CHAPTER 2

NETWORK FUNDAMENTALS

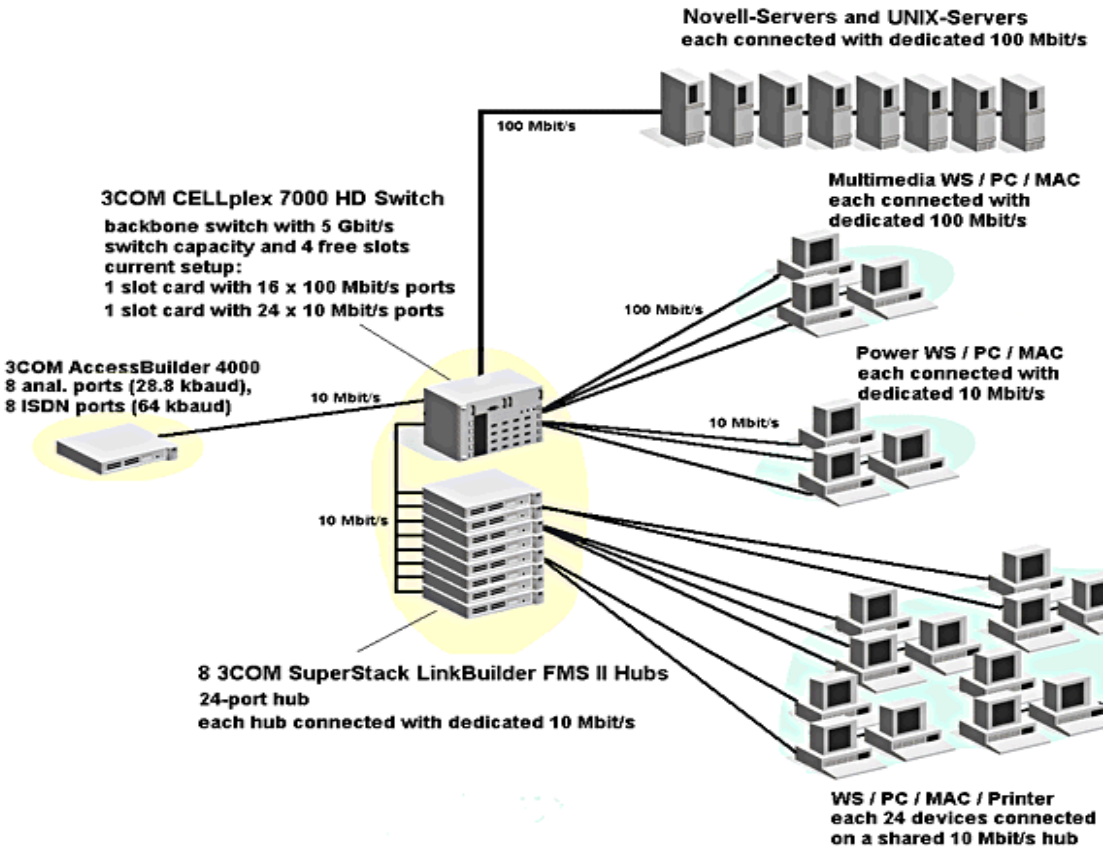
Outline

- Protocols and protocol layering (TCP/ IP)
- Frame, IP Packet, TCP and UDP segment
- Network devices
- IP addressing (Subnetting and Suppernetting)
- Address resolution protocol (ARP)
- ICMP
- VLAN
- Routing
- Routing protocols

What is Computer Network?

Network Fundamentals

The term *network* describes two or more connected computers that can share resources such as data, a printer, an Internet connection, applications, or a combination of these.



Network Protocols

- In order for data packets to travel from a source to a destination on a network, it is important that all the devices on the network speak the same language. This language is called protocol.
- A data communications protocol is a set of rules or an agreement that determines the data format and how transmission of data occurs.
- A protocol is a set of rules that make communication on a network more efficient.

Layered Models

- A reference model (Layered Model) is a conceptual blueprint of how communications should take place.
- It addresses all the processes required for effective communication and divides these processes into logical groupings called layers.
- When a communication system is designed in this manner, it is known as layered architecture.

Advantage of Layered Models

- It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
- It allows multiple-vendor development through standardization of network components.
- It encourages industry standardization by defining what functions occur at each layer of the model.
- It allows various types of network hardware and software to communicate.

Types of Layered Models

- OSI Layered Model
- TCP/IP Layered Model

The TCP/IP Model

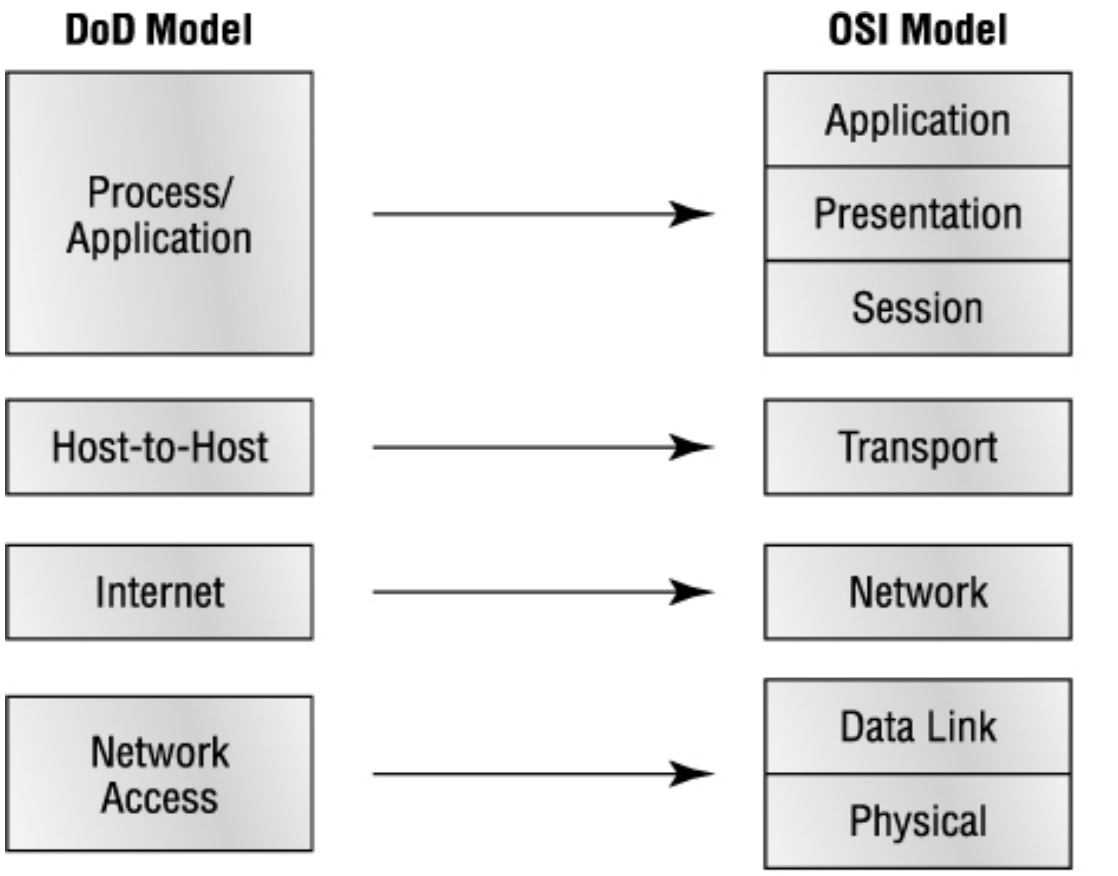
- The U.S. Department of Defense (DoD) created the TCP/IP reference model, because it wanted to design a network that could survive any conditions, including a nuclear war.

- In a world connected by different types of communication media such as copper wires, microwaves, optical fibers and satellite links, the DoD wanted transmission of packets every time and under any conditions.
- This very difficult design problem brought about the creation of the TCP/IP model.

The TCP/IP Model

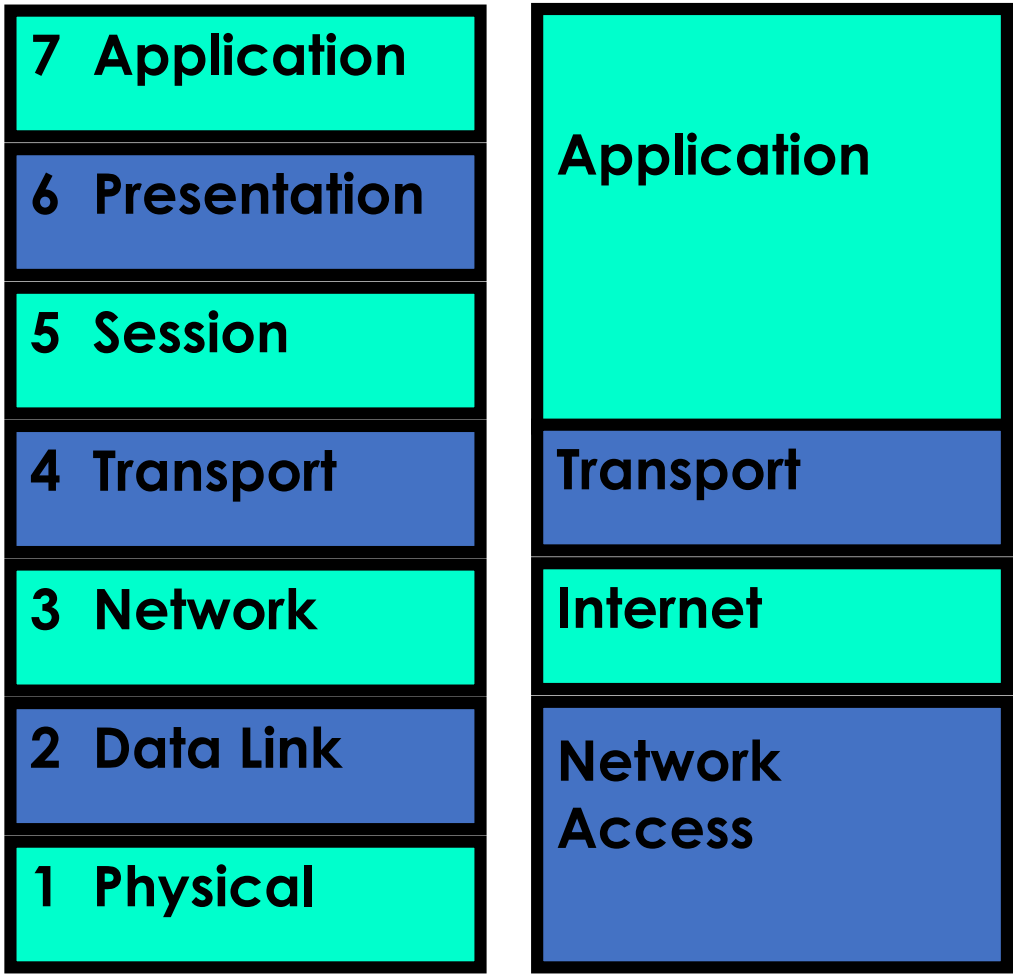
- The DoD model is basically a condensed version of the OSI model
- It's composed of four, instead of seven, layers:
    - Application layer
    - Transport layer
    - Internet layer
    - Network Access layer

Two Models



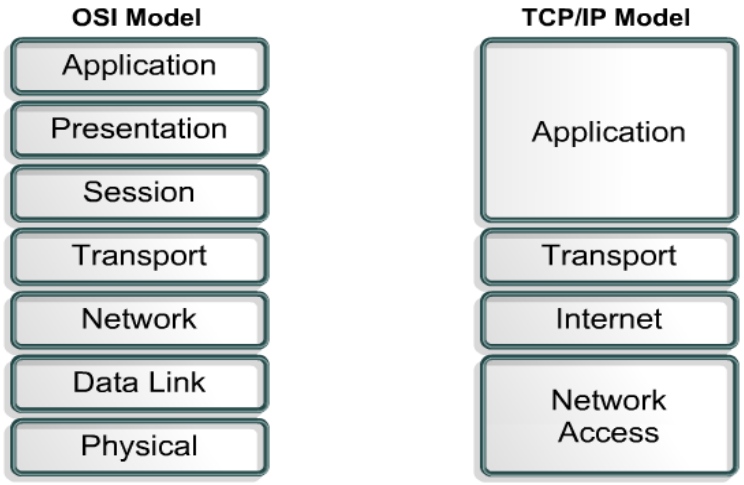
lammle.com

Two Models: Side-By-Side



Comparing TCP/IP with OSI

FIGURES
1
2
3
4



and packet switching occur at this layer.

The relationship between IP and TCP is an important one. IP can be thought to point the way for the packets, while TCP provides a reliable transport.

The name of the network access layer is very broad and somewhat confusing. It is also known as the host-to-network layer. This layer is concerned with all of the components, both physical and logical, that are required to make a physical link. It includes the networking technology details, including all the details in the OSI physical and data link layers.

Figure 2 illustrates some of the common protocols specified by the TCP/IP reference model layers. Some of the most commonly used application layer protocols include the following:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)
- Trivial File Transfer Protocol (TFTP)

The common transport layer protocols include:

- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)

The primary protocol of the Internet layer is:

- Internet Protocol (IP)

TCP/IP vs OSI

Similarities include:

- Both have layers.
- Both have application layers, though they include very different services.
- Both have comparable transport and network layers.
- Both models need to be known by networking professionals.
- Both assume packets are switched.

TCP/IP vs OSI

Differences include:

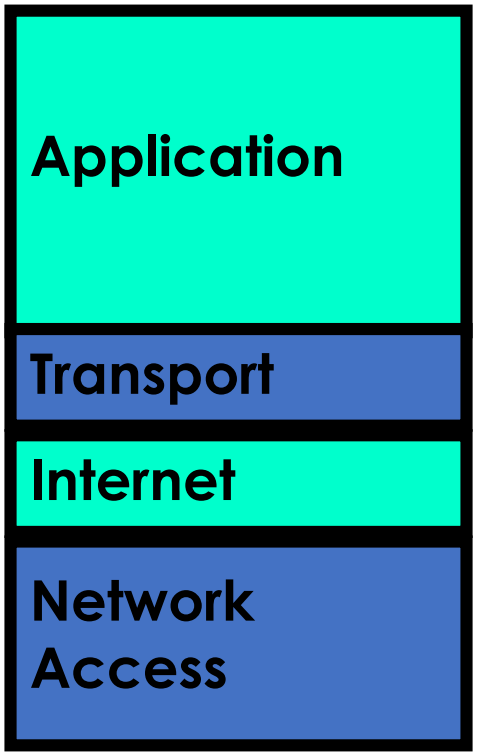
- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears simpler because it has fewer layers.
- TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols.

TCP/IP vs OSI

Although TCP/IP protocols are the standards with which the Internet has grown, the OSI model is useful for the following reasons:

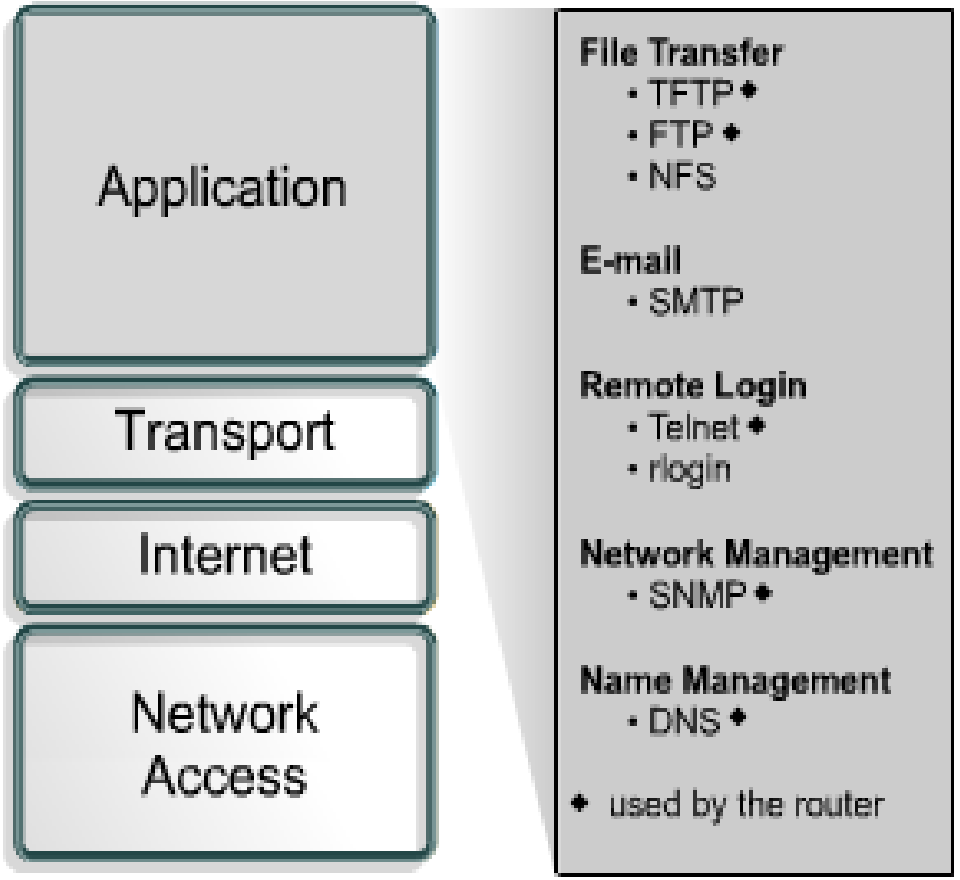
- It is a generic standard.
- It has more details, which make it more helpful for teaching and learning.
- It has more details, which can be helpful when troubleshooting.
- Networking professionals differ in their opinions on which model to use. Due to the nature of the industry it is necessary to become familiar with both.

