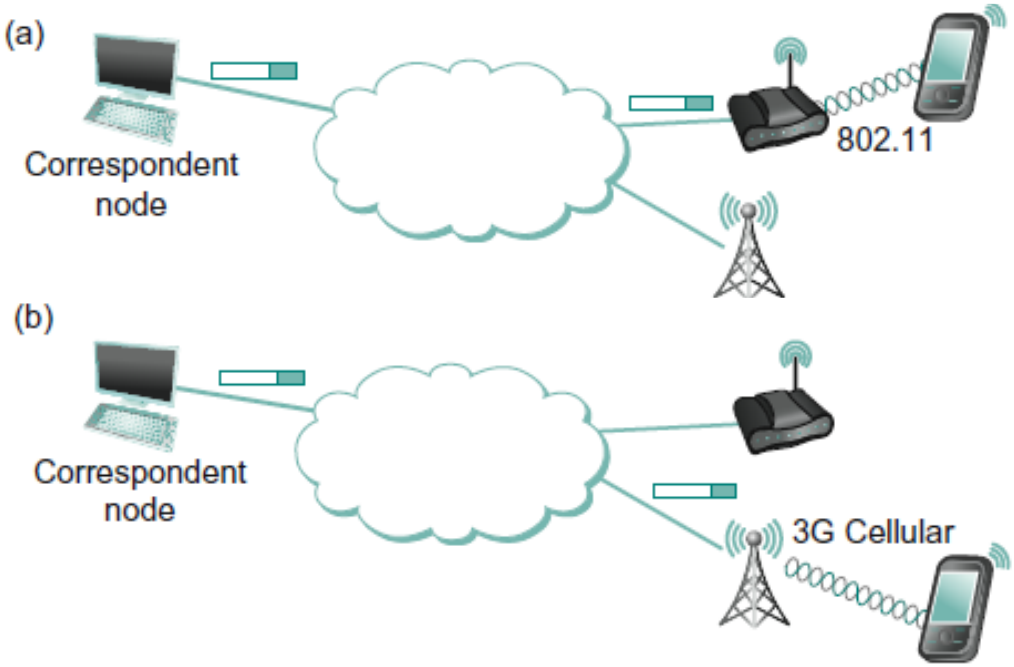
- Common ways mobile devices connect to Internet are:

1. Through cellular data networks (like 4G/5G) used for Internet access, VoIP calls, video calls, media streaming, etc.
2. Connecting through wireless hotspots (WiFi), Internet cafes, airport, or home supported by service providers.

- What do the mobiles devices need to communicate over Internet?
- A **unique IP address** for a mobile device to be recognized and for other hosts and routers on Internet to be in touch continuously with the mobile device, while it moves from one network to the other.
  - Scenario, while you are on a Skype call from the mobile, move from one hotspot to another or switch from WiFi to 3G network, without affecting the Skype call.

Connecting to a Hotspot and Moving Across .. contd.

- Consequently, in the absence of some other mechanism, packets would continue to be sent to the address where the mobile device used to be, not where it is now.
- As the mobile node moves from an 802.11 network to a cellular network, somehow packets from the **correspondent node** need to find their way to the new network and then on to the mobile node.



- Assuming that there is some way to redirect packets, another important concern is:
  - To prevent some attacker **impersonating** the device and redirecting the packets meant for the device.

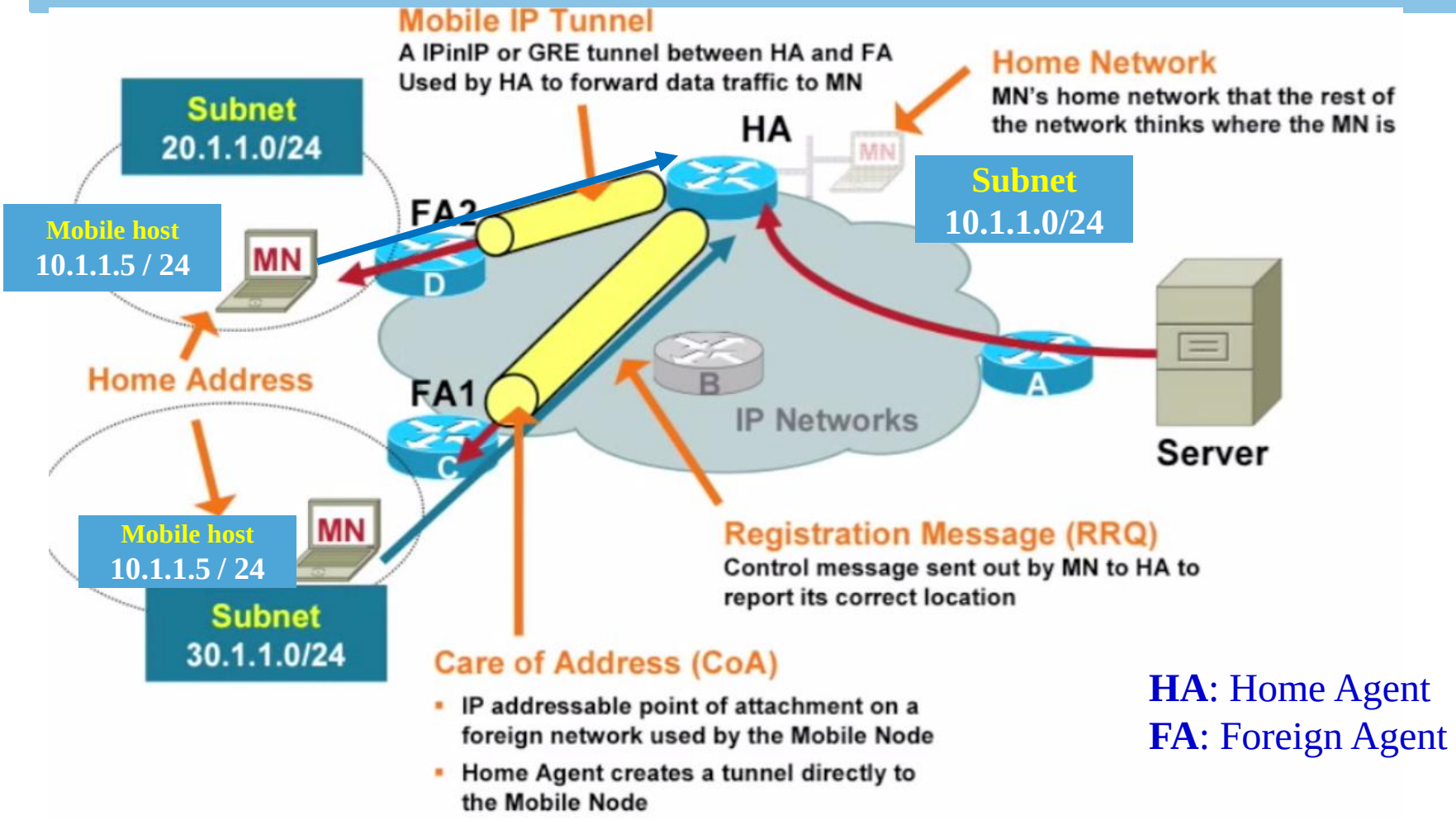
Impersonate: Pretend to be (another person) for entertainment or fraud

Mobility and Security are to be taken care of.

