



University of
Nottingham

UK | CHINA | MALAYSIA

COMP1047: Systems and Architecture

Dr. Fazl Ullah (Khan)

AY2023-24, Spring Semester
Week 10

Computer Networks:
IP Protocol & Subnetting

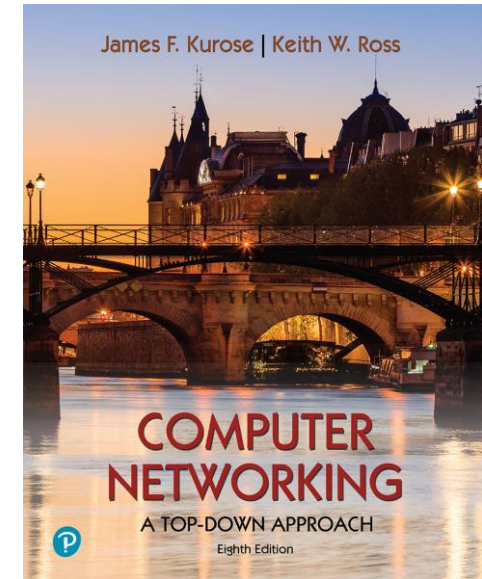


Introduction

- Most of the slides are based on the Books

1. Computer Networking: A Top-Down Approach

8th edition by Jim Kurose, Keith Ross



Overview-Internet Protocol Addressing

Learning Outcomes

- Understand the Services of IP
 - Internet Protocol
- IP datagram format
 - IP datagram header
- IP Addressing
 - IP Format
 - Subnetting
 - Supernetting

Roadmap:

- IP: Internet Protocol
- Review of Binary Numbers
- Connectionless Networking
- IP Addressing
- IP Versions





Overview

■ *Recap from last Week*

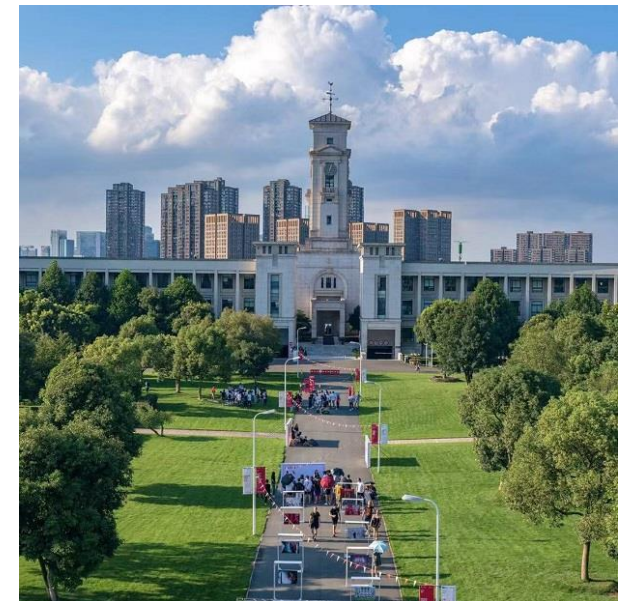
- Principles behind Internet Protocol
 - IP datagram header
 - Header format
- Binary Numbers
 - Quick Review
- Connectionless Networking
 - Design issues
- IP: Addressing
 - Addressing Types
 - IP Classes
 - Addressing Format

■ IP: Addressing

- Subnetting
- Classless Inter-Domain Routing
- Supernetting
- Variable length subnet masking

■ IPv6

- Rules
- Notations

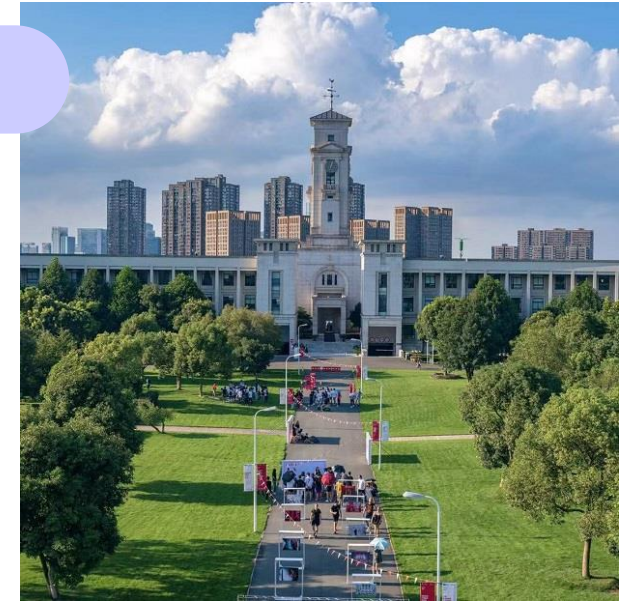


Recap from the Last Week

Last Week, we discussed

- Block TCP Flow Problem
 - Deadlock like situation
- TCP: Connection-oriented protocol
 - Ack, Sequence No. and RTT
 - Connection Management
 - Congestion Control
- Performance Analysis
 - Delay
 - Throughput
 - Packets drop

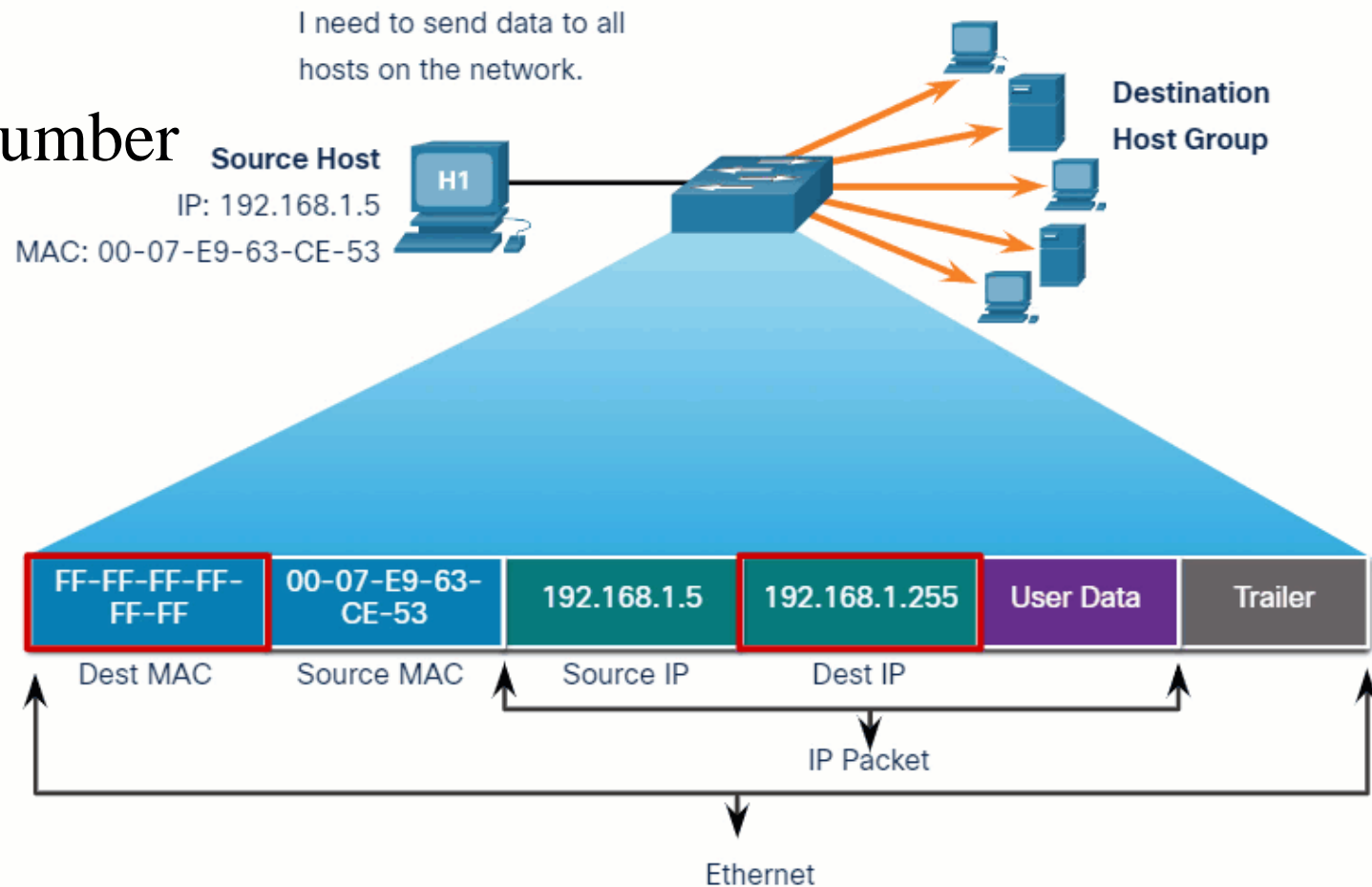
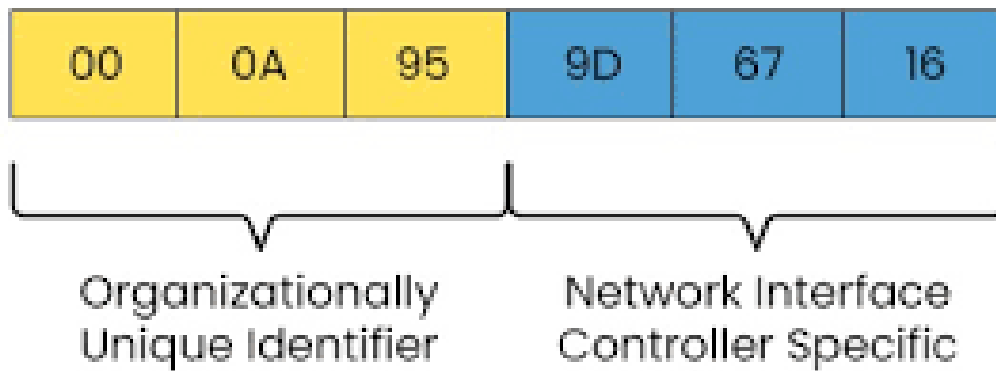
**Any
question
in
previous
lecture?**



Addressing-Types

- Layer 2 – MAC Addresses (Media Access Control)
 - **00-0A-95-9D-67-16** A **MAC** Address
 - **00-0A-95** Vendor Code
 - **9D-67-16** Serial Number

Media Access Control Address





Addressing-Types

- **Layer 3 – Logical Addresses** (IPv4 or IPX)
- Common tasks for an IP address
 - identification of a host or a network
 - identifying the location of a device
- Assignment of IP Addresses
 - Static Addresses – assigned by an Administrator
 - Dynamic Addresses – DHCP (Dynamic Host Configuration Protocol)
 - “Hierarchical” vs. “Flat” Addressing Schemes
 - Hierarchical utilizes multiple routing tables to organize network information.
 - Flat utilizes a single routing table to organize network information

- **Logical (IP) Address**
- It has 4 Octets
 - **8 Bits**
- Each Bit has a “Binary Value”
 - a **One** or a **Zero**
- Example of the Octet



Types of IP Addresses

- **Four types of IP address**

- Public IP address

- external facing
- mostly routers

- Private IP address

- internal facing
- device IP

- Static IP address

- no automatic change

- Dynamic IP address

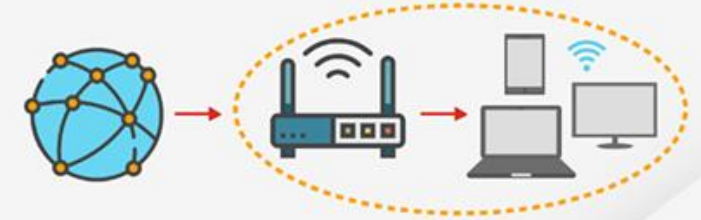
- dynamic allocation

Four types of IP Addresses

Public



Private



Static



Dynamic





Can you count in Binary

- We are Very Familiar with our Decimal System...

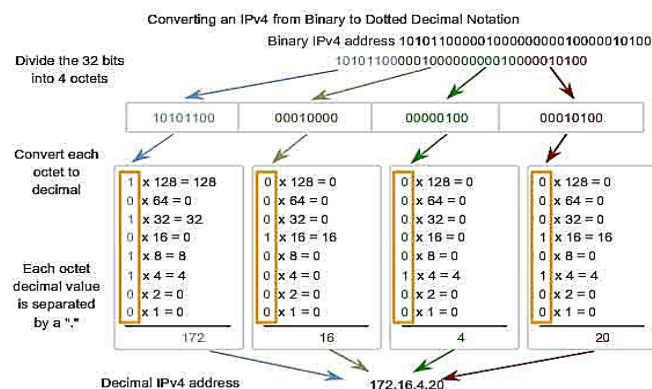
0 1 2 3 4 5 6 7 8 9 10 11 12 13...

But

- We Need to Become Familiar with the Binary System

only 0's and 1's

00 01 10 11 100 101 110 111 1000 1001 ...
 0 1 2 3 4 5 6 7 8 9 ...



The base 10 of Binary numbers

1 0 1 1 0 0 0 0
128 64 32 16 8 4 2 1
 $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$

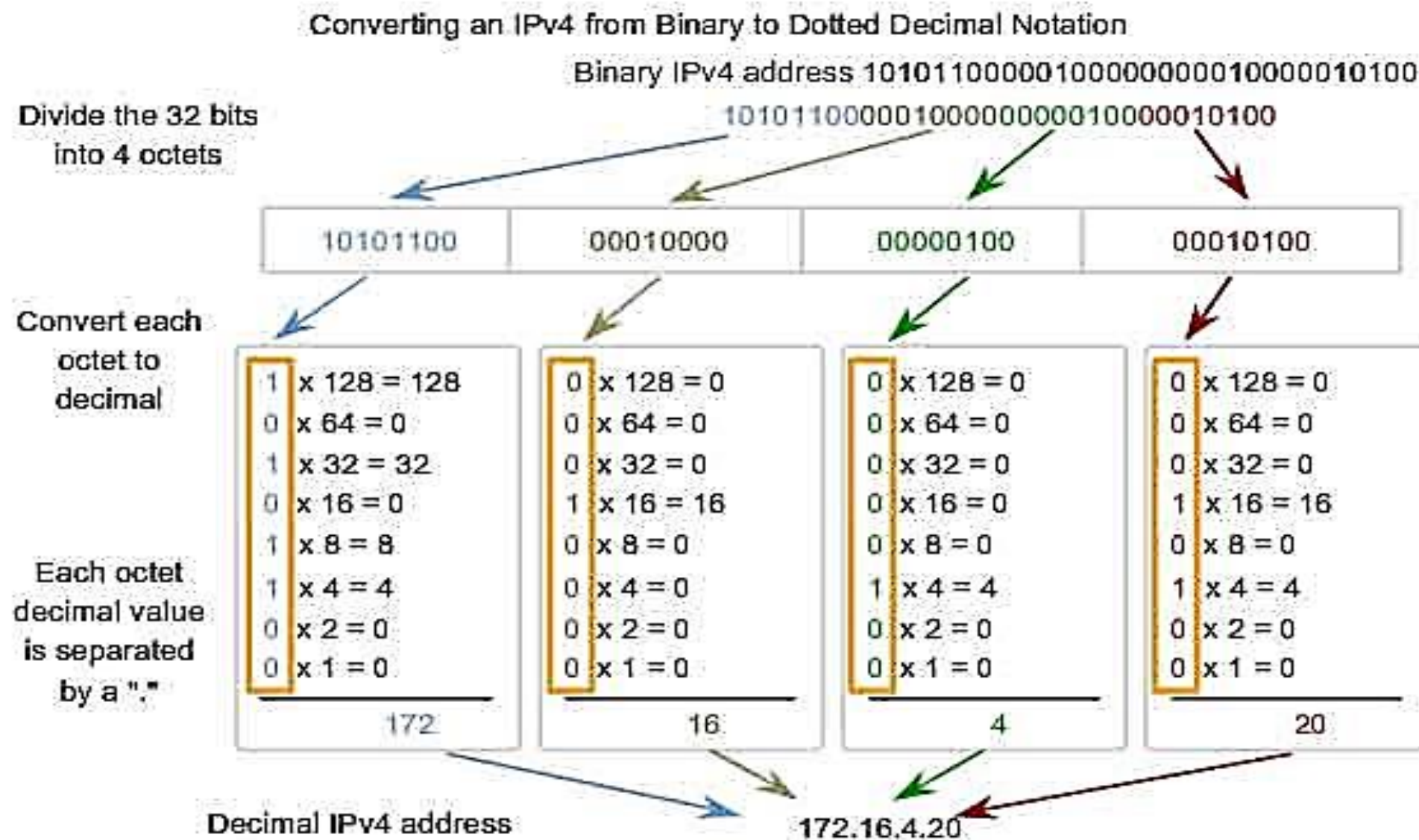


Decimal Equivalents of Bit Patterns

128	64	32	16	8	4	2	1		
↓	↓	↓	↓	↓	↓	↓	↓		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255



Can you count in Binary





Internet Protocol (1/2)

- The **IP** is the network layer communications protocol in the TCP/IP protocol suite
- It relays datagrams across network boundaries
- It is responsible for routing and addressing data packets
 - Packets can travel across networks and arrive at the correct destination
- The routing function enables internetworking
 - essentially establishes the Internet
- It can be used with several transport protocols, including TCP/UDP

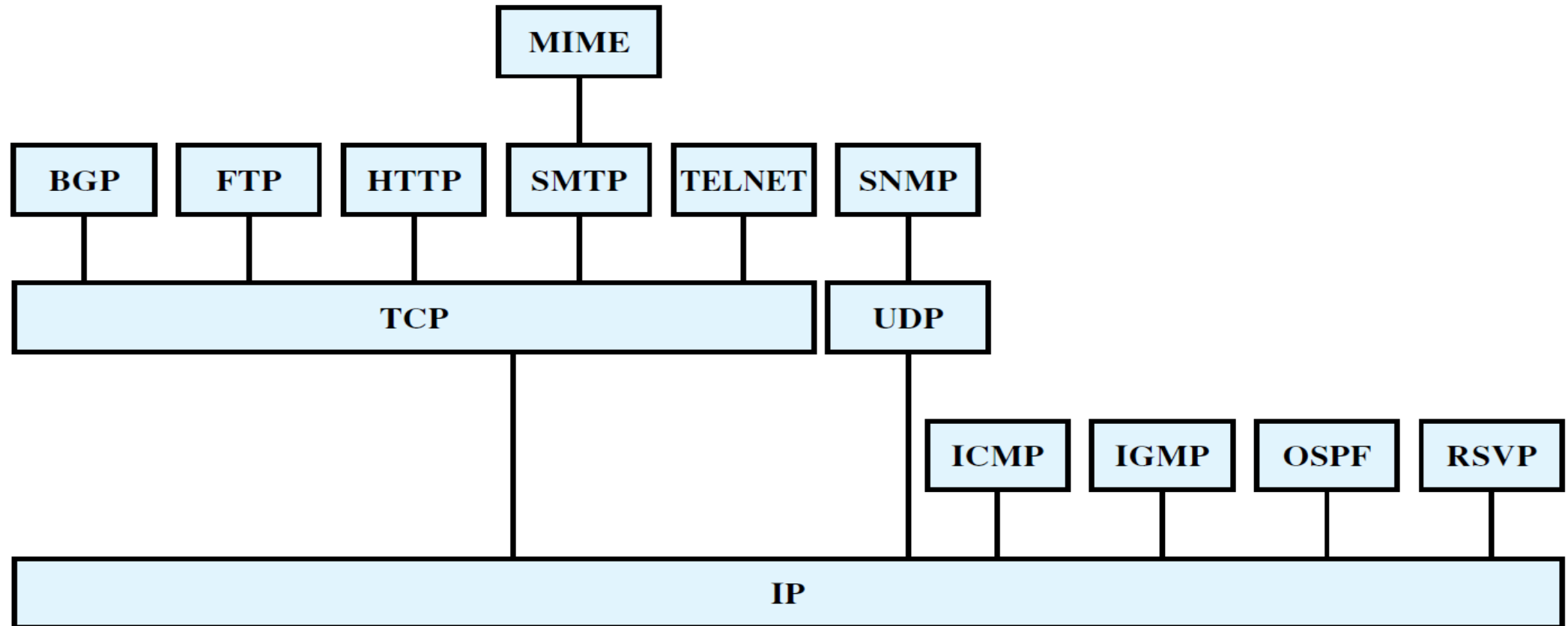


Internet Protocol (2/2)