TCP/IP Model



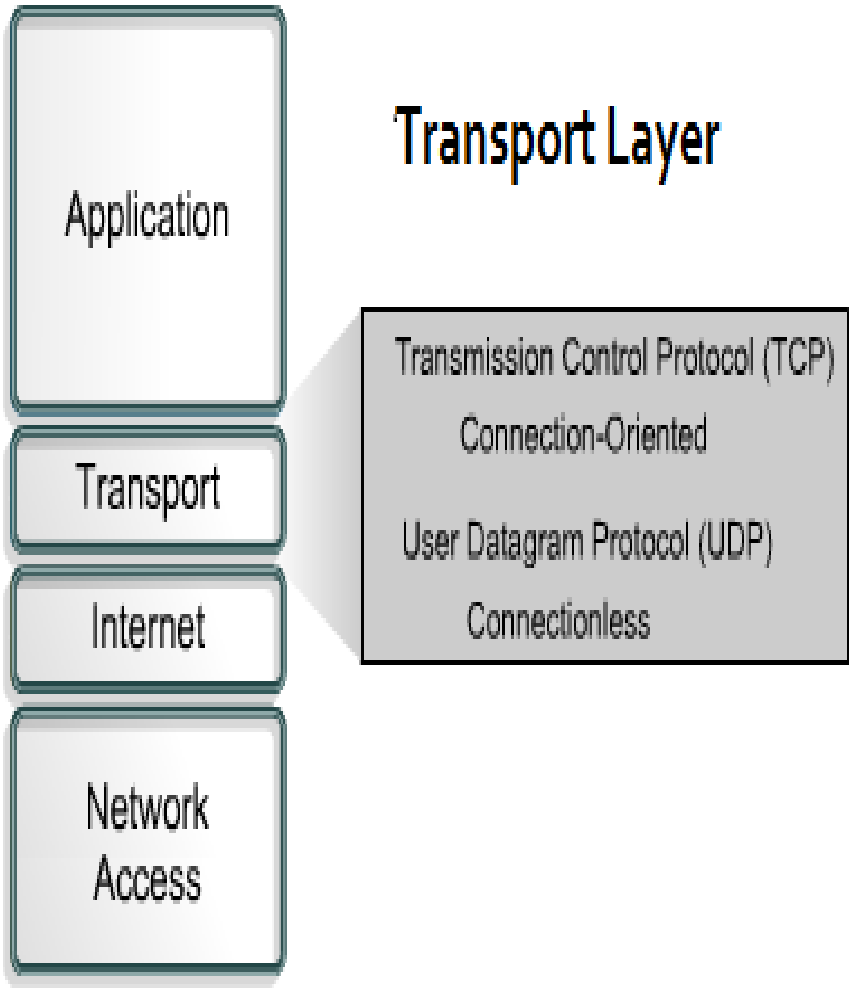
The Application Layer

The application layer of the TCP/IP model handles high-level protocols, issues of representation, encoding, and dialog control.



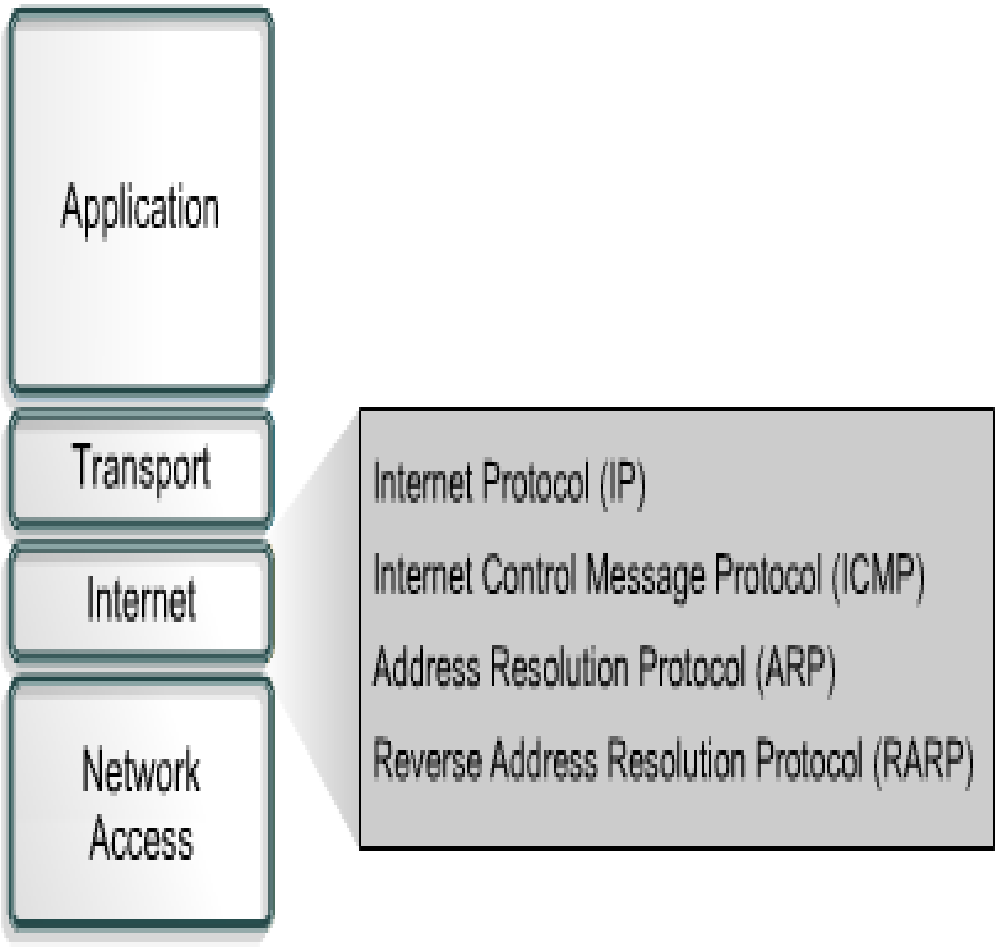
The Transport Layer

The transport layer provides transport services from the source host to the destination host. It constitutes a logical connection between these endpoints of the network. Transport protocols segment and reassemble upper-layer applications into the same data stream between endpoints.
The transport layer data stream provides end-to-end transport services.



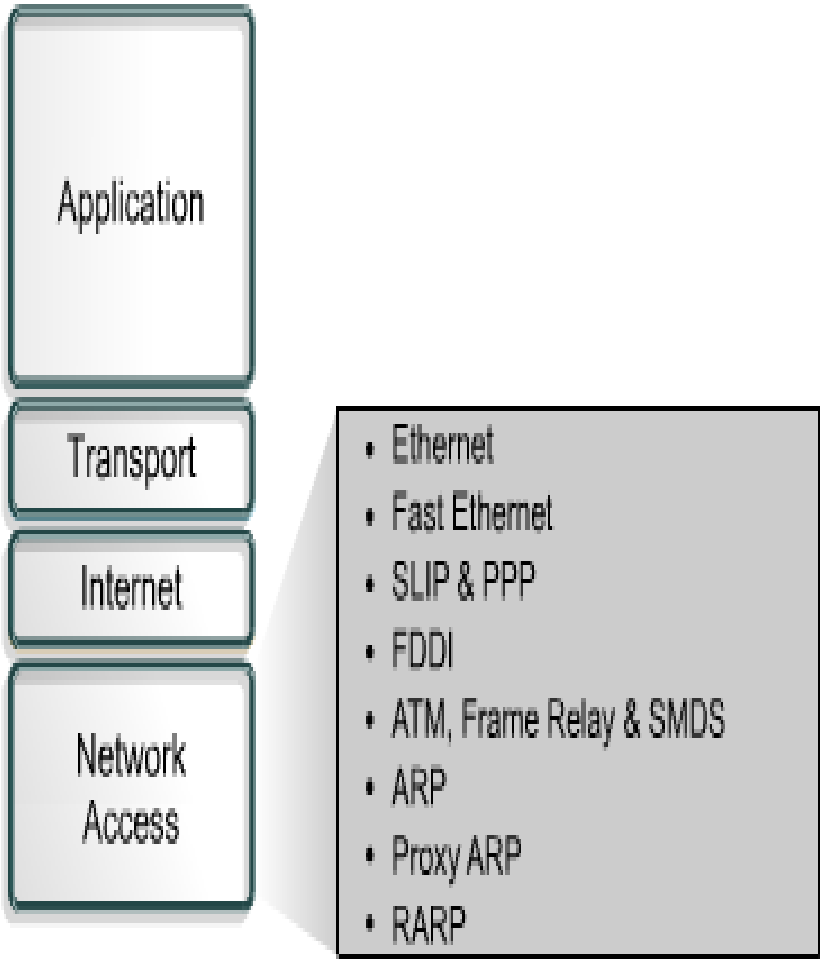
The Internet Layer

The purpose of the Internet layer is to select the best path through the network for packets to travel. The main protocol that functions at this layer is the Internet Protocol (IP). Best path determination and packet switching occur at this layer.



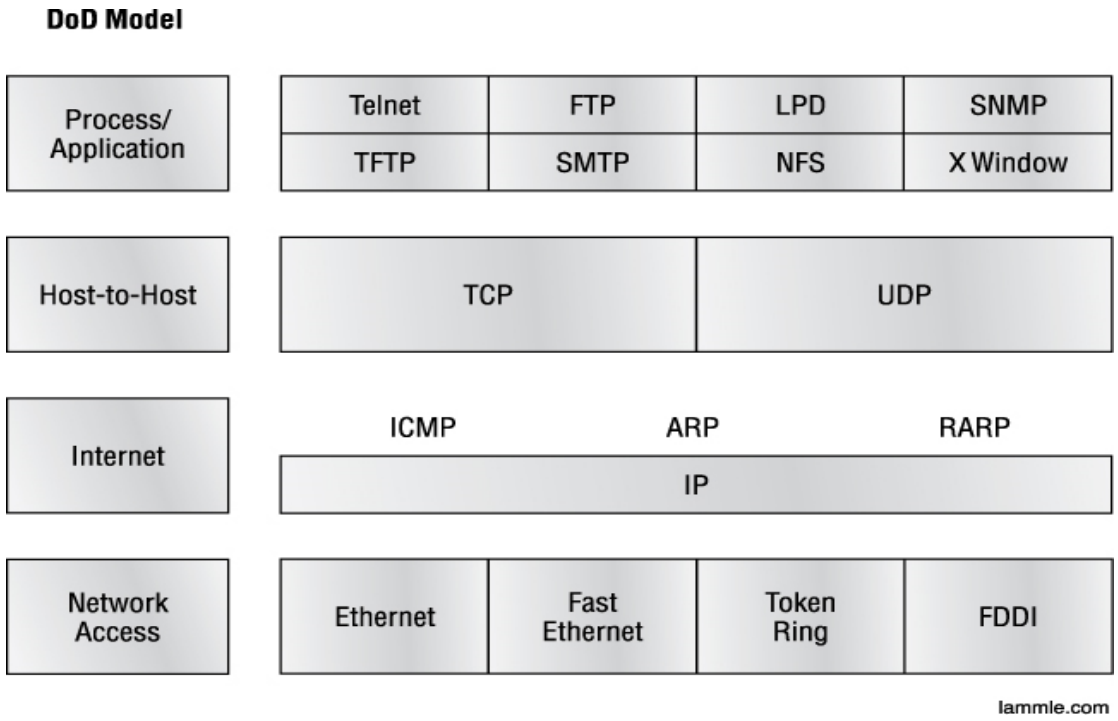
The Network Access Layer

The network access layer is also called the host-to-network layer. It is the layer that is concerned with all of the issues that an IP packet requires to actually make a physical link to the network media. It includes LAN and WAN details, and all the details contained in the OSI physical and data-link layers. NOTE: ARP & RARP work at both the Internet and Network Access Layers.



The TCP/IP Protocol Suite

The DoD and OSI models are alike in design and concept and have similar functions in similar layers.



The TCP/IP Protocol

- Internet Protocols are most popular open system protocol suite
- Internet Protocols are used for LAN and WAN communications.
- The two best known Internet Protocols are
  - Transmission Control Protocol (TCP)
  - Internet Protocol (IP)

The TCP/IP Protocol

- Protocols are rules for communication on a network or between two hosts
- The Transmission Control Protocol/Internet Protocol is a protocol stack, or grouping of many related protocols, each working together within a prescribed standard.
- TCP/IP is the most popular model for connection to the Internet and within most networks

Transmission Control Protocol(TCP)

Features

- Connection establishment
- Transport layer protocol
- Error checking of data
- Guaranteed packet delivery
- Breaks data into pieces at transmitter and reassembles at receiver
- Only handled by the sender and receiver

Internet Protocol (IP)

Features

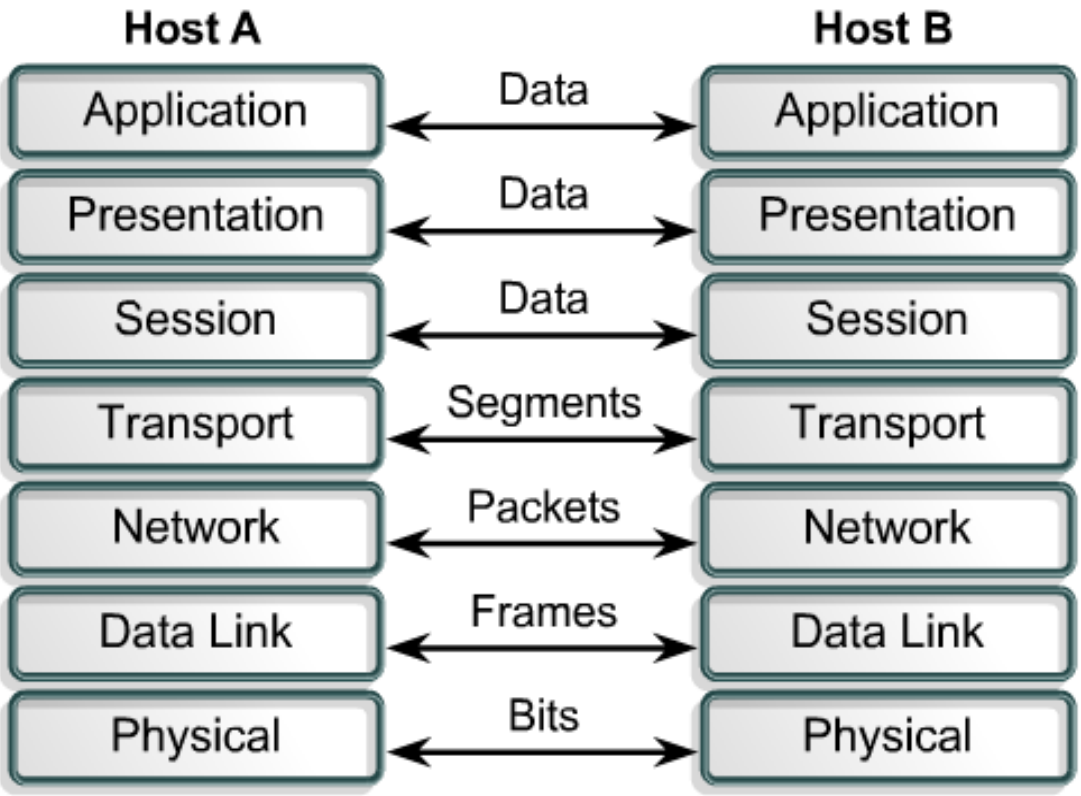
- Network layer protocol
- Provides addressing of sender and receiver on the internet
- Protocol defines how to route messages through a network
- Packetized
- Not continuous
- Delivery not guaranteed
- Dealt with at every router on the way from sender to receiver

TCP/IP Protocols Suite

- **FTP** - File Transport Protocol at the application layer.
- **Telnet** - Remote session at the application layer.
- **SMTP** - Simple Mail Transport Protocol at the application layer.
- **DHCP** - Dynamic host configuration protocol is used to assign IP addresses dynamically to network cards. It works at the application layer.
- **TCP** - Transport Control protocol is a connection oriented reliable protocol working at the transport layer.
- **UDP** - User Datagram Protocol is a connection less unreliable protocol working at the transport layer.
- **ICMP** - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer.
- **IGMP** - Internet Group Management Protocol is used to manage multicast groups and it works at the transport layer.
- **IP** - Internet Protocol is used for software addressing of computers and works at the network layer.
- **ARP** - Address Resolution Protocol is used to resolve the hardware address of a card to package the Ethernet data. It works at the network layer.
- **RARP** - Reverse Address Resolution Protocol used for disk less computers to determine their IP address using the network. It works at the network layer.