Correspondent node: The device which is having communication with a mobile device.

IP Tunneling (IP-in-IP)

IP Tunneling to Mobile Hosts

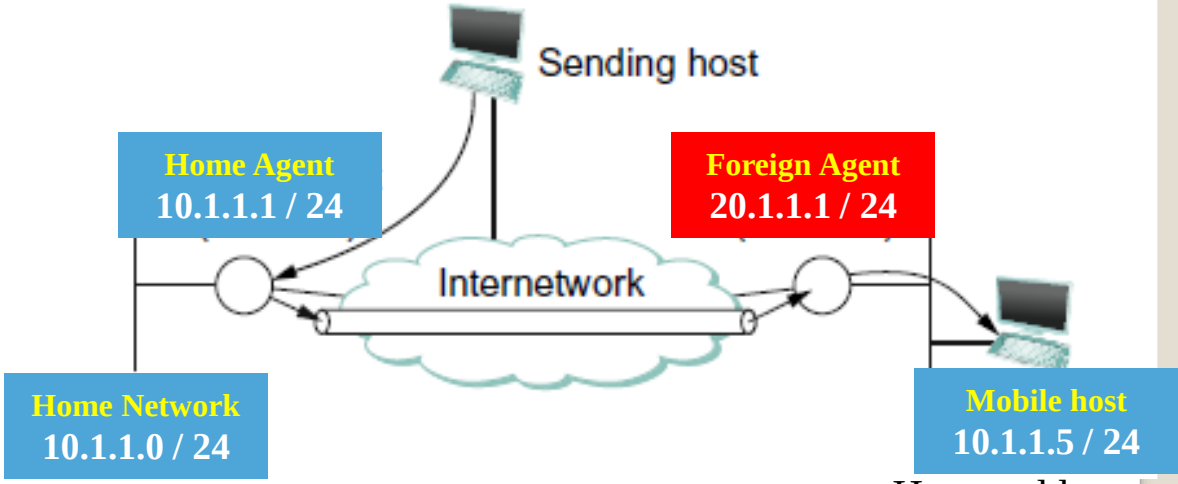


HA: Home Agent
FA: Foreign Agent

GRE: Generic Routing Encapsulation (**GRE** is a **tunneling** protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network

Mobile Hosts and Home Address

- The **mobile host** is assumed to have a permanent IP (10.1.1.5), called its **home address**, which has a network prefix equal to that of its **home network**.

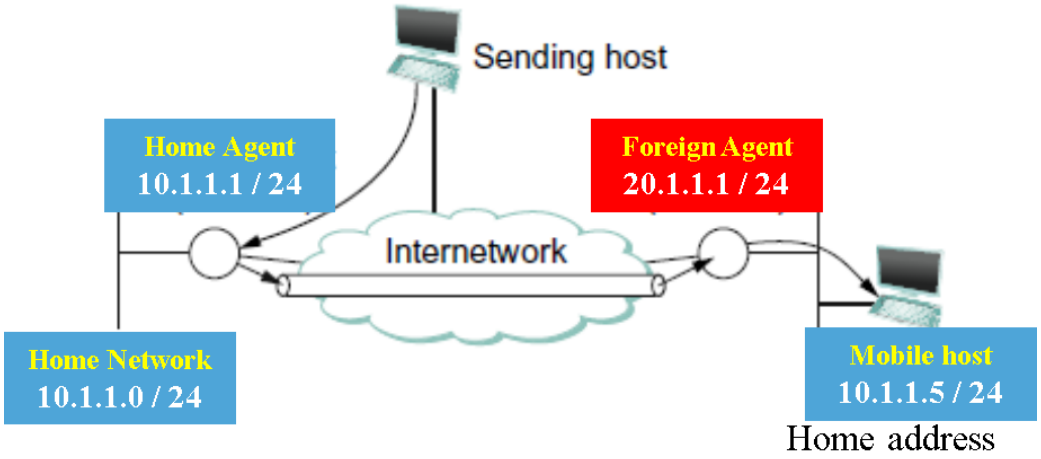


Home address

- This is the address that will be used by other hosts when they initially send packets to the mobile host;
- Because it does not change, it can be used by long-lived applications (TCP connections, voice/video calls, etc.) as the host roams.
- We can think of this as the long-lived identifier of the host.
- When the **host moves** to a new **foreign network** away **from** its **home network**, it registers with the foreign agent by providing its home network details along with home agent's address.

Mobile Host on Foreign Network

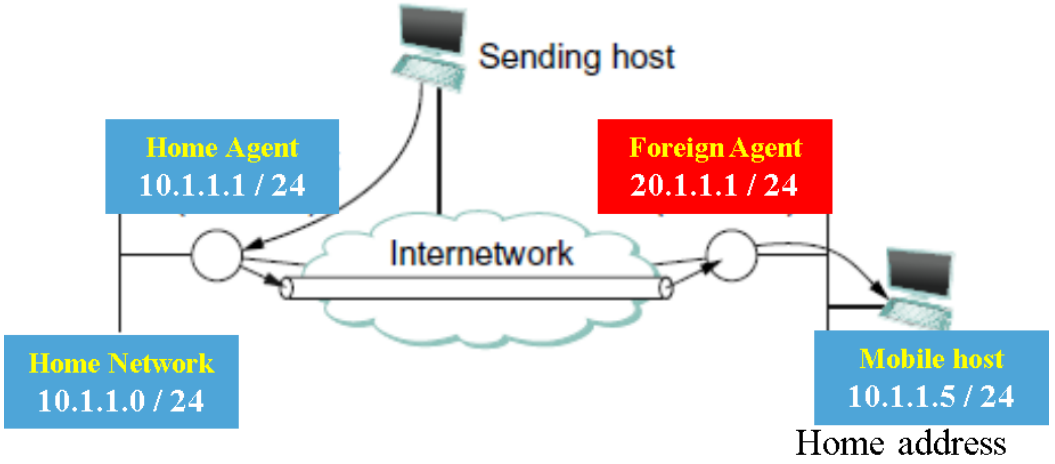
- It is important to note that the mobile host does not lose its permanent home address while it is on the foreign network.



- This home address is critical to its ability to sustain communications as it moves.
- While the routers in the core of the Internet remain unchanged, mobility support does require some new functionality in the routers in the home networks (**home agents)** of the mobile node and also the routers of the foreign networks (**Foreign agents**).
- This change is required for them to re-route the packets that arrive at the home agent to the mobile node in the foreign network through its current foreign agent.