- It delivers packets from the source to the destination based on the **IP addresses**
- IP address is a 32-bit identifier associated with sender/receiver
 - IP address is stored in datagram (packet) headers
- It encapsulates the data to be delivered in its **packet format**
- It defines addressing methods that are used to label the datagram
 - source information
 - destination information



Internetworking Protocols



BGP = Border Gateway Protocol

FTP = File Transfer Protocol

HTTP = Hypertext Transfer Protocol

ICMP = Internet Control Message Protocol

IGMP = Internet Group Management Protocol

IP = Internet Protocol

MIME = Multipurpose Internet Mail Extension

OSPF = Open Shortest Path First

RSVP = Resource ReSerVation Protocol

SMTP = Simple Mail Transfer Protocol

SNMP = Simple Network Management Protocol

TCP = Transmission Control Protocol

UDP = User Datagram Protocol



IP - Connectionless Internetworking

- **Advantages**

- Flexibility- **requires little from networks**
- Robust- **highly robust service**
- No unnecessary overhead

- **Unreliable**

- Not guaranteed delivery
- Not guaranteed order of delivery
 - Packets can take different routes
- Reliability is responsibility of next layer up (e.g., TCP)

Design Issues

- Routing
- Datagram lifetime
- Fragmentation and re-assembly
- Error control
- Flow control



Design Issues- Routing

- End systems and routers maintain routing tables
 - Indicate next router to which datagram should be sent
 - Static Table
 - May contain alternative routes, if some routes are unavailable
 - Dynamic Table
 - Flexible response to congestion and errors
 - Source routing
 - Source specifies route as sequential list of routers to be followed
 - Security
 - Priority
- Route recording
 - Each router appends its internet address to a list in the datagram



Design Issues- Datagram Lifetime

- Datagrams could loop indefinitely due to dynamic/alternate routes
 - Consumes resources
 - Transport protocol may need upper bound on datagram life
- Datagram marked with lifetime
 - Time To Live field in IP
 - Once lifetime expires, datagram discarded (not forwarded)
 - Hop count
 - Decrement time to live on passing through a each router
 - Time count
 - Need to know how long since last router forwarded it
 - It can be used in the reassembly algorithm



Design Issues- Fragmentation and Re-assembly

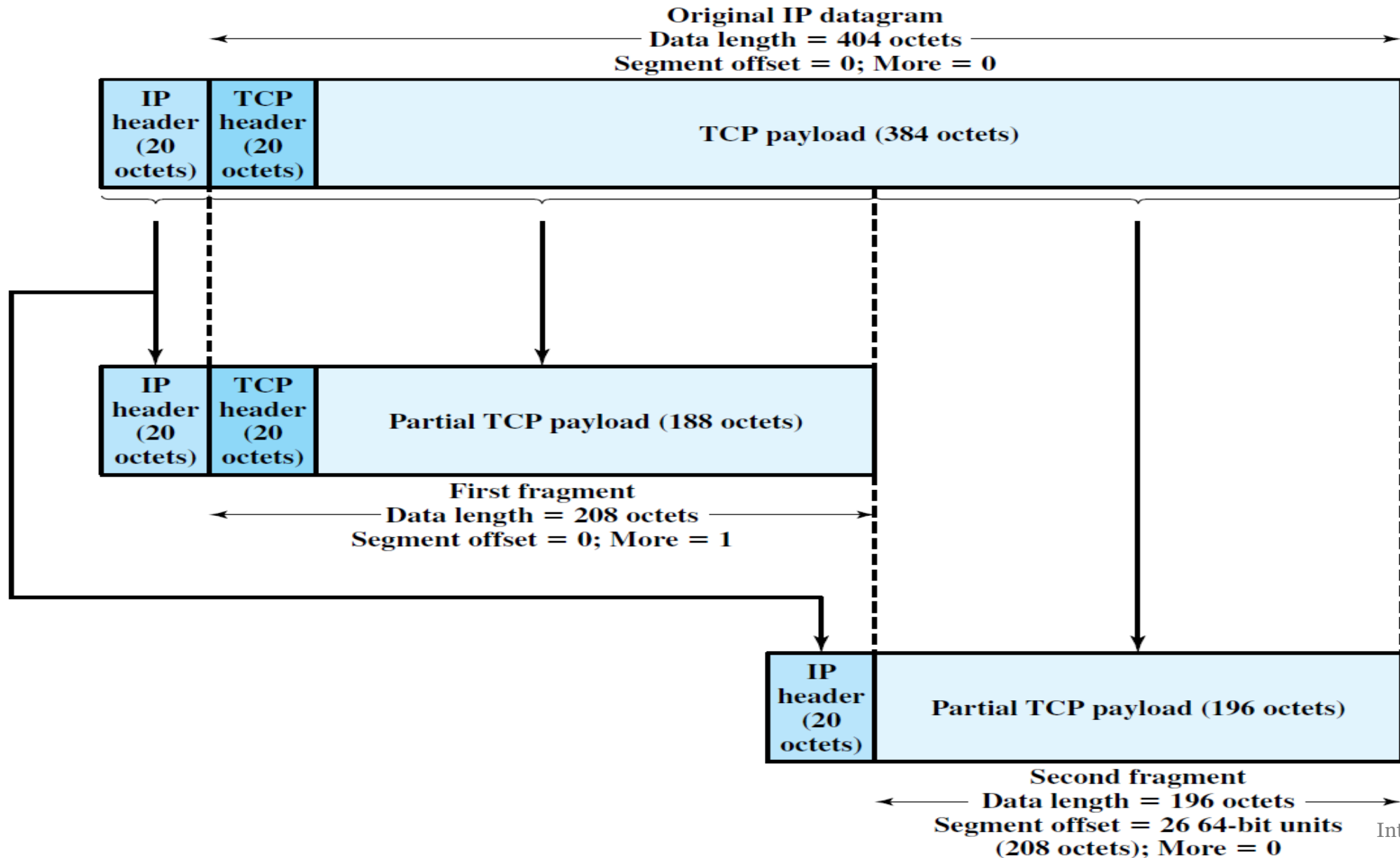
- Different packet sizes need to be divided
- When to re-assemble
 - At destination
 - Results in packets getting smaller as data traverses Internet
 - Intermediate re-assembly
 - Need large buffers at routers
 - Buffers may fill with fragments
- All fragments must go through same router
 - Inhibits dynamic routing

Design Issues- IP Fragmentation

- IP re-assembles at destination only
- Use fields in header
 - Data Unit Identifier (ID)
 - Identifies end system originated datagram
 - Source and destination address
 - Protocol layer generating data (TCP)
 - Identification supplied by that layer
 - Data length
 - Length of user data in octets
 - Offset
 - Position of fragment of user data in original datagram
 - In multiples of 64 bits (8 octets)
- *More* flag
 - Indicates that this is not the last fragment



Fragmentation Example





Design Issues- Dealing with Failure

- Re-assembly may fail if some fragments get lost
- Need to detect failure
- Re-assembly time out
 - Assigned to first fragment to arrive
 - If timeout expires before all fragments arrive, discard partial data
- Use packet lifetime (time to live in IP)
 - If time to live runs out, kill partial data



Design Issues- Error Control

- Not guaranteed delivery
- Router should attempt to inform source if packet discarded
 - e.g. for time to live expiring
- Source may modify transmission strategy
- May inform high layer protocol
- Datagram identification needed
- (Look up ICMP)
 - Internet Control Message Protocol



Design Issues- Flow Control

- Allows routers and/or stations to limit rate of incoming data
- Limited in connectionless systems
- Send flow control packets
 - Requesting reduced flow
- e.g. ICMP



IP Services

- The services between IP and TCP are expressed in terms of *primitives* and *parameters*
- **Parameters**
 - Used to pass data and control information
- **Primitives**
 - Functions to be performed
 - Form of primitive implementation dependent
 - e.g. subroutine call
 - Send primitive
 - Request transmission of data unit
 - Deliver primitive
 - Notify user of arrival of data unit



Parameters (1)

- **Parameters associated with two primitives**
 - **Source address**
 - **Destination address**
 - **Protocol**
 - Recipient e.g., TCP
 - **Type of Service**
 - Specify treatment of data unit during transmission through networks
 - **Identification**
 - Combined with source, destination address and user protocol
 - Uniquely identifies PDU (Protocol Data Unit)
 - Needed for re-assembly and error reporting
 - Send only



Parameters (2)

- **Parameters associated with two primitives**
- **Don't fragment indicator**
 - Can IP fragment data
 - If not, may not be possible to deliver
 - Send only
- **Data length**
 - Length of data being transmitted.
- **Time to live**
 - Measured in seconds
- **Option data**
 - Options requested by the IP user.
- **User data**
 - User data to be transmitted

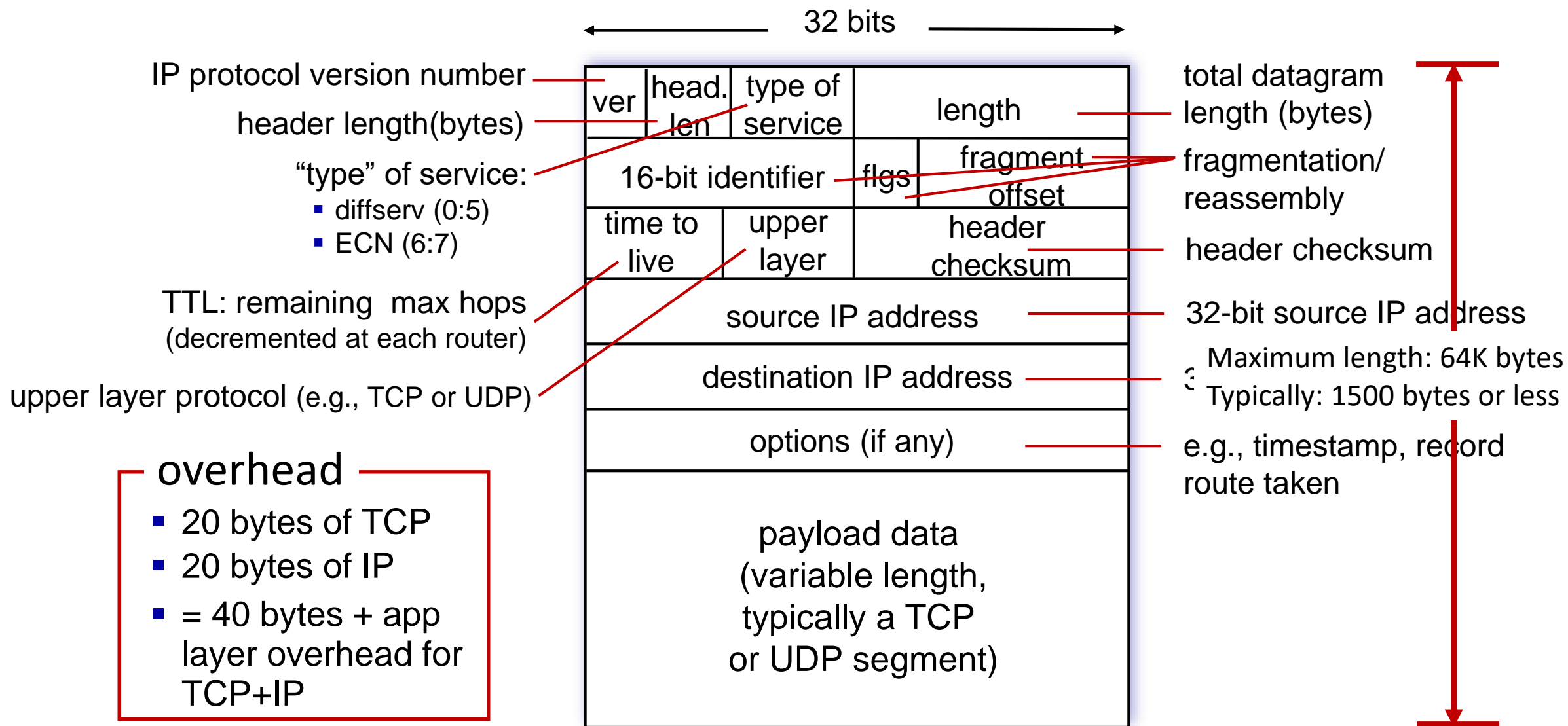


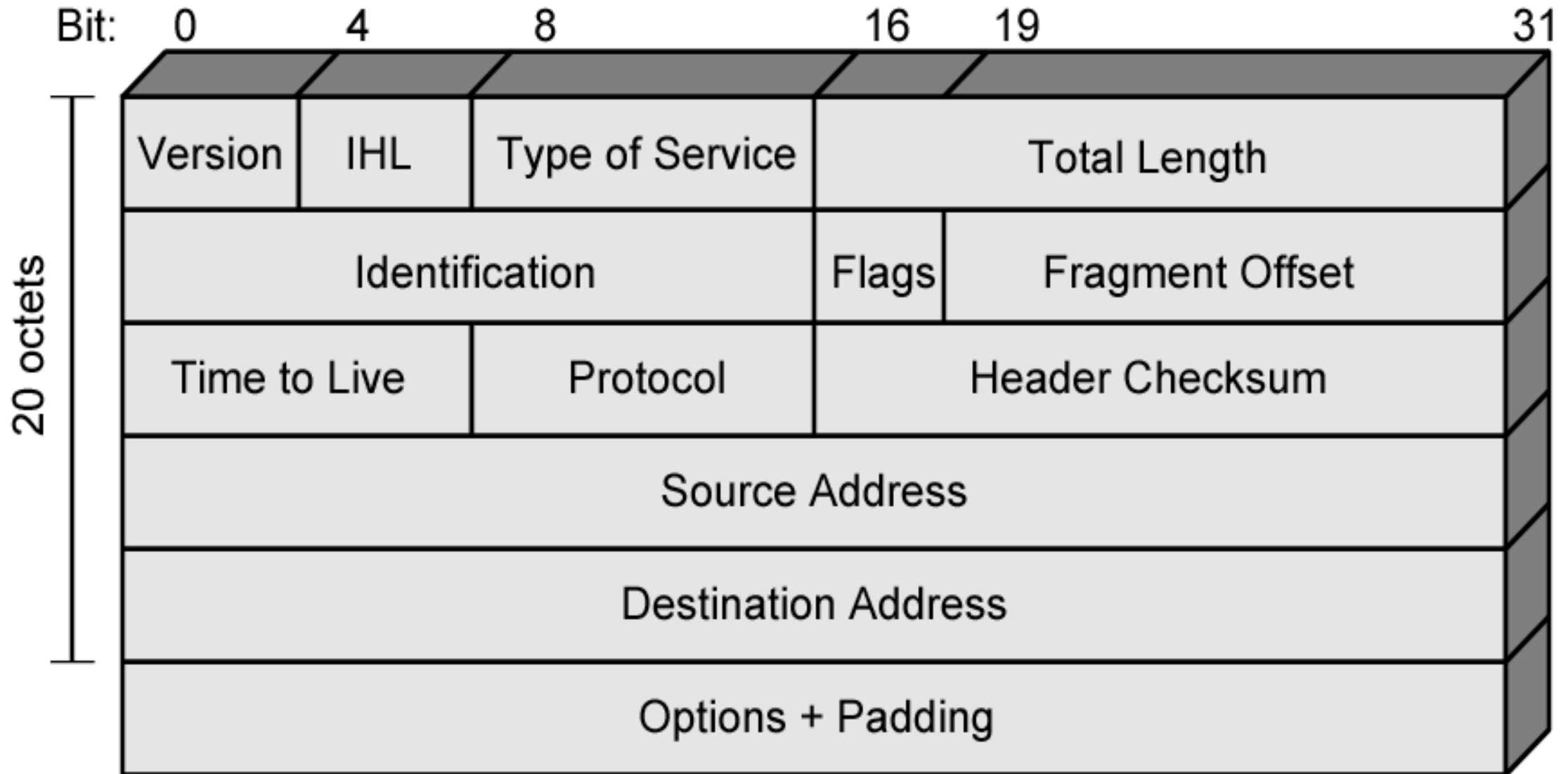
Types of Services

- Precedence
 - 8 levels, higher value shows higher importance
- Reliability
 - Normal or high
- Delay
 - Normal or low
- Throughput
 - Normal or high



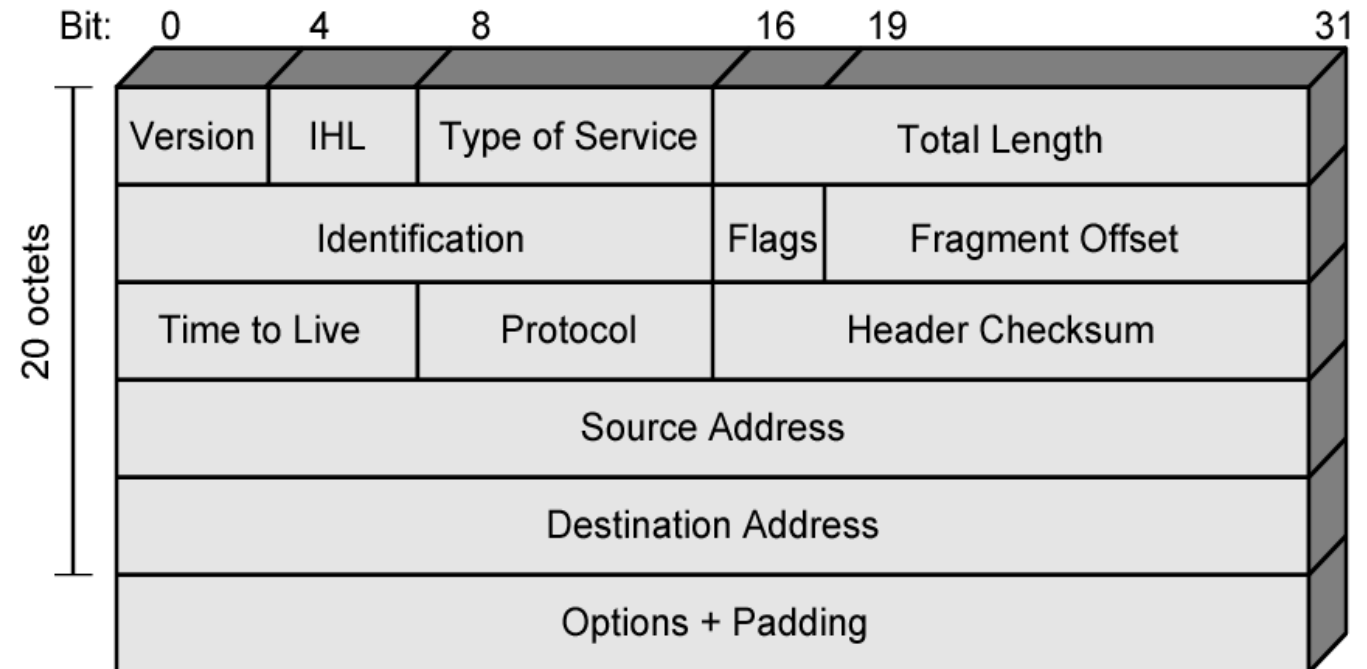
IP Datagram Format





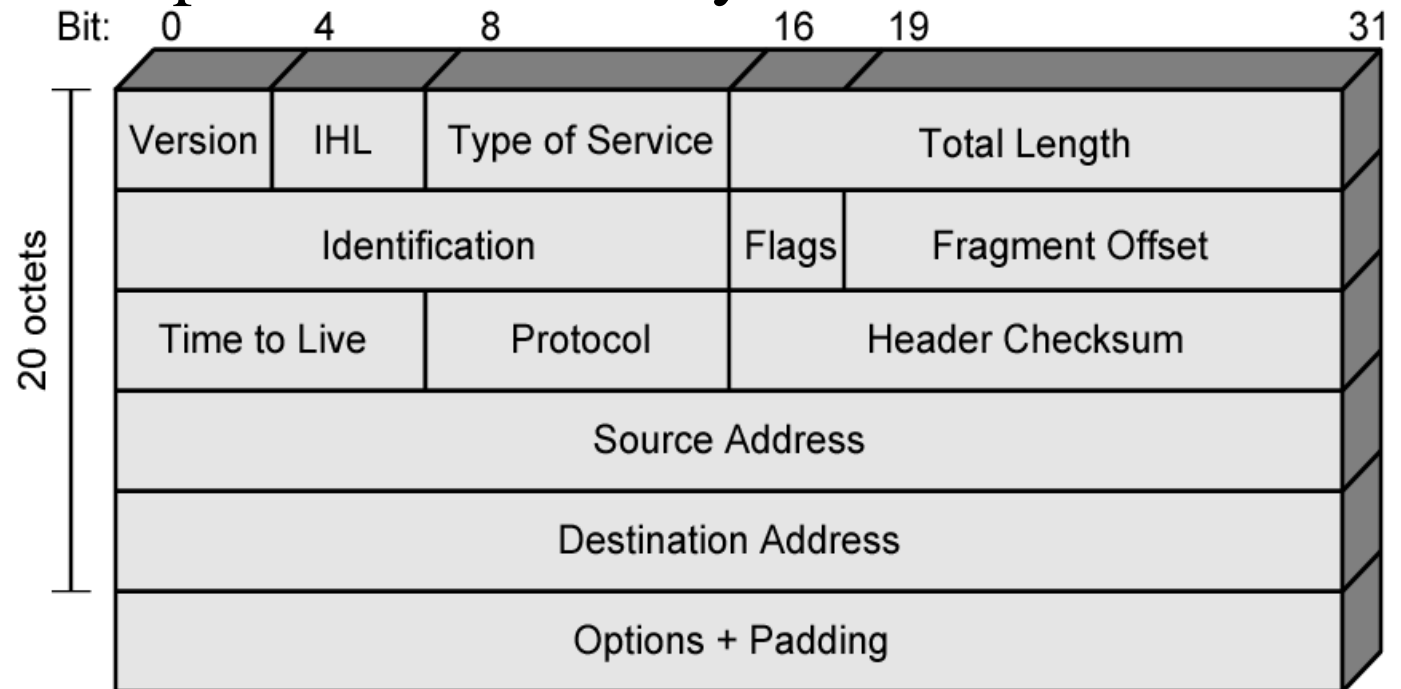
Header Fields (1)