Bits, Frame, IP Packet, TCP Segment, UDP Segment

Reading Assignment



Networking Devices

- NIC
- Repeater
- Hub
- Bridge
- Switch
- Router
- Brouter
- Others?-Explore!

Network Interface Card (NIC)

At source:

- Receives the data packet from the Network Layer
- Attaches its MAC address to the data packet
- Attaches the MAC address of the destination device to the data packet
- Converts data in to packets suitable for the particular network (Ethernet, Token Ring, FDDI)
- Converts packets in to electrical, light or radio signals
- Provides the physical connection to the media

NIC…

As a destination device

- Provides the physical connection to the media
- Translates the signal in to data
- Reads the MAC address to see if it matches its own address
- If it does match, passes the data to the Network Layer

Repeater

- Allows the connection of segments
- Extends the network beyond the maximum length of a single segment
- Functions at the Physical Layer of the OSI model
- A multi-port repeater is known as a Hub
- Connects segments of the same network, even if they use different media
- Has three basic functions
  - Receives a signal which it cleans up
  - Re-times the signal to avoid collisions
  - Transmits the signal on to the next segment

Advantages and disadvantages

Repeater

- Advantages – Can connect different types of media, can extend a network in terms of distance, does not increase network traffic
- Disadvantages – Extends the collision domain, can not connect different network architectures, limited number only can be used in network

Hub

- A central point of a star topology
- Allows the multiple connection of devices
- Can be more than a basic Hub – providing additional services (Managed Hubs, Switched Hubs, Intelligent Hubs)
- In reality a Hub is a Repeater with multiple ports
- Functions in a similar manner to a Repeater
- Works at the Physical Layer of the OSI model
- Passes data no matter which device it's addressed to; and this feature adds to congestion

Advantages and…

Hub

- Advantages – Cheap, can connect different media types
- Disadvantages – Extends the collision domain, can not filter information, passes packets to all connected segments

Bridge

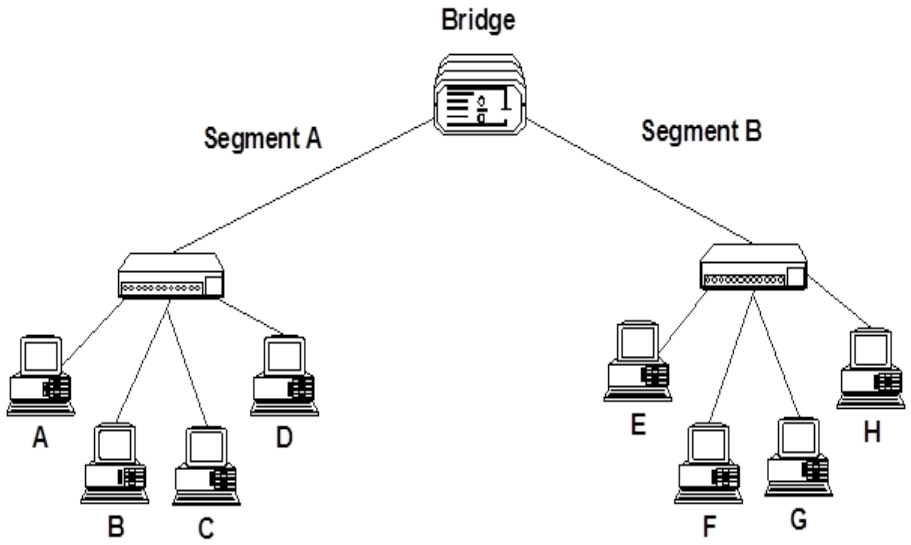
- Like a Repeater or Hub it connects segments
- Works at Data Layer – not Physical
- Uses Mac address to make decisions
- Acts as a ’filter’, by determining whether or not to forward a packet on to another segment

Bridge…

- Builds a Bridging Table, keeps track of devices on each segment
- Filters packets, does not forward them, by examining their MAC address
- It forwards packets whose destination address is on a different segment from its own
- It divides a network in to multiple collision domains – so reducing the number of collisions

Bridge..

- **Uses the Spanning Tree Protocol (STP) – to decide whether to pass a packet on to a different network segment**



A Transmits to C, bridge **will not** pass it to Segment B

G Transmits to B, bridge **will** pass it to Segment A

Advantages and…

Bridge

- Advantages – Limits the collision domain, can extend network distances, uses MAC address to filter traffic, eases congestion, can connect different types of media, some can connect differing architectures
- Disadvantages – more expensive than a repeater, slower than a repeater – due to additional processing of packets

Switch

- A multiport Bridge, functioning at the Data Link Layer
- Each port of the bridge decides whether to forward data packets to the attached network
- Keeps track of the Mac addresses of all attached devices (just like a bridge)
- Similarly priced to Hubs – making them popular
- Acts like a Hub, but filters like a Bridge
- Each port on a Switch is a collision domain

Advantages and…

Switch

- Advantages - Limits the collision domain, can provide bridging, can be configured to limit broadcast domain
- Disadvantages – More expensive than a hub or bridge, configuration of additional functions can be very complex

Router

- Works at Network Layer in an intelligent manner
- Can connect different network segments, if they are in the same building or even on the opposite side of the globe
- Works in LAN, MAN and WAN environments
- Allows access to resources by selecting the best path
- Can interconnect different networks – Ethernet with Token Ring
- Changes packet size and format to match the requirements of the destination network

Router…

- Two primary functions – to determine the ‘best path’ and to share details of routes with other routers
- Routing Table – a database which keeps track of the routes to networks and the associated costs
- Static Routing – routes are manually configured by a network administrator
- Dynamic Routing – adjust automatically to changes in network topology, and information it receives from other routers
- Routing Protocol – uses a special algorithm to route data across a network eg RIP

Advantages and…

Router

- Advantages – Limits the collision domain, can function in LAN or WAN, connects differing media and architectures, can determine best path/route, can filter broadcasts
- Disadvantages – Expensive, must use routable protocols, can be difficult to configure (static routing), slower than a bridge

Brouter

- Functions both as Bridge and a Router – hence name
- Can work on networks using different protocols
- Can be programmed only to pass data packets using a specific protocol forward to a segment – in this case it is functioning in a similar manner to a Bridge
- If a Brouter is set to route data packets to the appropriate network with a routed protocol such as IP, it is functioning as a Router

Gateways

- Allow different networks to communicate by offering a translation service from one protocol stack to another
- They work at all levels of the OSI model – due to the type of translation service they are providing
- Address Gateway – connects networks using the same protocol, but using different directory spaces such as Message Handling Service
- Protocol Gateway – connects network using different protocols. Translates source protocol so destination can understand it
- Application Gateway – translates between applications such as from an Internet email server to a messaging server

IP ADDRESSING

What is an IP Address?

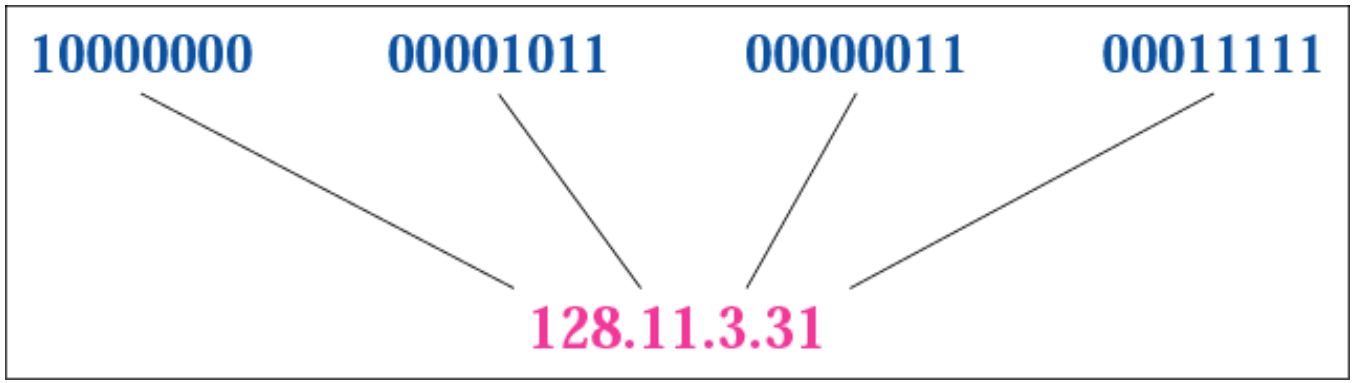
- An IP address (IPV4) is a 32-bit address.
- The IP addresses are unique
- Each device on a network is assigned an IP address.
- Each IP address has two fundamental parts:
  - The *network* portion, which describes the physical wire the device is attached to.
  - The *host* portion, which identifies the host on that wire.

What is an IP Address?

- The address space in a protocol that uses N-bits to define an Address is 2^n
- The address space of IPv4 is

$$2^{32} \text{ or } 4{,}294{,}967{,}296.$$

Binary Notation



Dotted-decimal notation

Change the following IP address from binary notation to dotted-decimal notation.

10000001 00001011 00001011 11101111

129.11.11.239

Find the error in the following IP address

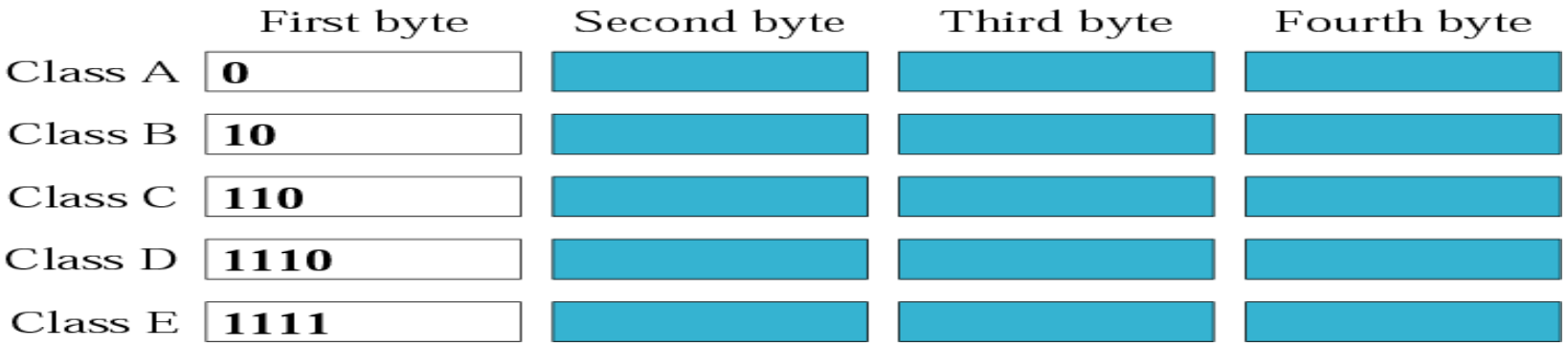
111.56.045.78

There are no leading zeroes in Dotted-decimal notation (045)

