IPv6 (IP version 6) Essentials Ch0: Overwiew

Louis Chuang
Fu Jen Catholic University
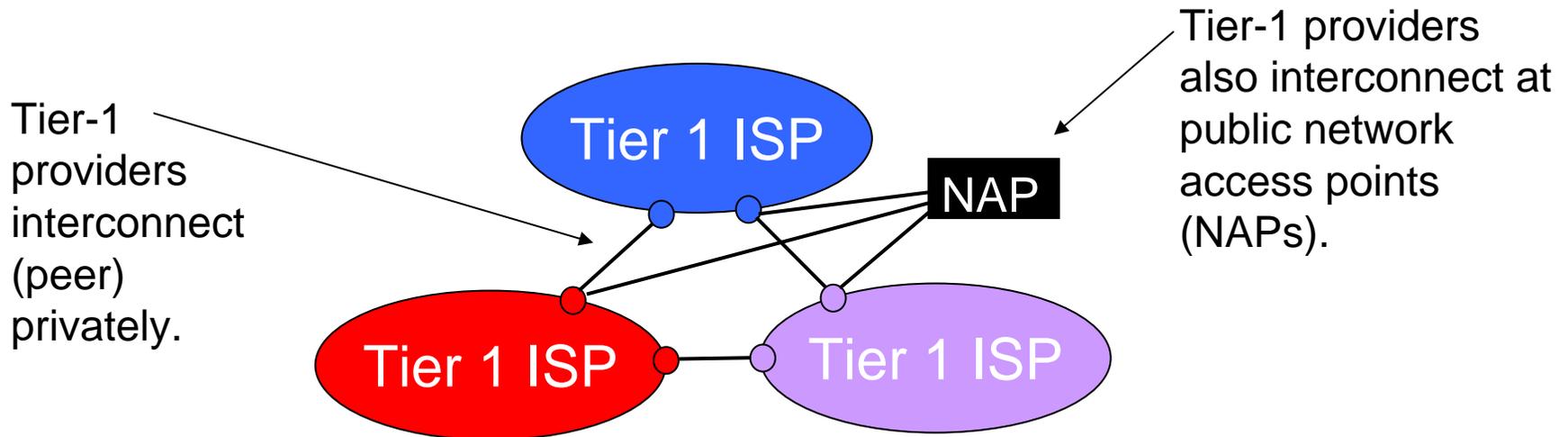**EE ENCL**

What's the Internet

- Protocols control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, FTP, PPP
- Internet: "network of networks"
  - loosely hierarchical
  - public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force

