Network Fundamentals Review

Cisco | Networking Academy®
Mind Wide Open™

Version 4.0

Content

- Introduction to Networks
- Communicating over the Network
- Network Devices
- Addressing
- Routing

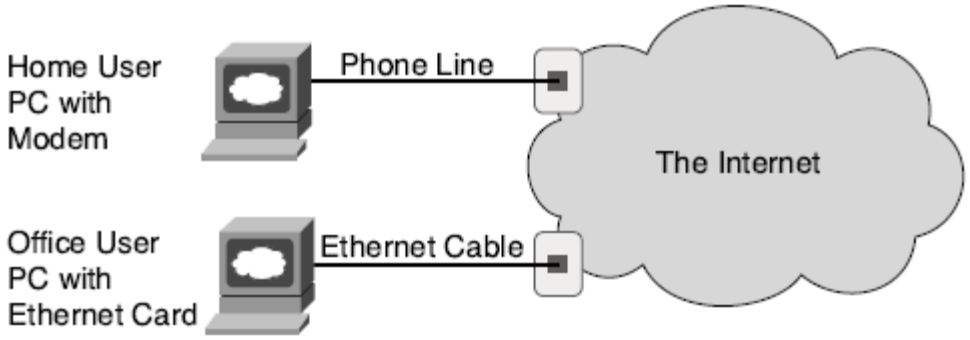
Network Fundamentals Review

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Introduction To Networking

- Describes the connection of two of more computers by some type of medium
  - Example: A computer connected to the internet over the public telephone system
  - Two computer connected by a wire cable



Origins Of Networking

- Difficult to actually place the origin of networking
- Many devices have been networked throughout history
  - Example: 1930s electrical engineers used a Network Analyzer for simulating electrical power grids
- The earliest mainframe computers were placed into networks
- Networks today include a wide variety of computers and peripheral components

Why Do We Use Networks?

- Efficiency
- Convenience
- Networks allow the transfer of
  - Files
  - Data
  - Shared applications
- Networks allow computers and users to share
  - Printers
  - Scanners
  - Fax Machines
  - Processors
  - Disk drives
  - Many other resources

Communicating over the Network

Communicating over the Network

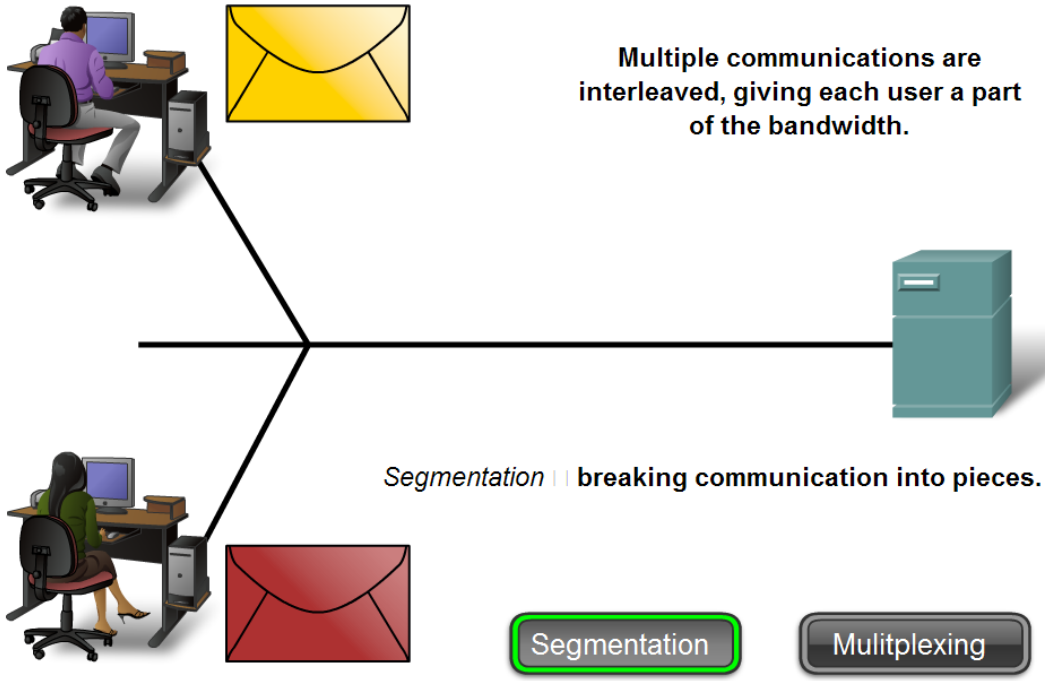
Cisco | Networking Academy®
Mind Wide Open™

Network Structure

- Communication begins with a message, or information, that must be sent from one individual or device to another.
- People exchange ideas using many different communication methods. All of these methods have three elements in common
  - Message source
  - The channel
  - Message destination

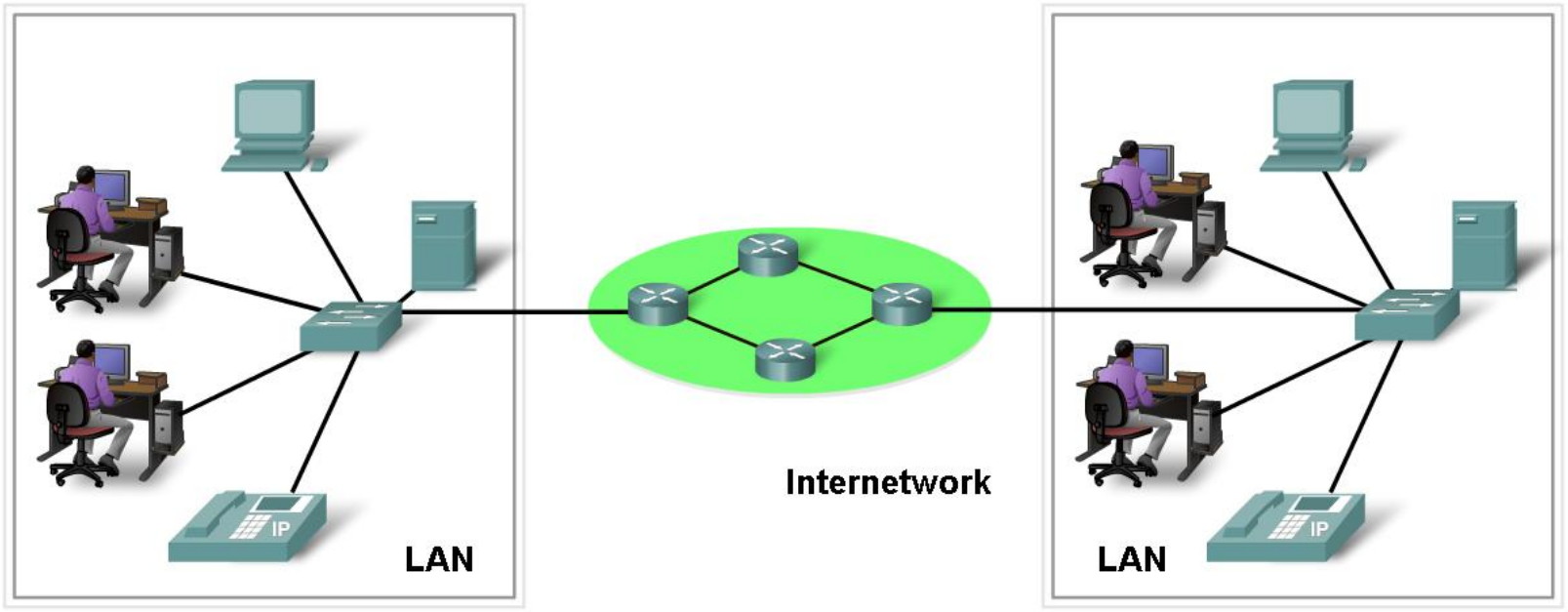
Network Structure

- A better approach is to divide the data into smaller, more manageable pieces to send over the network. This division of the data stream into smaller pieces is called segmentation.



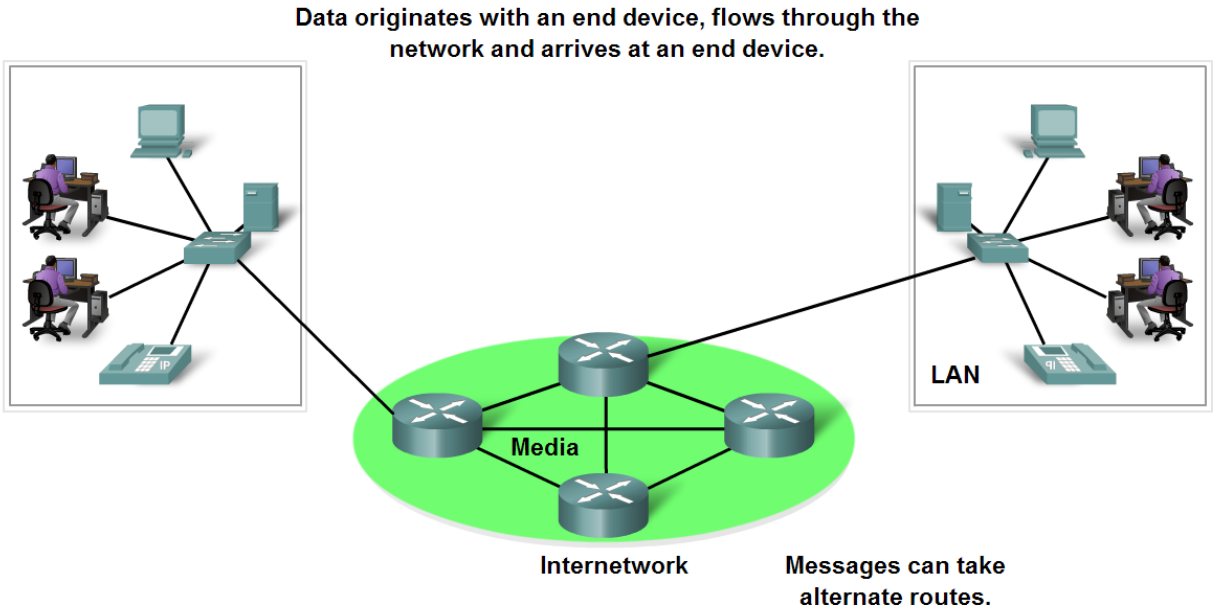
Network Structure

- Network components
  - Hardware: Devices and media
  - Software: Services and processes
- Devices: physical elements



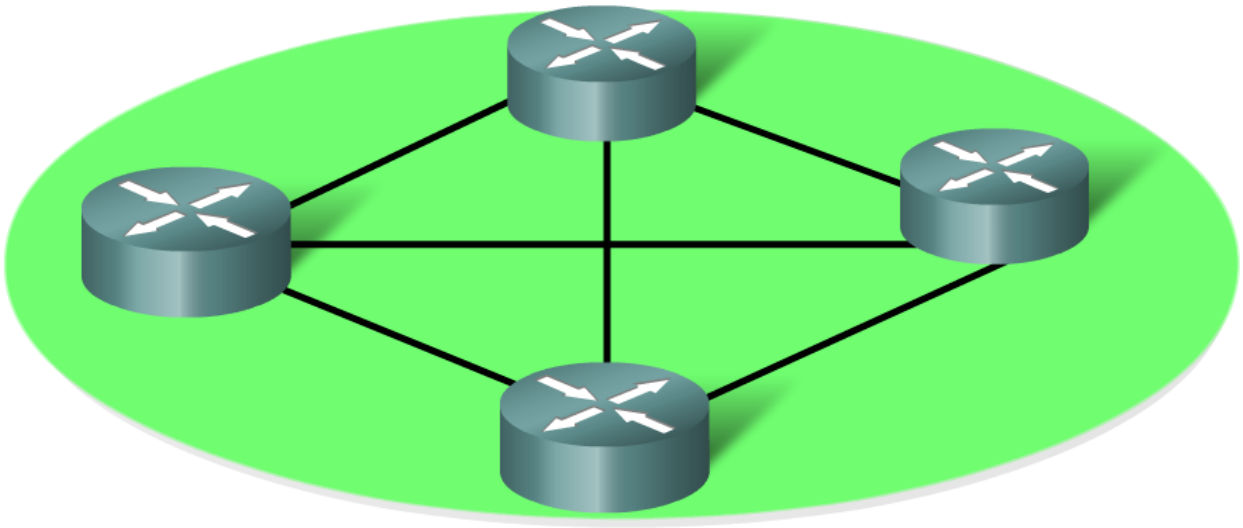
Network Structure

- The network devices that people are most familiar with are called end devices. These devices form the interface between the human network and the underlying communication network. Some examples of end devices are:
  - Computers (work stations, laptops, file servers, web servers)
  - Network printers
  - VoIP phones
  - Security cameras
  - Mobile handheld devices (such as wireless barcode scanners, PDAs)



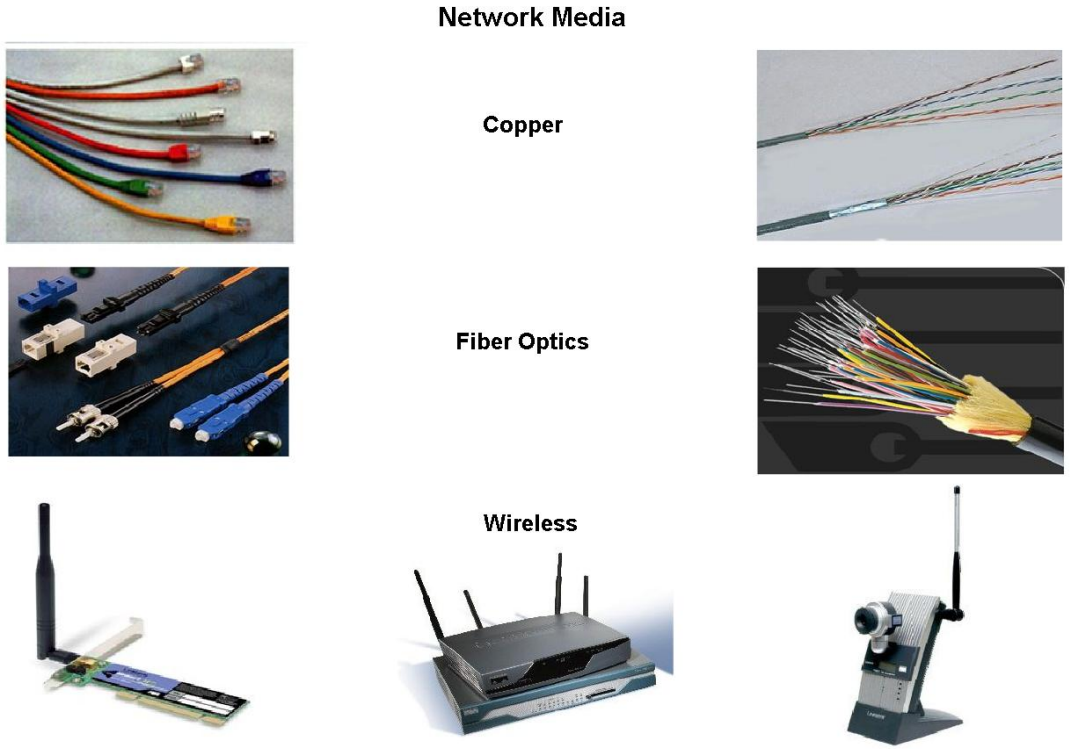
Network Structure

- Intermediary devices to provide connectivity and to work behind the scenes to ensure that data flows across the network.
- These devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.



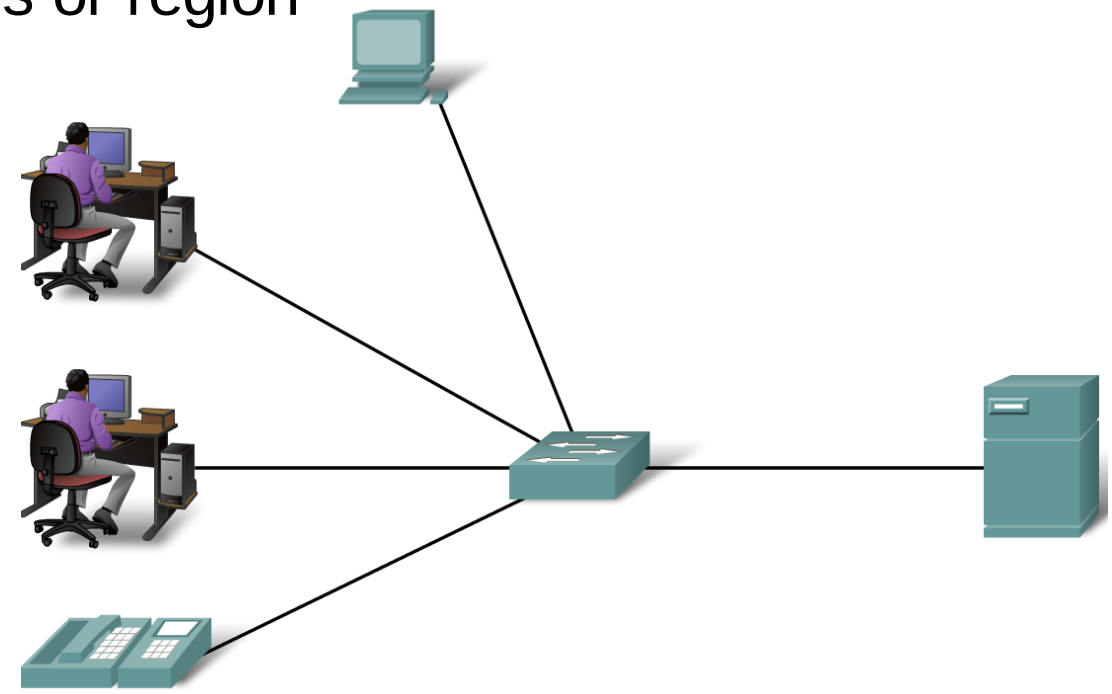
Network Structure

- Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination
- These media are:
  - Metallic wires within cables
  - Glass or plastic fibers
  - Wireless transmission



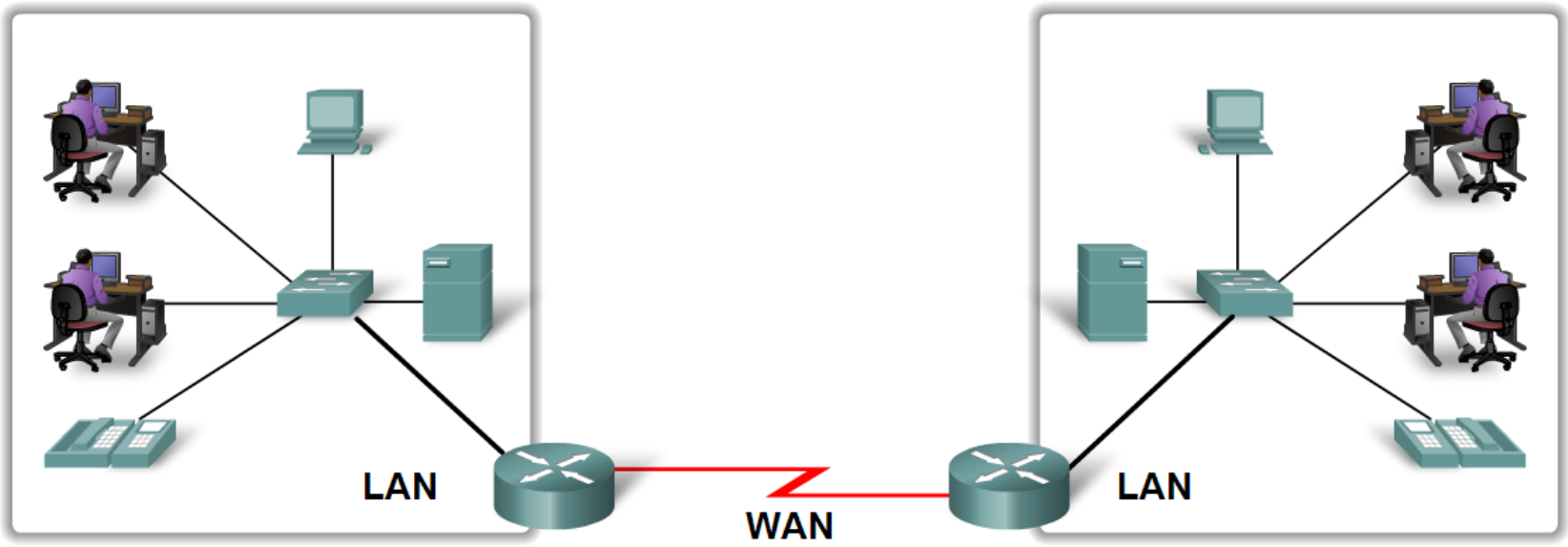
Network Types

- **Local Area Network (LAN):** An individual network usually spans a single geographical area, providing services and applications to people within a common organizational structure, such as a single business, campus or region



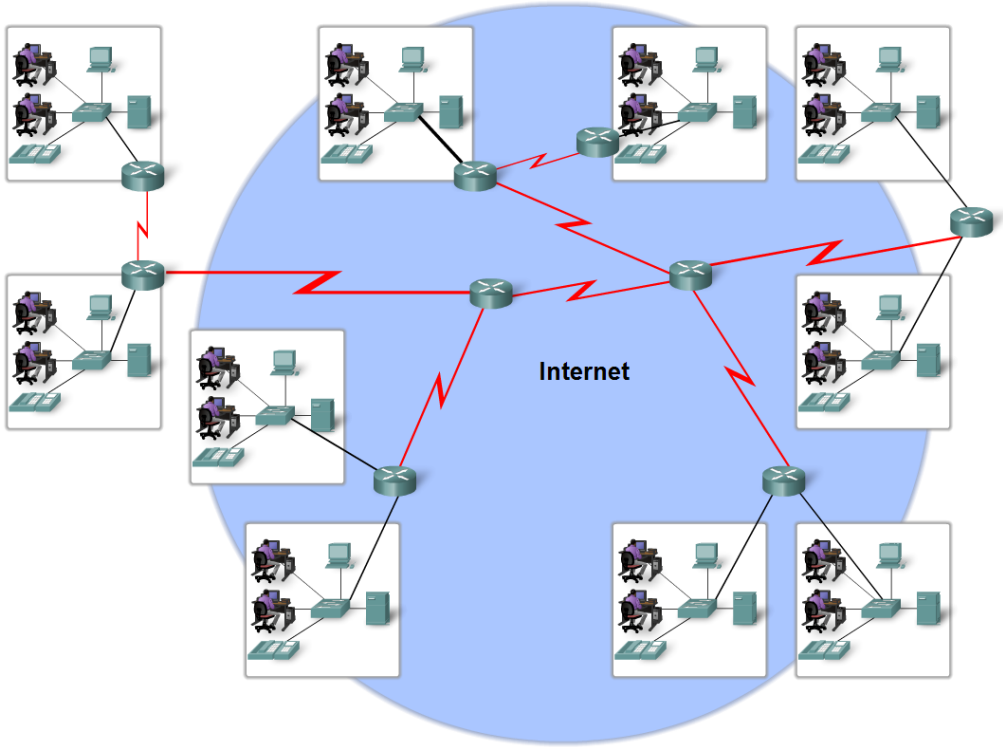
Network Types

- LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN)
- WANs use specifically designed network devices to make the interconnections between LANs.