- Version
 - We discuss 4
 - IP v6 - later
- Internet header length
 - In 32 bit words
 - Including options
- Type of service
- Total length
 - Of datagram in octets



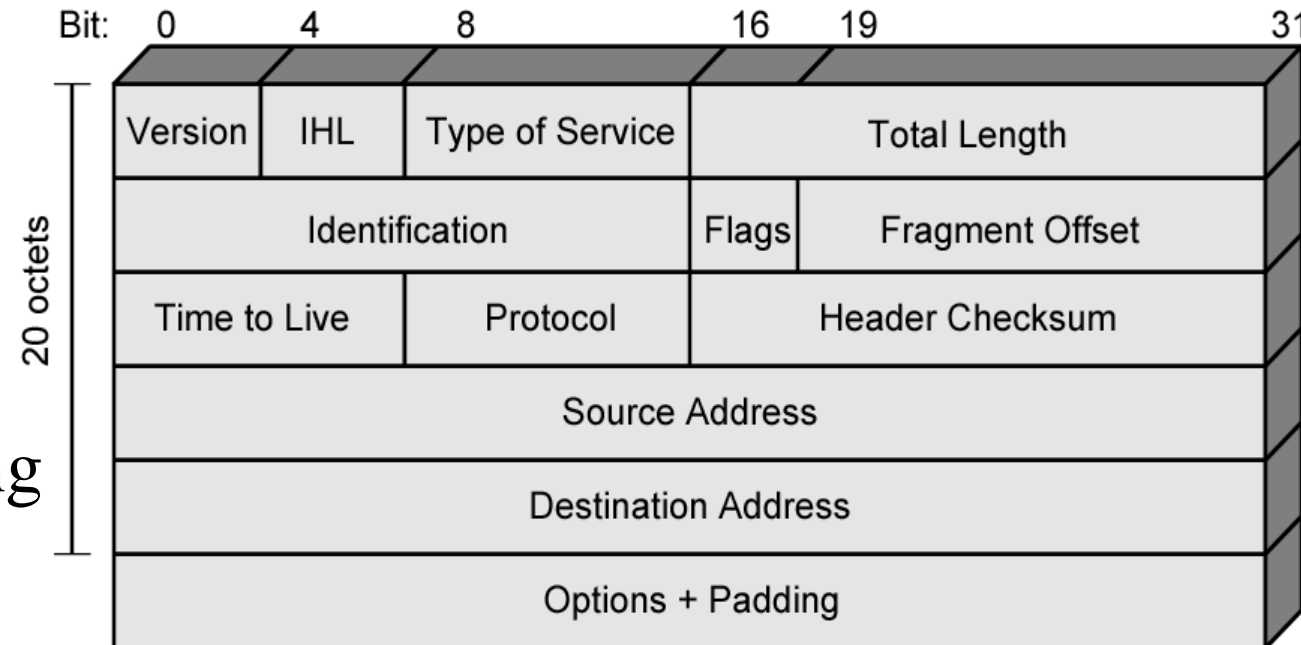
Header Fields (2)

- Identification
 - Sequence number
 - Used with addresses and user protocol to identify datagram uniquely
- Flags
 - More bit
 - Don't fragment
- Fragmentation offset
- Time to live
- Protocol
 - Next higher layer to receive data field at destination



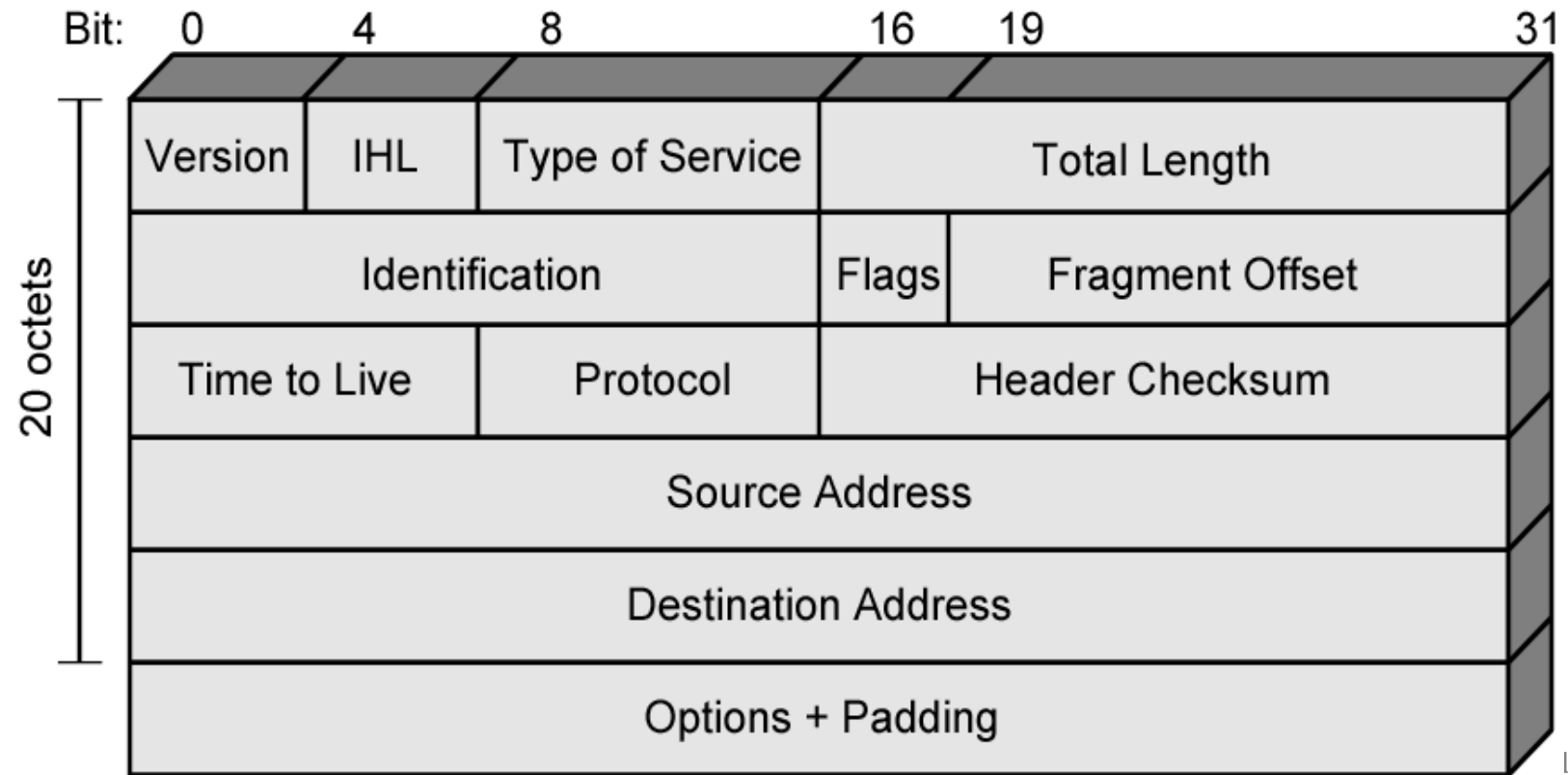
Header Fields (3)

- Header checksum
 - Reverified and recomputed at each router
 - 16 bit ones complement sum of all 16 bit words in header
 - Set to zero during calculation
- Source address
- Destination address
- Options
 - To fill to multiple of 32 bits long



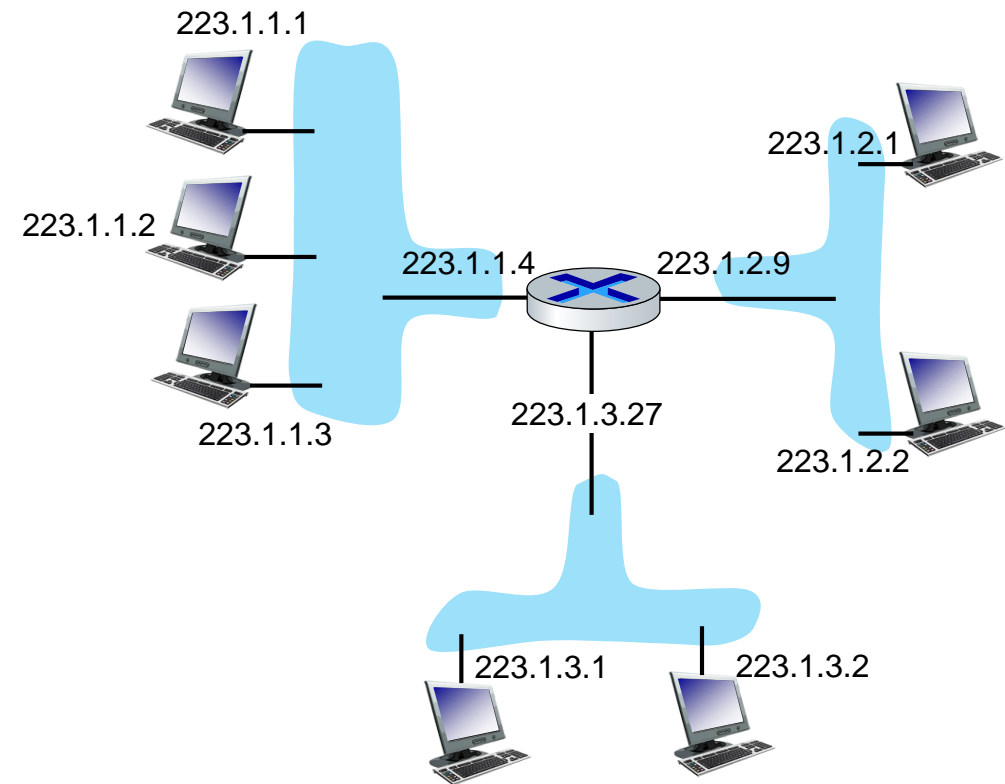
Data Field

- Carries user data from next layer up
- Integer multiple of 8 bits long (octet)
- Max length of datagram (header plus data) 65,535 octets



IP addressing: introduction

- **IP address:** 32-bit identifier associated with each host or router *interface*
- **Interface:** connection between host/router and physical link
 - router's typically have multiple interfaces
 - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)



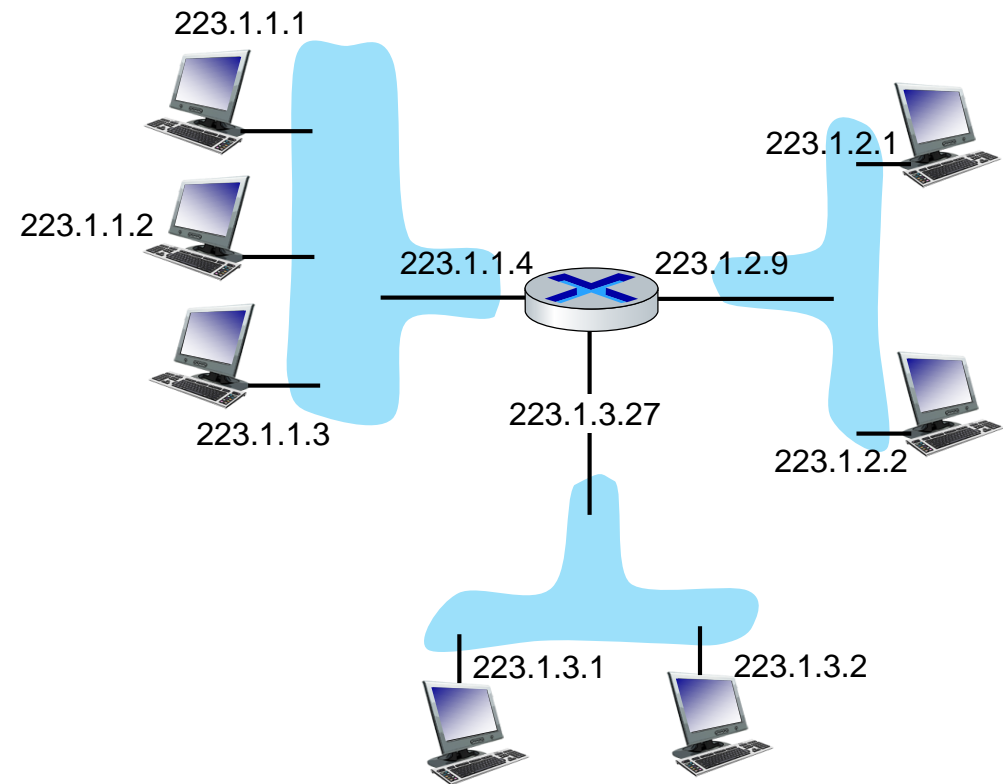
dotted-decimal IP address notation:

223.1.1.1 = $\underbrace{11011111}_{223} \underbrace{00000001}_{1} \underbrace{00000001}_{1} \underbrace{00000001}_{1}$



IP addressing: introduction

- **IP address:** 32-bit identifier associated with each host or router *interface*
- **interface:** connection between host/router and physical link
 - router's typically have multiple interfaces
 - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)



dotted-decimal IP address notation:

223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Network Layer: 4-38

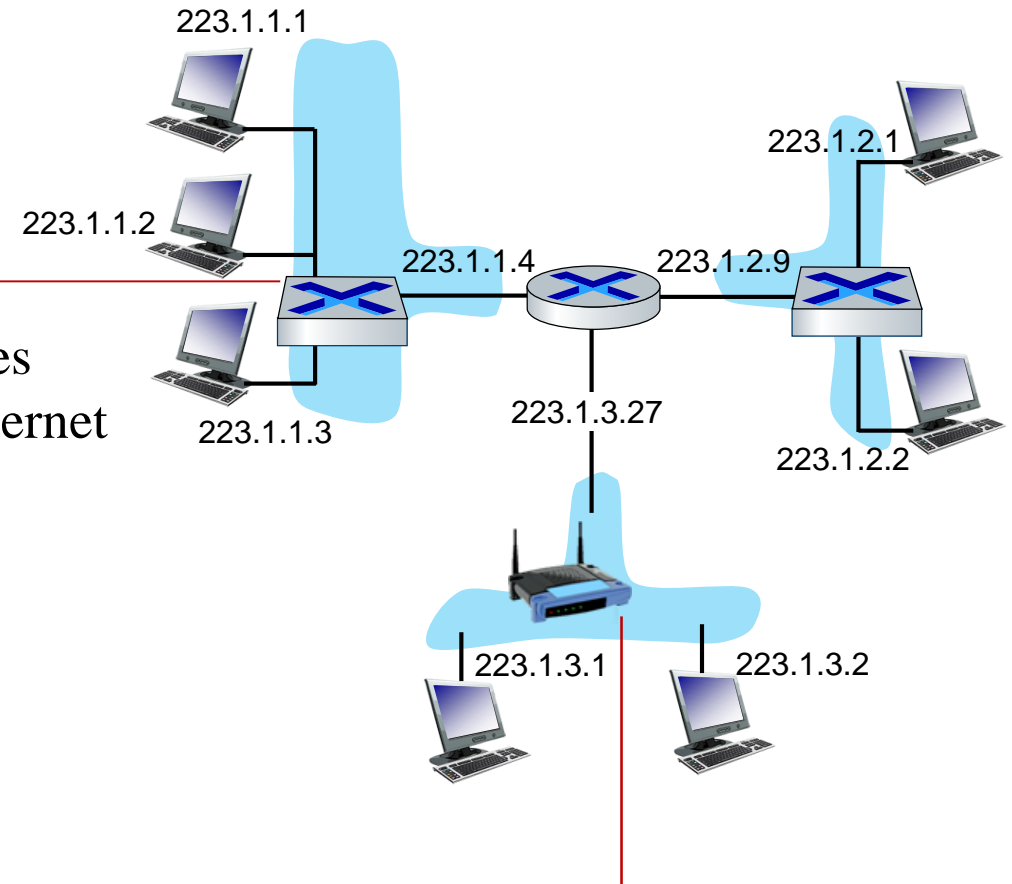
IP addressing: introduction

Q: how are interfaces actually connected?