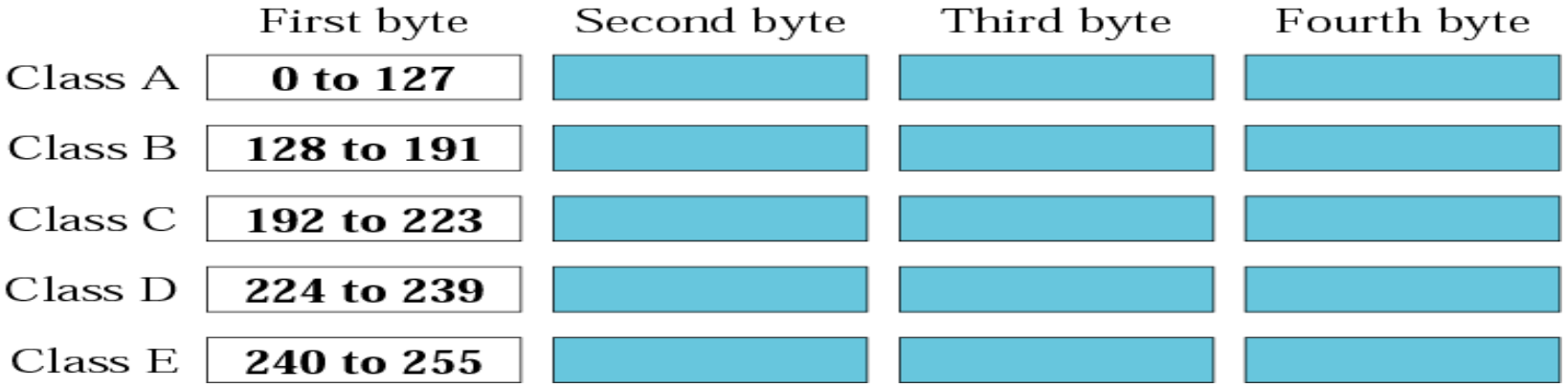
75.45.301.14

- In decimal notation each number <= 255
- 301 is out of the range

Finding the class in Binary notation



Finding the class in decimal notation



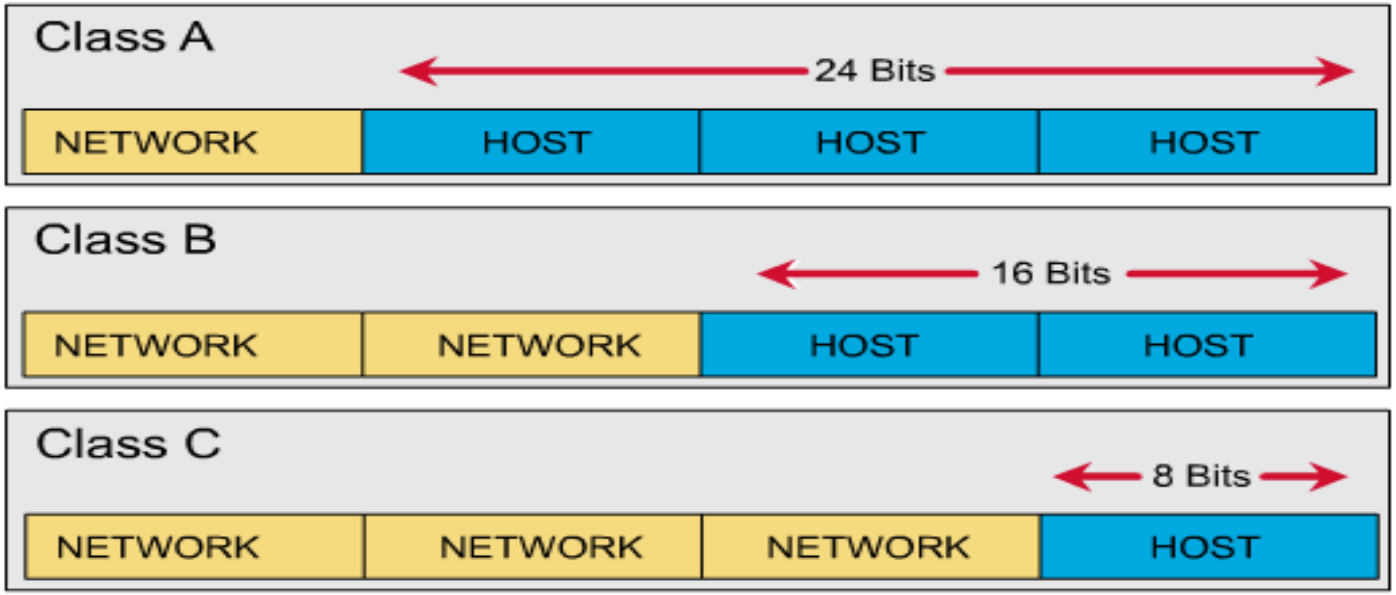
- Show that Class A *has*

$$2^{31} = 2{,}147{,}483{,}648 \text{ addresses}$$

- Show that Class B *has*

- Show that Class C *has*

Hosts for Classes of IP Addresses

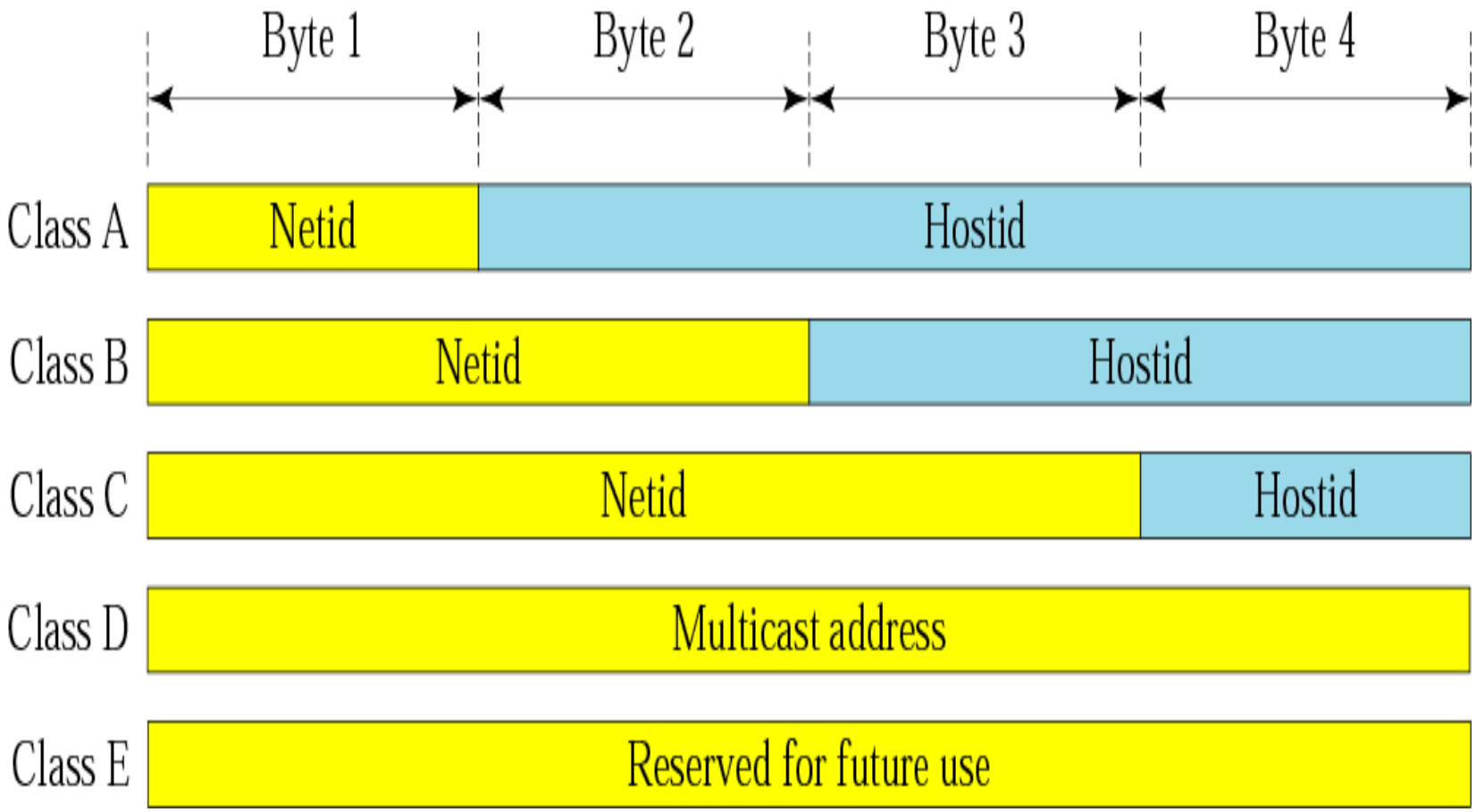


Class A (24 bits for hosts) $2^{24} - 2^{*}$ = 16,777,214 maximum hosts

Class B (16 bits for hosts) $2^{16} - 2^{*}$ = 65,534 maximum hosts

Class C (8 bits for hosts) $2^{8} - 2^{*}$ = 254 maximum hosts

Network id and Host id

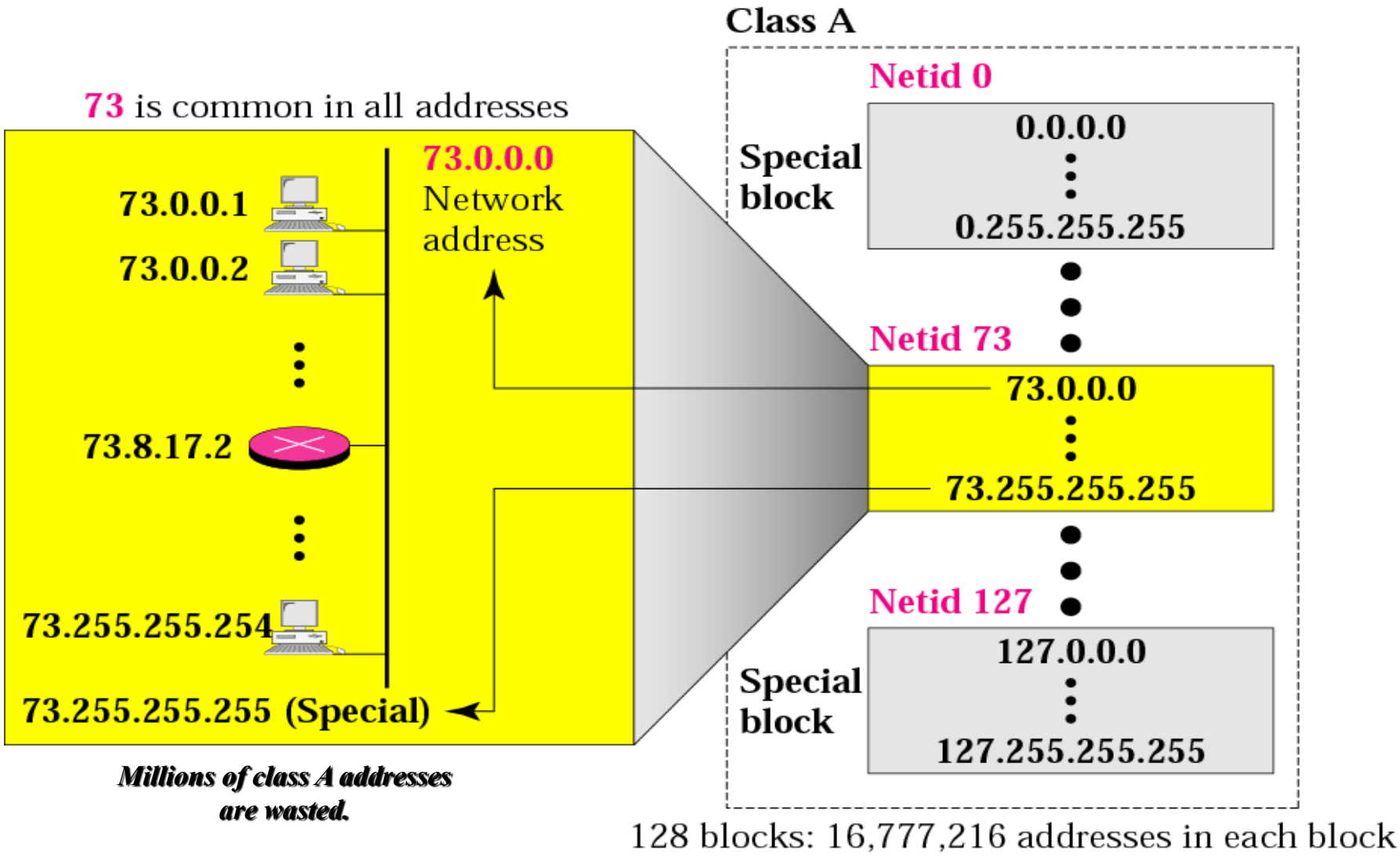


IP Addresses as Decimal Numbers

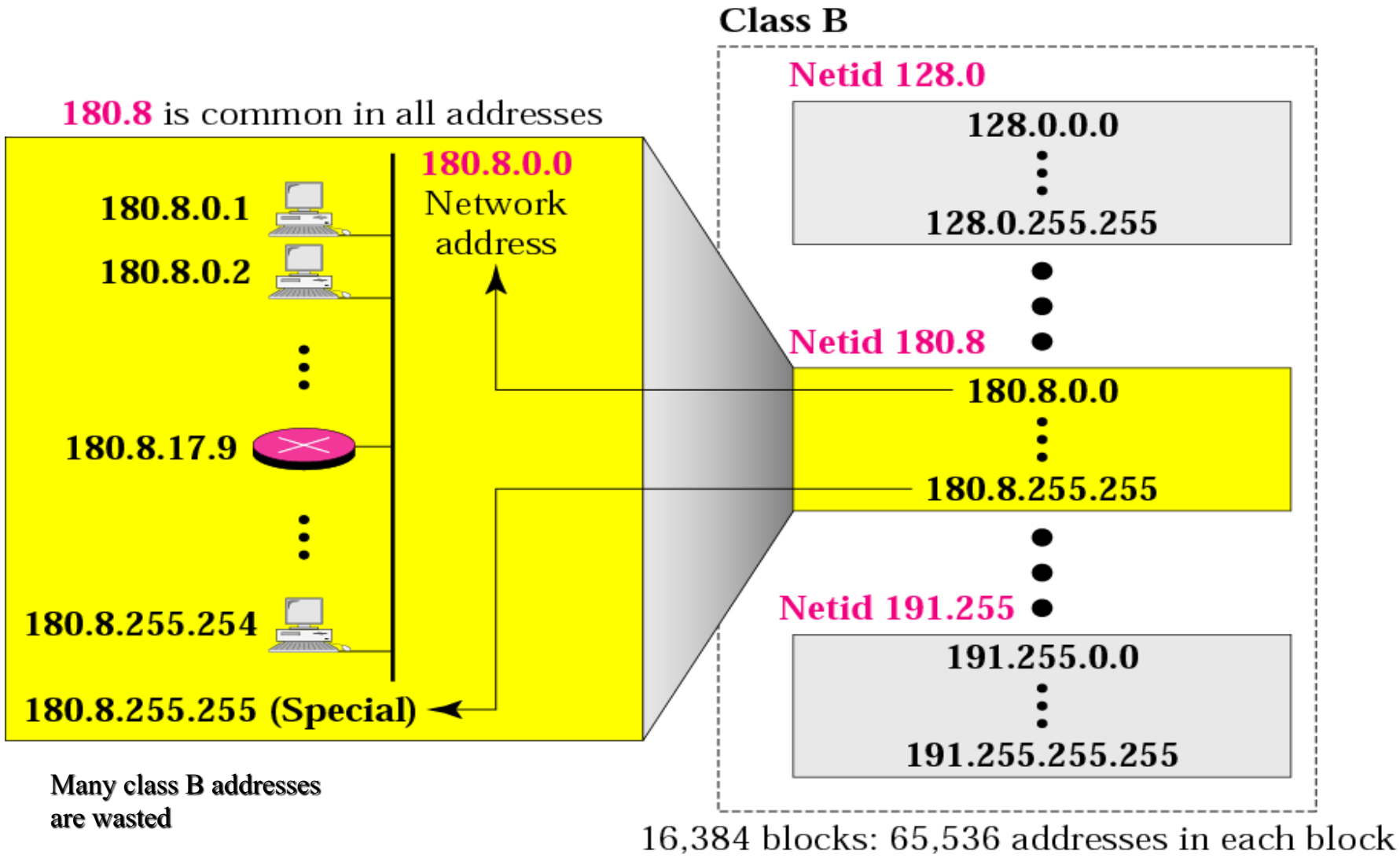
Class	Starts with	Binary range	Decimal Value range	Maximum subnets	Maximum hosts	Routing mask
A	0	00000000-01111111	0-127*	127	16,777,214	255.0.0.0
B	10	10000000-10111111	128-191	16,384	65,534	255.255.0.0
C	110	11000000-11011111	192-223	2,097,152	254	255.255.255.0
D	1110	11100000-11101111	224-239			
E	1111	11110000-11111111	240-255			

* The 0 octet is forbidden in the RFC, and 127 is reserved for loopback testing.

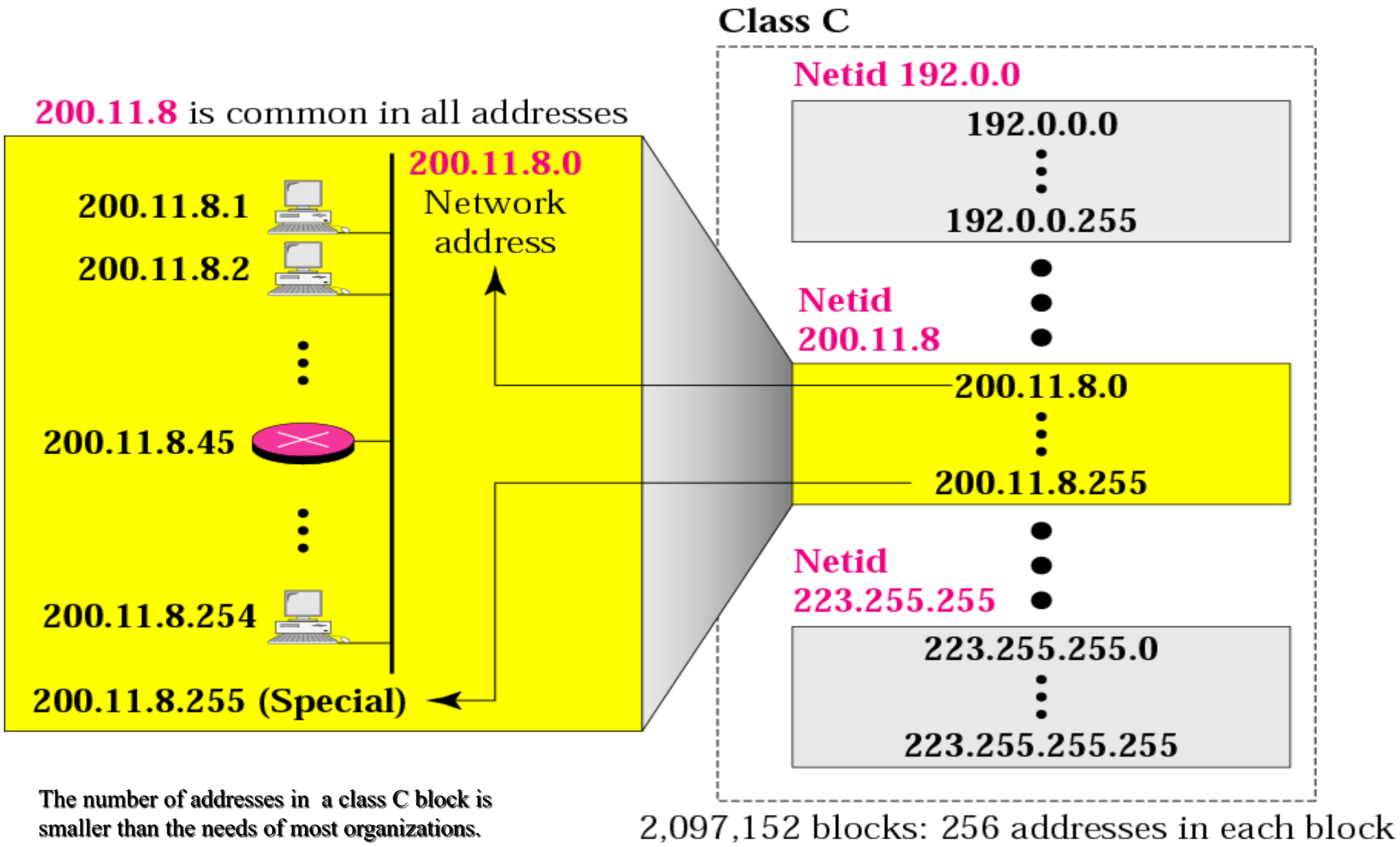
Blocks in class A



Blocks in class B



Blocks in class C



The number of addresses in a class C block is smaller than the needs of most organizations.