router

workstation

server

mobile

local ISP
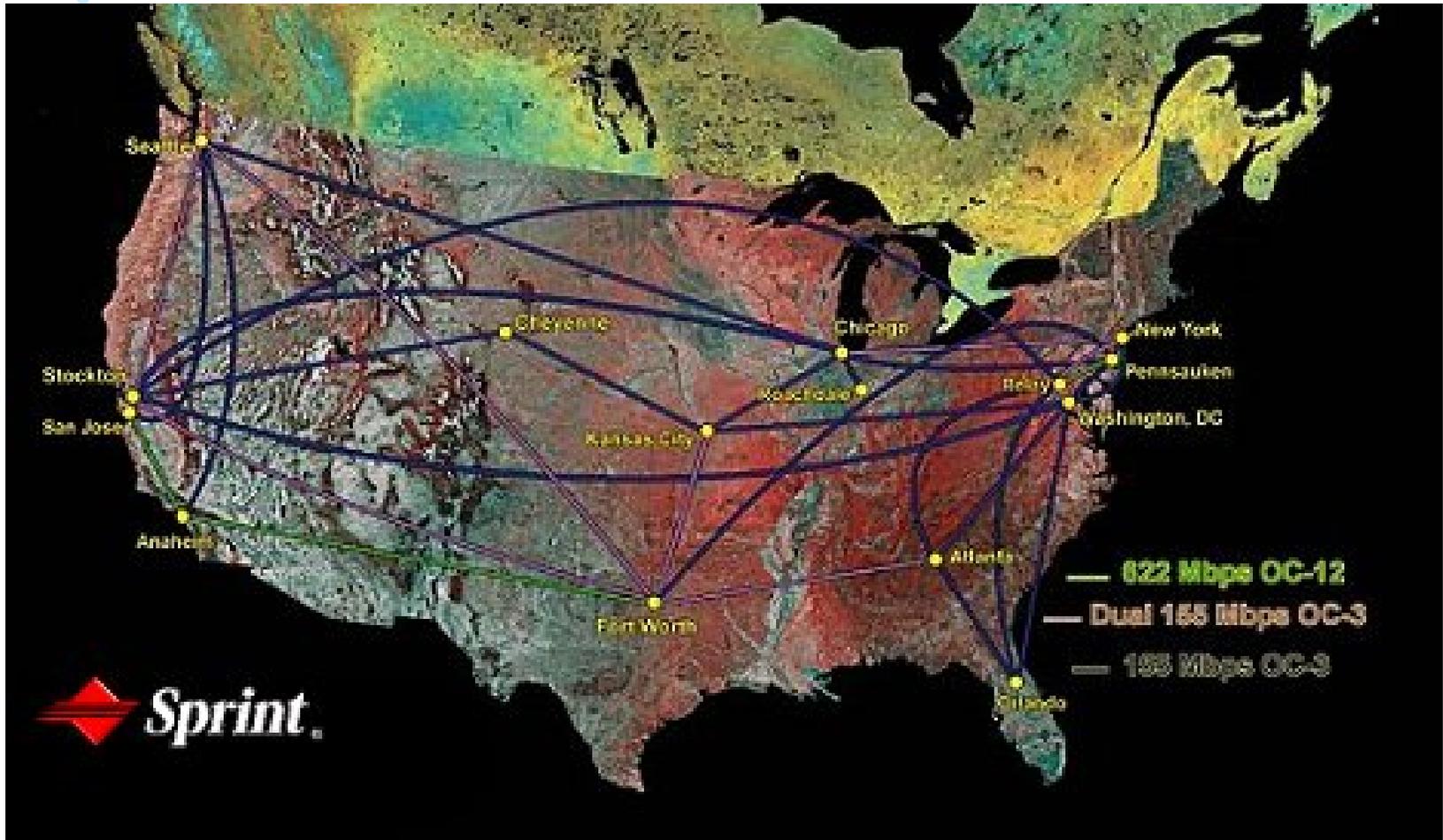
regional ISP

company network
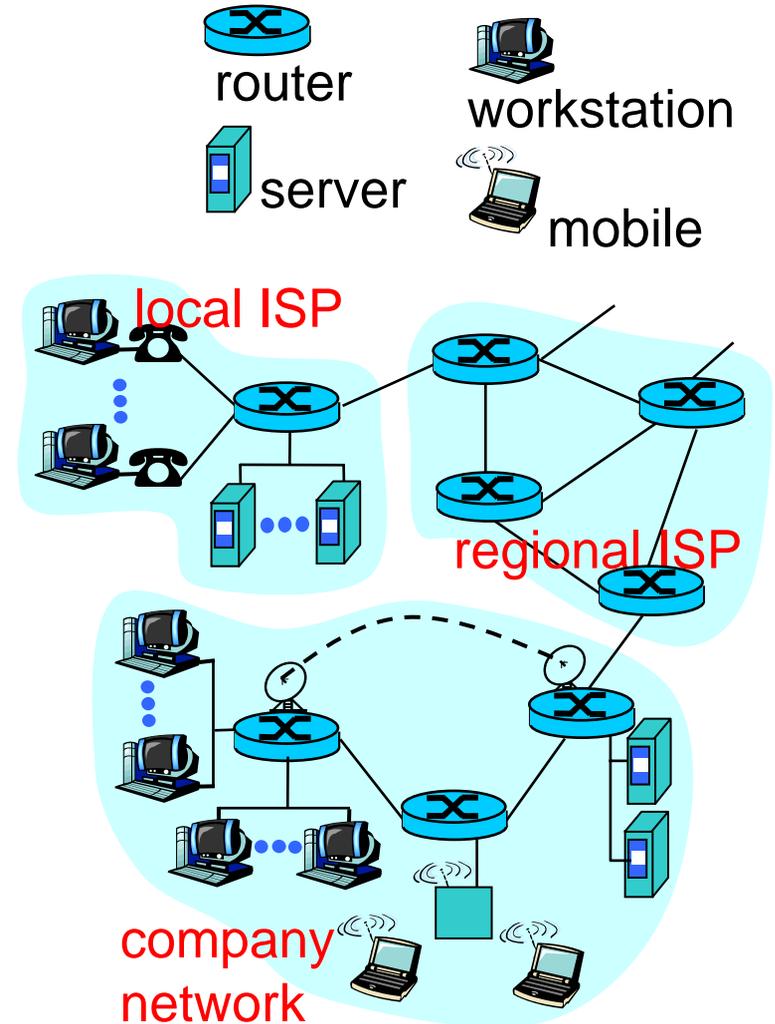
Internet Structure (1)

- Roughly hierarchical:
  - At center: "tier-1" ISPs (e.g., UUNet, BBN/Genuity, Sprint, AT&T), national/international coverage
    - ❖ Treat each other as equals

Tier-1 providers interconnect (peer) privately.

Tier-1 providers also interconnect at public network access points (NAPs).

Tier 1 ISP

Tier 1 ISP

Tier 1 ISP

NAP

Internet Structure (2)

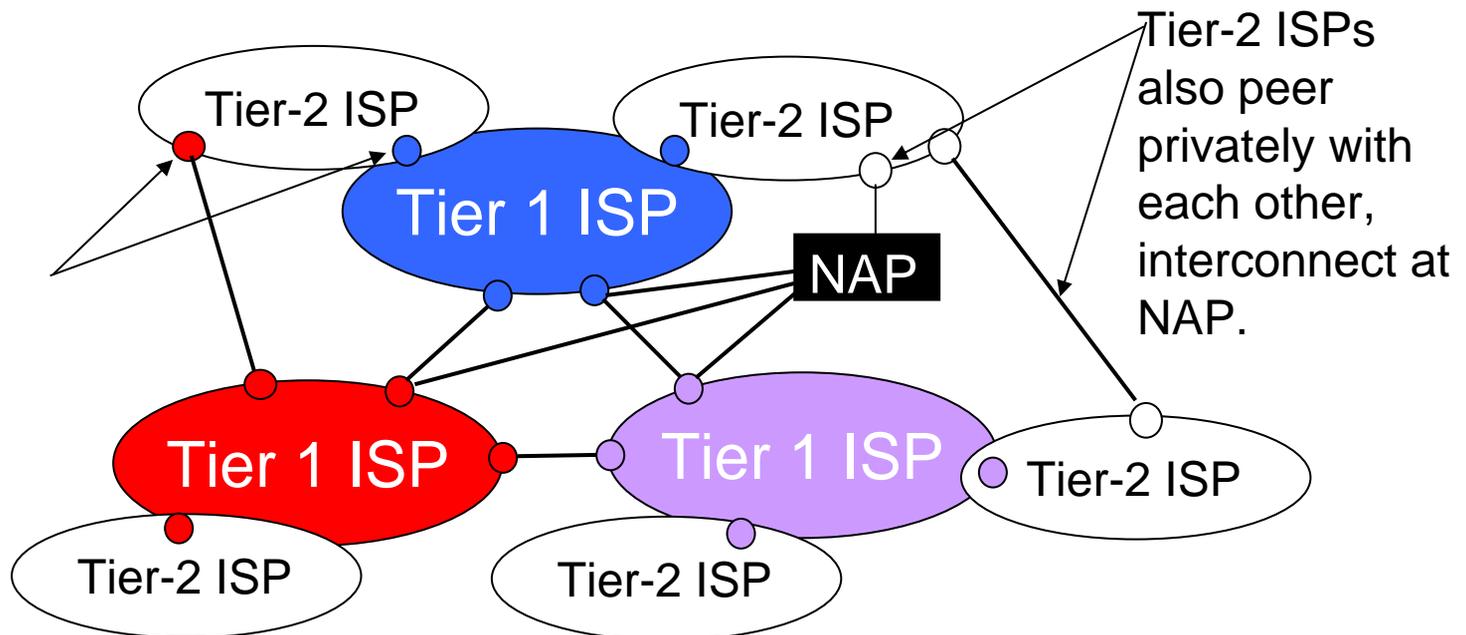Tier-1 ISP: e.g., Sprint (Sprint US backbone network).

Internet Structure (3)

- "Tier-2" ISPs: smaller (often regional) ISPs.
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs.

Tier-2 ISP pays tier-1 ISP for connectivity to rest of Internet. Tier-2 ISP is customer of tier-1 provider.
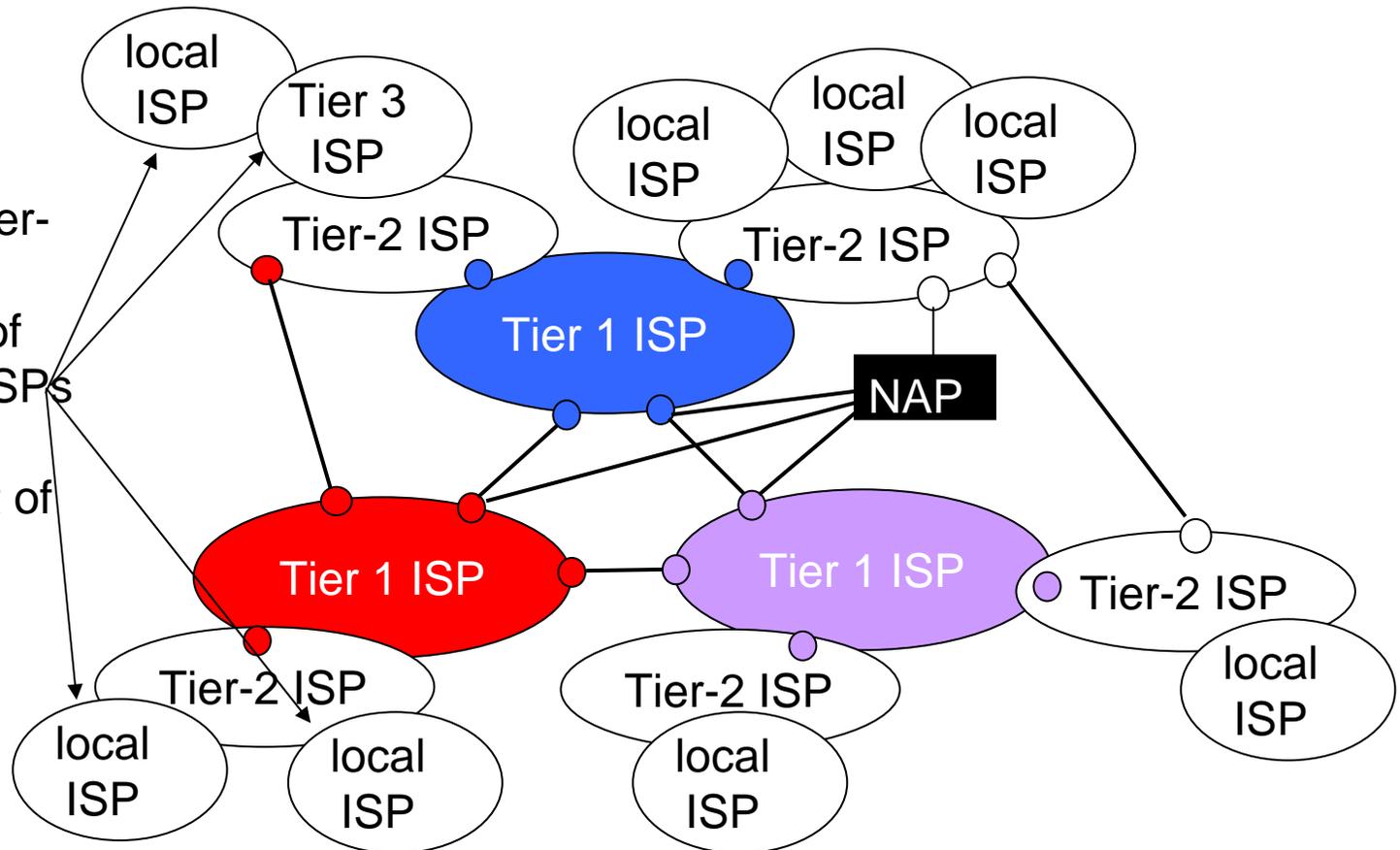
Tier-2 ISPs also peer privately with each other, interconnect at NAP.

