TY B. Tech.
(Computer Engineering)
2020 Pattern

- **Prerequisites :**
- □ Digital Electronics
- **Course Objectives :**
- To study the fundamentals of networking
- To understand functionalities of Physical layer
- To understand the functionalities of Logical Link Layer
- To study various protocols at Medium Access Control Layer

Course Outcomes :

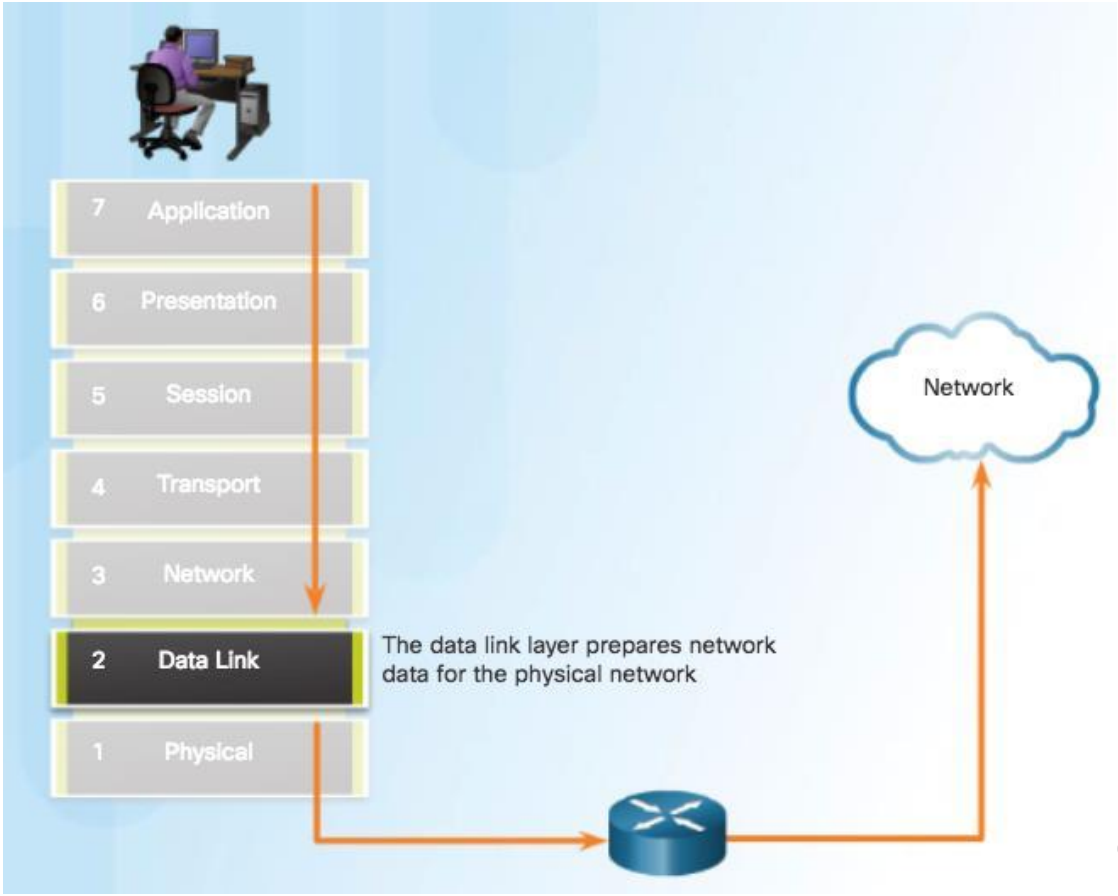
- After completion of the course, student will be able toAfter completion of the course, student will be able to
- 1. Explore network design issues- REMEMBER
- 2. Recognize the functions of OSI layers & TCP/IP protocol stack- UNDERSTAND
- 3. Describe the functionality of Logical Link layer- UNDERSTAND
- 4. Describe the functionality of Medium Access Control Layer- UNDERSTAND

Unit III: Data Link Layer and Network Layer:

- Data Link Layer Protocols, Media Access Control.
- Types of Errors: Redundancy, Detection Versus Correction, Forward Error Correction Versus Retransmission.
- Network Layer Protocols, Routing, Routers, Configuring a Cisco Router.
- IP Addressing: IPv4 Network Addresses, IPv6 Network Addresses, Connectivity Verification.
- Subnetting IP Networks: Subnetting an IPv4 Network, Addressing Schemes, Address Schemes, Design consideration for IPv6

