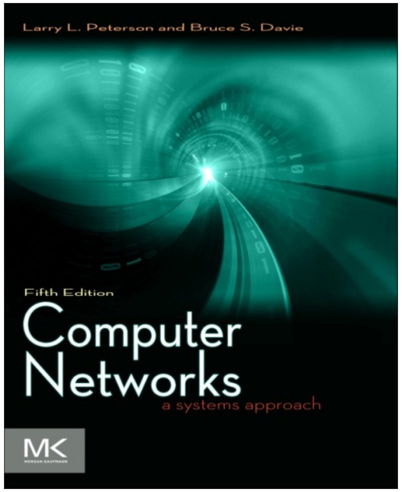


Chapter 4

Advanced Internetworking

Problems

- How do we build a routing system that can handle hundreds of thousands of networks and billions of end nodes?
- How to handle address space exhaustion of IPV4?
- How to enhance the functionalities of Internet?

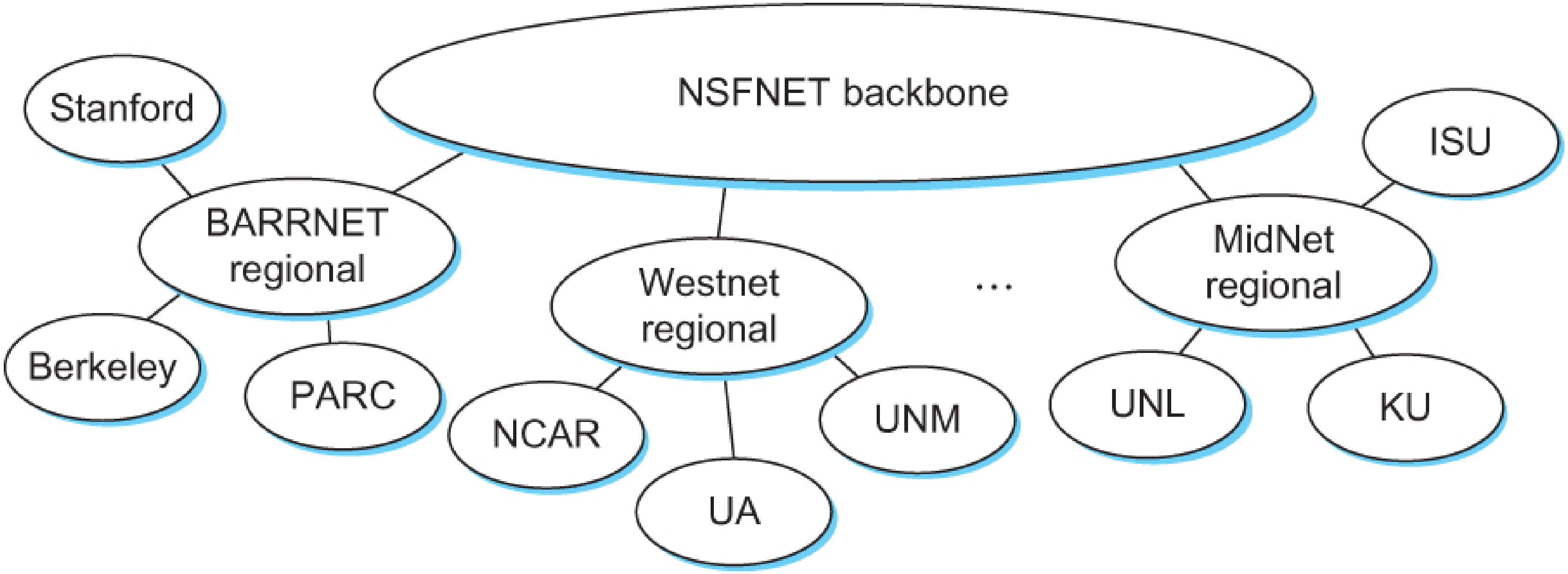
Chapter Outline

- Global Internet
- Mobile IP

Chapter Goal

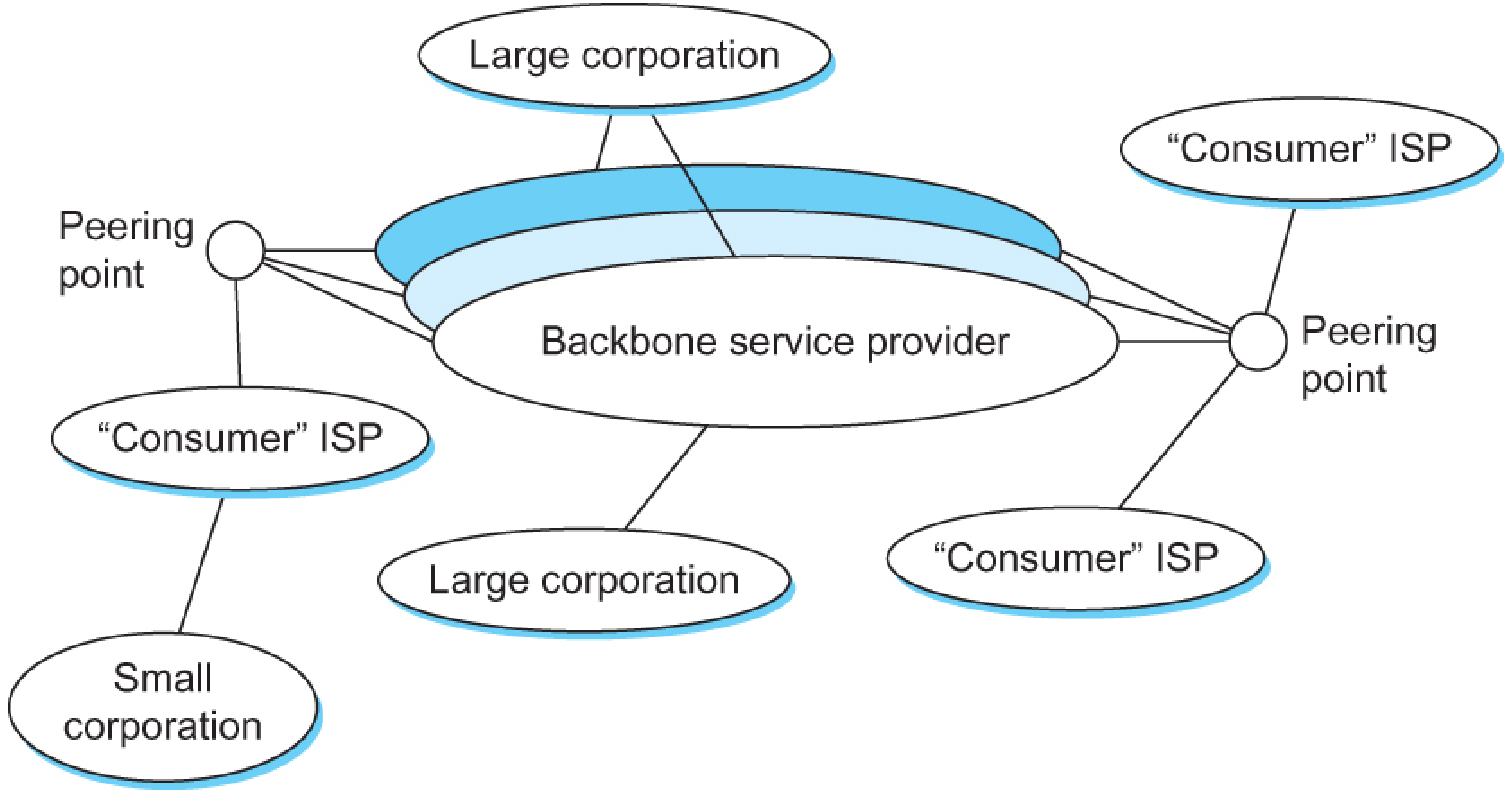
- Understanding the scalability of routing in the Internet
- Discussing IPv6
- Discussing Mobile IP

The Global Internet



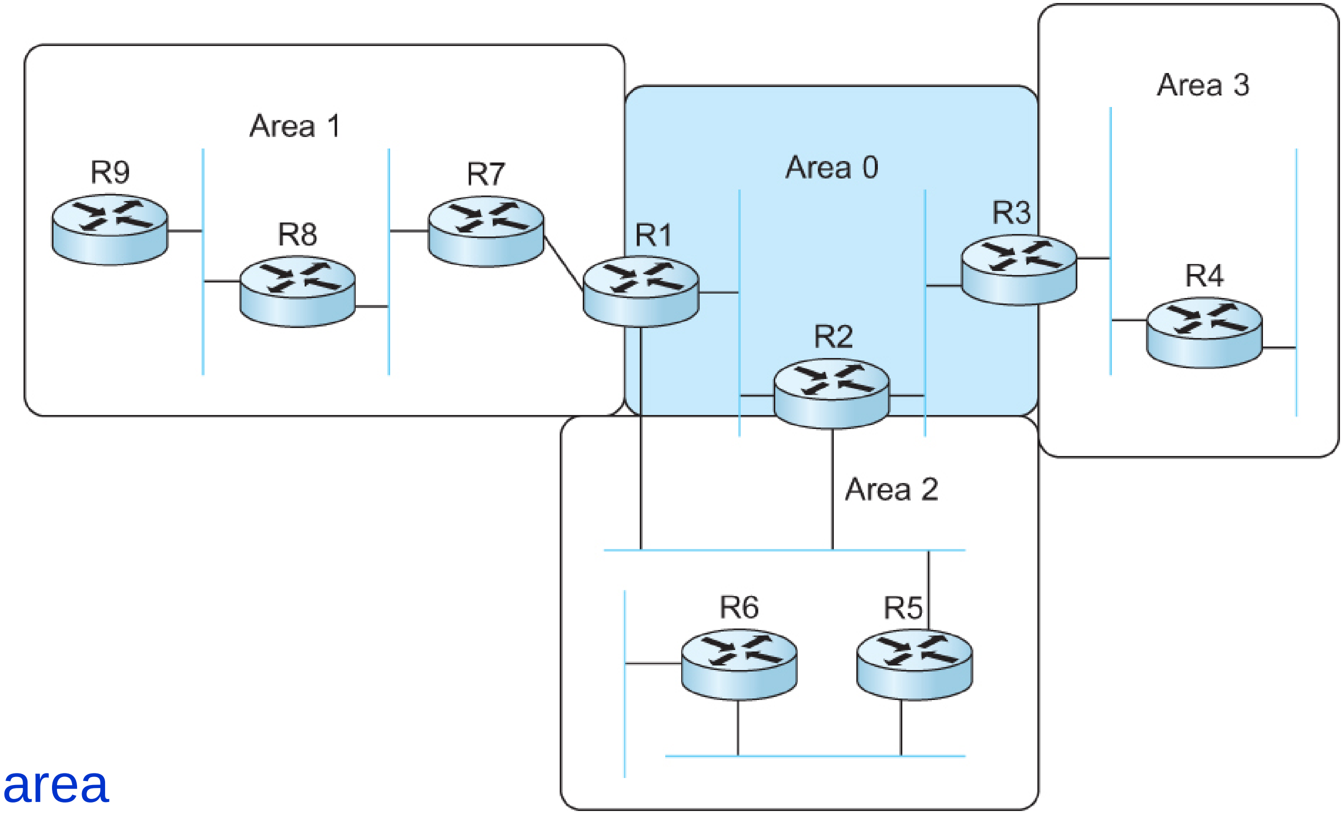
The tree structure of the Internet in 1990

