Computer Networks

L6 – Network Layer I

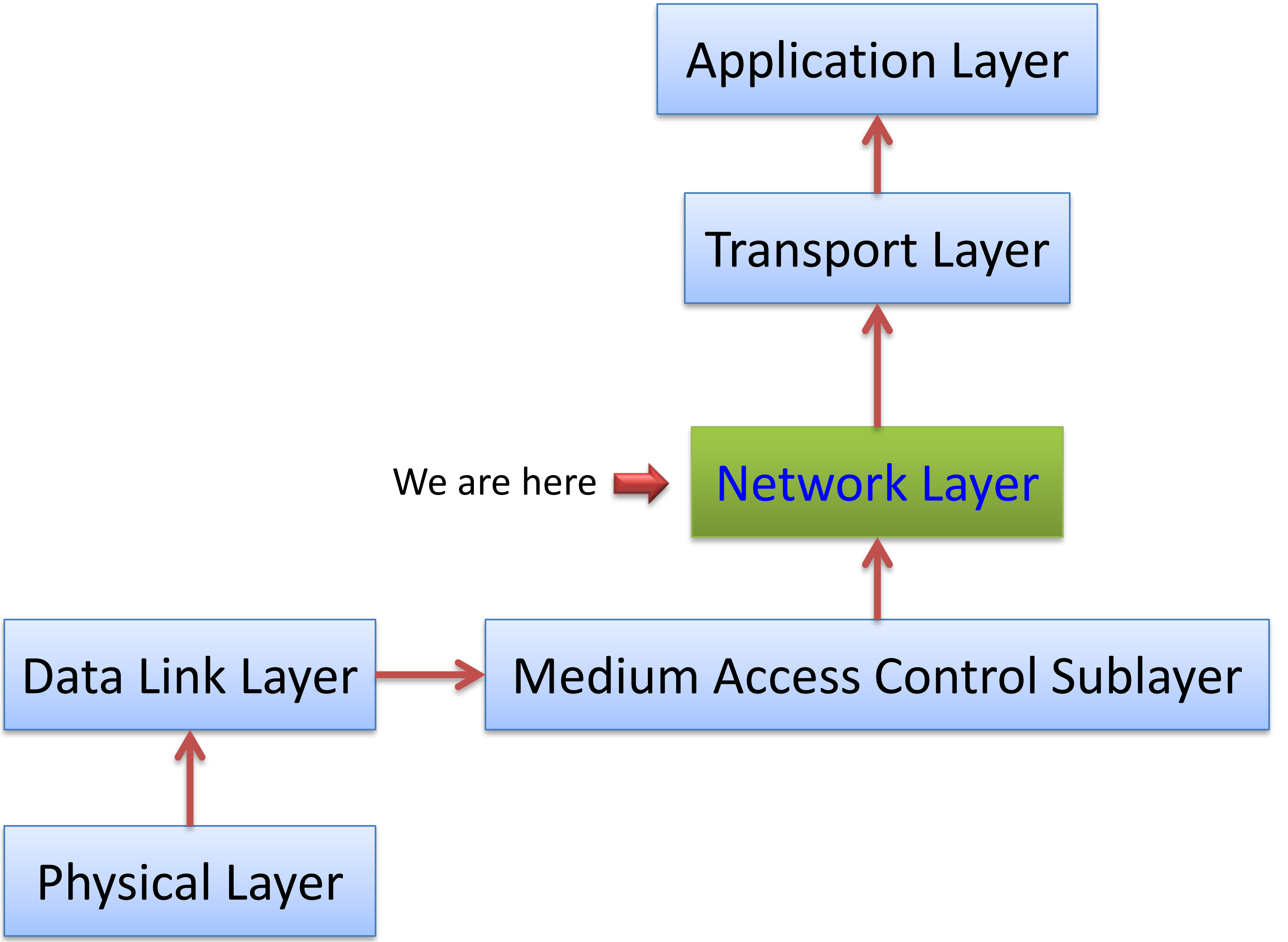
Lecturer: CUI Lin

Department of Computer Science
Jinan University

The Network Layer

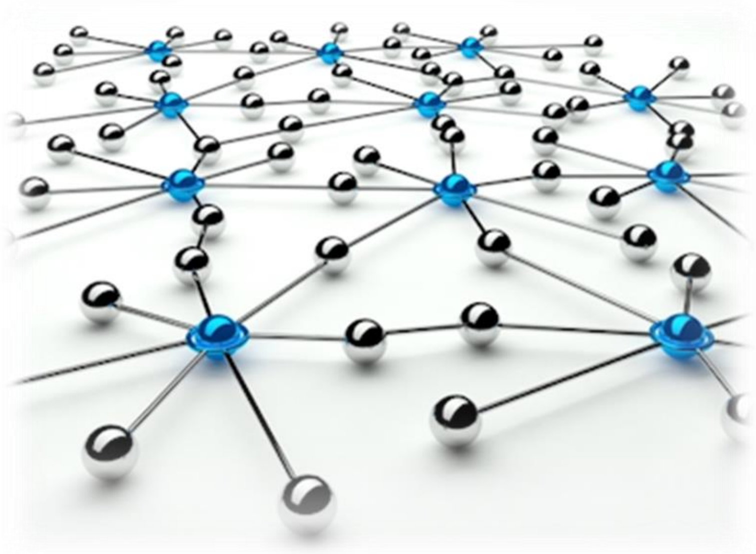
Chapter 5

Roadmap of this course



The Network Layer

- Responsible for delivering packets between endpoints over multiple links
  - Concerns about getting packets from source to destination, no matter how many hops it may take.
  - The lowest layer that deals with end-to-end transmission.



Application
Transport
Network
Link
Physical

Topics in Network Layer

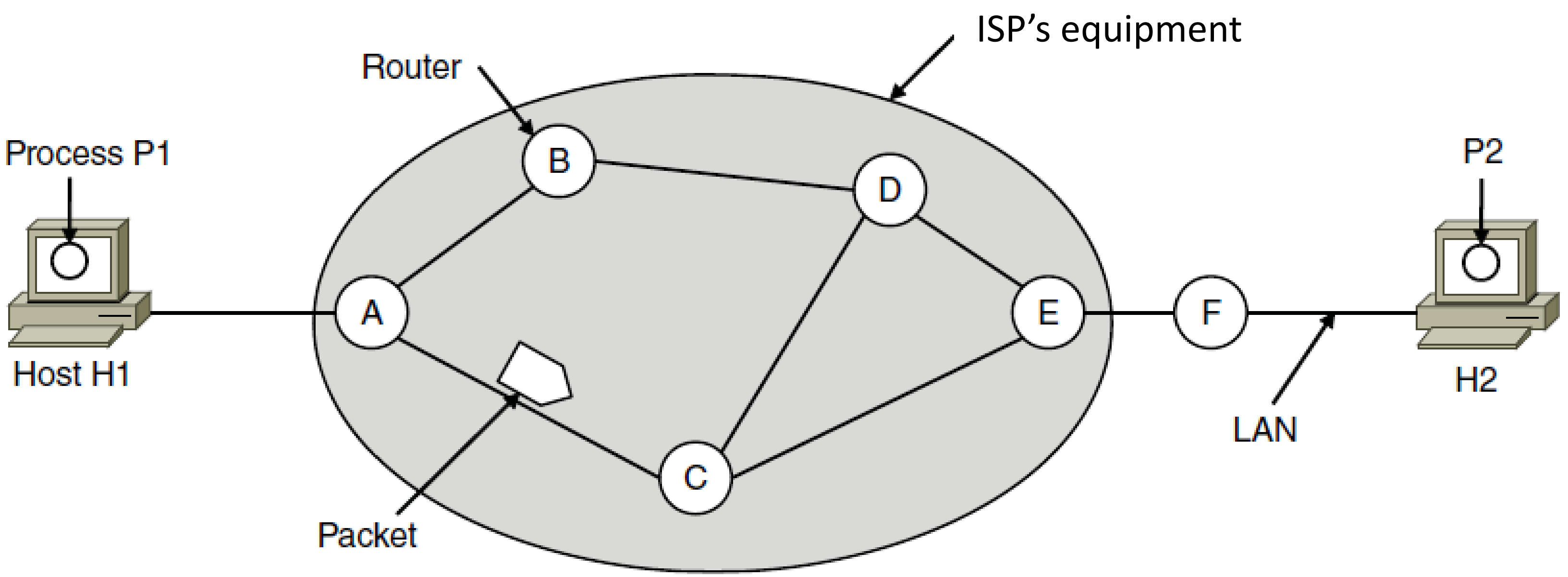
- Design Issues
- Internetworking
- Network Layer in the Internet
  - IP
- Routing Algorithms
- Internet Routing and Multicasting

Network Layer Design Issues

- Store-and-forward packet switching
- Connectionless service – datagrams
- Connection-oriented service – virtual circuits
- Comparison of virtual-circuits and datagrams

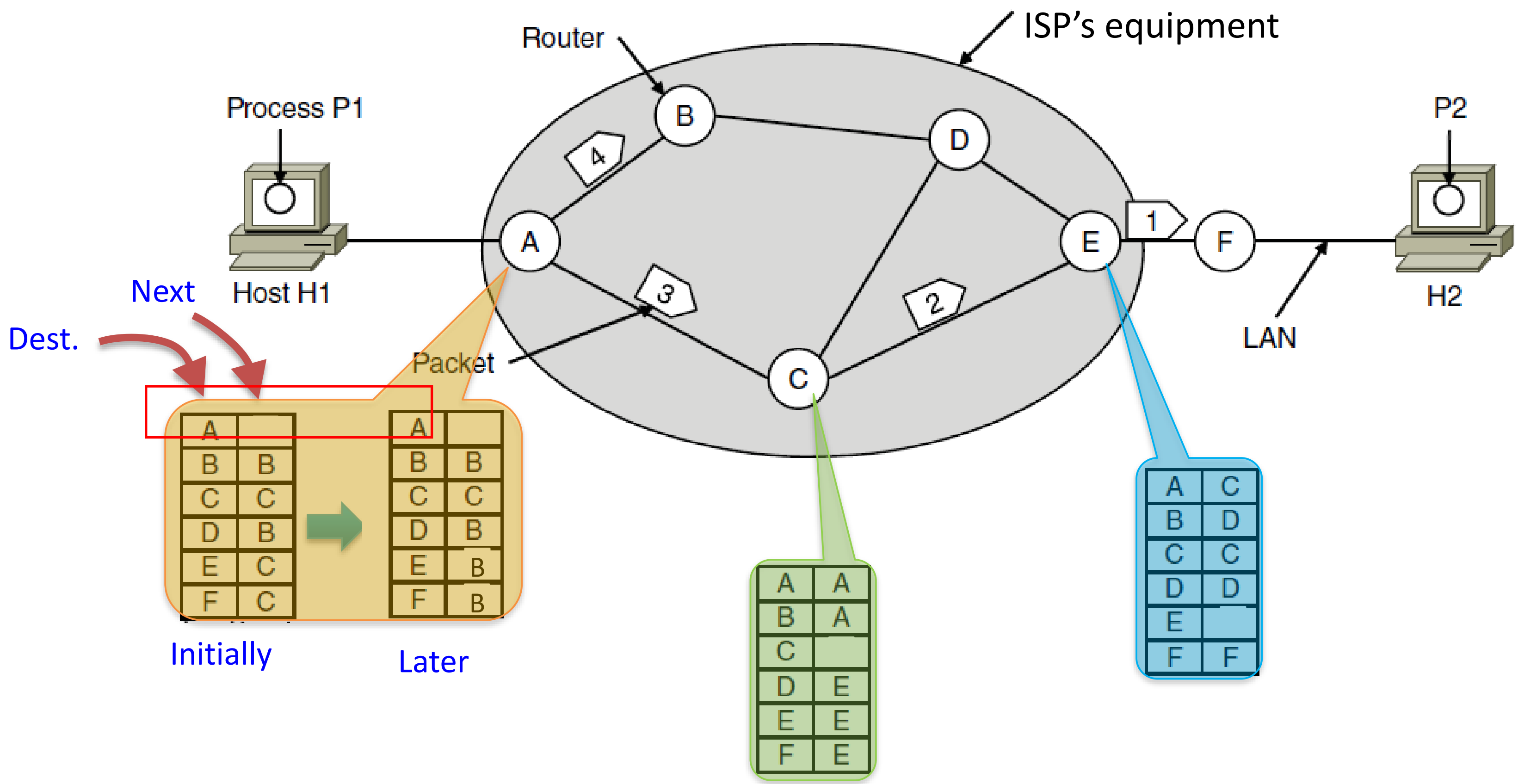
Store-and-Forward Packet Switching

- Hosts send packets into the network
- Packets are forwarded by routers hop by hop using store-and-forward switching



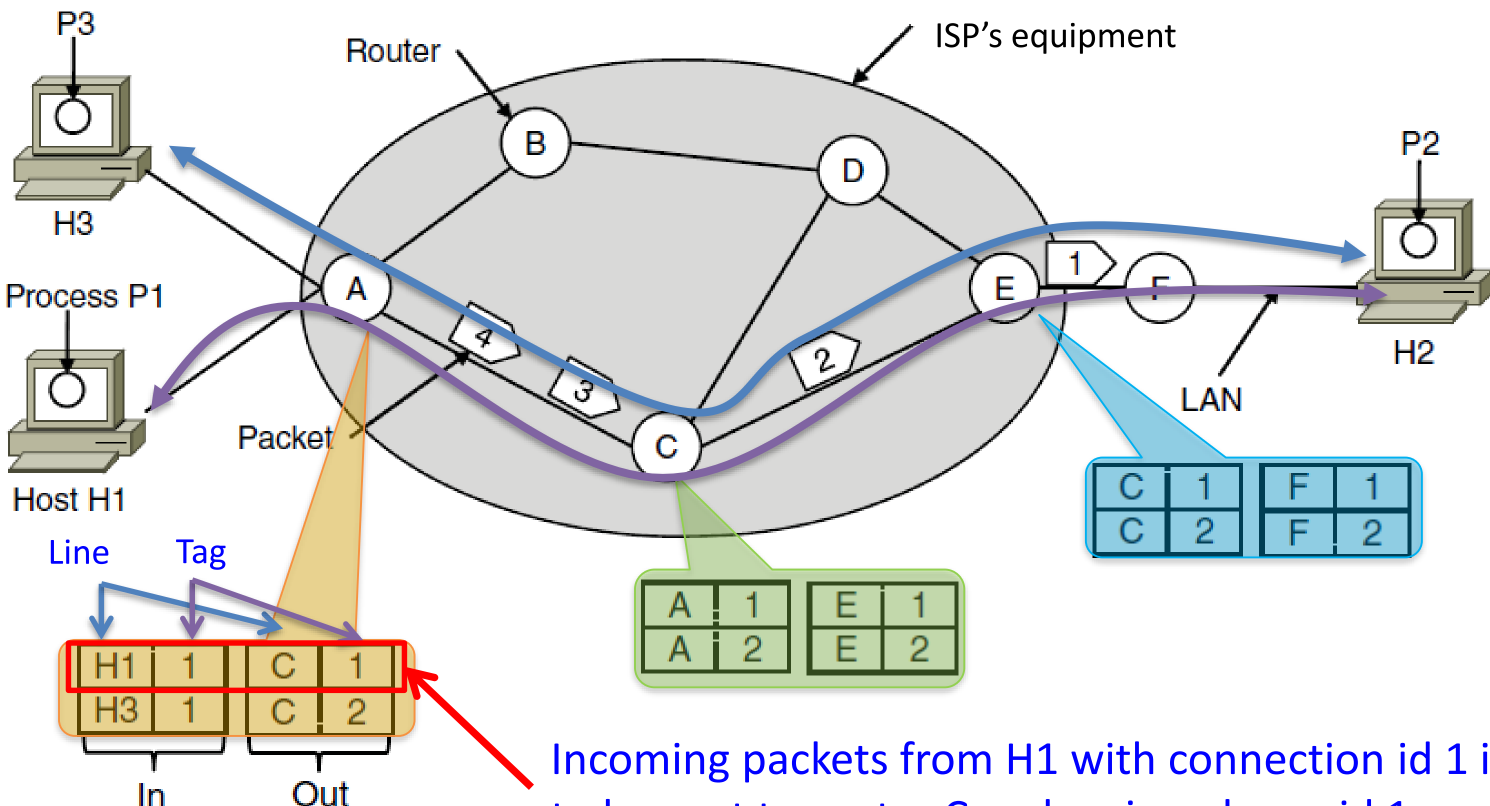
Connectionless Service – Datagrams

- Packet is forwarded using destination address inside it
  - Different packets may take different paths, e.g., IP



Connection-Oriented – Virtual Circuits

- Packet is forwarded along a virtual circuit using tag inside it
  - Virtual circuit (VC) is set up ahead of time



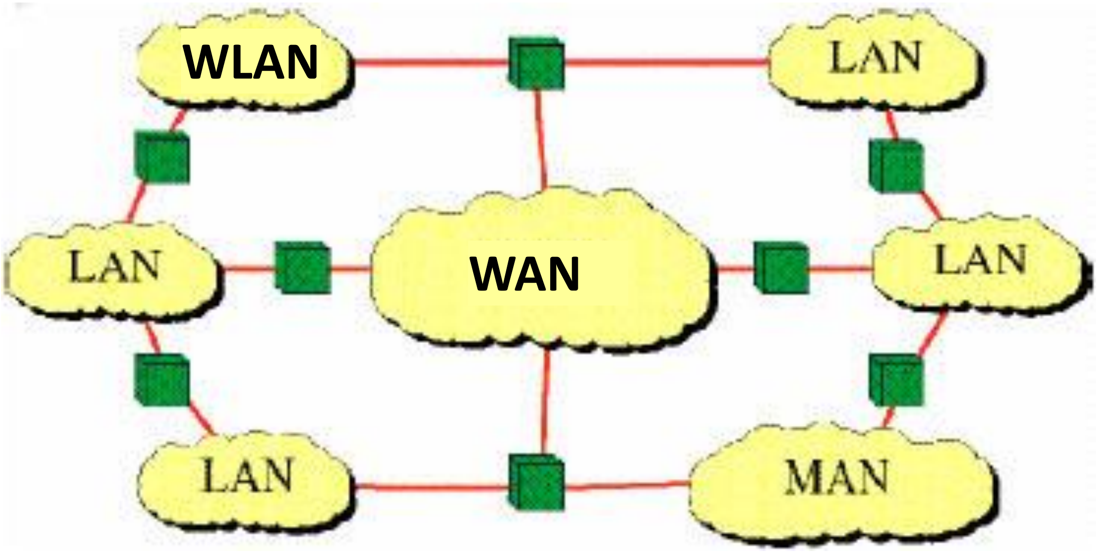
Incoming packets from H1 with connection id 1 is to be sent to router C and assigned new id 1

Datagrams vs. Virtual-Circuits Networks

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Internetworking

Internetworking joins multiple, different networks into a single larger network



Internetworking

- Multiple networks and multiple network types (protocols) are a fact of life
  - Ethernet, WiFi, satellite networks, cable networks, telephone networks, powerlines
- internet:
  - Connection of two or more networks
- The Internet, the more generic term, networks of TCP/IP

How networks differ

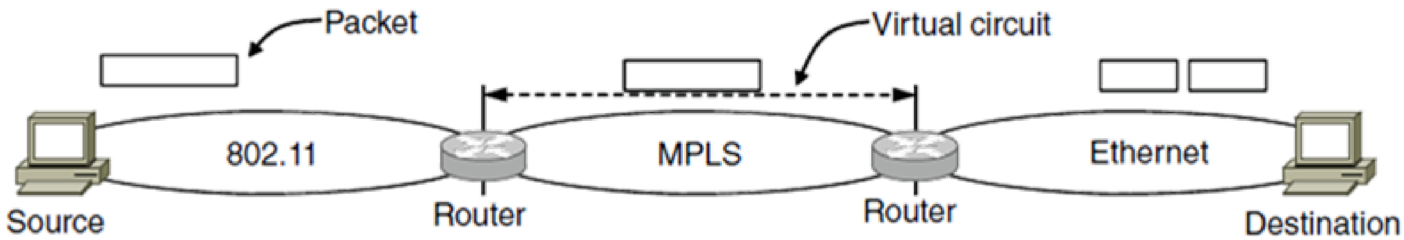
Differences can be large and complicates

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

PSTN vs. Ethernet

Ethernet vs. IEEE 802.11

How networks can be connected?