Class D and C

- Class D addresses are used for multicasting
  - There is only one block in this class

- Class E addresses are reserved for special purposes such as research and most of the block is wasted.

PRIVATE and SPECIAL IP Address Ranges

Class A: 10.0.0.0—10.255.255.255

Class B: 172.16.0.0—172.31.255.255

Class C: 192.168.0.0—192.168.255.255

- Private addresses created by RFC 1918 are to be used for addressing internal networks.
- These IP addresses are not routable

Network Addresses

- In classful addressing, the network address (the first address in the block) is the one that is assigned to the organization.
- The network address defines the network to the rest of the Internet.
- Given the network address, we can find the class of the address, the block, and the range of the addresses in the block
- It retains the netid of the block and sets the hostid to zero.

Ex. Given the network address 132.21.0.0, find

the class

the block

the range of the addresses

- The 1st byte is between 128 and 191. Hence, Class B
- The block has a netid of 132.21.
- The addresses range from 132.21.0.0 to 132.21.255.255.

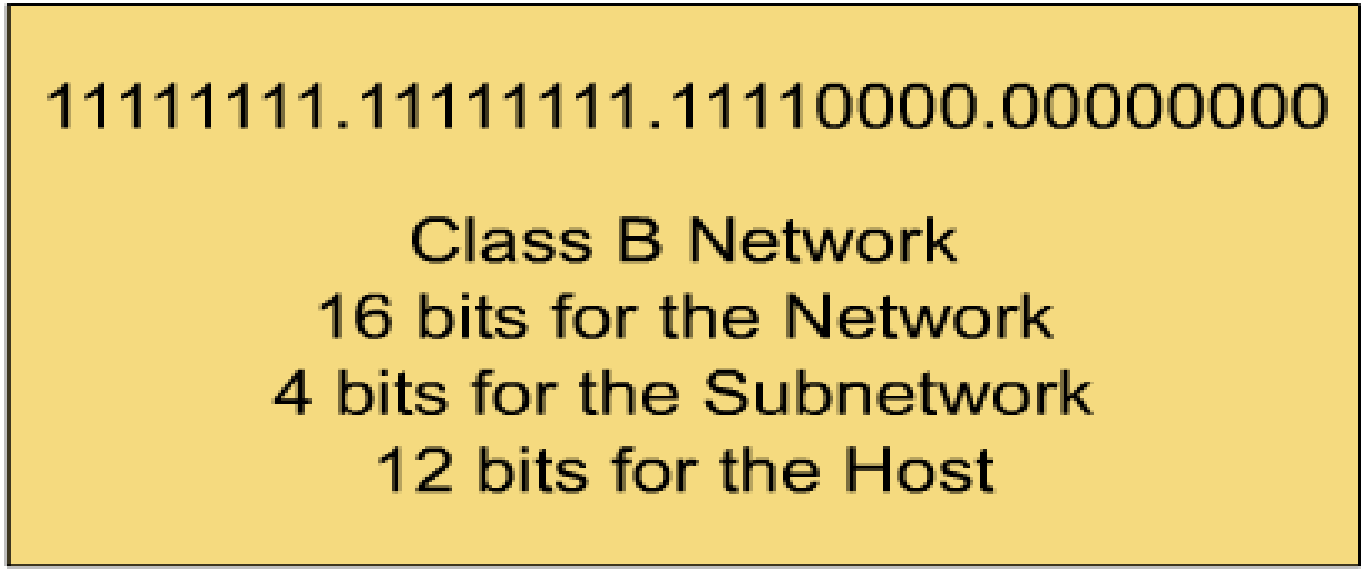
Default Mask

- The subnet masks for various IP address classes have certain default values.
- The actual subnet mask can be derived from these values.
- The default subnet masks for various address classes are:
  - Class A default mask is 255.0.0.0
  - Class B default mask is 255.255.0.0
  - Class C Default mask 255.255.255.0

Subnet Mask

- It determines which part of an IP address is the network field and which part is the host field
- Follow these steps to determine the subnet mask:
  1. Express the subnetwork IP address in binary form.
  2. Replace the network and subnet portion of the address with all 1s.
  3. Replace the host portion of the address with all 0s.
  4. Convert the binary expression back to dotted-decimal notation.

Subnet Mask



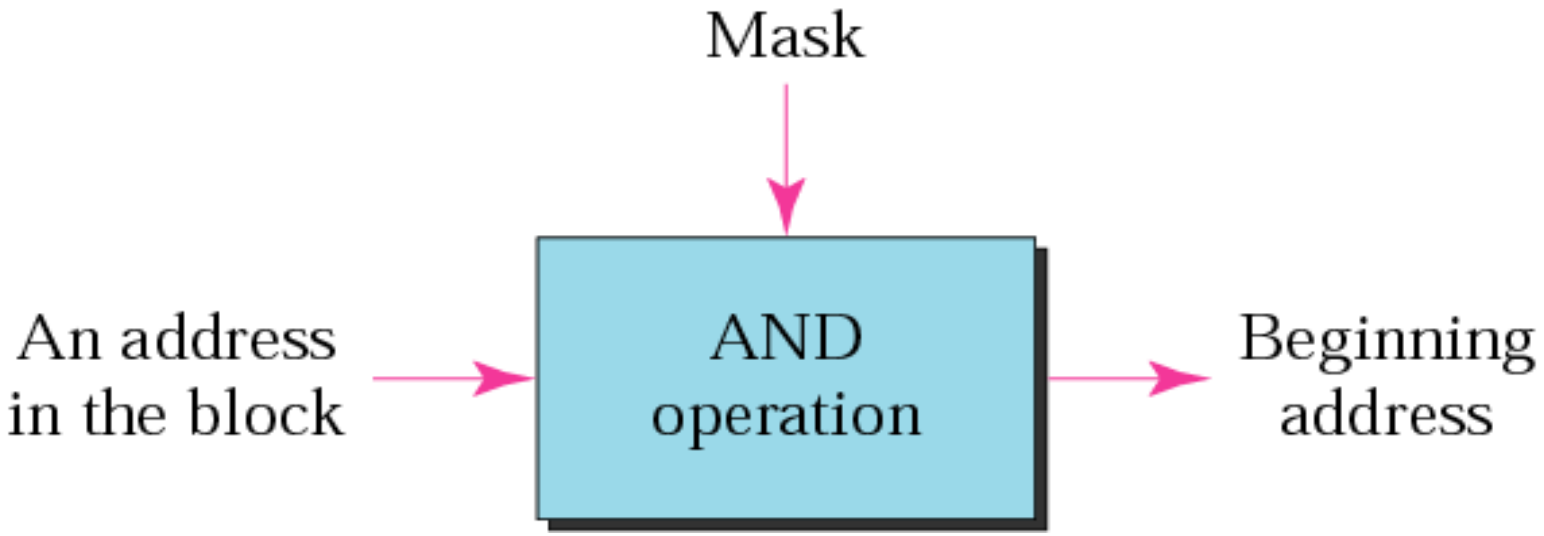
Subnet mask in decimal = 255.255.240.0

- 32 bits long
- Divided into four octets
- Network and subnet portions all 1's
- Host portion all 0's

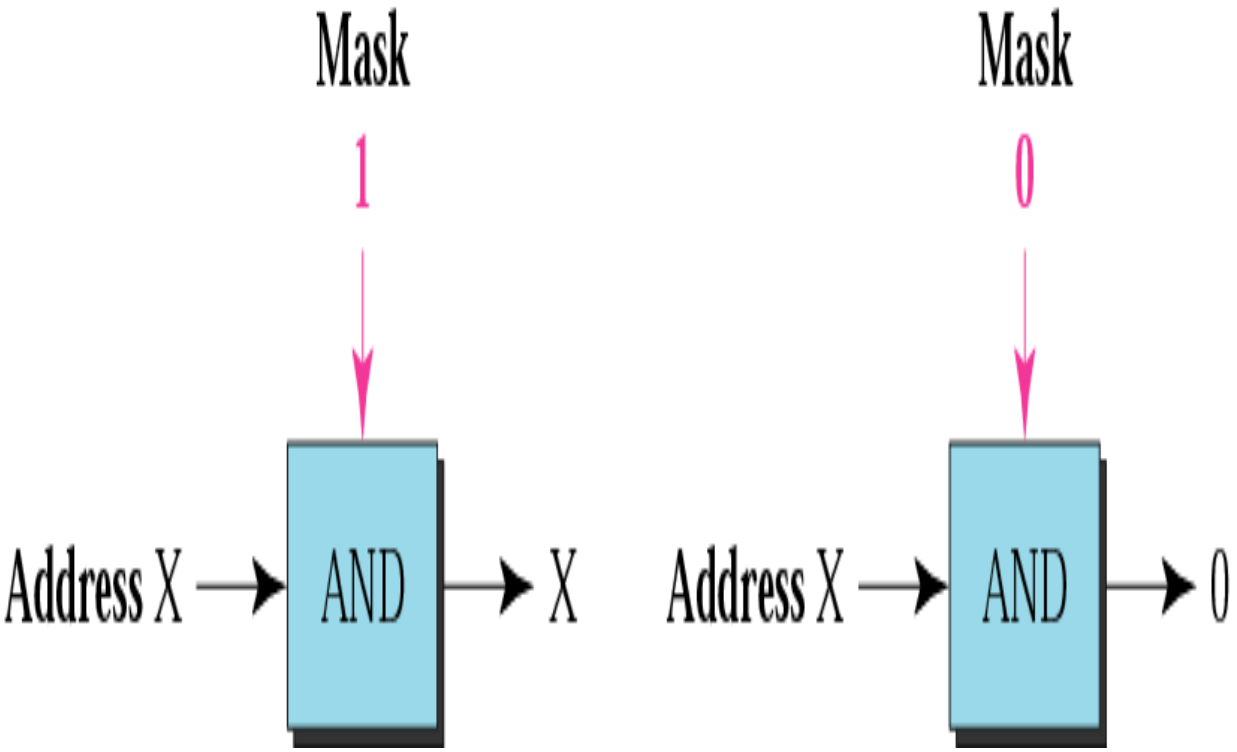
Subnet Mask

- A mask is a 32-bit binary number.
- The mask is ANDed with IP address to get the block address (Network address)

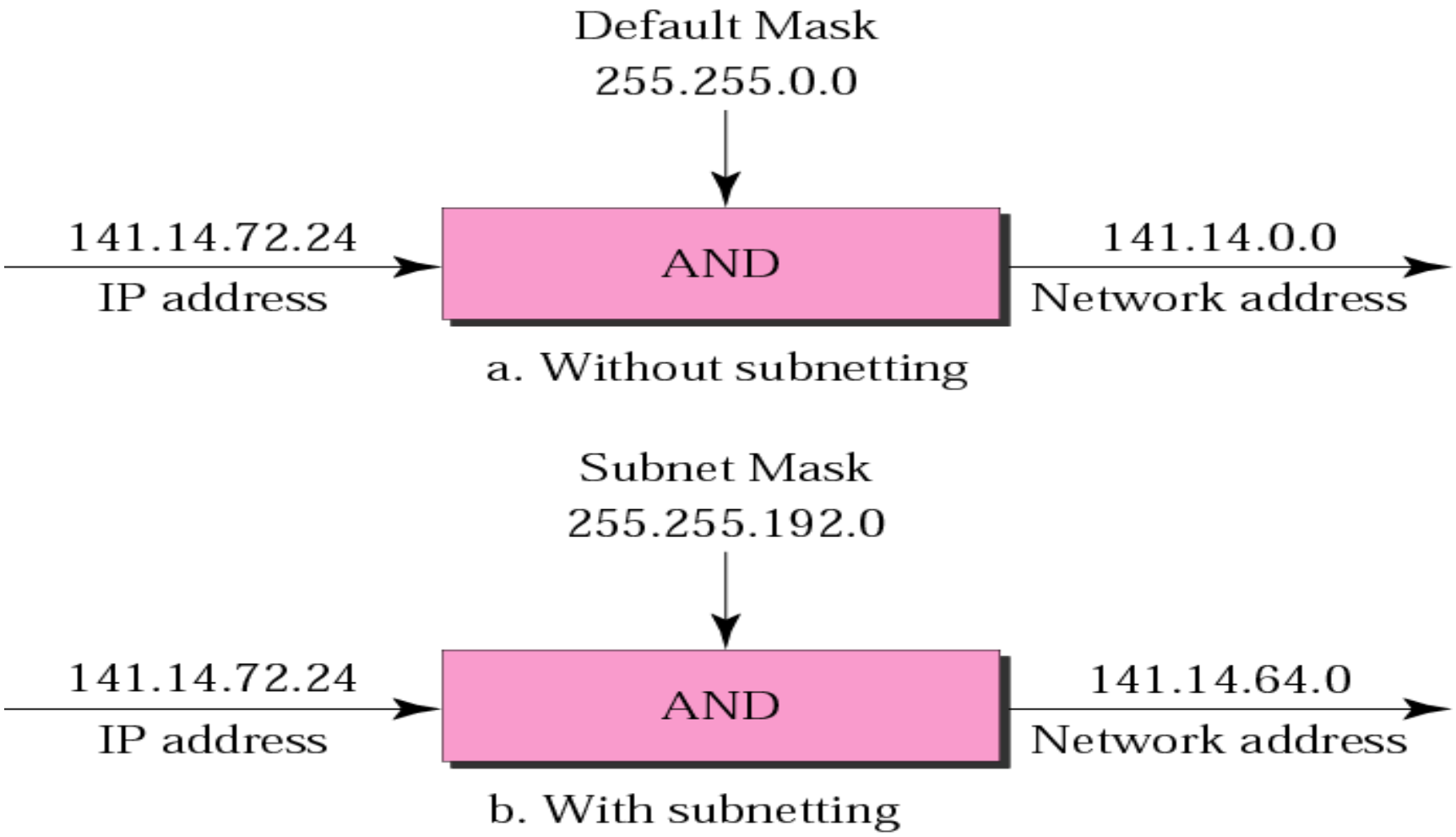
Mask And IP address = Block Address



AND operation



Default mask and subnet mask



1. 192.168.3.55/24
    - What is the subnet mask?
    - What is the network address?
2. 192.168.3.55/28
    - What is the subnet mask?
    - What is the network address?
    - What is the broadcast address?

SUBNETTING

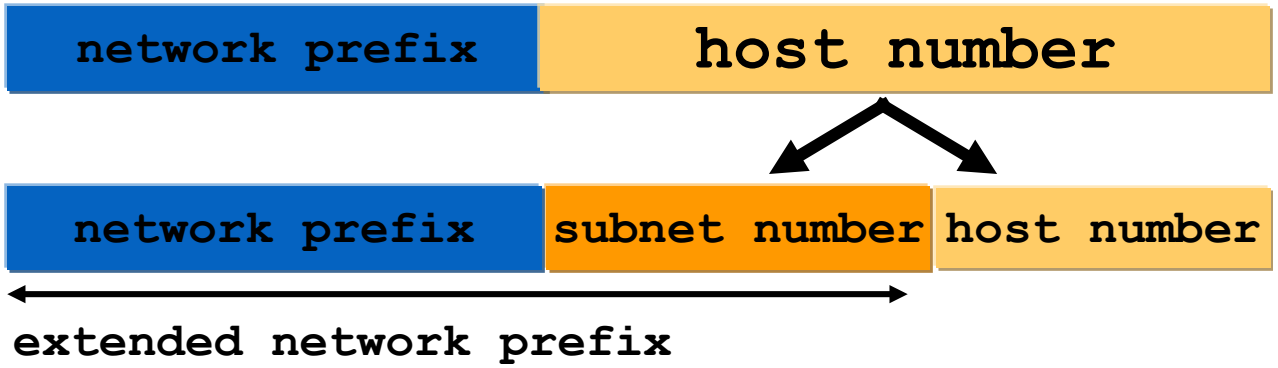
- The process of splitting a network into smaller networks is called subnetting, and the smaller networks thus formed are known as subnets
- Subnets are connected to the rest of the network through address-resolving devices called routers.
- Subnets can be freely assigned within the organization
    - Internally, subnets are treated as separate networks
    - Subnet structure is not visible outside the organization

Subnetting . . .