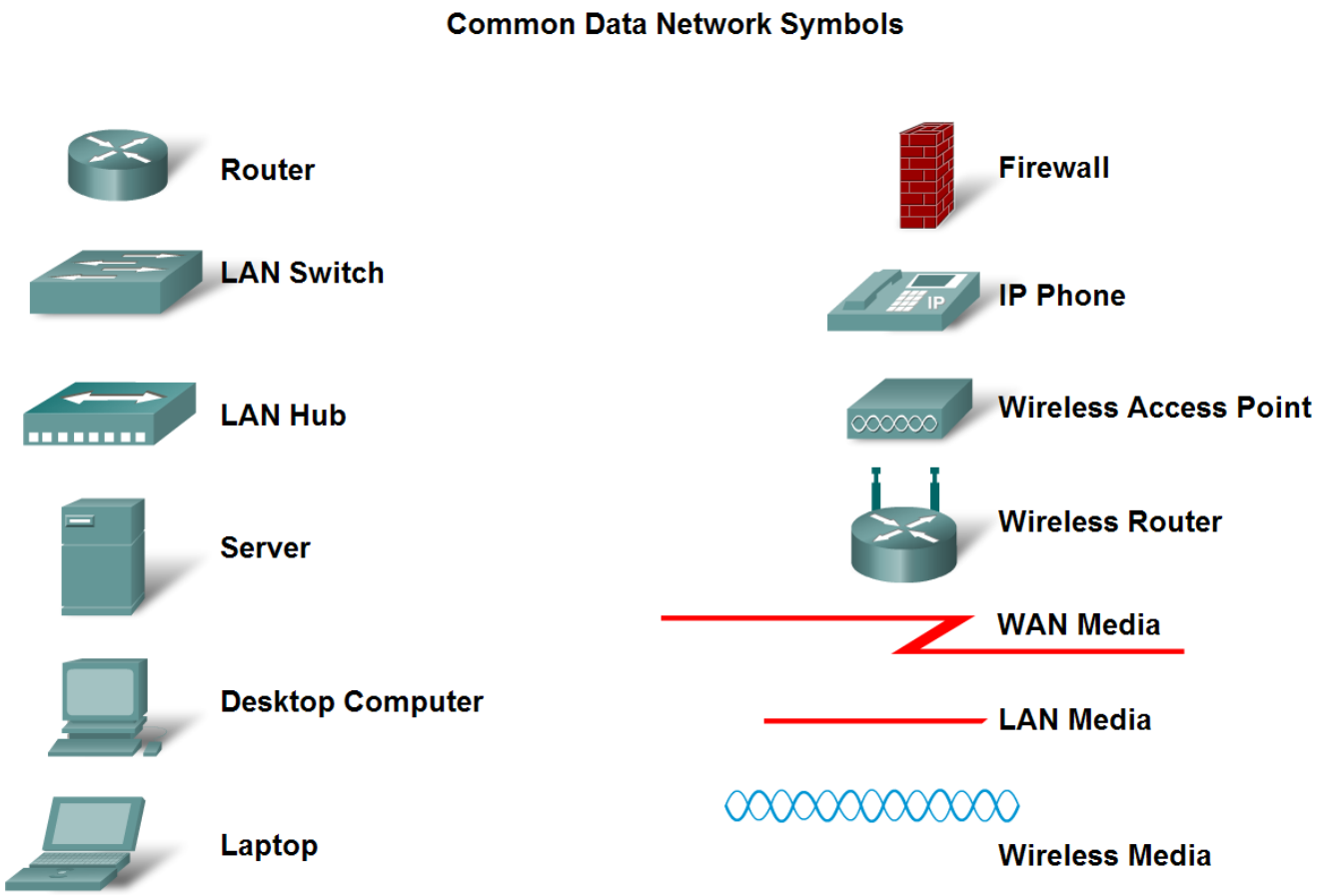
Network Types

- The internet is defined as a global mesh of interconnected networks



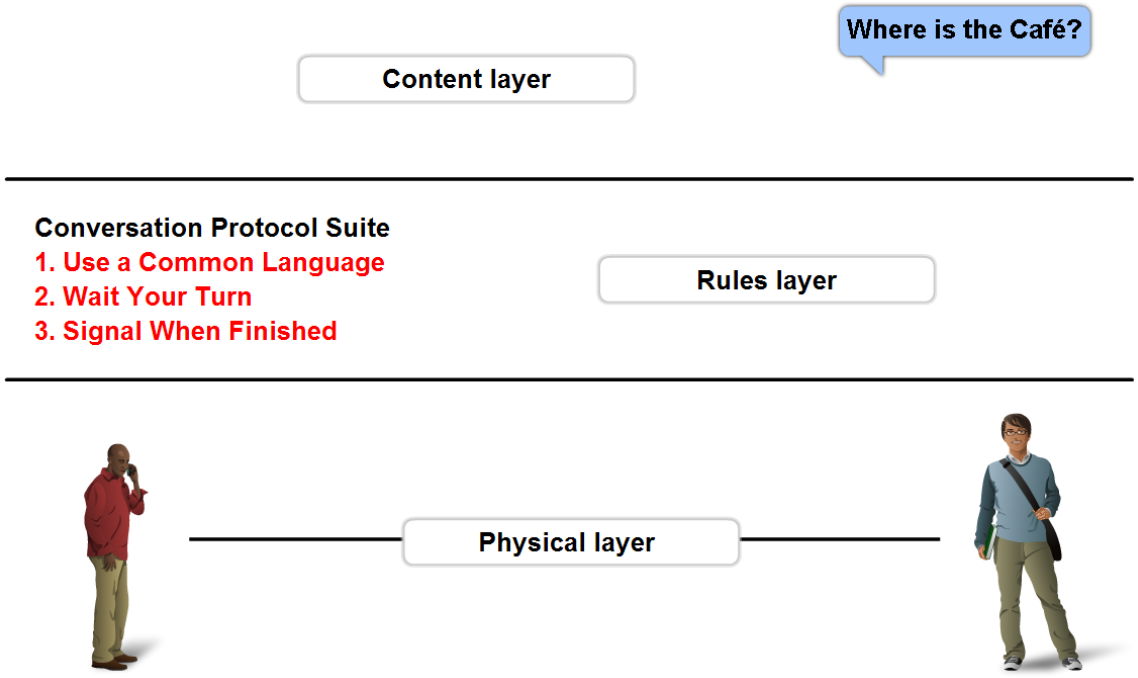
Network Types

- Describe network representations



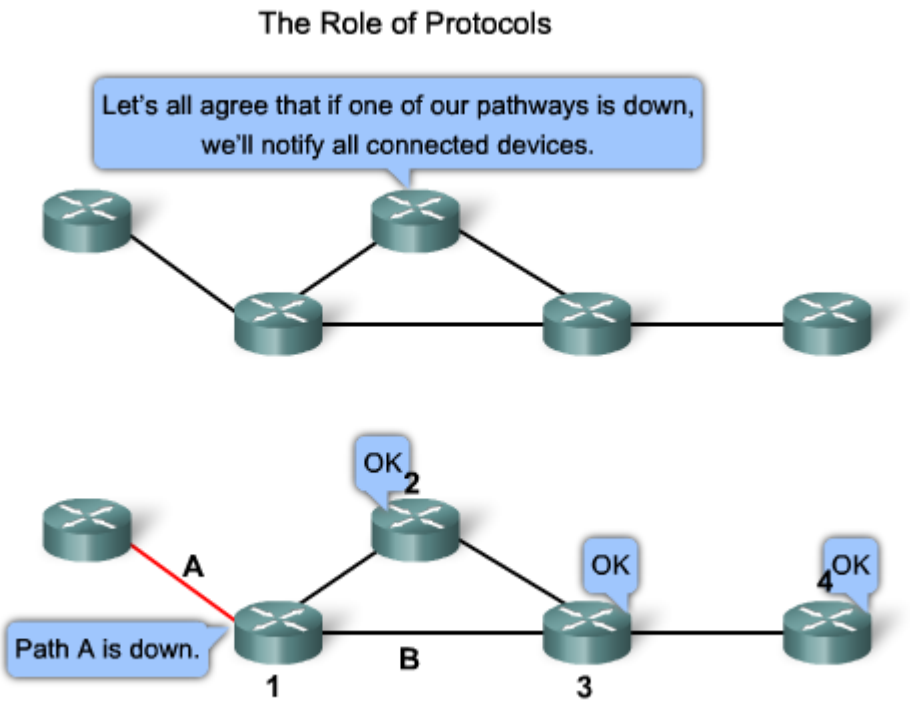
Function of Protocol in Network Communication

- A protocol is a set of predetermined rules
- The protocols are viewed as a layered hierarchy, with each higher level services depending on the functionality defined by the protocols shown in the lower levels



Function of Protocol in Network Communication

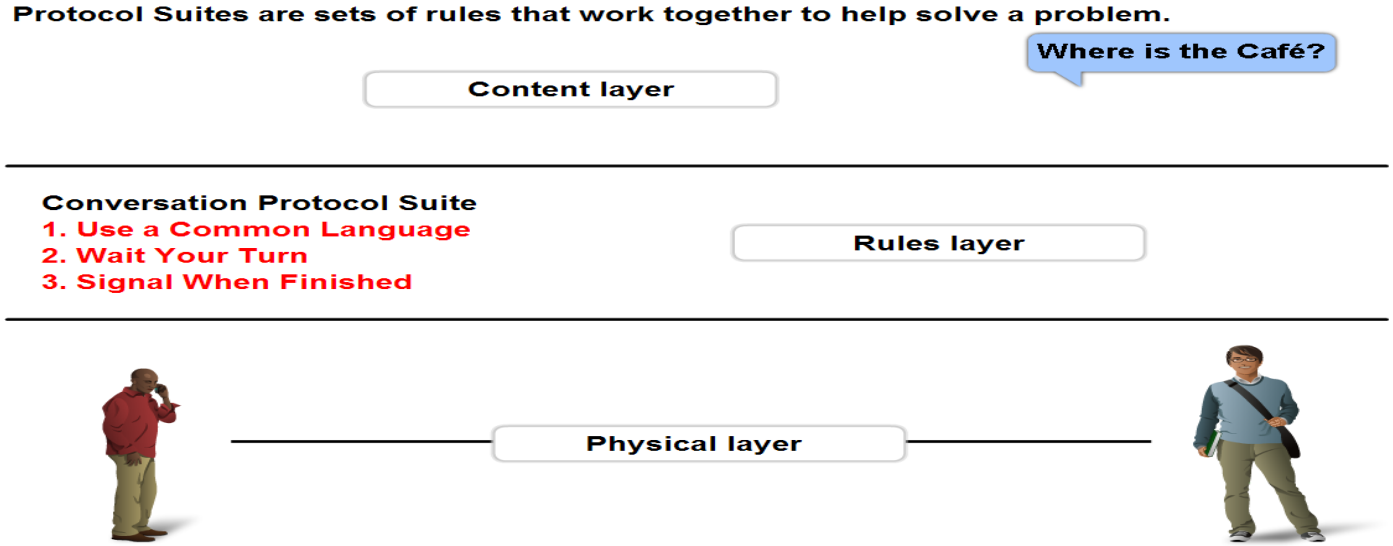
- Network protocols are used to allow devices to communicate successfully



The process by which networking devices share information about pathways to other networks

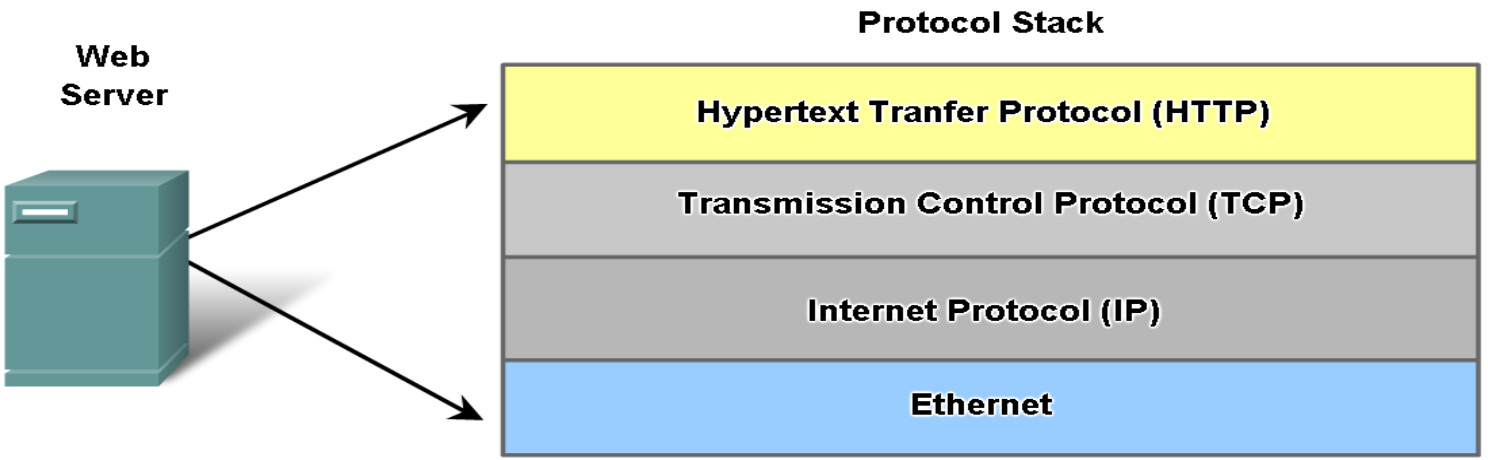
Function of Protocol in Network Communication

- A standard is a process or protocol that has been endorsed by the networking industry and ratified by a standards organization
- The use of standards in developing and implementing protocols ensures that products from different manufacturers can work together for efficient communications.



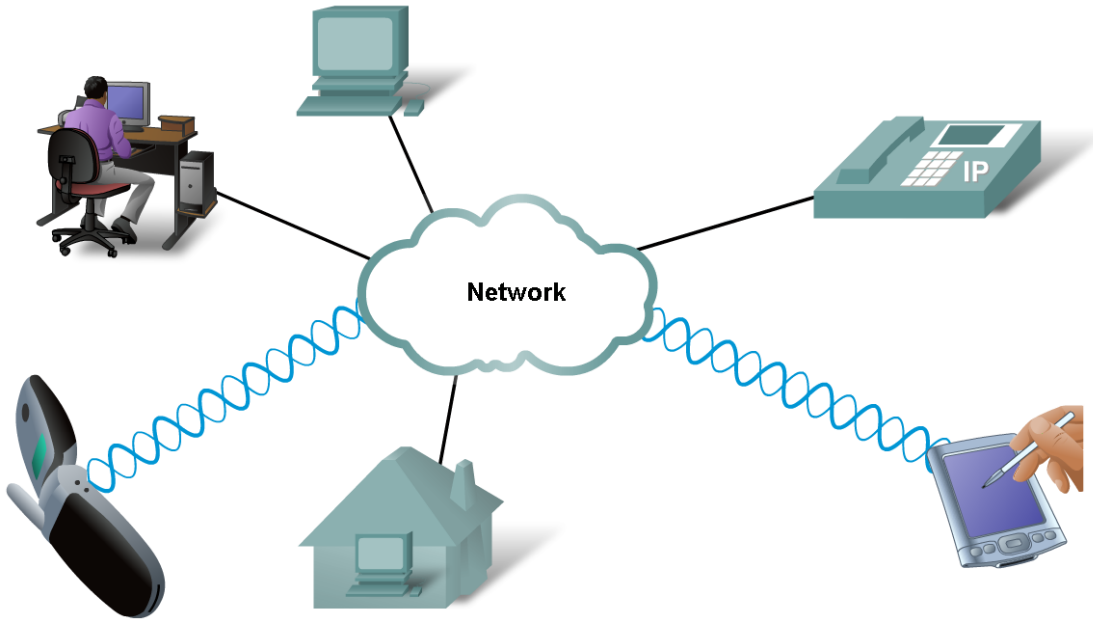
Function of Protocol in Network Communication

- An example of the use of a protocol suite in network communications is the interaction between a web server and a web browser.
- This interaction uses a number of protocols and standards in the process of exchanging information between them.



Function of Protocol in Network Communication

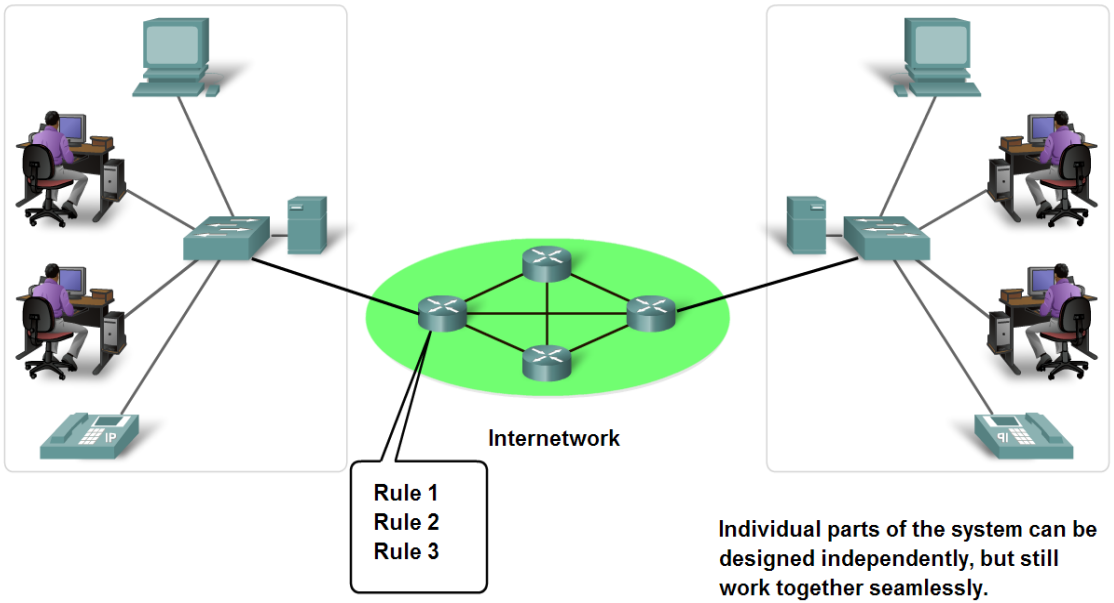
- Technology independent Protocols
  - Many diverse types of devices can communicate using the same sets of protocols
  - This is because protocols specify network functionality, not the underlying technology to support this functionality



Layers with TCP/IP and OSI Model

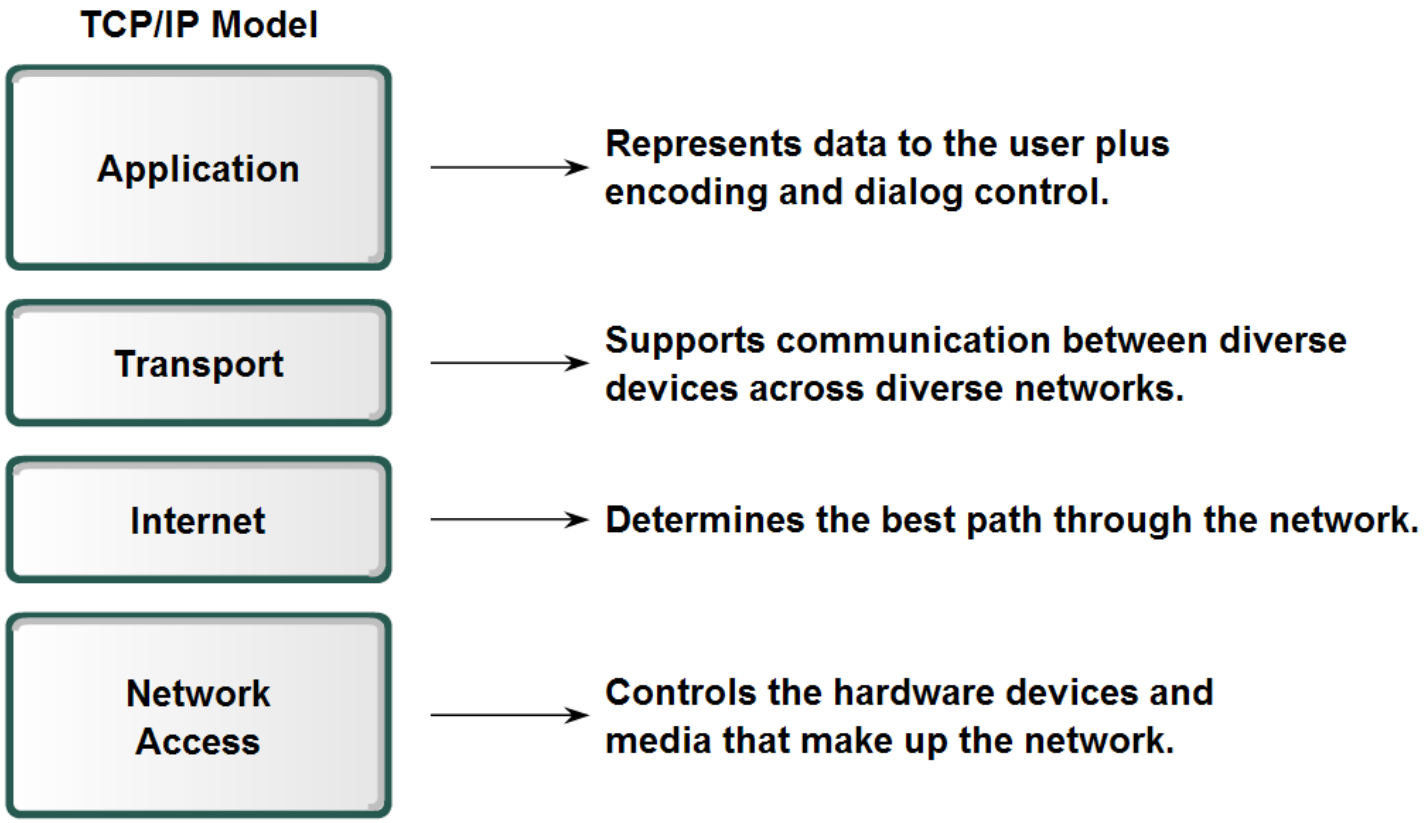
- Benefits of using a layered model to describe network protocols and operations. Using a layered model:
  - Assists in protocol design.
  - Fosters competition because products from different vendors can work together.
  - Changes in one layer do not affect other layer.
  - Provides a common language

Using a layered model helps in the design of complex, multi-use, multi-vendor networks.