- Two basic choices:
  - Build devices that translate or convert packets from each kind of network into packets for each other network.
  - By adding a layer of indirection and building a common layer on top of the different networks.
- In either case, the devices are placed at the boundaries between networks, e.g., routers or gateways

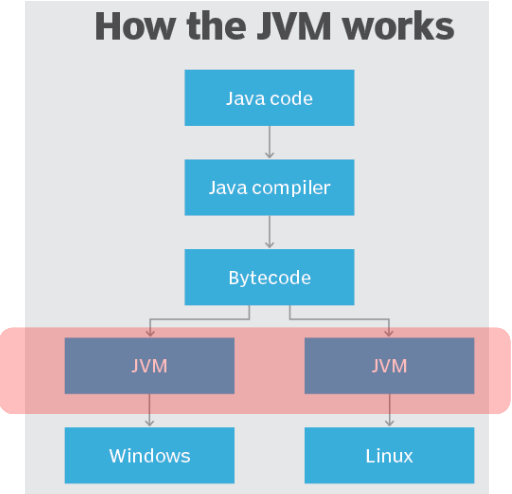
The Philosophy

- The classic solution for all such problems in computer science is to

"Add one level of indirection"

Similar example: Java VM

JVM



An idea for a universal "internet" packet

- IP: a common layer to hide the differences of existing networks
- Cerf and Kahn's idea (1974)
  - They were awarded the 2004 Turing Award
- IP provides a universal packet format that all routers recognize and that can be passed through almost every network
  - Telephone networks, wireless LAN, Ethernet

Internetworking Devices

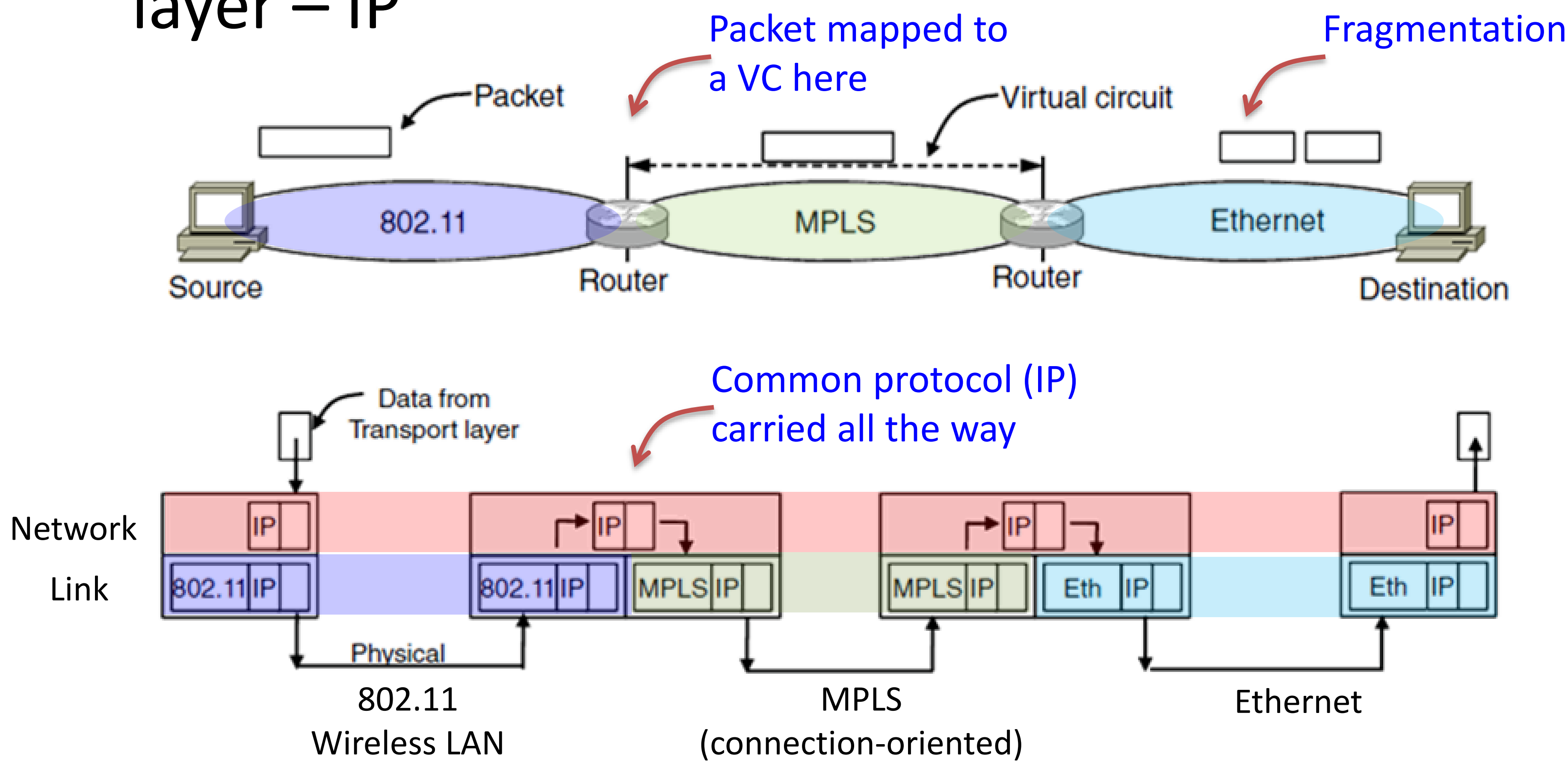
- Repeaters, hubs (physical layer)
  - Just move the bits from one wire to another.
- Bridges and Switches (data link layer)
  - Only with minor protocol translation in the process, e.g. 10/100/1000Mbps Ethernet switches
- Routers (network layer)
  - They can connect two networks (fully aware of different network technologies)

Router vs Switch Internetworking

- Bridges/switches are predominantly used to connect the same kind of network at the link layer, e.g., two Ethernet LANs.
- Routers connect different networks at the network layer, e.g., LAN and WAN.

How networks can be connected

- Internetworking based on a common network layer – IP

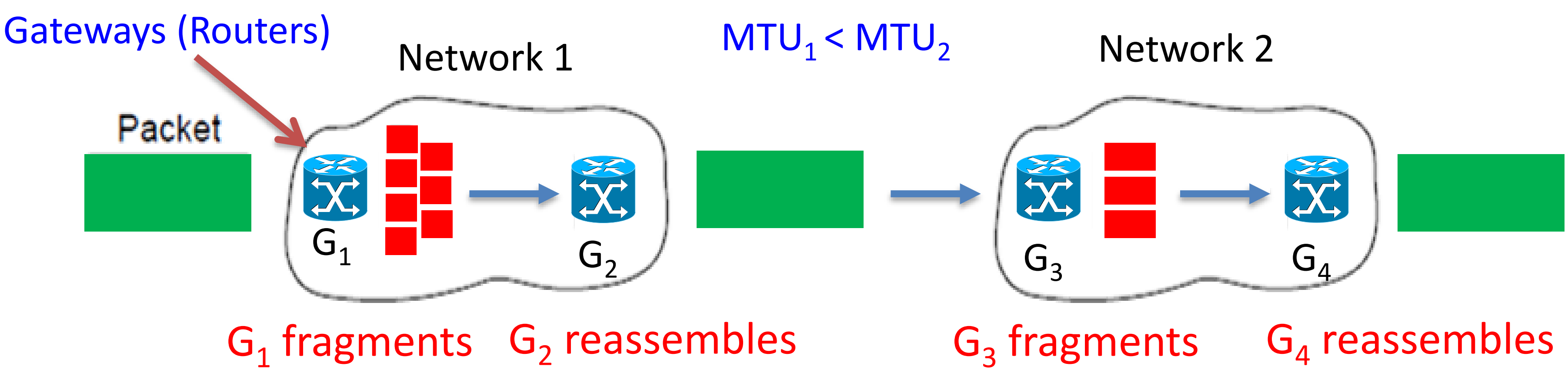


Packet Fragmentation

- Each network or link imposes some maximum size on its packets. These limits have various causes, e.g.,
  - Hardware (e.g., the size of an Ethernet frame)
  - Operating system (e.g., all buffers are 512 bytes)
  - Protocols (e.g., the number of bits in the packet length field)
- The smallest packet size on a path is called the Path MTU (Path Maximum Transmission Unit)
  - Difficult for source to know MTU

Packet Fragmentation

- Networks have different packet size (MTU)
  - Large packets sent with fragmentation & reassembly (分片和重组)



Transparent – packets fragmented / reassembled in **each** network

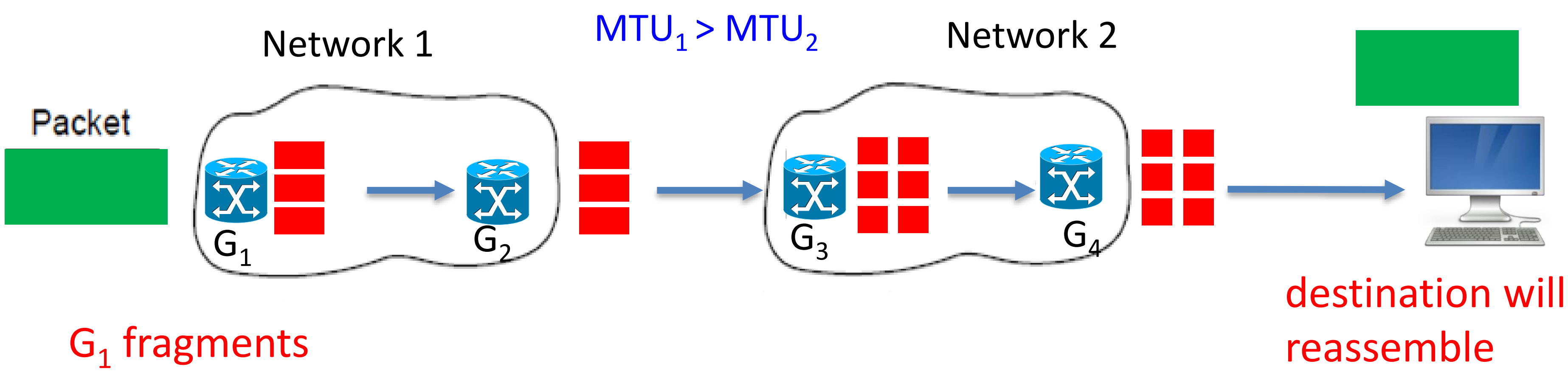
Transparent Fragmentation

Drawbacks

- The exit router must know when it has received all pieces
- All fragments must exit via the same router, some performance may be lost
- Fragments buffer needed
- The overhead for a packet required to repeatedly fragmented and reassembled passing through a series of small-packet networks

Packet Fragmentation

- Networks have different packet size (MTU)
  - Large packets sent with fragmentation & reassembly (分片和重组)



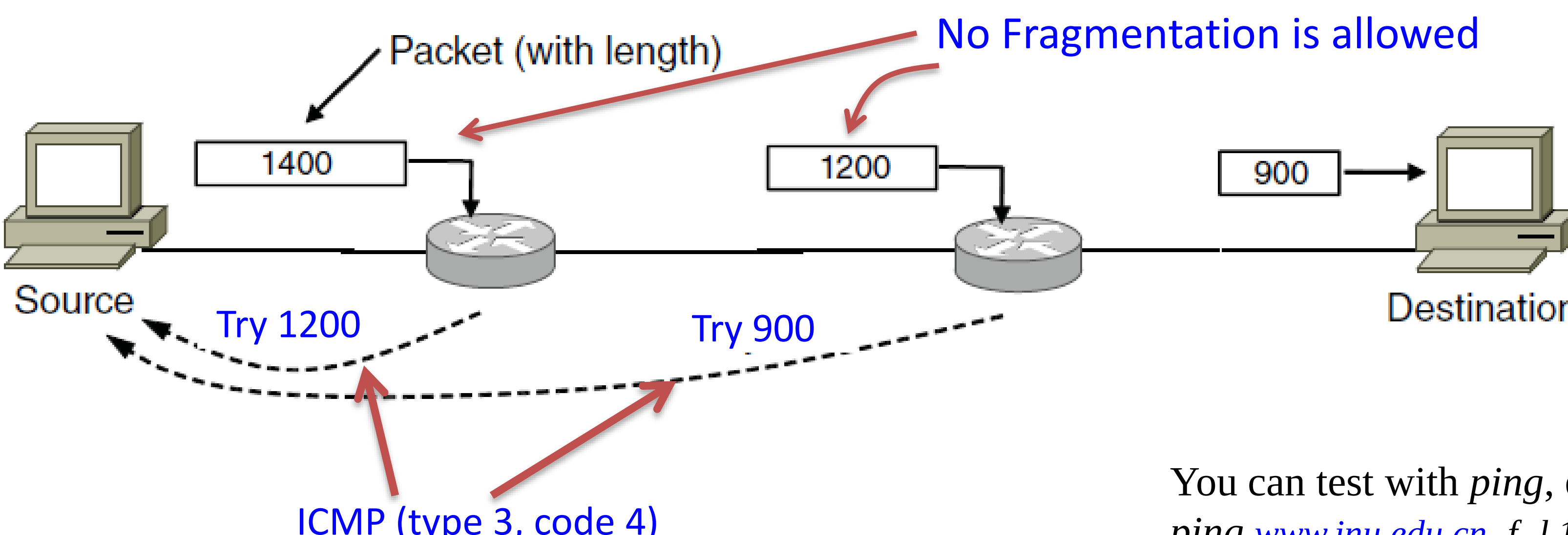
Non-transparent – fragments are reassembled at **destination**

Non-Transparent Fragmentation

- The main advantage is that it requires routers to do less work
  - IP works this way (TCP/IP)
- Problems are:
  - It requires every host to be able to do reassembly
  - Overhead of carrying along small segments lasts until destination (because each fragment must have a header)
  - A whole packet is lost if its fragments are lost

Path MTU Discovery

- Path MTU Discovery avoids network fragmentation
  – Routers return MTU (Max. Transmission Unit) to source and discard large packets