- To create a subnet address, a network administrator borrows bits from the original host portion and designates them as the subnet field.
- A network with no subnets will have one of these default subnet mask values depending upon its class address.
- However, when subnetting is implemented, the actual subnet mask value is calculated to determine valid IP addresses for hosts on a subnet.

Basic Idea of Subnetting

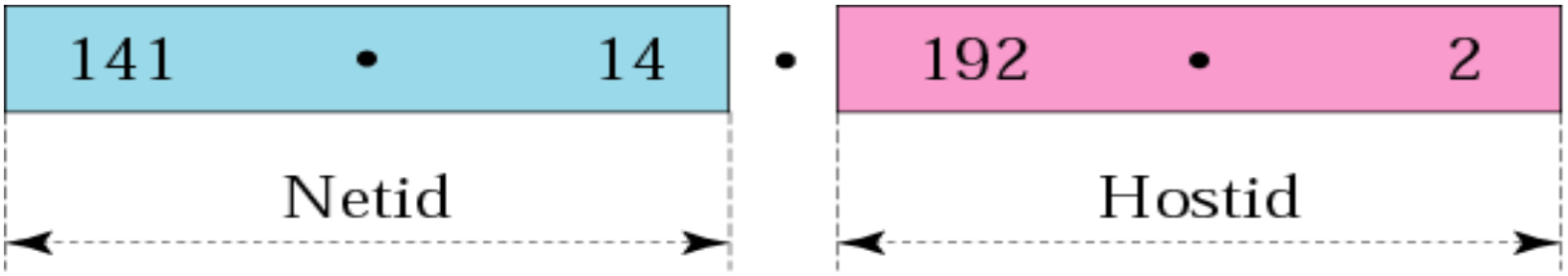
- Split the host number portion of an IP address into a **subnet number** and a (smaller) **host number**.
- Result is a 3-layer hierarchy



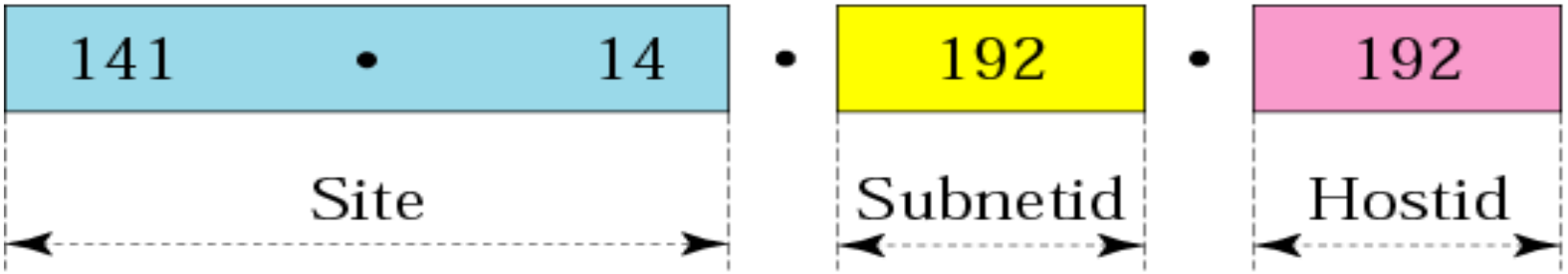
Advantages of Subnetting

- Improves efficiency of IP addresses by not consuming an entire address space for each physical network.
- Reduces router complexity. Since external routers do not know about subnetting, the complexity of routing tables at external routers is reduced.
- Reduced network traffic
- Optimized network performance
- Simplified management
- Facilitated spanning of large geographical distances.

Addresses in a network with and without subnetting



a. Without subnetting



b. With subnetting

Finding the Subnet Address

- Given an IP address, we can find the subnet address the same way we found the network address.
- Apply the mask to the address
- Use binary notation for both the address and the mask and then apply the AND operation to find the subnet address.

Finding the Subnet Address

What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

- 11001000 00101101 00100010 00111000
- 11111111 11111111 11110000 00000000
- 11001000 00101101 00100000 00000000

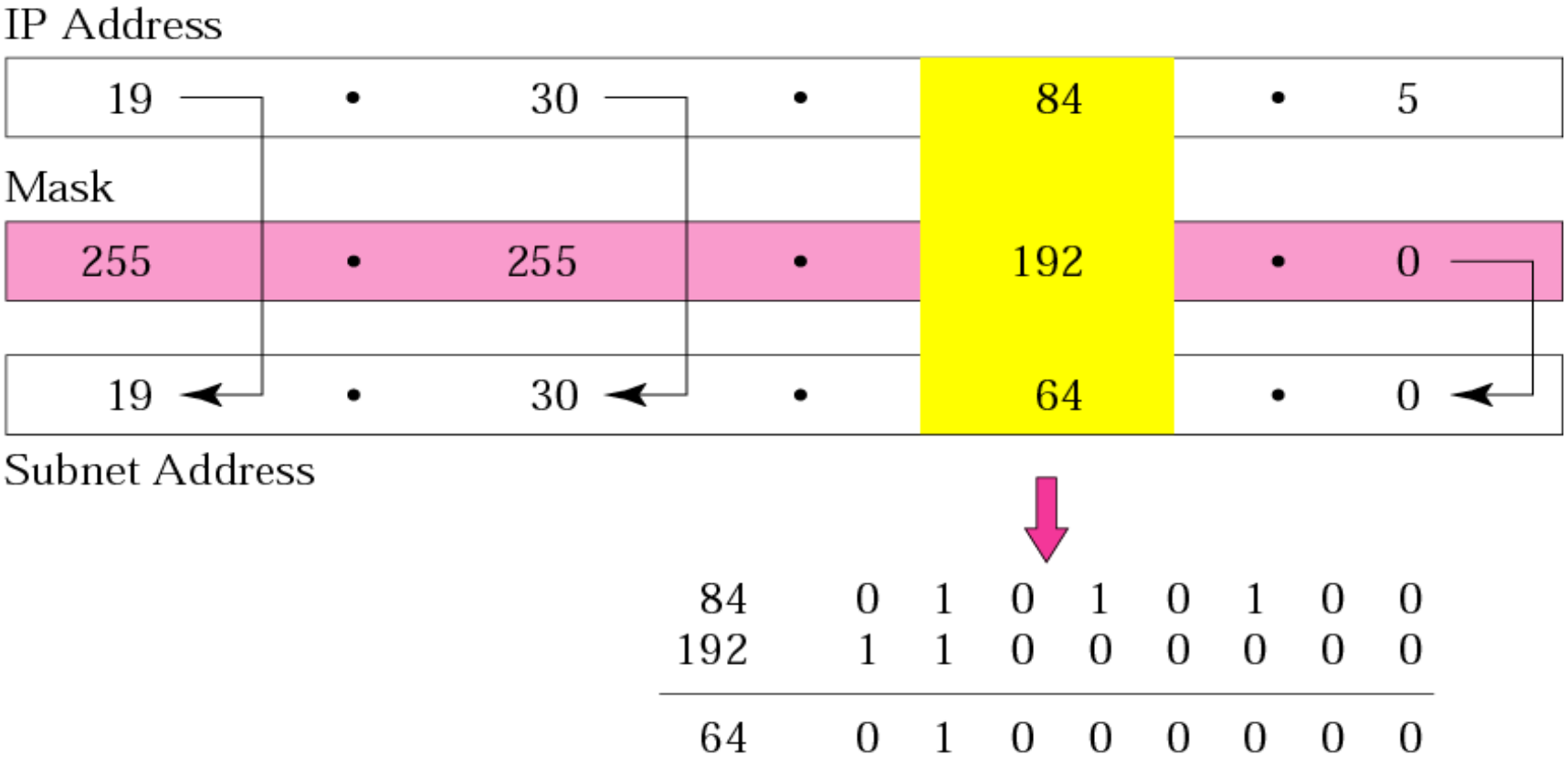
The subnetwork address is 200.45.32.0.

Finding the Subnet Address

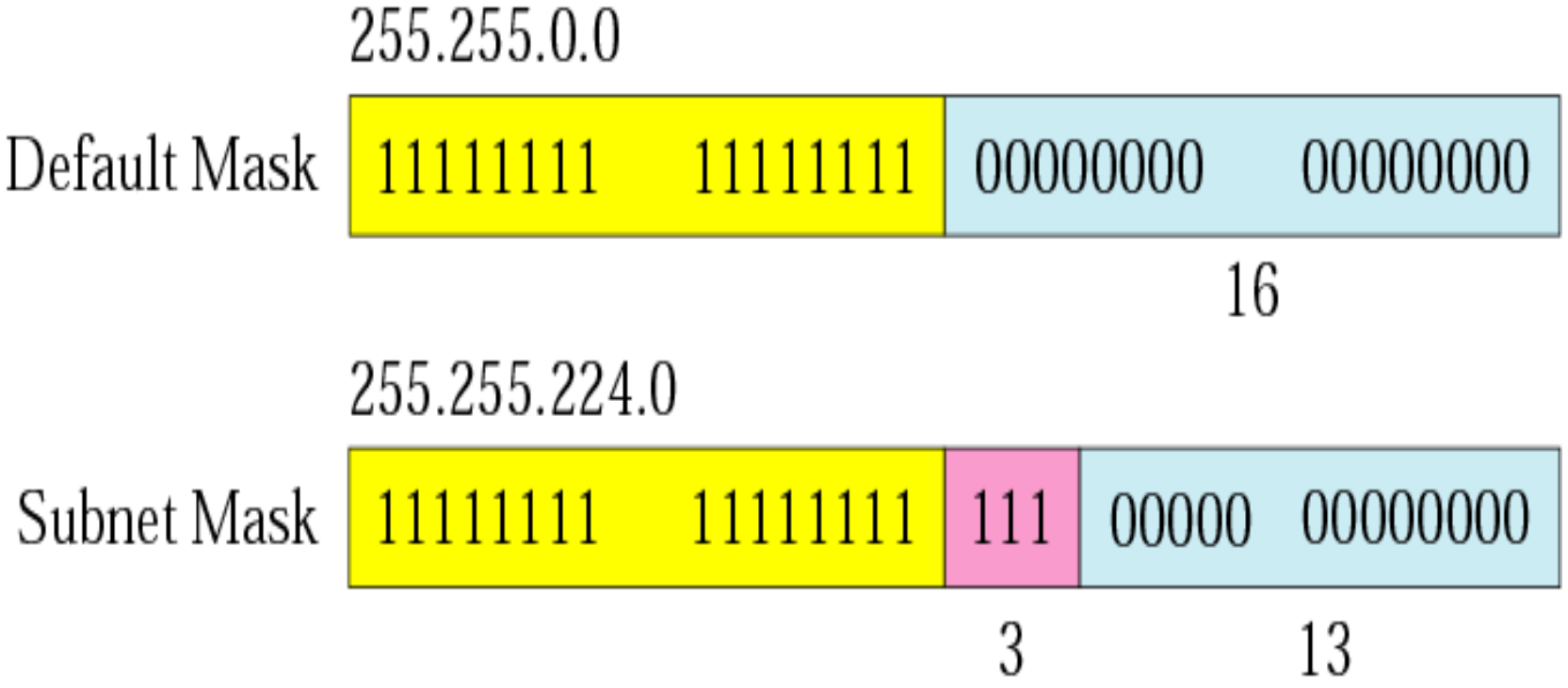
- If the byte in the mask is 255, copy the byte in the address.
- If the byte in the mask is 0, replace the byte in the address with 0.
- If the byte in the mask is neither 255 nor 0, we write the mask and the address in binary and apply the AND operation.

Finding the Subnet Address

- What is the subnetwork address if the destination address is 19.30.80.5 and the mask is 255.255.192.0?



Comparison of a default mask and a subnet mask



A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.

- The number of 1s in the default mask is 24 (class C).
- The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3). We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27 (24 + 3).
- The total number of 0s is 5 (32 – 27).

The mask is

11111111 11111111 11111111 11100000

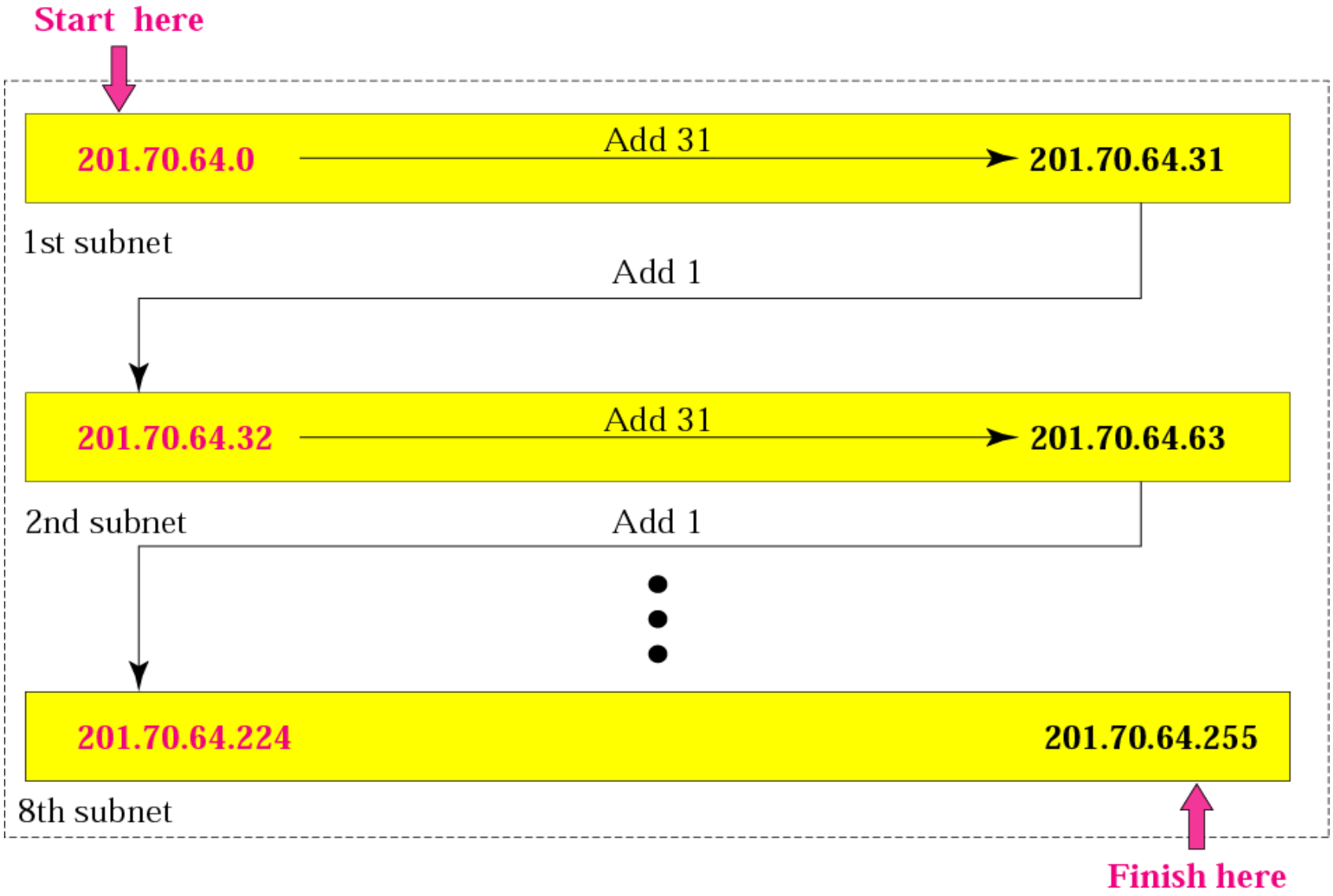
or

255.255.255.224

The number of subnets is 8.

The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.

The number of host is 32-2=30


Start here
201.70.64.0
Add 31
201.70.64.31
1st subnet
Add 1
201.70.64.32
Add 31
201.70.64.63
2nd subnet
Add 1
201.70.64.224
201.70.64.255
8th subnet
Finish here

Exercise:

You have a network that needs 29 subnets while maximizing the number of host addresses available on each subnet.