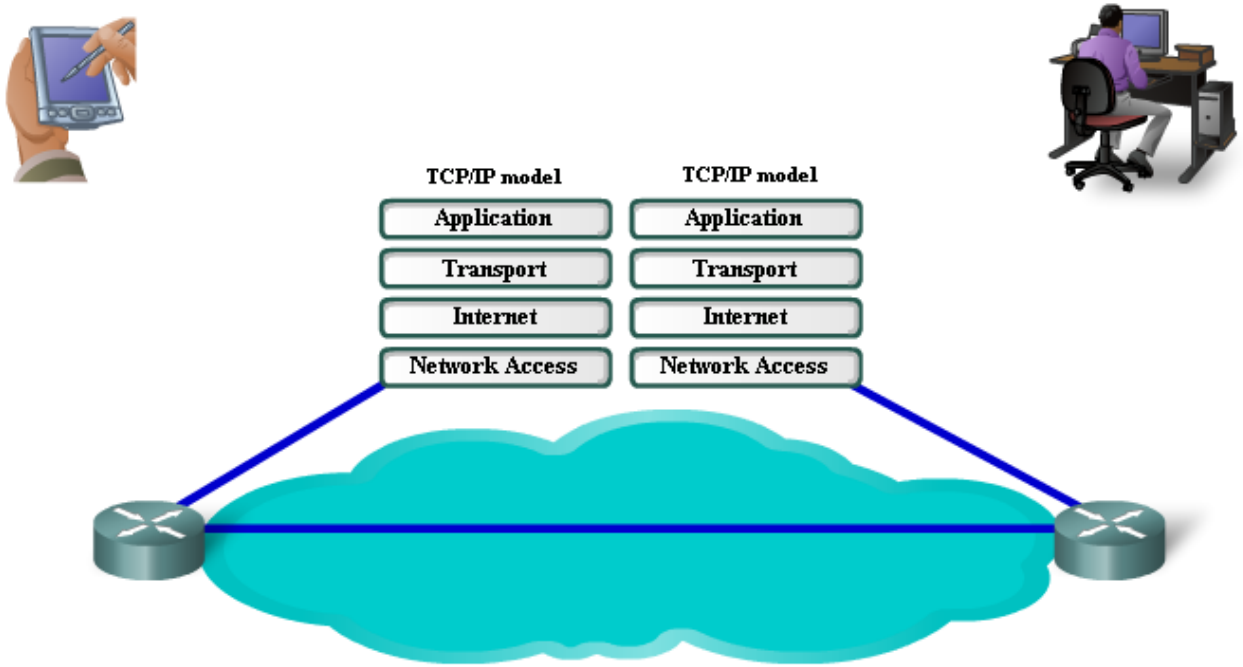
Layers with TCP/IP and OSI Model

- The first layered protocol model for internetwork communications was created in the early 1970s and is referred to as the Internet model



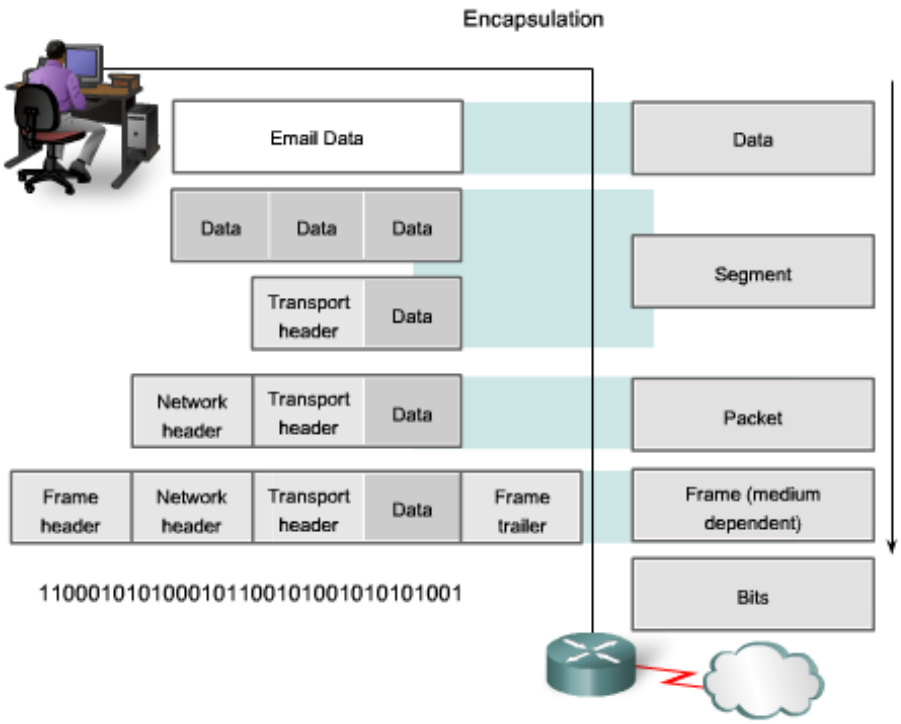
Layers with TCP/IP and OSI Model

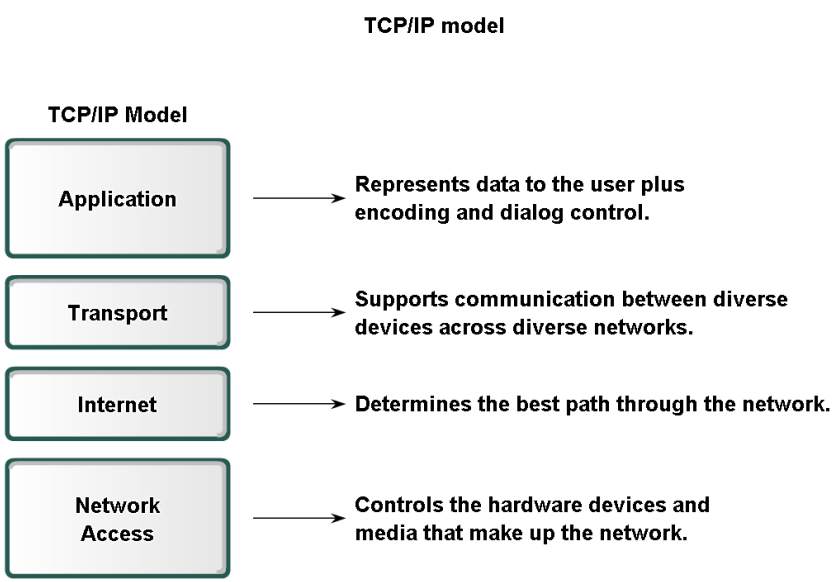
- The TCP/IP model describes the functionality of the protocols that make up the TCP/IP protocol suite. These protocols, which are implemented on both the sending and receiving hosts, interact to provide end-to-end delivery of applications over a network



Layers with TCP/IP and OSI Model

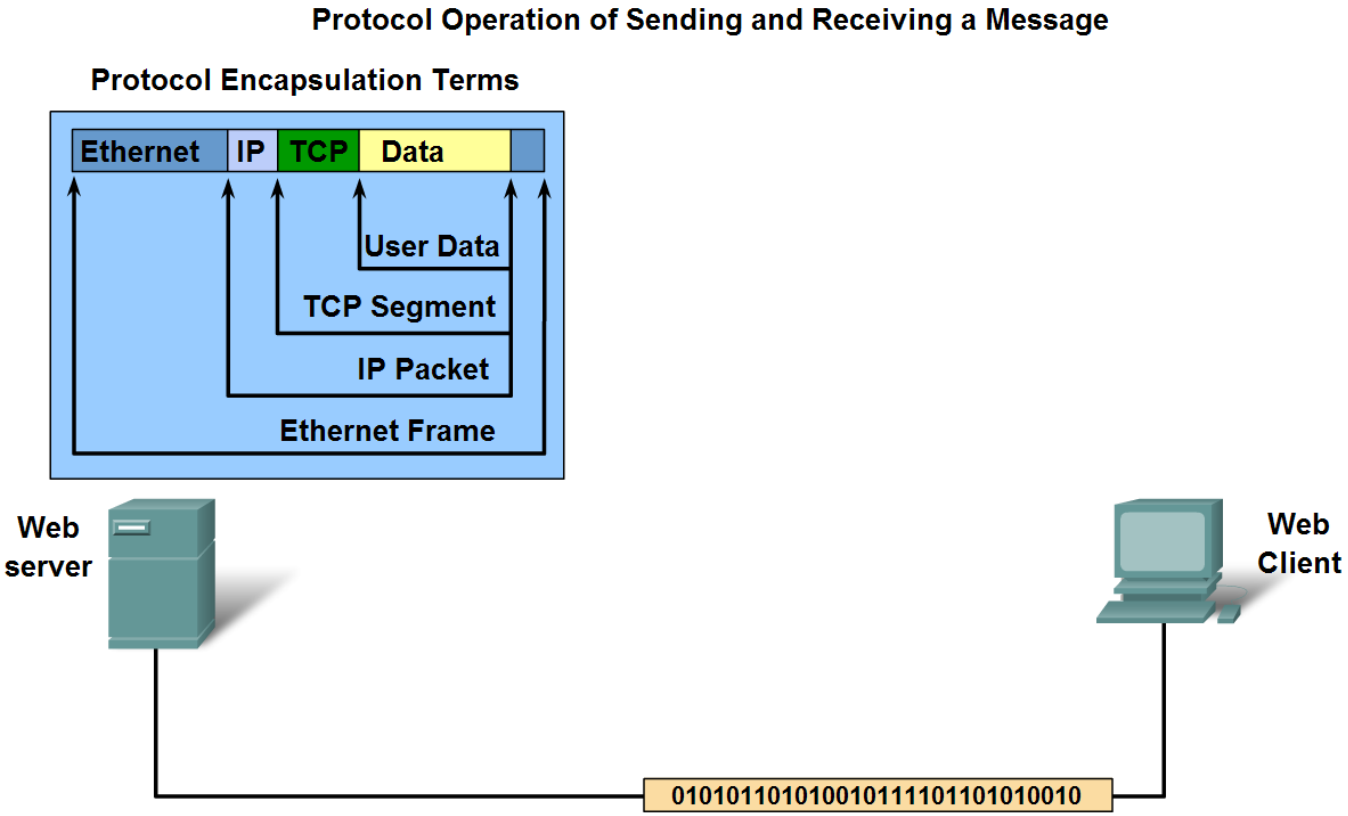
- Encapsulation process: application data is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level
- The form that a piece of data takes at any layer is called a Protocol Data Unit (PDU).





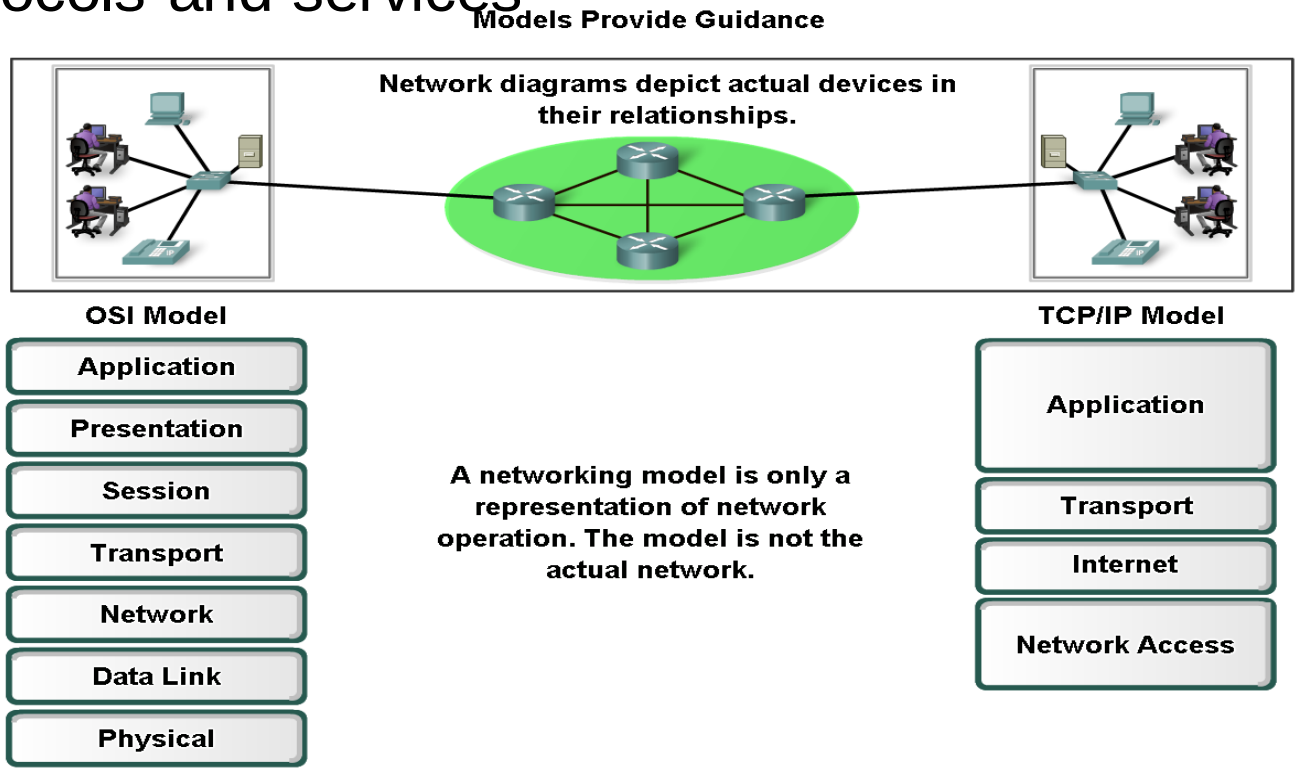
Layers with TCP/IP and OSI Model

- Describe the process of sending and receiving messages



Layers with TCP/IP and OSI Model

- A protocol model provides a model that closely matches the structure of a particular protocol suite
- A reference model provides a common reference for maintaining consistency within all types of network protocols and services

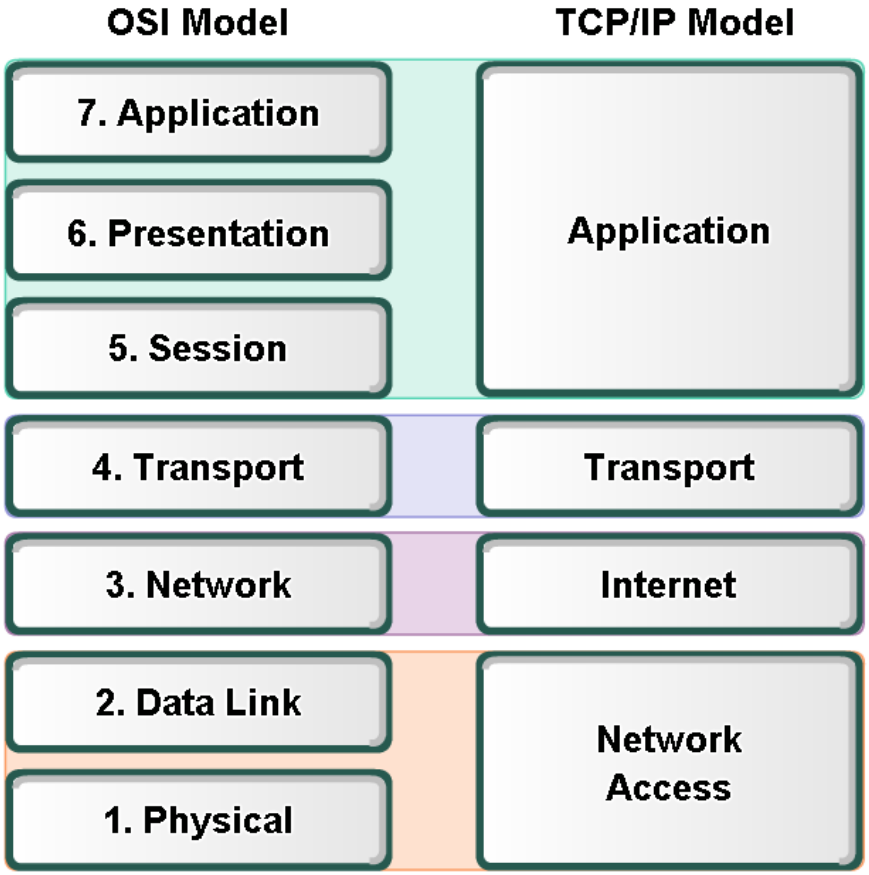


Layers with TCP/IP and OSI Model

- Initially the OSI model was designed by the International Organization for Standardization (ISO) to provide a framework on which to build a suite of open systems protocols.

Layers with TCP/IP and OSI Model

- Compare OSI and TCP/IP model



The key parallels are in the Transport and Network layers.

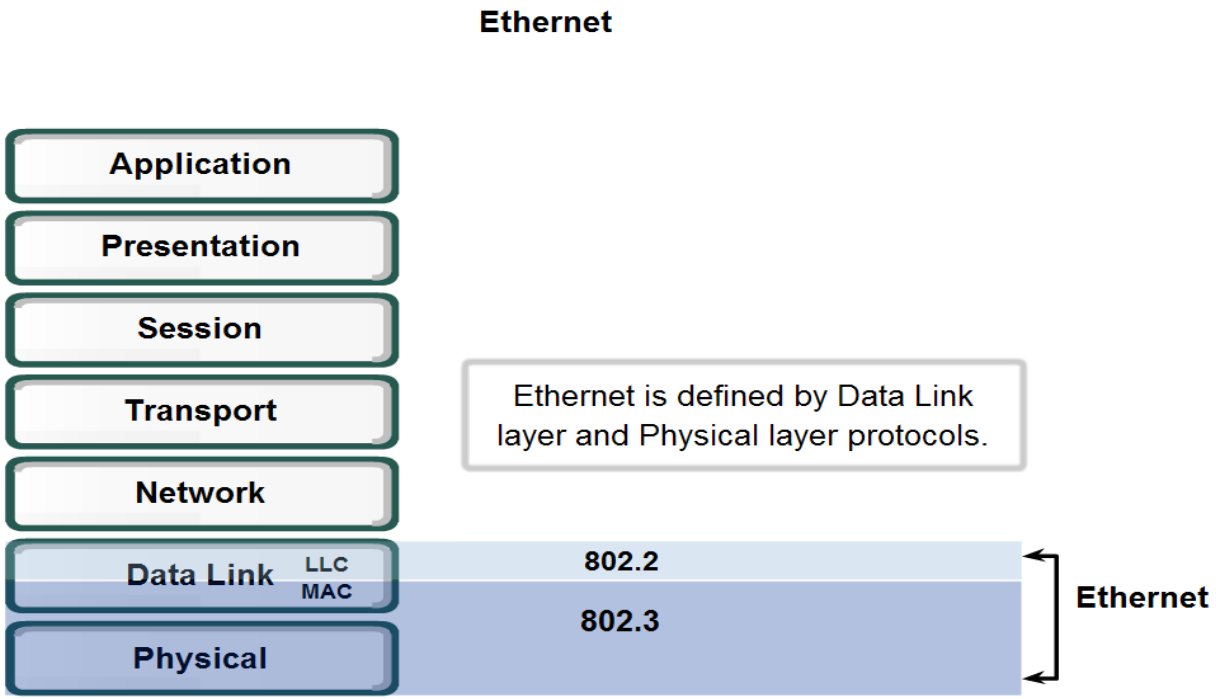
Network Fundamentals Review

Network Devices

Cisco | Networking Academy®
Mind Wide Open™

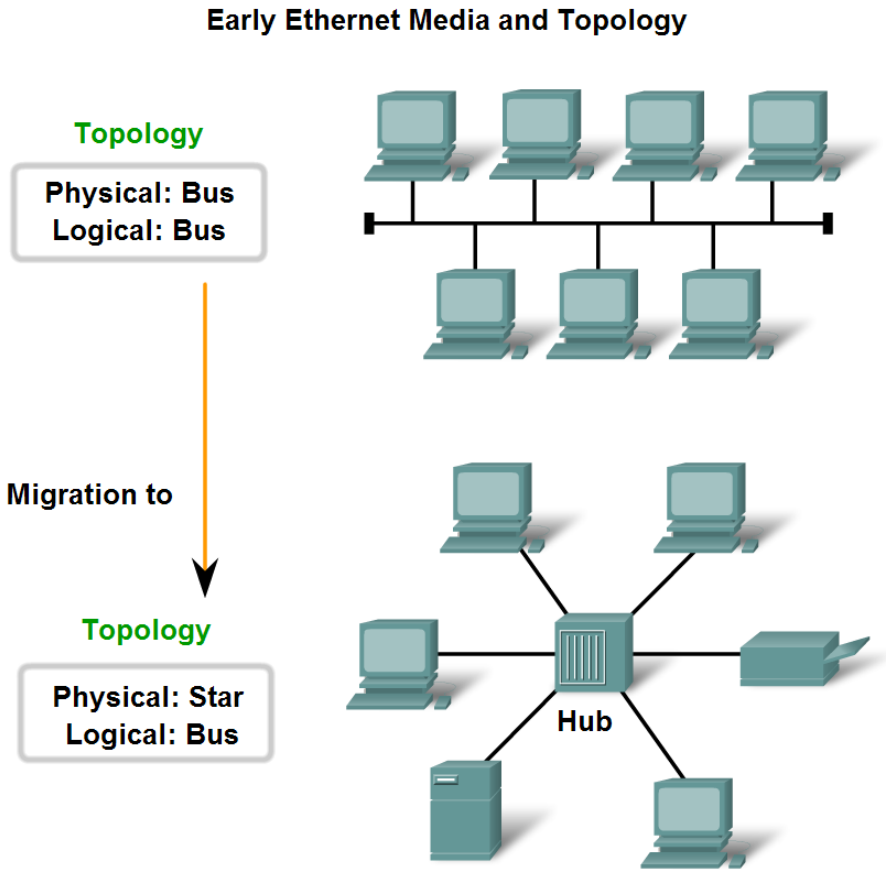
Ethernet

Ethernet is a family of frame-based computer networking technologies for local area networks (LAN). It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and a variety of Medium Access Control procedures at the lower part of the Data Link Layer

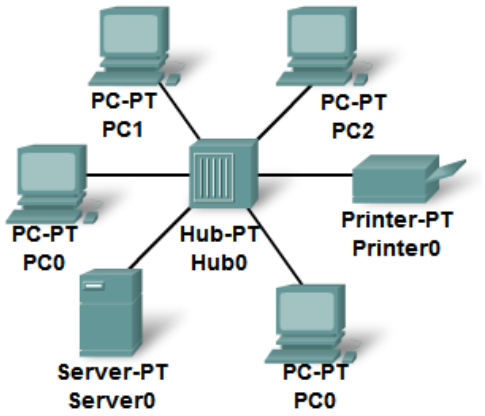


Characteristics of Network Media used in Ethernet

- Identify several characteristics of Ethernet in its early years



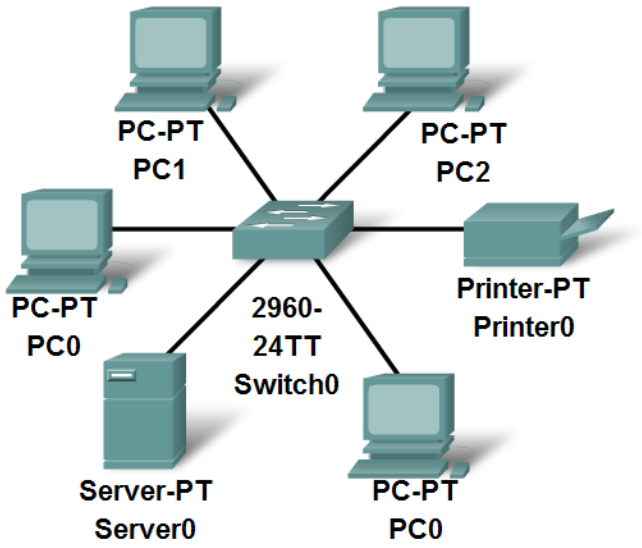
Ethernet Collision



- In 10BASE-T networks, typically using a hub. This created a shared media. Only one station could successfully transmit at a time: half-duplex
- More devices, more collisions.
- Using CSMA/CD to manage collisions, with little or no impact on performance. As the number of devices and subsequent data traffic increase, however, the rise in collisions can have a significant impact on the user's experience communication