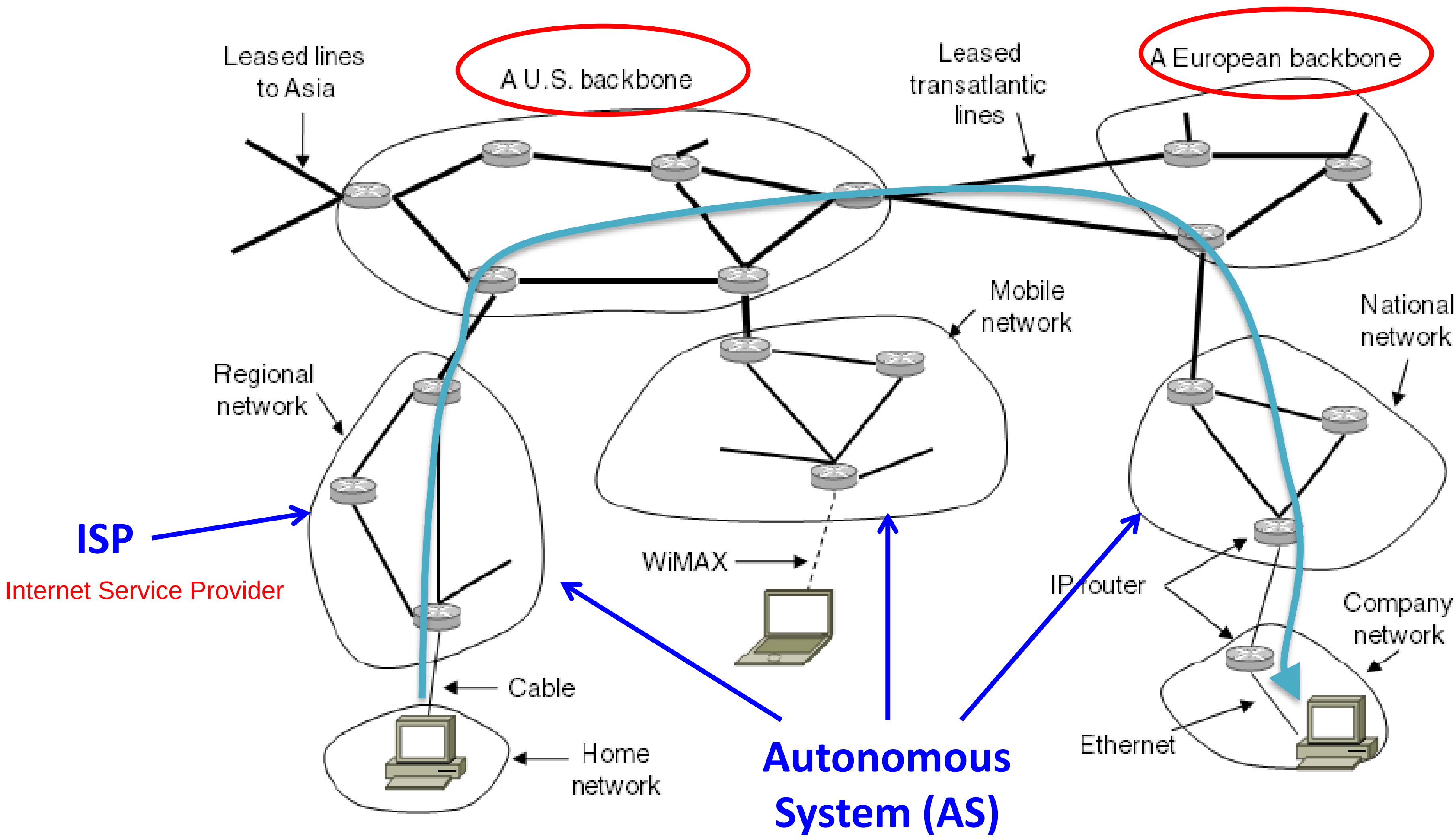
You can test with *ping*, e.g., *ping* *www.jnu.edu.cn -f -l 1500*

Network Layer in the Internet

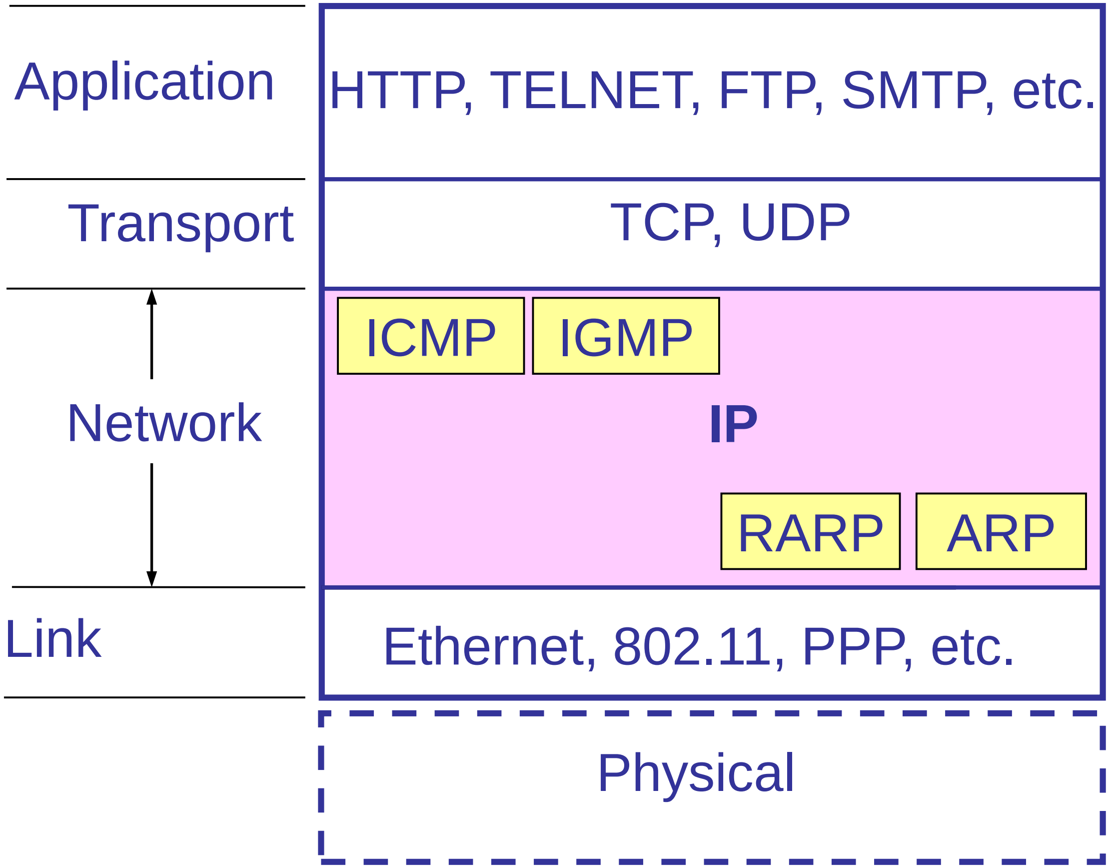
- IP Version 4
- IP Addresses
- IP Version 6
- Internet Control Protocols
- OSPF—An Interior Gateway Routing Protocol
- BGP—The Exterior Gateway Routing Protocol
- Internet Multicasting

The Internet Protocol (IP)

- Internet is an interconnected collection of many networks that is held together by the IP



TCP/IP Protocol Stack



ICMP: Internet Control Messages Protocol

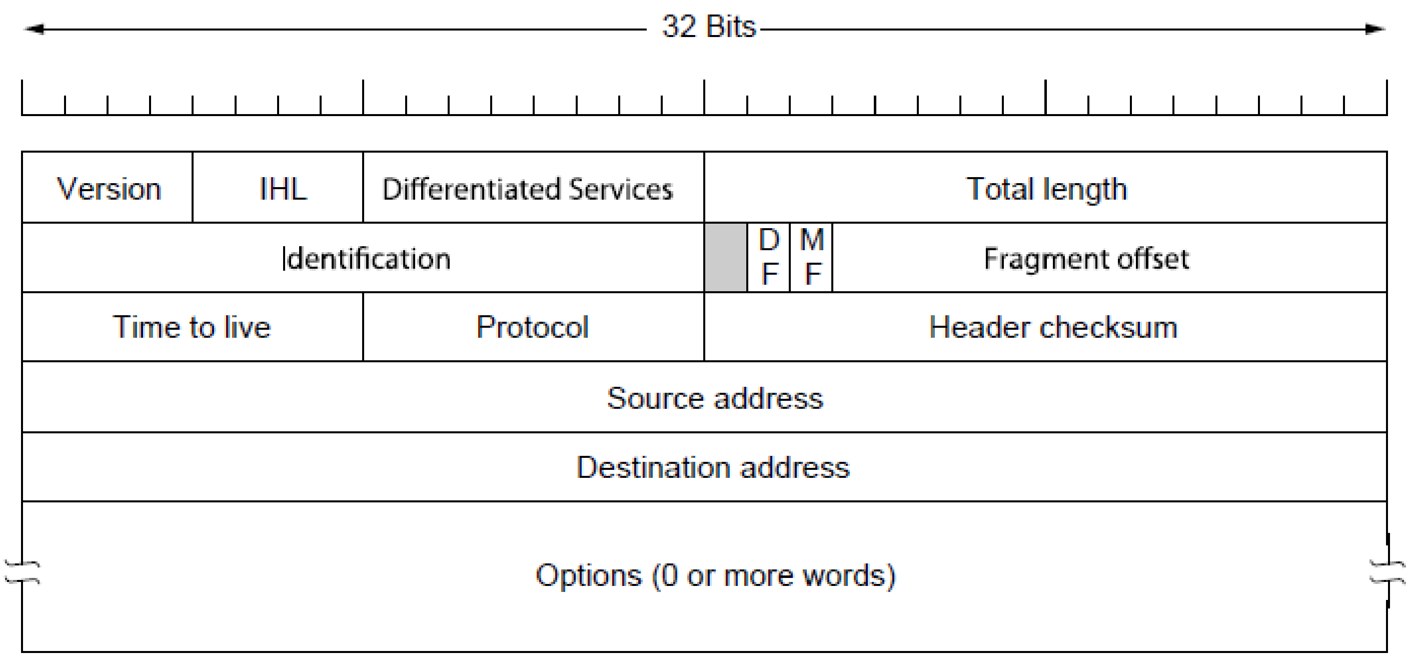
IGMP: Internet Group Management Protocol

ARP: Address Resolution Protocol

RARP: Reverse Address Resolution Protocol

IP Version 4 Protocol

- IPv4 (Internet Protocol) header is carried on all packets and has fields for the key parts of the protocol:



- Bits are transmitted from left to right and top to bottom.
- This is a ''big-endian'' network byte order. On little-endian machines (e.g., Intel x86), a software conversion is required on both transmission and reception.

IPv4 Header

TTL: max number remaining hops (decremented at each router, <=255)

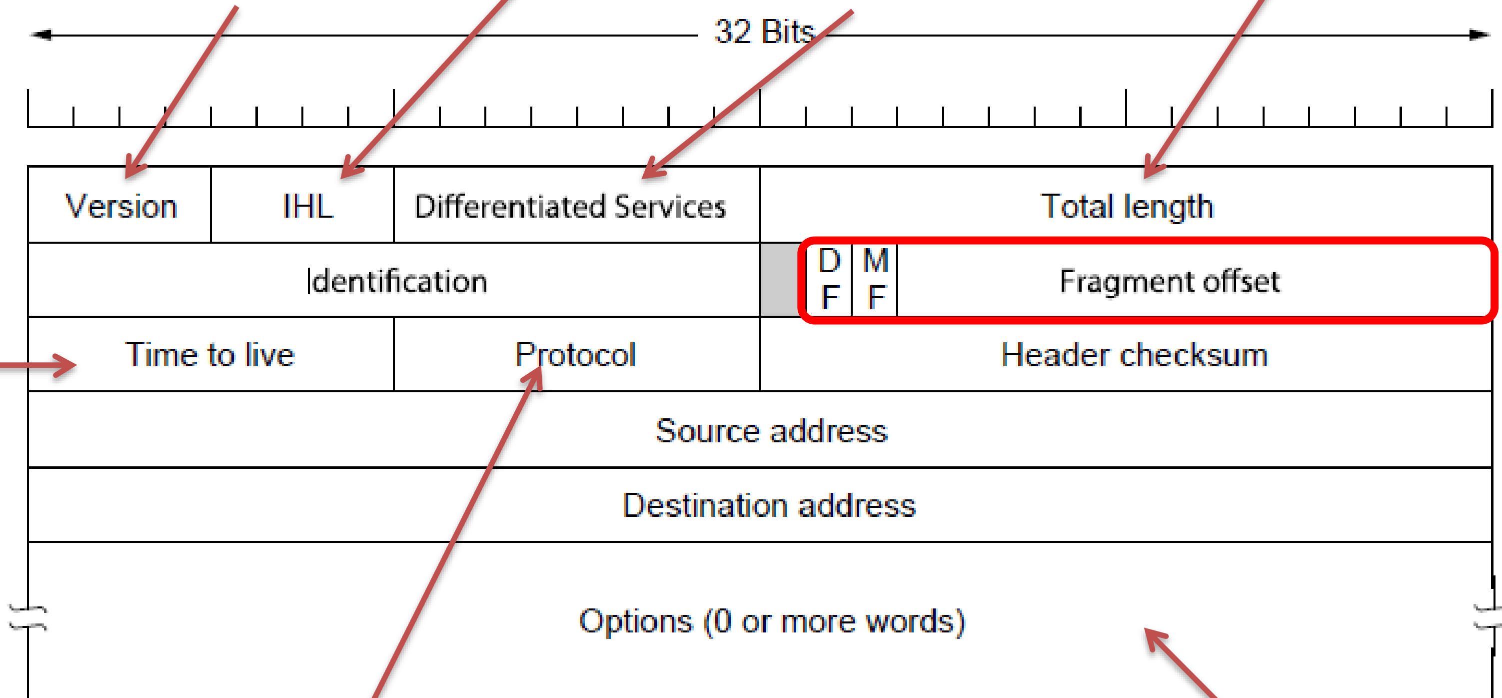
header length (in 32bits word, [5,15])

total datagram length, both header & data (bytes, <=65,535 bytes)

IP protocol version number

Service classes, old name TOS

fragmentation & reassembly



upper layer protocol in payload(e.g., TCP or UDP)

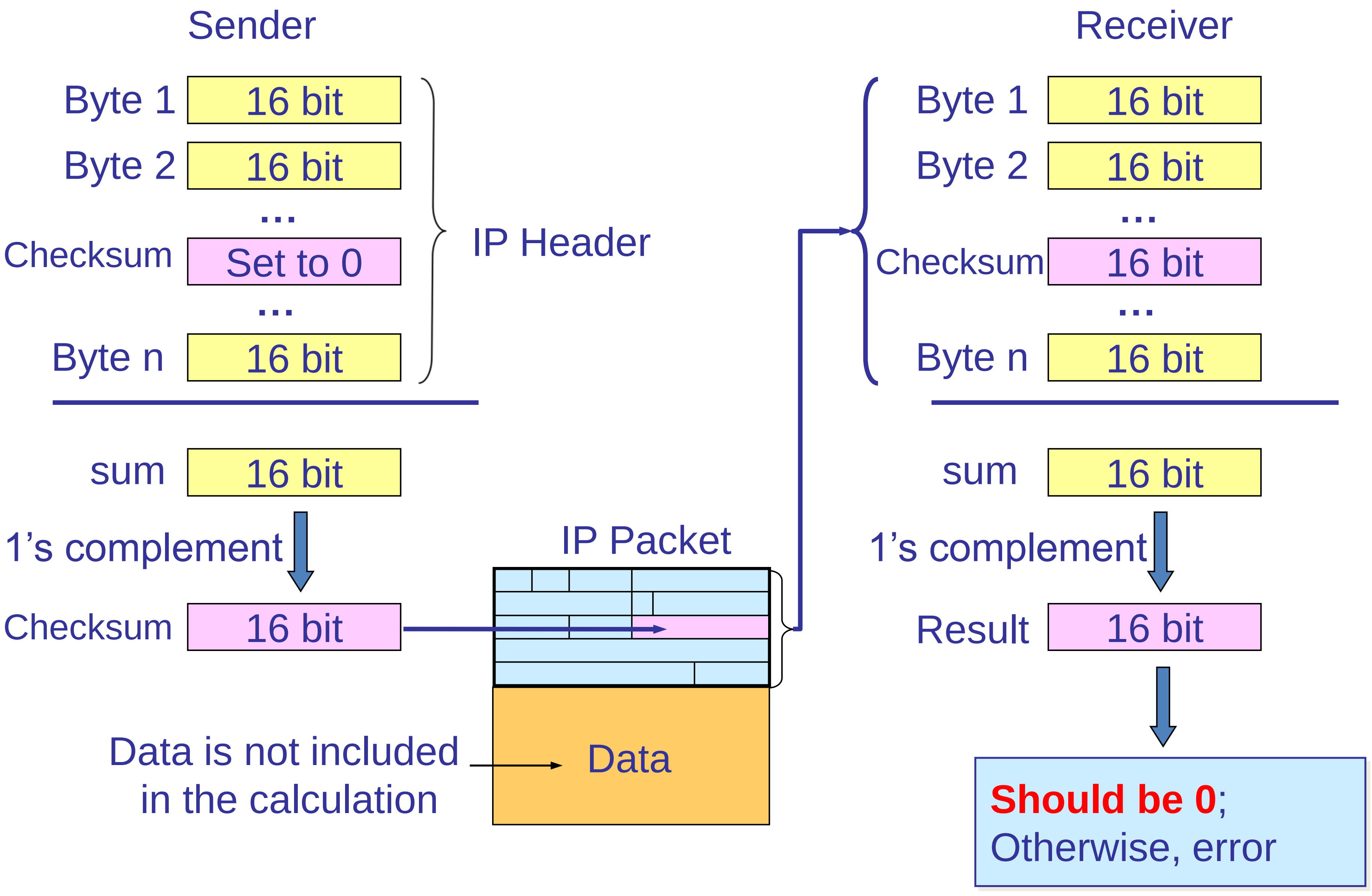
E.g. timestamp, record route taken, specify list of routers to visit.

IPv4 Header: *Protocol*

- Protocol field (8-bits)
  - What type of data the IP datagram carries (e.g., TCP, UDP, etc.).
  - Needed by the receiver to determine the higher level service that will next handle the data
  - The numbering of protocols is global across the entire Internet (www.iana.org)
    - ICMP:1 00000001
    - IGMP:2 00000010
    - TCP :6 00000110
    - UDP:17 00010001
    - OSPF:89 01011001

IPv4 Header: *Checksum*

- Header Checksum (16-bits): A checksum of the IP header ONLY
  - IP checksum treat header as 16-bit words
  - It is much weaker than the CRC
  - The header must be recalculated at every router since the time_to_live (TTL) field is decremented.