A: We will not cover more details in this lecture

For now: don't need to worry about how one interface is connected to another (with no intervening router)

A: wired Ethernet interfaces connected by Ethernet switches



A: wireless WiFi interfaces connected by WiFi base station



IPv4 Addressing

- **IP Address**

- 32-bit address
- Four 8-bit decimal values between 0 and 255 separated by periods (octets)

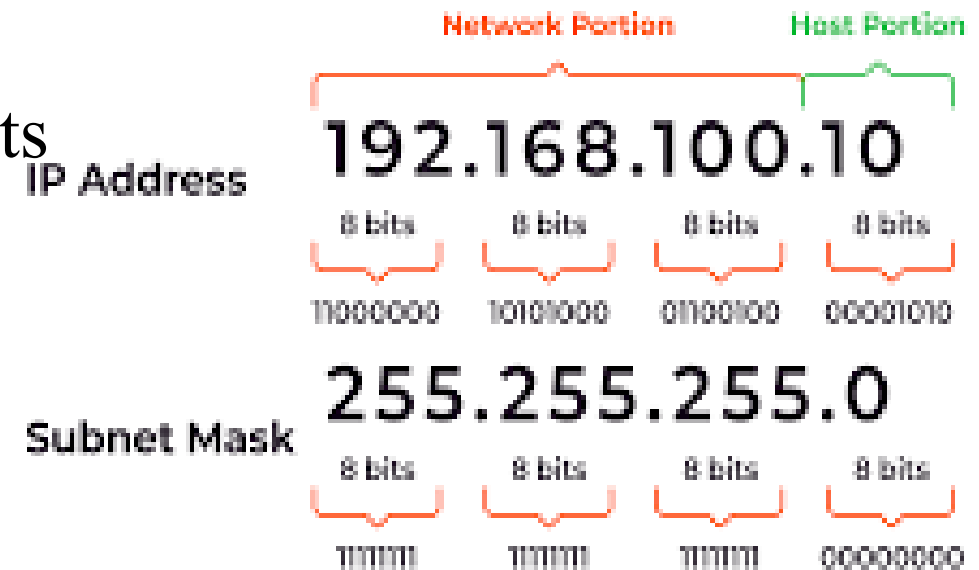
- **Subnet Mask**

- 32-bit value of 0's and 1's
- 1's designate network bits, 0's are host bits

Examples: IP Address **192.168.100.10**

Subnet Mask **255.255.255.0**

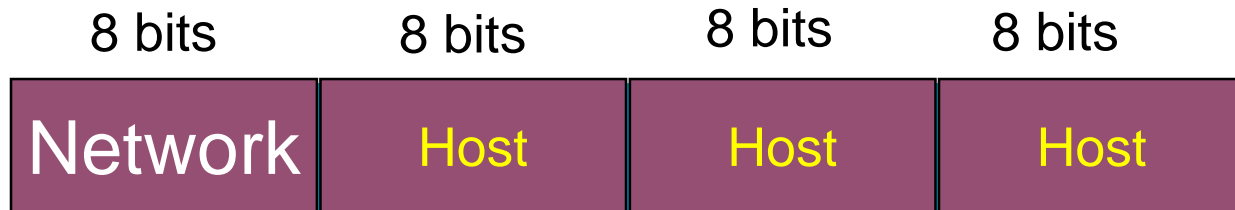
Binary Notation of IP Address and Subnet





IP Addressing-Classes

- Class A:



- Class B:

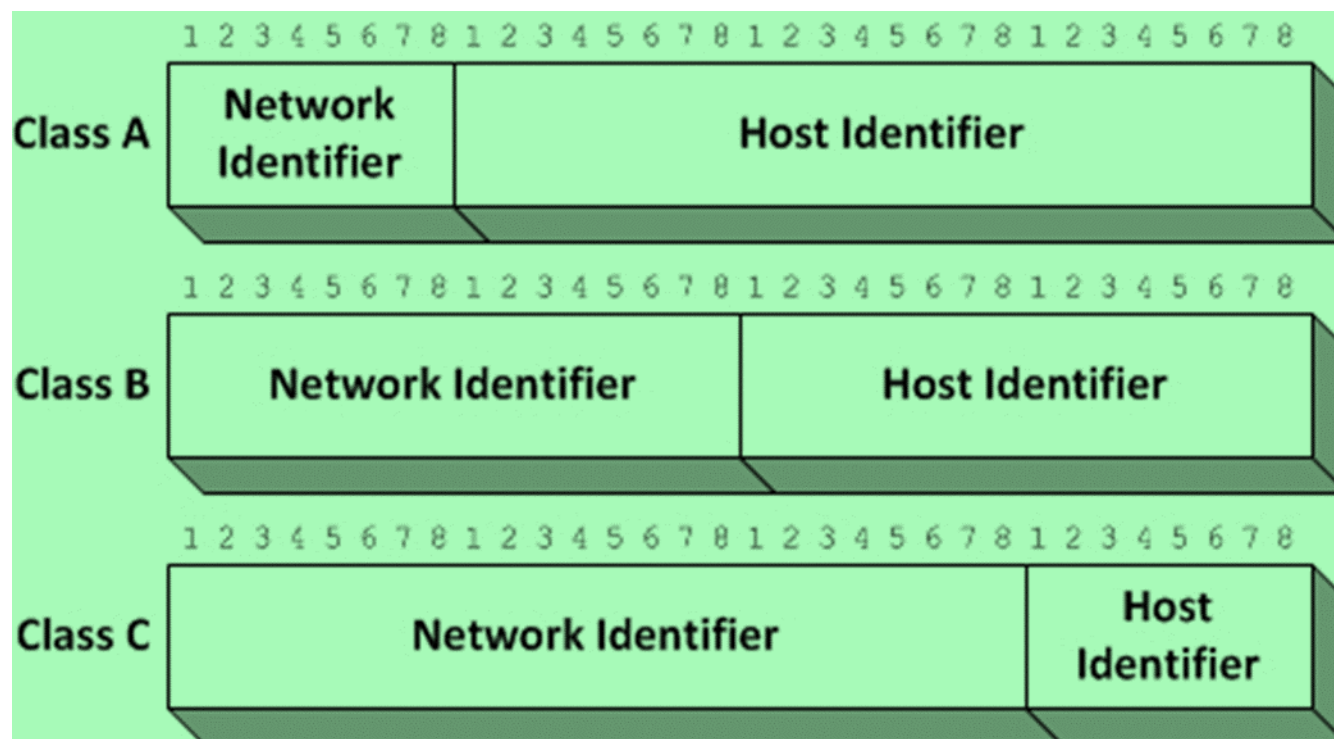


- Class C:



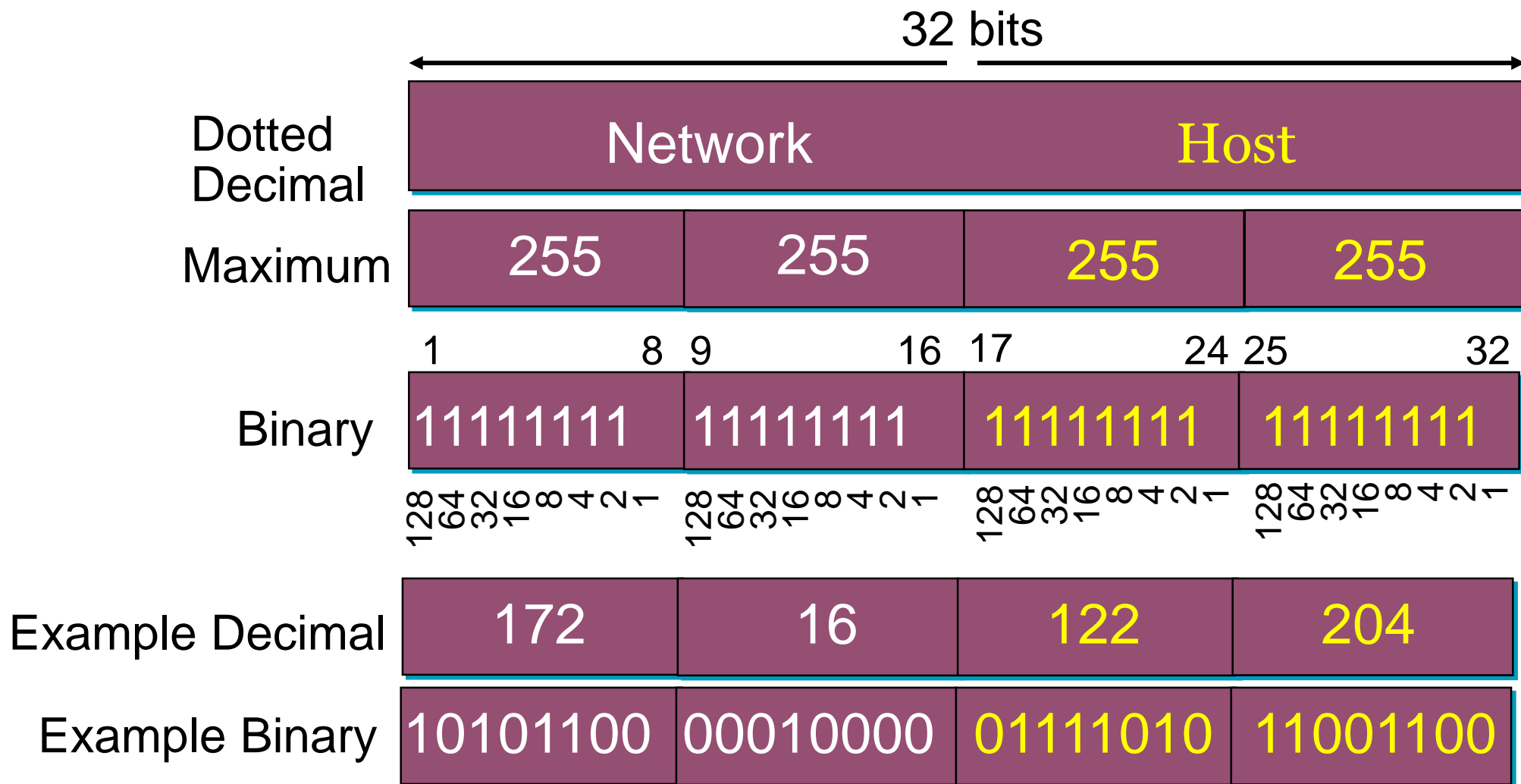
- Class D: Multicast

- Class E: Research



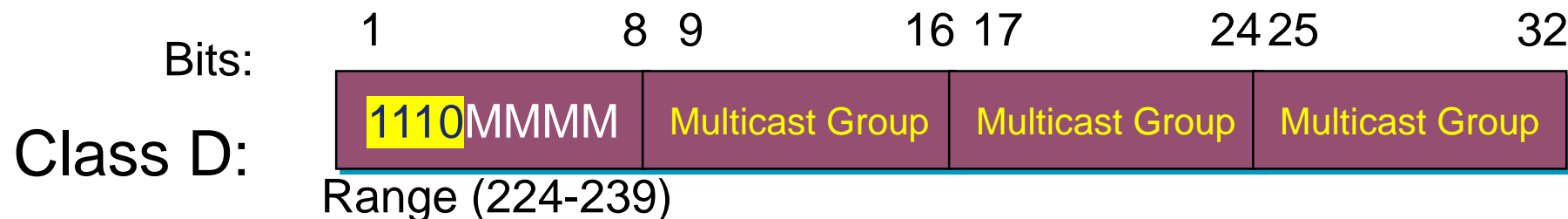
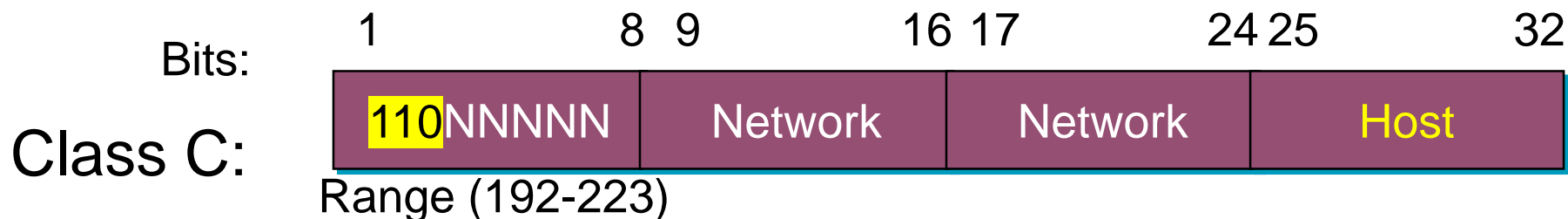
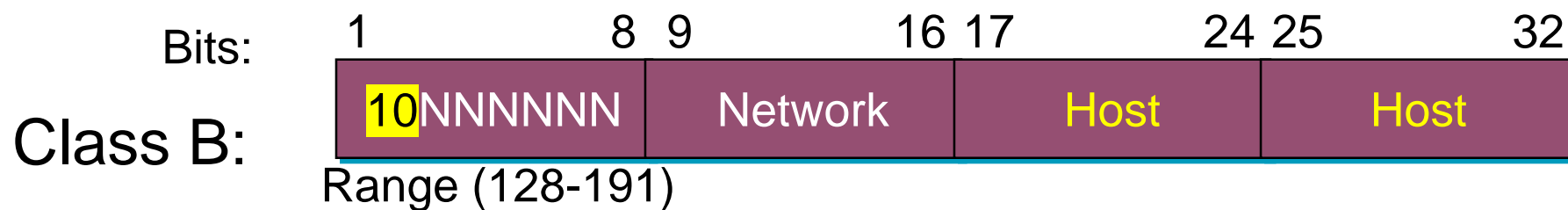
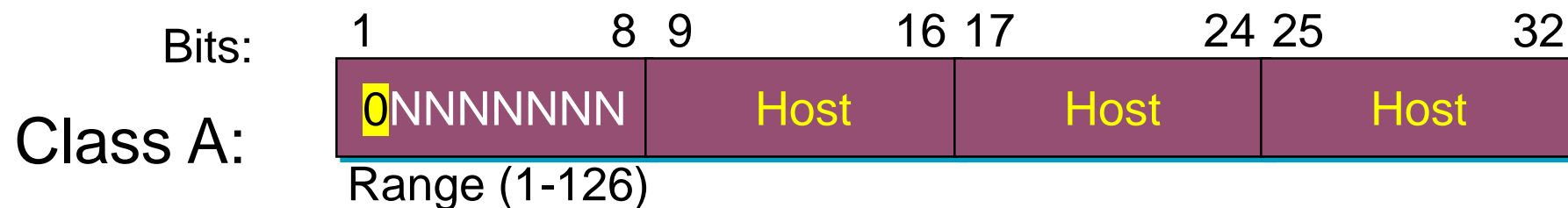


IP Addressing Formats



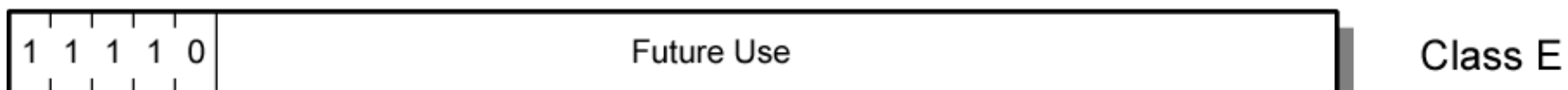
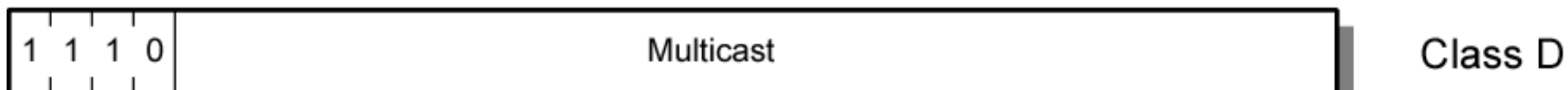
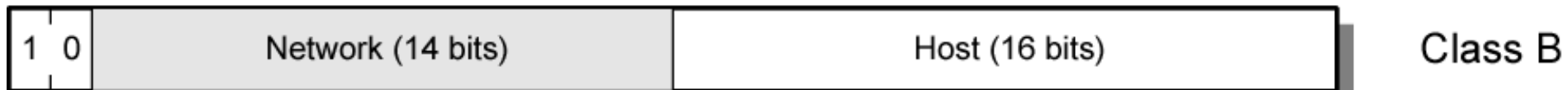
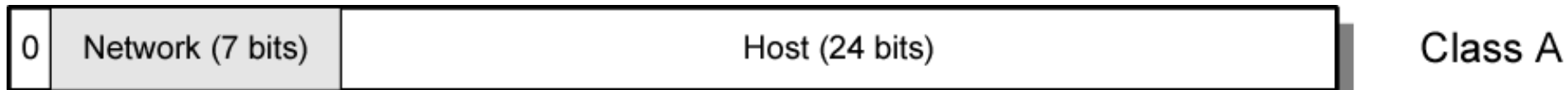


IP Addressing Formats

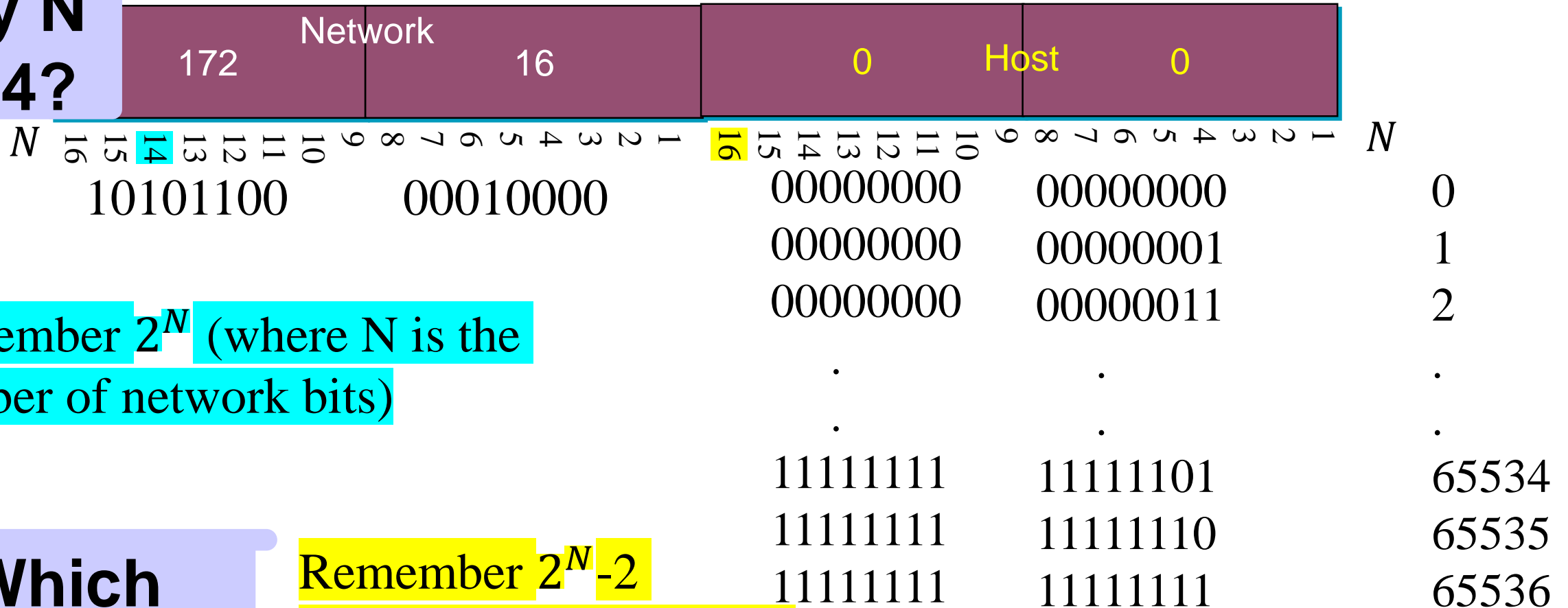




IPv4 Address Formats



- # Why N is 14?



Which Class IP?

Remember $2^N - 2$
(where N is the number
of host bits)

$$2^{16} - 2 = 65534$$



Networks/Host Ranges

<i>IP Address Class</i>	<i>Class A</i>	<i>Class B</i>	<i>Class C</i>
First bit values (binary)	0	10	110
First byte value (decimal)	0–127	128–191	192–223
Number of network identifier bits	8	16	24
Number of host identifier bits	24	16	8
Number of possible networks	126	16,384	2,097,152
Number of possible hosts	16,777,214	65,534	254

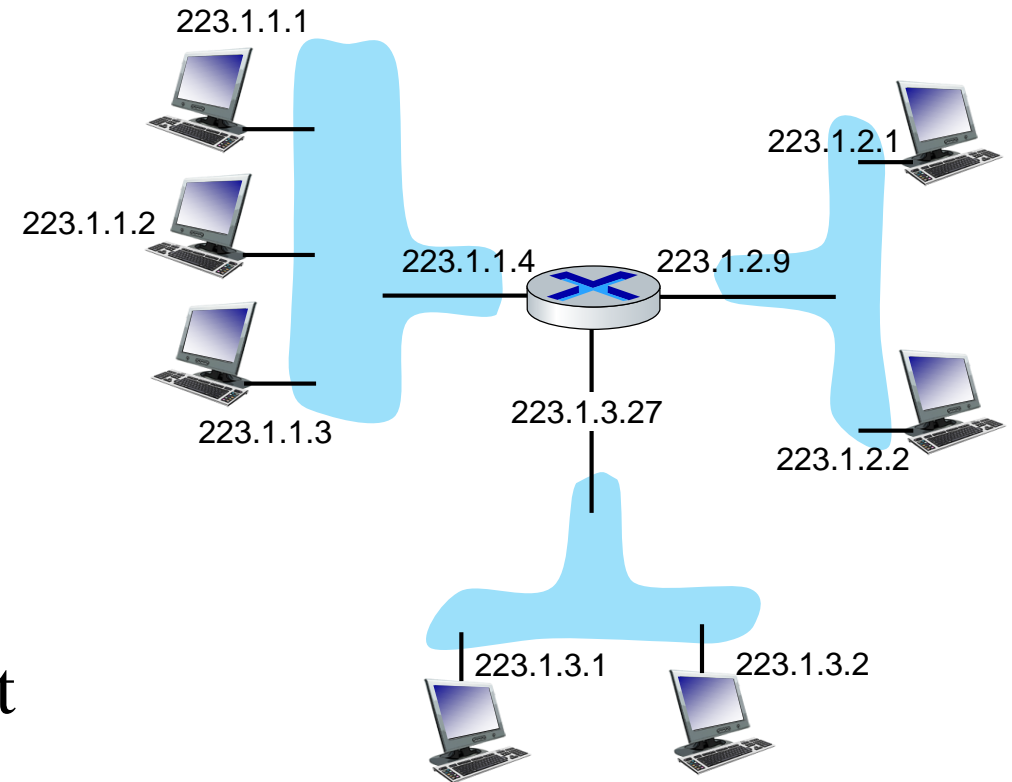


Subnets and Subnet Masks

- Allow arbitrary complexity of internetworked LANs within organization
- Insulate overall internet **from growth of network numbers** and routing complexity
- Site looks to rest of internet like single network
- Each LAN assigned subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- **Subnet mask** indicates which bits are subnet number and which are host number

Subnets

- *What's a subnet ?*
 - device interfaces that can physically reach each other **without passing through an intervening router**
- IP addresses have structure:
 - **subnet part:** devices in same subnet have common high order bits
 - **host part: remaining** low order bits