Home Agents and Foreign Agents

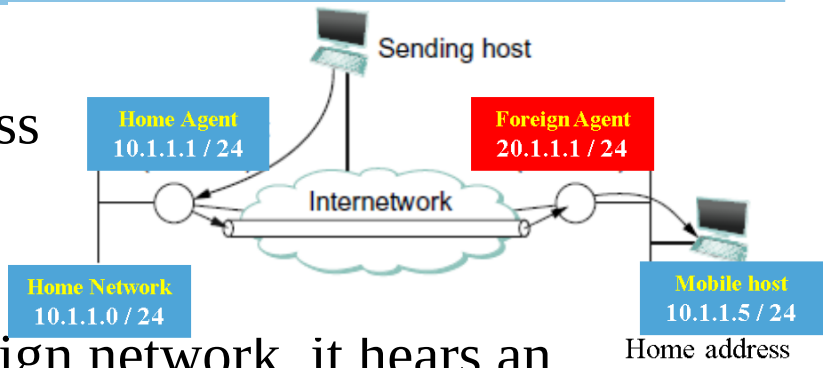
- **Home agent** is located on the home network of the mobile host.
- A second router with enhanced functionality is the **foreign agent** in the foreign network.



- Foreign agent is located on a network to which the mobile node attaches itself when it is away from its home network.
- Both home and foreign agents periodically announce their presence on the networks to which they are attached using agent advertisement messages.
- A mobile node may also solicit an advertisement when it attaches to a new network.

Steps taken by Mobile Host

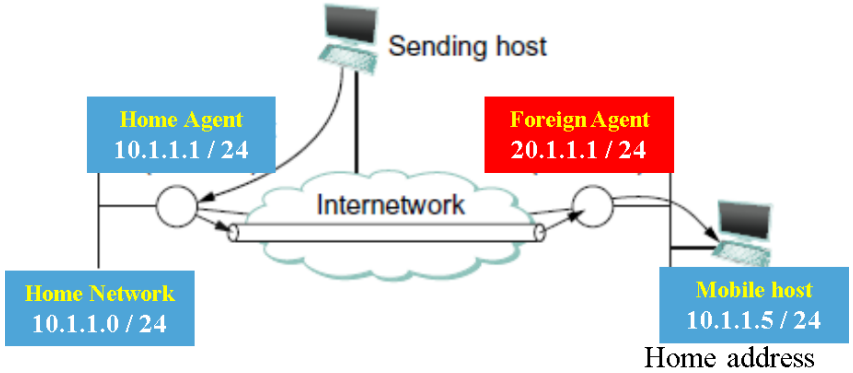
- The advertisement by the home agent enables a mobile host to learn the address (**10.1.1.1**) of its home agent before it leaves its home network.



- When the mobile host attaches to a foreign network, it hears an advertisement from a foreign agent and registers with the agent, providing the address of its home agent and its own IP address in its home network.
- The foreign agent then contacts the home agent, providing a **care-of address** (**its own address**) on behalf of the mobile device to its home agent.
  - This is the IP address (**12.1.1.1**) of the foreign agent.
- Since mobile host has a fixed home address, any device that tries to send a packet to the mobile host will always send it with a destination address equal to the home address of that node.
- Normal IP forwarding will cause that packet to arrive at the home network of the mobile node on which the **home agent** is part of (gateway).

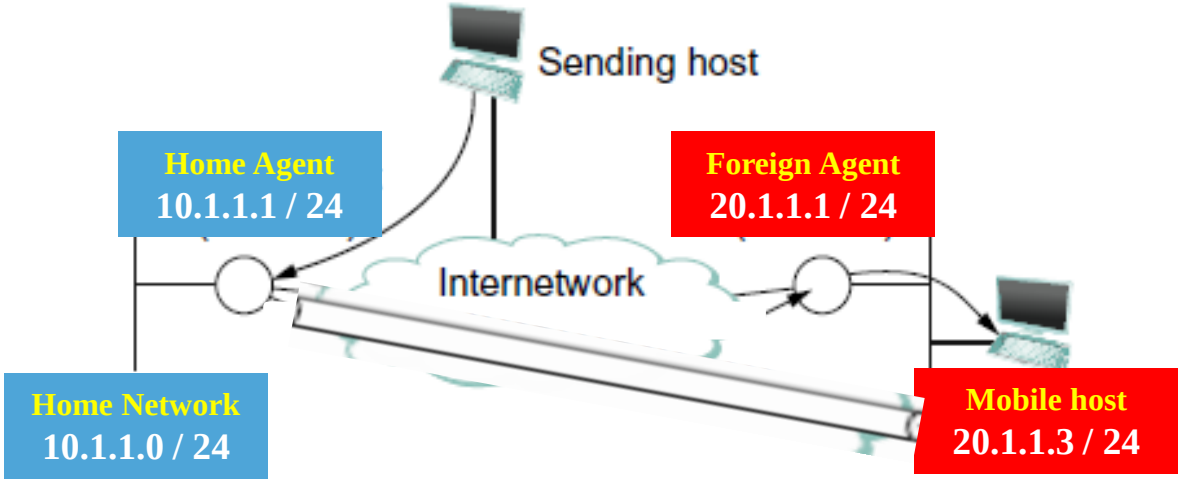
Three Parts of Delivering Pkts to Mobile Host

- Thus, we can divide the problem of delivering the packet to the mobile node into three parts:



1. How does the home agent intercept a packet that is destined for the mobile node?
   - The home agent is the default gateway of the home network and thus it must receive all the packets that are destined to the mobile node.
2. How does the home agent then deliver the packet to the foreign agent?
   - Since it has learnt about the current **care-of-address** of the mobile node, it prepares another IP packet to be delivered to foreign agent, by packing the original IP packet of mobile node and sends it out. – **IP Tunnelling**
3. How does the foreign agent deliver the packet to the mobile node?
   - The foreign agent is the default gateway of the foreign network and thus it must receive all the packets that are destined to the **foreign agent (FA)** and because of the mobile node's registration with it, FA can now deliver the original IP packet sent by the home agent by unpacking it and deliver it through the datalink layer (MAC address of mobile node) of the foreign network.