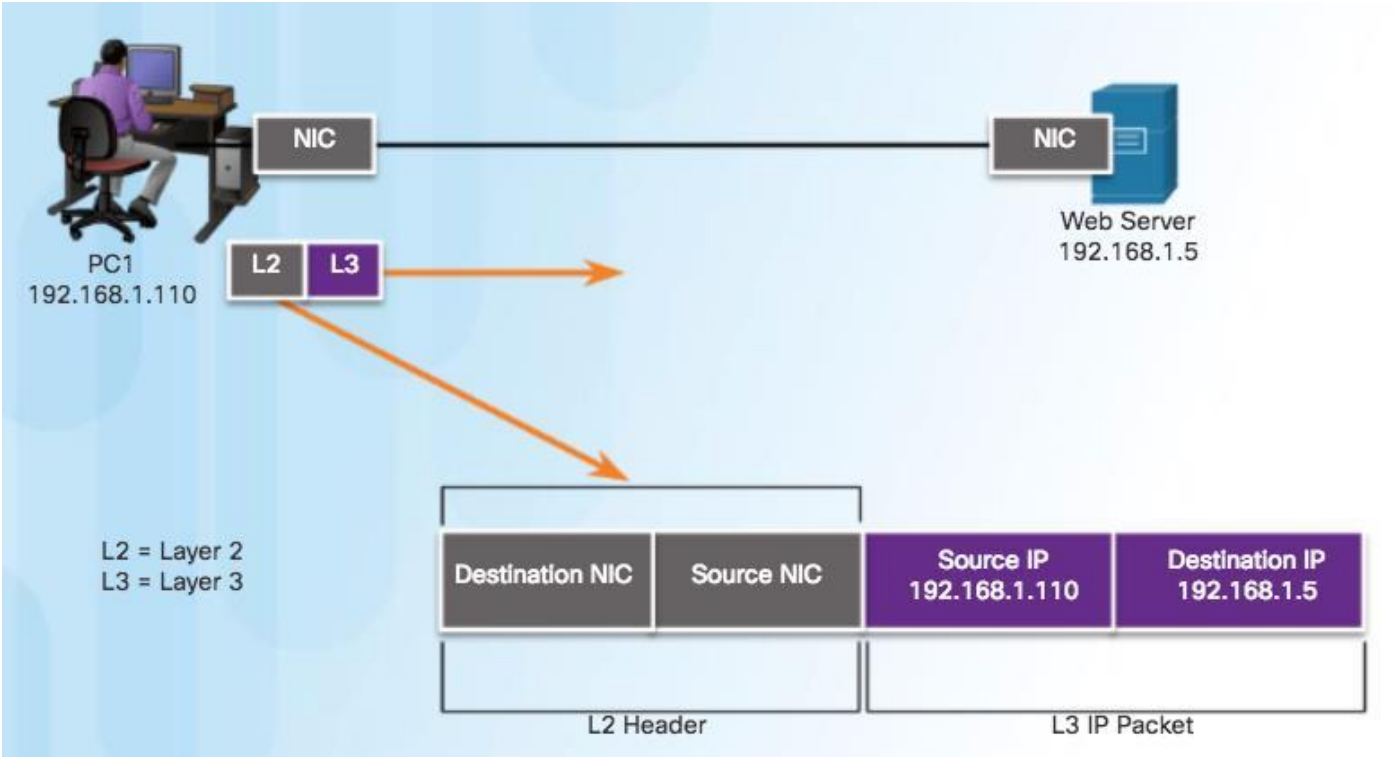
Data Link Protocols

The Data Link Layer

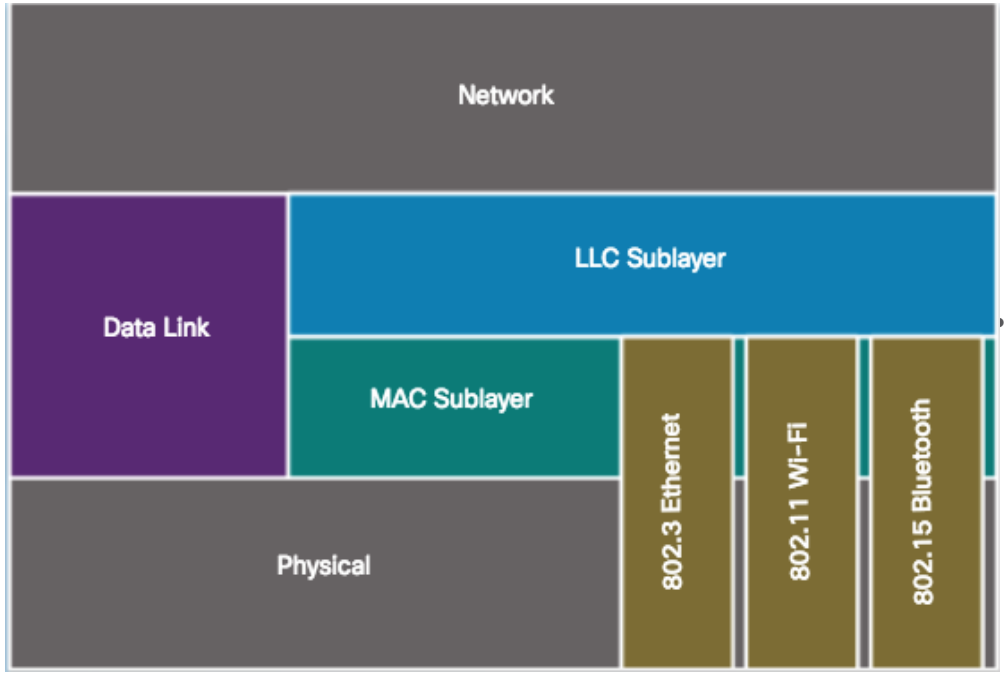


The Data Link Layer (Cont.)

Layer 2 Data Link Addresses

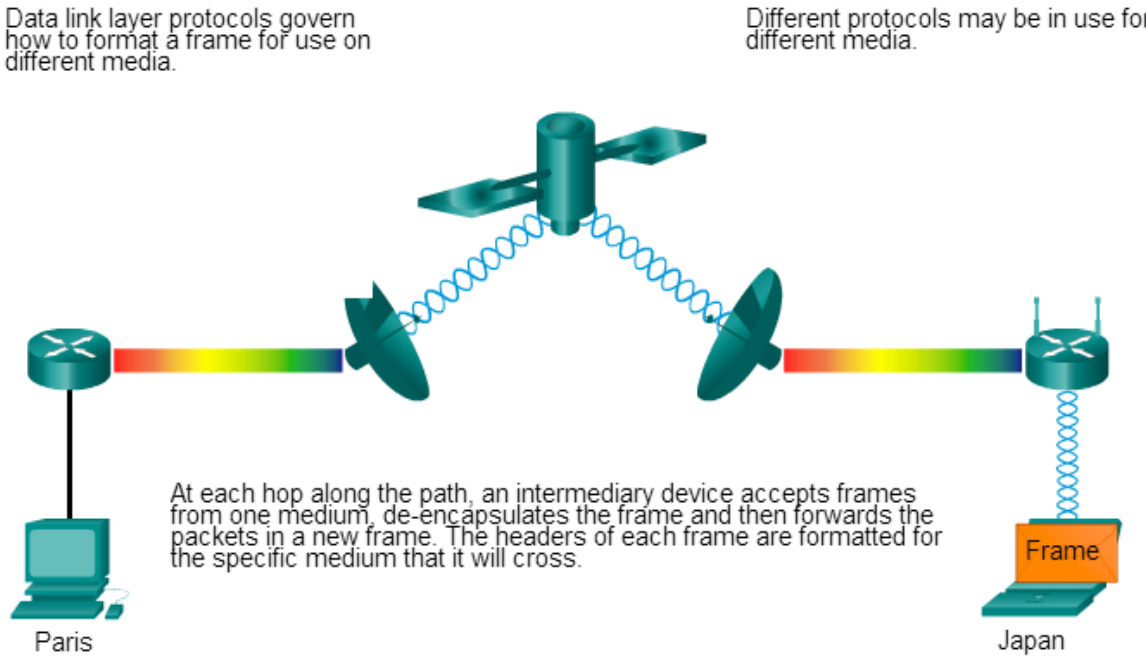


Data Link Sublayers



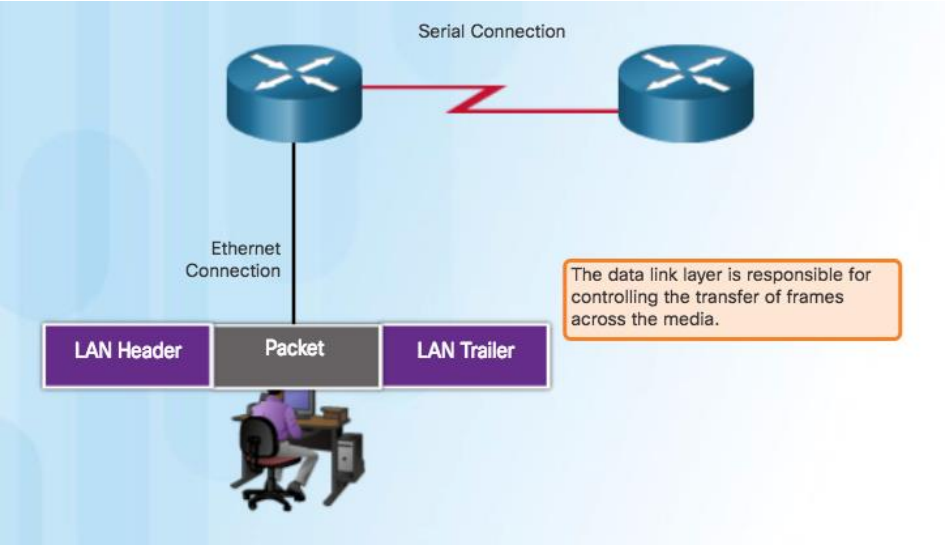
- Data link layer is divided into two sublayers:
  - **Logical Link Control (LLC)**
    - Communicates with the network layer.
    - Identifies which network layer protocol is being used for the frame.
    - Allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
  - **Media Access Control (MAC)**
    - Defines the media access processes performed by the hardware.
    - Provides data link layer addressing and access to various network technologies.
    - Communicates with Ethernet to send and receive frames over copper or fiber-optic cable.
    - Communicates with wireless technologies such as Wi-Fi and Bluetooth.

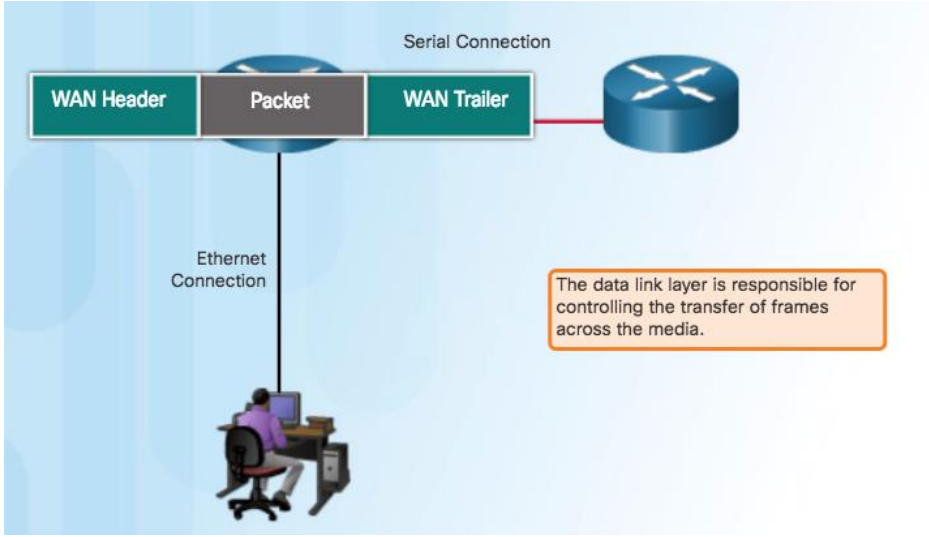
Media Access Control



- As packets travel from the source host to the destination host, they travel over different physical networks.
- Physical networks can consist of different types of physical media such as copper wires, optical fibers, and wireless consisting of electromagnetic signals, radio and microwave frequencies, and satellite links.