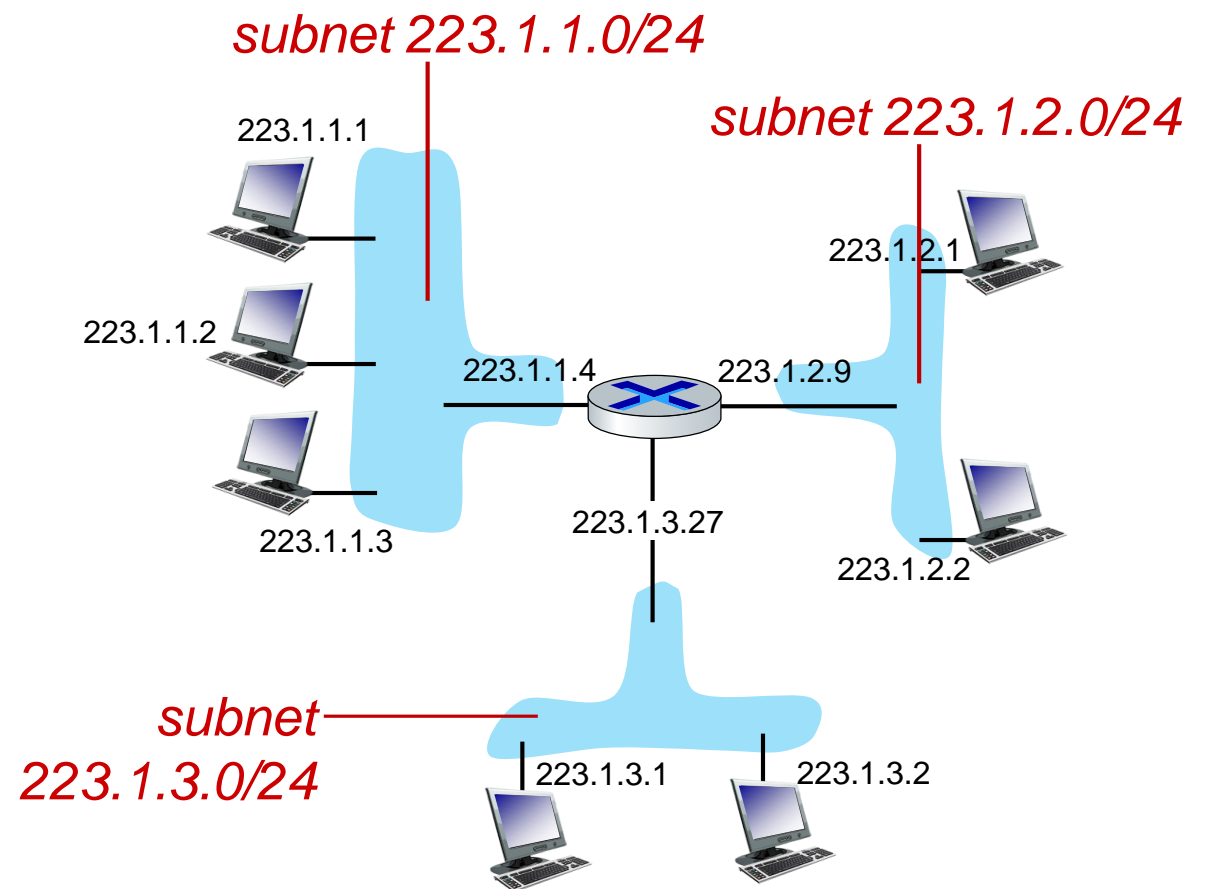


network consisting of 3 subnets

Subnets

Recipe for defining subnets:

- detach each interface from its host or router, creating “islands” of isolated networks
- each isolated network is called a *subnet*



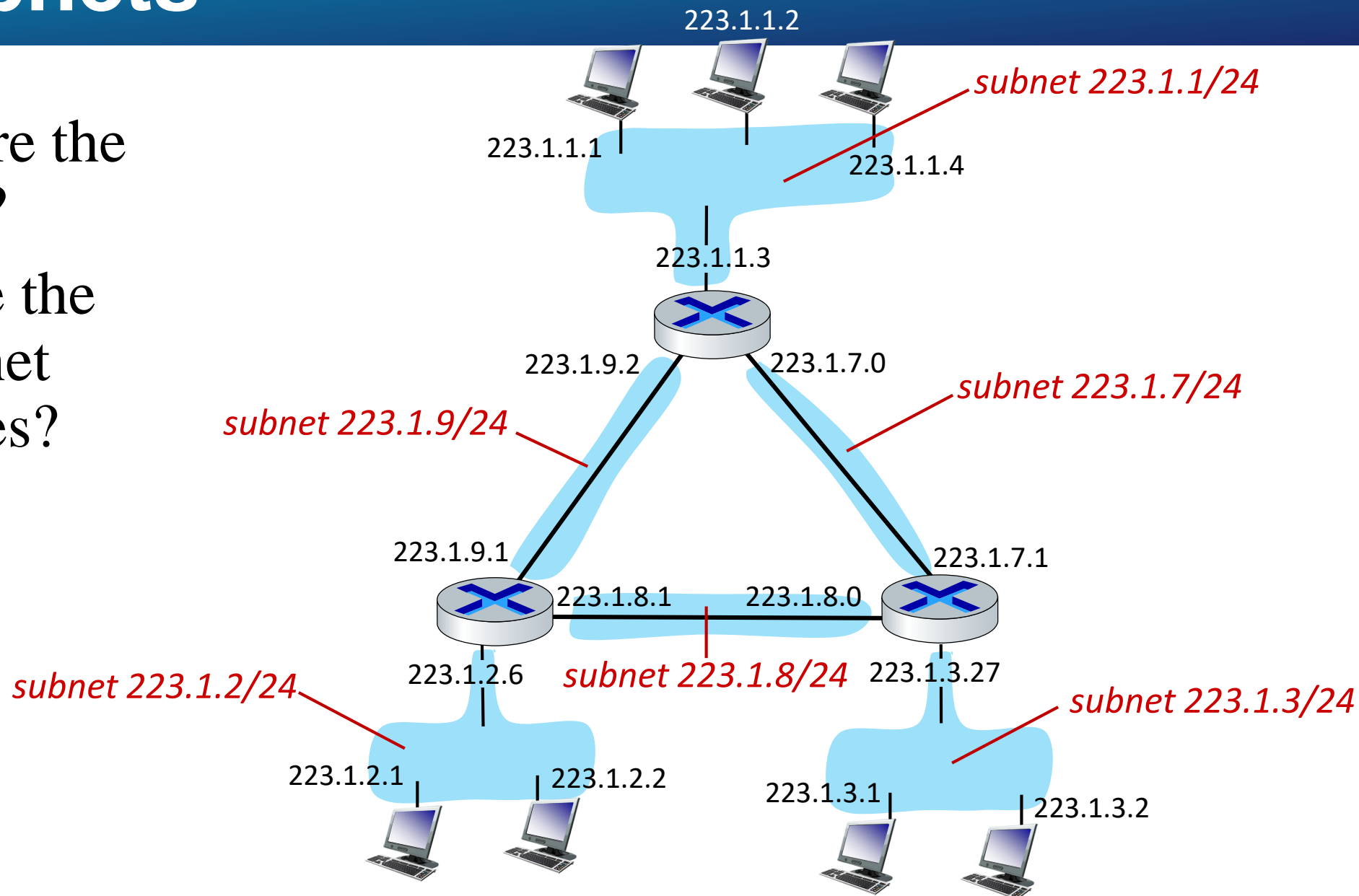
subnet mask: /24

(high-order 24 bits: subnet part of IP address)

Network Layer: 4-49

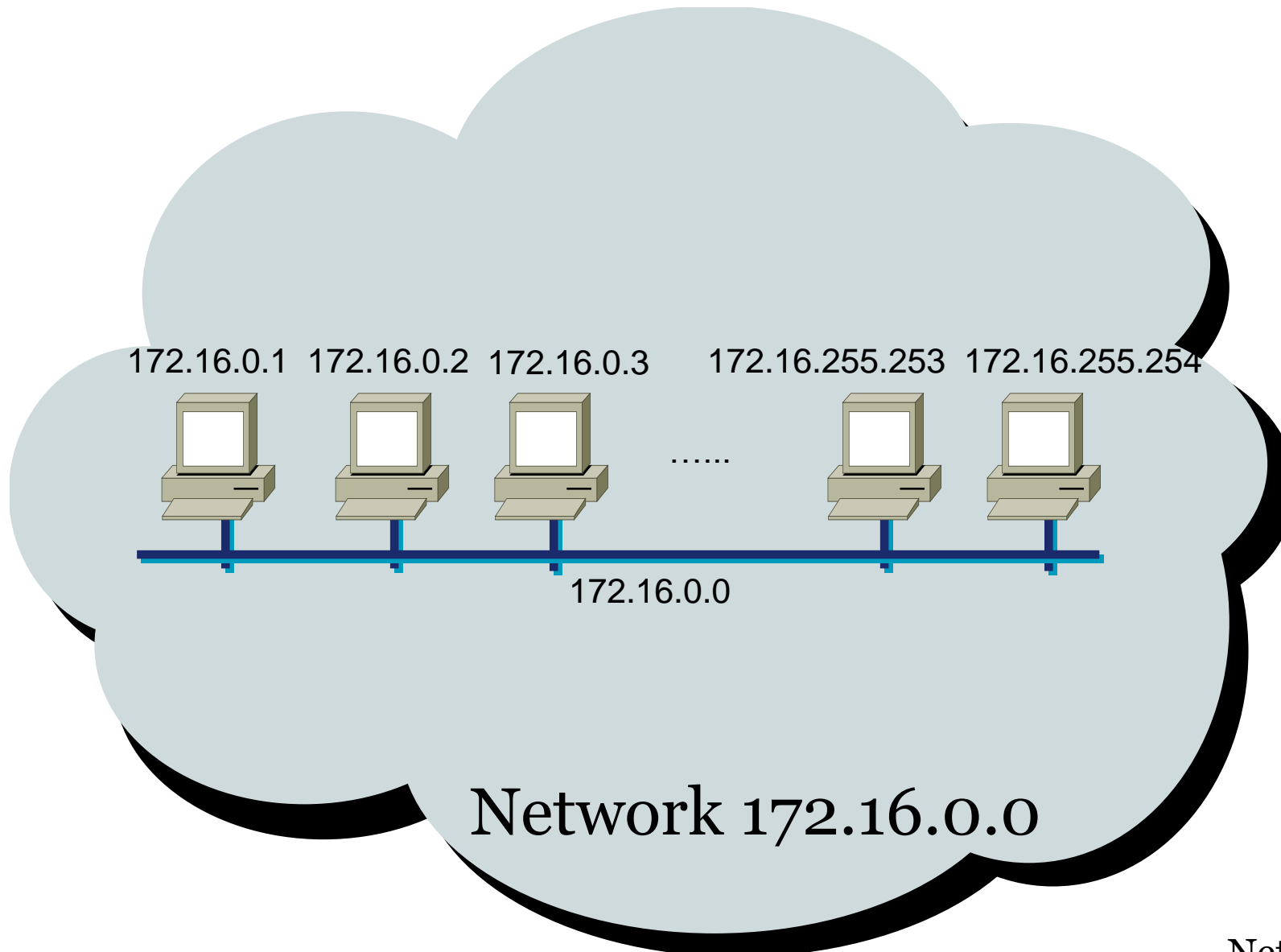
Subnets

- where are the subnets?
- what are the /24 subnet addresses?



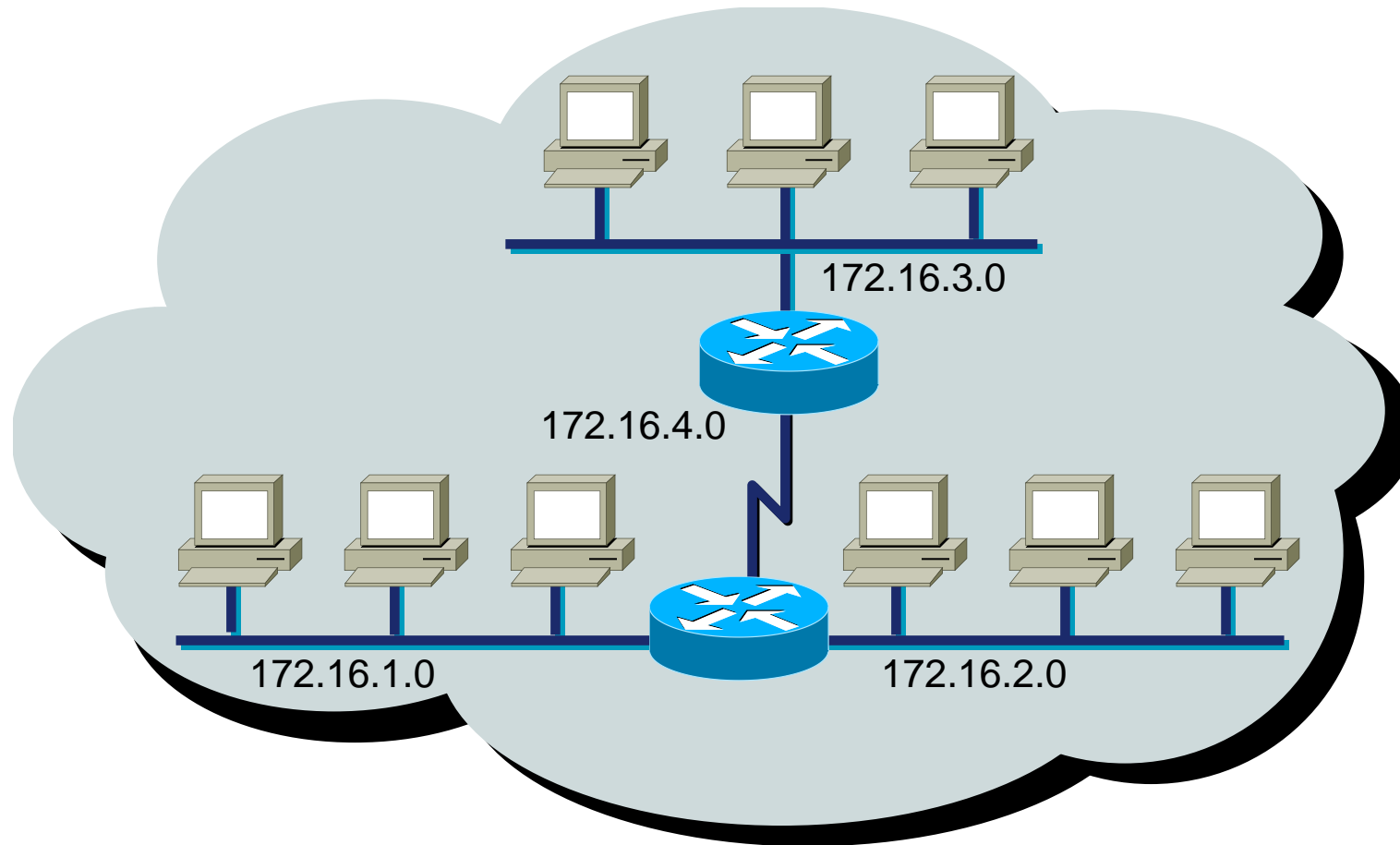


Addressing without Subnets





Addressing with Subnets



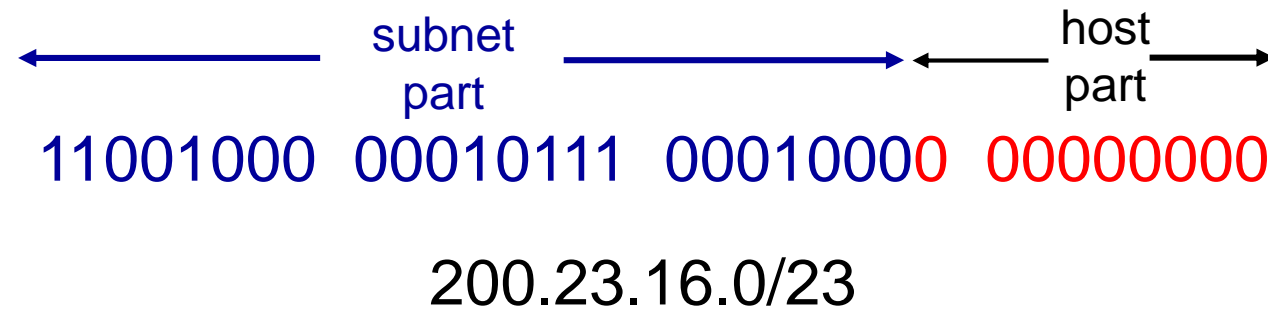
Network 172.16.0.0



IP addressing: CIDR

CIDR: **C**lassless **I**nter**D**omain **R**outing (pronounced “cider”)

- subnet portion of address of arbitrary length
- address format: **a.b.c.d/x**
 - where x is the number of bits in subnet portion of address





IP addressing: CIDR

- Classful addressing was gradually phased out by a series of subnetting methods
 - Variable length subnet masking (VLSM)
 - **Classless Inter-Domain Routing (CIDR)**
- **CIDR** is a subnetting method that enables administrators
 - to place the division between the network bits and the host bits anywhere in the address, not just between octets.
- **VLSM** is a technique used to allocate IP addresses efficiently by dividing a network into smaller subnets of varying sizes
- It is an extension of the traditional subnetting method, which divides a network into fixed-size subnets.



CIDR notation: **192.168.43.0/26**

- Where the **/26** means 26 bits of the address are used as the network identifier
- In binary, the subnet mask translates to:
11111111.11111111.11111111.11000000
or **255.255.255.192** in decimal
- This would allow us to divide this address into **4 networks**, each with up to **62 hosts**



CIDR 192.168.43.0/26 Networks

<i>Network Address</i>	<i>Starting IP Address</i>	<i>Ending IP Address</i>	<i>Subnet Mask</i>
192.168.43.0	192.168.43.1	192.168.43.62	255.255.255.192
192.168.43.64	192.168.43.65	192.168.43.126	255.255.255.192
192.168.43.128	192.168.43.129	192.168.43.190	255.255.255.192
192.168.43.192	192.168.43.193	192.168.43.254	255.255.255.192



Public and Private IPv4 Addressing

- Registered IP addresses are not necessary for workstations that merely access resources on the Internet
- The three blocks of addresses allocated for private use are as follows:
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- Localhost
 - In computer networking, localhost is a hostname that refers to the current computer used to access it
- Localhost address
 - 127.0.0.1
 - ping this IP address means the computer is communicating with itself



IPv4 Subnetting

- Allows you to split one IP address range into multiple networks
 - You can take the 10.0.0.0/8 private IP address range and use the entire second octet as a subnet ID).
- This creates up to 256 subnets with up to 65,536 hosts.
- The subnet masks will be 255.255.0.0 and the network addresses will proceed as follows:
 - 10.0.0.0/16
 - 10.1.0.0/16
 - 10.2.0.0/16
 - ...
 - 10.254.0.0/16
 - 10.255.0.0/16

When you are working on an existing network, the subnetting process is more difficult.



Calculate IPv4 Subnets

1. Determine how many subnet identifier bits you need to create the required number of subnets
2. Subtract the subnet bits you need from the host bits and add them to the network bits
3. Calculate the subnet mask by adding the network and subnet bits in binary form and converting the binary value to decimal
4. Take the least significant subnet bit and the host bits, in binary form, and convert them to a decimal value
5. Increment the network identifier (including the subnet bits) by the decimal value you calculated to determine the network addresses of your new subnets.



Supernetting

- Allows contiguous networks to be added to a routing table with one entry to reduce the size of Internet routing tables.