Sender
Byte 1
16 bit
Byte 2
16 bit
...
Checksum
Set to 0
...
Byte n
16 bit
IP Header
sum
16 bit
1's complement
Checksum
16 bit
IP Packet
Data is not included in the calculation
Data
Receiver
Byte 1
16 bit
Byte 2
16 bit
...
Checksum
16 bit
...
Byte n
16 bit
sum
16 bit
1's complement
Result
16 bit
Should be 0;
Otherwise, error

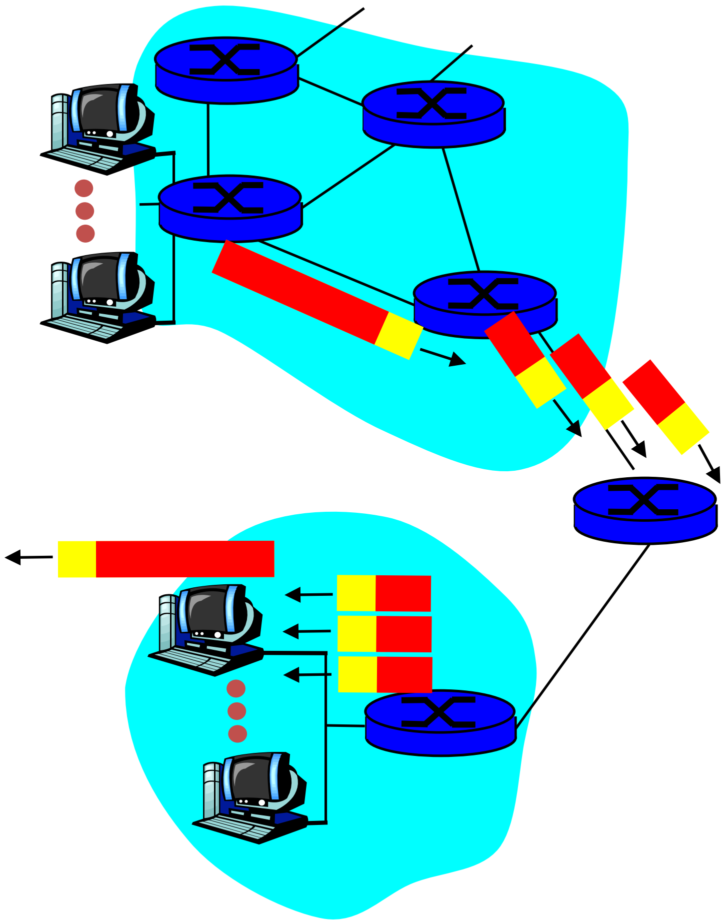
See example ->

IPv4 Header: *DF, MF & Offset*

- DF (Don't Fragment , 1 bit)
  - Prevent routers from fragmenting the datagram.
  - It is used as part of the process to discover the path MTU. By marking the datagram
  - With the DF bit, the sender knows it will either arrive in one piece, or an error message will be returned to the sender.
- MF (More Fragments, 1bit)
  - All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.
- Fragment offset (13 bits)
  - The offset tells where in the current packet this fragment belongs.
  - All fragments except the last one in a datagram must be a multiple of 8 bytes
  - 13 bits -> a maximum of 8192 fragments per datagram

IP Fragmentation & Reassembly

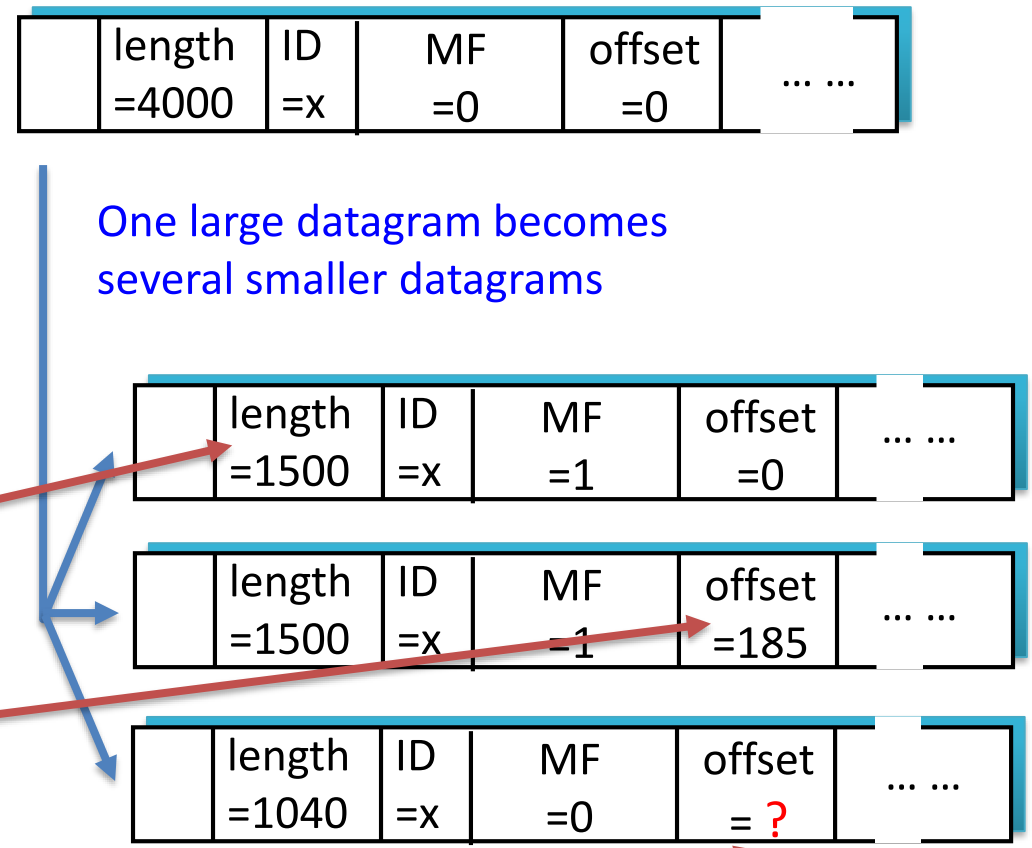
- Networks have different MTU
- Large IP datagram is fragmented
  - one datagram becomes several datagrams
  - Reassembled only at final destination



IP Fragmentation & Reassembly

Example:

- 4000 byte IP packet (20 Bytes header)
- MTU = 1500 bytes



1480 bytes in data field

offset = 1480/8

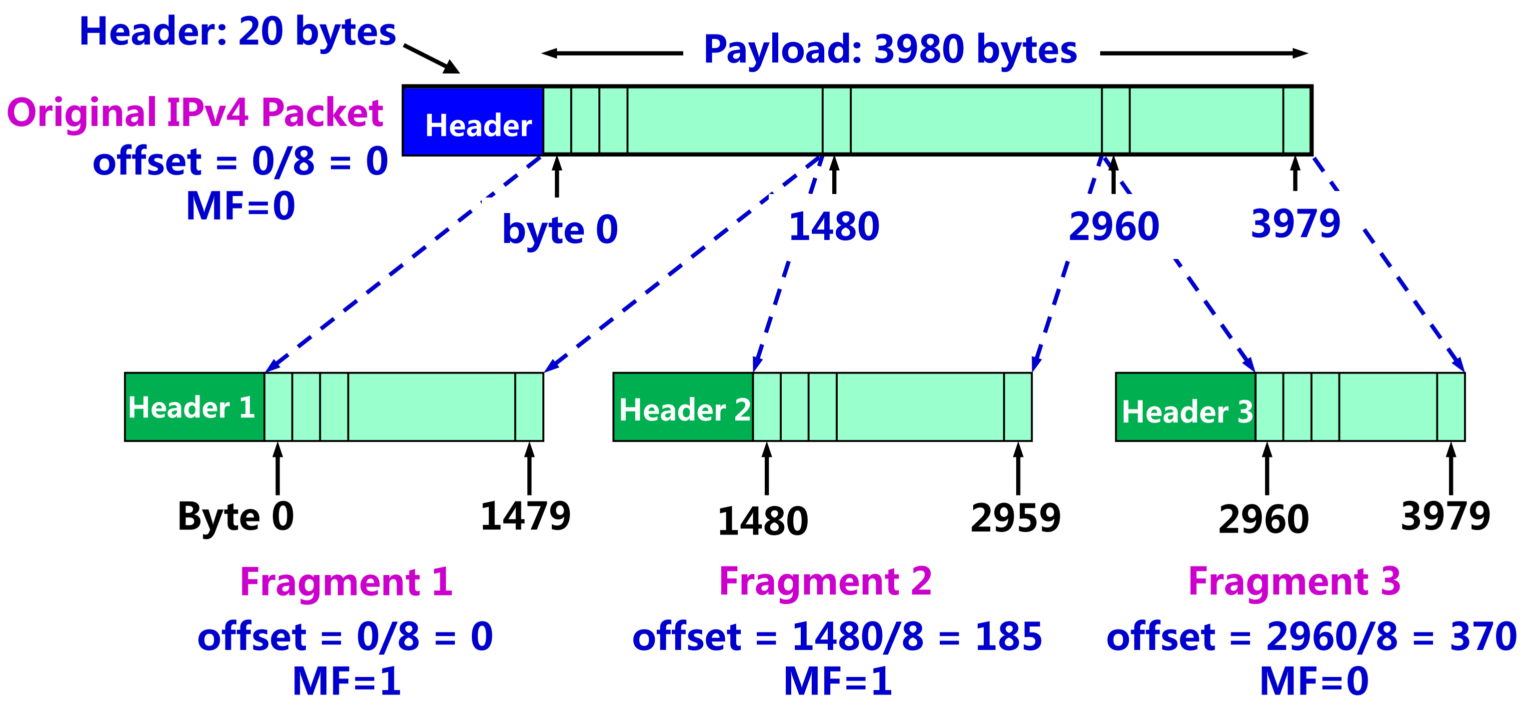
offset = 2960/8 = 370

DF = 0

Example (Cont'd)

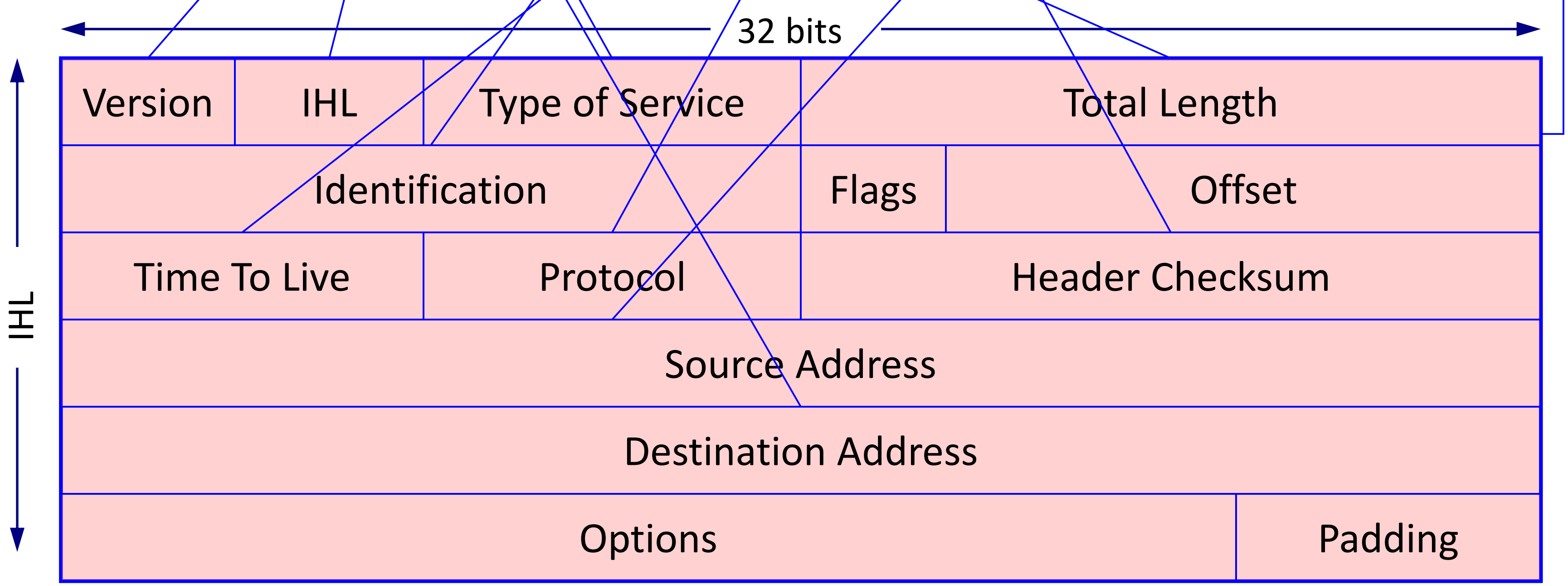
Example:

- 4000 byte IP packet (20 Bytes header)
- MTU = 1500 bytes



IP Header Format

```
12:12:23.323832 IP 202.112.0.89.22 > 59.66.24.130.49893: P 1:41(40) ack 1
win 57920 <nop,nop,timestamp 497903510 1198492021>
        0x0000:  4500 005c 0700 4000 3606 1f0f ca70 0059  E..\..@.6....p.Y
        0x0010:  3b42 1882 0016 c2e5 3c1c e61f 7172 3969  ;B......<...qr9i
        0x0020:  8018 e240 edb1 0000 0101 080a 1dad 6796  ...@..........g.
        0x0030:  476f 8975 5353 482d 312e 3939 2d4f 7065  Go.uSSH-1.99-Ope
        0x0040:  6e53 5348 5f33 2e35 7031 2046 7265 6542  nSSH_3.5p1.FreeB
        0x0050:  5344 2d32 3030 3330 3230 310a
```



```c
/* Definitions for internet protocol version 4.  RFC 791, September 1981.*/
typedef struct iPHDR
{
#if MY_BYTE_ORDER == LITTLE_ENDIAN
      unsigned char ip_hl:4;                /* header length */
      unsigned char ip_v:4;                  /* version */
#else
      unsigned char ip_v:4;                 /* version */
      unsigned char ip_hl:4;                /* header length */
#endif
      unsigned char ip_tos;                 /* type of service */
      unsigned short ip_len;                /* total length */
      unsigned short ip_id;                 /* identification */
      unsigned short ip_off;                /* fragment offset field */
      unsigned char ip_ttl;                 /* time to live */
      unsigned char ip_p;                   /* protocol */
      unsigned short ip_sum;                /* checksum */
      unsigned int ip_src;                  /* source address */
      unsigned int ip_dst;                  /* destination address */
} IPHDR;
```

IPv4 Address

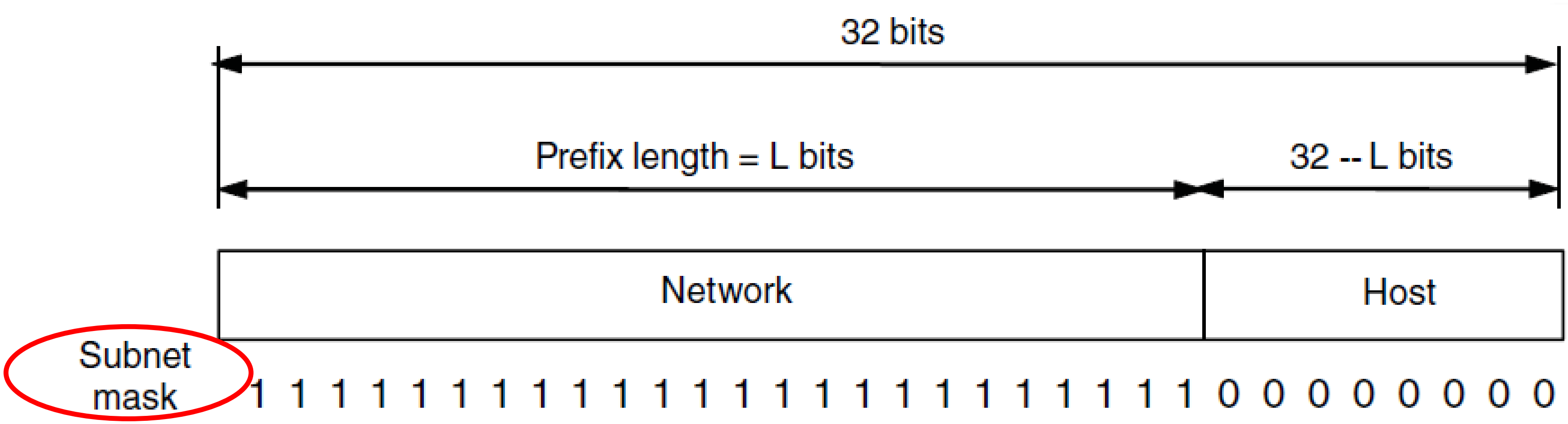
- Addresses consist of 32-bit
- They are represented as four octets in dotted decimal format: 233.14.17.68
- Address encodes its *network ID* and *host ID*. The combination is unique: in principle, no two machines on the Internet have the same IP address

Addresses Assignment

- Network numbers are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers) to avoid conflicts.
- IPv4 address exhaustion
  - The end of IPv4 (Internet Protocol version 4) addresses was announced in a ceremony in Miami on February 3, 2011

IP Addresses – Prefixes

- Addresses are allocated in blocks called prefixes
  - Prefix (前缀) is determined by the network portion
  - Written address/length, e.g., 18.0.31.0/24
  - Subnet mask: binary mask of 1s in network portion



Subnet mask can be ANDed with the IP address to extract only the network portion.