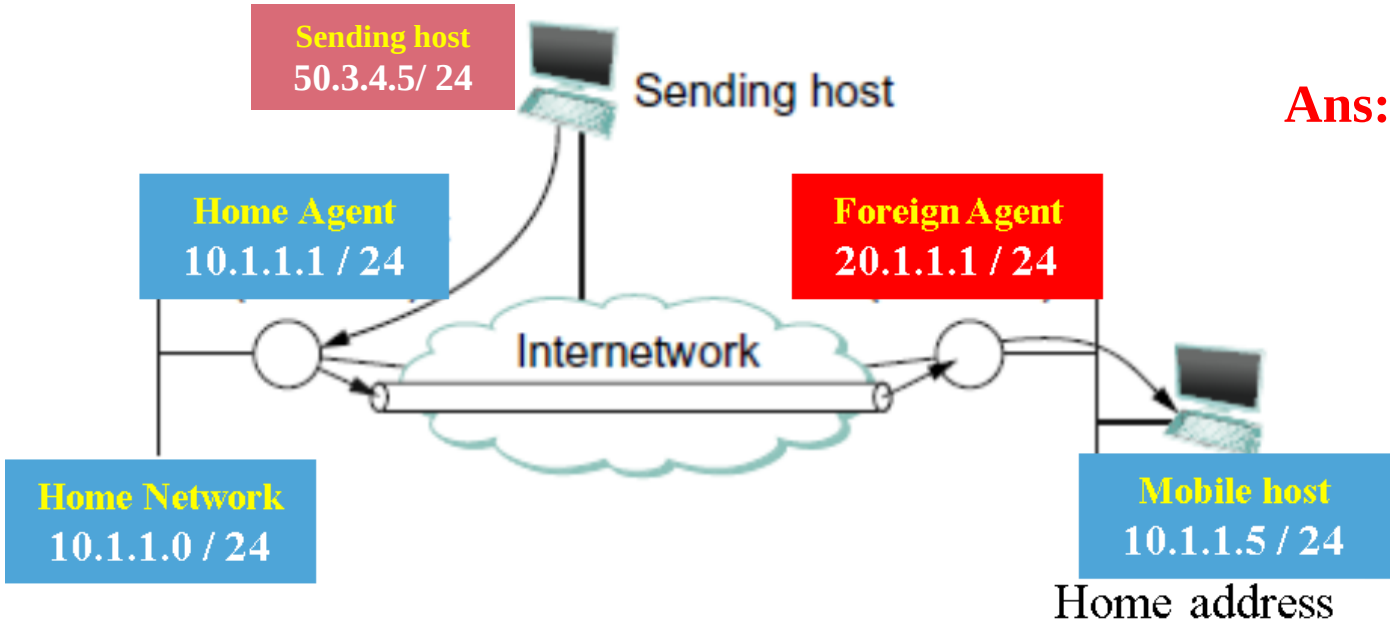
Co-located Care-of-address



Home address: 10.1.1.5/24

- **Another scenario** is where the mobile host gets a new IP address (**20.1.1.3**) in its current foreign network through DHCP.
- Here, the **mobile host** informs its **home agent** about its current **co-located care-of-address** in its current foreign network.
- In this case the **co-located care-of-address** is used by the Home Agent to forward the traffic destined to the mobile host directly.

Quiz 1: Mobile host from a Foreign Network

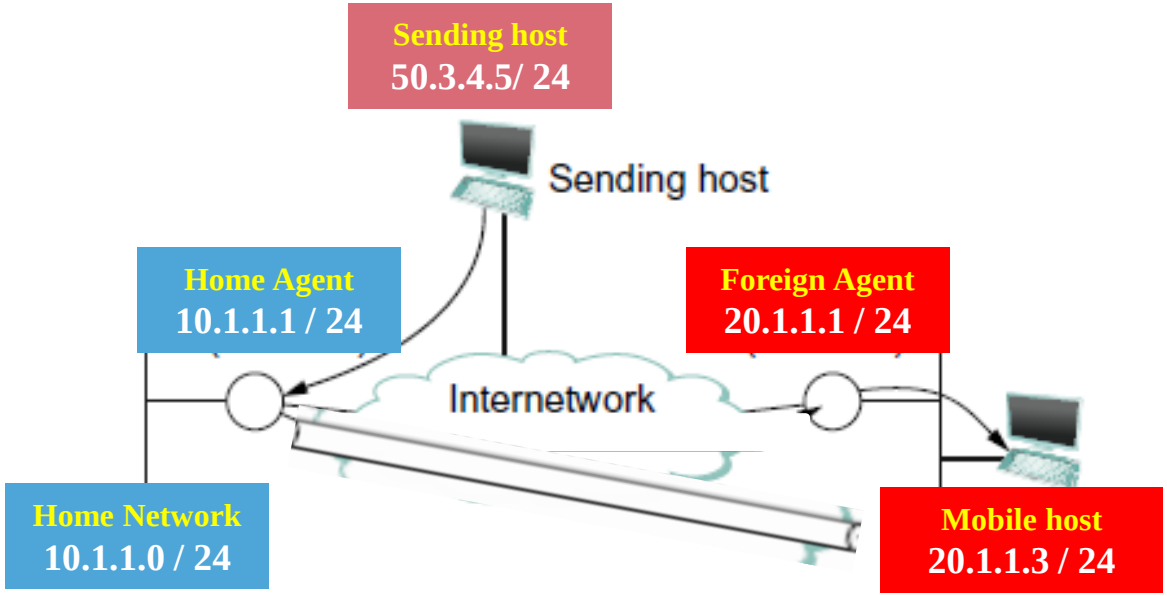


Ans: C

- When the mobile host from the current foreign network sends a packet to the sending host, the **Source IP** and **Destination IP** fields respectively would be:
  - A. Src: 10.1.1.5 and Dest: 20.1.1.1
  - B. Src: 10.1.1.5 and Dest: 10.1.1.1
  - C. Src 10.1.1.5 and Dest: 50.3.4.5
  - D. None of the given options is correct.

Note: The packets from the mobile node do not go through the home Agent, they go straight to the sending host. No IP tunneling is required. IP tunneling is only required to receive packets from the sending host by the mobile node.

Quiz 2: Sending host to a mobile node in a Foreign Network with a co-located care-of-address



Ans: B

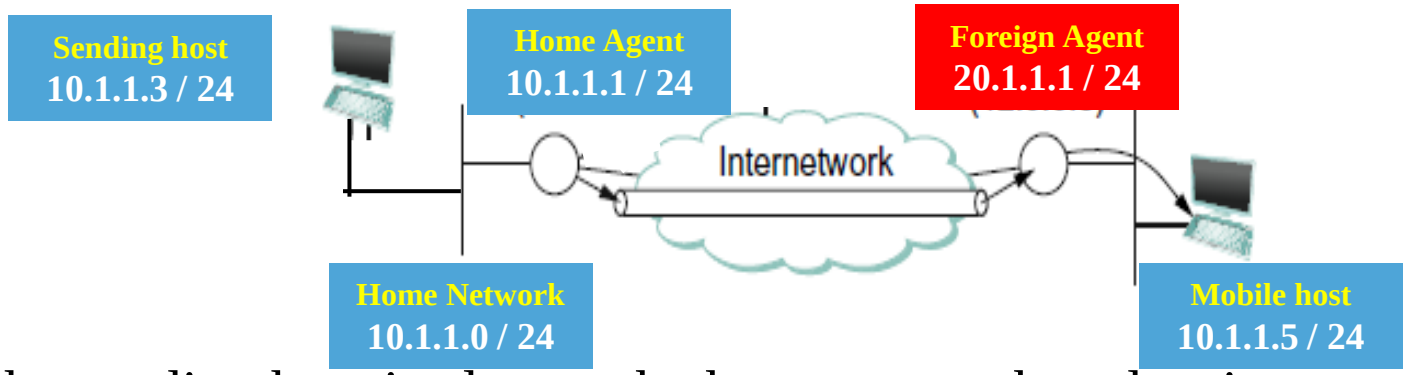
Home address: 10.1.1.5/24

- When the sending host sends a packet to the mobile node, the **Source IP** and **Destination IP** fields respectively would be:

A. Src: 50.3.4.5 and Dest: 20.1.1.3
B. Src: 50.3.4.5 and Dest: 10.1.1.5
C. Src 50.3.4.5 and Dest: 10.1.1.1
D. Src 50.3.4.5 and Dest: 20.1.1.1.