How many bits must you borrow from the host field to provide the correct subnet mask?

Class C subnetting

192.168.1.153/27

1. What is the subnet mask?
2. how many subnets?
3. how many hosts?
4. what are the valid hosts?
5. what are the valid subnet?
6. what are the broadcast address for each subnet?

Class B subnetting

172.16.0.0

255.255.255.224

1. how many subnets?
2. how many hosts?
3. what are the network address of each subnet?
4. what are the broadcast address for each subnet?
5. what are the valid hosts?

Class B subnetting

255.255.240.0/20

1. how many subnets?
2. how many hosts?
3. what are the valid subnet?
4. what are the broadcast address for each subnet?
5. what are the valid hosts?

subnetting

255.255.0.0 (/20)

1. how many subnets?
2. how many hosts?
3. what are the valid subnet?
4. what are the valid hosts?
5. what are the broadcast address for each subnet?

Subnetting

A company would like to break its Class B private IP address 172.16.0.0 into as many subnets as possible provided that they can get at least 300 clients per subnet. Find ranges of IP addresses for each subnet and new mask.

- If an Ethernet port on a router were assigned an IP address of 172.16.112.1/25, what would be the valid subnet address of this host?

- A.172.16.112.0
- B.172.16.0.0
- C.172.16.96.0
- D.172.16.255.0

A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.

The number of 1s in the default mask is 16 (class B).

The company needs 1000 subnets. This number is not a power of 2. The next number that is a power of 2 is 1024 (2^{10}). We need 10 more 1s in the subnet mask.

The total number of 1s in the subnet mask is 26 (16 + 10).

The total number of 0s is 6 (32 – 26).

The mask is

11111111 11111111 11111111 11000000

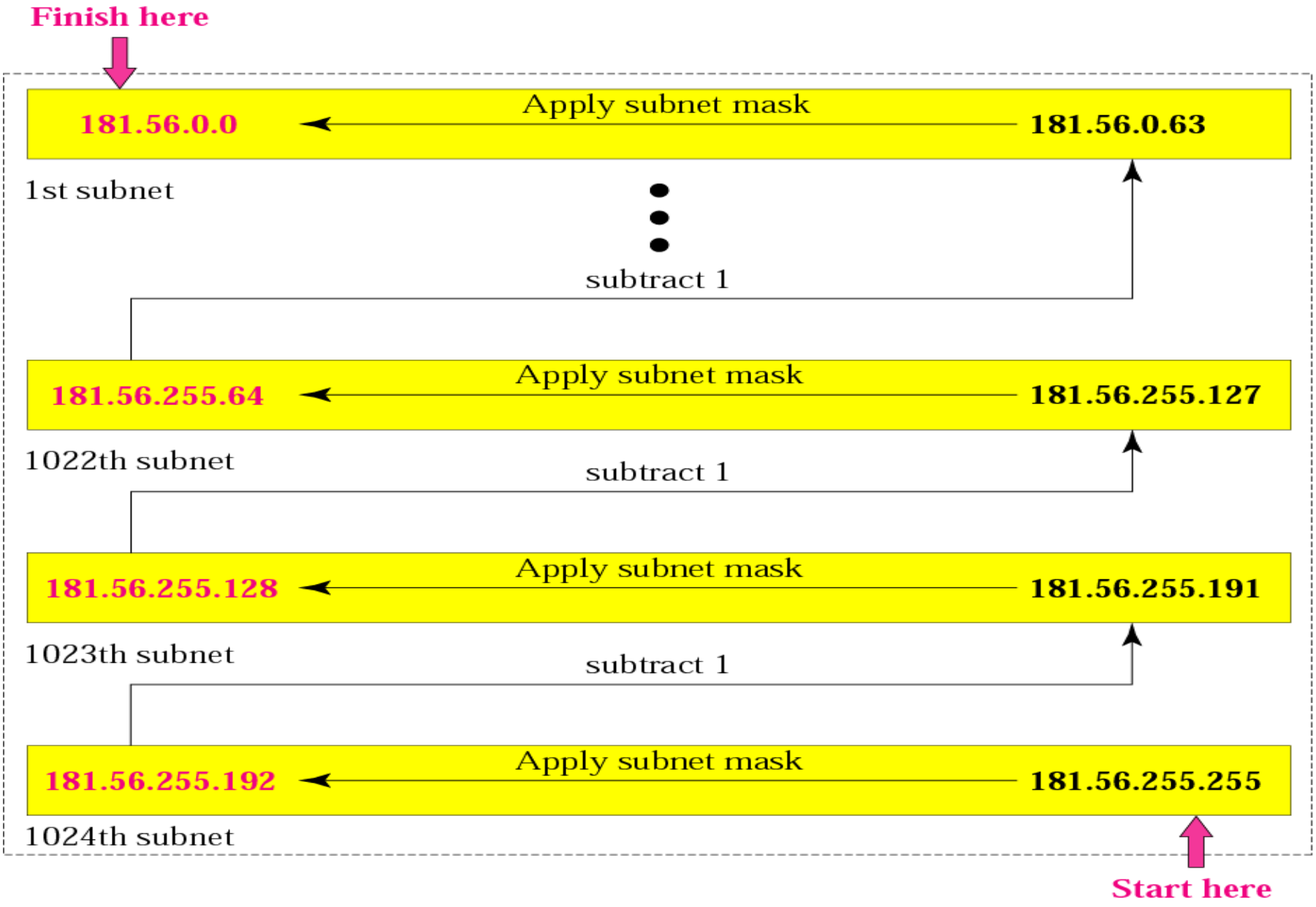
or

255.255.255.192.

The number of subnets is 1024.

The number of addresses in each subnet is 2^6 (6 is the number of 0s) or 64.

See next slide


Finish here
181.56.0.0
Apply subnet mask
181.56.0.63
1st subnet
subtract 1
181.56.255.64
Apply subnet mask
181.56.255.127
1022th subnet
subtract 1
181.56.255.128
Apply subnet mask
181.56.255.191
1023th subnet
subtract 1
181.56.255.192
Apply subnet mask
181.56.255.255
1024th subnet
Start here

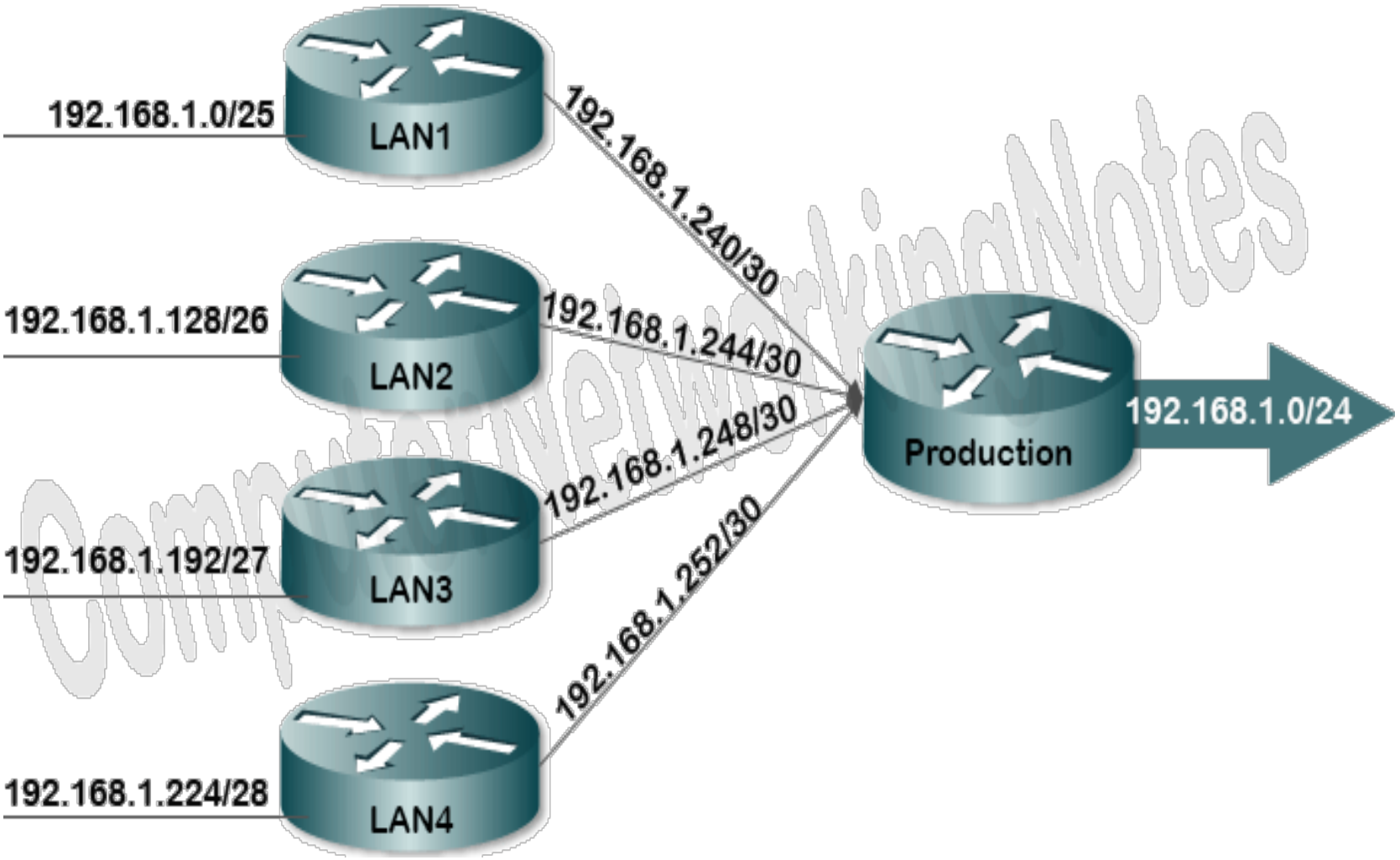
SUPERNETTING

- Supernetting is combining a group of networks into one large supernetwork.
- Supernetting is the opposite of subnetting
- Converting network bits to host bits
- In subnetting you borrow bits from the host part, Supernetting is done by borrowing bits from the network side.
- Supernetting is the process of summarizing a bunch of contiguous Subnetted networks back in a single large network.
- Supernetting is also known as route summarization and route aggregation

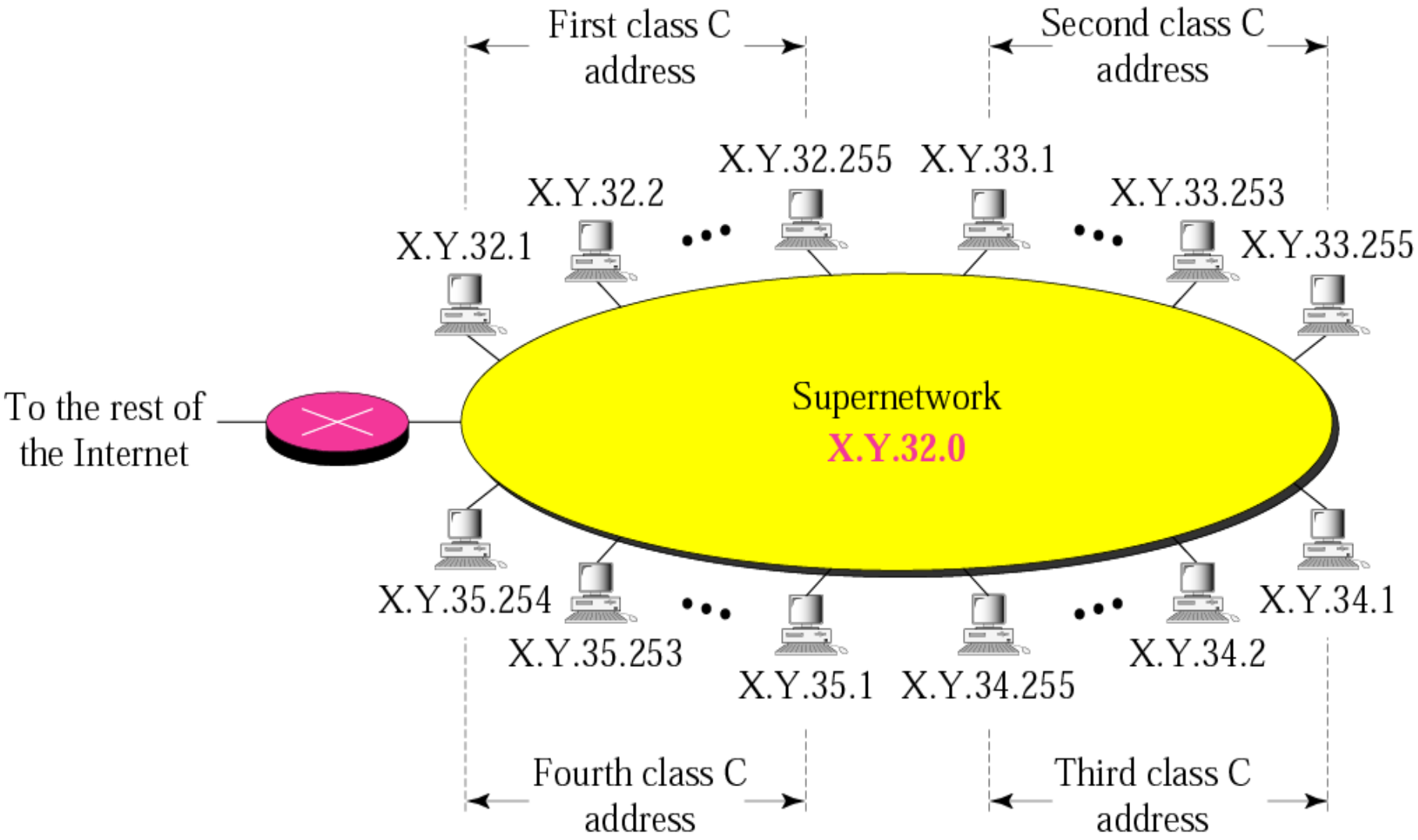
SUPERNETTING

- Supernetting is mainly done for optimizing the routing tables.
- A routing table is the summary of all known networks.
- Routers share routing tables to find the new path and locate the best path for destination.
- Without Supernetting, router will share all routes from routing tables as they are.
- With Supernetting, it will summarize them before sharing.
- Route summarization reduces the size of routing updates dramatically.