Special IP Addresses

Network ID	Host ID	Src. IP	Dest. IP	Usage	Example
0	0	OK	N.A	This host (used in DHCP)	0.0.0.0
0	host-id	OK	N.A	A host (i.e., host-id) on this network	0.0.0.67
all 1s	all 1s	N.A	OK	Broadcast on the local network	255.255.255.255
net-id	all 1s	N.A	OK	Broadcast on a distant network specified by the net-id	219.223.13.255
127	Anything	OK	OK	Loopback test (won't put on wire)	127.0.0.1

IP Addressing Methods

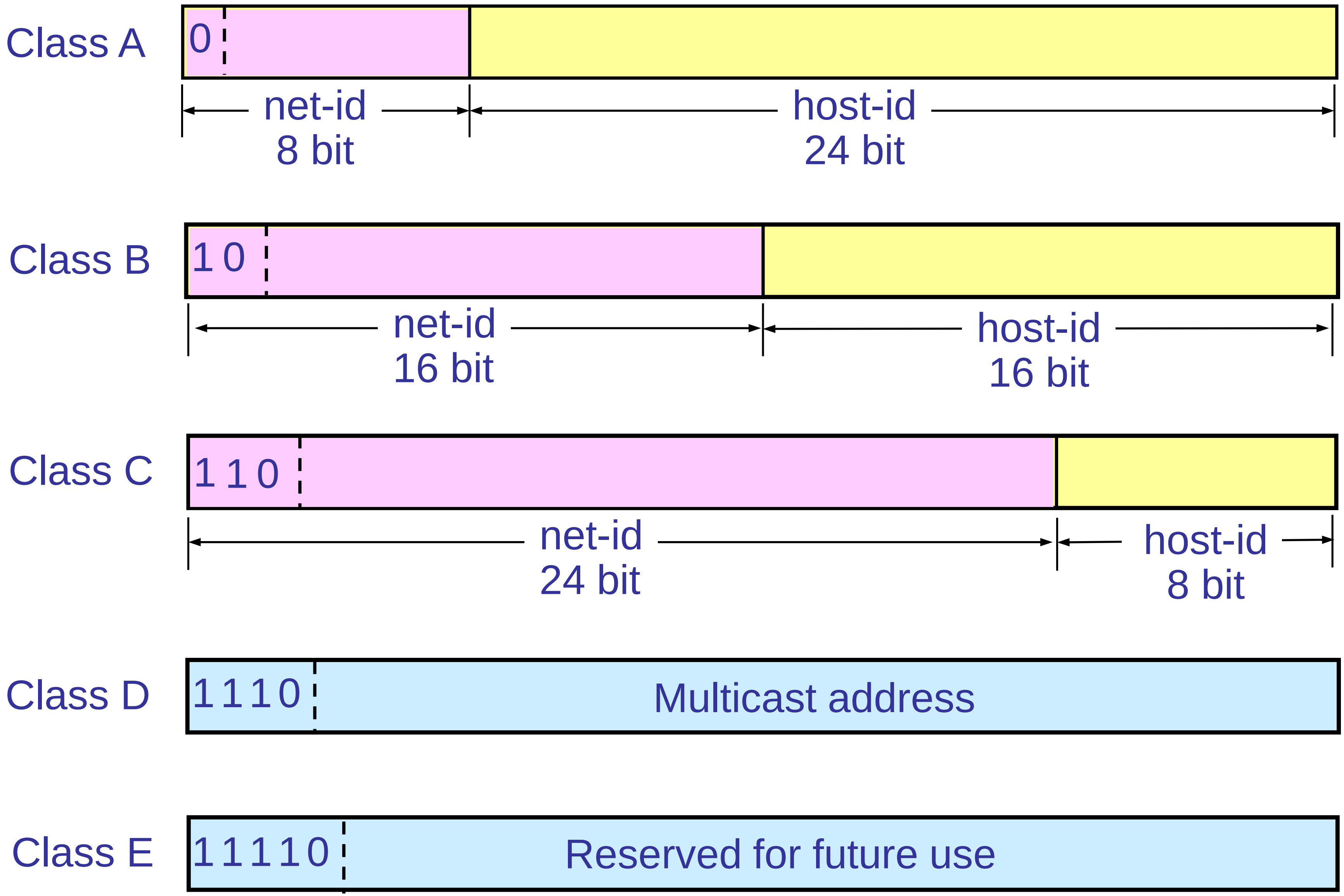
- Classful Addressing: introduced by RFC 791 in 1981
- Subnet: improvement to classful addressing, defined in RFC 950, 1985
- CIDR: replaced classful addressing, starting in 1993 with RFC 1518 and 1519

Classful Addresing (分类寻址)

- This method is just history
- Addresses came in blocks of fixed size
  - Carries size as part of address, but lacks flexibility
  - Called classful (vs. classless) addressing

IP Address: { <Network ID>, <Host ID>}

Classful Addresing

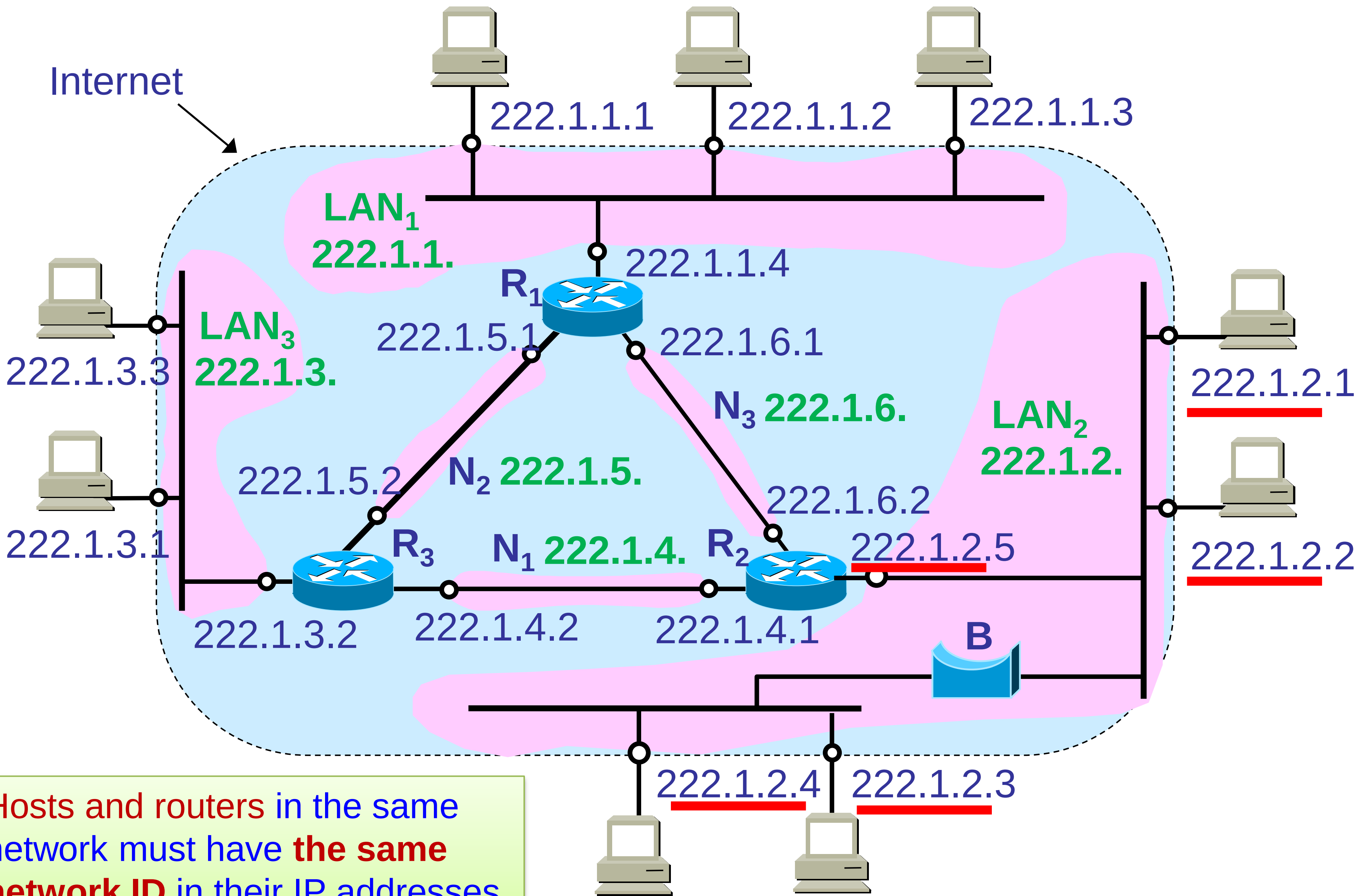


Classful Addressing

- IP address range of three common classes:

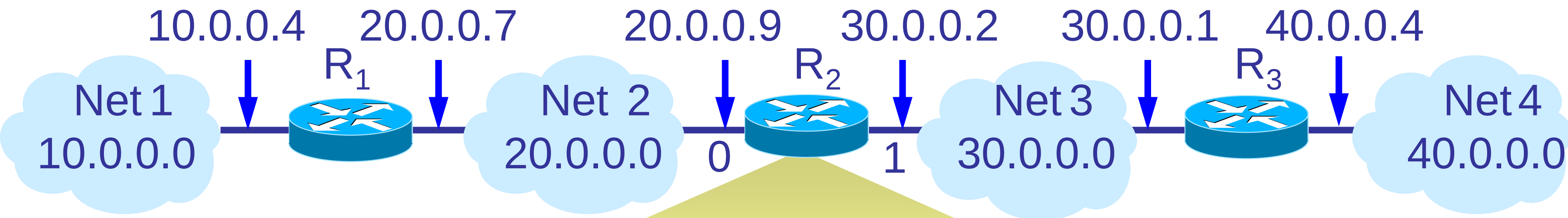
Classes	Max. # of networks	First network ID	Last network ID	Max. # of hosts in each network
A	126 ($2^7 – 2$)	1	126	16,777,214
B	16,383 (2^{14})	128.0	191.255	65,534
C	2,097,151 (2^{21})	192.0.0	223.255.255	254

IP Addresses in Internet



Hosts and routers in the same network must have **the same network ID** in their IP addresses

Routing Example



Routing Table of R_2

Networks	Next
20.0.0.0	Direct, Interface 0
30.0.0.0	Direct, Interface 1
10.0.0.0	20.0.0.7
40.0.0.0	30.0.0.1

Pros and Cons of Classful Addressing

- Pros
  - Routers can forward packets based on only the network portion of the address, as long as each of the networks has a unique address block. This makes the routing table much smaller.
- Cons
  - The IP address of a host depends on where it is located in the network.
  - The hierarchy is wasteful of addresses unless it is carefully managed.

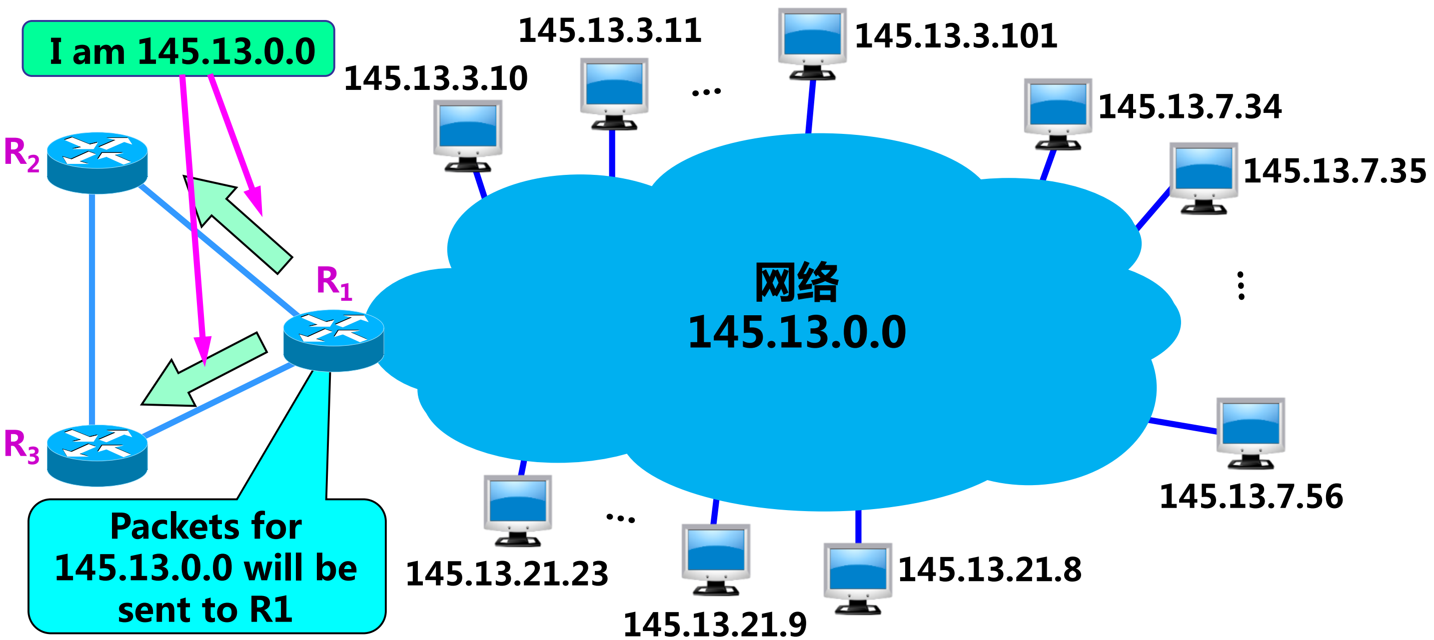
Subnets (子网)

- Use a single network address for the entire organization, and internally divide the host address space into a subnet address and a host id
- To implement subnetting, router needs a subnet mask that indicate network ID and subnet ID

IP Address: { <Network ID>, <Subnet ID>, <Host ID>}

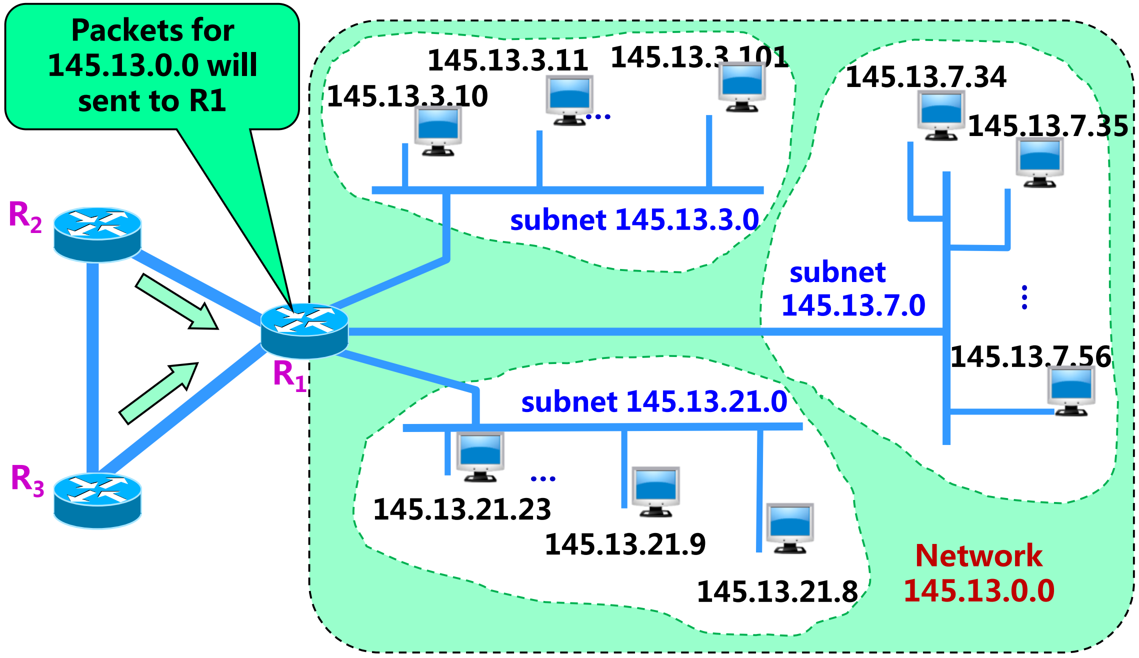
Subnetting example

A network without subnetting

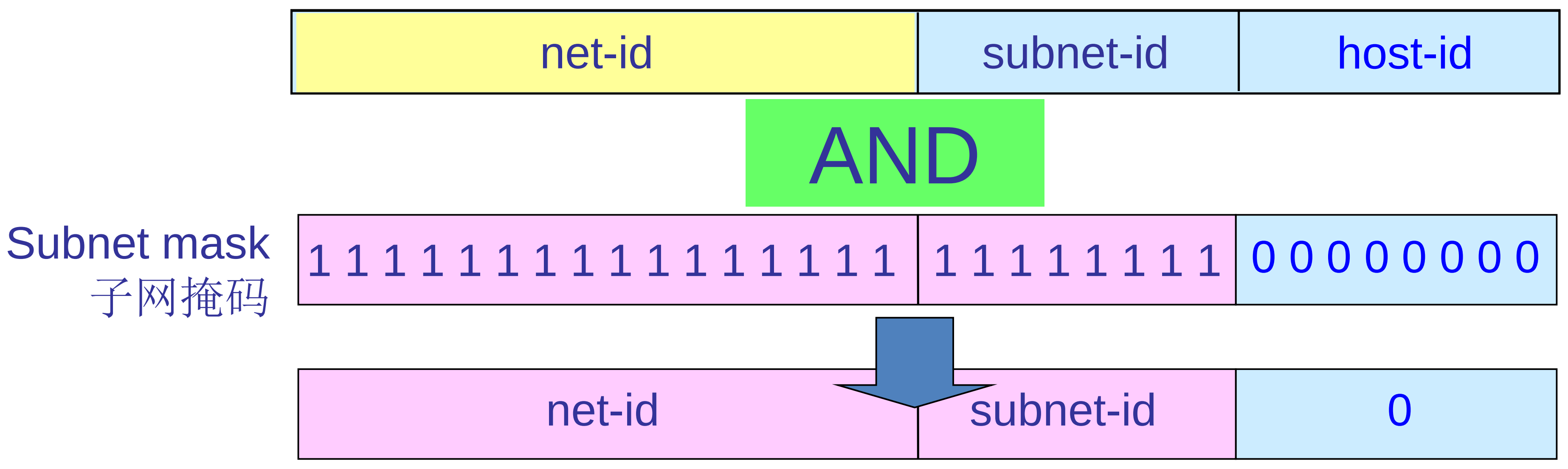


Subnetting example

A network with three subnets



Subnet and Subnet Mask



Default Subnet Masks

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Calculating a Subnet

- We will subnet the IP address:
  - 223.14.17.0
- What class IP address is this?
  - Class C