The Global Internet



A simple multi-provider Internet

Routing Areas



Backbone area

Area border router (ABR)

A domain divided into area

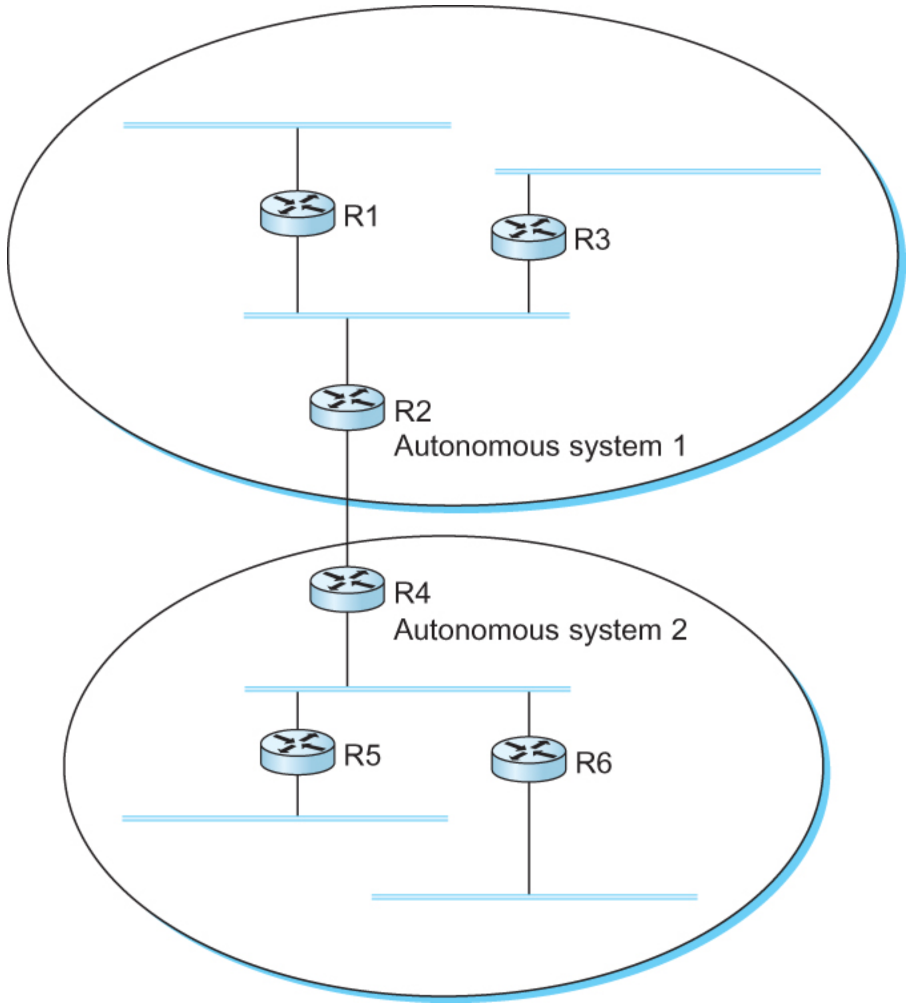
Interdomain Routing (BGP)

- Internet is organized as autonomous systems (AS) each of which is under the control of a single administrative entity

- Autonomous System (AS)
  - corresponds to an administrative domain
  - examples: University, company, backbone network

- A corporation's internal network might be a single AS, as may the network of a single Internet service provider

Interdomain Routing



A network with two autonomous system

Route Propagation

- Idea: Provide an additional way to hierarchically aggregate routing information is a large internet.
  - Improves scalability
- Divide the routing problem in two parts:
  - Routing within a single autonomous system
  - Routing between autonomous systems
- Another name for autonomous systems in the Internet is routing domains
  - Two-level route propagation hierarchy
    - Inter-domain routing protocol (Internet-wide standard)
    - Intra-domain routing protocol (each AS selects its own)

EGP and BGP

- Inter-domain Routing Protocols
  - Exterior Gateway Protocol (EGP)
    - Forced a tree-like topology onto the Internet
    - Did not allow for the topology to become general
      - Tree like structure: there is a single backbone and autonomous systems are connected only as parents and children and not as peers
  - Border Gateway Protocol (BGP)
    - Assumes that the Internet is an arbitrarily interconnected set of ASs.
    - Today's Internet consists of an interconnection of multiple backbone networks (they are usually called service provider networks, and they are operated by private companies rather than the government)
    - Sites are connected to each other in arbitrary ways

BGP

- Some large corporations connect directly to one or more of the backbone, while others connect to smaller, non-backbone service providers.
- Many service providers exist mainly to provide service to “consumers” (individuals with PCs in their homes), and these providers must connect to the backbone providers
- Often many providers arrange to interconnect with each other at a single “peering point”

BGP-4: Border Gateway Protocol

- Assumes the Internet is an arbitrarily interconnected set of AS's.
- Define *local traffic* as traffic that originates at or terminates on nodes within an AS, and *transit traffic* as traffic that passes through an AS.
- We can classify AS's into three types:
  - *Stub AS*: an AS that has only a single connection to one other AS; such an AS will only carry local traffic (*small corporation in the figure of the previous page*).
  - *Multihomed AS*: an AS that has connections to more than one other AS, but refuses to carry transit traffic (*large corporation at the top in the figure of the previous page*).
  - *Transit AS*: an AS that has connections to more than one other AS, and is designed to carry both transit and local traffic (*backbone providers in the figure of the previous page*).

BGP

- The goal of Inter-domain routing is to find any path to the intended destination that is loop free
  - We are concerned with reachability than optimality
  - Finding path anywhere close to optimal is considered to be a great achievement
- Why?

BGP

- Scalability: An Internet backbone router must be able to forward any packet destined anywhere in the Internet
  - Having a routing table that will provide a match for any valid IP address
- Autonomous nature of the domains
  - It is impossible to calculate meaningful path costs for a path that crosses multiple ASs
  - A cost of 1000 across one provider might imply a great path but it might mean an unacceptable bad one from another provid
- Issues of trust
  - Provider A might be unwilling to believe certain advertisements from provider B

BGP

Each AS has:

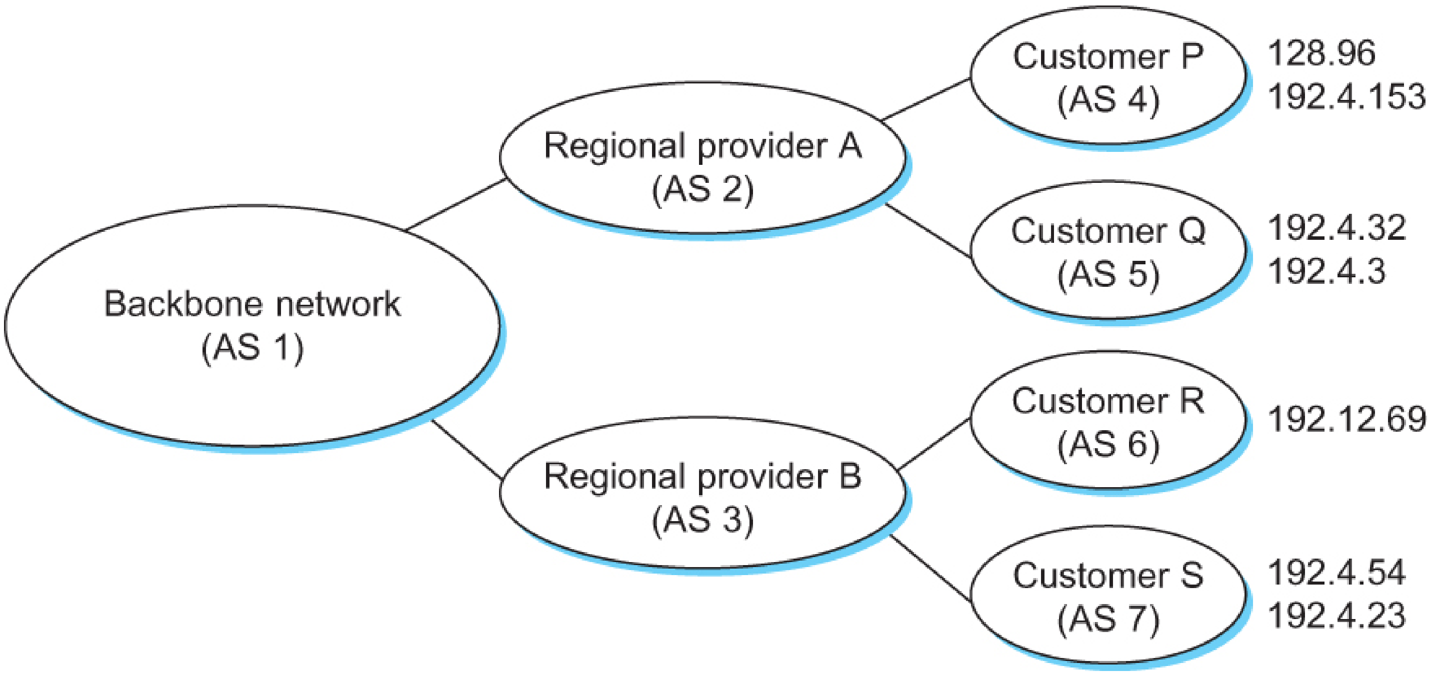
- One BGP *speaker* that advertises:
  - local networks
  - other reachable networks (transit AS only)
  - gives *path* information
- In addition to the BGP speakers, the AS has one or more border “gateways” which need not be the same as the speakers
- The border gateways are the routers through which packets enter and leave the AS