Characteristics of Network Media used in Ethernet

Migration to Ethernet Switches

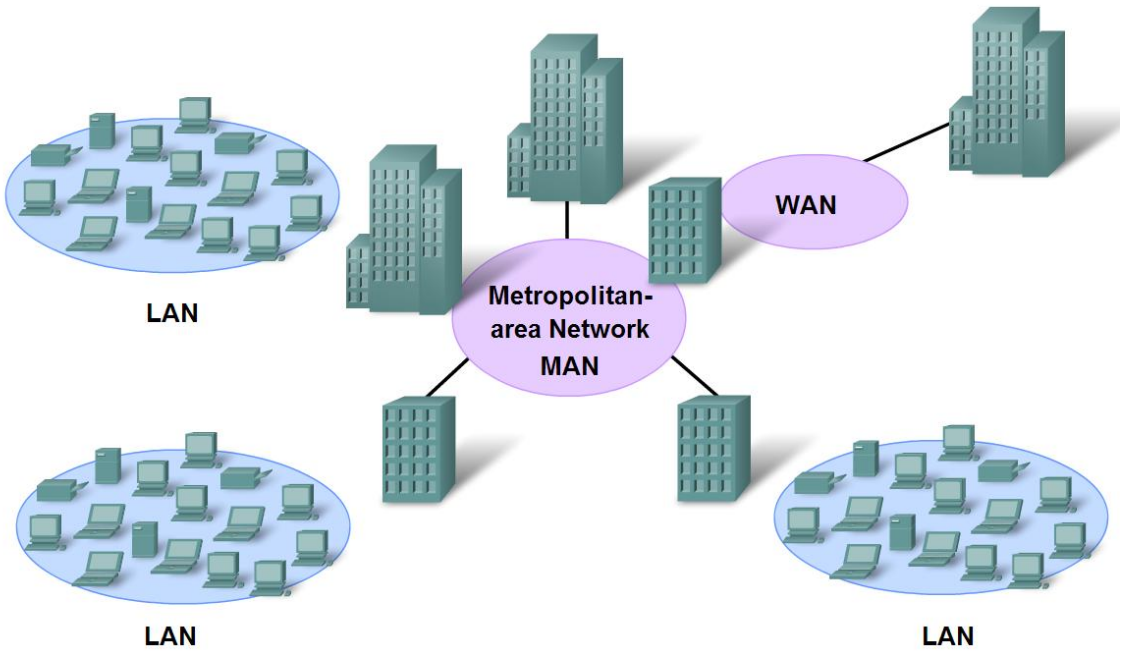


Characteristics of Network Media used in Ethernet

- The increased cabling distances enabled by the use of fiber-optic cable in Ethernet-based networks has resulted in a blurring of the distinction between LANs and WANs. Ethernet was initially limited to LAN cable systems within single buildings, and then extended to between buildings. It can now be applied across a city in what is known as a Metropolitan Area Network (MAN).

Gigabit Ethernet

Gigabit Ethernet technology is applied beyond the enterprise LAN to MAN and WAN-based networks.



Physical and Data Link Features of Ethernet

- Media Access Control (MAC)

MAC—Getting Data to the Media

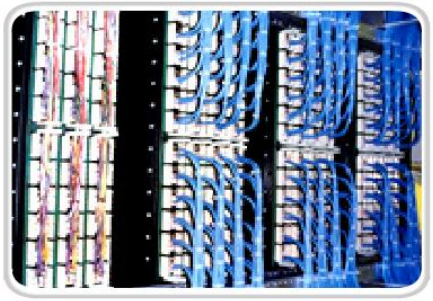
MEDIA ACCESS CONTROL

- Data Encapsulation
  - Frame delimiting
  - Addressing
  - Error detection
- Media Access Control
  - Control of frame placement on and off the media
  - media recovery

Physical and Data Link Features of Ethernet

- Physical Implementations of the Ethernet

Physical Devices Implementing Ethernet



UTP patch panels in a rack

Ethernet switches

Ethernet fiber connectors

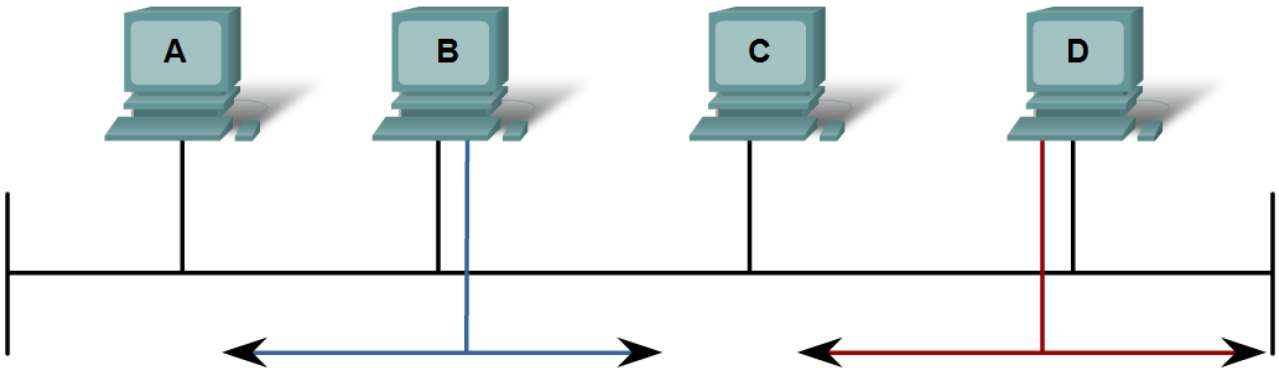
Ethernet switch

Function and Characteristics of the Media Access Control Method

- MAC in Ethernet

Media Access Control in Ethernet

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



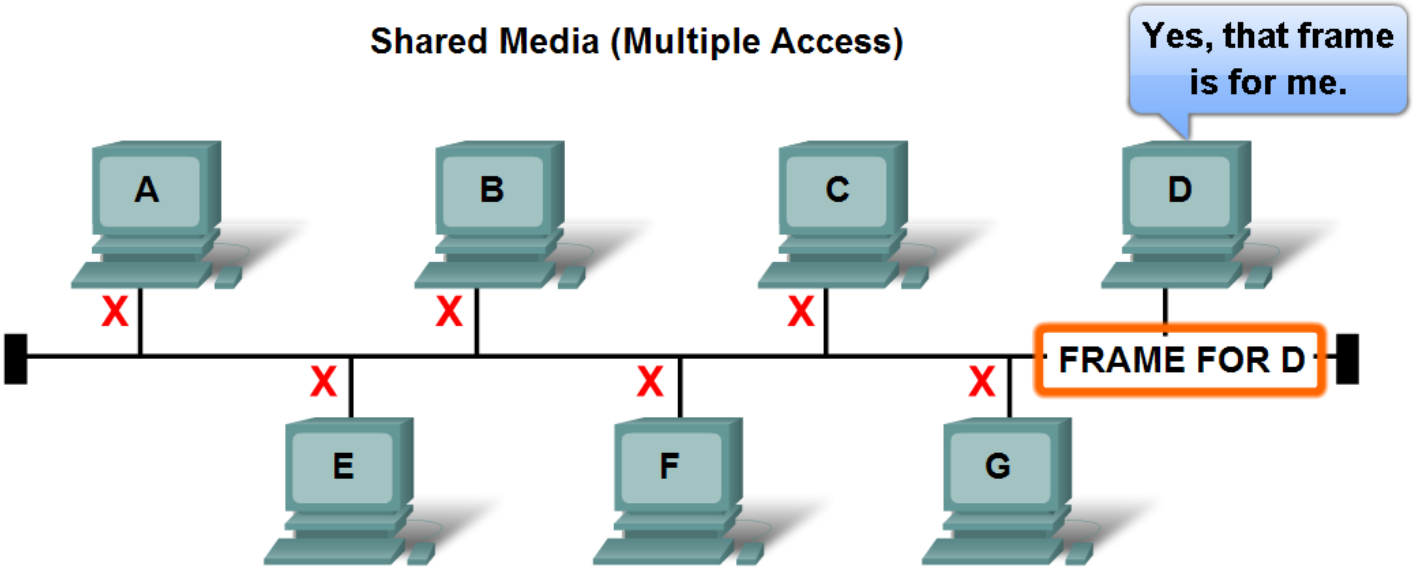
CSMA/CD controls access to the shared media. If there is a collision, it is detected and frames are retransmitted.

Layer 2 Addressing and Its Impact on Network Operation and Performance

- The Ethernet MAC Address

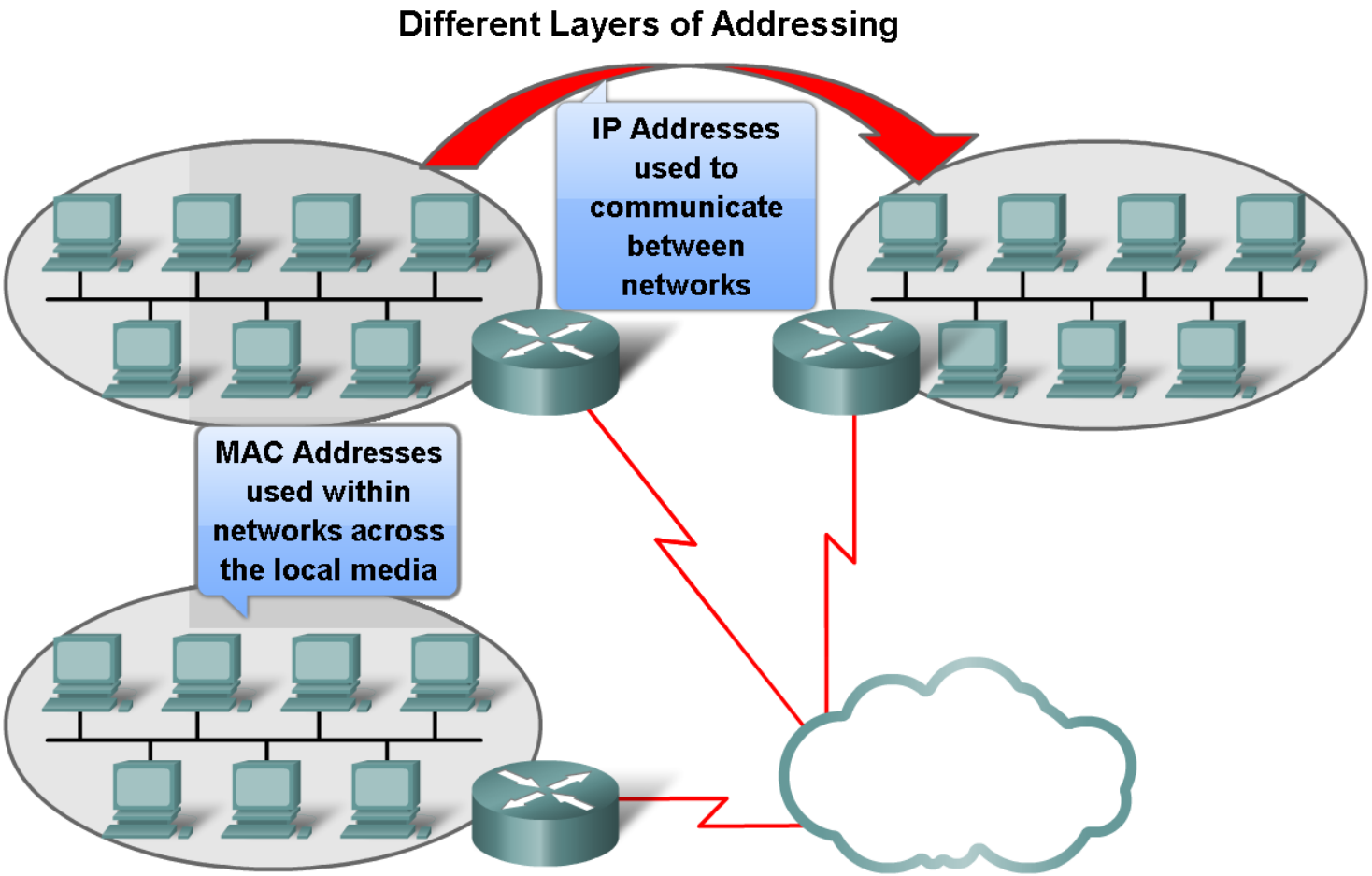
The MAC Address—Addressing in Ethernet

All Ethernet nodes share the media.
To receive the data sent to it, each node needs a unique address.



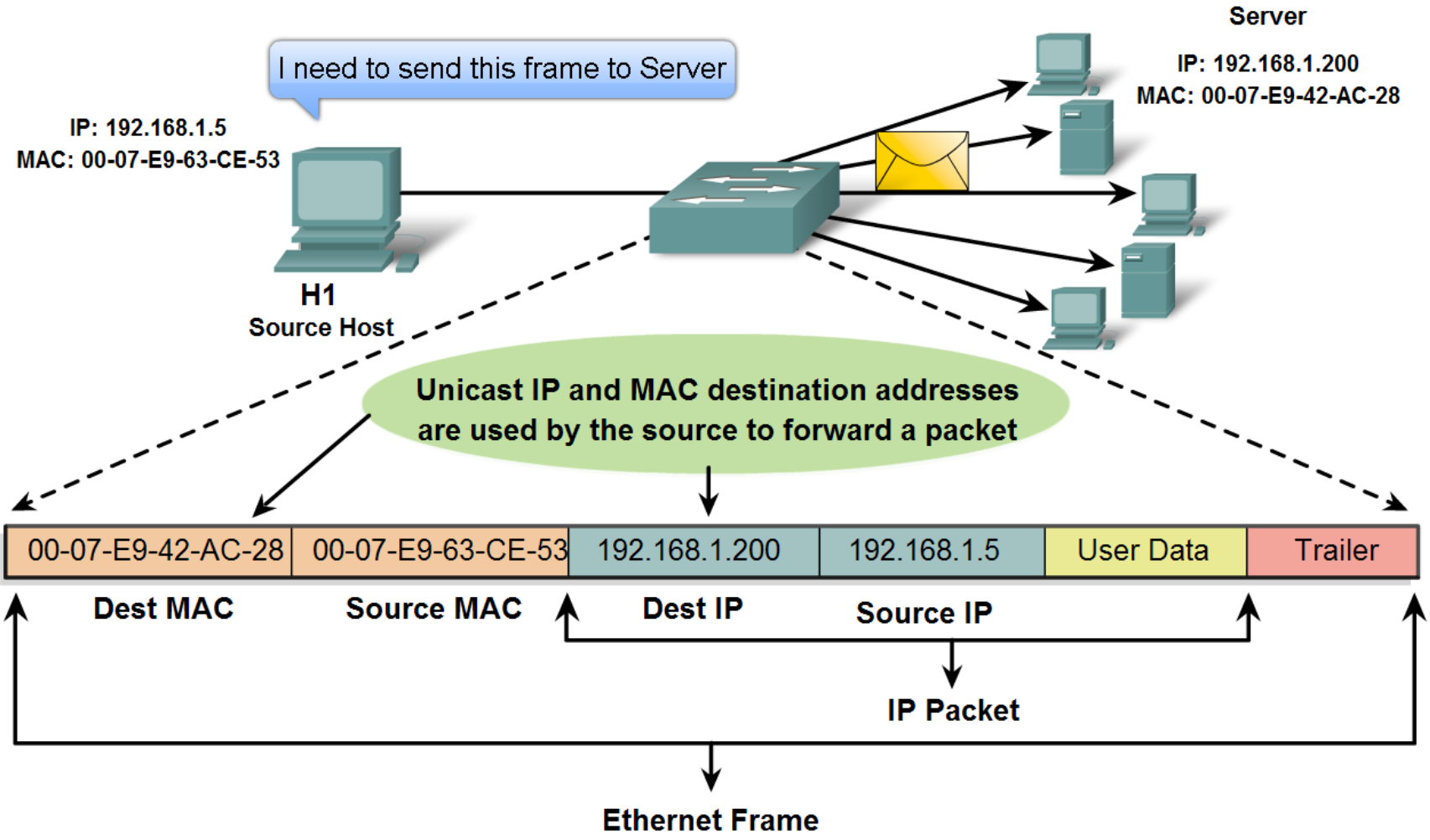
Layer 2 Addressing and Its Impact on Network Operation and Performance

- Another Layer of Addressing



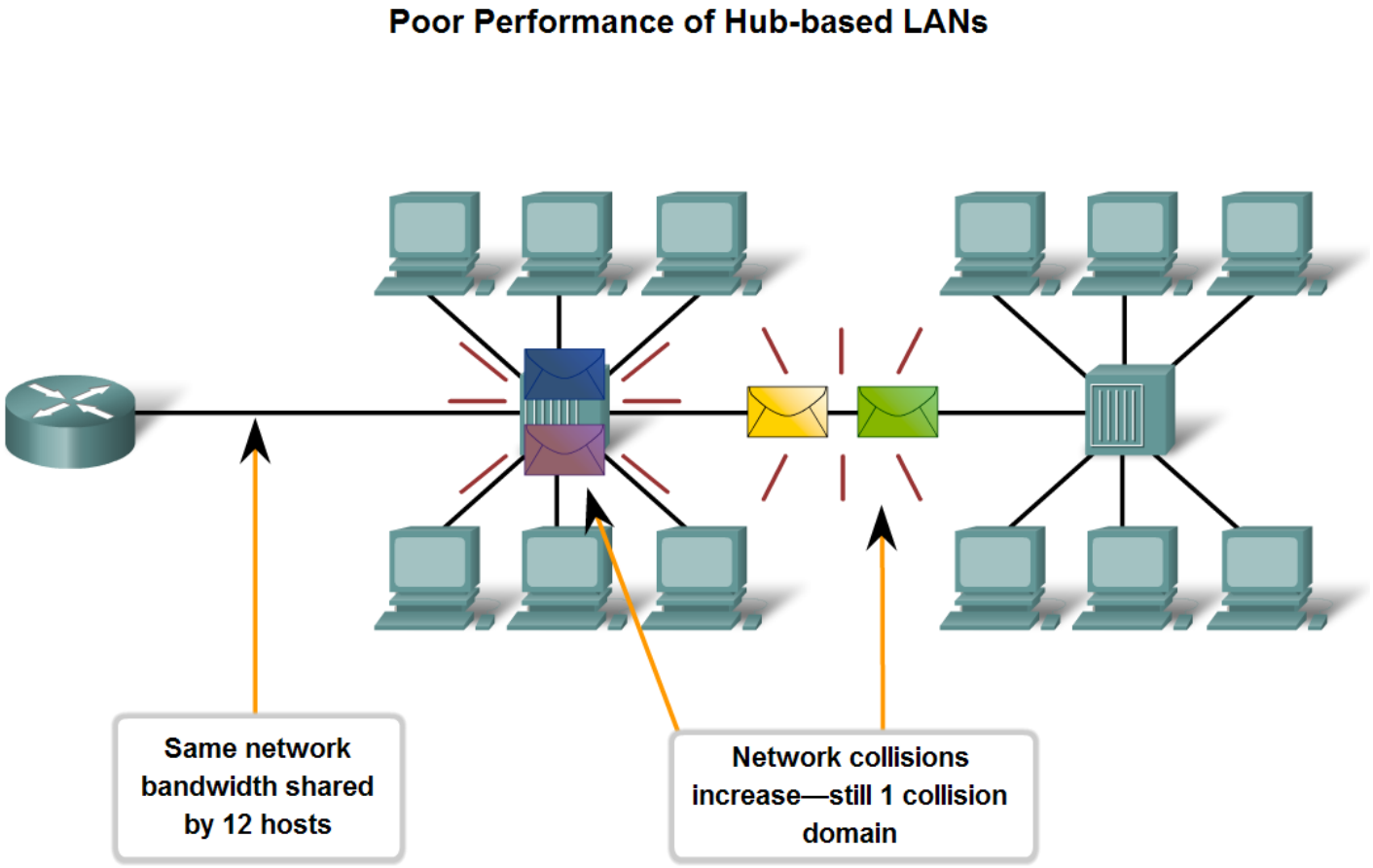
Layer 2 Addressing and Its Impact on Network Operation and Performance