Step #1

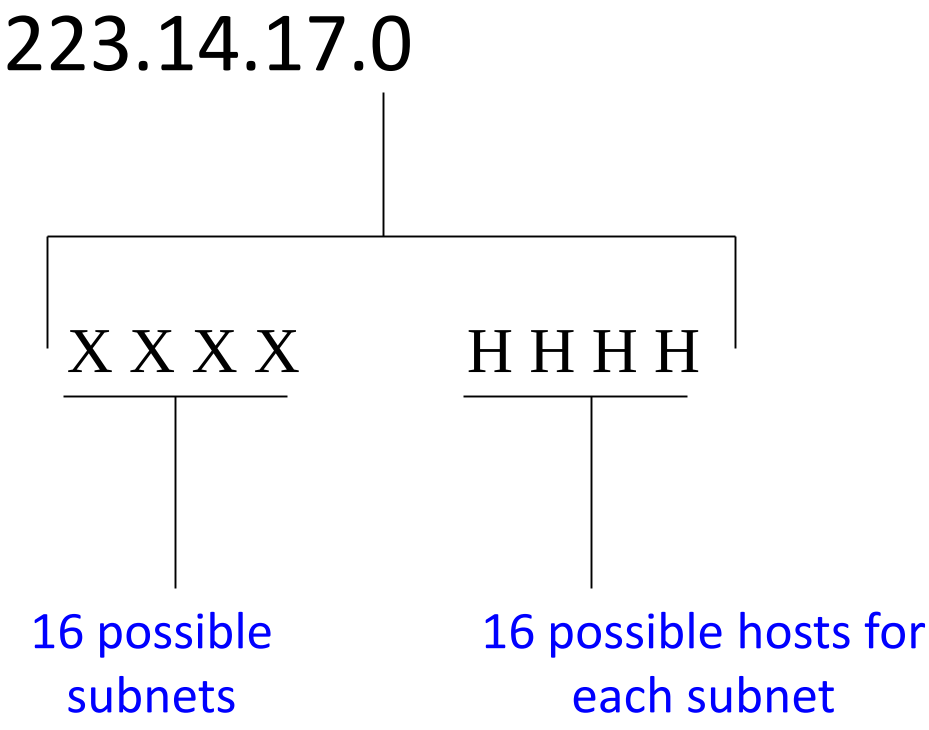
- Determine the default subnet mask

- Class C default subnet mask:
  - 255.255.255.0

Step #2

- Determine the number of subnets needed and the number of hosts needed on each subnet to determine how many bits to borrow from the host ID.
- For 223.14.17.0, its host portion contains 8 bits
- Assume we need:
  - 13 subnets
  - 10 hosts on each subnet
- we will borrow 4 bits from the host

Step #3


223.14.17.0
X X X X
H H H H
16 possible subnets
16 possible hosts for each subnet

Step #4

- Determine the subnet mask.

223.14.17.0

X X X X   H H H H

$128 + 64 + 32 + 16 = \boxed{240}$

- The subnet mask is: 255.255.255.240

Step 5

- Determine the ranges of host addresses for each subnet.

Subnet #	Subnet Bits	Host Bits	In Decimal
1	0000	0000-1111	.0 -.15
2	0001	0000-1111	.16 - .31
3	0010	0000-1111	.32 - .47
4	0011	0000-1111	.48 - .63
5	0100	0000-1111	.64 - .79
6	0101	0000-1111	.80 - .95
7	0110	0000-1111	.96 - .111
8	0111	0000-1111	.112 - .127

……

Fixed and Variable Subnet Mask

- FLSM (Fixed Length Subnet Masks) Subnetting
  - All subnets use same subnet mask and are equal in size.
- VLSM (Variable Length Subnet Masks) Subnetting
  - Subnets use different subnet masks, and are variable in size.
  - More efficient by allowing a routed system of different mask length to suit requirements

Refer to course website for more details and examples about VLSM.

Determining the subnetwork for incoming packets

- Destined for which department?
  - Match (Dest.IP AND subnet_mask) with each subnet’s prefix
  - Send to corresponding subnet

Determining the subnetwork for outgoing packets

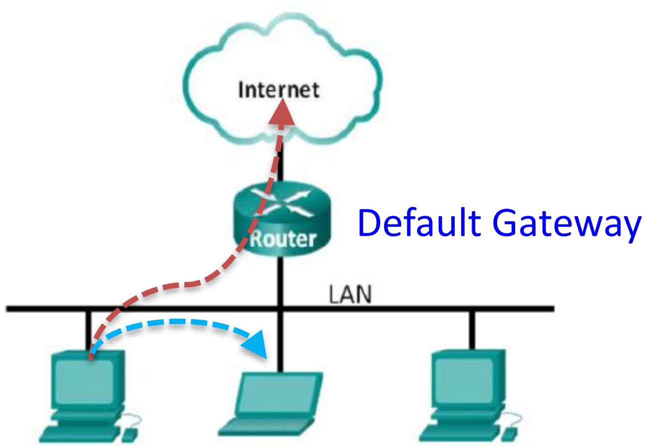
- Destined for Local or Remote Network?

  If ((Network_interface_address AND subnet_mask) == (Dest.IP AND subnet_mask))

  Local Network, Send directly

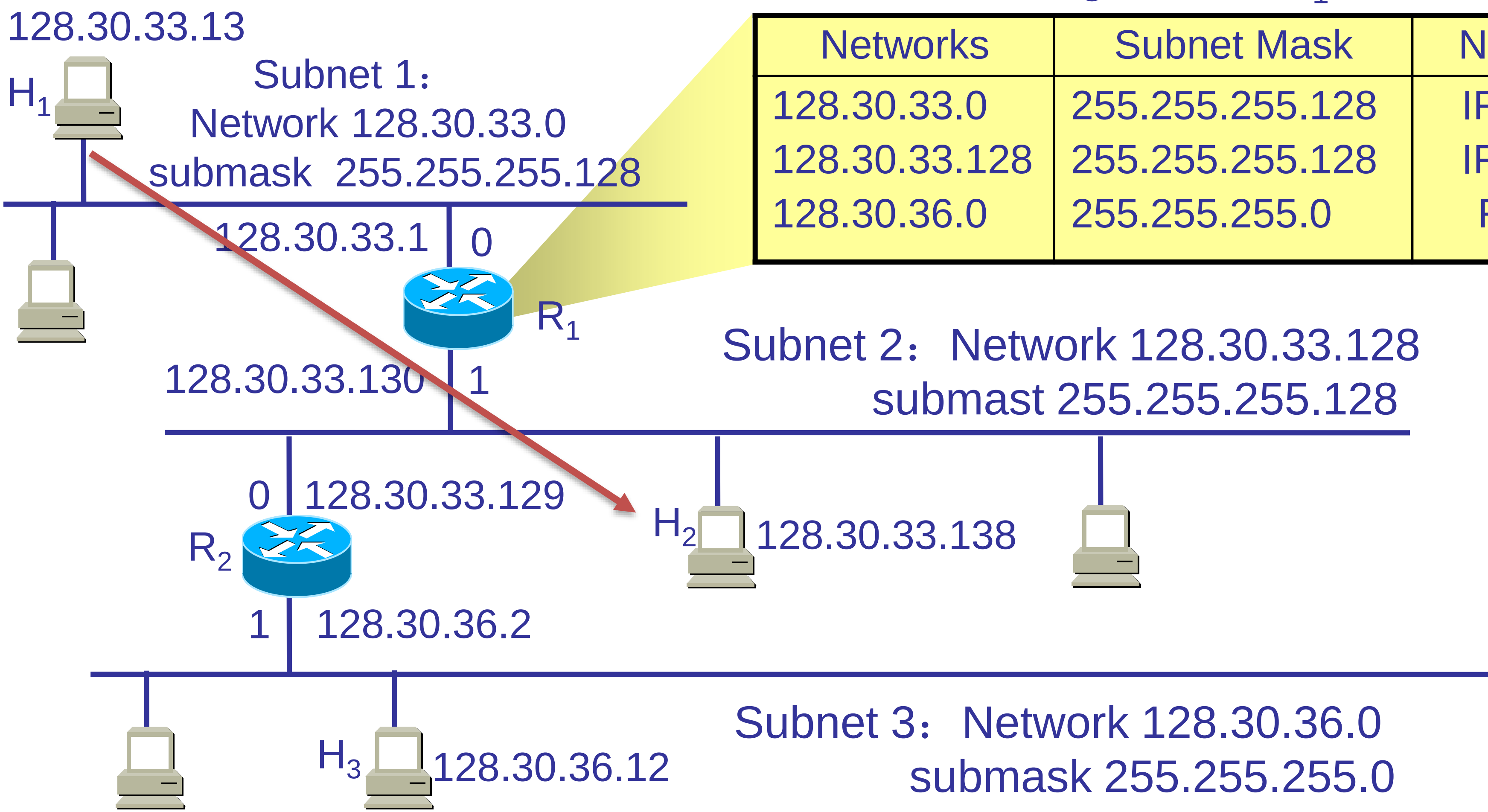
  Else

  Remote Network, Send to default router/gateway (默认网关)



To send data to a device on another network, host sends to a default gateway.

H_1 sends an IP packet to H_2

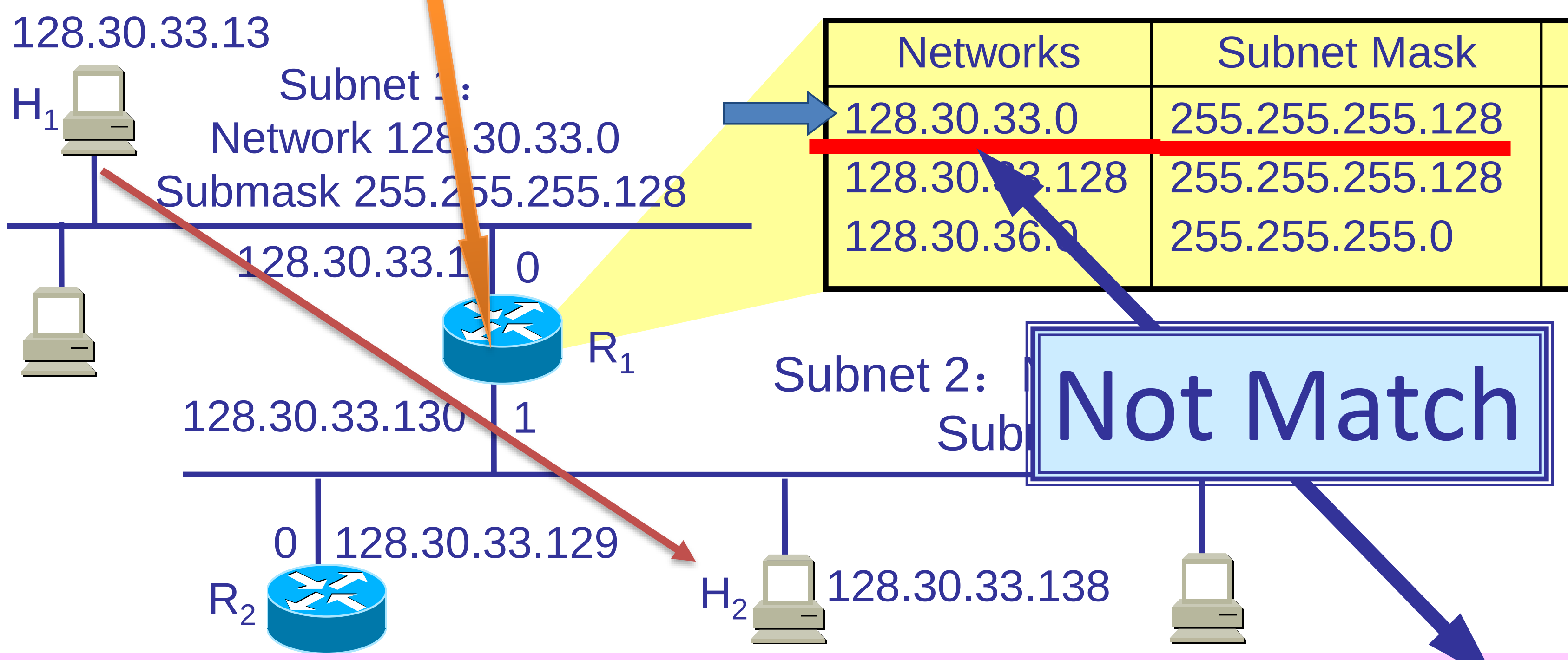


Routing table of R_1

Networks	Subnet Mask	Next
128.30.33.0	255.255.255.128	IF. 0
128.30.33.128	255.255.255.128	IF. 1
128.30.36.0	255.255.255.0	R_2

Router R_1 check the first entry in routing table

Dest. IP of incoming packets： 128.30.33.138



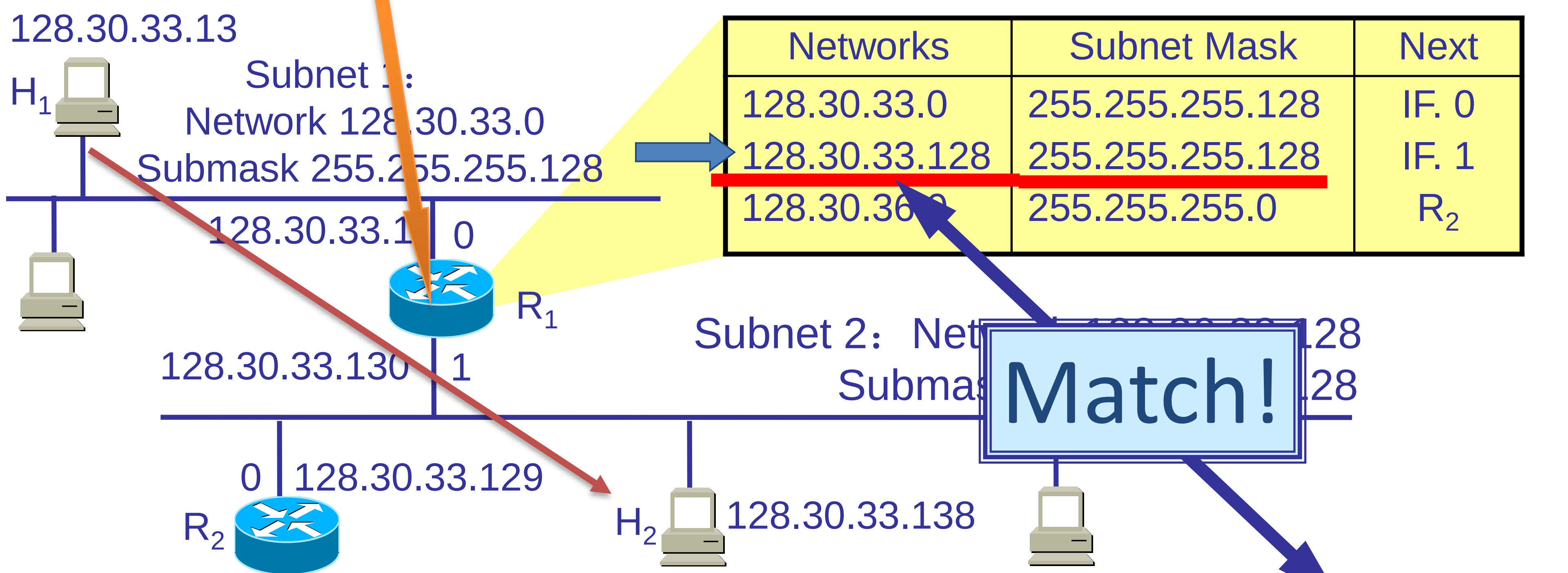
Networks	Subnet Mask	Next
128.30.33.0	255.255.255.128	IF. 0
128.30.33.128	255.255.255.128	IF. 1
128.30.36.0	255.255.255.0	R_2

255.255.255.128 AND 128.30.33.138 = 128.30.33.128

Not Match!

Router R_1 check the second entry in routing table

Dest. IP of incoming packets: 128.30.33.138



Networks	Subnet Mask	Next
128.30.33.0	255.255.255.128	IF. 0
128.30.33.128	255.255.255.128	IF. 1
128.30.36.0	255.255.255.0	R_2

255.255.255.128 AND 128.30.33.138 = 128.30.33.128

Match!