Providing Access to Media





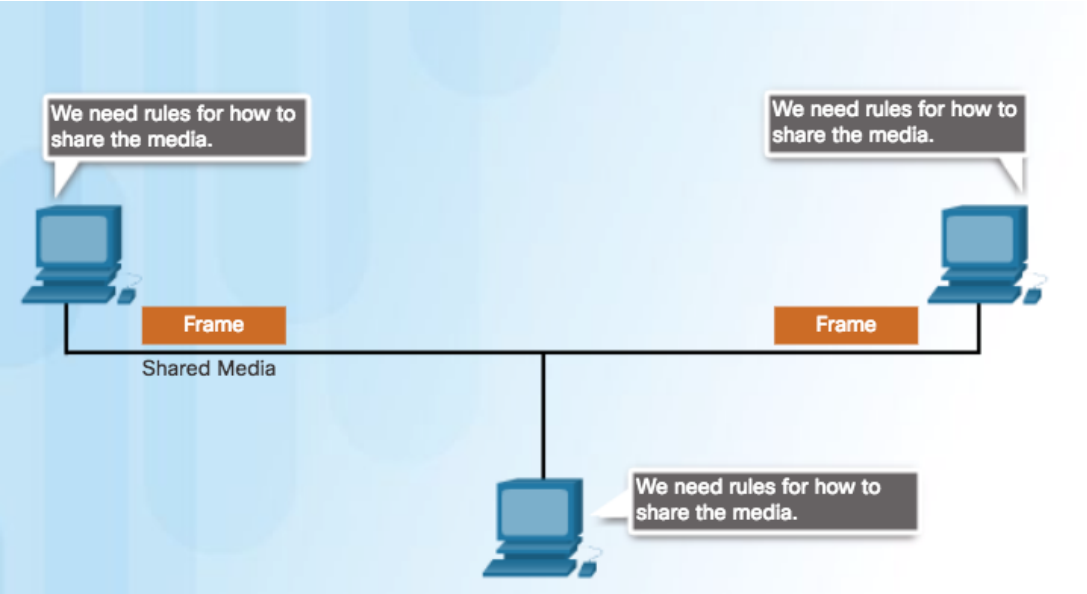
- At each hop along the path, a router:
  - Accepts a frame from a medium
  - De-encapsulates the frame
  - Re-encapsulates the packet into a new frame
  - Forwards the new frame appropriate to the medium of that segment

Data Link Layer Standards

- Engineering organizations that define open standards and protocols that apply to the network access layer include:
  - Institute of Electrical and Electronics Engineers (IEEE)
  - International Telecommunication Union (ITU)
  - International Organization for Standardization (ISO)
  - American National Standards Institute (ANSI)

Media Access Control

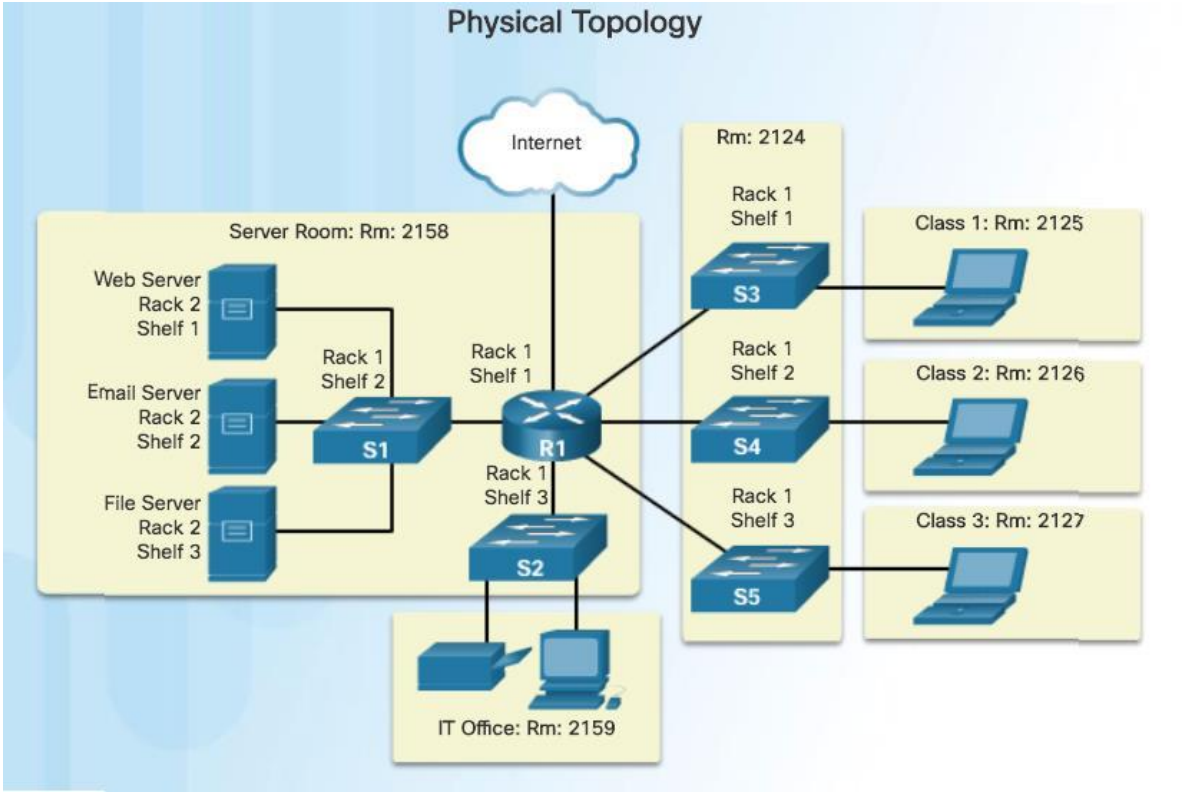
Controlling Access to the Media



Sharing the Media

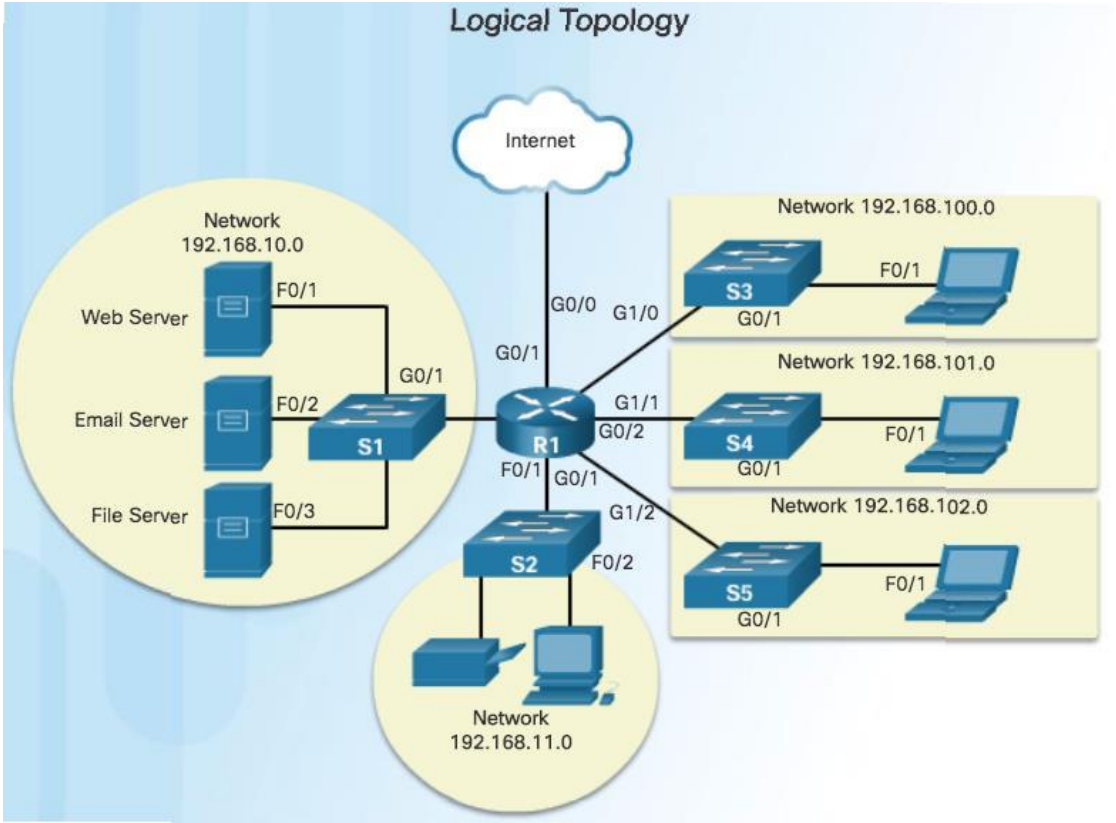
- Media access control is the equivalent of traffic rules that regulate the entrance of motor vehicles onto a roadway.
- The absence of any media access control would be the equivalent of vehicles ignoring all other traffic and entering the road without regard to the other vehicles.
- However, not all roads and entrances are the same. Traffic can enter the road by merging, by waiting for its turn at a stop sign, or by obeying signal lights. A driver follows a different set of rules for each type of entrance.