BGP

- BGP does not belong to either of the two main classes of routing protocols (distance vectors and link-state protocols)

- BGP advertises *complete paths* as an enumerated lists of ASs to reach a particular network

BGP Example



Example of a network running BGP

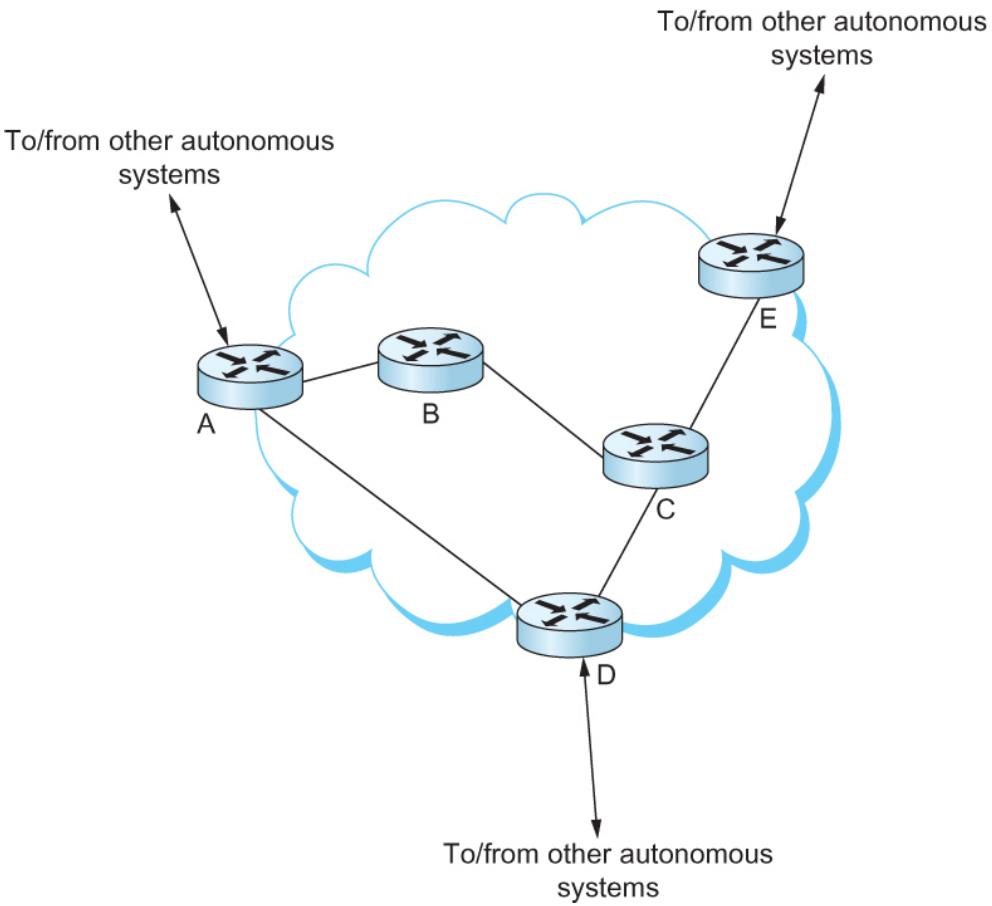
BGP Example

- Speaker for AS 2 advertises reachability to P and Q
  - Network 128.96, 192.4.153, 192.4.32, and 192.4.3, can be reached directly from AS 2.
- Speaker for backbone network then advertises
  - Networks 128.96, 192.4.153, 192.4.32, and 192.4.3 can be reached along the path <AS 1, AS 2>.
- Speaker can also cancel previously advertised paths

BGP Issues

- It should be apparent that the AS numbers carried in BGP need to be unique
- For example, AS 2 can only recognize itself in the AS path in the example if no other AS identifies itself in the same way
- AS numbers are 16-bit numbers assigned by a central authority

Integrating Interdomain and Intradomain Routing



All routers run iBGP and an intradomain routing protocol. Border routers (A, D, E) also run eBGP to other ASs

Integrating Interdomain and Intradomain Routing

Prefix	BGP Next Hop
18.0/16	E
12.5.5/24	A
128.34/16	D
128.69./16	A

BGP table for the AS

Router	IGP Path
A	A
C	C
D	C
E	C

IGP table for router B

Prefix	IGP Path
18.0/16	C
12.5.5/24	A
128.34/16	C
128.69./16	A

Combined table for router B

BGP routing table, IGP routing table, and combined table at router B

Advanced Internetworking

IPv6

IP Version 6 (IPv6)

- A new version of IP deals with **scaling problems** caused by the Internet's massive growth
- IPv6 provides a **128-bit** address space
  - Can address $\mathbf{3.4 \times 10^{38}}$ nodes for 100 % efficiency
  - To provide over **1500 addresses** per square foot of the earth's surface
- IPv6 addresses **do not have classes**, but the address space is still subdivided in various ways based on the leading bits

Address prefix assignments for IPv6

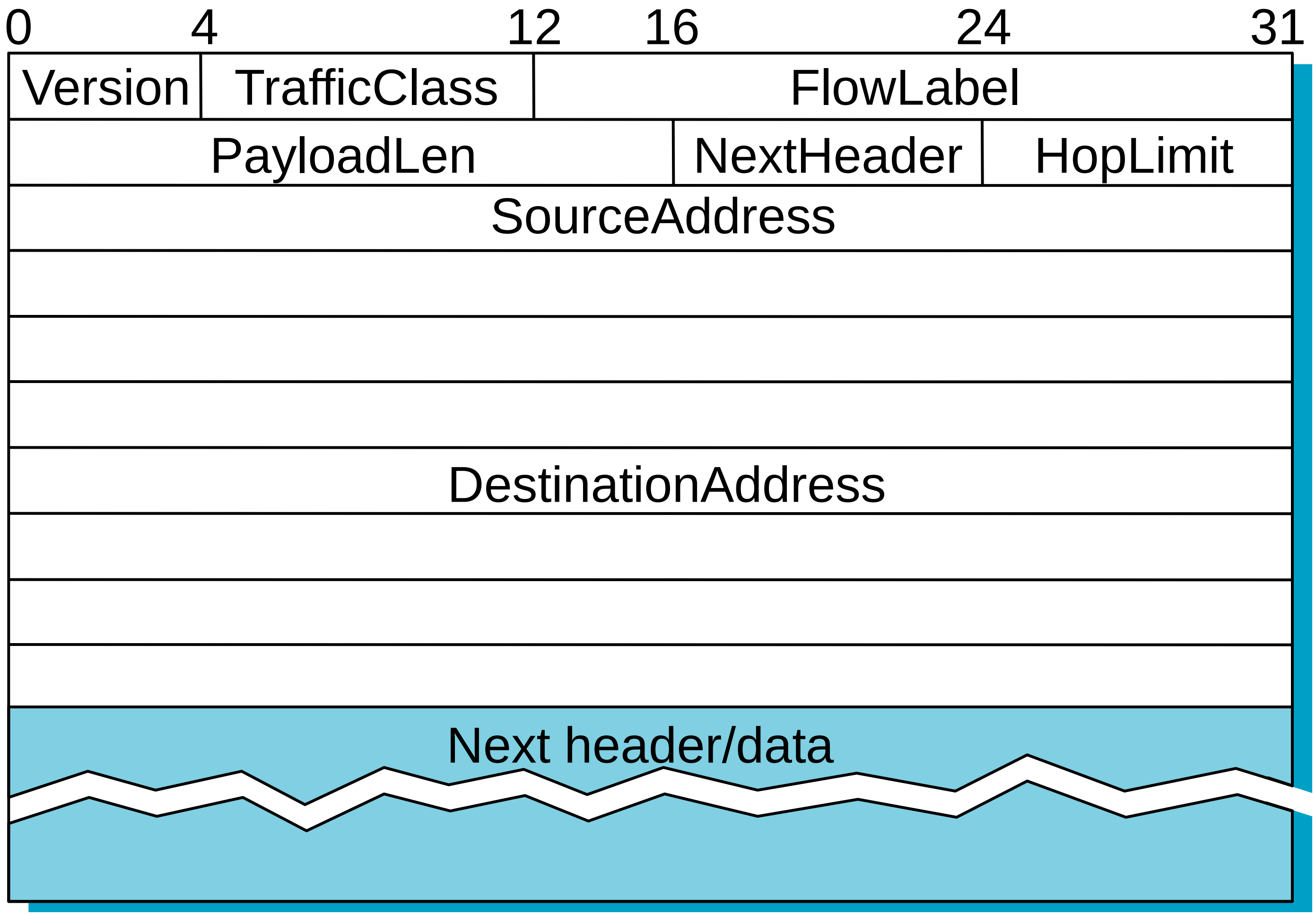
Prefix	Use	Prefix	Use
0000 0000	Reserved	…	…
…	…	1111 1110 11	Site local user addresses
001	Global Unicast Addresses	1111 1111	Multicast addresses

IP Version 6 (IPv6)

- IPv6 addresses: **X:X:X:X:X:X:X:X**
  - X is a hexadecimal representation of a **16-bit** piece
  - 47CD:1234:4422:ACO2:0022:1234:A456:0124
- For an address with a large number of contiguous 0s
  - 47CD:**0000:0000:0000:0000:0000**:A456:0124
    ⇒ 47CD**::**A456:0124 (omitting all the 0 fields)
- A node may be assigned an **"IPv4-compatible IPv6 address"** by **zero-extending** a 32-bit IPv4 address to 128 bits
  - **::**128.96.33.81
- For a node that is only capable of understanding IPv4: assigned an **"IPv4-mapped IPv6 address"** ⇒ **Prefix** the IPv4 address with **2 bytes of all 1s** and then zero-extending to 128 bits
  - **::FFFF:**128.96.33.81

IP Version 6 (IPv6)