- Ethernet Unicast, Multicast and Broadcast



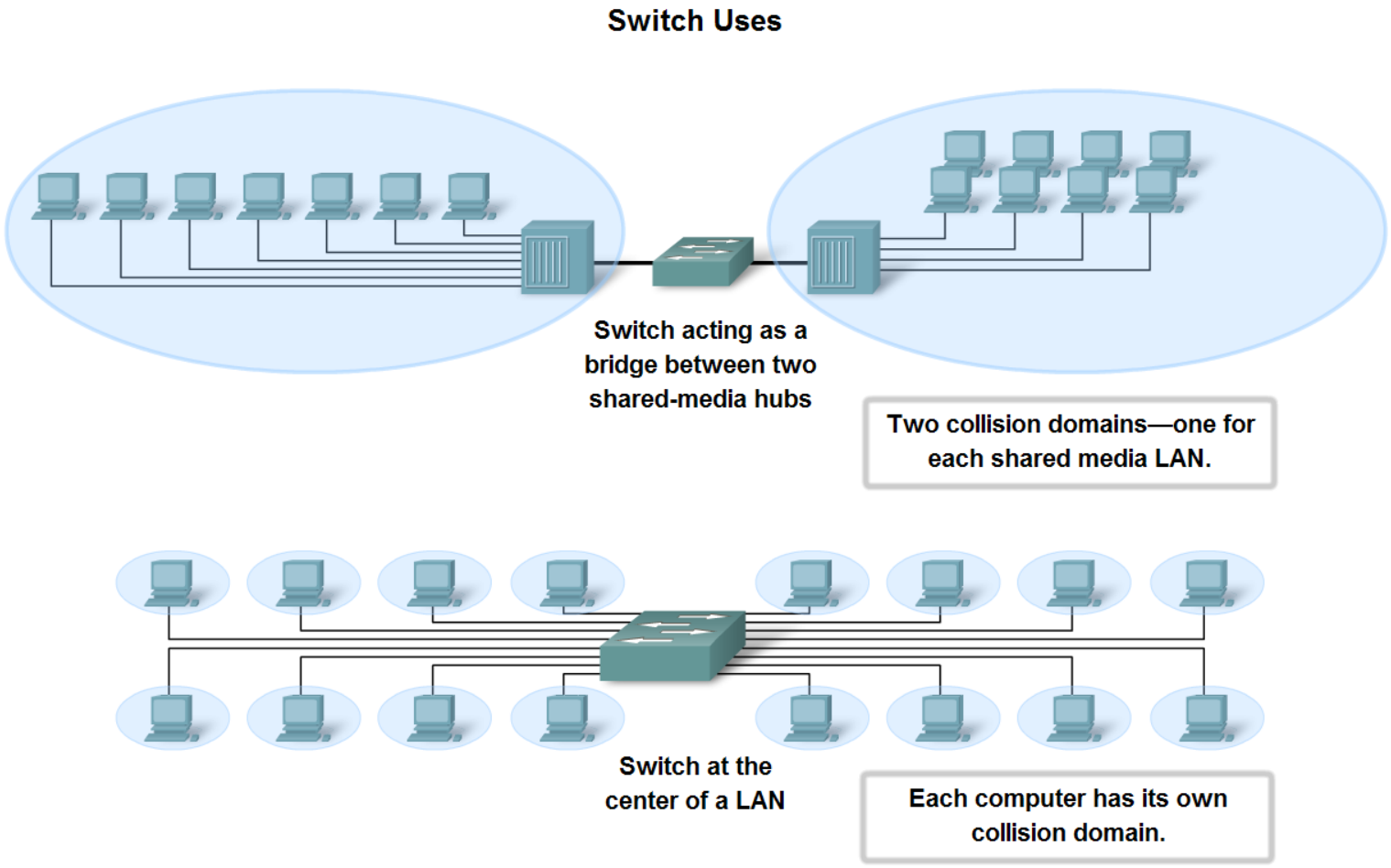
Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN

- Legacy Ethernet – Using Hubs



Compare and Contrast the Use of Ethernet Switches versus Hubs in a LAN

- Ethernet – Using Switches

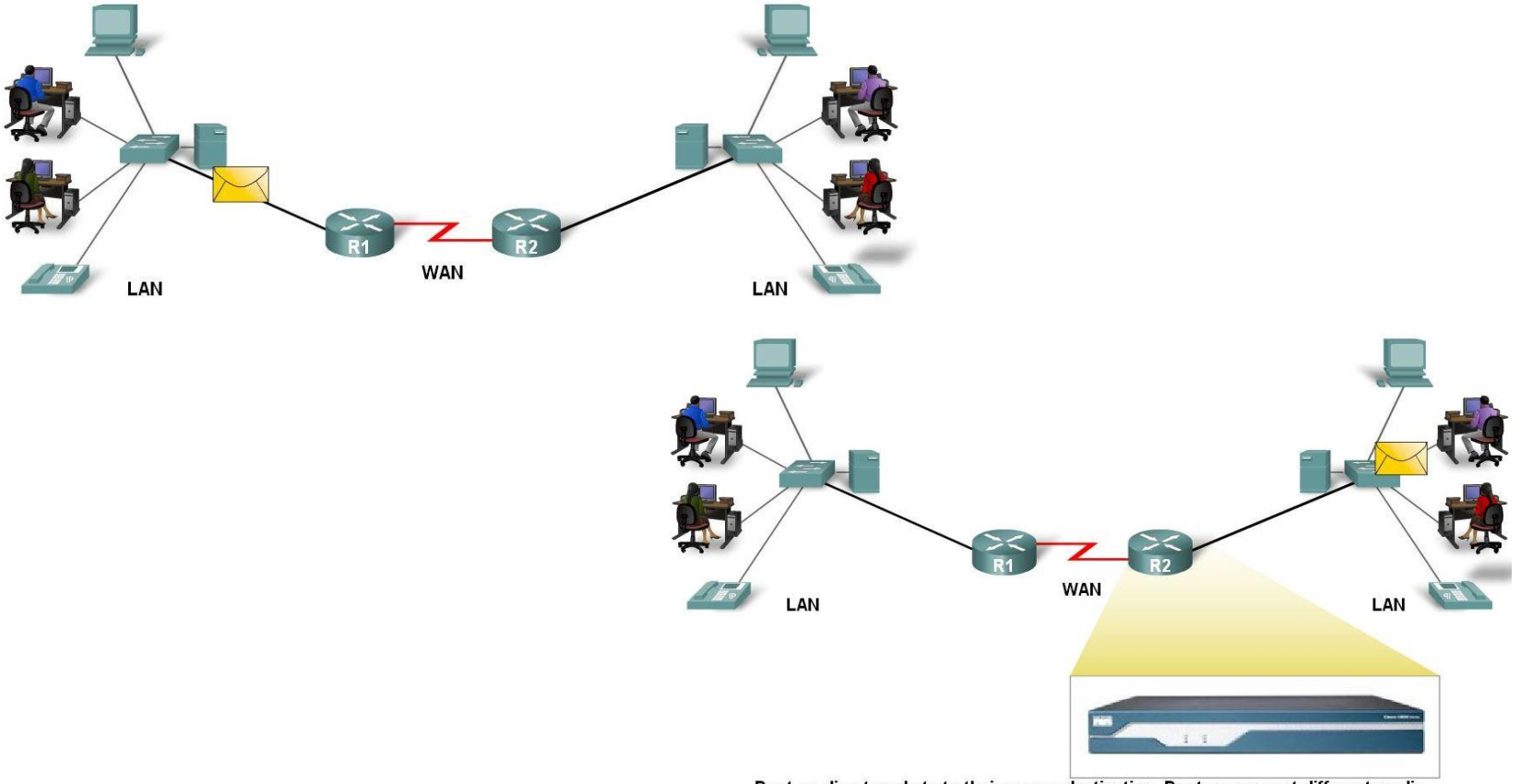


Router as a Computer

- Describe the basic purpose of a router
  - Computers that specialize in sending packets over the data network
  - They are responsible for interconnecting networks by selecting the best path for a packet to travel and forwarding packets to their destination
- Routers are the network center
  - Routers generally have 2 connections:
    - WAN connection (Connection to ISP)
    - LAN connection

Router as a Computer

- Data is sent in form of packets between 2 end devices
- Routers are used to direct packet to its destination



Routers direct packets to their proper destination. Routers connect different media.

Router as a Computer

- Router components and their functions:
  - CPU - Executes operating system instructions
  - Random access memory (RAM) - Contains the running copy of configuration file. Stores routing table. RAM contents lost when power is off.
  - Read-only memory (ROM) - Holds diagnostic software used when router is powered up. Stores the router's bootstrap program.
  - Non-volatile RAM (NVRAM) - Stores startup configuration. This may include IP addresses (Routing protocol, Hostname of router).
  - Flash memory - Contains the operating system (Cisco IOS).
  - Interfaces - There exist multiple physical interfaces that are used to connect network. Examples of interface types:
    - Ethernet / fast Ethernet interfaces
    - Serial interfaces
    - Management interfaces

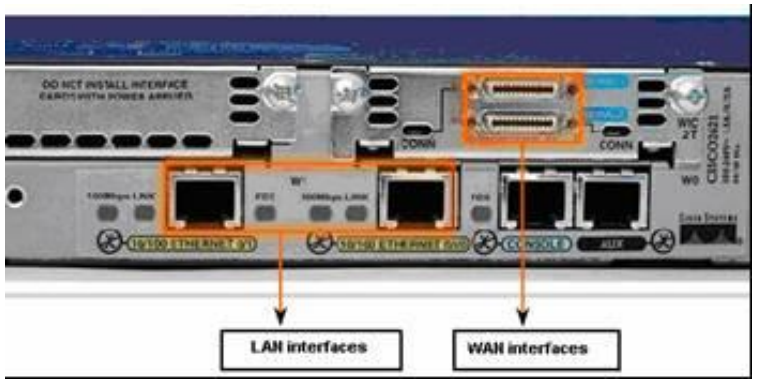
Router as a Computer

- Router Interface is a physical connector that enables a router to send or receive packets
- Each interface connects to a separate network
- Consist of socket or jack found on the outside of a router
- Types of router interfaces:
  - Ethernet
  - Fastethernet
  - Serial
  - DSL
  - ISDN
  - Cable

Each individual interface connects to a different network. Thus each interface has an IP address/mask from that network.

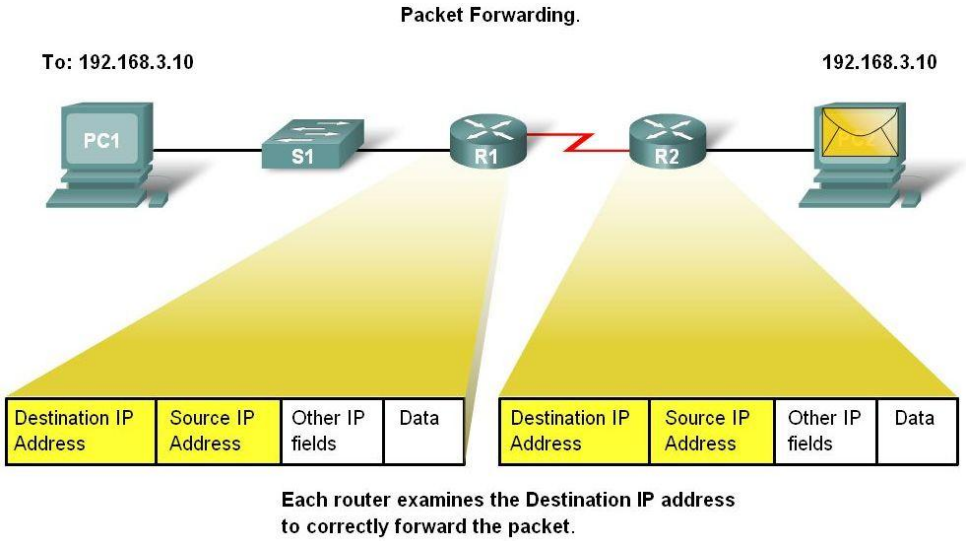
Router as a Computer

- Two major groups of Router Interfaces
  - LAN Interfaces
    - Are used to connect router to LAN network
    - Has a layer 2 MAC address
    - Can be assigned a Layer 3 IP address
    - Usually consist of an RJ-45 jack
  - WAN Interfaces
    - Are used to connect routers to external networks that interconnect LANs
    - Depending on the WAN technology, a layer 2 address may be used
    - Uses a layer 3 IP address



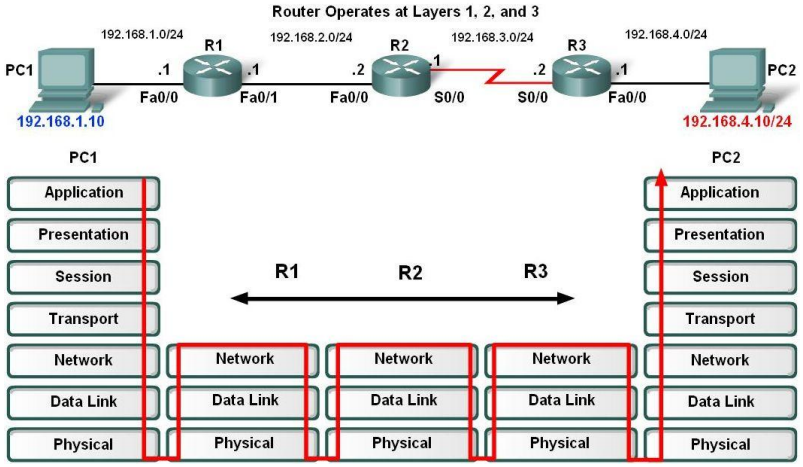
Router as a Computer

- Routers and the Network Layer
  - Routers use destination IP address to forward packets
    - The path a packet takes is determined after a router consults information in the routing table
    - After router determines the best path
    - Packet is encapsulated into a frame
    - Frame is then placed on network medium in form of Bits



Router as a Computer

- Routers Operate at Layers 1, 2 & 3
  - Router receives a stream of encoded bits
  - Bits are decoded and passed to layer 2
  - Router de-encapsulates the frame
  - Remaining packet passed up to layer 3
    - Routing decision made at this layer by examining destination IP address
  - Packet is then re-encapsulated & sent out outbound interface



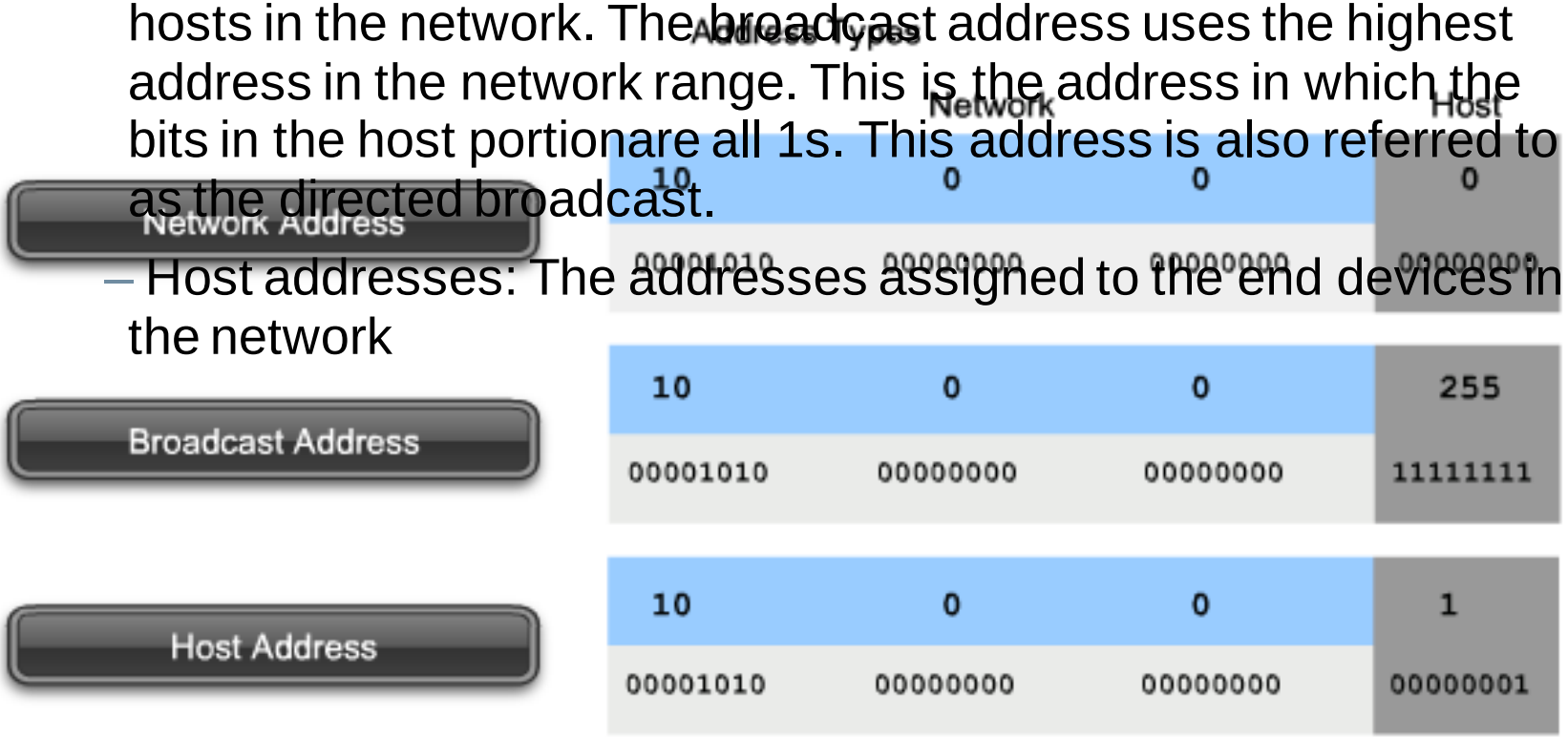
Network Fundamentals Review

Addressing

Cisco | Networking Academy®
Mind Wide Open™

Classify and Define IPv4 Addresses

- Three types of addresses:
  - Network address: The address by which we refer to the network. All hosts in a network will have the same network bits.
  - Broadcast address: A special address used to send data to all hosts in the network. The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portionare all 1s. This address is also referred to as the directed broadcast.
  - Host addresses: The addresses assigned to the end devices in the network



Classify and Define IPv4 Addresses

Address Types

	Network		Host
Network Address	10	0	0	0
	00001010	00000000	00000000	00000000
Broadcast Address	10	0	0	255
	00001010	00000000	00000000	11111111
Host Address	10	0	0	1
	00001010	00000000	00000000	00000001

Classify and Define IPv4 Addresses

- Determine the network, broadcast and host addresses for a given address and prefix combination

Given address/prefix of **144.83.250.97 /17**

For each row, enter the values for that type of address.

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network	00000000	0	144.83.128.0
Broadcast	11111111	255	144.83.255.255
First Usable Host Address	00000001	1	144.83.128.1
Last Usable Host Address	11111110	254	144.83.255.254

Classify and Define IPv4 Addresses

- Determine the network, broadcast and host addresses for a given address and prefix combination

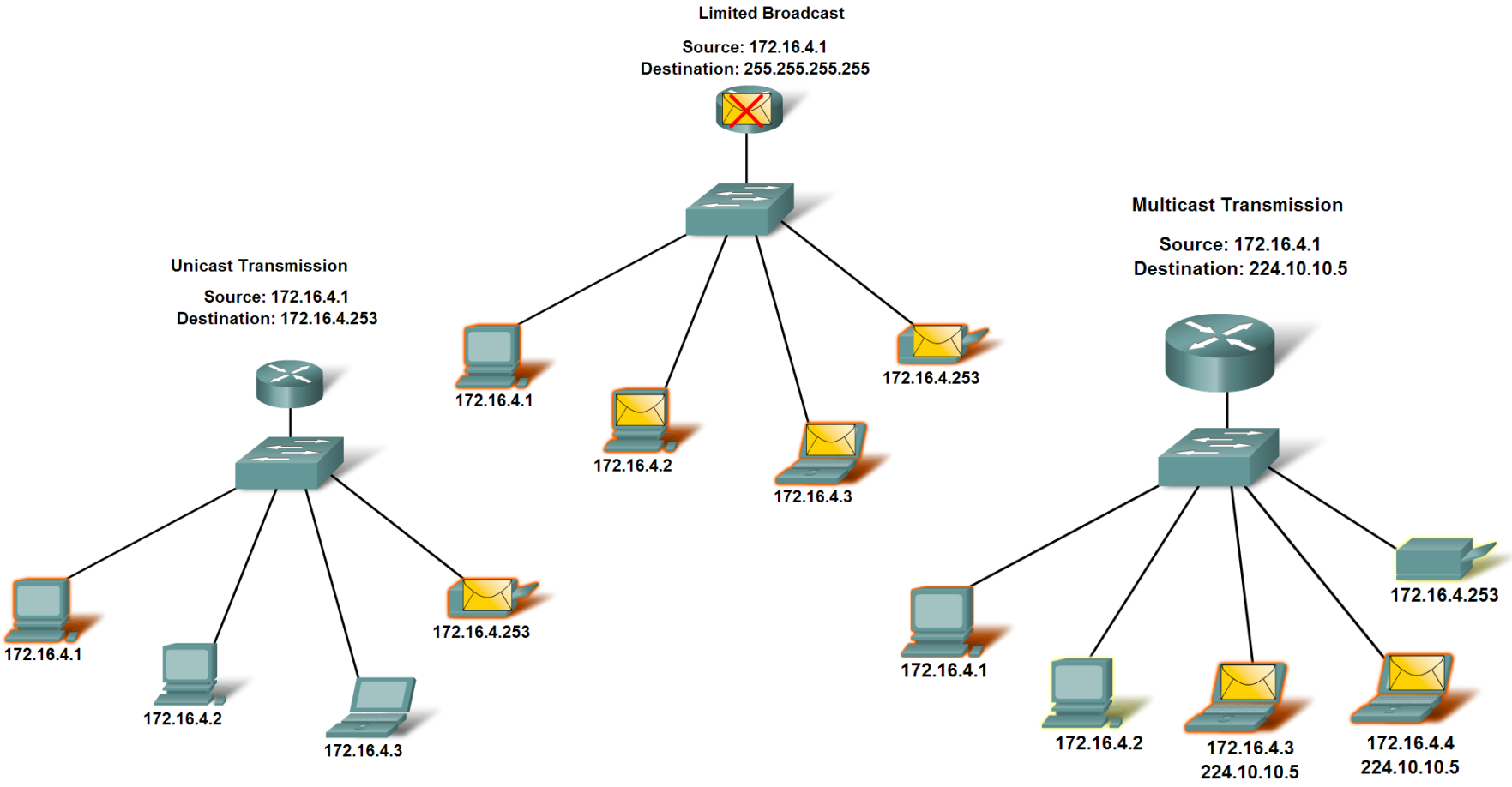
Given address/prefix of **172.16.4.32/28**

For each row, enter the values ...