Note: Even if the mobile node has been assigned A new IP address in its foreign network, the Sending host is not aware of it is current location, tt continues to send the packets to its original Home address. It is intercepted by the HA and IP tunneling is done directly to the Mobile node to its co-located care-of-address.

Proxy ARP: Sending Hosts in the Home Network



- If the sending host is also on the home network and trying to contact the mobile host, then the packets from it would never reach the mobile host, since the mobile host is not currently in the home network.
- To address this problem, the home agent actually impersonates the mobile node, using a technique called **proxy ARP**.
- It works same as ARP except that the home agent inserts the MAC address of its own, in its ARP response, impersonating the mobile node.
- So, the packets from the sending host first reaches the home agent:
  - which takes care of tunneling it to the mobile node through its current care-of-address of foreign agent or directly to the co-located care-of-address, which the sending host needn't be aware of.

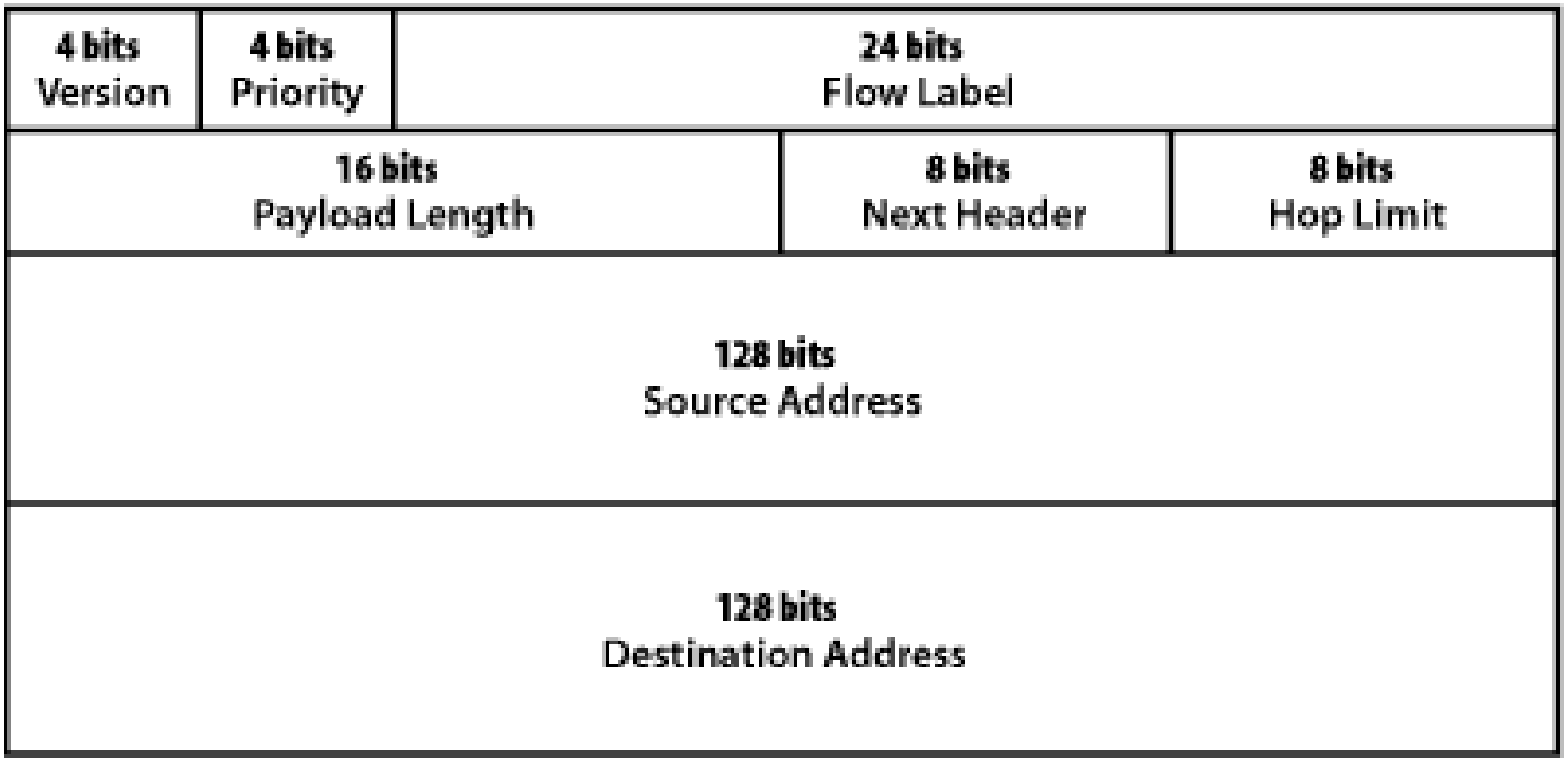
IPv6 or IPng

IPng: IP Next Generation

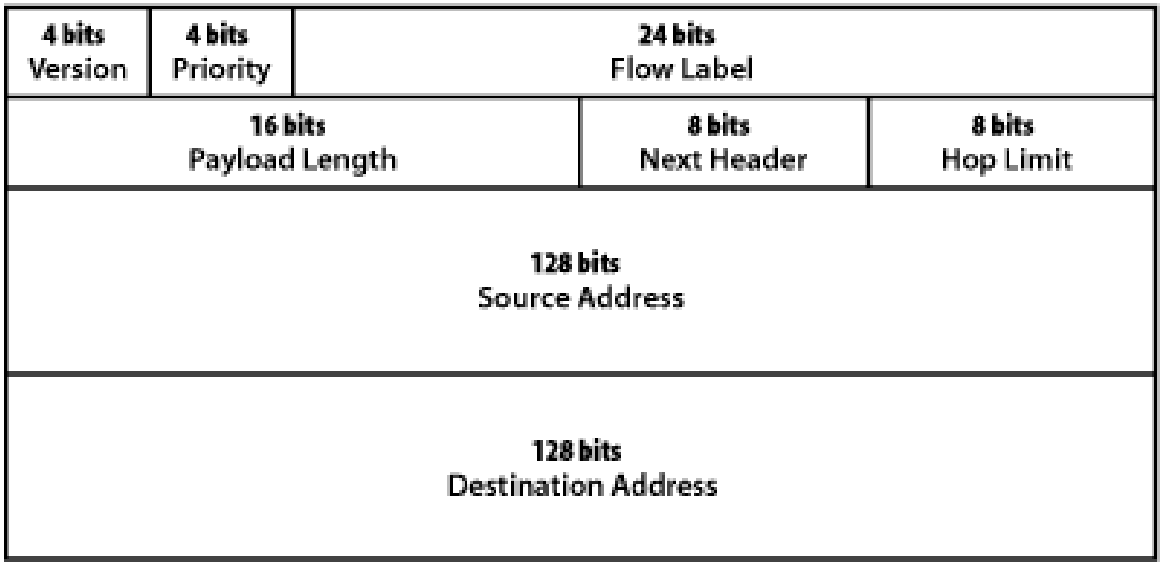
IPv6 Motivation: Design Goals

- **Address Space Expansion**: IPv6 provides a 128-bit address space (300 trillion trillion trillion unique addresses).
- **Simplified Header Format**: More efficient, improving routing performance and making the packet processing faster.
- **Built-in Security**: Unlike IPv4, IPSec is a mandatory feature in IPv6, and integrated into it, enabling end-to-end encryption and authentication at the network layer. – IPSec will be covered soon.
- **Improved Support for Mobility and Multicast**: IPv6 offers native support for mobile IP and more efficient multicast and **anycast** communication. No support for broadcast.
- **Auto-configuration** (Stateless Address Autoconfiguration - SLAAC): Devices can automatically generate their own IP addresses, simplifying network configuration without relying on DHCP.
  - **Router Advertisement (RA)** message from gateway gives its network prefix (e.g., 2001:db8:abcd:1234::/64) and auto-configure their address using SLAAC, device uses this prefix and appends its interface identifier (MAC) having an unique IPv6 address for itself.

IPv6 Header


4 bits
Version
4 bits
Priority
24 bits
Flow Label
16 bits
Payload Length
8 bits
Next Header
8 bits
Hop Limit
128 bits
Source Address
128 bits
Destination Address

IPv6 Header Fields



QoS: Quality of Service

Note: The **network prefix** is inferred from:
Routing tables, Interface Configurations,
Router Advertisements (RAs)
It is not part of the IPv6 header.
Though **/64** is common **NW prefix** it can be different.

- **Version**: Indicates the IP version; always set to **6** for **IPv6**.
- **Traffic Class**: Used for **prioritizing packets** and specifying **QoS**.
- **Flow Label**: Identifies **flows of packets** for special handling like real-time services.