- IPv6 packet header



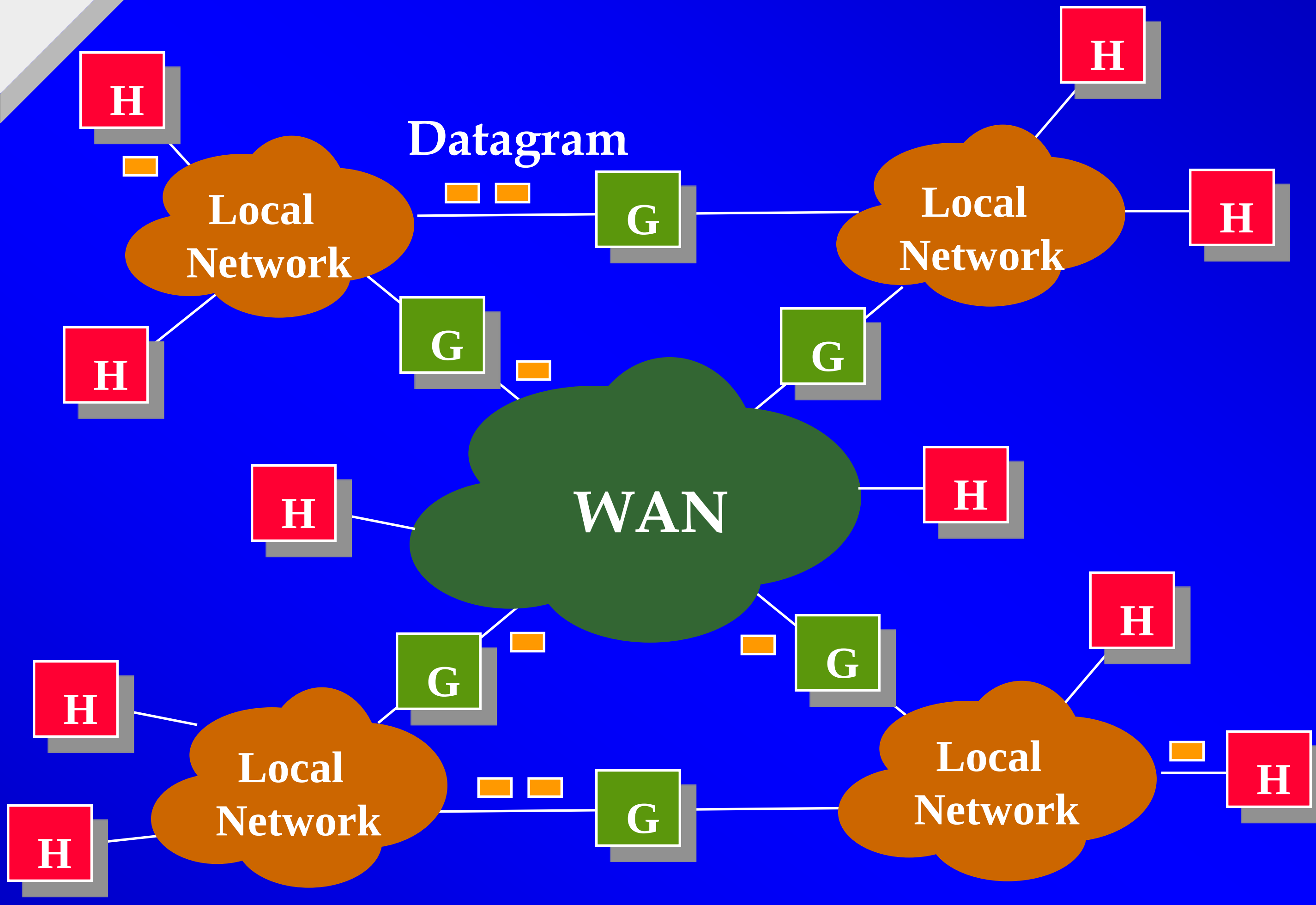
IPv6 (Internet Protocol Version 6)

國立清華大學資訊工程學系 黃能富教授
Tel: 03-573-1063
Fax: 03-572-3694
E-mail: nfhuang@cs.nthu.edu.tw
URL:http://www.cs.nthu.edu.tw/~nfhuang

IPv6 Outline

- The Design of IPv6
- Routing and Addressing
- Plug and Play
- Bringing Security to the Internet
- Real-time Support and Flows
- Transitioning the Internet

An Internet



H
Datagram
H
Local Network
G
Local Network
H
H
G
G
H
WAN
H
H
G
G
H
Local Network
H
Local Network
H
G
H

The Design of IPv6

- The Internet could not have been so successful in the past years if IPv4 had contained any major flaw.
- IPv4 was a very good design, and IPv6 should indeed keep most of its characteristics.
- It could have been sufficient to simply increase the size of addresses and to keep everything else unchanged.
- However, 10 years of experience brought lessons.
- IPv6 is built on this additional knowledge. It is not a simple derivation of IPv4, but a definitive improvement.

IPv6 Header Format

IPv6 Header

4	4	8	8	8 位元
Version	Prio	Flow Label		
Payload Length			Next Header	Hop Limit
Source IP address (128 位元)				
Destination IP address (128 位元)				

IPv4 Header

4	4	8	3	13 位元
Version	IHL	ToS	Total length	
Identifier			Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + Padding				
Data（不固定長度)				

A Comparison of Two Headers

- **Six fields were suppressed:**
  - Header Length, Type of Service, Identification, Flags, Fragment Offset, Header Checksum.
- **Three fields were renamed:**
  - Length, Protocol Type, Time to Live
- **The option mechanism was entirely revised.**
  - Source Routing
  - Route Recording
- **Two new fields were added:**
  - Priority and Flow Label (to handle the real-time traffic).

A Comparison of Two Headers

- Three major simplifications
  - Assign a fixed format to all headers (40 bytes)
  - Remove the header checksum
  - Remove the hop-by-hop segmentation procedure

34

From Options to Extension Headers

- Hop-by-Hop options header
- Routing header
- Fragment header
- Authentication header
- Encrypted security payload
- Destination options header

IPv6 Header Next Header=TCP	TCP Header	

IPv6 Header Next Header= Routing	Routing Header Next Header= TCP	TCP Header	

IPv6 Header Next Header= Routing	Routing Header Next Header= Fragment	Fragment Header Next Header= TCP	Fragment of TCP Header	

The Evolution of ICMP

ICMP Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Termination
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

- **The ICMP for IPv4 was streamlined, and was made more complete by incorporating the multicast control functions of the IPv4 Group Membership Protocol.**

Routing and Addressing

- **Three categories of IPv6 addresses:**
  - Unicast
  - Multicast
  - Anycast
- **Notation of IPv6 Addresses:**
  - Write 128 bits as eight 16-bit integers separated by colons
  - Example:

    FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  - A set of consecutive null 16-bit numbers can be replaced by two colons
  - Example: 1080:0:0:0:8:800:200C:417A =>
    1080::8:800:200C:417A

Some Addresses formats

3	n	m	o	p	125-m-n-o-p bits
010	registry ID	provider ID	subscriber ID	subnetwork ID	interface ID

8	16	8	24	8	16	48 bits
F+R	Prov-id	0	Subscr-id	0	subnet	station-id

8	8	8	8	8	8	8	8	16	48 bits
FE	C0	0	0	0	0	0	0	subnet	station-id

8	8	8	8	8	8	8	8	16	48 bits
FE	80	0	0	0	0	0	0	subnet	station-id

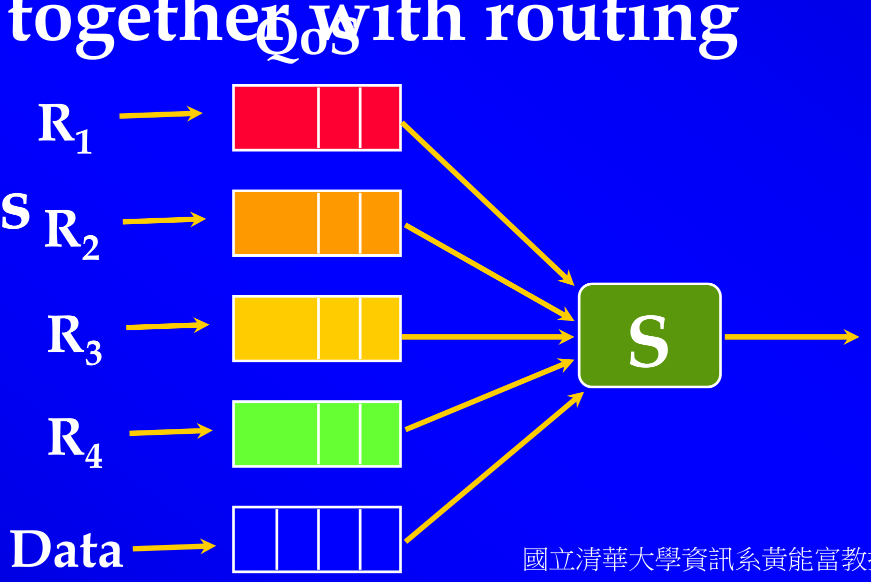
8	4	4	112 bits
11111111	flags	scope	group ID

Plug-and-Play -- Auto-configuration

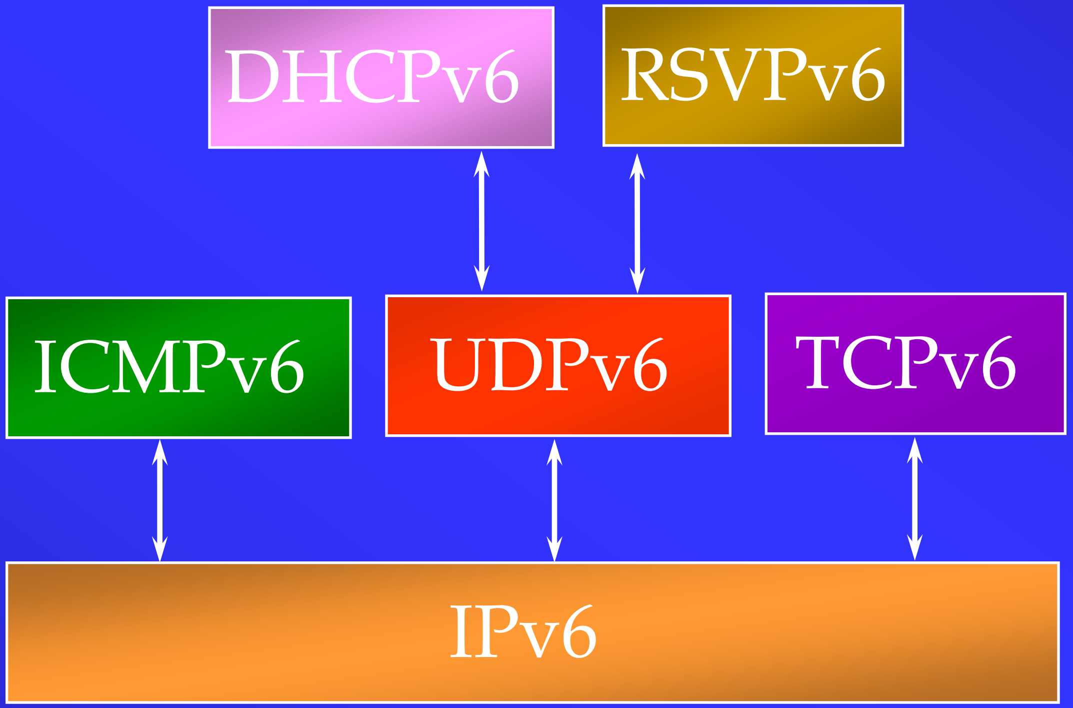
- Autoconfiguration means that a computer will automatically discover and register the parameters that it needs to use in order to connect to the Internet.
- One should be able to change addresses dynamically as one changes providers.
- Addresses would be assigned to interfaces for a limited lifetime. Link State Addresses