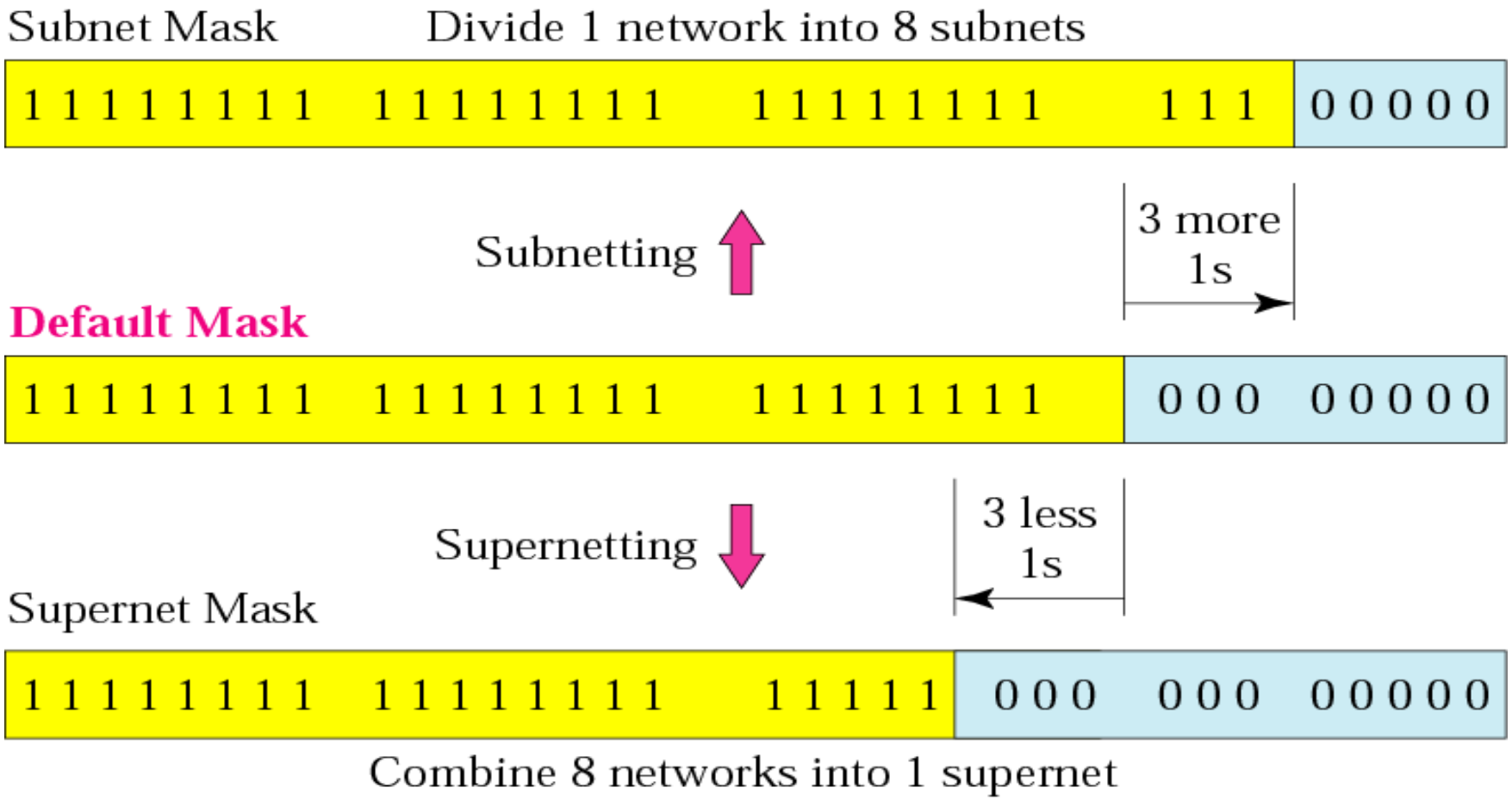
A supernetwork



A supernetwork



Comparison of subnet, default, and supernet masks



Example 1

Supernet the following IP addresses to a single network

200.1.0.0/24
200.1.1.0/24
200.1.2.0/24
200.1.3.0/24

Answer: 200.1.0.0/22

Example 2

Supernet the following IP Addresses

- 172.168.197.0/24
- 172.168.198.0/24
- 172.168.199.0/24
- 172.168.200.0/24
- 172.168.204.0/24
- 172.168.206.0/24

Example: 4 class C addresses appear to networks outside as a single network

- **4 address-contiguous networks:**

213.2.96.0	11010101.00000010.011000***00***.00000000
213.2.97.0	11010101.00000010.011000***01***.00000000
213.2.98.0	11010101.00000010.011000***10***.00000000
213.2.99.0	11010101.00000010.011000***11***.00000000

- **What is the Supernet mask?**

  255.255.252.0

- **What is the Supernet address?**

  213.2.96.0/22

  11010101 . 00000010 . 011000 00 . 00000000

- **In subnetting, we need the first address of the subnet and the subnet mask to define the range of addresses.**
- **In supernetting, we need the first address of the supernet and the supernet mask to define the range of addresses.**

We need to make a supernetwork out of 16 class C blocks. What is the supernet mask?

Solution

We need 16 blocks. For 16 blocks we need to change four 1s to 0s in the default mask. So the mask is

11111111 11111111 1111**0000** 00000000

or

255.255.240.0

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. A router receives three packets with the following destination addresses:

205.16.37.44

205.16.42.56

205.17.33.76

Which packet belongs to the supernet?

We apply the supernet mask to see if we can find the beginning address.

205.16.37.44 AND 255.255.248.0 → 205.16.32.0

205.16.42.56 AND 255.255.248.0 → 205.16.40.0

205.17.33.76 AND 255.255.248.0 → 205.17.32.0

Only the first address belongs to this supernet.

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. How many blocks are in this supernet and what is the range of addresses?

Solution

The supernet has 21 1s. The default mask has 24 1s. Since the difference is 3, there are 2^3 or 8 blocks in this supernet.

The blocks are 205.16.32.0 to 205.16.39.0.

The first address is 205.16.32.0.

The last address is 205.16.39.255.

ARP (Address Resolution Protocol)

- ARP is used for mapping a network address (IPv4 Address) to a physical address/Ethernet address (MAC address)
- The MAC address is always used for direct communications (i.e, is, sending information on the wire).
- ARP has to know the physical address of the machine to which it is going to send datagrams
- IP is used to determine routes and move packets from network to network.

ARP

- ARP is responsible for finding a map to any local physical address that IP may request.
- If ARP does not have a map in memory, it has to find one on the network.
- ARP uses a local broadcast, asking all the systems on the network if they have the IP that is being resolved.

How ARP works?

- ARP broadcasts a packet that contains the IP address and MAC of the originating host; these can then be stored at the target machine.
- The target stores the address and responds with a packet that contains its MAC address. The originating machine then stores this in the local ARP cache. The two systems now have each other's IP and MAC addresses and can communicate.
- ARP can resolve only the address of a local machine. When an IP address is determined to be on a remote subnet, IP sends the packet to the default gateway; in this case, ARP is used to find the MAC address of the gateway.

ICMP- INTERNET CONTROL MESSAGING PROTOCOL

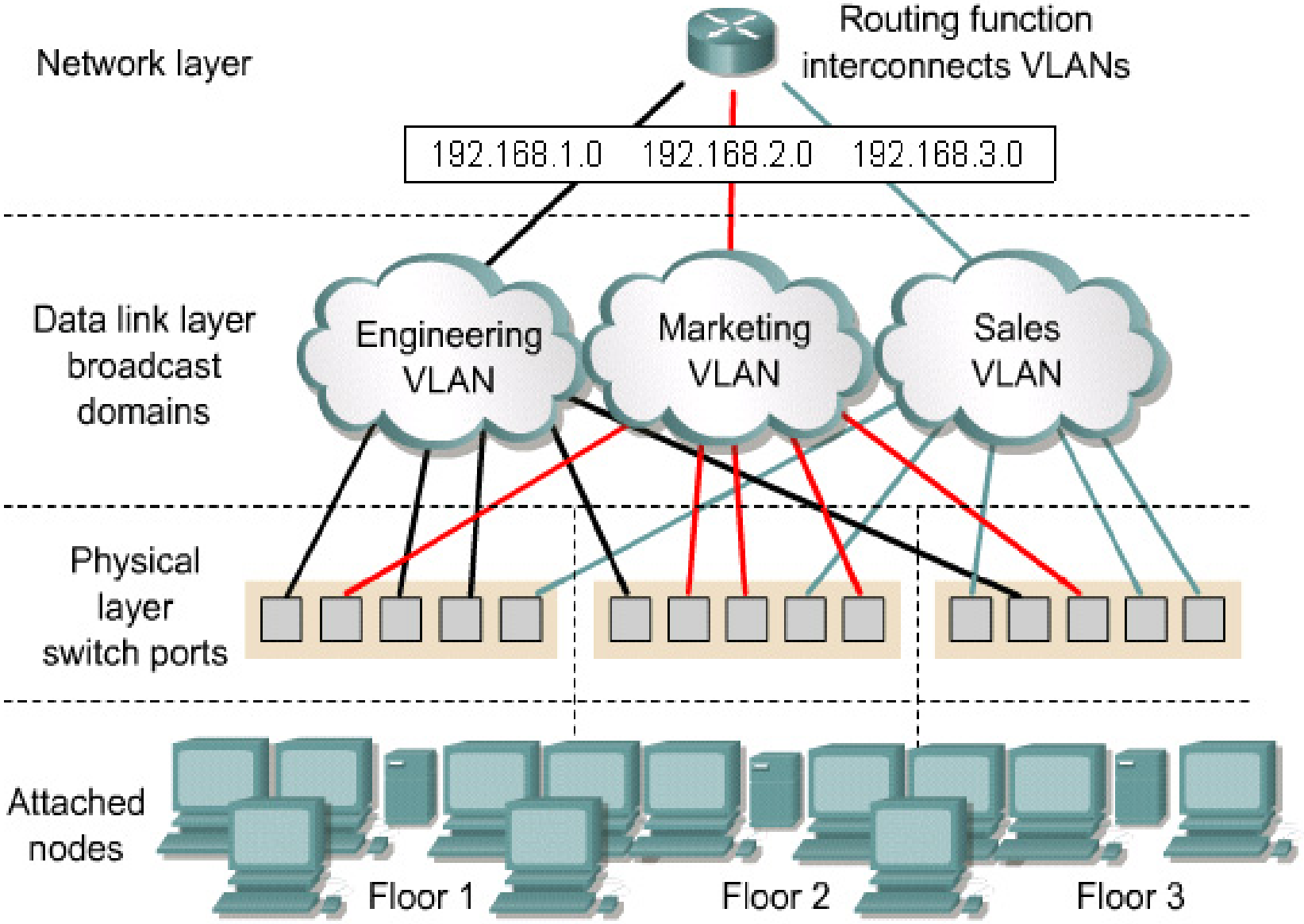
- Internet Control Message Protocol (ICMP), a part of the Internet layer, is responsible for reporting errors and messages regarding the delivery of IP datagrams.
- ICMP always reports error message to the original source

ICMP

- It is a protocol for the exchange of error messages and other vital information between (Physical) Internet entities such as hosts and routers.
- ICMP warns you when a destination host is unreachable, or informs you of how long it took to get to a destination host.
- ICMP Error messages include the following:
  - Destination unreachable
  - Source Quench
  - Time exceeded
  - Redirection
  - Parameter problem, etc…

VLAN (Virtual Local Area Network)

- A VLAN is a logical grouping of workstations, servers and network devices that appear to be on **the** same LAN despite **their** geographical distribution.
- VLAN can be grouped by function, department, or application, regardless of their physical segment location.
- VLANs function by *logically segmenting* the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN
- The router interconnecting each shared hub typically provides segmentation and can act as a broadcast firewall.


Network layer
Routing function
interconnects VLANs
192.168.1.0
192.168.2.0
192.168.3.0
Data link layer
broadcast
domains
Engineering
VLAN
Marketing
VLAN
Sales
VLAN
Physical
layer
switch ports
Attached
nodes
Floor 1
Floor 2
Floor 3

VLAN

- Routers in VLAN topologies provide
  - broadcast filtering
  - security
  - traffic flow management
- VLANs address
  - scalability,
  - security, and
  - network management
- Switches may not bridge any traffic between VLANs
- Traffic should only be routed between VLANs.

VLAN

- **VLAN**s can be **used** to create broadcast domains which eliminate the need for expensive routers.
- Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a **VLAN** can reduce the chances of an outsider gaining access to the data
- A **VLAN** allows several networks to work virtually as one LAN.

Routing

- Routing is used for taking a packet from one device and sending it through the network to another device on a different network
- Routers route traffic to all networks by selecting the best route to each remote network
- Routers communicate with one another to maintain their routing tables through the transmission of routing update messages

Routing

- A router is a network layer device that uses one or more routing metrics to determine the optimal path along which network traffic should be forwarded.
- Routers must maintain routing tables and make sure other routers know of changes in the network topology.
- When packets arrive at an interface, the router must use the routing table to determine where to send them.

Routing Protocol

- Routing protocols are created for routers
- Routing protocols have been designed to allow the exchange of routing tables between routers
- Routing protocols use various combinations of metrics for determining the best path for data.
- Routing metrics are values used in determining the advantage of one route over another
- Hop count, Bandwidth, Load, Delay and reliability are some of the metrics used to determine route

Routing Protocol

- Some routing protocols transmit update messages periodically, while others send them only when there are changes in the network topology
- Some protocols transmit the entire routing table in each update message, and some transmit only routes that have changed

Metrics

- **Bandwidth** – The data capacity of a link.
- **Delay** – The length of time required to move a packet along each link from source to destination
- **Load** – The amount of activity on a network resource such as a router or a link
- **Reliability** – Usually a reference to the error rate of each network link
- **Hop count** – The number of routers that a packet must travel through before reaching its destination.
- **Cost** – An value based on bandwidth, monetary expense, or other measurement, that is assigned by a network administrator

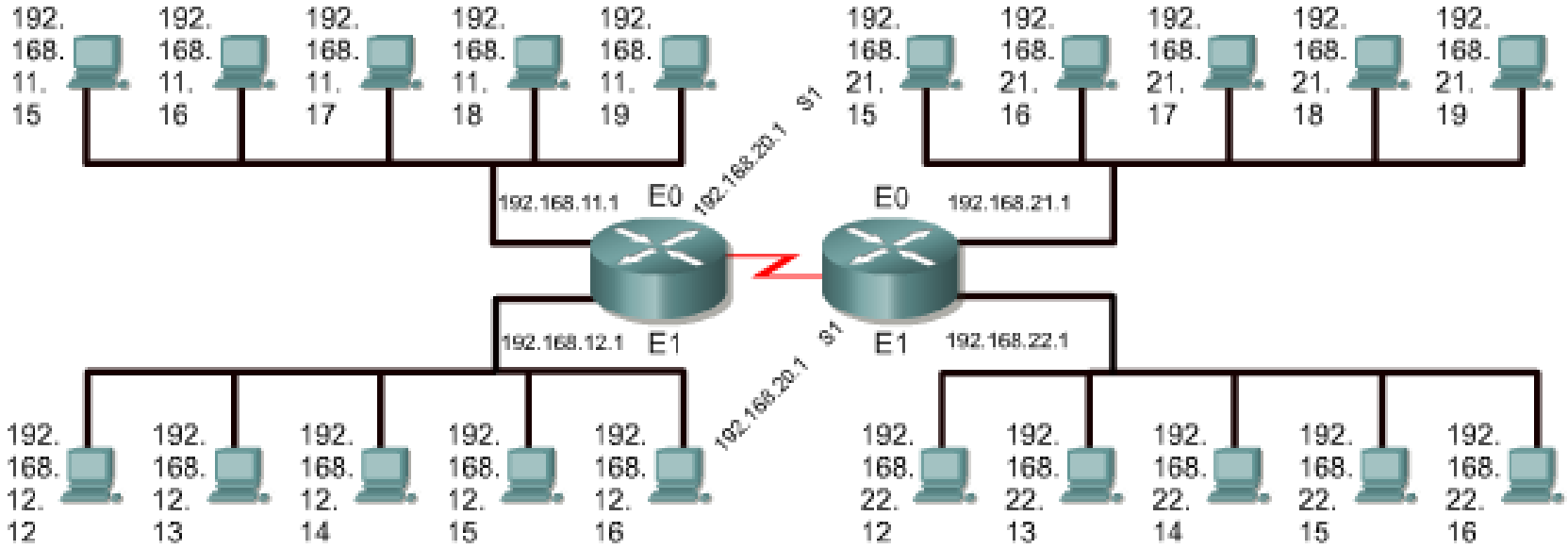
Routing Table

- A **routing table** is a set of rules, often viewed in **table** format, that is used to determine where data packets traveling over an Internet Protocol (IP) network **will** be directed.
- All IP-enabled devices, including **router**s and switches, use **routing tables.** A routing table contains the **information** necessary to forward a packet along the best path toward its destination. Each packet contains **information** about its origin and destination
- A **routing table** does not **contain** a list of all possible destinations. Rather, it **contains** a list of destinations that are next in line to the **router**. Each **router contains** this list and when it receive packets of data it directs that packet to the next link or hop in the network until it reaches its final destination.

Routing Table

- Routers use routing protocols to build and maintain routing tables that contain route information
- Routing protocols fill routing tables with a variety of route information
- Routing tables contain the information necessary to forward data packets across connected networks
- Routing Table contains information like:
  - **Protocol type**
  - **Destination/next-hop associations**
  - **Outbound interfaces**

Routing Table



Routing Table				
Learned		Network Address	Hop	Interface
C	-	192.168.11.0	0	E0
C	-	192.168.12.0	0	E1
C	-	192.168.20.0	0	S0
R	-	192.168.21.0	1	S0
R	-	192.168.22.0	1	S0

Routing Table				
Learned		Network Address	Hop	Interface
C	-	192.168.21.0	0	E0
C	-	192.168.22.0	0	E1
C	-	192.168.20.0	0	S1
R	-	192.168.11.0	1	S1
R	-	192.168.12.0	1	S1

Routing protocol (Reading Assignment)

- Rip- Routing Information Protocol
- IGP- **Interior gateway protocol**
- IGRP- **Interior Gateway Routing Protocol**
- EIGRP- Enhanced Interior Gateway Routing Protocol
- BGP- Border Gateway Protocol
- OSPF- Open Shortest Path First