Tier-2 ISP

Tier-2 ISP

Tier 1 ISP

NAP

Tier 1 ISP

Tier 1 ISP

Tier-2 ISP

Tier-2 ISP

Tier-2 ISP

Internet Structure (4)

- "Tier-3" ISPs and local ISPs .
  - last hop ("access") network (closest to end systems).

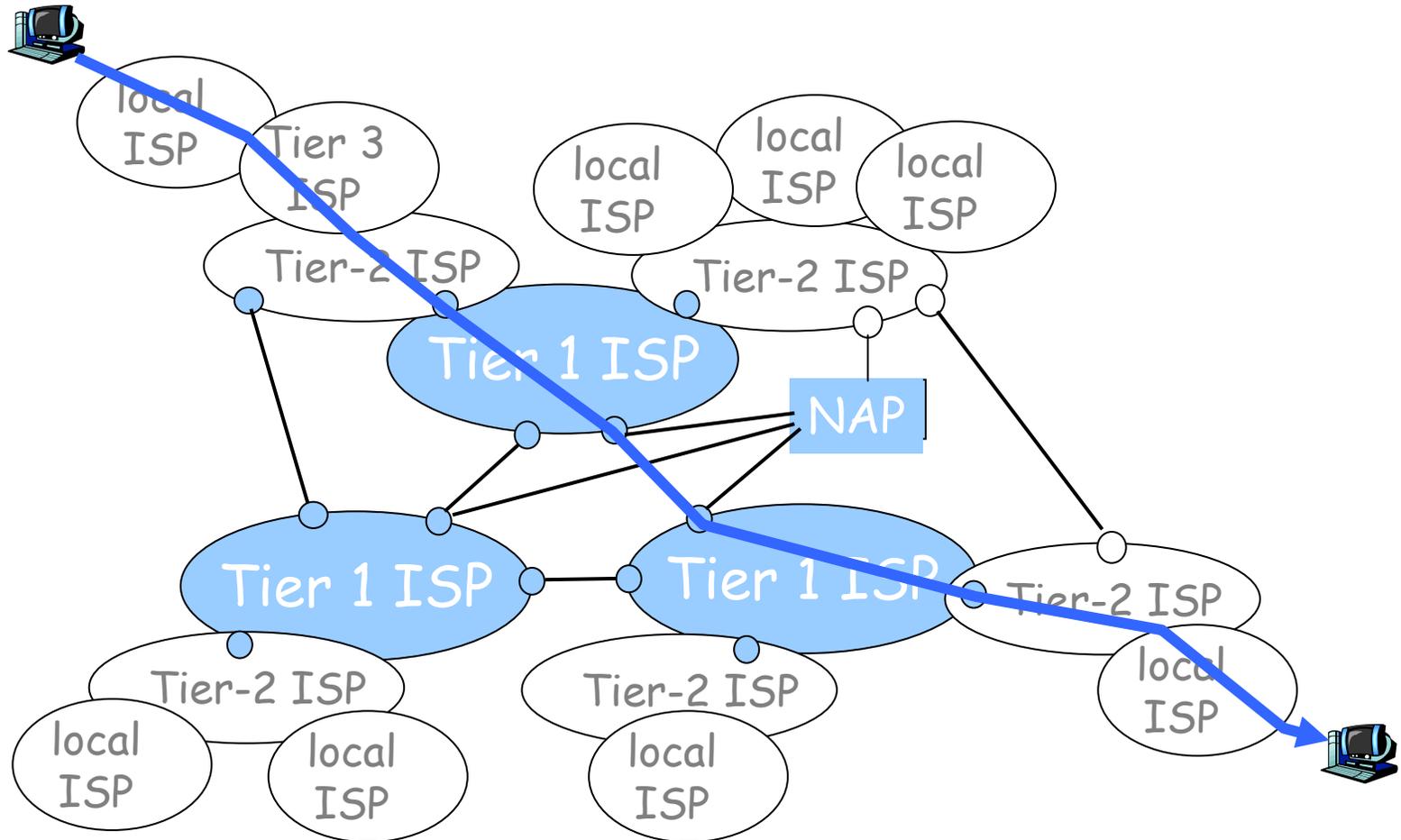Local and tier-3 ISPs are customers of higher tier ISPs connecting them to rest of Internet.

local ISP

Tier 3 ISP

local ISP

local ISP

local ISP

Tier-2 ISP

Tier-2 ISP

Tier 1 ISP

NAP

Tier 1 ISP

Tier 1 ISP

Tier-2 ISP

Tier-2 ISP

local ISP

local ISP

local ISP

Tier-2 ISP

local ISP

Internet Structure (5)

■ A packet passes through many networks.

Internet Protocol Stack (1)

- Application: supporting network applications.
  - FTP, SMTP, STTP.
- Transport: host-host data transfer.
  - TCP, UDP.
- Network: routing of datagrams from source to destination.
  - IP, routing protocols.
- Link: data transfer between neighboring network elements.
  - PPP, Ethernet, WLAN.
- Physical: bits "on the wire".