Physical and Logical Topologies



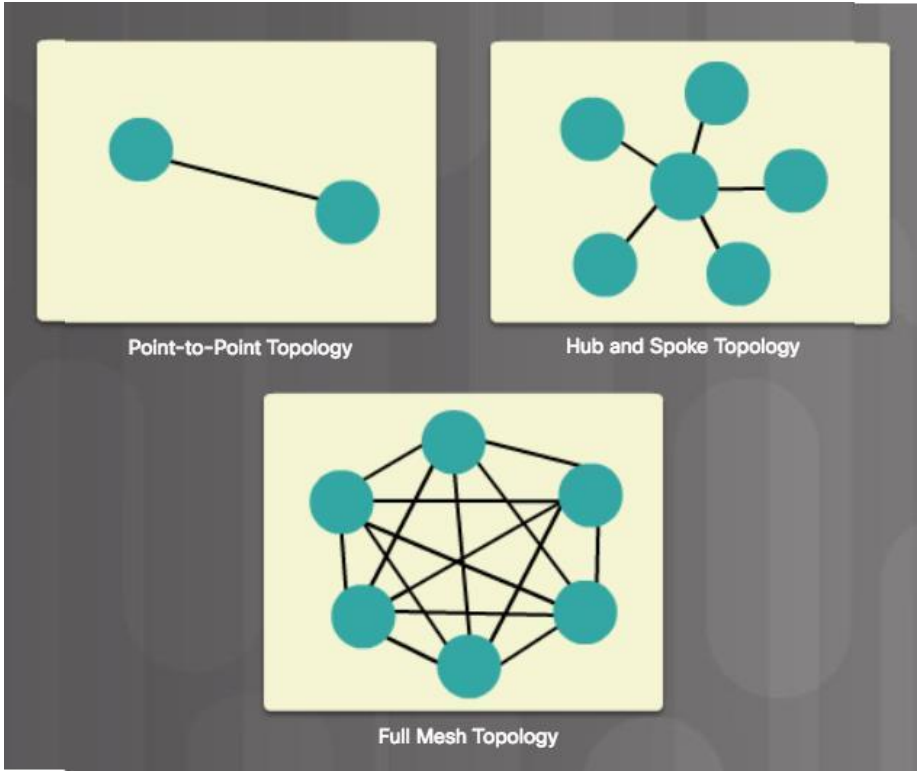
- **Physical topology** - Refers to the physical connections and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected.

Physical and Logical Topologies (Cont.)



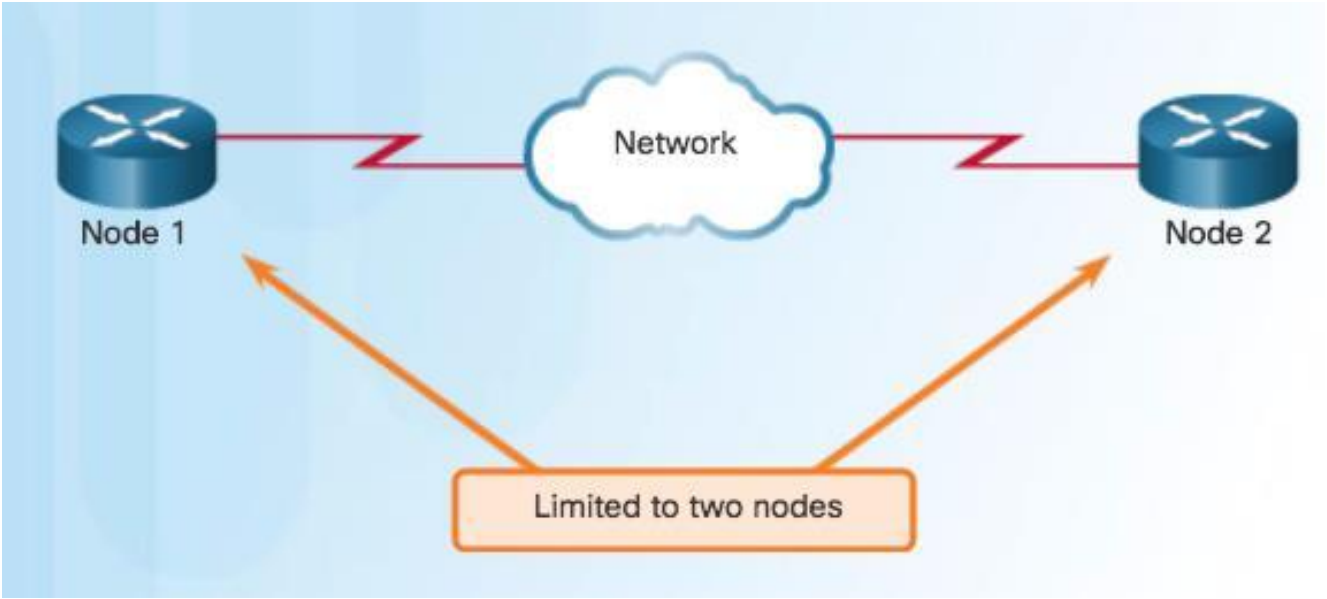
- **Logical Topology:** Refers to the way a network transfers frames from one node to the next. These logical signal paths are defined by data link layer protocols.

Common Physical WAN Topologies



- **Point-to-Point -** Permanent link between two endpoints.
- **Hub and Spoke** - A central site interconnects branch sites using point-to-point links.
- **Mesh** - Provides high availability, but requires that every end system be interconnected to every other system. Administrative and physical costs can be significant.