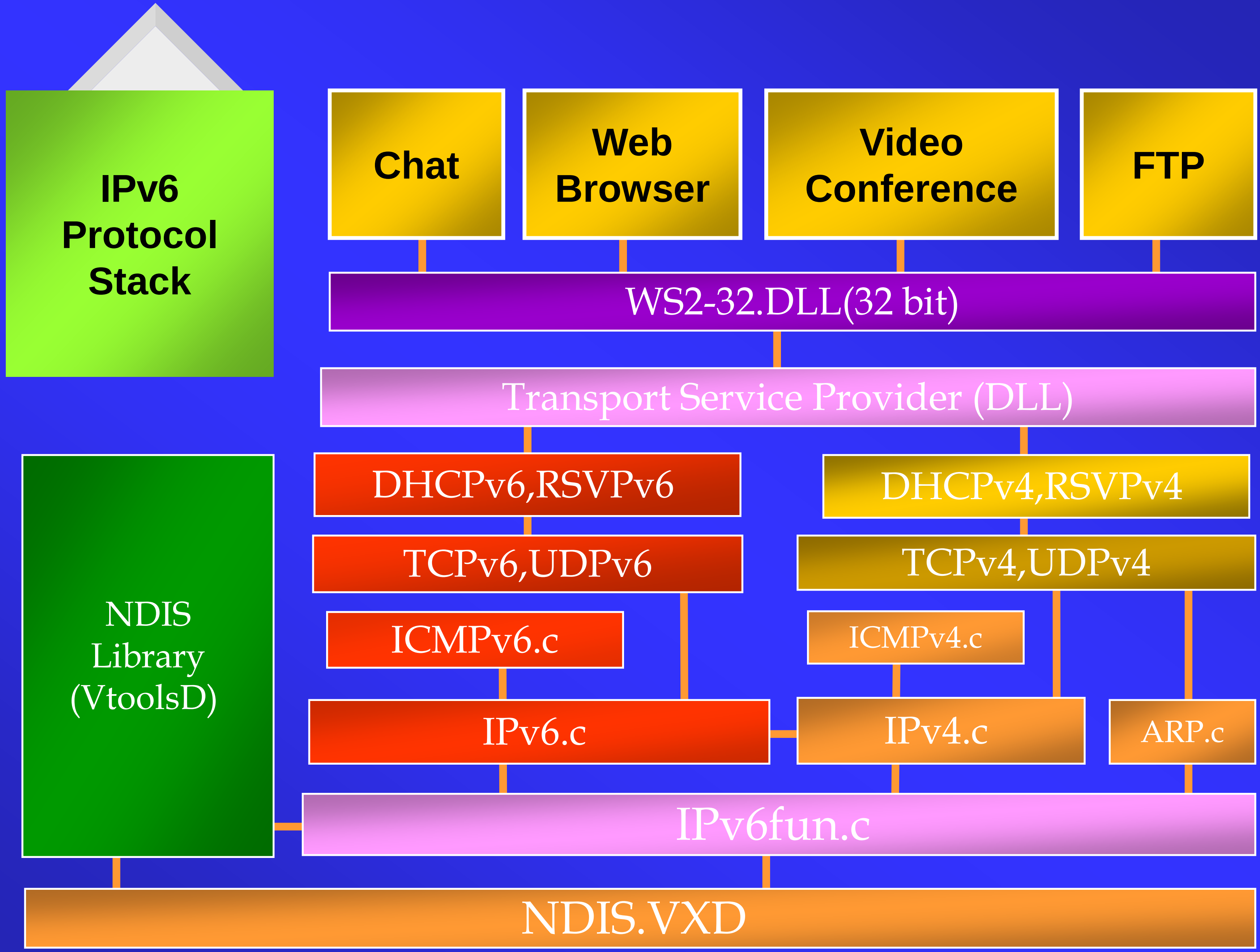
Real-time Support and Flows

- A flow is **a sequence of packets** sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers.
- Flow label may be used together with routing header.
- Supporting Reservations
  - Real-time flows
  - Using RSVP and Flows
  - Using Hop-by-Hop Options