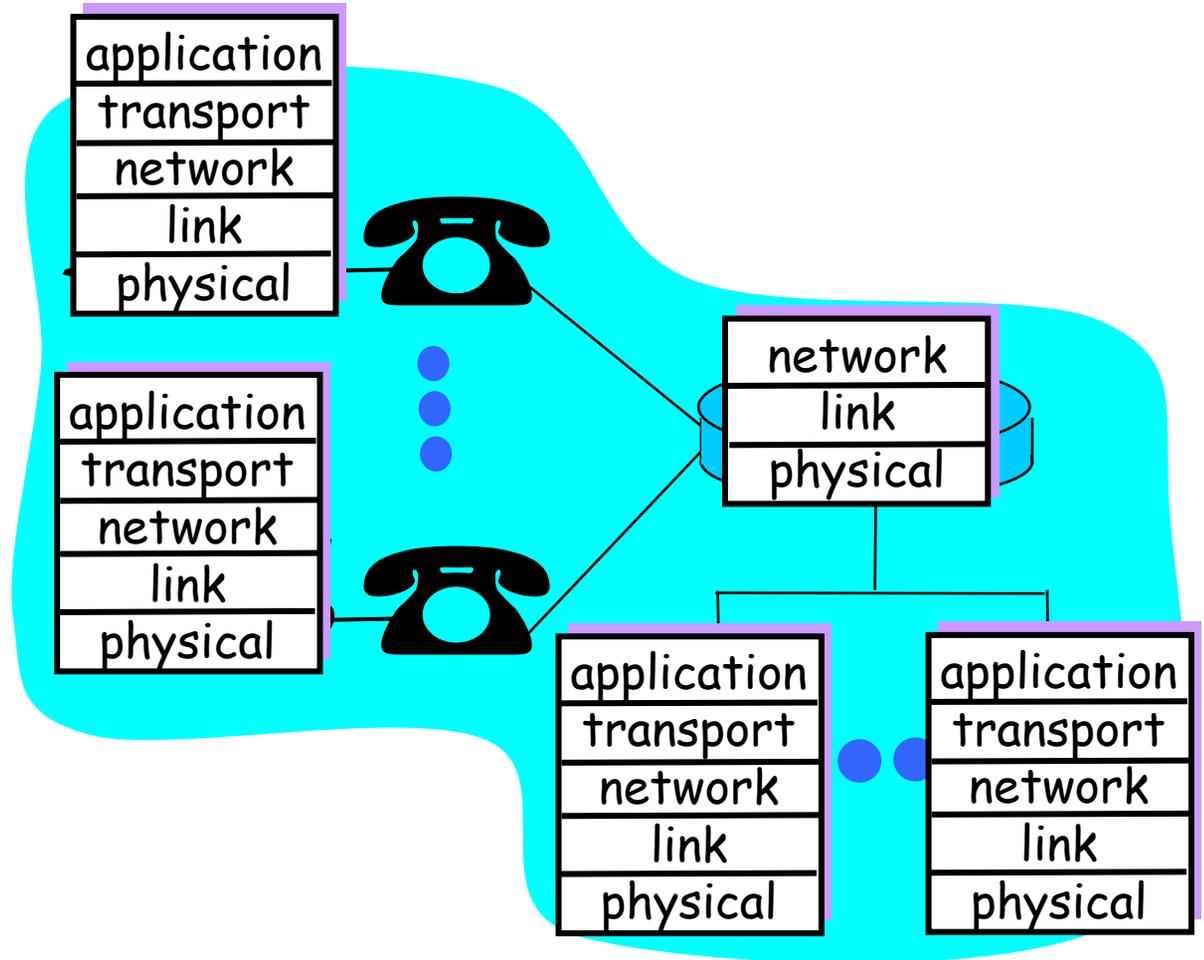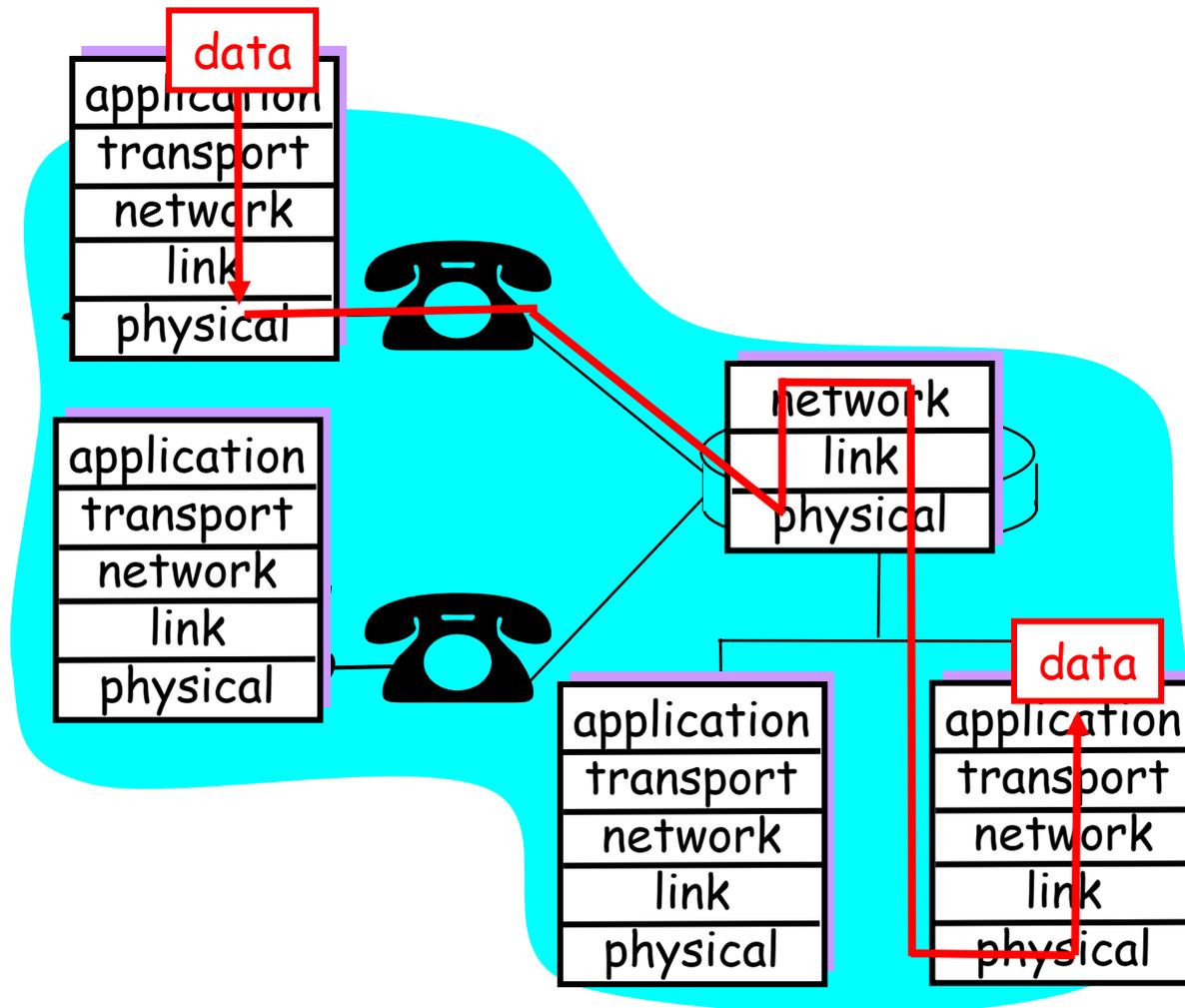| application |
| --- |
| transport |
| network |
| link |
| physical |
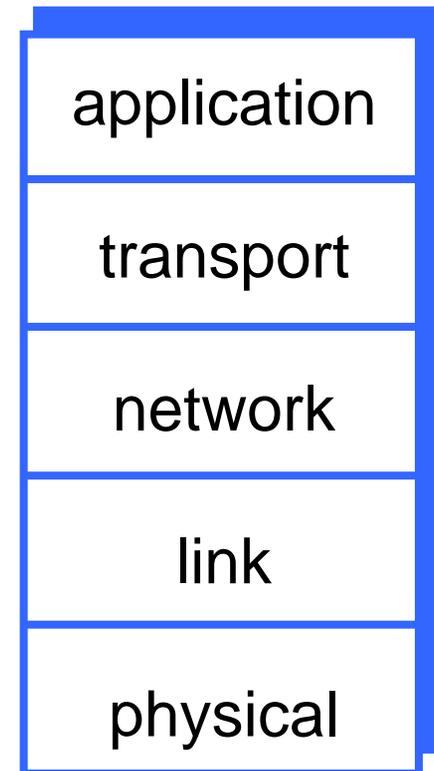
Internet Protocol Stack (2)