- For example:

172.16.43.0/24

172.16.44.0/24

172.16.45.0/24

172.16.46.0/24

172.16.47.0/24

- Can all be expressed in one supernet address:

172.16.40.0/21

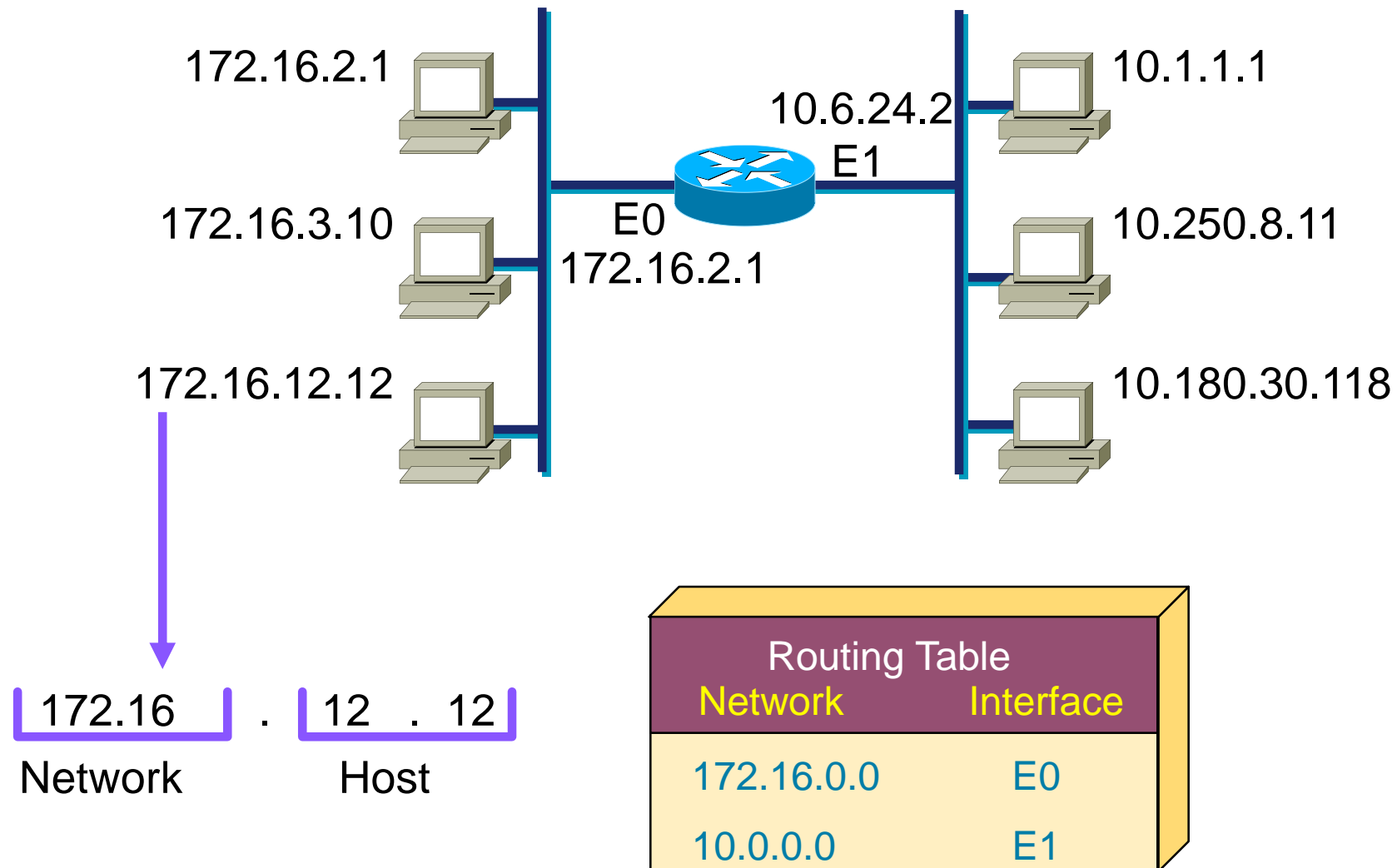
Important Points for Supernetting

- All the Networks should be contiguous.
- The block size of every network should be equal and must be in form of 2^n .
- First Network ID should be exactly divisible by whole size of supernet.

[More on supernetting here](#)



Host Addresses



Determining Available Host Addresses

Network

Host

172	16	0	0
-----	----	---	---

10101100 00010000

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 N

00000000 00000000
00000000 00000001
00000000 00000011
⋮
11111111 11111101
11111111 11111110
11111111 11111111