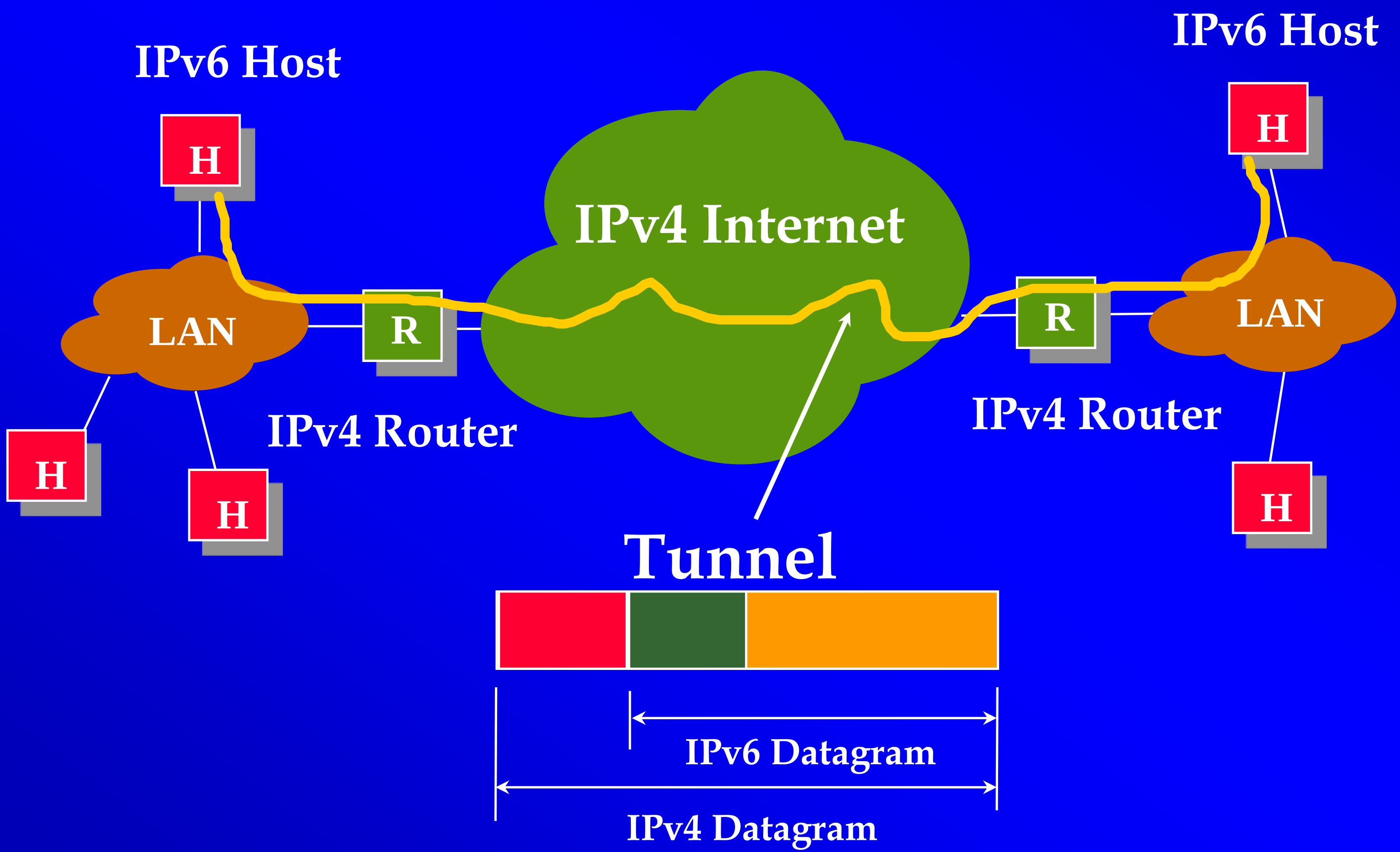


IPv6 Related Protocol Stack

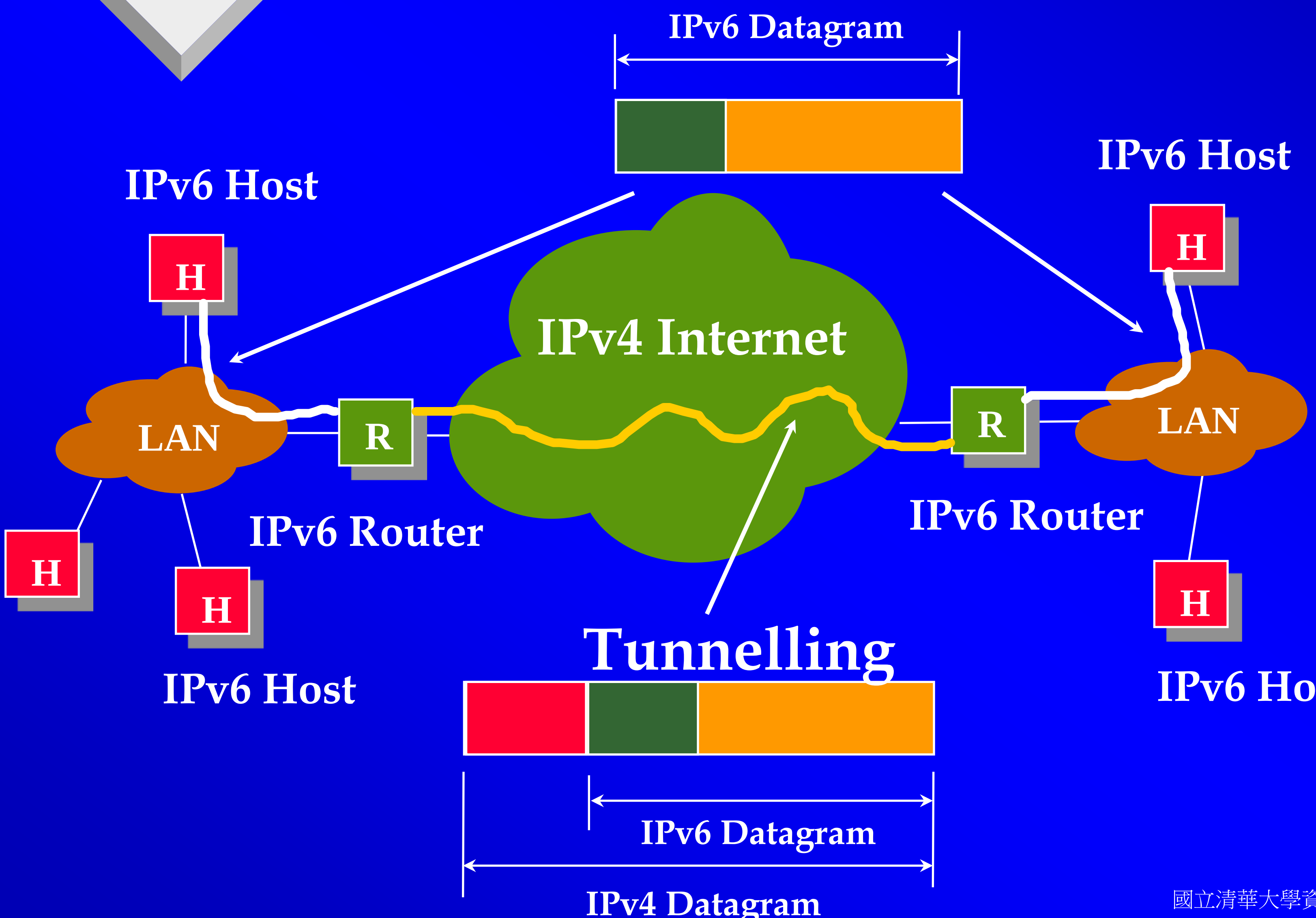



IPv6 Protocol Stack
Chat
Web Browser
Video Conference
FTP
WS2-32.DLL(32 bit)
Transport Service Provider (DLL)
NDIS Library (VtoolsD)
DHCPv6,RSVPv6
DHCPv4,RSVPv4
TCPv6,UDPv6
TCPv4,UDPv4
ICMPv6.c
ICMPv4.c
IPv6.c
IPv4.c
ARP.c
IPv6fun.c
NDIS.VXD