Each layer:

- Distributed.
- "Entities" implement layer functions at each node.
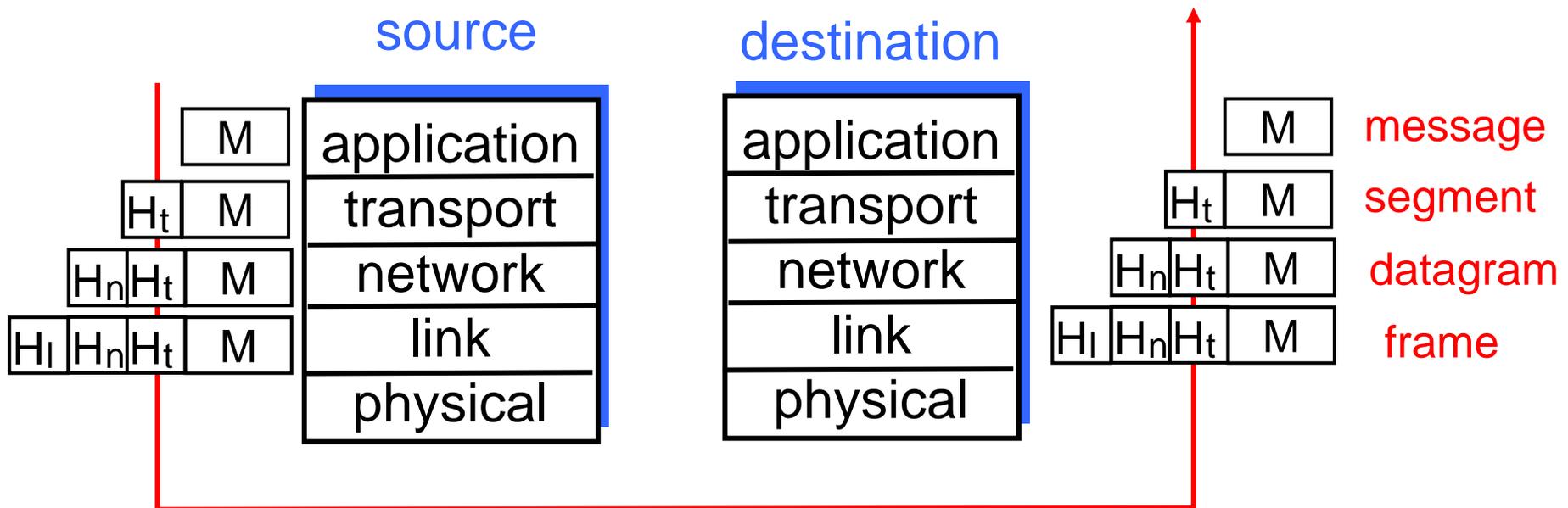- Entities perform actions, exchange messages with peers.
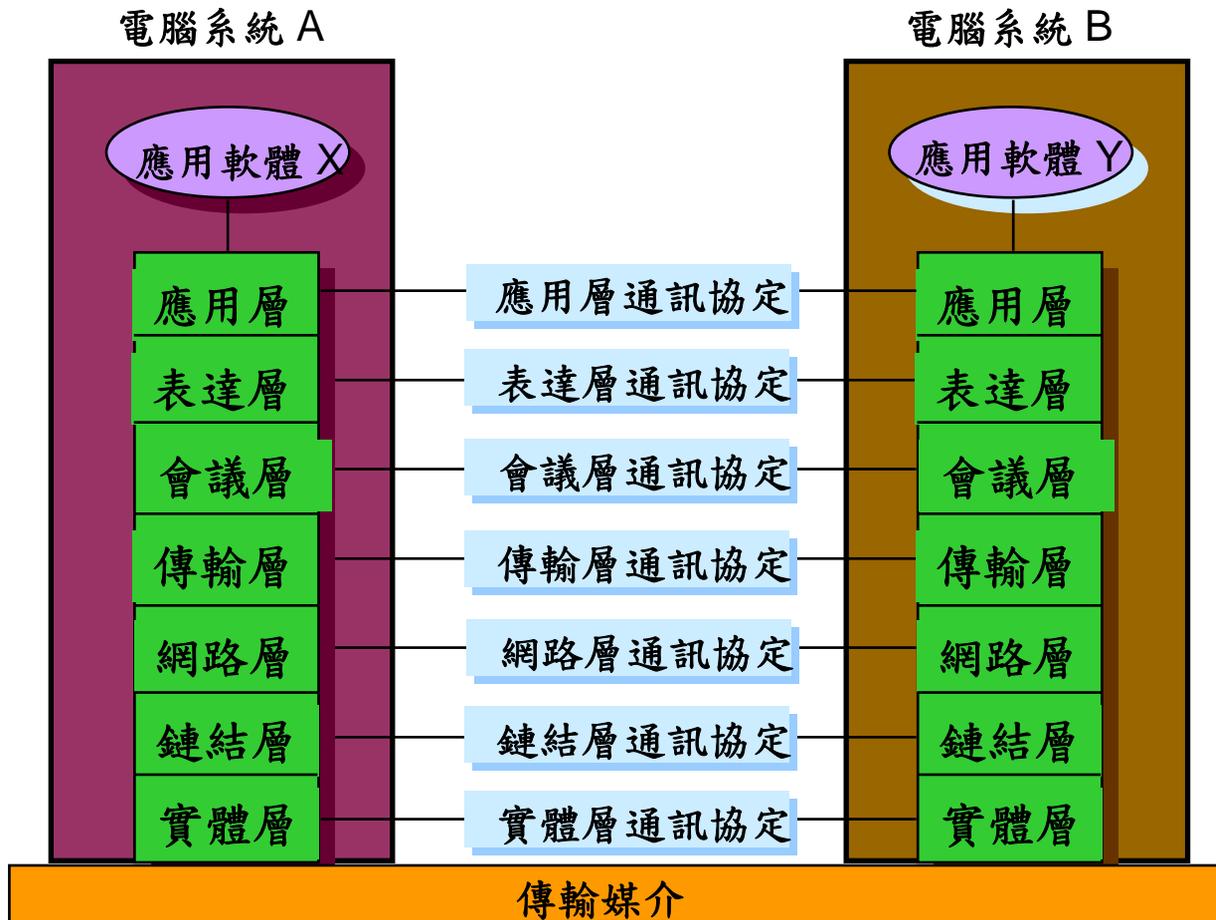
Internet Protocol Stack (3)

Protocol Layering & Data Encapsulation

- Each layer takes data from above.
  - Adds header information to create new data unit (PDU: protocol data unit).
  - Passes new data unit (SDU: service data unit) to layer below.

source	destination	
M **application**	**application**	M — message
H$_t$ M **transport**	**transport**	H$_t$ M — segment
H$_n$ H$_t$ M **network**	**network**	H$_n$ H$_t$ M — datagram
H$_l$ H$_n$ H$_t$ M **link**	**link**	H$_l$ H$_n$ H$_t$ M — frame
physical	**physical**	

ISO Protocol Stack

電腦系統 A

應用軟體 X

應用層	應用層通訊協定
表達層	表達層通訊協定
會議層	會議層通訊協定
傳輸層	傳輸層通訊協定
網路層	網路層通訊協定
鏈結層	鏈結層通訊協定
實體層	實體層通訊協定