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network			
Broadcast			
First Usable Host Address			
Last Usable Host Address			

Classify and Define IPv4 Addresses

- Three types of communication in the Network Layer: Unicast, Broadcast, Multicast

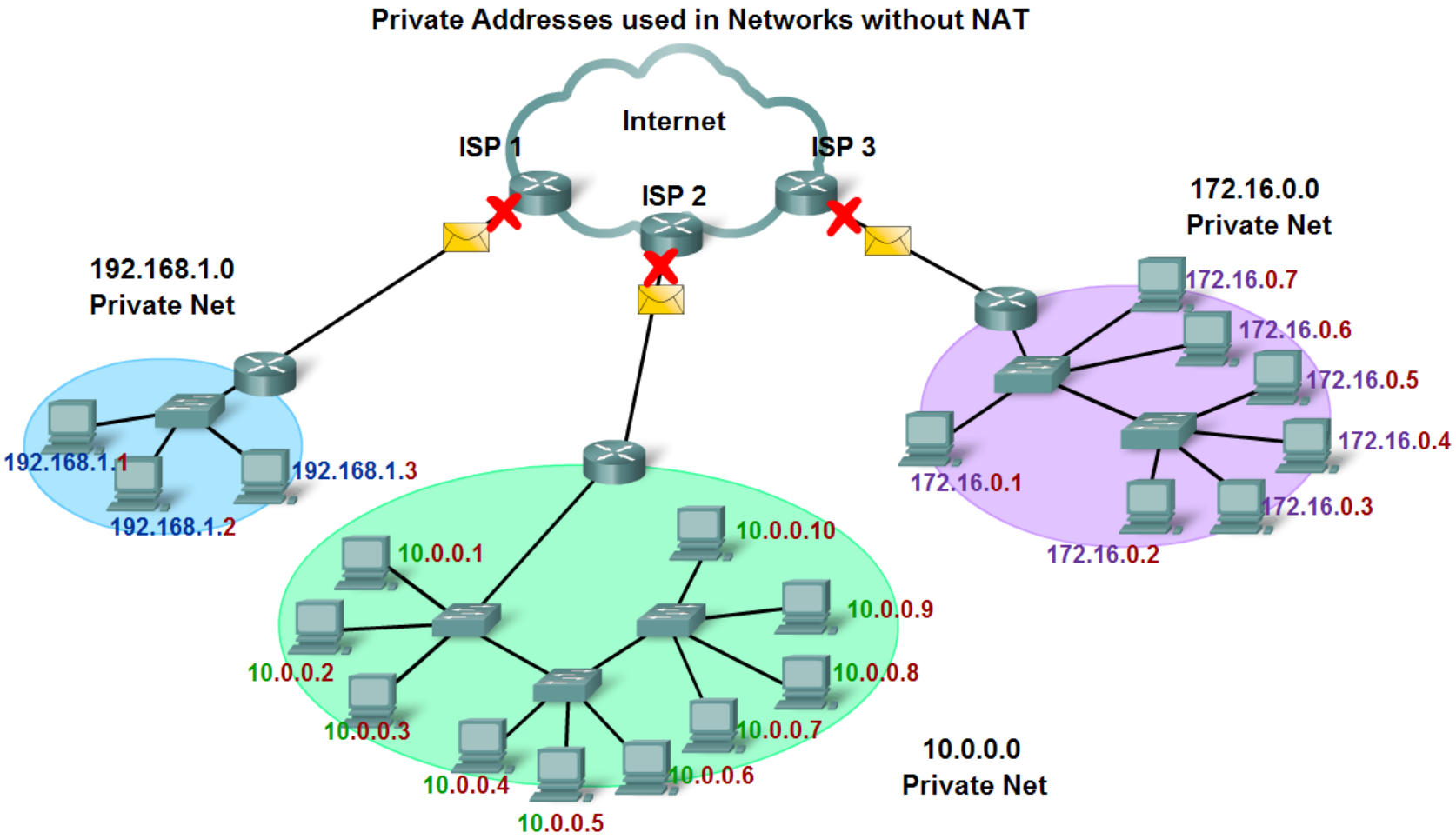


Classify and Define IPv4 Addresses

- **Unicast:**
  - Is used for the normal host-to-host communication in both a client/server and a peer-to-peer network.
  - Uses the host address of the destination device as the destination address and can be routed through an internetwork.
- **Broadcast:**
  - The process of sending a packet from one host to all hosts in the network
  - Host processes a broadcast address destination packet like unicast address.
  - A directed broadcast is sent to all hosts on a specific network.
  - The limited broadcast is used for communication that is limited to the hosts on the local network.
- **Multicast:**
  - The process of sending a packet from one host to a selected group of hosts.
  - Multicast transmission is designed to conserve the bandwidth of the IPv4 network.
  - The multicast clients use services initiated by a client program to subscribe to the multicast group.

Classify and Define IPv4 Addresses

- Define public address and private address



Public and Private addresses

- Private Addresses:are set aside for use in private networks.
  - 10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
  - 172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
  - 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)
- Public Addresses:are designed to be used in the hosts that are publicly accessible from the Internet.
- Network Address Translation (NAT):is used to translate private addresses to public addresses, be implemented on a device at the edge of the private network.

Classify and Define IPv4 Addresses - Legacy IPv4 Addressing

- **Classful addressing:** A company or organization was assigned an entire class A, class B, or class C address block.
- **Limits to the Class-based System**
  - Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses
- **Classless Addressing**
  - Address blocks appropriate to the number of hosts are assigned to companies or organizations without regard to the unicast class

Classify and Define IPv4 Addresses

- Identify the historic method for assigning addresses and the issues associated with the method

IP Address Classes

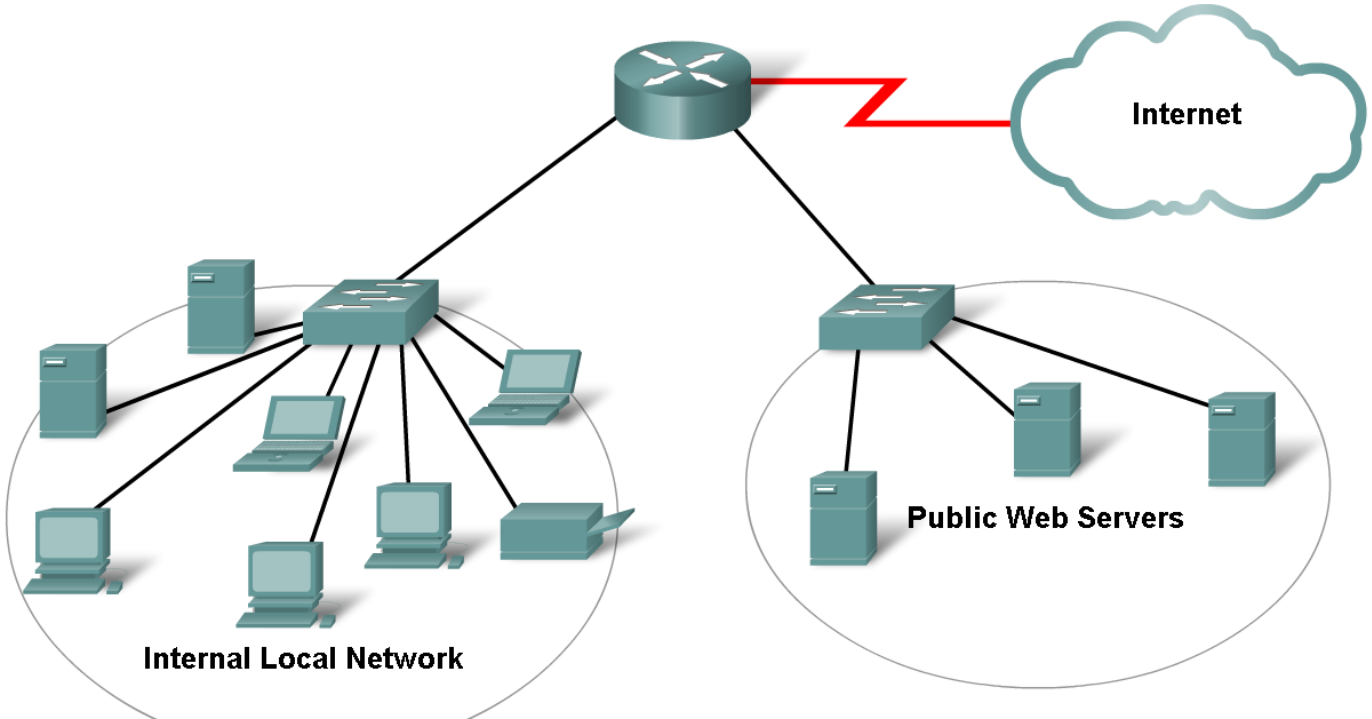
Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Assigning Addresses

- The allocation of these addresses inside the networks should be planned and documented for the purpose of
  - Preventing duplication of addresses
  - Providing and controlling access
  - Monitoring security and performance

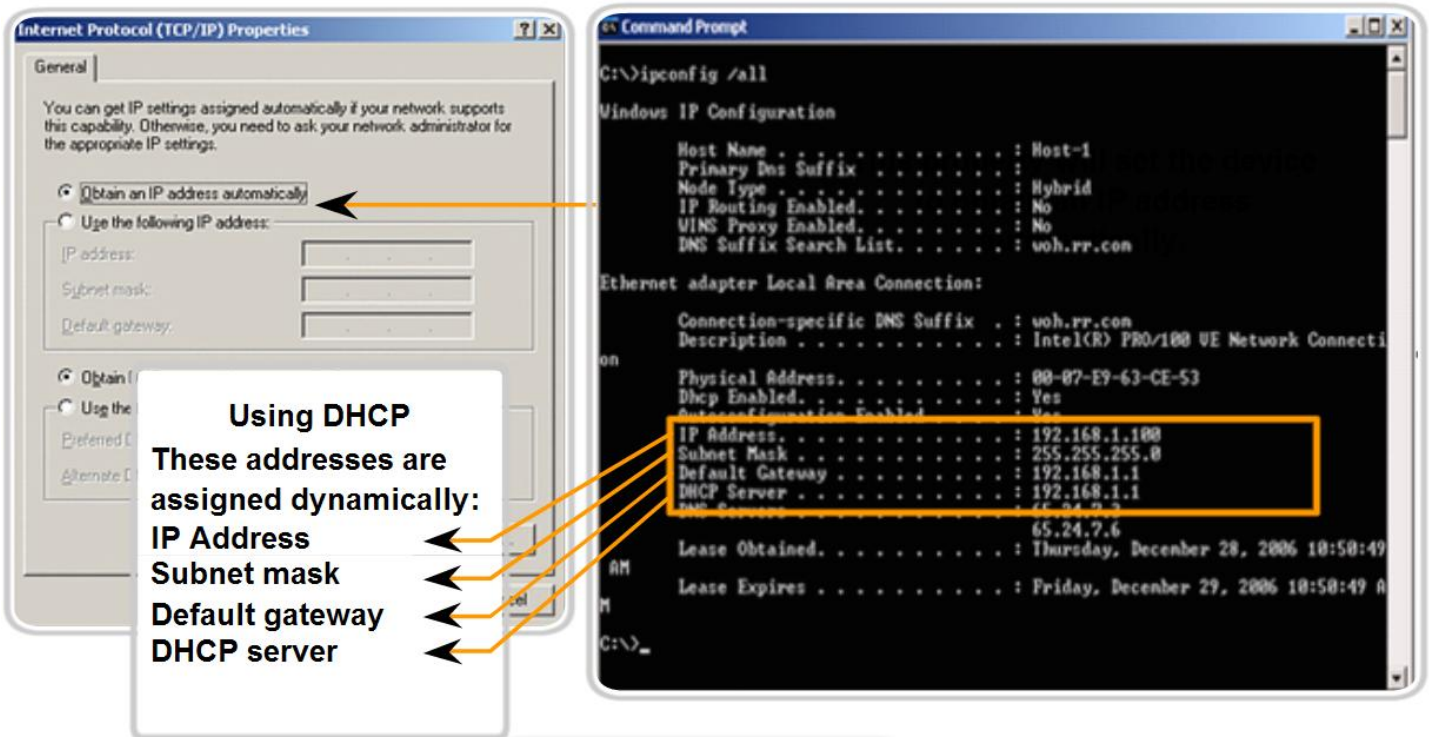
IPv4 Address Planning and Assignment
Public and Private Addresses



Assigning Addresses

- How end user devices can obtain addresses either statically through an administrator or dynamically through DHCP

Assigning Dynamic Addresses

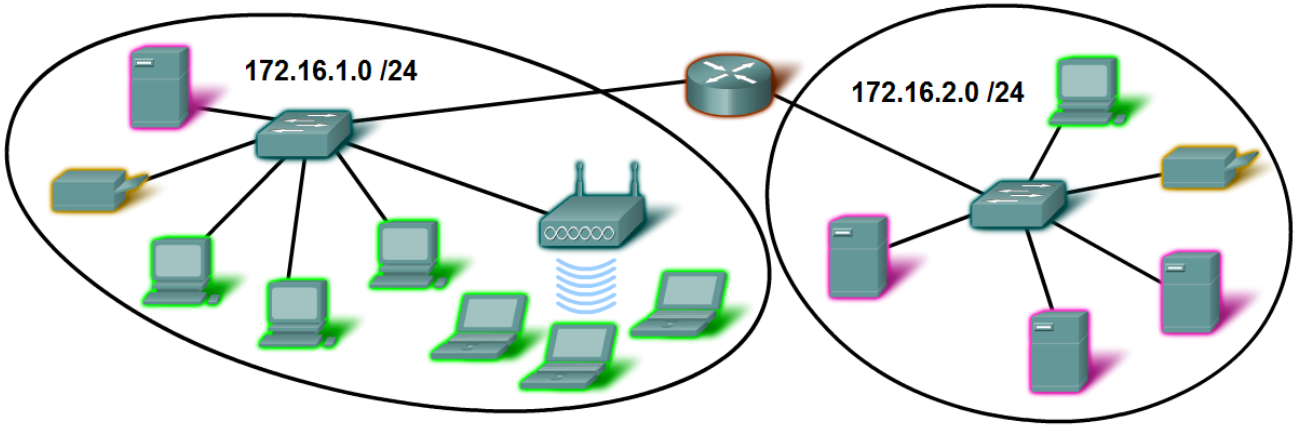


Assigning Addresses

- which types of addresses should be assigned to devices other than end user devices

Devices IP Address Ranges

Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



Assigning Addresses

- Describe the process for requesting IPv4 public addresses, the role ISPs play in the process, and the role of the regional agencies that manage IP address registries

Entities that Oversee IP Address Allocation

Global	**IANA**				
Regional Internet Registries	**AfriNIC** Africa Region	**APNIC** Asia/ Pacific Region	**LACNIC** Latin America And Caribbean Region	**ARIN** North America Region	**RIPE NCC** Europe, Middle East, Central Asia Region

Determine the network portion of the host address and the role of the subnet mask

- Use the subnet mask and ANDing process to extract the network address from the IP address

Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host Address	11000000	00000000	00000000	00000001
Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000
Network Address	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	0

Determine the network portion of the host address and the role of the subnet mask

- Use ANDing logic to determine an outcome

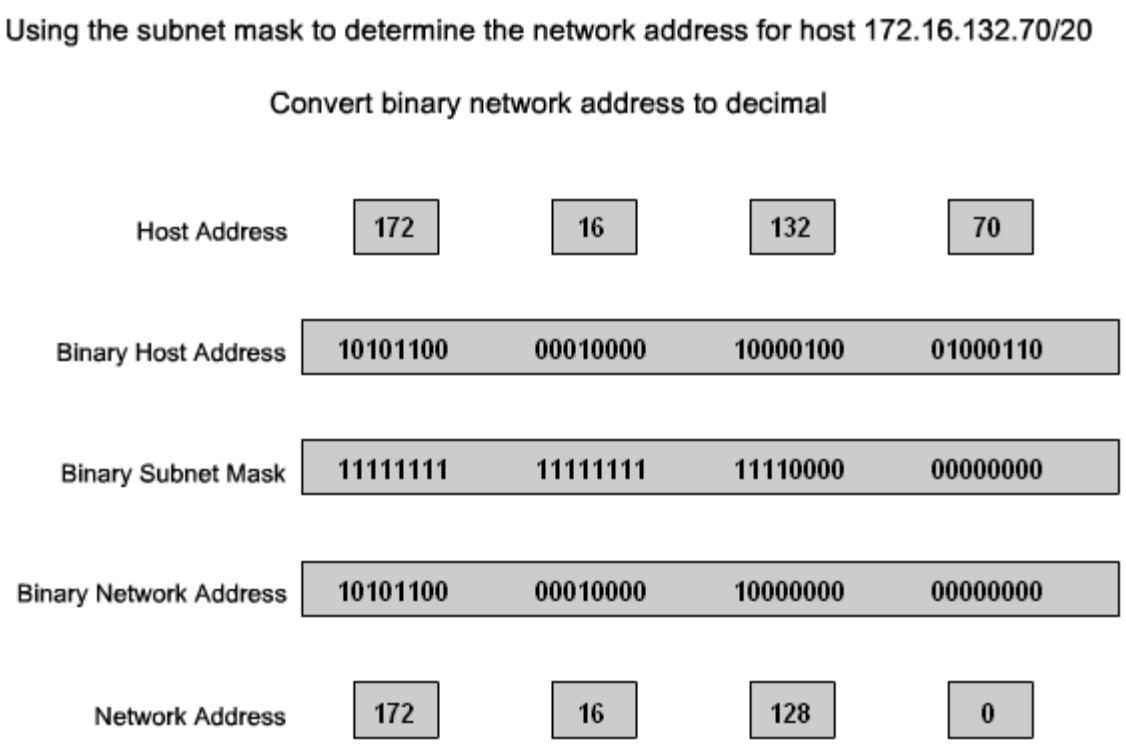
Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host Address	11000000	00000000	00000000	00000001
Subnet Mask	255	255	0	0
	11111111	11111111	00000000	00000000
Network Address	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	0

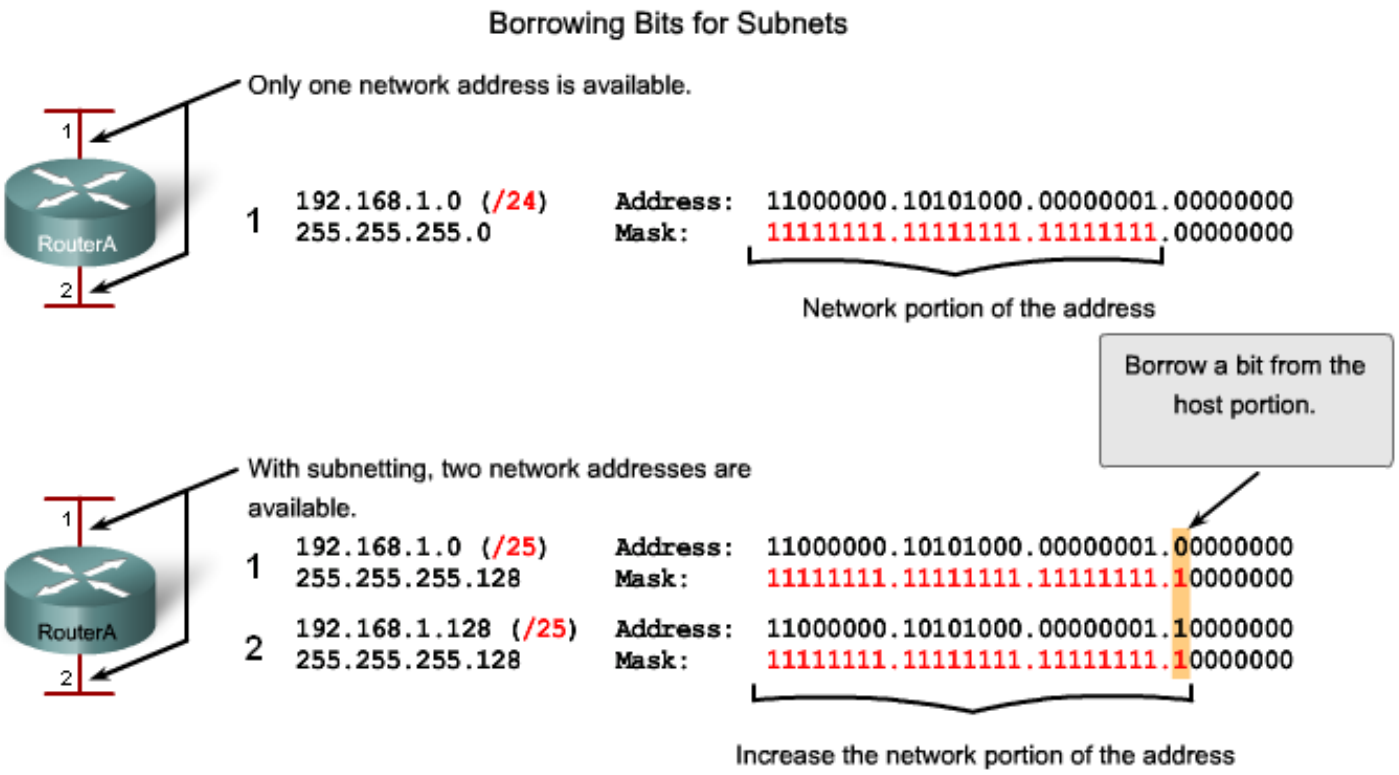
Determine the network portion of the host address and the role of the subnet mask

- Observe the steps in the ANDing of an IPv4 host address and subnet mask



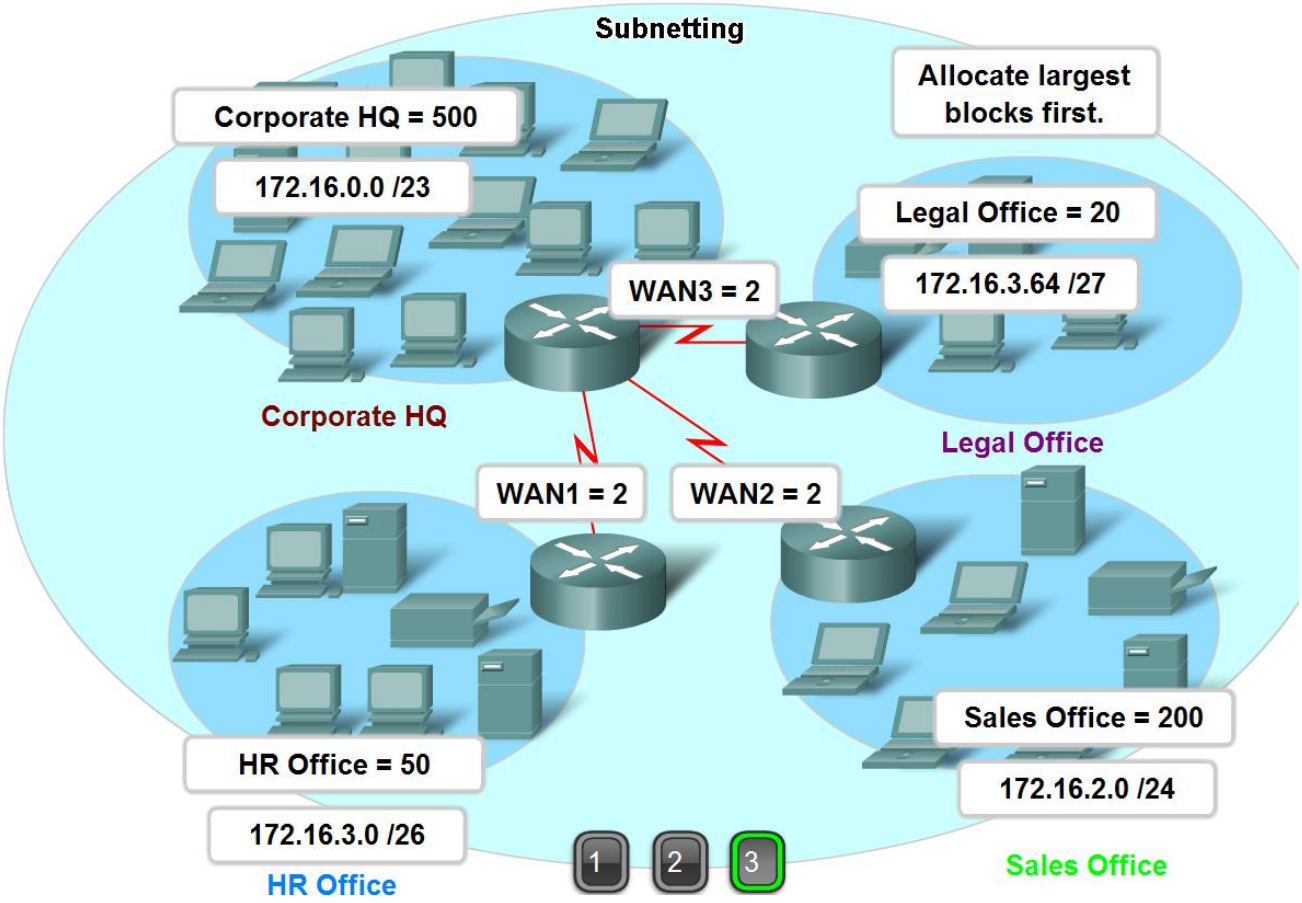
Calculating Addresses

- Use the subnet mask to divide a network into smaller networks and describe the implications of dividing networks for network planners



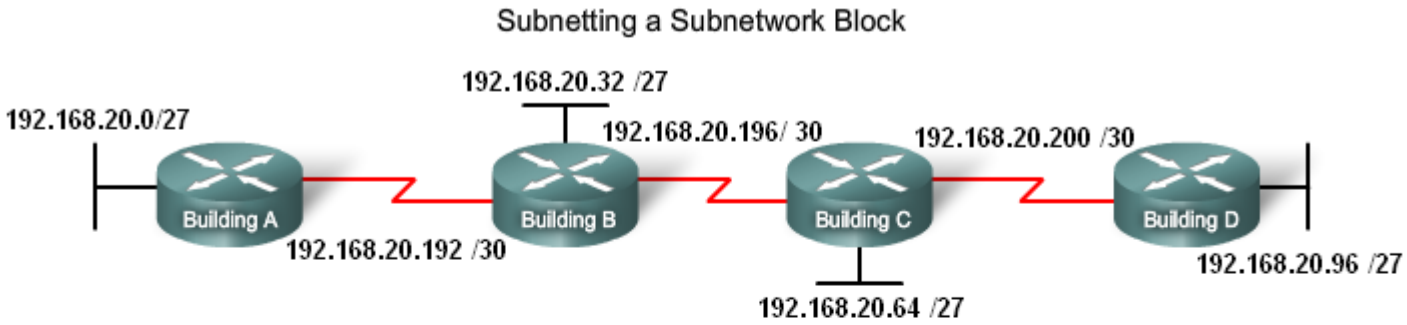
Calculating Addresses

- Extract network addresses from host addresses using the subnet mask



Calculating Addresses

- Calculate the number of hosts in a network range given an address and subnet mask



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.220/30

Calculating Addresses

- Given a subnet address and subnet mask, calculate the network address, host addresses and broadcast address

Activity

Given the host IP address and the subnet mask, enter the network address in binary and decimal.