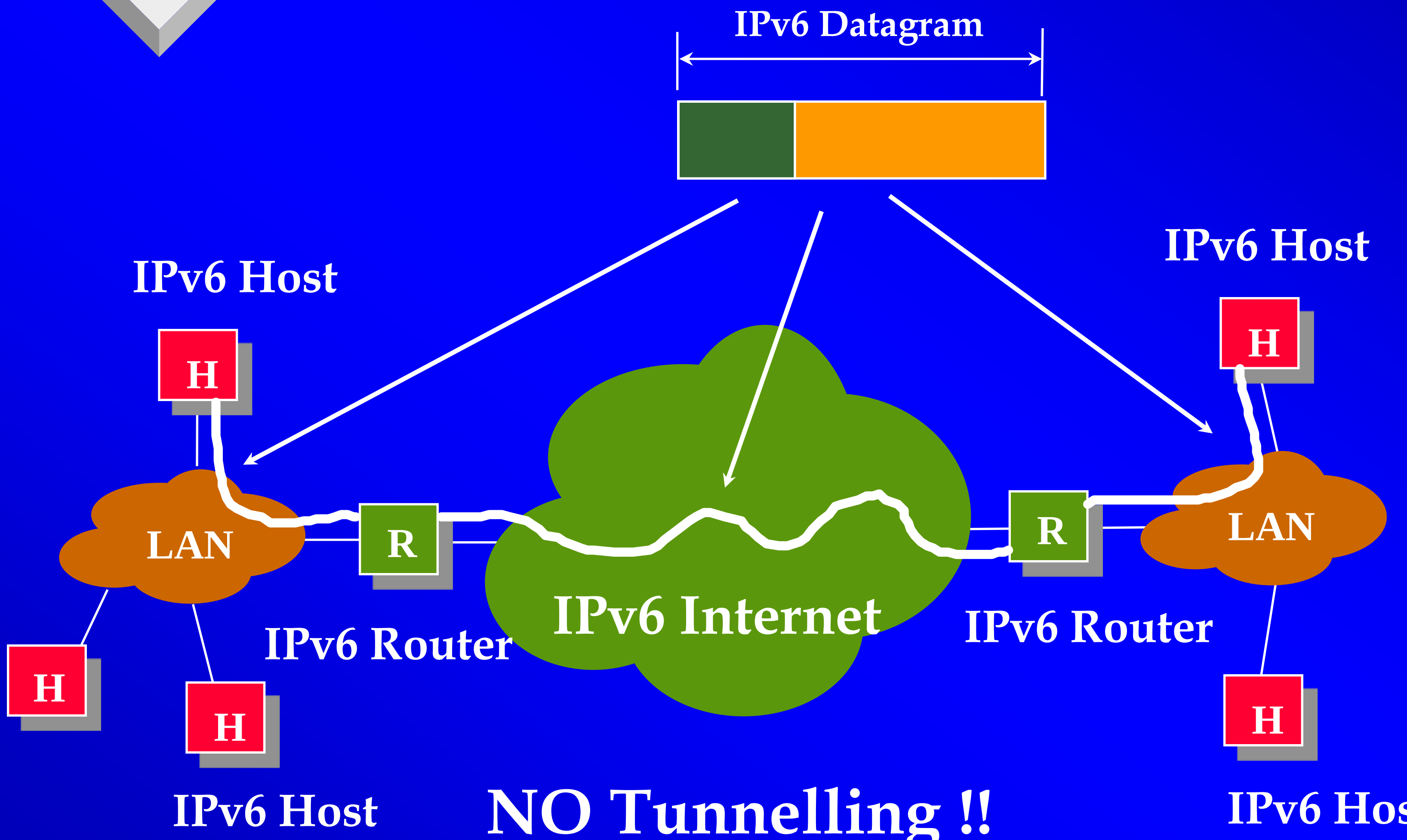
IPv6 Hosts + IPv4 Internet



IPv6 Routers + IPv4 Internet

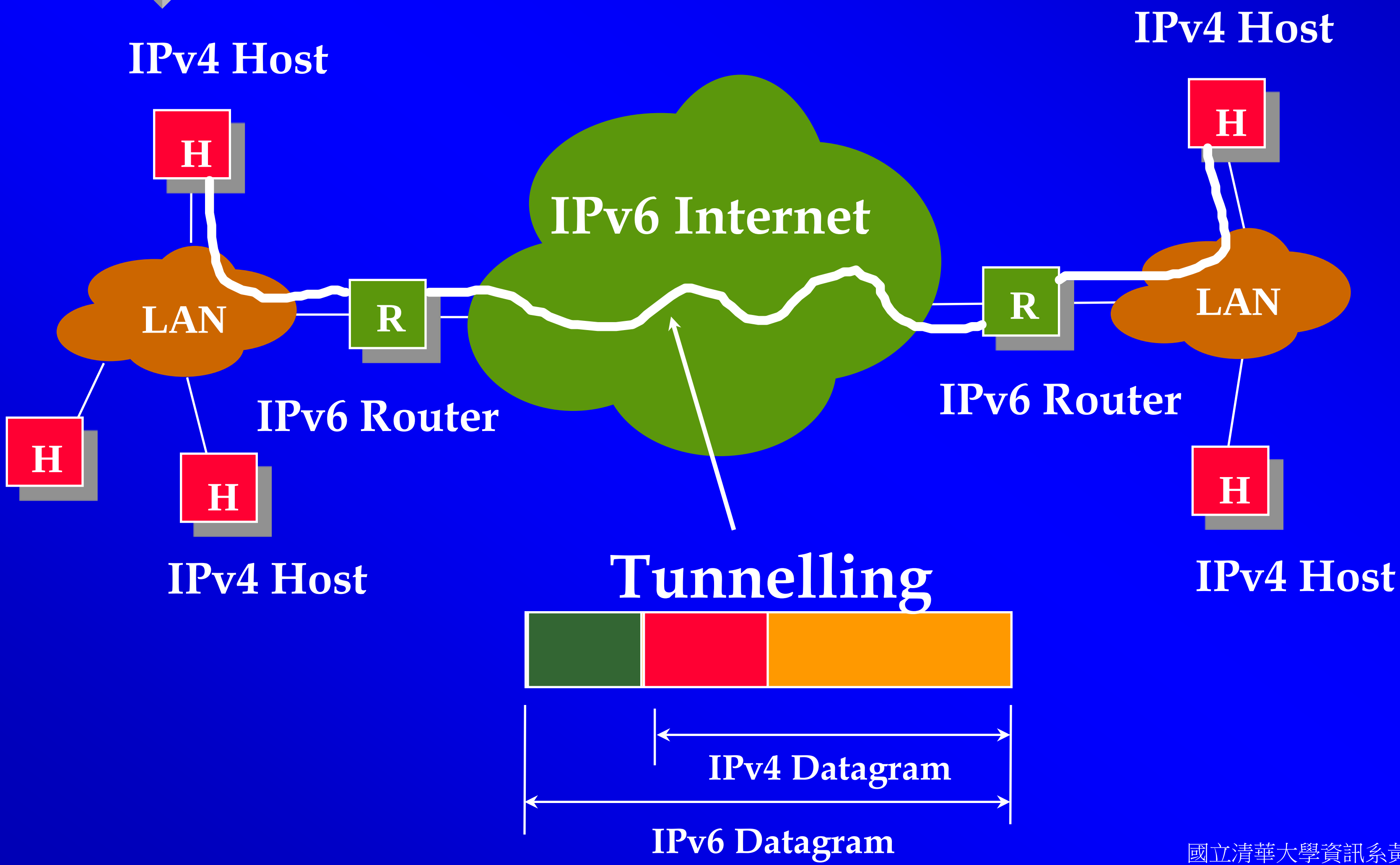


IPv6 Internet

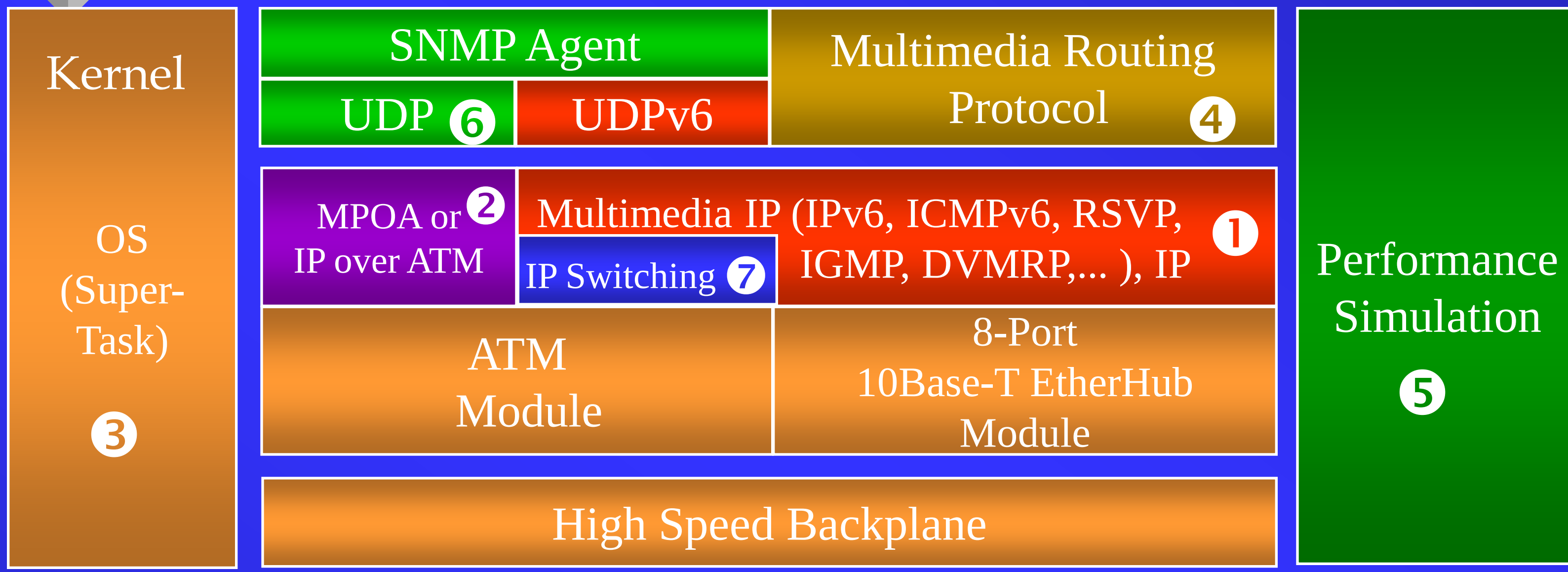


NO Tunnelling !!

Somedays -- IPv4 Host over IPv6 Internet



Router System Architecture



❶ 架構在 ATM 網路上之多媒體 IP 通訊協定之研製
❷ 架構在 ATM 網路上之多重通訊協定之研製
❸ ATM 多媒體路徑器環境之建立
❹ 多媒體路徑選擇通訊協定之研製
❺ 物件導向式 ATM 多媒體路徑器效能分析模擬器之研製
❻ ATM 多媒體路徑器上網管軟體之研製
❼ 架構在 ATM 網路上之 IP 交換通訊協定之研製

Routing for Mobile Hosts

Routing for Mobile Hosts

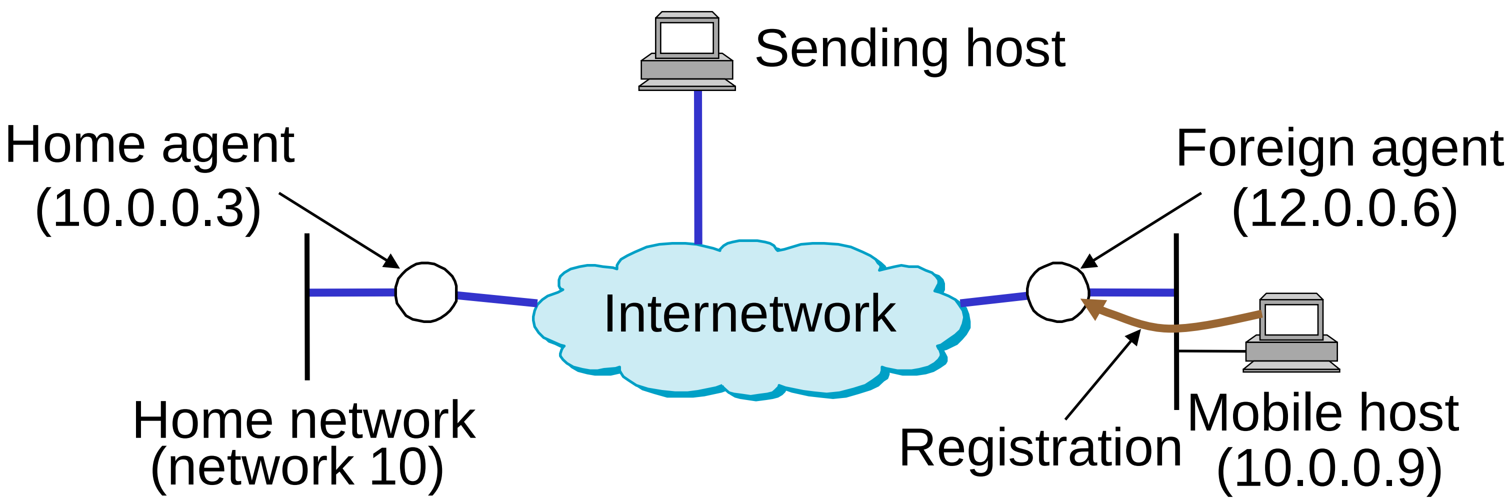
- If a host was disconnected from one network and connected to another without changing IP, it would become **unreachable**
- The obvious solution is to provide the host with a **new address**
  - Techniques such as **DHCP** can make this a simple process
- For wireless networks:
  - **Detach** and **attach** to networks **frequently**
  - Some applications should **continuously** run without interruption when it roams to another network
- The procedures that are designed to address this problem
  - **"Mobile IP"**

Routing for Mobile Hosts

- A new router, known as the **home agent**, is required
  - Located on the **"home" network** of the mobile host
  - The mobile host has a **permanent** IP address–**home address**
- In many cases, a second router, **foreign agent**, is also required
  - Located on the network to which the mobile node **attaches** when it is away from its home network
- Both home and foreign agents **periodically announce** their presence on the networks using agent **advertisement messages**

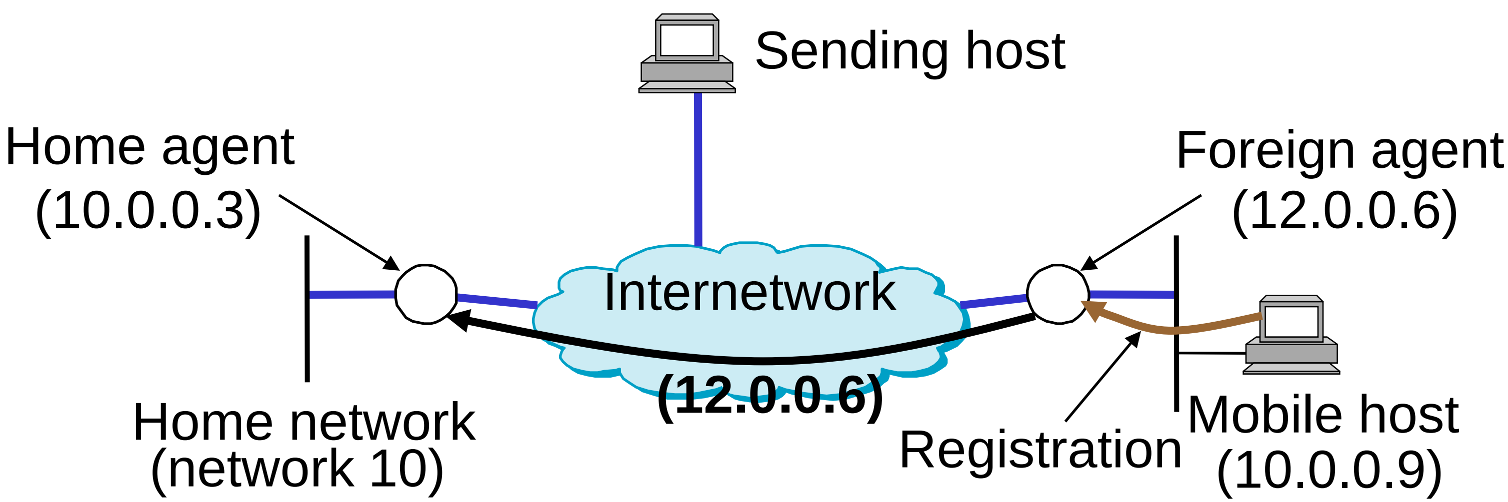
Routing for Mobile Hosts

- When the mobile host attached to a foreign network
  - It hears an advertisement from a foreign agent
  - It **registers** with the foreign agent, providing the address of its home agent



Routing for Mobile Hosts

- The foreign agent then contacts the home agent, providing a **care-of address** **(the IP address of the foreign agent)**
  - According to the IP address of the mobile host
- The home agent is notified that the mobile host **has attached** to the foreign network

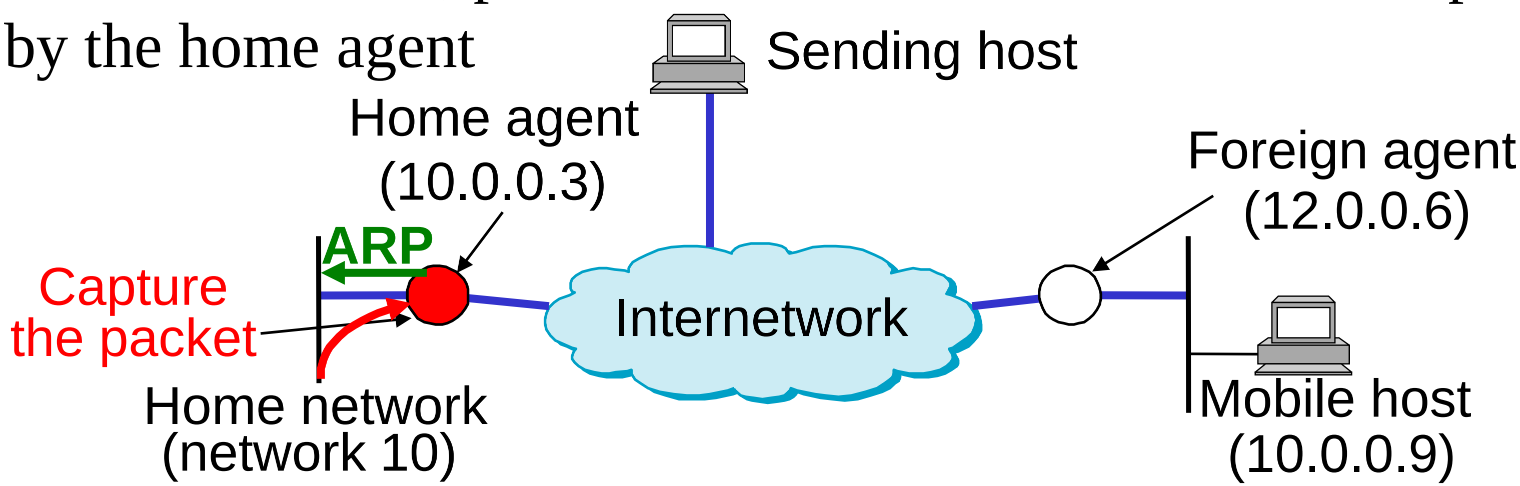


Routing for Mobile Hosts

- How does the home agent intercept a packet that is destined for the mobile host?
- How does the home agent then deliver the packet to the foreign agent?
- How does the foreign agent deliver the packet to the mobile node?