Routing Table Explosion

- Routers in ISPs and backbones in the middle of the Internet must have entries for every network and no simple default will work.
- These core routers are said to be in the default-free zone of the Internet
  - The Internet now contains millions networks, which make a very large routing table.
- Routing algorithms require each router to exchange information about the addresses it can reach with other router
  - The larger the tables, the more information needs to be communicated and processed

Refer to: [Global route table size]

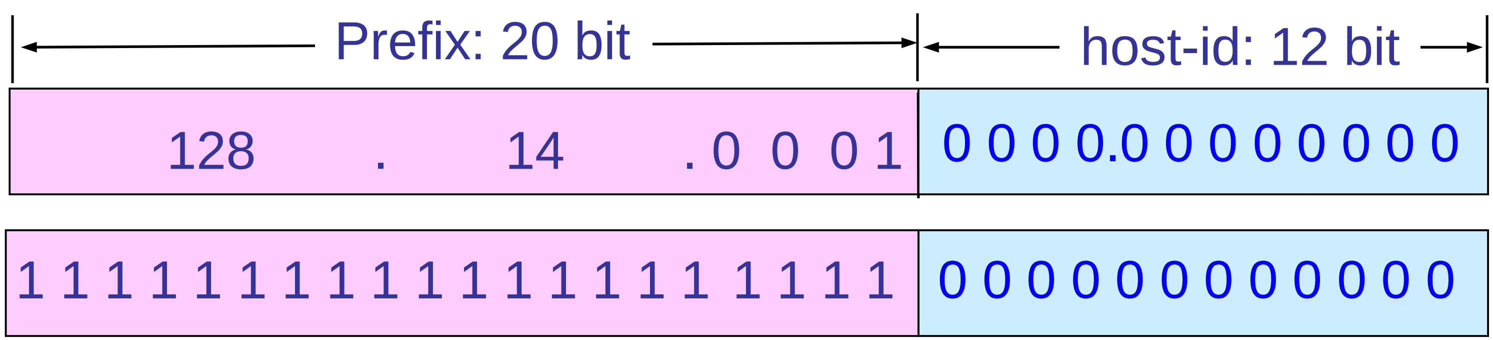
CIDR – Classless InterDomain Routing (无分类域间路由)

- Use VLSM: Variable Length Subnet Mask (prefix)
- No concept of Class A, B, C, etc.
- Allocate IP addresses more efficiently
- Reduce router table size

IP Address: { <Prefix>, <Host ID>}

CIDR Address Block

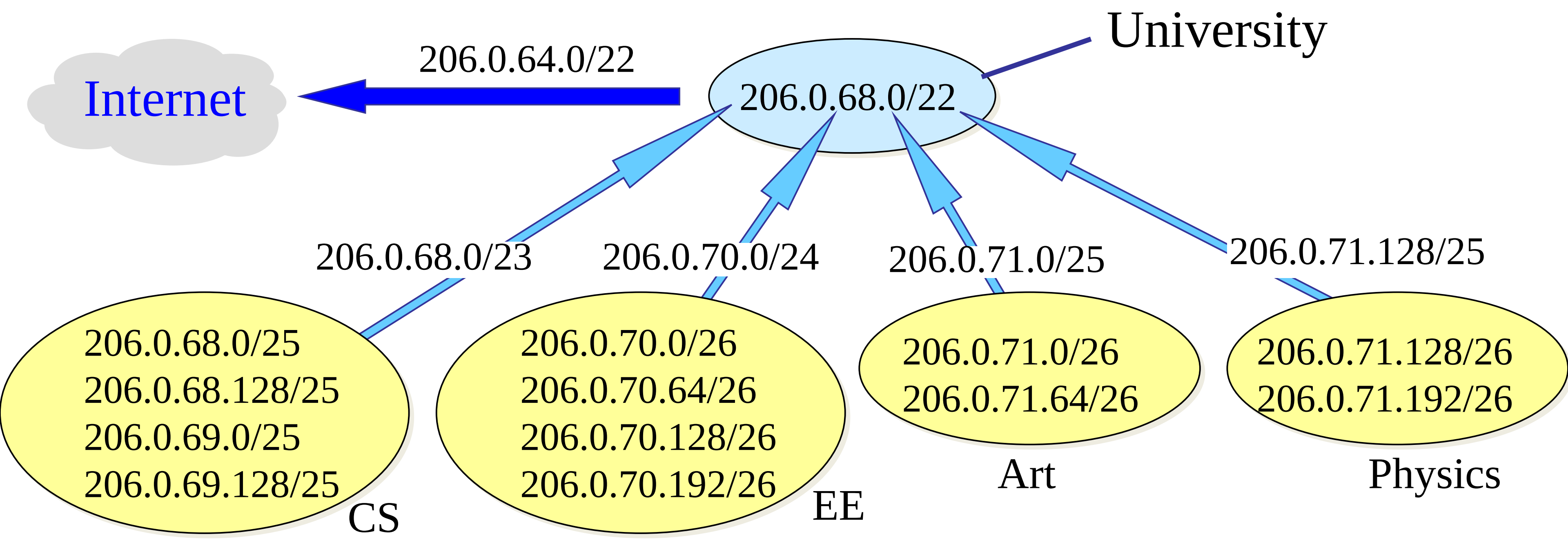
- 128.14.32.0/20 means there are 2^{12} addresses (20 bits prefix, 12 bits for hosts)
- First address in this block: 128.14.16.0
- Last address in this block: 128.14.31.255
- This block is also referred as "/20" block



Route Aggregation (路由聚合)

- To reduce routing table size
  - Routers at different locations can know about a given IP address as belonging to prefixes of different sizes
  - So a router can combine multiple small prefixes into a single larger prefix. This automatic process for routers is called route aggregation
  - The resulting larger prefix is sometimes called a supernet (超网), to contrast with subnets as the division of blocks of addresses

CIDR – Aggregation Example



	Address Block	Binaries Address	Size
University	206.0.68.0/22	11001110.00000000.010001*	1024
CS	206.0.68.0/23	11001110.00000000.0100010*	512
EE	206.0.70.0/24	11001110.00000000.01000110.*	256
Art	206.0.71.0/25	11001110.00000000.01000111.0*	128
Physics	206.0.71.128/25	11001110.00000000.01000111.1*	128

Some CIDR blocks

CIDR Prefix	Dotted decimal format	# of addresses	Compared to classful addressing
/13	255.248.0.0	512 K	8 Class B or 2048 Class C
/14	255.252.0.0	256 K	4 Class B or 1024 Class C
/15	255.254.0.0	128 K	2 Class B or 512 Class C
/16	255.255.0.0	64 K	1 Class B or 256 Class C
/17	255.255.128.0	32 K	128 Class C
/18	255.255.192.0	16 K	64 Class C
/19	255.255.224.0	8 K	32 Class C
/20	255.255.240.0	4 K	16 Class C
/21	255.255.248.0	2 K	8 Class C
/22	255.255.252.0	1 K	4 Class C
/23	255.255.254.0	512	2 Class C
/24	255.255.255.0	256	1 Class C
/25	255.255.255.128	128	1/4 Class C
/26	255.255.255.192	64	1/4 Class C
/27	255.255.255.224	32	1/8 Class C

CIDR – Longest Matching Prefix

- Routing table consists of triples of

  (IP address, subnet mask, outgoing line)
- It is possible that multiple entries (with different subnet mask lengths) match
- The longest mask (i.e., longest matching prefix) is used, which is the most specific route.
- Such method is called Longest Prefix Matching(LPM, 最长前缀匹配)
  - Example: if there is a match for a /20 mask and a /24 mask, the /24 entry is used

Longest Matching Prefix Example

For an incoming packet with destination of *Dst. IP* = 206.0.71.128

Routing Table:

Prefix	Out line
206.0.68.0/22	University
206.0.71.128/25	CS

Check the first entry with /22 mask:

$$
\begin{array}{rllll}
M = & 11111111 & 11111111 & 11111100 & 00000000 \\
\text{AND } \; Dst.\ IP = & 206. & 0 & .01000100. & 0 \\
\hline
 & 206. & 0 & .01000100. & 0
\end{array}
$$

The Dst. IP matches 206.0.68.0/22

Longest Matching Prefix Example

For an incoming packet with destination of *Dst. IP* = 206.0.71.128

Routing Table:

Prefix	Out line
206.0.68.0/22	University
206.0.71.128/25	CS

Å

Check the second entry with /25 mask:

M =	11111111 11111111 11111111 10000000
AND *Dst. IP* =	206. 0 . 71 .10000000
	206. 0 . 71 . 10000000

The Dst. IP matches 206.0.71.0/25

Two matches, choose /25

Network Address Translation

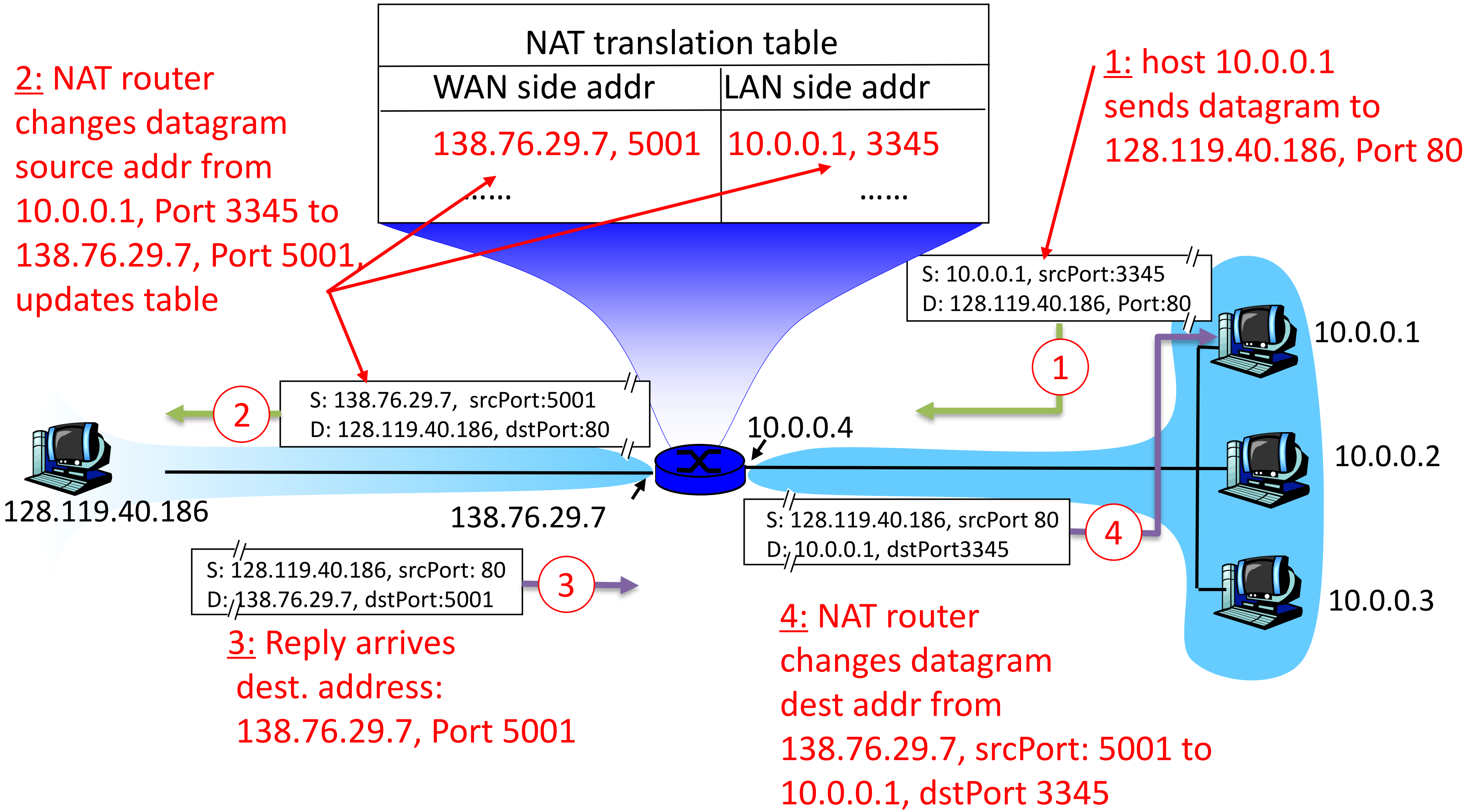
Remember these IP Addr

- Reserved private (internal) IP addresses:
  - 10.0.0.0 ~ 10.255.255.255/8 (16,777,216 hosts)
  - 172.16.0.0 ~ 172.31.255.255/12 (1,048,576 hosts)
  - 192.168.0.0 ~ 192.168.255.255/16 (65,536 hosts)
- No packets contain these address may appear on the Internet
- NAT (Network Address Translation) maps one external IP address to many internal IP addresses
  - Uses TCP/UDP port to tell connections apart
  - Violates layering; very common in homes, etc.

NAT: Network Address Translation

- Most traffic on the Internet are carried by TCP/UDP
  - TCP/UDP protocols use port number for source/destination
- Implementation of NAT gateway:
  - *Outgoing datagrams: replace (source IP address, port #)* of every datagram to (*NAT IP address, new port #*)
    - remote clients/servers will respond using (NAT IP address, new port #) as destination addr.
  - *Remember* every (*source IP address, port #*) to (*NAT IP address, new port #*) mapping pair in NAT table
  - *Incoming datagrams: replace* (*NAT IP address, new port #*) in destination fields of every datagram with corresponding (*source IP address, port #*) stored in NAT table

NAT: Network Address Translation



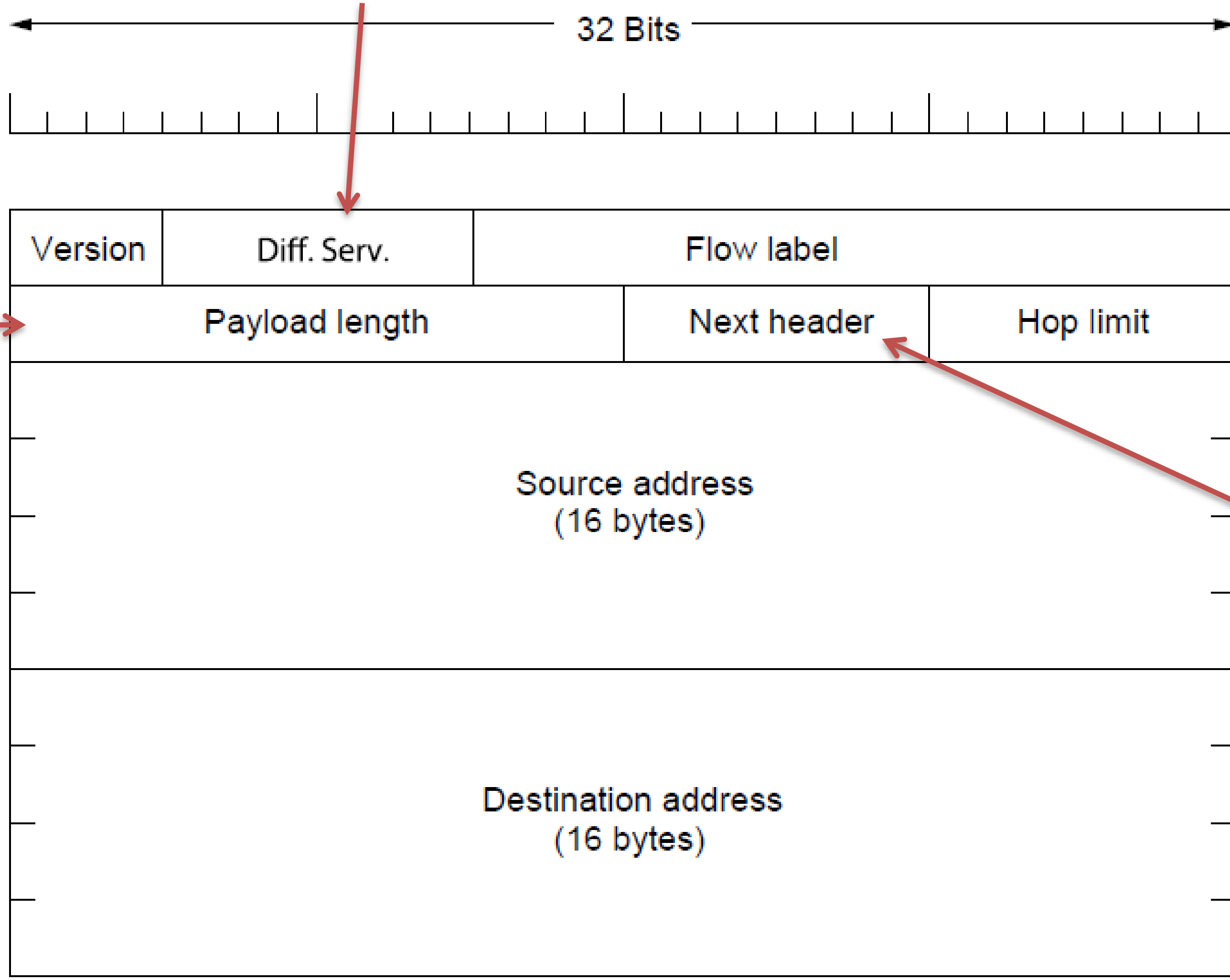
IP Version 6

- Major upgrade in the 1990s due to impending address exhaustion
- Deployment has been slow & painful, but may pick up pace now since IPv4 addresses are exhausted
- IPv6 protocol header has much longer addresses (128 vs. 32 bits) and is simpler (by using extension headers)
- IPv6 is a different network layer protocol that does not really interwork with IPv4, despite many similarities.

IPv6 Header

6+2bits: The 6 most-significant bits is Differentiated Services (DS) field to classify packets. Remaining 2 bits are used for ECN.