Physical Point-to-Point Topology

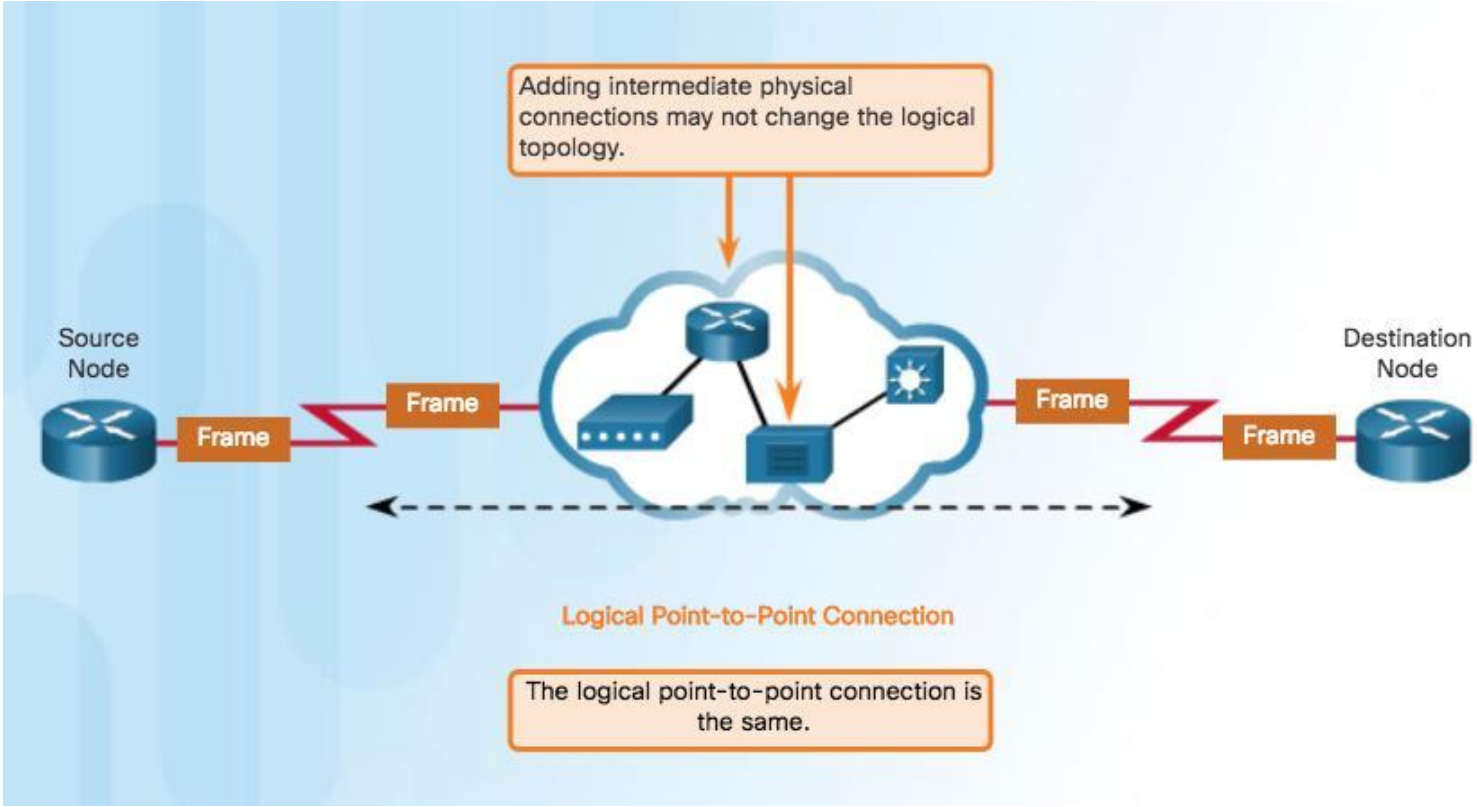


- Frames are placed on the media by the node at one end and taken from the media by the node at the other end of the point-to-point circuit.

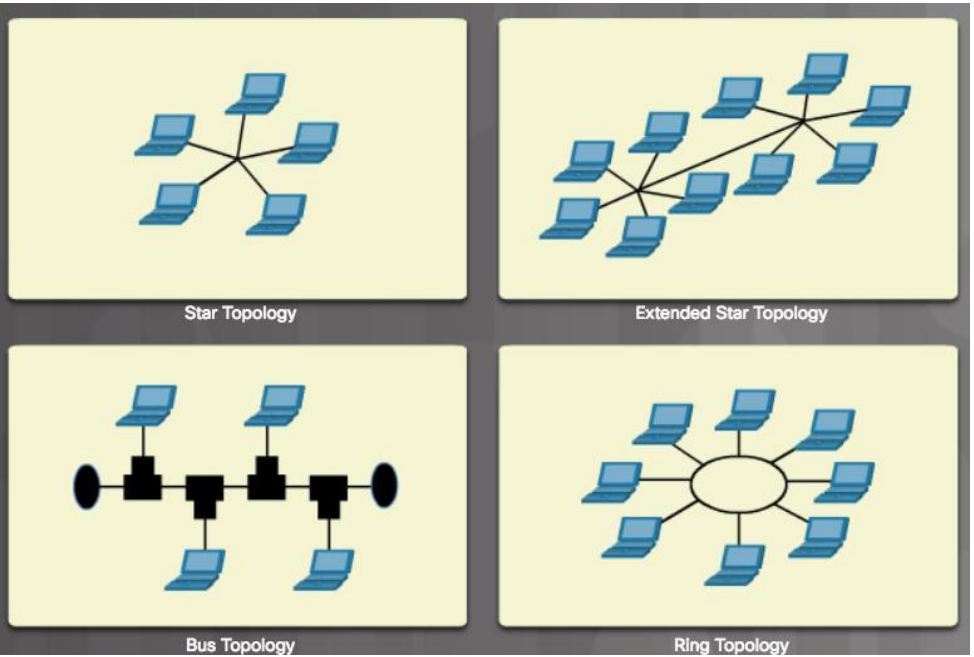
Logical Point-to-Point Topology

- End nodes communicating in a point-to-point network can be physically connected via a number of intermediate devices.
- However, the use of physical devices in the network does not affect the logical topology.
- The logical connection between nodes forms what is called a virtual circuit.

Logical Point-to-Point Topology (Cont.)

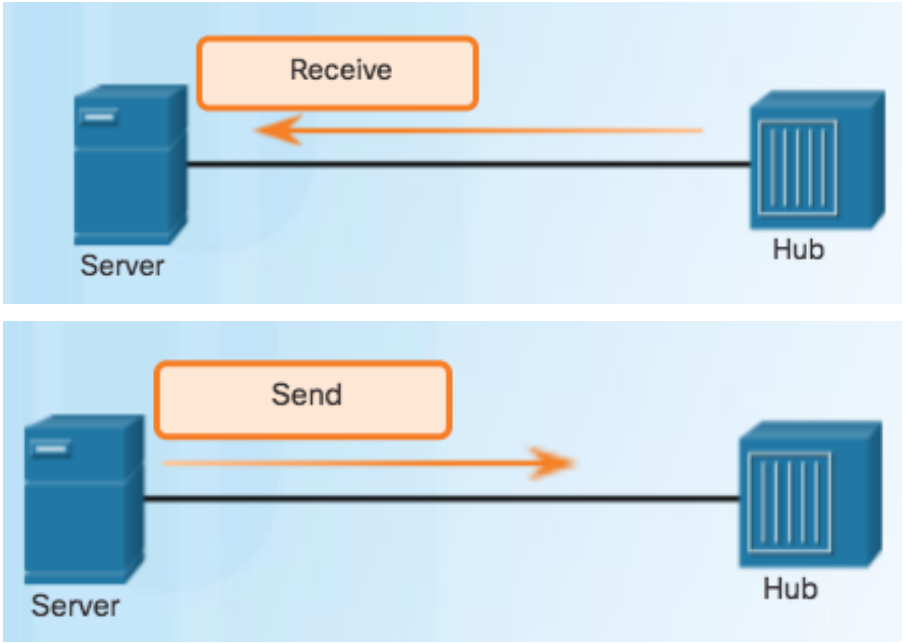


Physical LAN Topologies



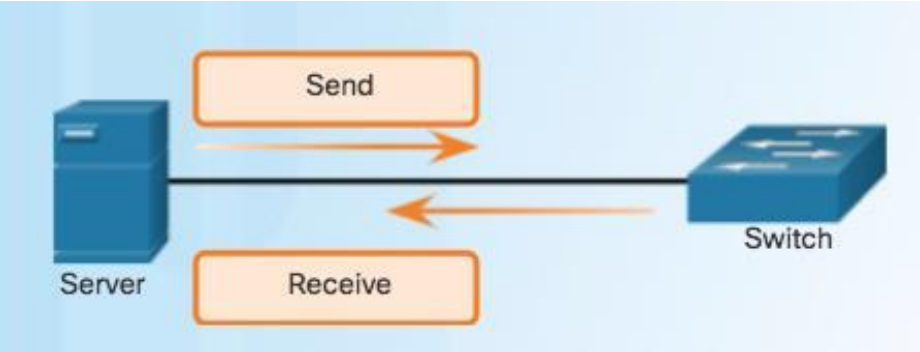
- **Star** - End devices are connected to a central intermediate device. Use Ethernet switches.
- **Extended Star** - Additional Ethernet switches interconnect other star topologies.
- **Bus** - Used in legacy networks. All end systems are chained to each other and terminated in some form on each end. Switches are not required to interconnect the end devices. Bus topologies using coax cables were used in legacy Ethernet networks because it was inexpensive and easy to set up.
- **Ring** - End systems are connected to their respective neighbor forming a ring. Unlike the bus topology, the ring does not need to be terminated. Ring topologies were used in legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks.