Host Address	10	148	100	54
Subnet Mask	255	255	255	240
Host Address in binary	00001010	10010100	01100100	00110110
Subnet Mask in binary	11111111	11111111	11111111	11110000
Network Address in binary				
Network Address in decimal				

Calculating Addresses

- Given a pool of addresses and masks, assign a host parameter with address, mask and gateway

Given the network address and the subnet mask, enter the number of possible hosts. Click next to Number of Hosts to enter your response.

Network Address	10	0	0	0
Subnet Mask	255	255	254	0
Network address in binary	00001010	00000000	00000000	00000000
Subnet Mask in binary	11111111	11111111	11111110	00000000
Number of hosts				

Calculating Addresses

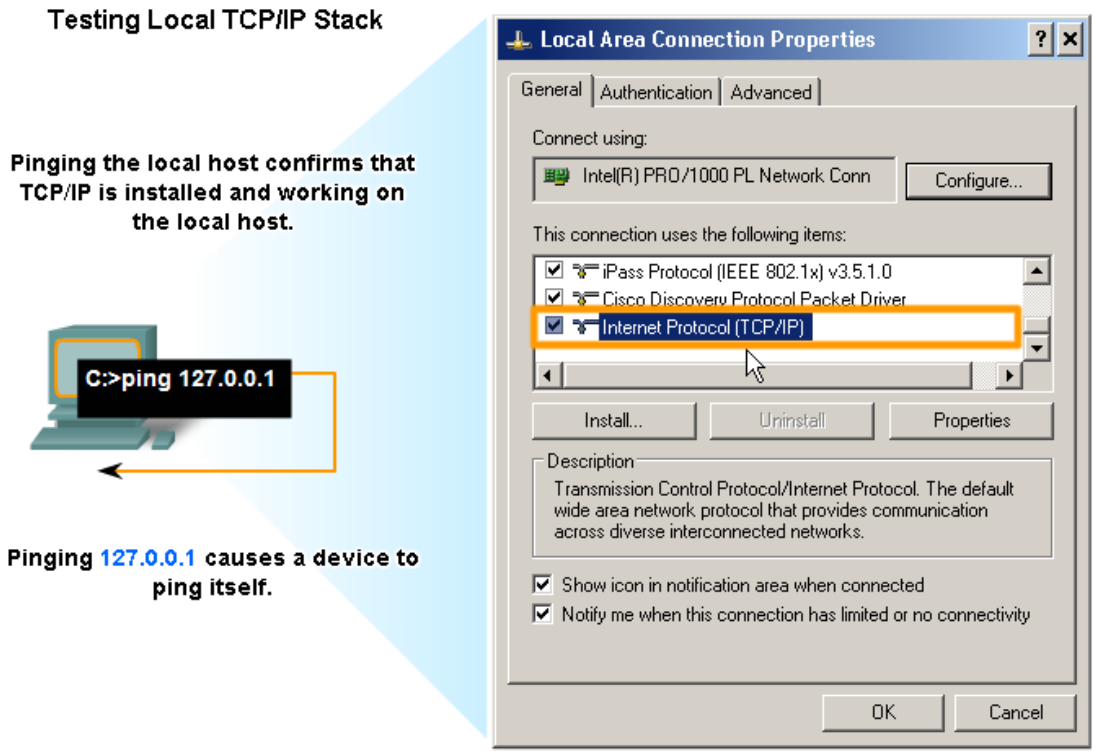
- Given a diagram of a multi-layered network, address range, number of hosts in each network and the ranges for each network, create a network scheme that assigns addressing ranges to each network

Given the network address and the subnet mask, define the range of hosts, the broadcast address, and the next network address.

Network Address in decimal	10	187	0	0
Subnet Mask in decimal	255	255	224	0
Network address in binary	00001010	10111011	00000000	00000000
Subnet Mask in binary	11111111	11111111	11100000	00000000
First Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Last Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Broadcast Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Next Network Address in decimal	1st octet	2nd octet	3rd octet	4th octet

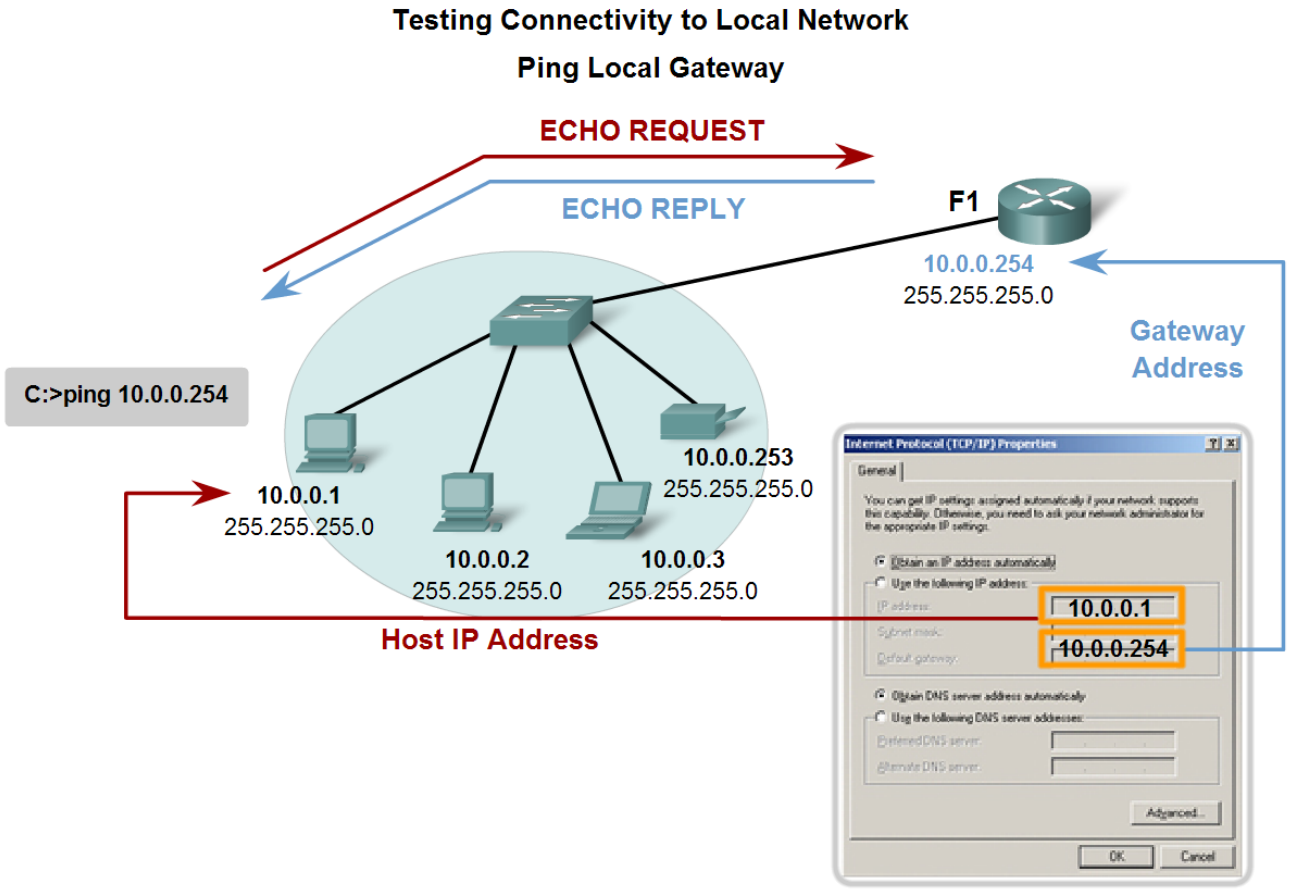
Testing the Network Layer

- Describe the general purpose of the ping command, trace the steps of its operation in a network, and use the ping command to determine if the IP protocol is operational on a local host



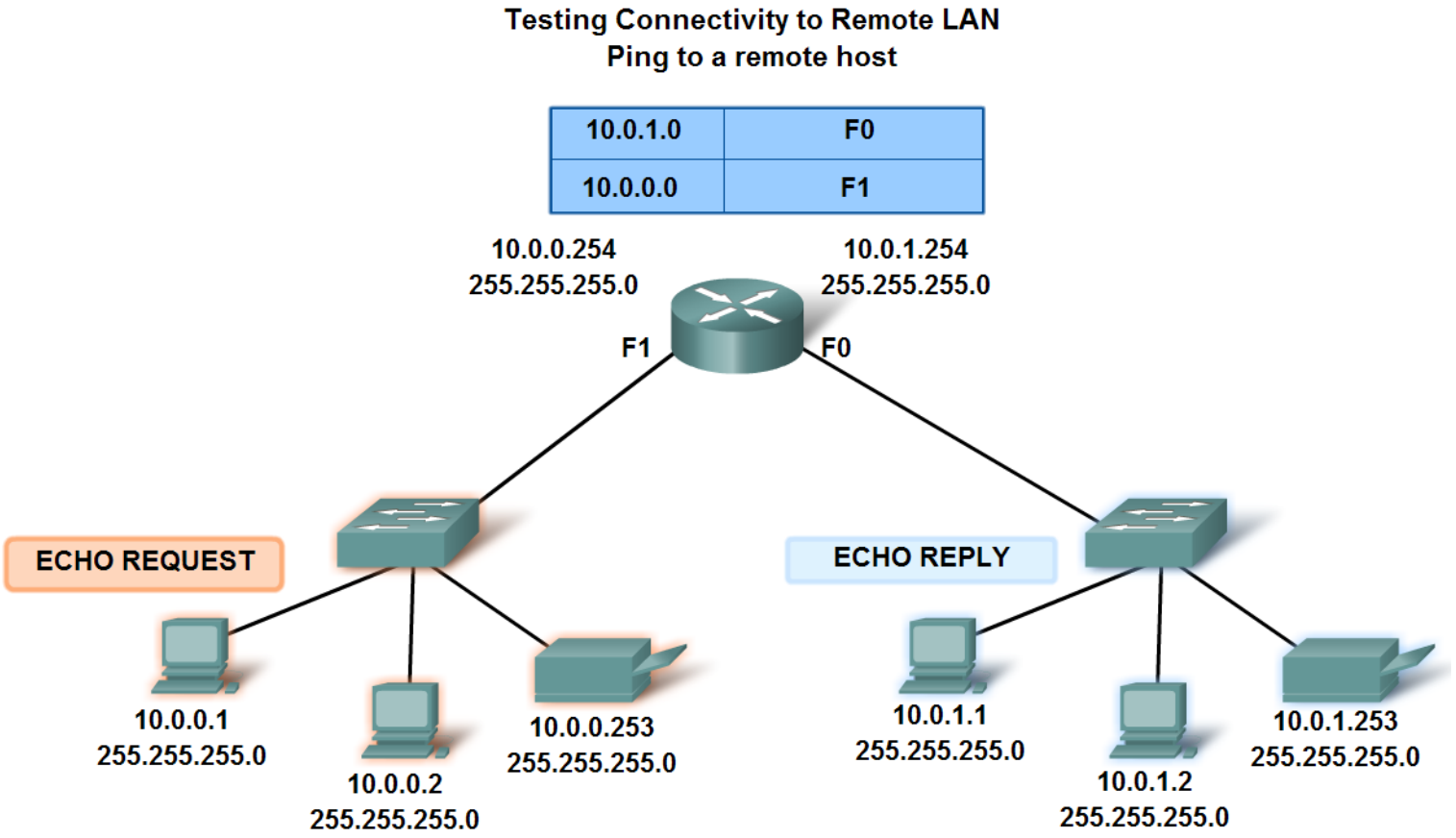
Testing the Network Layer

- Use ping to verify that a local host can communicate with a gateway across a local area network



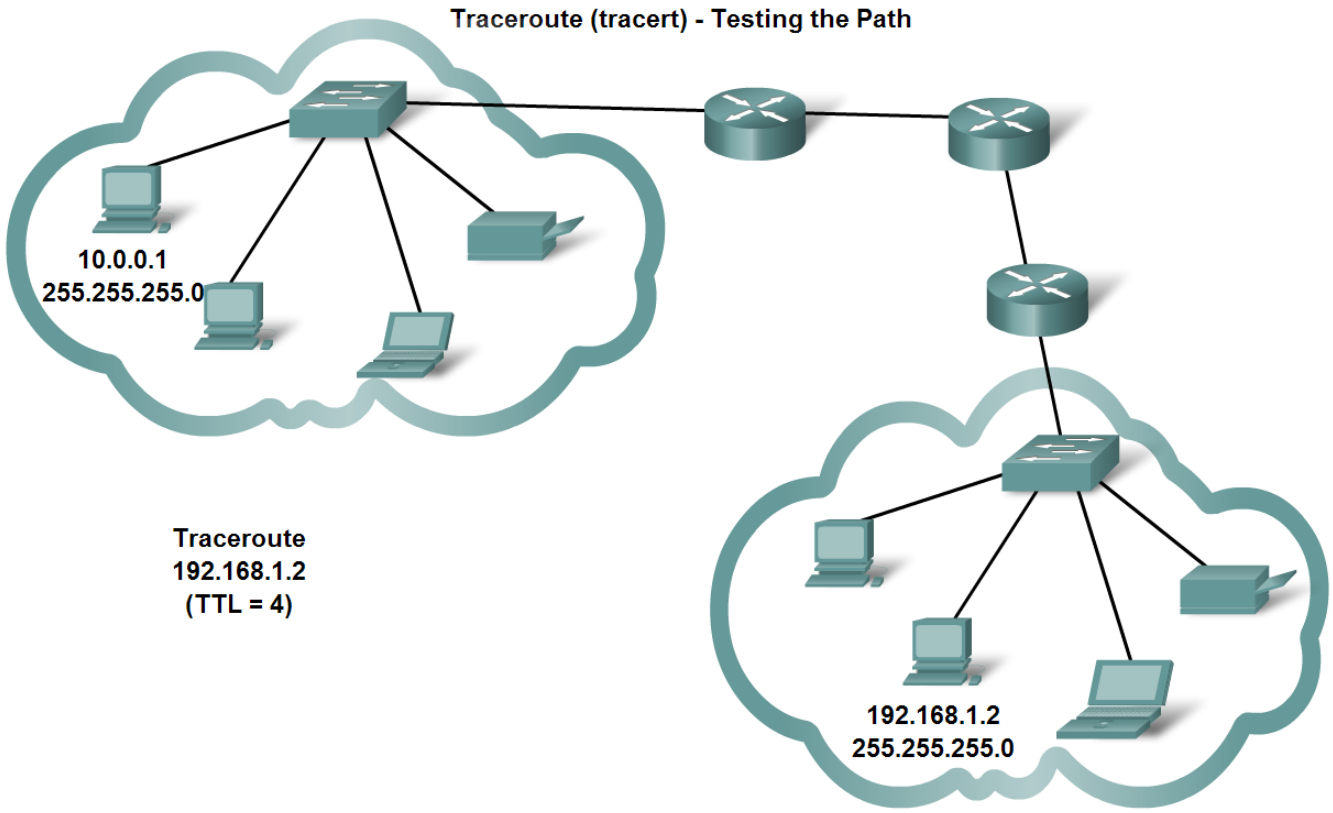
Testing the Network Layer

- Use ping to verify that a local host can communicate via a gateway to a device in remote network



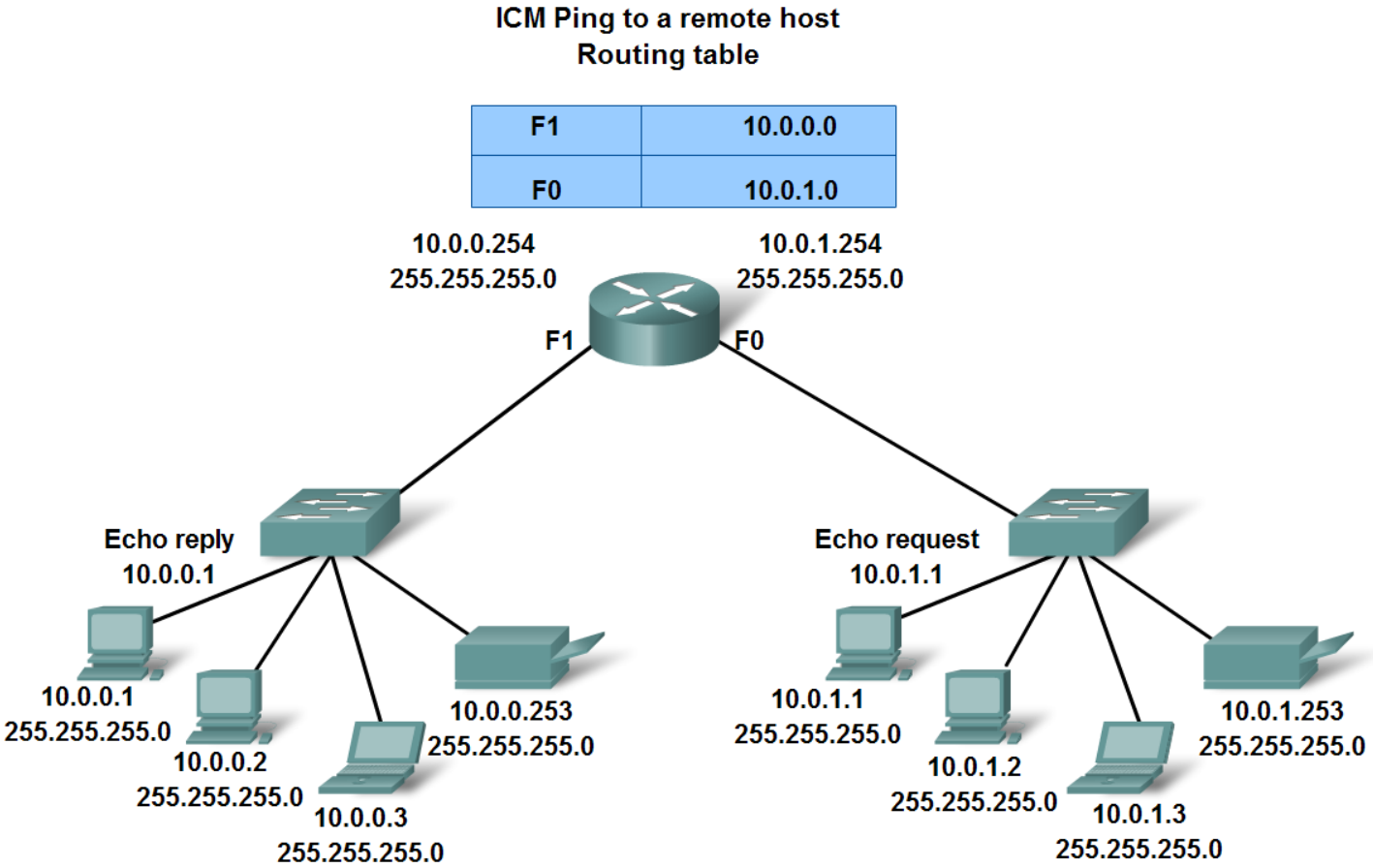
Testing the Network Layer

- Use tracert/traceroute to observe the path between two devices as they communicate and trace the steps of tracert/traceroute's operation



Testing the Network Layer

- Describe the role of ICMP in the TCP/IP suite and its impact on the IP protocol



Network Fundamentals Review

Routing

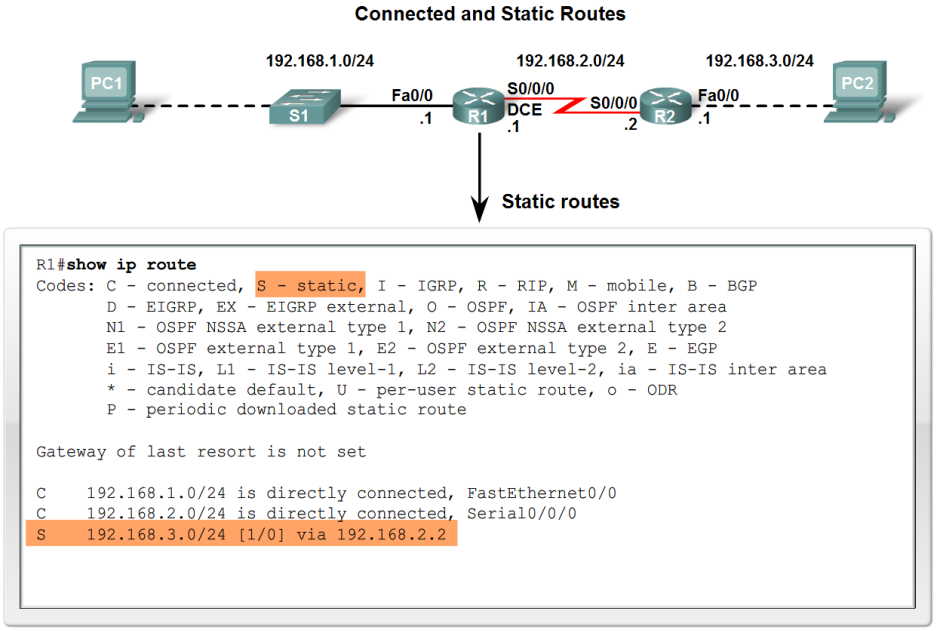
Cisco | Networking Academy®
Mind Wide Open™