Only count payload



Specifies next header type or the transport layer protocol

IPv6 Header

- IPv6 extension headers handles other functionality

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

IPv6 Address

- An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons (:)
- For example:

    2001:0db8:85a3:0000:0000:8a2e:0370:7334

- An IPv6 address can be abbreviated with the following rules:
    - Omit leading zeroes in a 16-bit value.
    - Replace one group of consecutive zeroes by a double colon

    2001:db8:85a3::8a2e:370:7334

IPv6 Address Type

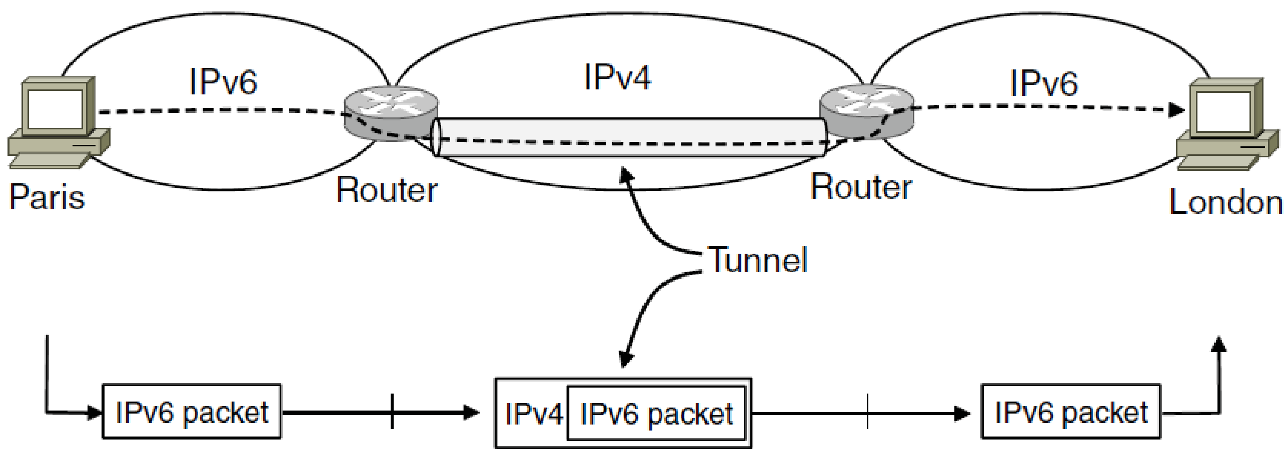
Unicast

Address Type	IPv6 Prefix	IPv4 Equivalent
Unspecified	::/128 (all 0s)	0.0.0.0
Loopback	::1/128 (00…1)	127.0.0.1
Unique Local Addresses (ULAs)	FC00::/7	Private address: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
Link-Local Addresses	FE80::/10	169.254.0.0/16 Used only to communicate with devices on the same local link
Global Unicast	2000::/3	Public IPv4 address
Multicast	FF00::/8	224.0.0.0/4

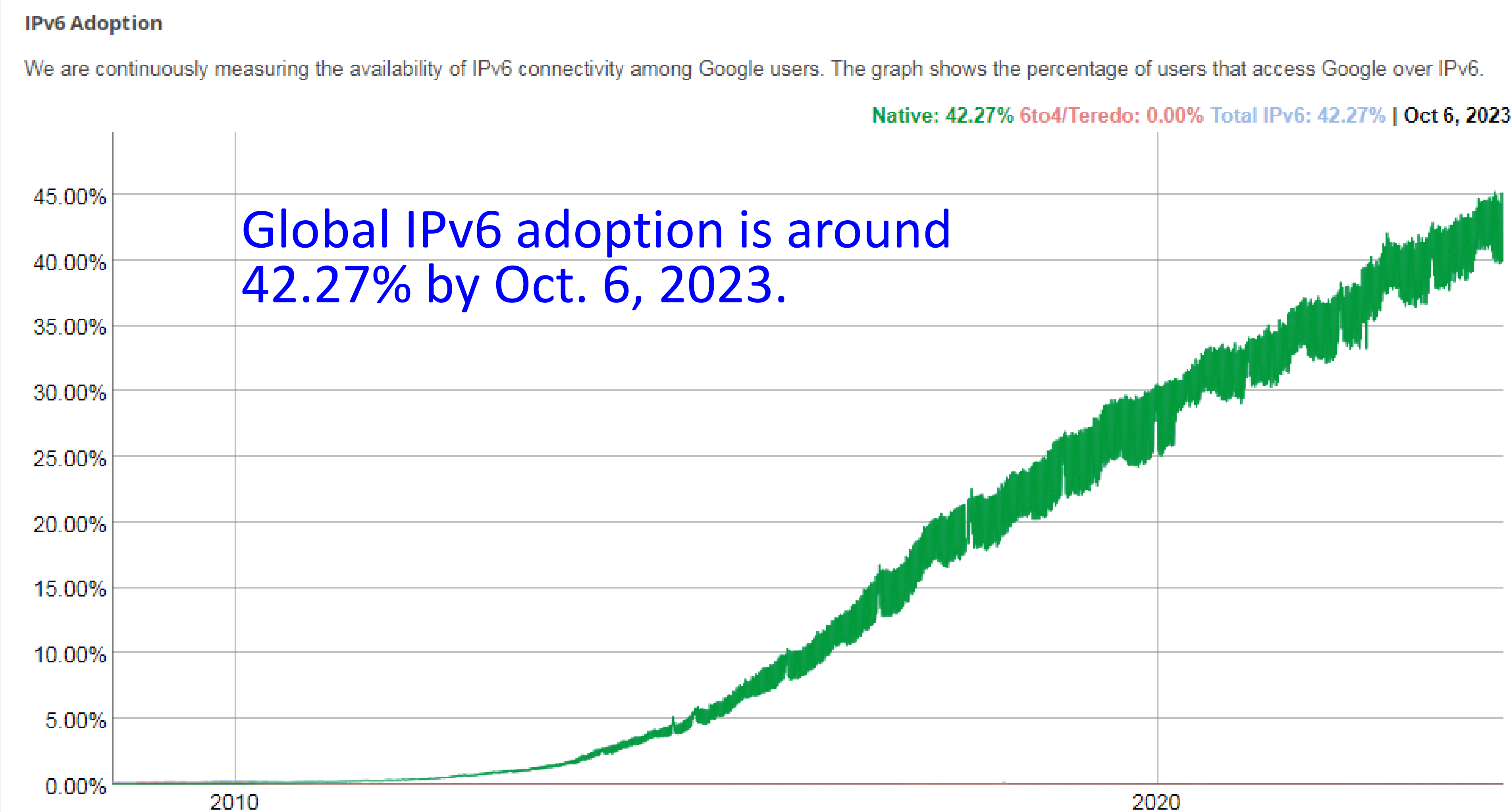
Refer course website for detailed IPv6 Address Types

Transition From IPv4 To IPv6

- Not all routers can be upgraded simultaneous
- Two proposed approaches:
  - Dual Stack (双协议栈): some routers with dual stack (v6, v4) can “translate” between formats
  - Tunneling (隧道): IPv6 carried as payload in IPv4 datagram among IPv4 routers

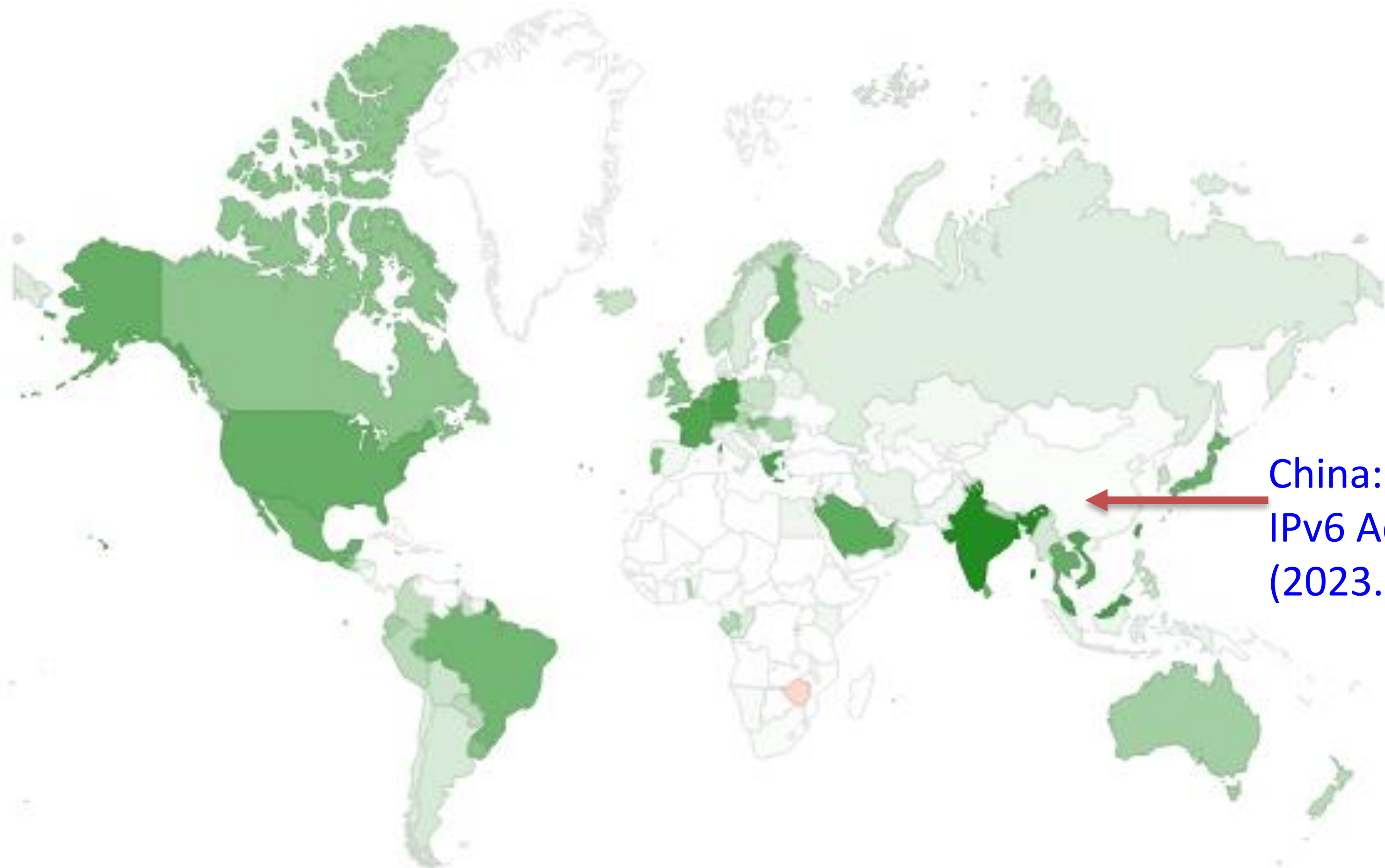


Google IPv6 Statistics



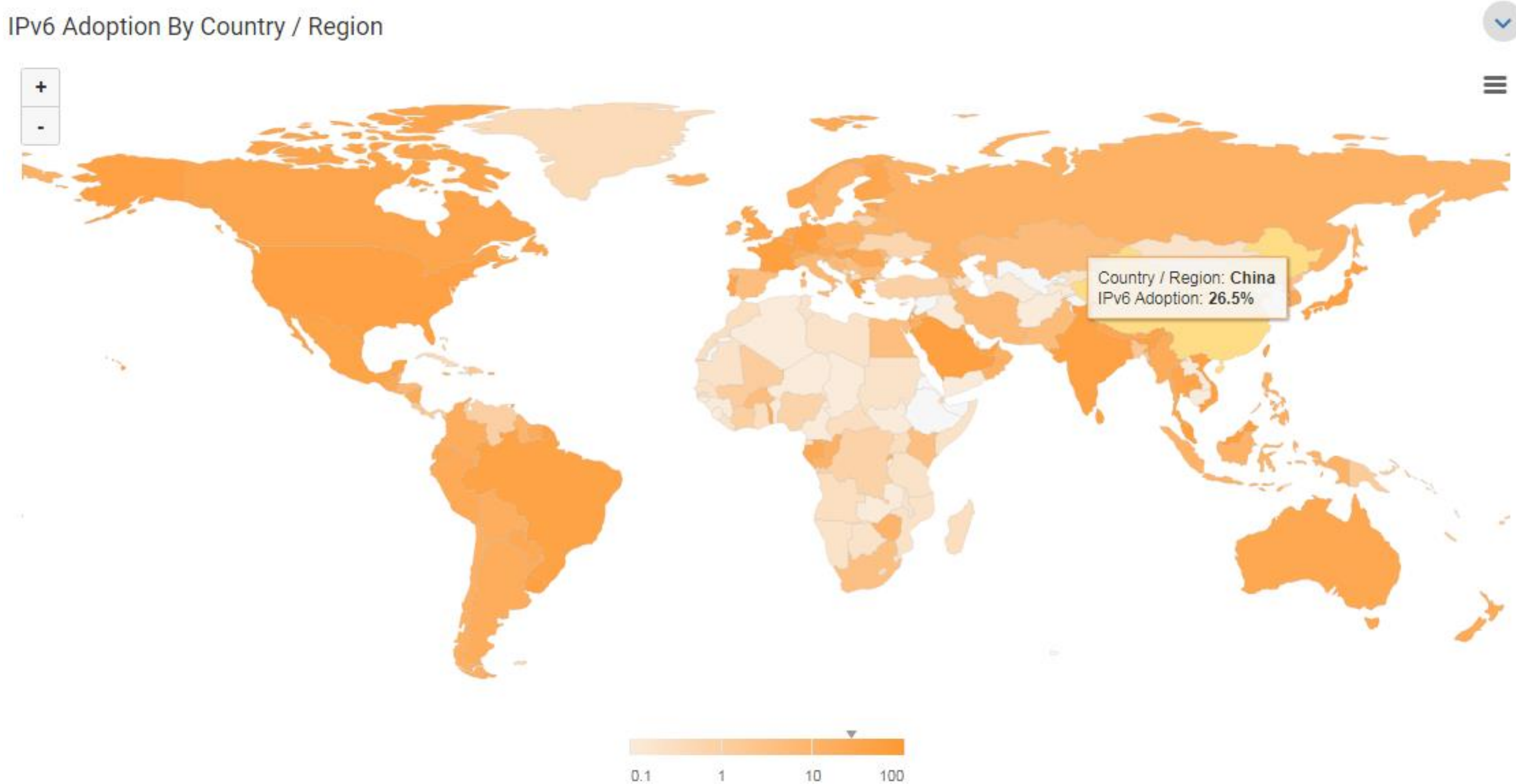
https://www.google.com/intl/en/ipv6/statistics.html

Google IPv6 Statistics



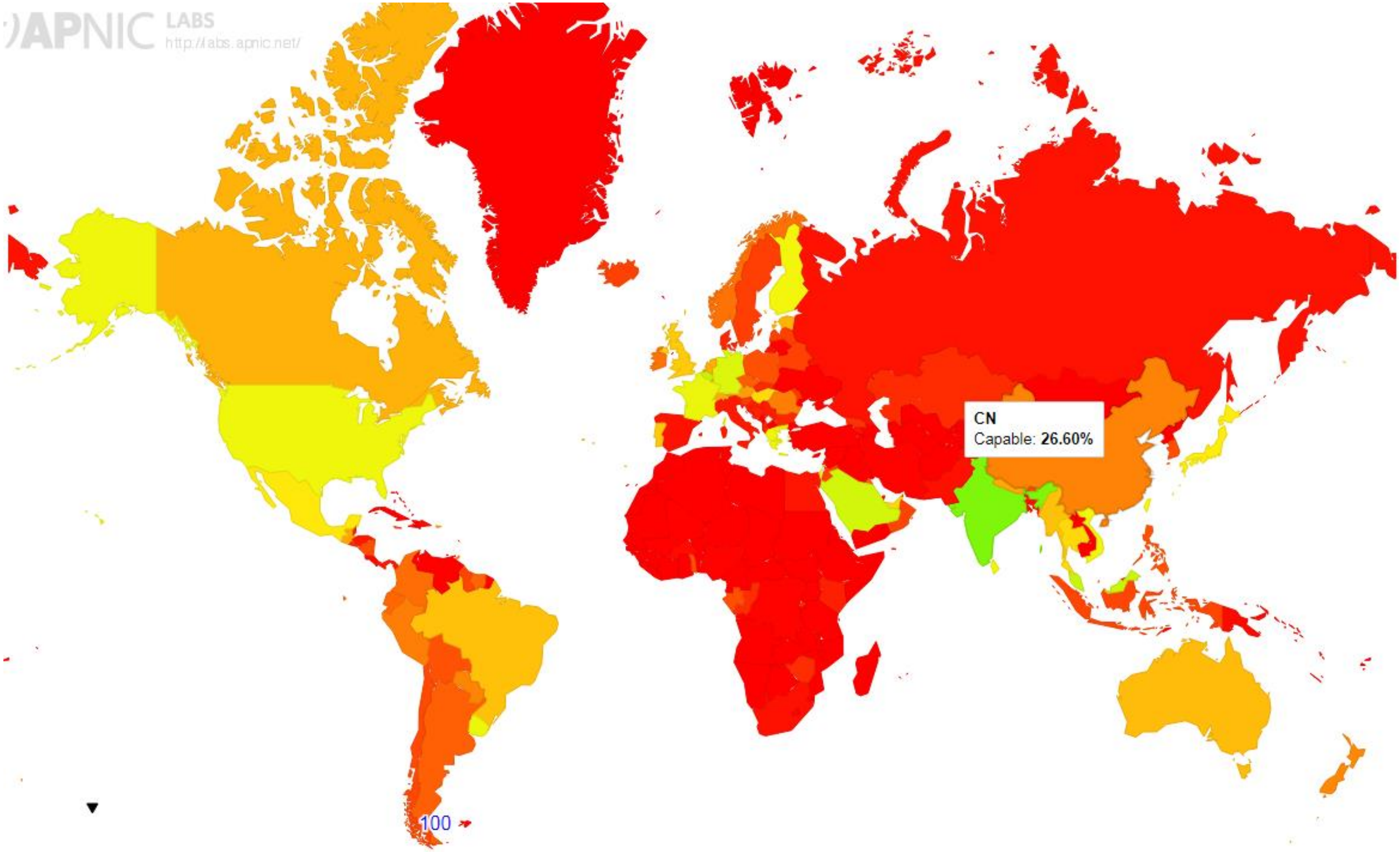
China:
IPv6 Adoption 4.68%
(2023.10.06)

Akamai IPv6 Adoption Trends



Link: [Akamai IPv6 Adoption Trends by Country and Network]

APNIC IPv6 Statistic



APNIC IPv6 Statistic: https://stats.labs.apnic.net/ipv6

IPv6 in China

- 2017-11-26:
  - The General Office of the State Council of P.R. China issued an action plan for promoting the large-scale deployment of Internet Protocol Version 6 (IPv6).
  - The plan points out the significance of IPv6, and the general requirements and major goals of the work, including in terms of internet infrastructure and network security.

  国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》

IPv6 support in China

https://www.china-ipv6.cn/

Date: 2023.10.06

Thank you!

Q & A