1
2
3
⋮

65534

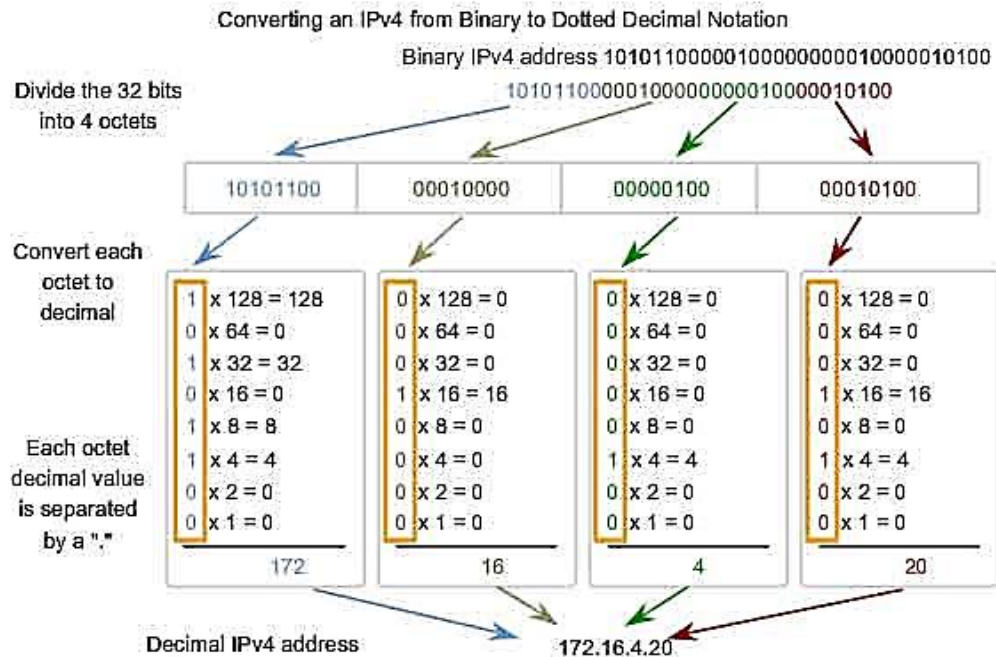
65535

65536

- 2

65534

$$2^N - 2 = 2^{16} - 2 = 65534$$



Network Layer: 4-62



IP Address Classes Exercise

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

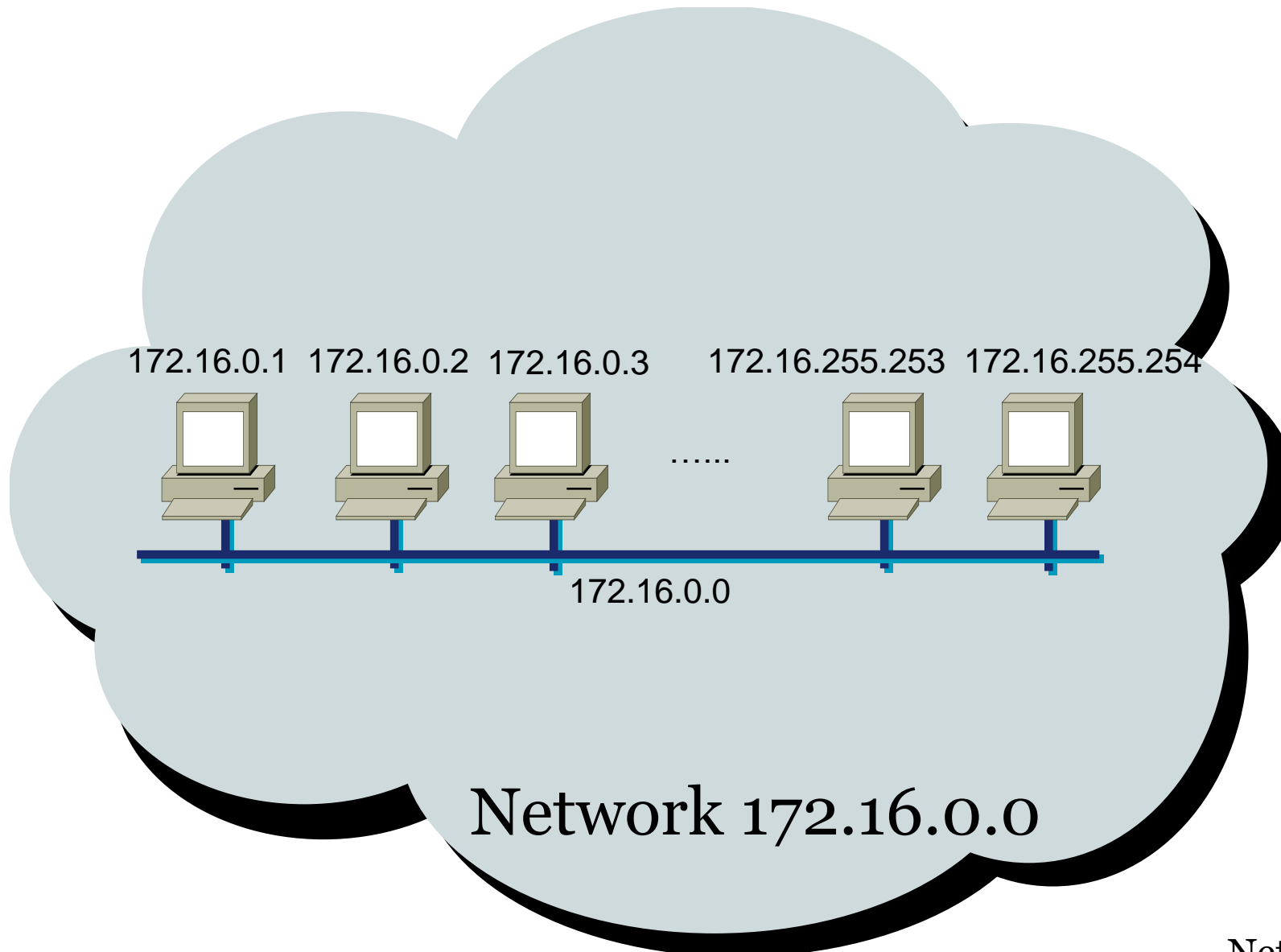


IP Address Classes Exercise Answers

Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
256.241.201.10	Nonexistent		



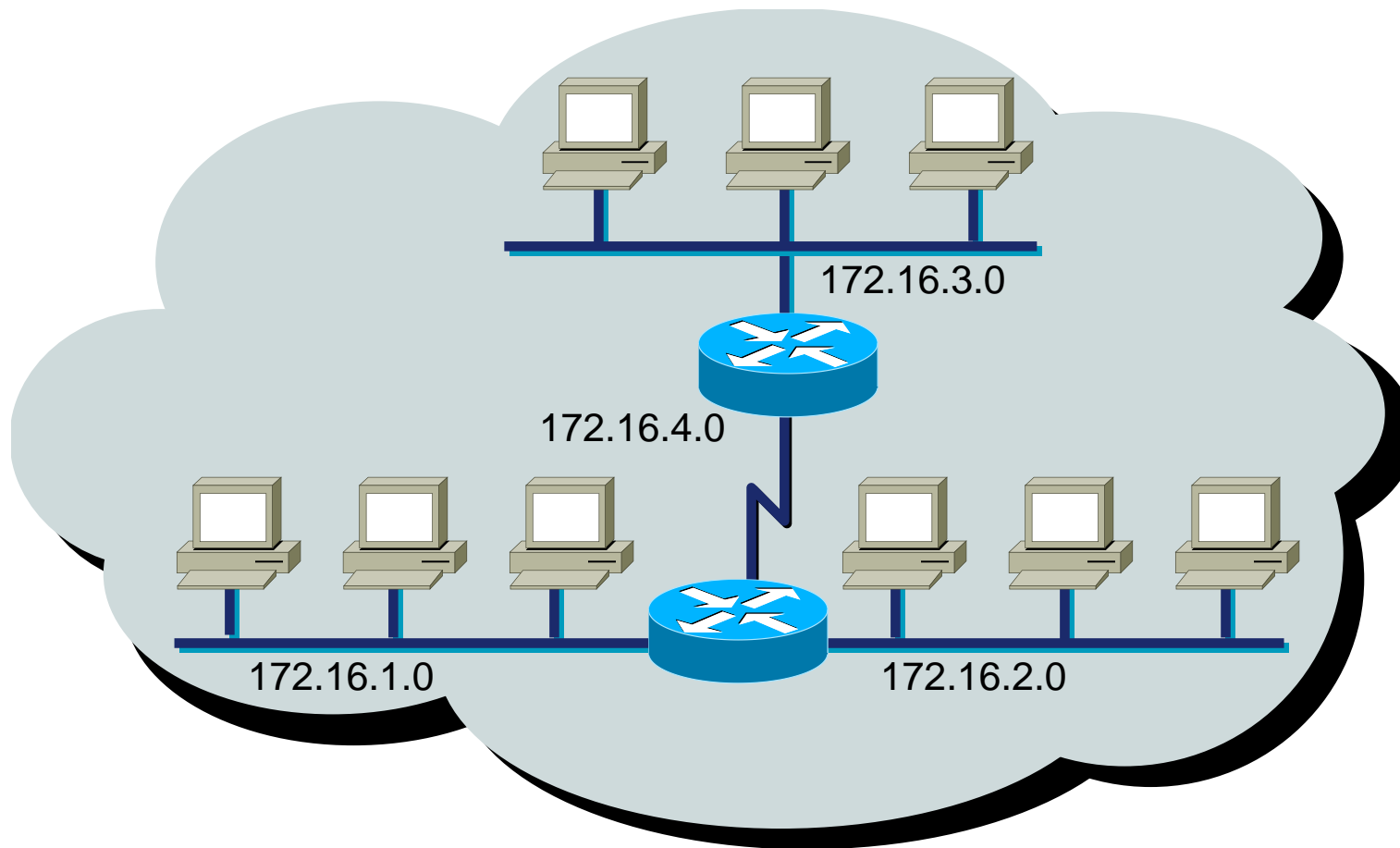
Addressing without Subnets - Recap





Addressing with Subnets

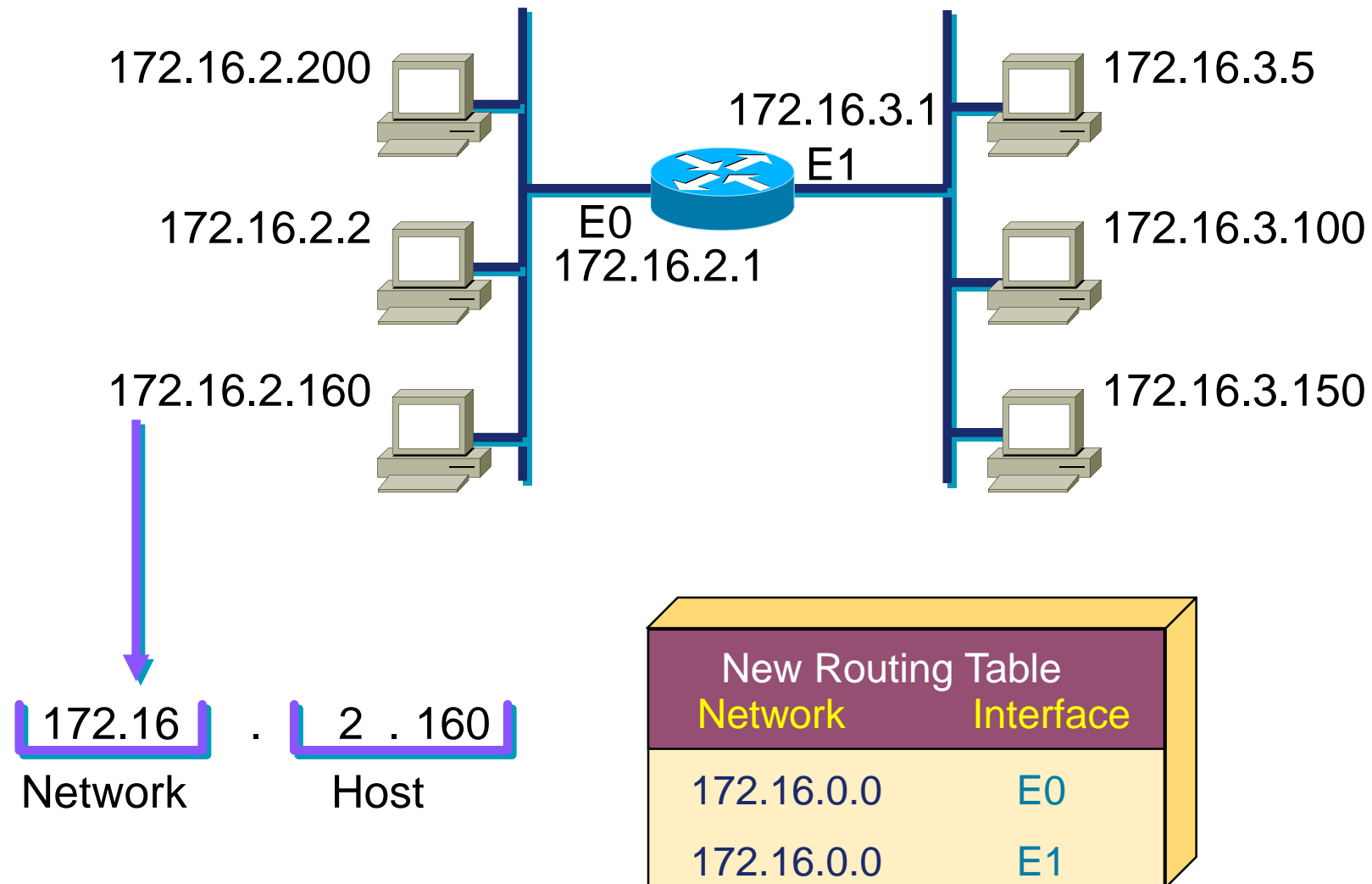
Recap



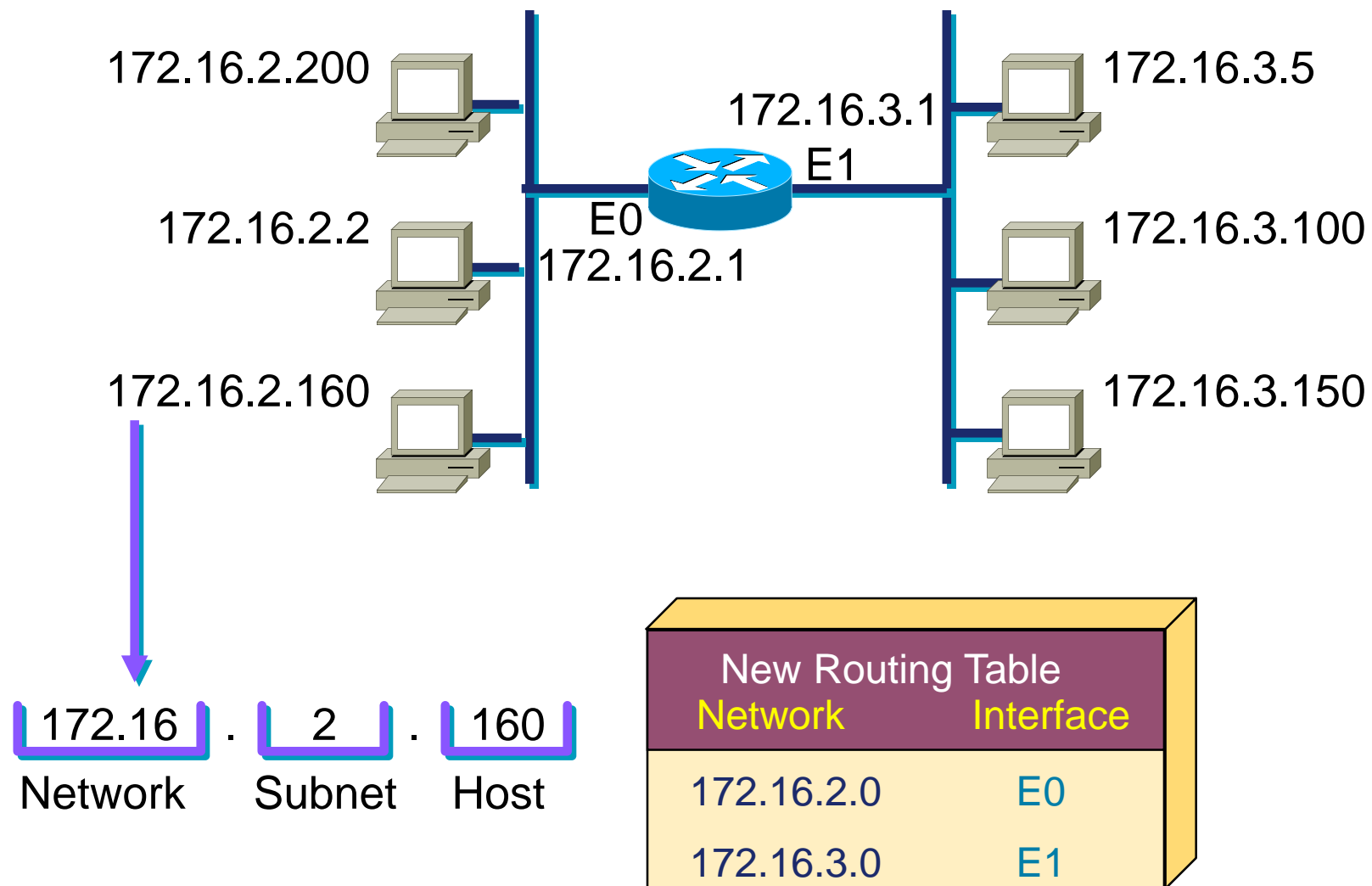
Network 172.16.0.0



Subnet Addressing

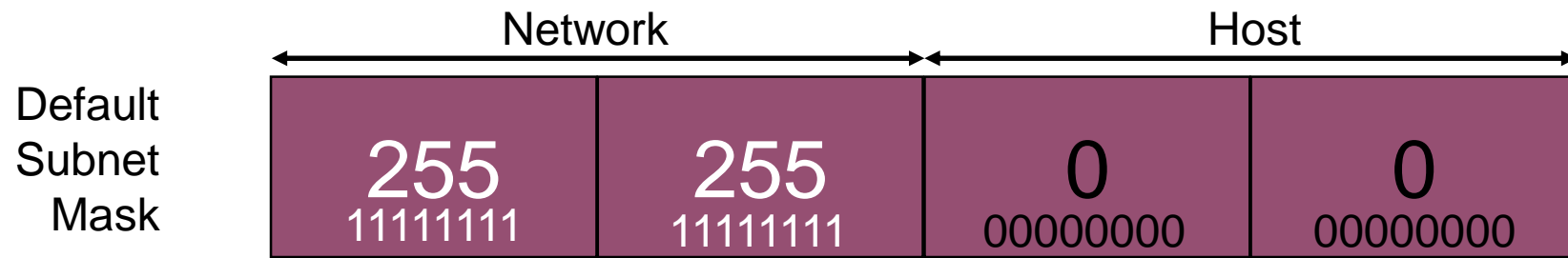
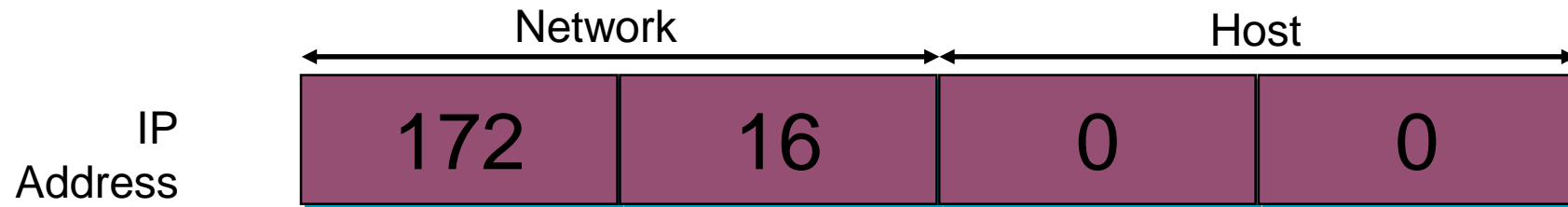


Subnet Addressing

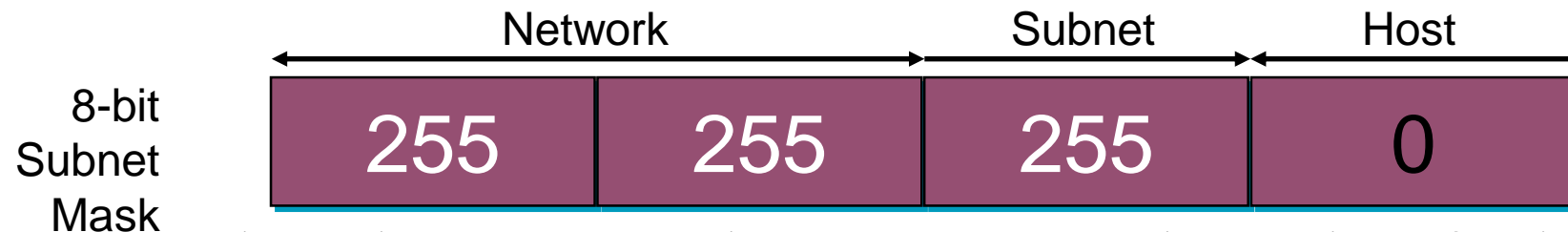




Subnet Mask



Also written as “/16” where 16 represents the number of 1s in the mask.



Also written as “/24” where 24 represents the number of 1s in the mask.



Subnet Mask without Subnets

	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

Subnets not in use—the default



Subnet Mask with Subnets

	Network		Subnet		Host
172.16.2.160	10101100	00010000	00000010		10100000
255.255.255.0	11111111	11111111	11111111		00000000
	10101100	00010000	00000010		00000000
			128 192 224 240 248 252 254 255		

Network
Number

172	16	2	0
-----	----	---	---

- Network number extended by eight bits



Subnet Mask with Subnets (cont.)

	Network		Subnet		Host
172.16.2.160	10101100	00010000	00000010		10100000
255.255.255.192	11111111	11111111	11111111		11000000
	10101100	00010000	00000010		10000000
			128 192 224 240 248 252 254 255		128 192 224 240 248 252 254 255
Network Number	172	16	2		128

- Network number extended by ten bits



Subnet Mask Exercise

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0		
10.6.24.20	255.255.240.0		
10.30.36.12	255.255.255.0		



Subnet Mask Exercise Answers

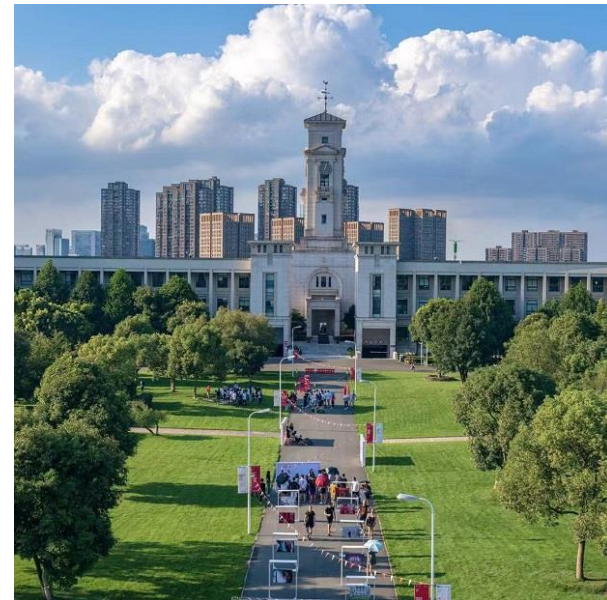
Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0	B	172.16.2.0
10.6.24.20	255.255.240.0	A	10.6.16.0
10.30.36.12	255.255.255.0	A	10.30.36.0



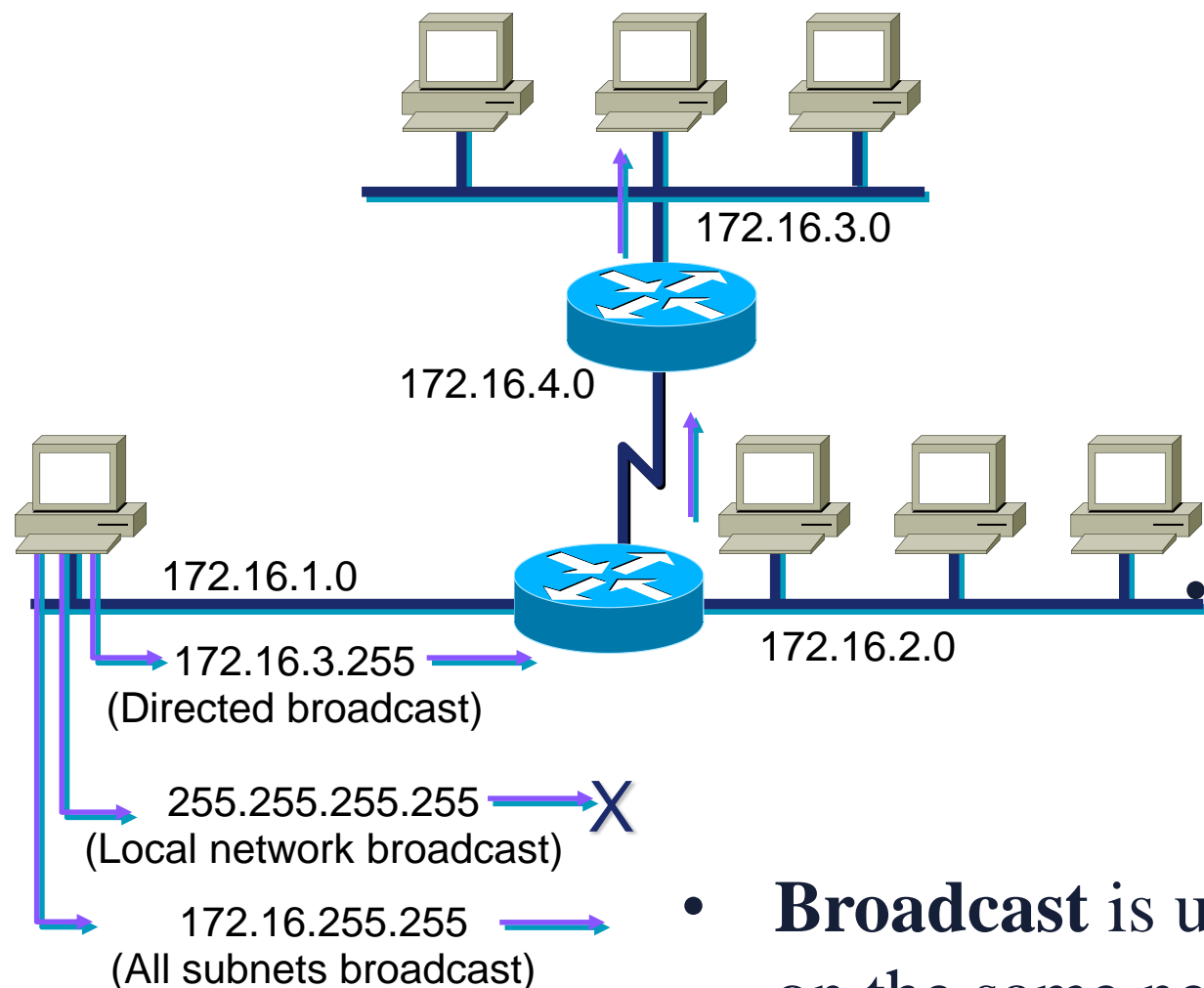
Overview

- Principles behind Internet Protocol
 - IP datagram header
 - Header format
- Binary Numbers
 - Quick Review
- Connectionless Networking
 - Design issues
- IP: Addressing
 - Addressing Types
 - IP Classes and Format
 - Subnetting
 - Supernetting
 - VLSM and CIDR
- Special IP Addressing
 - Broadcast
 - Localhost
 - Addressing Summary
- IPv6
 - Rules and Notations
 - IPv6 and Subnetting

**Any
question
in
previous
lecture?**



Broadcast Addresses



- **Multicast** transmits data to multiple receivers
 - online gaming
 - audio videos
- **Unicast** is used for one-to-one communication.

The **anycast** addressing method forwards messages to a single device of a *specific group of devices*.

- **Broadcast** is used to transmit data to all the devices on the same network, i.e., television networks



Special IPv4 Addresses

- There are certain addresses that cannot be assigned to hosts for various reasons
- There are also special addresses that can be assigned to hosts but with restrictions on how those hosts can interact within the network.

Loopback (27.0.0.0 to 127.255.255.255)

- The IPv4 loopback address 127.0.0.1
- The loopback is a special address that hosts use to direct traffic to themselves

Network and Broadcast Addresses

- Within each network the **first** and **last** addresses cannot be assigned to hosts
- These are the network address and the broadcast addresses.

Default Route

- The IPv4 default route as 0.0.0.0, which is used as a "catch all" route when a more specific route is not available
- The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.



Special IPv4 Addresses

Link-Local Addresses

- IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) are designated as link-local addresses
- These addresses can be automatically assigned to the local host by the OS in environments where no IP configuration is available
- These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from DHCP server.

TEST-NET Addresses

- The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) is set aside for teaching and learning purposes
- These addresses can be used in documentation and network examples.



Addressing Summary Example

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192					Mask
					Subnet
					Broadcast
					First
					Last



Addressing Summary Example

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet
					Broadcast
					First
					Last



Addressing Summary Example

	172	16	2	160	
					3
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet
					Broadcast
					First
					Last

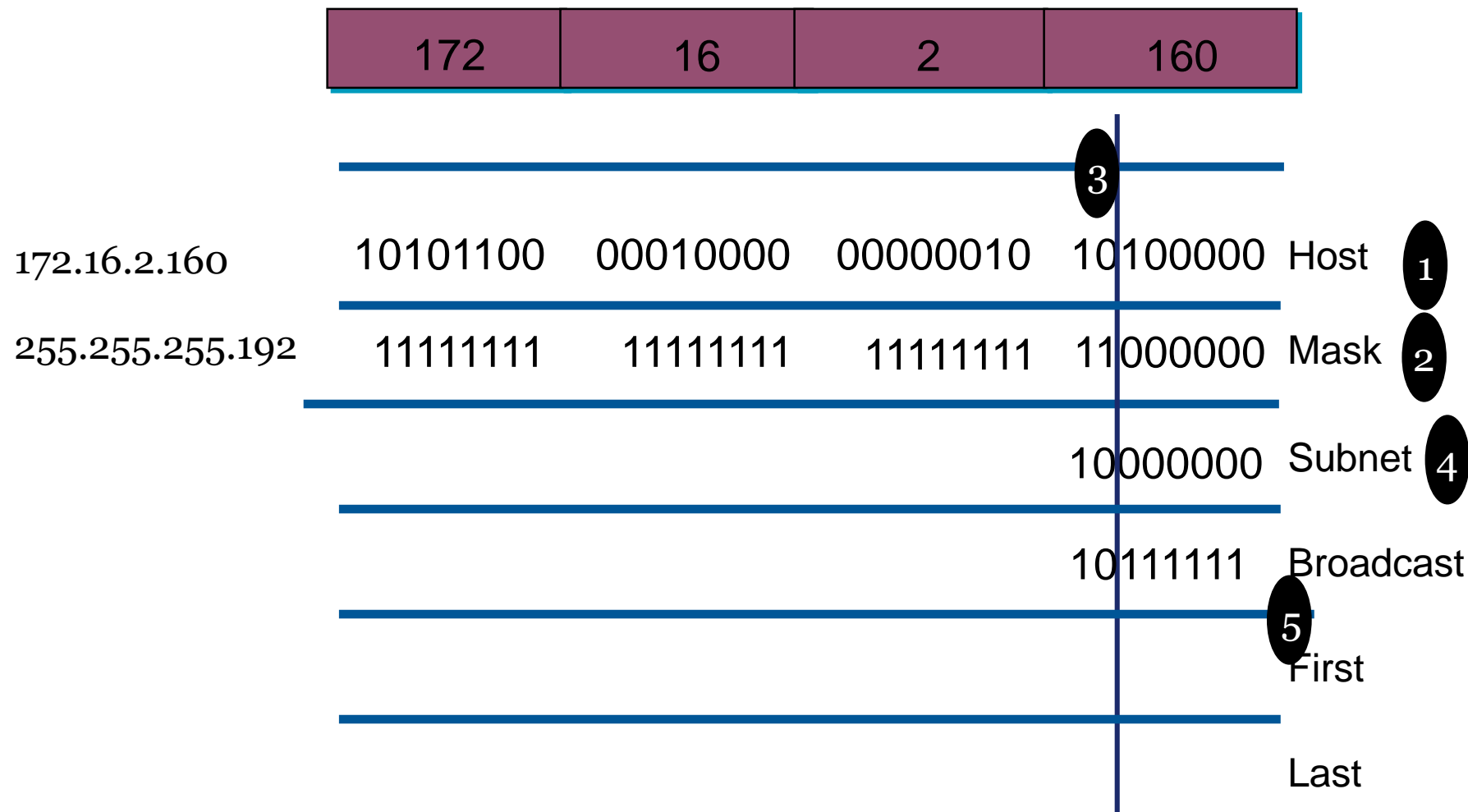


Addressing Summary Example

	172	16	2	160	
					3
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
				10000000	Subnet 4
					Broadcast
					First
					Last