- **Payload Length**: Specifies the **length of the data** following the header (in bytes).
- **Next Header**: Indicates the **type of the next header**, such as TCP, UDP, or extension headers.
- **Hop Limit**: Limits packet lifetime by **decrementing at each hop**; replaces IPv4's TTL.
- **Source Address**: The **IPv6 address of the sender**.
- **Destination Address**: The **IPv6 address of the receiver**.

IPv6 Addressing Conventions

- IPv6 addresses are 128 bits long, represented in **8 groups of 16-bit hexadecimal blocks**, separated by colons (:).
  - **Example: 2001:0db8:0000:0000:0000:ff00:0042:8329**
- **Zero compression**: A single contiguous sequence of all-zero blocks can be replaced with :: **only once** in the address.
  - **Example: 2001:0db8::ff00:0042:8329**

Only once, to avoid ambiguity on the number of zeros in it.

- Leading zeros in each block can be omitted.
  - **Example: 2001:db8::ff00:42:8329**
- IPv6 uses CIDR-style prefix length to denote subnetting, written as /n
  - **Example**: **2001:db8::223:45/64** the **first 64 bits are the network prefix**.
  - **Network ID: 2001:db8::/64**
  - **Host ID: ::223:45 (or 0000:0000:0223:0045 in full)**
- **Multicast ff00::/8**
- **Loopback ::1**

Note: Only one loopback address in IPv6, not a block of loopback addresses as in IPv4

IPv6 Addressing Scheme

- **Global Unicast**: Publicly routable addresses on the Internet, **e.g., 2001:db8::34:13** **Note**: Need to **start** with **binary 001** or in the **2000::/3 range**
- **Link-Local Unicast**: Used for communication within the same link (not globally routed), **e.g., fe80::45:21**
- **Unique Local Address** (ULA): Private addressing within an organization, not routed on the Internet, **e.g., fd00::abcd**
- **Multicast**: One-to-many communication, sent to all subscribed interfaces, **e.g., ff02::34** (all nodes on local link).
- **Anycast**: Same **public IP address** is assigned to multiple devices; delivered to the nearest one, **e.g., a DNS resolver with 2001:db8::53**
- **Loopback**: Refers to the local device, used for testing, **e.g., ::1**
- **Unspecified Address**: Used when an address is not yet assigned (e.g., during DHCPv6), **e.g., ::**

Note: NAT is not required in IPv6, though private IP addresses are used for local use.
Note: Anycast is used for specific services like DNS, for CDN edge servers, etc.

IPv6: Salient Features

- **Larger address space:**
  - Global reachability and flexibility
  - Aggregation
  - Multihoming
  - Autoconfiguration
  - Plug-and-play
  - End-to-end without NAT
  - Renumbering
- **Mobility and security:**
  - Mobile IP RFC-compliant
  - IPsec mandatory (or native) for IPv6
- **Simpler header:**
  - Routing efficiency
  - Performance and forwarding rate scalability
  - No broadcasts
  - No checksums
  - Extension headers
  - Flow labels
- **Transition richness:**
  - Dual stack
  - 6to4 and manual tunnels
  - Translation

Note: No **IP header checksum**, because of **mandatory support for IPSec** in **IPv6**