Half and Full Duplex



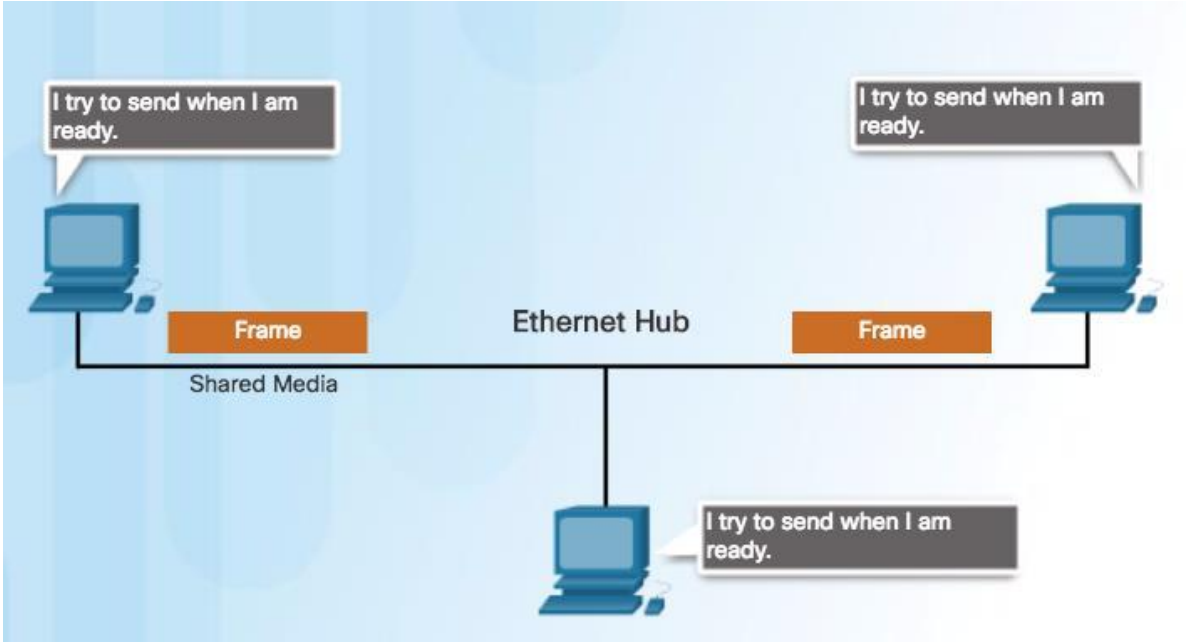
- **Half-Duplex Communication**
  - Both devices can transmit and receive on the media but cannot do so simultaneously.
  - Used in legacy bus topologies and with Ethernet hubs.
  - WLANs also operate in half-duplex.

Half and Full Duplex (Cont.)



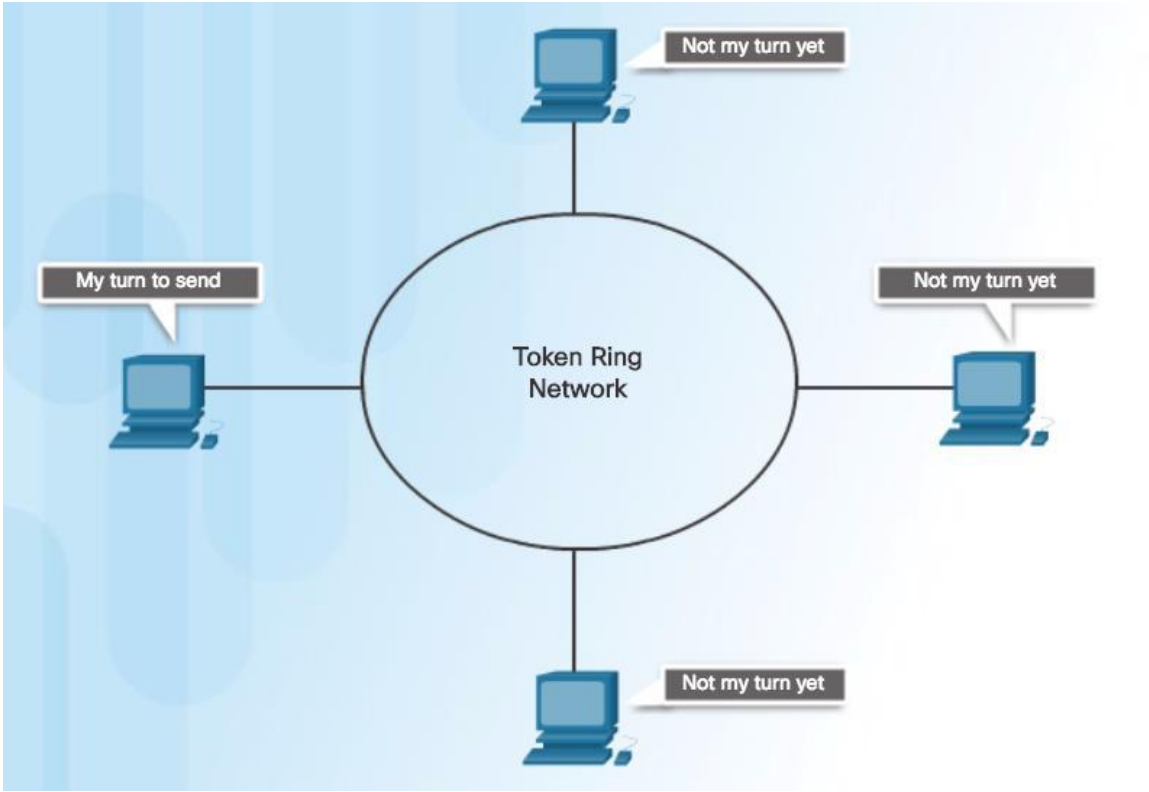
- **Full-Duplex Communication**
  - Both devices can transmit and receive on the media at the same time.
  - Data link layer assumes that the media is available for transmission for both nodes at any time.
  - Ethernet switches operate in full-duplex mode by default, but can operate in half-duplex if connecting to a device such as an Ethernet hub.

Media Access Control Methods



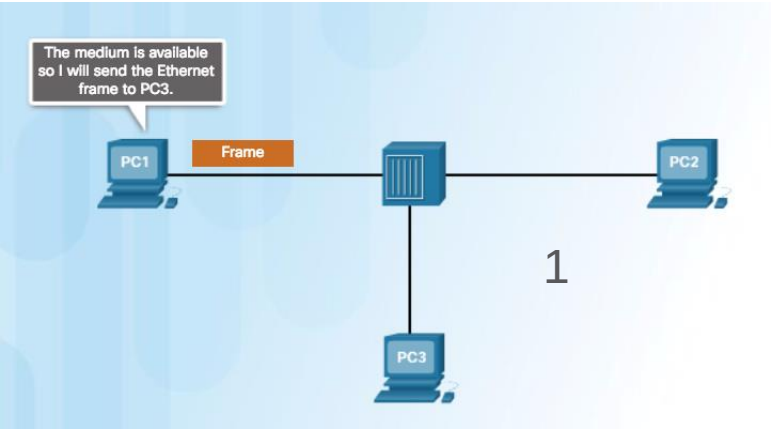
- Contention-Based Access
  - Nodes operate in half-duplex.
  - Compete for the use of the medium.
  - Only one device can send at a time.

Media Access Control Methods (Cont.)

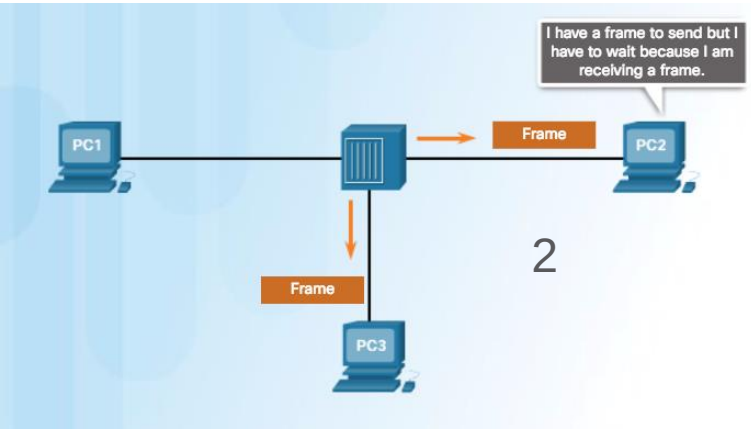


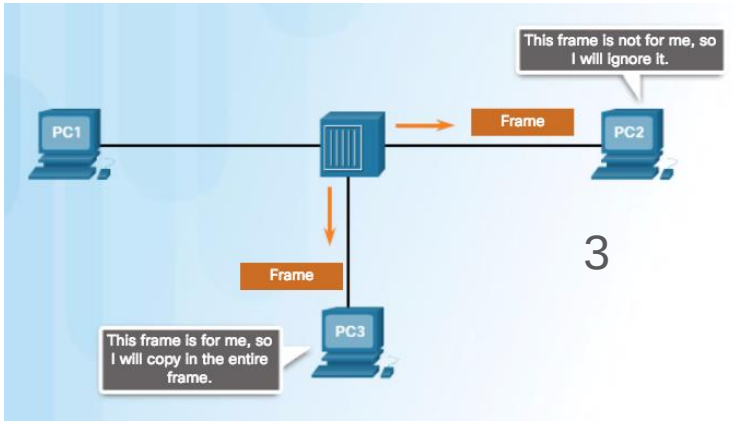
- Controlled Access
  - Each node has its own time to use the medium.
  - Legacy Token Ring LANs are an example