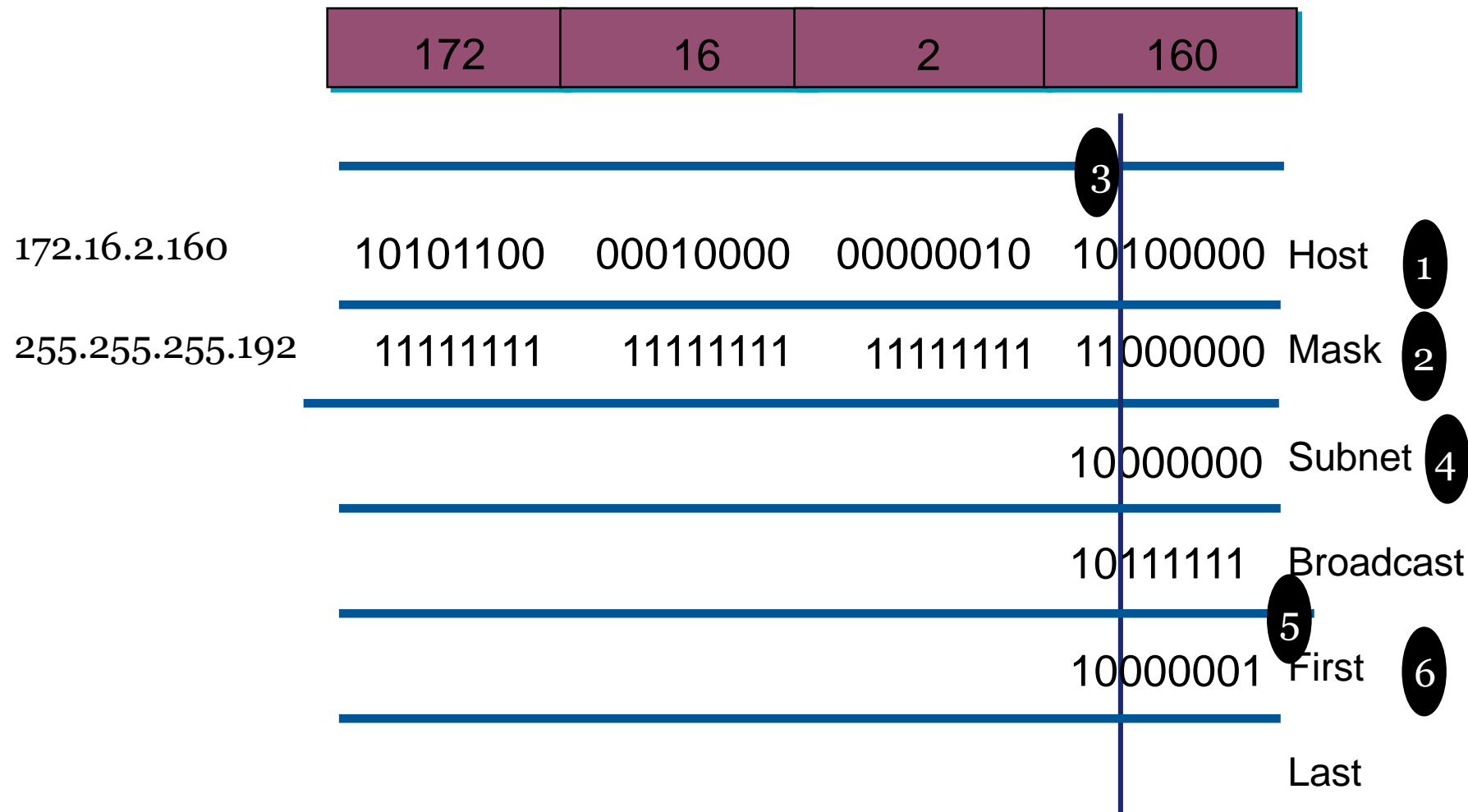


Addressing Summary Example

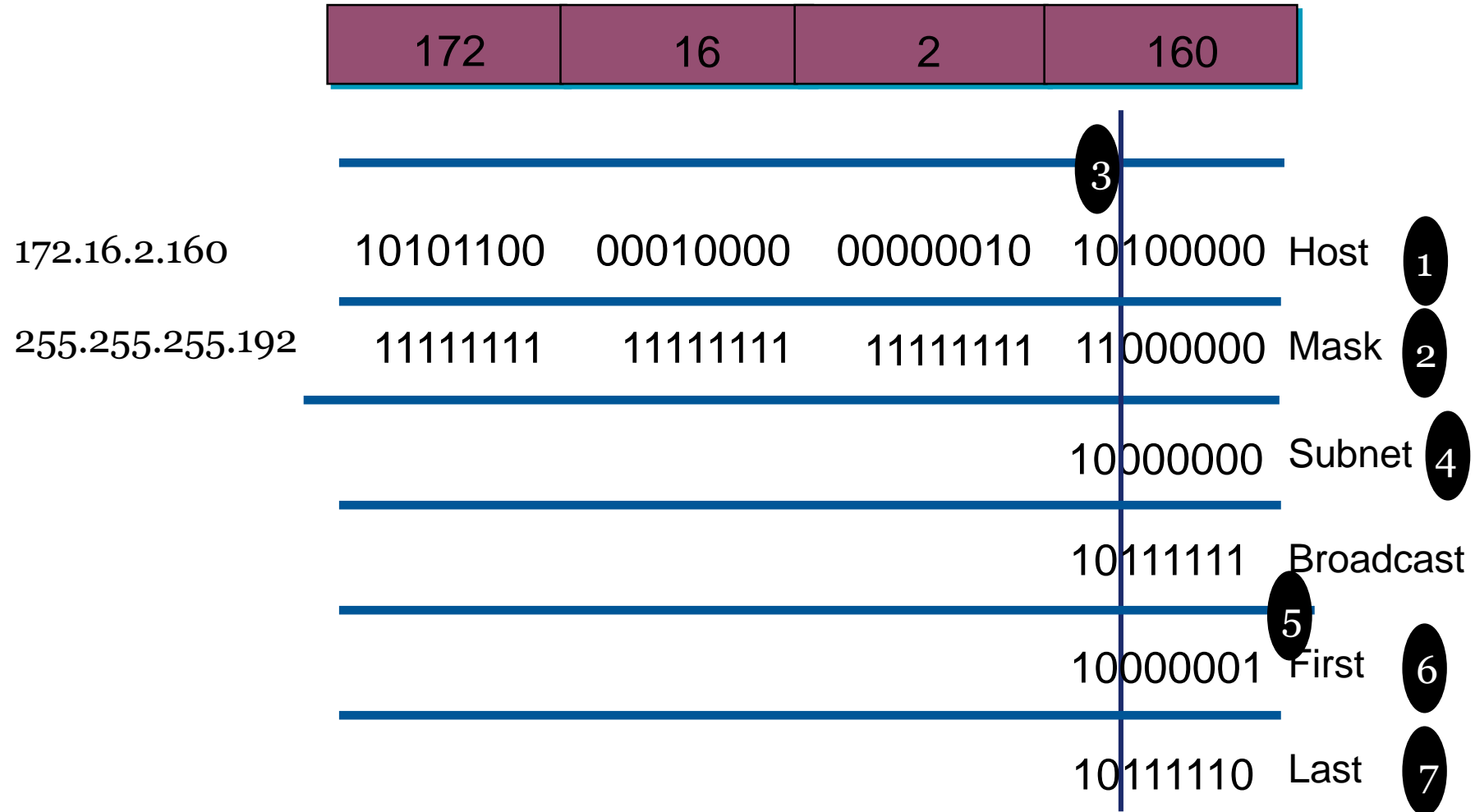




Addressing Summary Example



Addressing Summary Example



Addressing Summary Example

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
8						
	10101100	00010000	00000010	10000000	Subnet	4
	10101100	00010000	00000010	10111111	Broadcast	
					5	
	10101100	00010000	00000010	10000001	First	6
	10101100	00010000	00000010	10111110	Last	7

Addressing Summary Example

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
9 172.16.2.128	10101100	00010000	00000010	10000000	Subnet	4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast	
172.16.2.129	10101100	00010000	00000010	10000001	First	6
172.16.2.190	10101100	00010000	00000010	10111110	Last	7



Class B Subnet Example

IP Host Address: 172.16.2.121

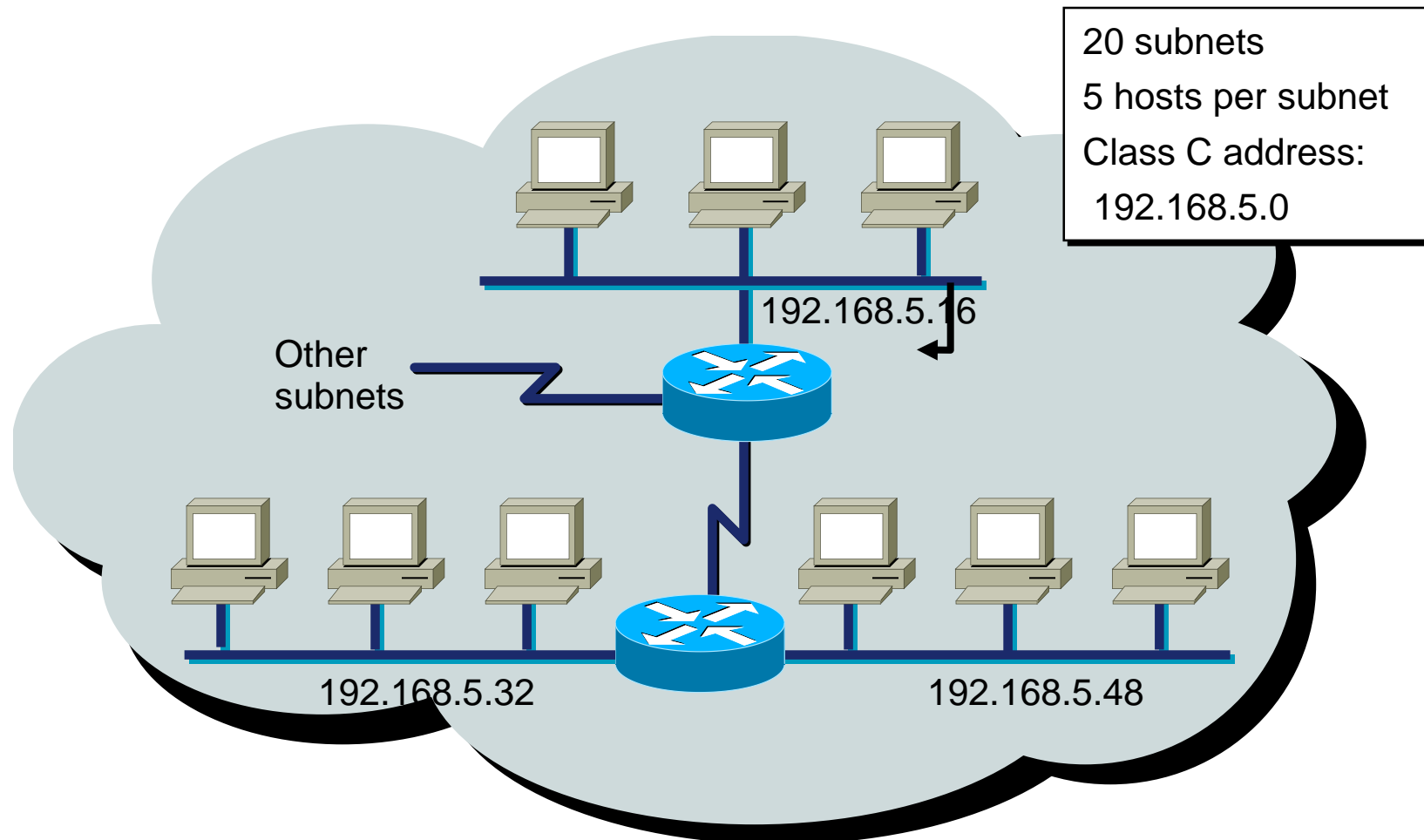
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subnet:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

- Subnet Address = 172.16.2.0
- Host Addresses = 172.16.2.1–172.16.2.254
- Broadcast Address = 172.16.2.255
- Eight bits of subnetting



Subnet Planning



Class C Subnet Planning Example

IP Host Address: 192.168.5.121

Subnet Mask: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111	001
255.255.255.248:	11111111	11111111	11111111	11111	000
Subnet:	11000000	10101000	00000101	01111	000
Broadcast:	11000000	10101000	00000101	01111	111

- Subnet Address = 192.168.5.120
- Host Addresses = 192.168.5.121–192.168.5.126
- Broadcast Address = 192.168.5.127
- Five Bits of Subnetting



Broadcast Addresses Exercise

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248			
15.16.193.6	255.255.248.0			
128.16.32.13	255.255.255.252			
153.50.6.27	255.255.255.128			



Broadcast Addresses Exercise Answers

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248	C	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	A	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	B	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	B	153.50.6.0	153.50.6.127



Manual IPv4 Address Configuration

- Manually enter IP address, subnet mask, default gateway and DNS servers.
- Use a GUI or command line.
- Not difficult, but it can be time consuming on a large network.
- Difficult to troubleshoot if information is entered incorrectly.



Dynamic Host Configuration Protocol

- Client computers are configured to Obtain an IP address automatically.
- DHCP Servers on the network contain a pool of addresses and other IPv4 configuration.
- Clients request configuration at boot up.
- DHCP Servers respond to the requests.
- IPv4 configurations are leased for a period of time and renewed as necessary.
- No addresses are duplicated.

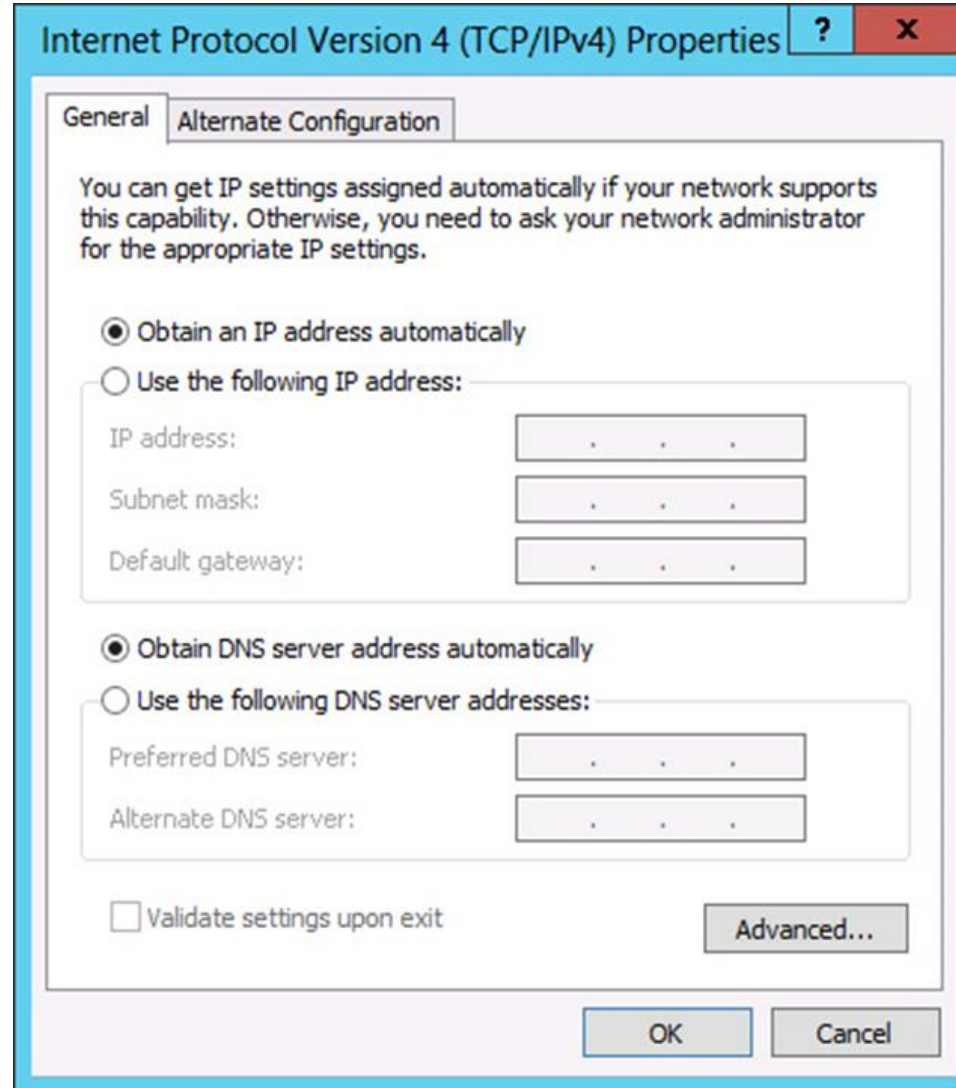


Assigning IPv4 Addresses

To assign IPv4 addresses, there are three basic methods:

- Manual configuration
- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)

Assigning IPv4 Addresses



Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel



Automatic Private IP Addressing (APIPA)

- A DHCP failover mechanism used by all current Microsoft Windows operating systems.
- If a system fails to locate a DHCP server on the network, APIPA takes over and automatically assigns an address on the 169.254.0.0/16 network to the computer.
- For a small network that consists of only a single LAN, APIPA is a simple and effective alternative to installing a DHCP server.



IPv6 Addressing

- **128 bits (or 16 bytes) long:** four times as long as its predecessor.
- 2^{128} : about 340 billion billion billion billion different addresses
- **Colon hexadecimal notation:**
 - addresses are written using 32 hexadecimal digits.
 - digits are arranged into 8 groups of four to improve the readability.
 - Groups are separated by colons

2001:0718:1c01:0016:020d:56ff:fe77:52a3

- Note:
 - DNS plays an important role in the IPv6 world
 - (manual typing of IPv6 addresses is not an easy thing,
 - Some **zero suppression rules** are allowed to lighten this task at least a little.

IPv6 Address Notation: Example

128.91.45.157.220.40.0.0.0.0.252.87.212.200.31.255

Binary

```
1000000001011011001011011001110111011100001010000000000000000000
0000000000000000001111110001010111110101001100100000011111111111
```

Dotted
Decimal

128	91	45	157	220	40	0	0	0	0	252	87	212	200	31	255
-----	----	----	-----	-----	----	---	---	---	---	-----	----	-----	-----	----	-----

Hexadecimal

0	32		64		96		128	
805B	2D9D	DC28	0000	0000	FC57	D4C8	1FFF	
805B	2D9D	DC28	0	0	FC57	D4C8	1FFF	
805B	2D9D	DC28	::		FC57	D4C8	1FFF	
805B	2D9D	DC28	::		FC57	212	200	31 255



Rule 1- IPv6 Zero Suppression

- Some types of addresses contain long sequences of zeros.
- To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in the colon hexadecimal format can be compressed to “::”, **known as *double-colon***.
- For example:
 - **link-local address**
 - FE80:0:0:0:2AA:FF:FE9A:4CA2 → FE80::2AA:FF:FE9A:4CA2.
 - **multicast address**
 - FF02:0:0:0:0:0:0:2 → FF02::2
 - **loopback address**
 - 0:0:0:0:0:0:0:1 → ::1



Rule 1- IPv6 Zero Suppression

- Zero compression can only be used to compress a single contiguous series of 16-bit blocks expressed in colon hexadecimal notation.
- You cannot use zero compression to include part of a 16-bit block.
- For example,
 - cannot express FF02:30:0:0:0:0:0:5 as FF02:3::5
 - correct representation = FF02:30::5
- Leading zeroes in every group can be omitted.

2001:718:1c01:16:20d:56ff:fe77:52a3



Rule 1- IPv6 Zero Suppression

- **To determine the number of 0 bits represented by the “::”**
 1. count the number of blocks in the compressed address
 2. (-) subtract this number from 8
 3. (*) multiply the result by 16.
- **For example**
 1. FF02::2
 2. two blocks - “FF02” block and “2” block.
 3. The number of bits expressed by the “::” is 96 ($96 = (8 - 2) \times 16$).
- **Zero compression can only be used once in a given address.**
 - Otherwise, you could not determine the number of 0 bits represented by each instance of “::”.

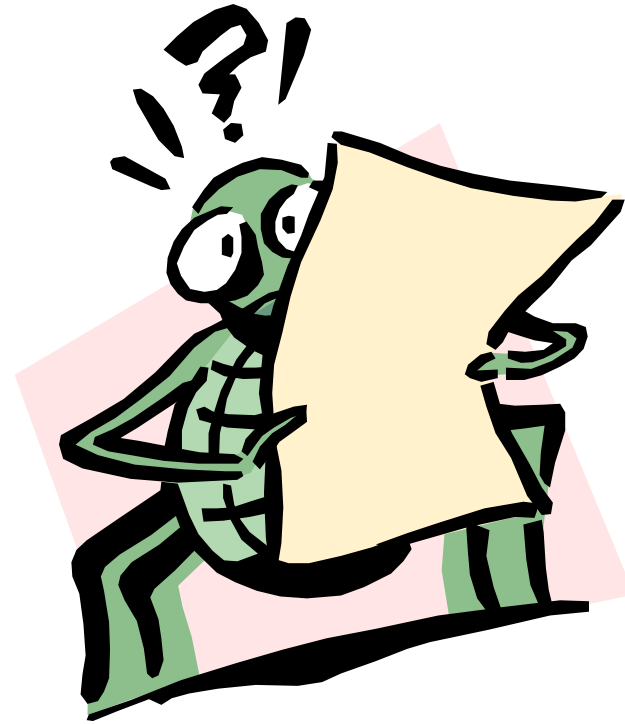
- The prefix is the part of the address that indicates the bits that have fixed values or are the bits of the subnet prefix.
- Prefixes for IPv6 subnets, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4.
- An IPv6 prefix is written in *address/prefix-length* notation.
 - For example, **21DA:D3::/48** and **21DA:D3:0:2F3B::/64** are IPv6 address prefixes.
- **Note** IPv4 implementations commonly use a dotted decimal representation of the network prefix known as the subnet mask.
- A subnet mask is not used for IPv6. Only the prefix length notation is supported.



Special IPv6 Addresses

- The following are special IPv6 addresses:
- **Unspecified address**
 - unspecified address (0:0:0:0:0:0:0:0 or ::) is only used to indicate the absence of an address.
 - equivalent to the IPv4 unspecified address of 0.0.0.0.
 - used as a source address for packets attempting to verify the uniqueness of a tentative address.
 - never assigned to an interface or used as a destination address.
- **Loopback address**
 - The loopback address (0:0:0:0:0:0:0:1 or ::1) is used to identify a loopback interface, enabling a node to send packets to itself.
 - It is equivalent to the IPv4 loopback address of 127.0.0.1.
 - Packets addressed to the loopback address must never be sent on a link or forwarded by an IPv6 router.

- How many IPv6 addresses can a host have?





IPv6 Addresses for a Host

- An IPv4 host with a single network adapter typically has a single IPv4 address assigned to that adapter.
- An IPv6 host, however, usually has multiple IPv6 addresses - even with a single interface.
- An IPv6 host is assigned the following unicast addresses:
 1. A link-local address for each interface
 2. Unicast addresses for each interface (which could be a site-local address and one or multiple global unicast addresses)
 3. The loopback address (::1) for the loopback interface



IPv6 Addresses for a Host

- Typical IPv6 hosts are **logically multihomed** because they have at least two addresses with which they can receive packets
 1. a link-local address for local link traffic
 2. a routable site-local or global address.
- Additionally, each host is **listening for traffic** on the following multicast addresses:
 1. The interface-local scope all-nodes multicast address (FF01::1)
 2. The link-local scope all-nodes multicast address (FF02::1)
 3. The solicited-node address for each unicast address on each interface
 4. The multicast addresses of joined groups on each interface



IPv6 and Subnetting

- The only acceptable form to represent a network mask in IPv6 is CIDR notation.
- Although IPv6 addresses are in hexadecimal format, the network mask value is still a decimal value.

IPv6 Prefix	Description
2001:410:0:1:0:0:0:45FF/128	Represents a subnet with only one IPv6 address.
2001:410:0:1::/64	Network prefix 2001:410:0:1::/64 can handle 2^{64} nodes. This is the default prefix length for a subnet.
2001:410:0::/48	Network prefix 2001:410:0::/48 can handle 2^{16} network prefixes of 64-bit. This is the default prefix length for a site.



University of
Nottingham
UK | CHINA | MALAYSIA



Thanks