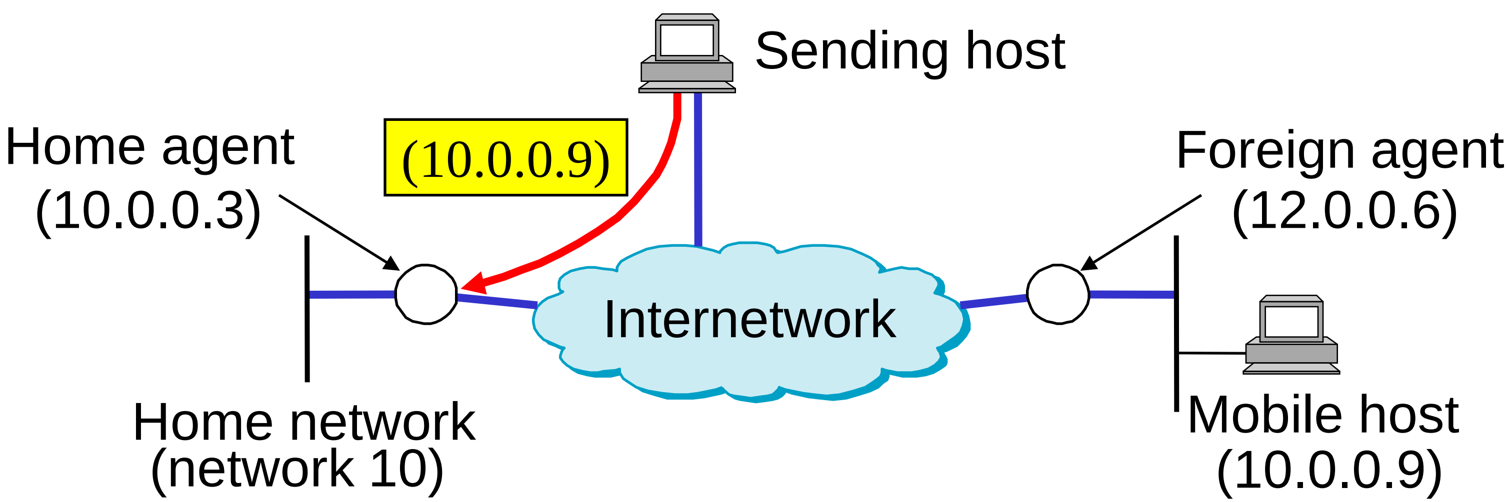
Routing for Mobile Hosts

- The home agent actually **impersonates** the mobile node
  - **"Proxy ARP"** (ARP: Address Resolution Protocol)
- The home agent issues an ARP message **as soon as** the mobile node registers with a foreign agent, with
  - The **IP address** of the mobile node
  - The **hardware address** of the **home agent**
- In home network, packets for the mobile node will be captured by the home agent



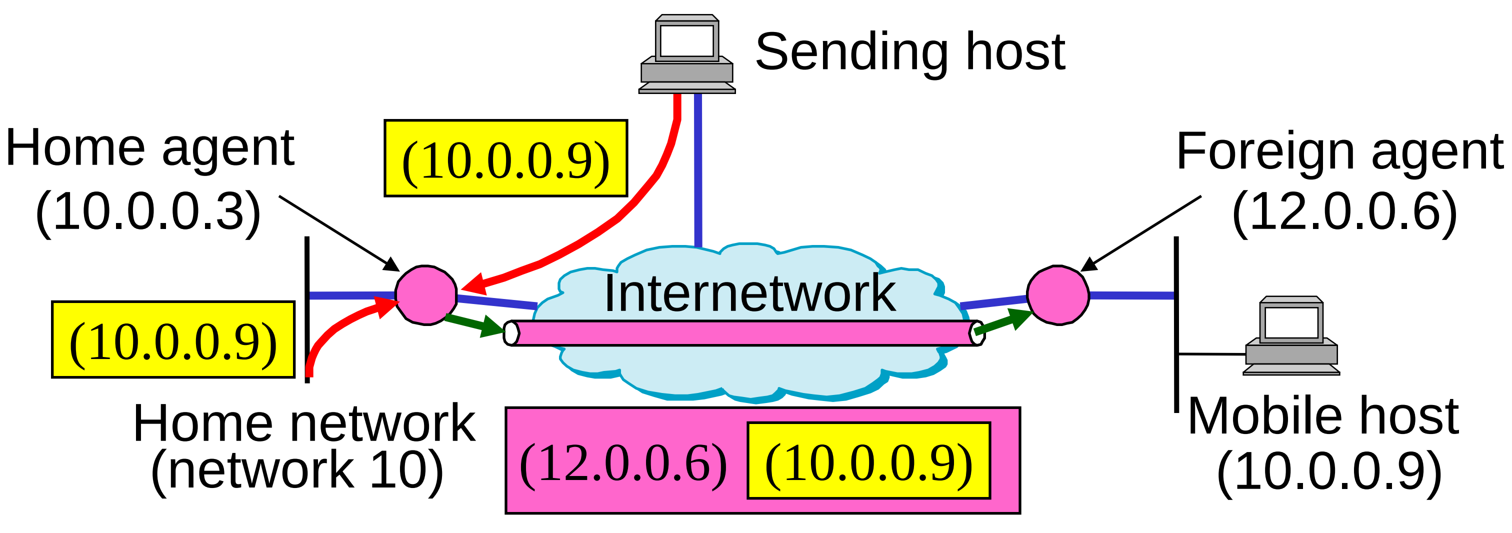
Routing for Mobile Hosts

- Any host that tries to send a packet to the mobile host will send it with a destination address equal to the mobile **home address**
  - The packet to arrive on the **home network** of the mobile node, on which the home agent is sitting
- From the internetwork, the packets for the mobile node will be captured by the home agent



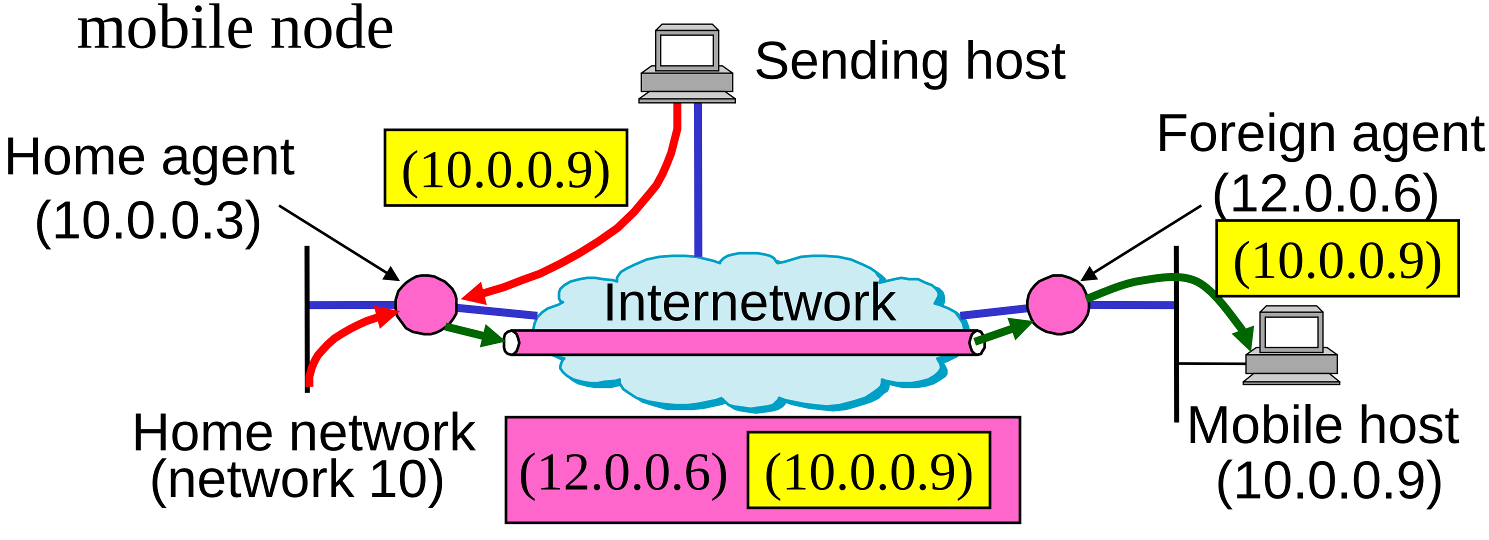
Routing for Mobile Hosts

- How does the home agent then deliver the packet to the foreign agent?
- Use the **tunneling technique**
  - An IP tunnel is established between the **home agent** and the **foreign agent**
  - The home agent transmits the packet into the IP tunnel



Routing for Mobile Hosts

- How does the foreign agent deliver the packet to the mobile node?
- Find inside an IP packet destined for the mobile node
  - The foreign agent has to recognize the address belonging a **registered mobile node**
  - It delivers the packet to the **hardware address** of the mobile node



Route Optimization

- Triangle routing
- What if both the sender and the mobile host are on the same network?
- Solution: let the sender know the care-of address
- The home agent sends a binding update message to the sender.
- Then the sender can send packets directly to the foreign agent.
- Problem: the mobile host moves to a new network.
- The foreign agent sends a binding warning message back to the sender.