電腦系統 B

應用軟體 Y

應用層
表達層
會議層
傳輸層
網路層
鏈結層
實體層

傳輸媒介

ISO Protocol Stack & Data Encapsulation

往下送時訊框包裝

往上送時訊框拆裝

應用軟體 X

資料 | 資料 | 資料 | 資料

應用軟體 Y

FTP/HTTP/ Telnet/DNS	應用層	AH 資料	應用層	FTP/HTTP/ Telnet/DNS
	表達層	PH 資料	表達層	
	會議層	SH 資料	會議層	
TCP/UDP	傳輸層	TH 資料	傳輸層	TCP/UDP
IP	網路層	NH 資料	網路層	IP
CSMA/CD	鏈結層	F A C 資料 FCS F	鏈結層	CSMA/CD
	實體層	位元串	實體層	

通訊路徑
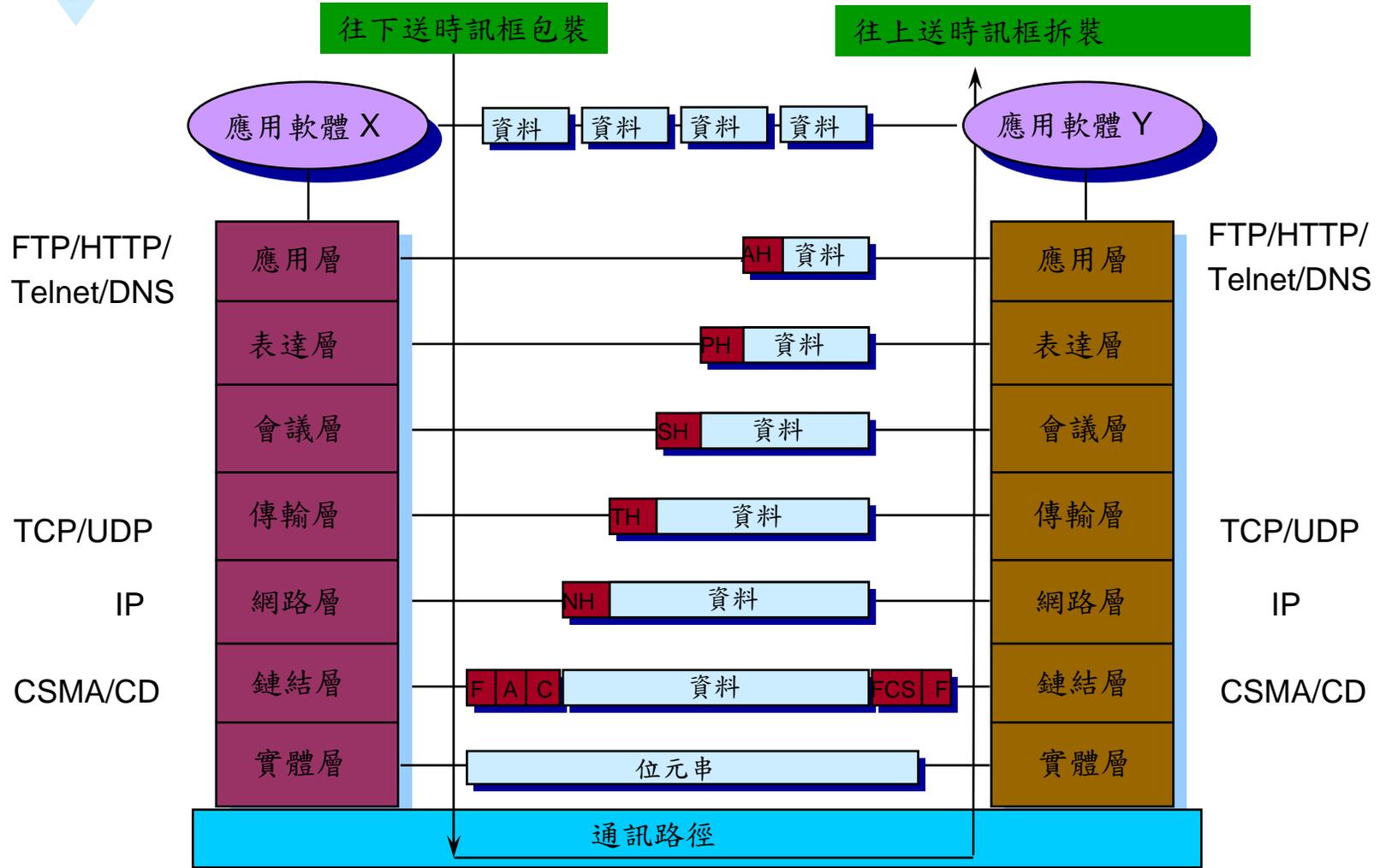
Urgent Issues to Solve before IPv6 deployment

- Running out of IPv4 address.
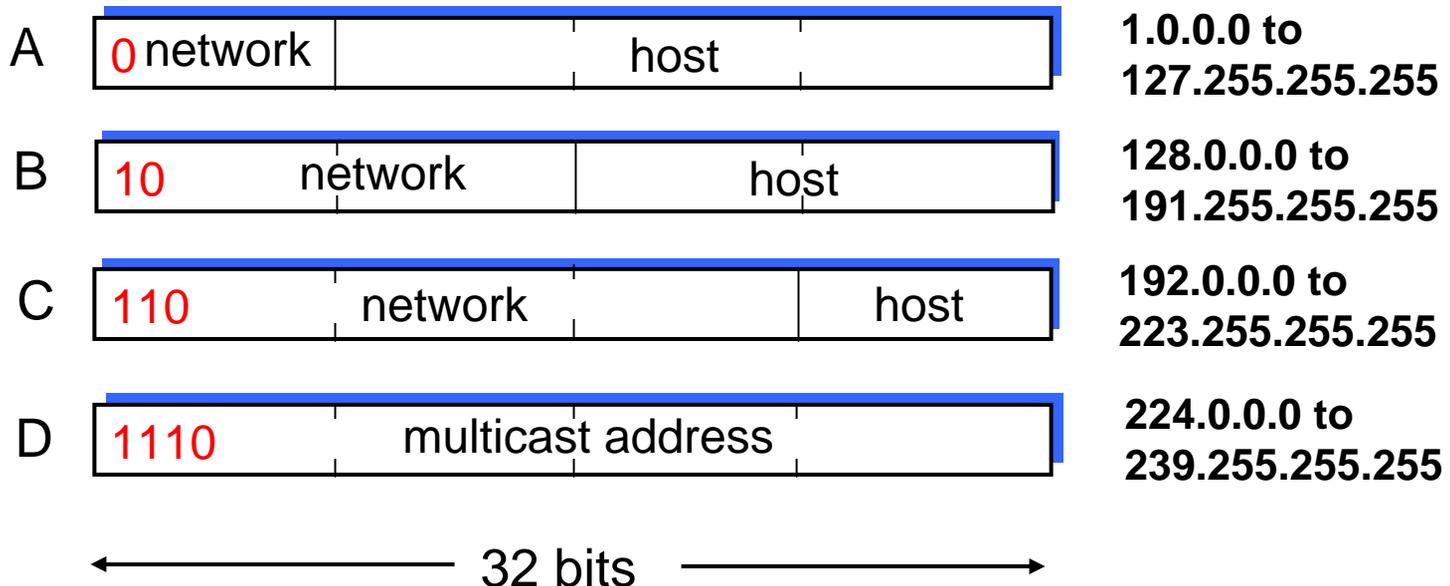- Growth of routing entries in the router.
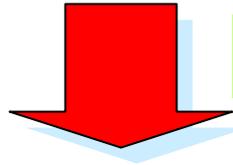
Short Term Solution

- CIDR: Classless Inter-Domain Routing.
  - (Before) 4 classes: classful addressing (is not suitable).
  - Can be useful even with IPv6.
- NAT: Network Address Translation.
  - We need NAT for inter-networking with IPv4 and IPv6.
  - We do not need with "native" IPv6.
- Private IP Address.
  - Can be useful even with IPv6.
- DHCP.