Contention-based Access - CSMA/CD

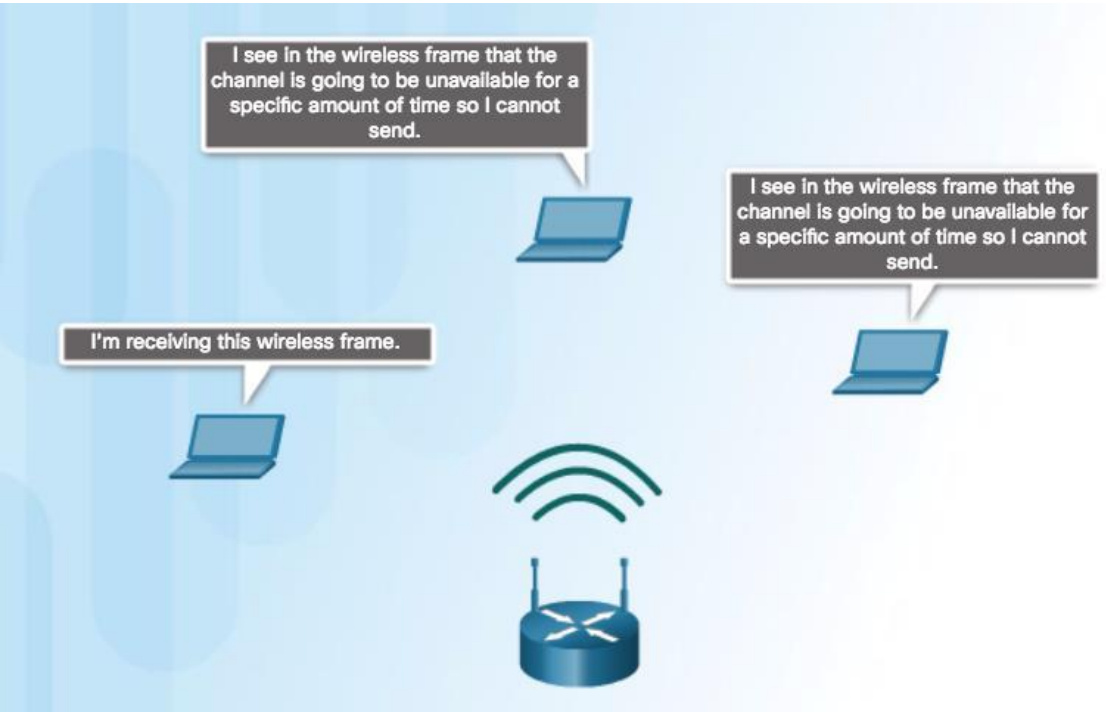


- Carrier Sense Multiple Access/Collision Detection (CSMA/CD) process is used in half-duplex Ethernet LANs.
  - If two devices transmit at the same time, a collision will occur.
  - Both devices will detect the collision on the network.
  - Data sent by both devices will be corrupted and will need to be resent.



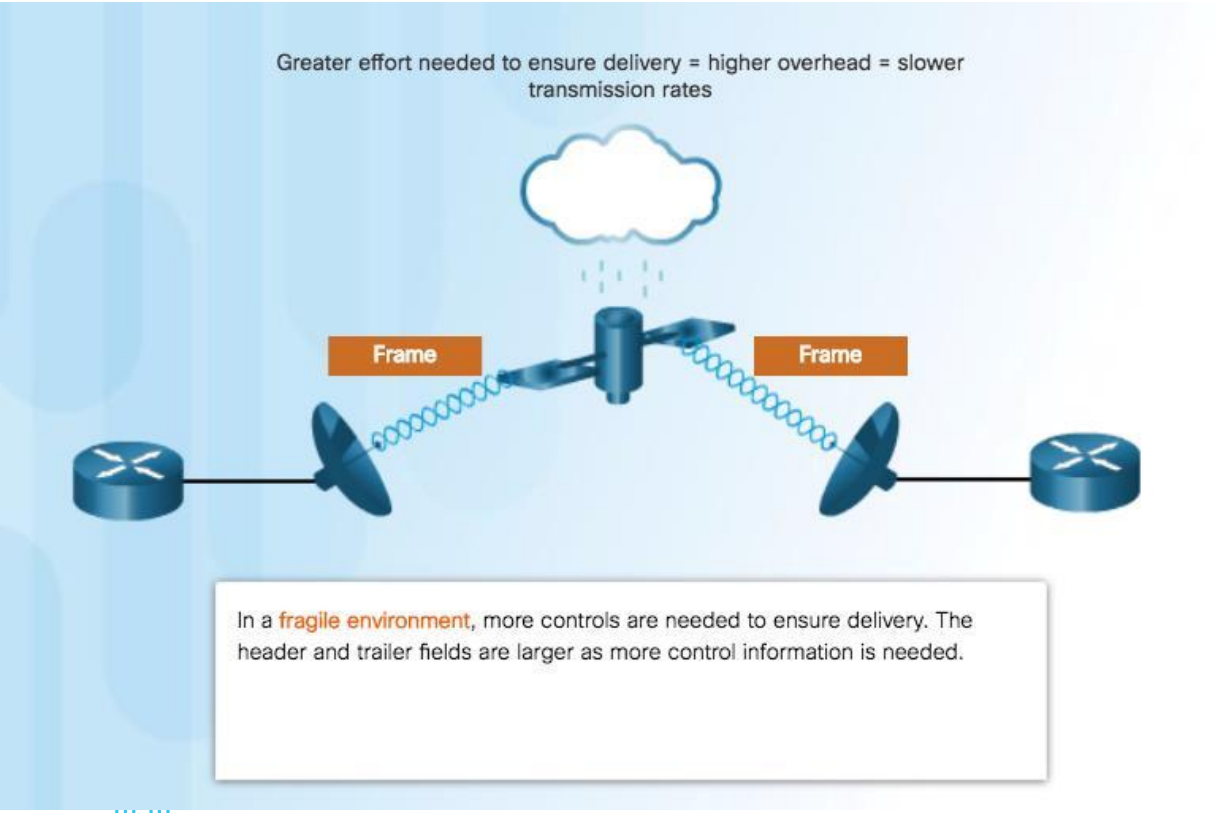


Contention-based Access - CSMA/CA



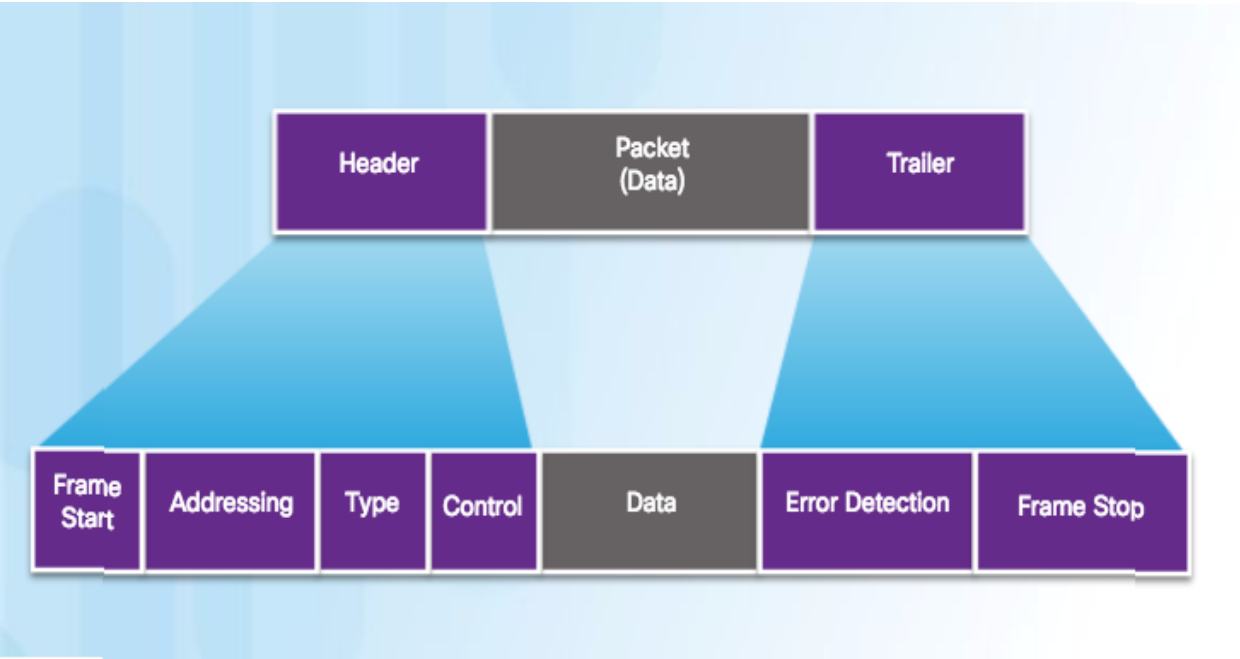
- **CSMA/CA**
  - Uses a method to detect if the media is clear.
  - Does not detect collisions but attempts to avoid them by waiting before transmitting.
- **Note**: Ethernet LANs using switches do not use a contention-based system because the switch and the host NIC operate in full-duplex mode.