Routing Table Structure

- Routing Table is stored in ram and contains information about:
  - Directly connected networks - this occurs when a device is connected to another router interface
  - Remotely connected networks - this is a network that is not directly connected to a particular router
  - Detailed information about the networks include source of information, network address & subnet mask, and Ip address of next-hop router

Routing Table Structure

- Adding a connected network to the routing table
  - Router interfaces
    - Each router interface is a member of a different network
    - In order for static and dynamic routes to exist in routing table you must have directly connected networks

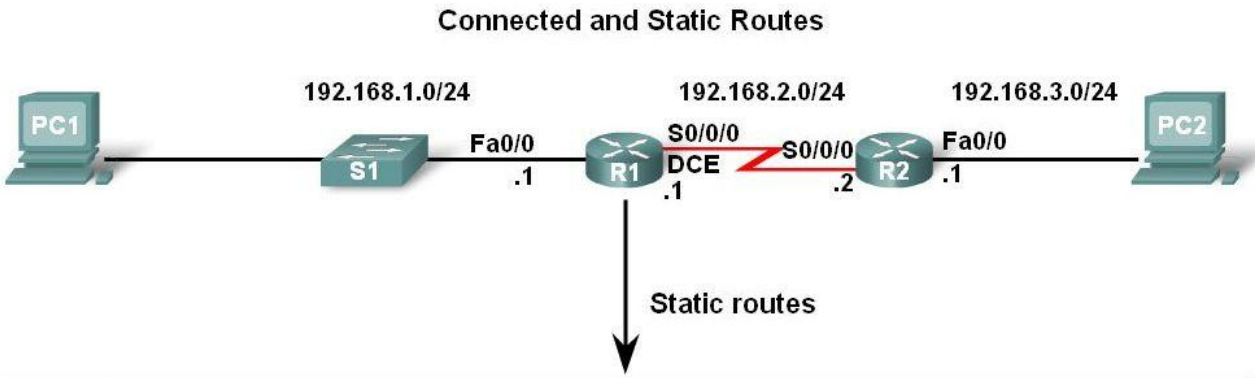


Routing Table Structure

- Static routes in the routing table
  - Includes: network address and subnet mask and IP address of next hop router or exit interface
  - Denoted with the code **S** in the routing table
  - Routing tables must contain directly connected networks used to connect remote networks before static or dynamic routing can be used
- When to use static routes
  - When network only consists of a few routers
  - Network is connected to internet only through one ISP
  - Hub & spoke topology is used on a large network

Routing Table Structure

- Connected and Static routes



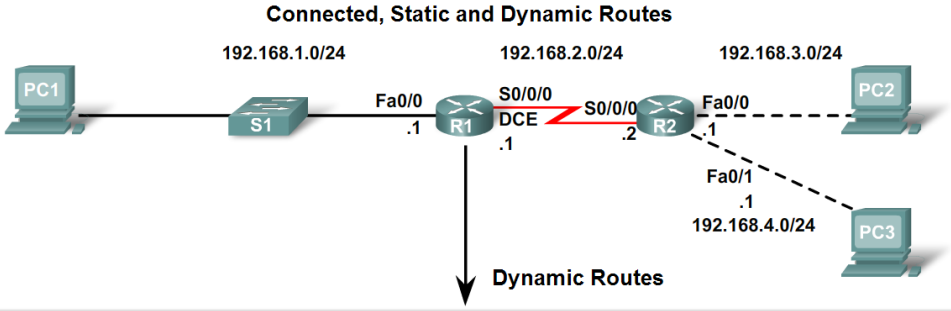

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Routing Table Structure

- Dynamic routing protocols
  - Used to add remote networks to a routing table
  - Are used to discover networks
  - Are used to update and maintain routing tables
- Automatic network discovery
  - Routers are able discover new networks by sharing routing table information

Routing Table Structure

- Maintaining routing tables
  - Dynamic routing protocols are used to share routing information with other router & to maintain and up date their own routing table
- IP routing protocols - example of routing protocols include:
  - RIP
  - IGRP
  - EIGRP
  - OSPF



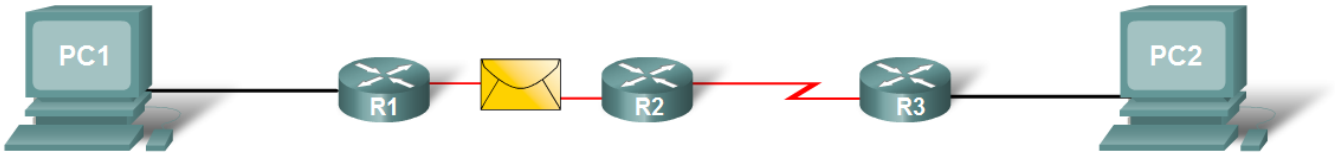

```
R1#show ip route
Codes:   C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
         D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
         area
         * - candidate default, U - per-user static route, o - ODR
         P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:20, Serial0/0/0
```

Routing Table Structure

- Routing Table Principles
  - 3 principles regarding routing tables:
    - Every router makes its decisions alone, based on the information it has in its routing table
    - Different routing table may contain different information
    - A routing table can tell how to get to a destination but not how to get back

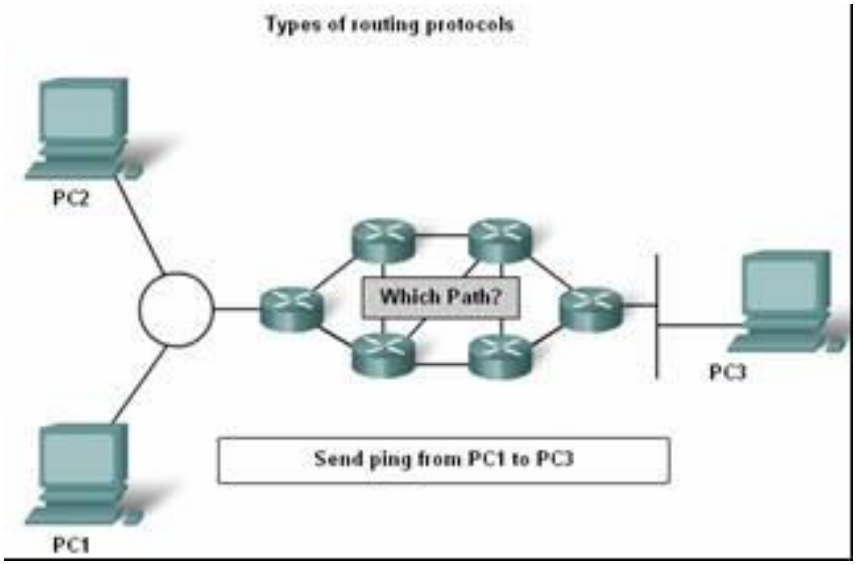
Routing Principle 3 in Action

R1 has a route to PC2's network.



Routing Table Structure

- Effects of the 3 Routing Table Principles
  - Packets are forwarded through the network from one router to another, on a hop by hop basis
  - Packets can take path “X” to a destination but return via path “Y” (Asymmetric routing)

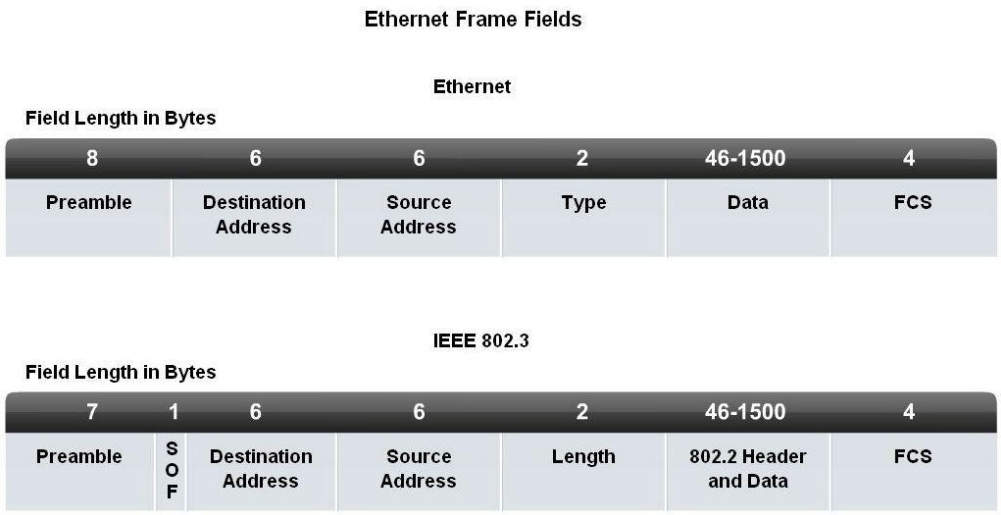


Router Paths and Packet Switching

- Internet Protocol (IP) packet format contains fields that provide information about the packet and the sending and receiving hosts
- Fields that are importance for CCNA students:
  - Destination IP address
  - Source IP address
  - Version & TTL
  - IP header length
  - Precedence & type of service
  - Packet length

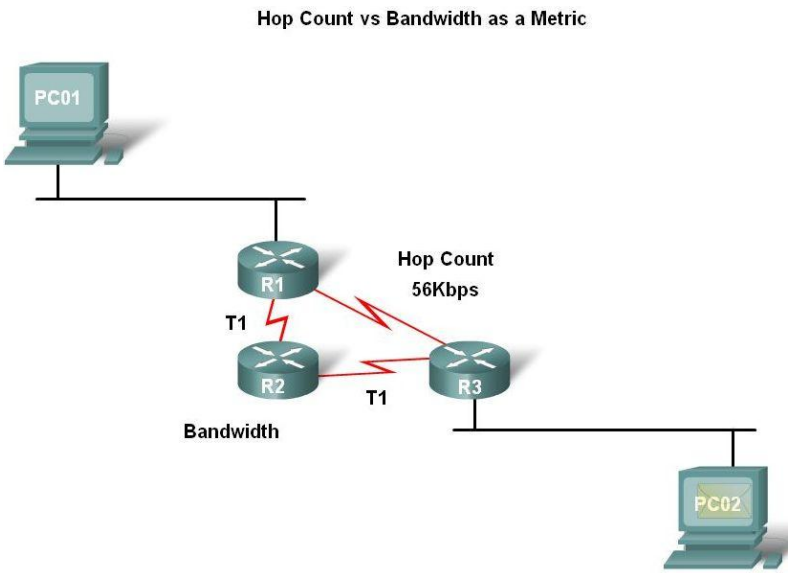
Router Paths and Packet Switching

- MAC Layer Frame Format
- MAC Frames are also divided into fields - they include:
  - Preamble
  - Start of frame delimiter
  - Destination MAC address
  - Source MAC address
  - Type/length
  - Data and pad
  - Frame check sequence



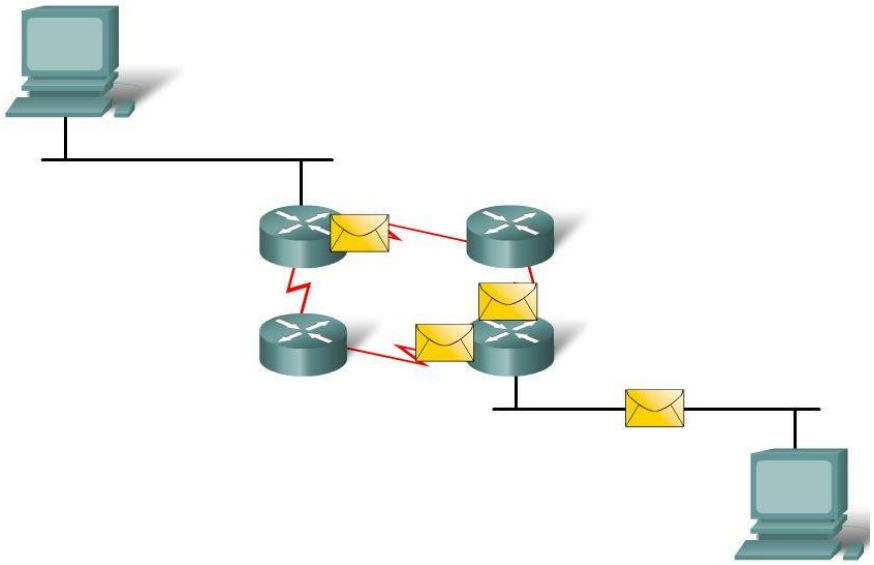
Router Paths and Packet Switching

- A **Metric** is a numerical value used by routing protocols help determine the best path to a destination
  - The smaller the metric value the better the path
- 2 types of metrics used by routing protocols are:
  - Hop count - this is the number of routers a packet must travel through to get to its destination
  - Bandwidth - this is the "speed" of a link also known as the data capacity of a link



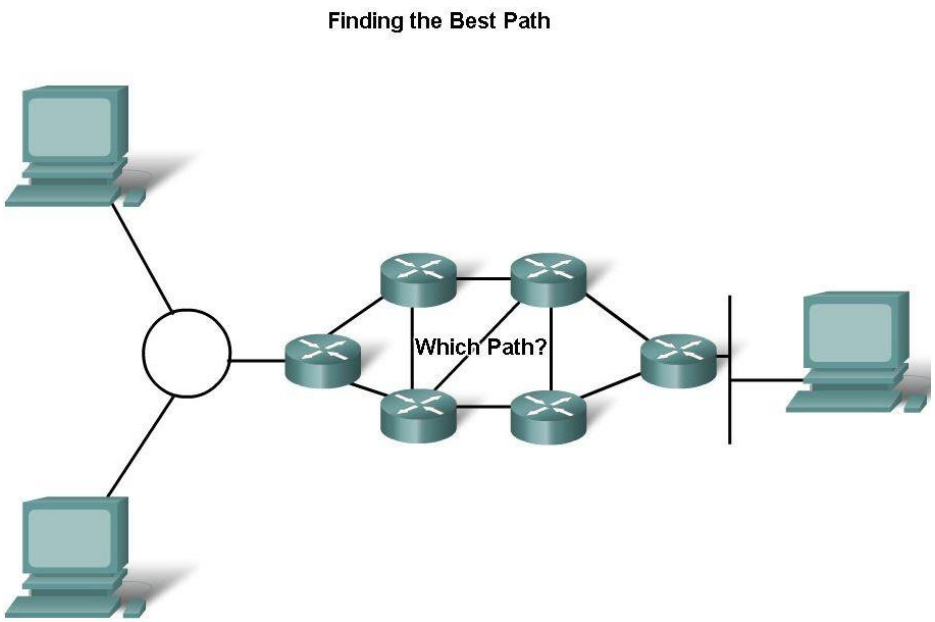
Router Paths and Packet Switching

- **Equal cost metric** is a condition where a router has multiple paths to the same destination that all have the same metric
- To solve this dilemma, a router will use Equal Cost Load Balancing - this means the router sends packets over the multiple exit interfaces listed in the routing table.



Router Paths and Packet Switching

- **Path determination** is a process used by a router to pick the best path to a destination
- One of 3 path determinations results from searching for the best path
  - Directly connected network
  - Remote network
  - No route determined

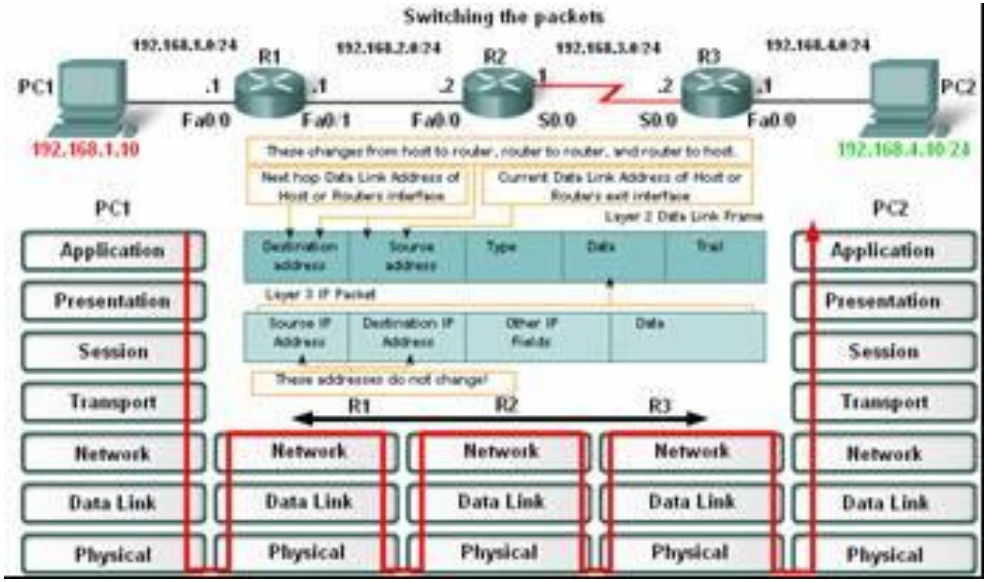


Router Paths and Packet Switching

- **Switching Function** of Router is the process used by a router to switch a packet from an incoming interface to an outgoing interface on the same router
  - A packet received by a router will do the following:
    - Strips off layer 2 headers
    - Examines destination IP address located in Layer 3 header to find best route to destination
    - Re-encapsulates layer 3 packet into layer 2 frame
    - Forwards frame out exit interface

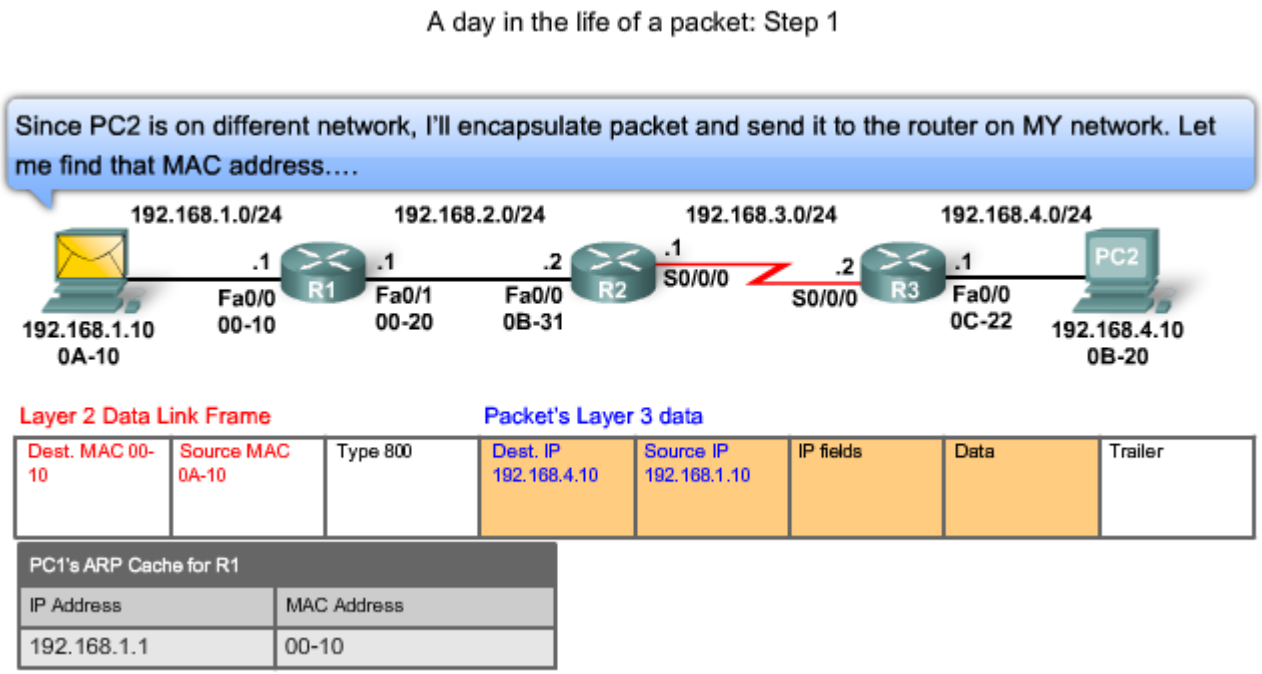
Router Paths and Packet Switching

- As a packet travels from one networking device to another
  - The Source and Destination IP addresses **NEVER** change
  - The Source & Destination MAC addresses **CHANGE** as packet is forwarded from one router to the next
  - TTL field decrement by one until a value of zero is reached at which point router discards packet (prevents packets from endlessly traversing the network)



Router Paths and Packet Switching

- Path determination and switching function details. PC1 wants to send something to PC 2.
  - **Step 1** - PC1 encapsulates packet into a frame - frame contains R1's destination MAC address

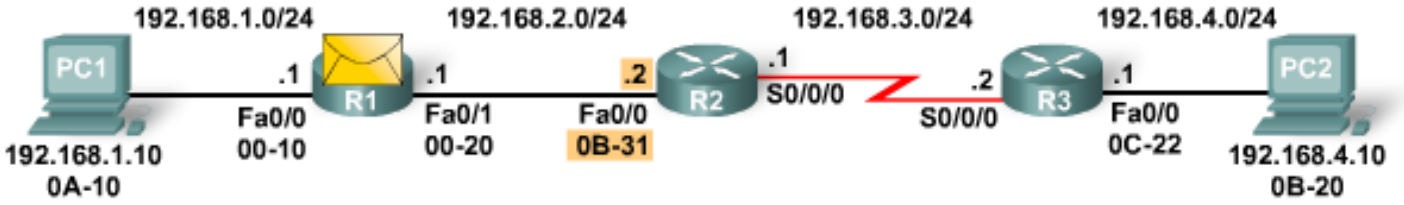


Router Paths and Packet Switching

- **Step 2** - R1 receives Ethernet frame
  - R1 sees that destination MAC address matches its own MAC
  - R1 then strips off Ethernet frame
  - R1 Examines destination IP
  - R1 consults routing table looking for destination IP
  - After finding destination IP in routing table, R1 now looks up next hop IP address
  - R1 re-encapsulates IP packet with a new Ethernet frame
  - R1 forwards Ethernet packet out Fa0/1 interface

Router Paths and Packet Switching

A day in the life of a packet: Step 2



Layer 2 Data Link Frame | Packet's Layer 3 data

Dest. MAC		Type 800	Dest. IP	Source IP	IP fields	Data	Trailer
0B-31			192.168.4.10	192.168.1.10			

R1's ARP Cache

IP Address	MAC Address
192.168.2.2	0B-31

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	Fa0/0
192.168.2.0/24	0	Dir. Connect.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1