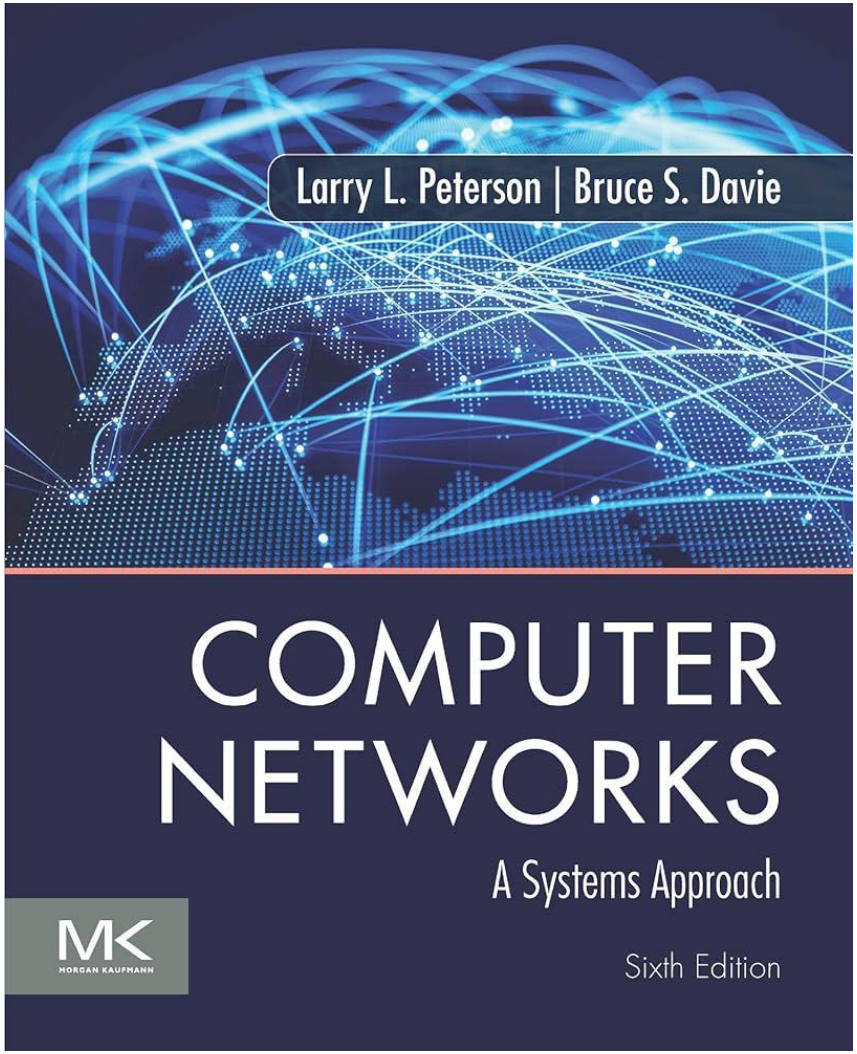
Session 6D: Summary

- Mobile IP
  - Mobile Hosts and Home Addresses
  - Home Agents and Foreign Agents
  - Routing to Mobile Hosts
  - IP Tunneling
  - Proxy ARP
- IPv6
  - Motivation and Design Goals
  - Addressing Conventions and Scheme
  - Header
  - Features

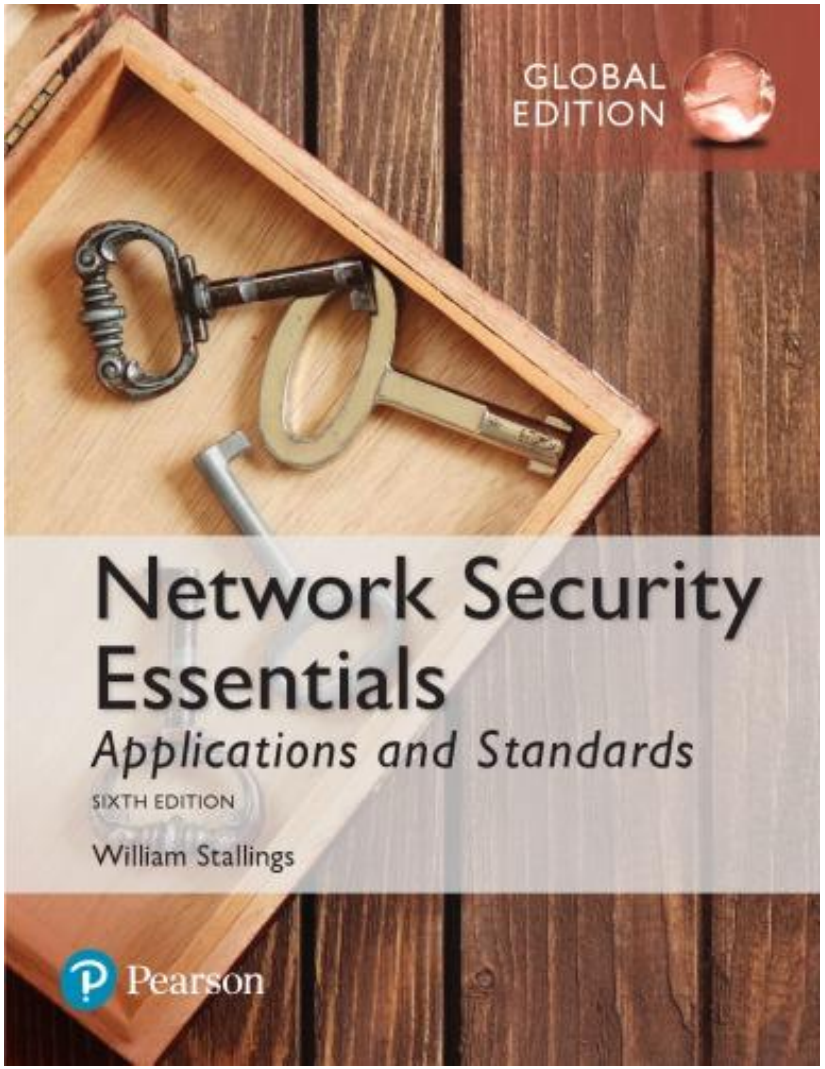
Course page where the course materials will be posted as the course progresses:

Textbooks

Textbook 1

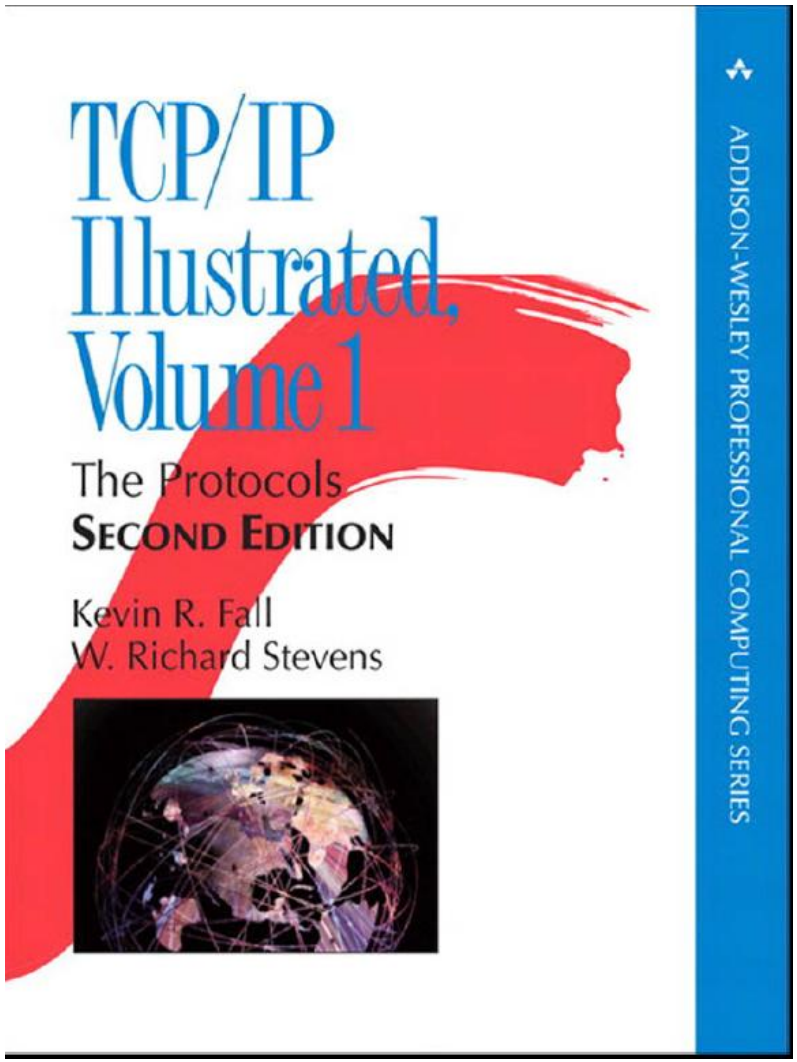


Textbook 2



References

Ref 1



Ref 2

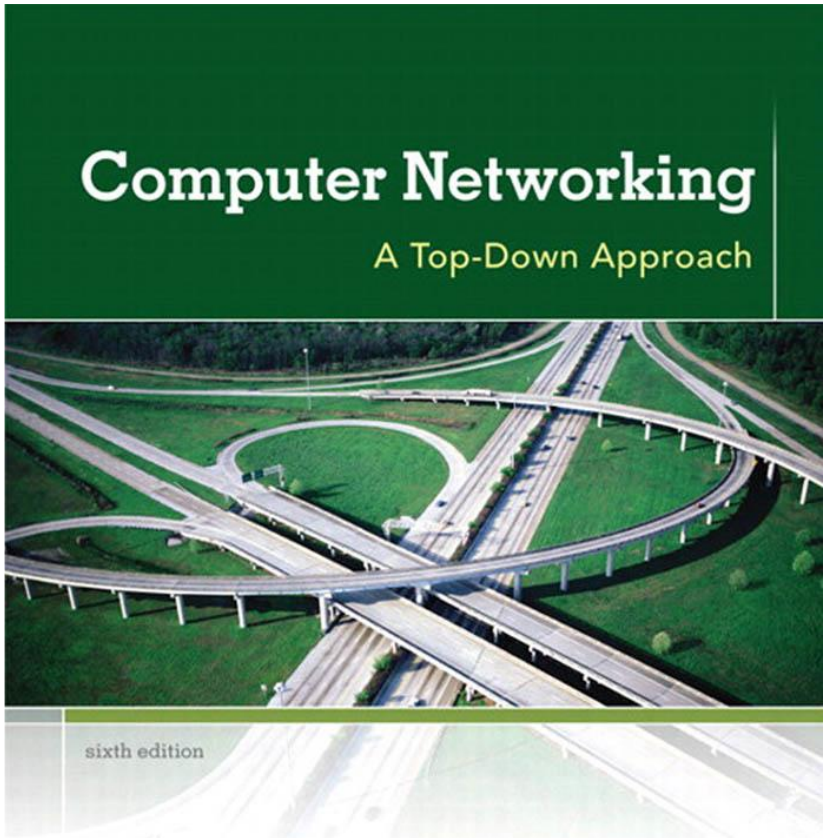
TCP Congestion Control: A Systems Approach

TCP Congestion Control: A Systems Approach

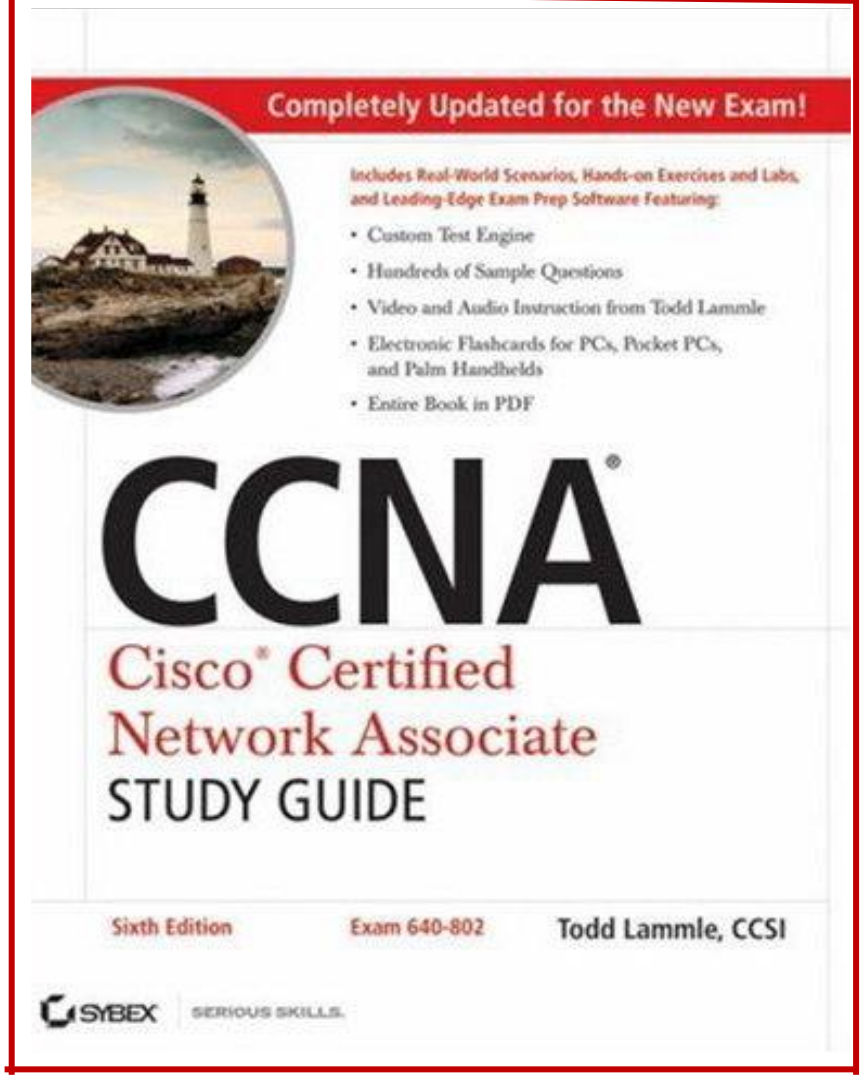
Peterson, Brakmo, and Davie

References

Ref 3



Ref 4



References

Ref 5