Features of CIDR (1)

- Before: IPv4 address classification.
  - Class A (8 bits), Class B(16 bits), Class C(24 bits), Class D (multicast), Class E (11110; for future use).

class

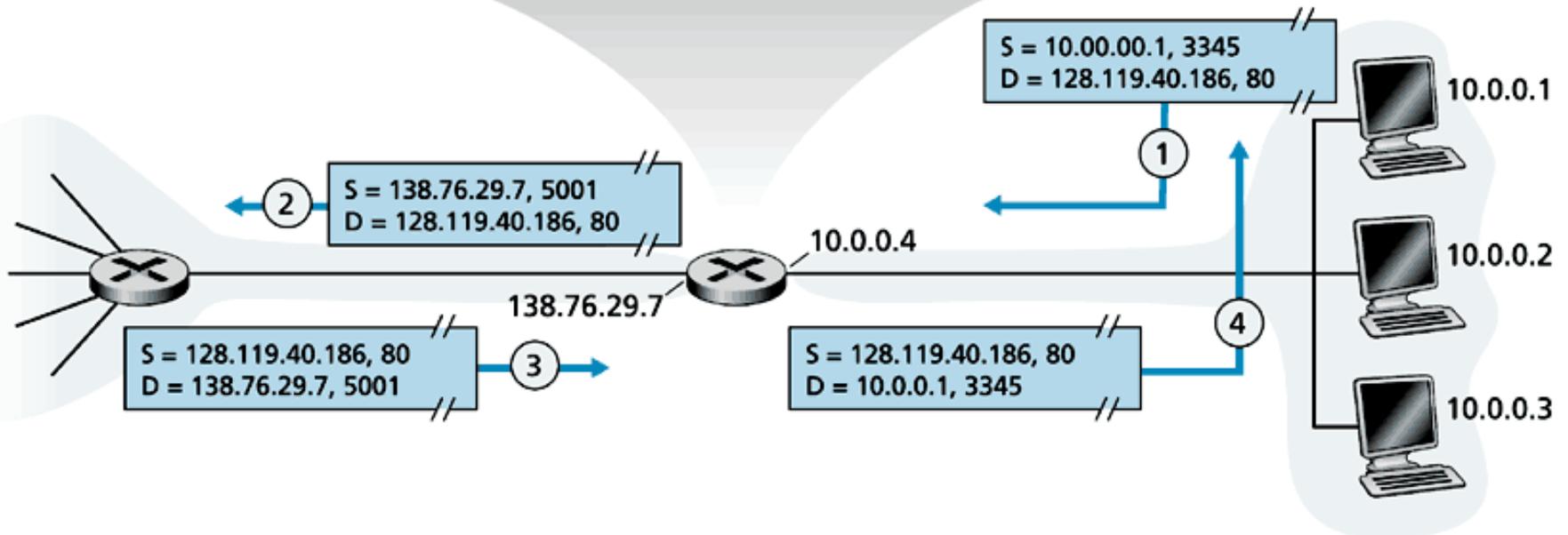| A	0 network	host		1.0.0.0 to 127.255.255.255
B	10 network	host		128.0.0.0 to 191.255.255.255
C	110 network	host		192.0.0.0 to 223.255.255.255
D	1110 multicast address			224.0.0.0 to 239.255.255.255

← 32 bits →

Features of CIDR (2)

- CIDR: Network ID -> any length.
  - a.b.c.d/x : X represents network ID (prefix length).
  - Subnetting: 2000 hosts -> a.b.c.d/21.

ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Organization 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Organization 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	…..	….	….
Organization 7	11001000 00010111 00011110	00000000	200.23.30.0/23

NAT (Network Address Translation)

NAT translation table	
WAN side	LAN side
138.76.29.7, 5001	10.00. 00.1, 3345
. . .	. . .

S = 10.00.00.1, 3345
D = 128.119.40.186, 80

①

S = 138.76.29.7, 5001
D = 128.119.40.186, 80

②

10.0.0.4

138.76.29.7

S = 128.119.40.186, 80
D = 138.76.29.7, 5001

③

S = 128.119.40.186, 80
D = 10.0.0.1, 3345

④

10.0.0.1

10.0.0.2

10.0.0.3

Private IP Addresses

- Reserved by IANA, RFC 1918 defines three ranges of IP address to be the private IP address.

  Address range   mask
  ```
  10.0.0.0    – 10.255.255.255,  255.0.0.0
  172.16.0.0  – 172.31.255.255,  255.240.0.0
  192.168.0.0 – 192.168.255.255, 255.255.255.0
  ```

- Private IP address for nodes, that does not need to access to outside nodes (Internet) with IP-level.

- For pure internal business.

- These hosts with private IP address are behind firewall router.

- Multiple nodes, in different private/internal networks, can be allocated the same IP address.

DHCP (1)
(Dynamic Host Configuration Protocol)

- Allow host to dynamically obtain its IP address from network server when it joins network.
    - Can renew its lease on address in use.
    - Allows reuse of addresses.
    - Support for mobile users who want to join network.
- DHCP overview :
    - Host broadcasts "DHCP discover" msg.
    - DHCP server responds with "DHCP offer" msg.
    - Host requests IP address: "DHCP request" msg.
    - DHCP server sends address: "DHCP ack" msg.

DHCP server:
223.1.2.5

Arriving client

DHCP (2)
(Dynamic Host Configuration Protocol)

DHCP discover

src: 0.0.0.0, 68
dest: 255.255.255.255,67
DHCPDISCOVER
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255,68
DHCPOFFER
yiaddrr: 223.1.2.4
transaction ID: 654
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

DHCP request

src: 0.0.0.0, 68
dest: 255.255.255.255, 67
DHCPREQUEST
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255,68
DHCPACK
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

Time

Time

IPv4 Packet Format

IP protocol version Number (4 bits)

header length (4 bits)

type of data (8 bits)

max number remaining hops (seconds) (8 bits)

upper layer protocol to deliver payload to (8 bits)

■ Header length 20~60 bytes (at least 20 bytes).

32 bits

ver	head. len	type of service	length	
16-bit identifier			flgs	fragment offset
time to live	upper layer		Internet checksum	
source IP address (32 bit)				
destination IP address (32 bit)				
Options (if any)				
data (variable length) Including a typical TCP or UDP segment				

total datagram length (16 bits)

for packet fragmentation/ Reassembly (16 bits, 3 bits, 13bits)

error detect (16 bits)

E.g. timestamp, record route taken, or specify a list of routers to visit.

IPv6 Packet Format

IP protocol version Number (4 bits)

like TOS in IPv4, identify priority among datagrams in flows (8 bits)

Payload length (16 bits)

- Header changes to facilitate QoS.
- New "anycast" address: route to "best" of several replicated servers.
- Fixed-length 40 bytes header.
- No fragmentation in router.
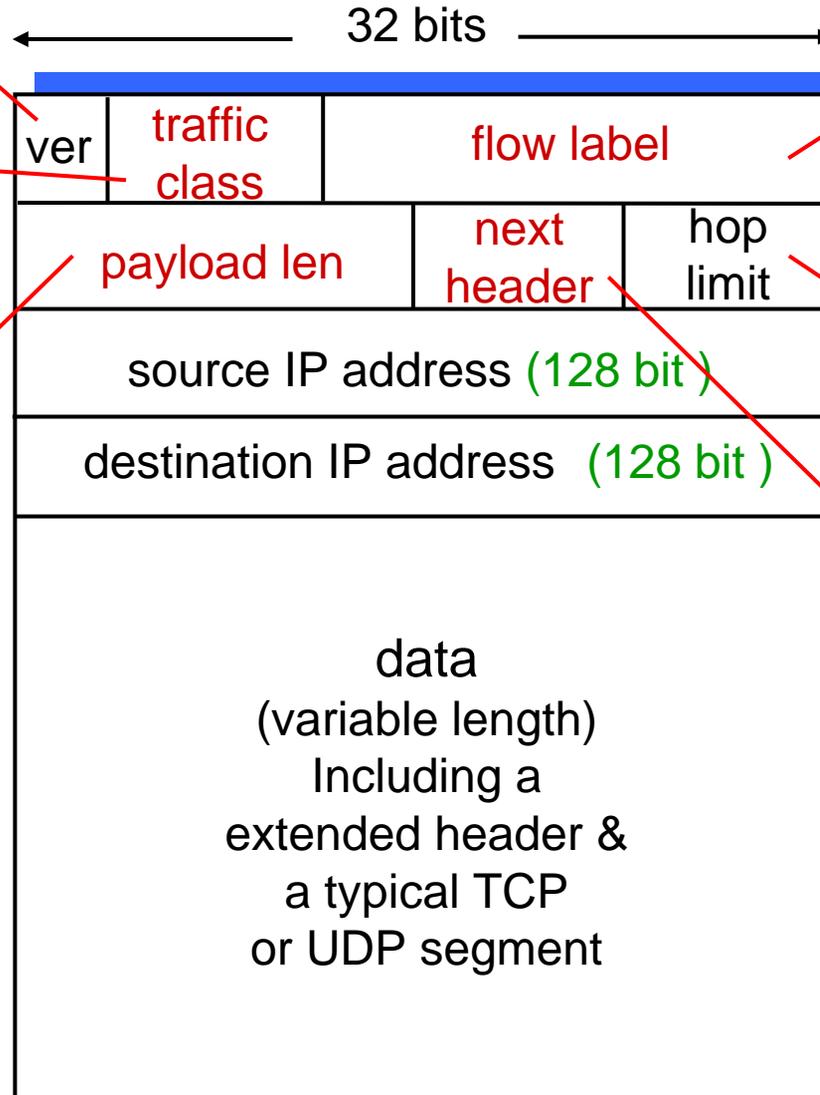
identify datagrams in the same flow (20 bits)

max number remaining hops (hops) (8 bits)

identify the upper layer protocol carry in the extended header (8 bits)

32 bits

ver	traffic class	flow label	
payload len		next header	hop limit
source IP address (128 bit)			
destination IP address (128 bit)			
data (variable length) Including a extended header & a typical TCP or UDP segment			

Setup IPv6 in Windows XP (1) (Using Command Line)

- Using DOS Command: ipv6 install.
- View ipv4/ipv6 configuration: ipconfig.

Setup IPv6 in Windows XP (2) (Using GUI: Schematic)
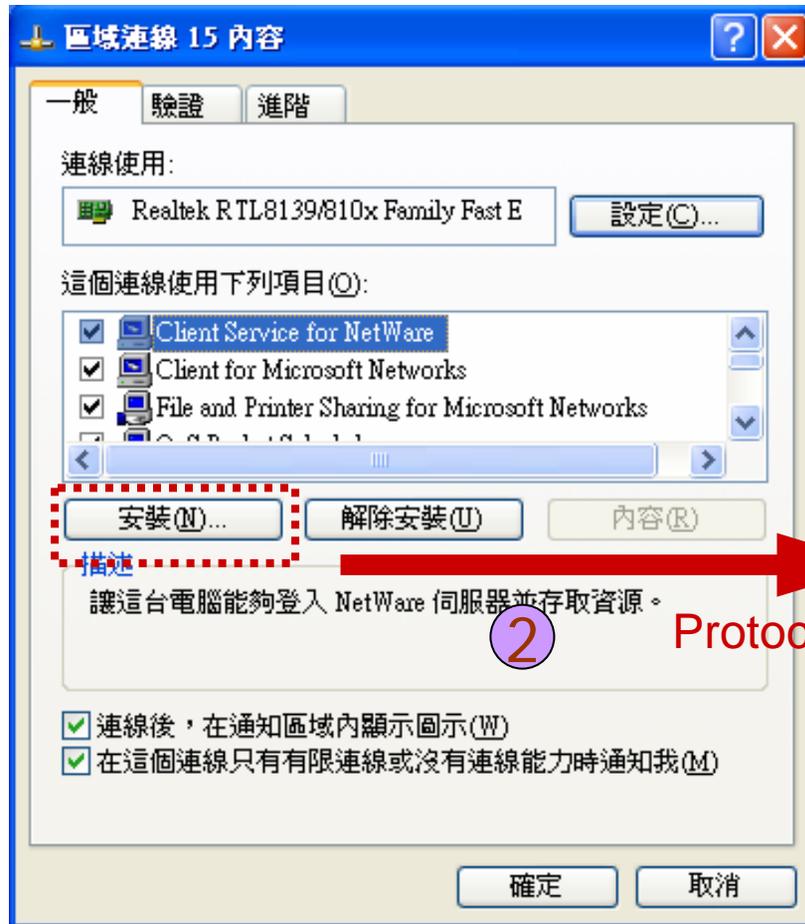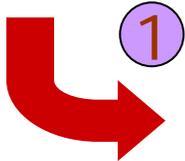
Setup IPv6 in Windows XP (3) (Using GUI: Schematic)

Setup IPv6 in Linux (Using Command Line)

- Setup IPv6 in Linux (RedHat 9.0):
    - Use "root" login to your Linux server.
    - # insmod ipv6
    - # ifconfig eth0
    - See as follows:
    - eth0   Link encap: Ethernet   HWaddr 00:64:11:07:14:11
    -           inet addr: 192.168.0.1   Bcast:192.168.0.255
              Mask:255.255.255.0
    -           inet6 addr: fe80::264:11ff:fe07:1411/64 Scope:Link
    -           inet6 addr: 2002:ac15:21f:1::1/64 Scope:Global
    -           UP BROADCAST RUNNING MULTICAST   MTU:1500   Metric:1
    -           RX packets:212   errors:0   dropped:0   overruns:0   frame:0
    -           TX packets:391   errors:0   dropped:0   overruns:0   carrier:0
    -           collisions:0   txqueuelen:1000
    -           RX bytes:22160 (21.6 kiB)   TX bytes:272284 (265.9 kiB)
    -           Interrupt:6

IPv6 Certification Test (1) (Conformance & IOT)

http://www.ipv6ready.org/frames.html

IPv6 Certification Test (2) (Conformance & IOT)

■ IPv6 certification test tool:

PMTU (Path Maximum Transmission Unit) Discovery

- Each link has a MTU value for packet size.
- The smallest MTU on the path.
- Using ICMPv6 Packet Too Big message.

Initial PMTU=1500bytes;
(1) PMTU=1400bytes;
(2) PMTU=1280bytes.

Initial PMTU=1400bytes;
(1) PMTU=1280bytes.

Initial PMTU=1280bytes;

Initial PMTU=1350bytes;

Client C1 (3FFE::C1)

v6 Router R1   v6 Router R2   v6 Router R3   v6 Router R4

Client C2 (3FFE::C2)

IPv6 Local Network

Initial PMTU=1500bytes;
(1) PMTU=1400bytes;
(2) PMTU=1280bytes.

IPv6 Backbone Network

Initial PMTU=1350bytes;

IPv6 Local Network