The Frame



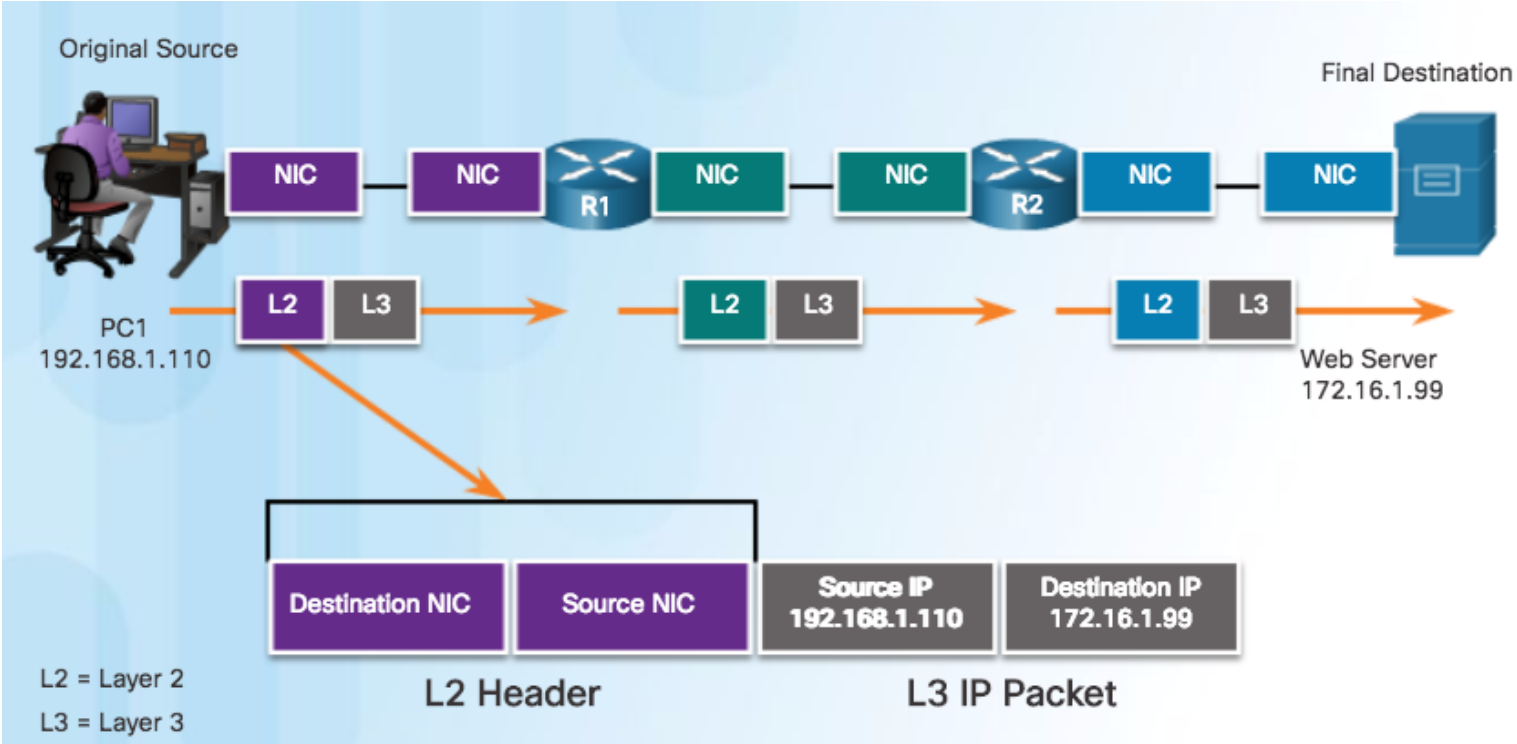
- Each frame type has three basic parts:
  - Header
  - Data
  - Trailer
- Structure of the frame and the fields contained in the header and trailer depend on Layer 3 protocol.

Frame Fields



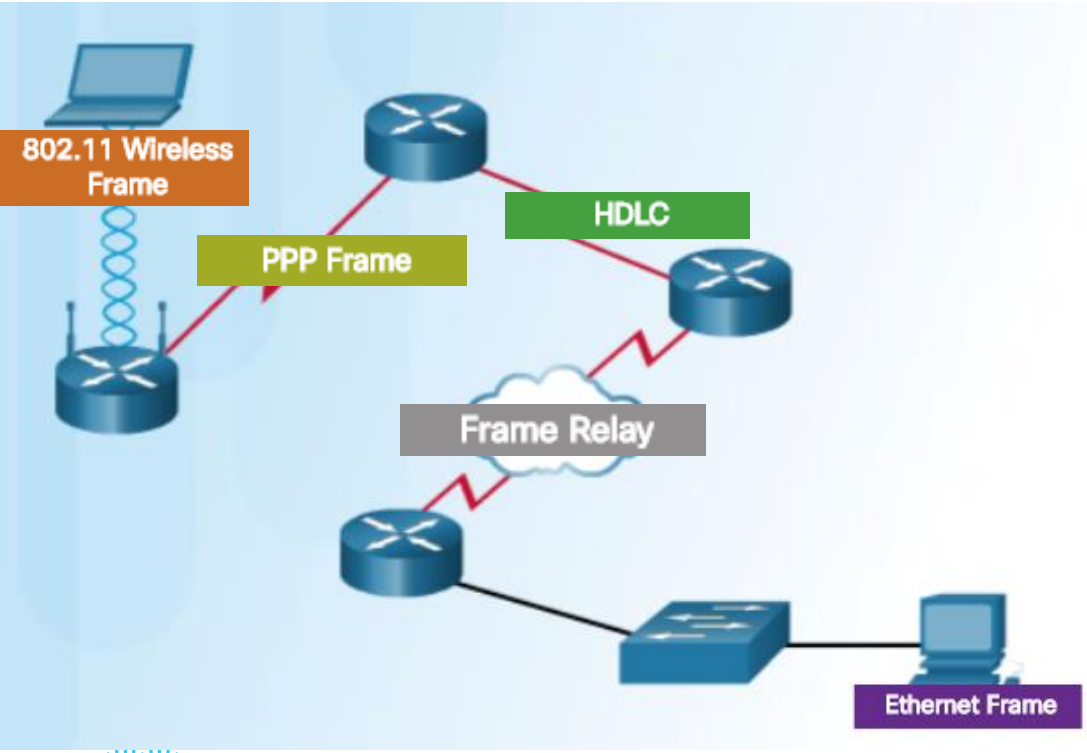
- **Frame start and stop indicator flags** - Identifies the beginning and end limits of the frame.
- **Addressing** - Indicates the source and destination nodes.
- **Type** - Identifies the Layer 3 protocol in the data field.
- **Control** - Identifies special flow control services such as QoS.
- **Data** - Contains the frame payload (i.e., packet header, segment header, and the data).

Layer 2 Addresses



Each data link frame contains the source data link address of the NIC card sending the frame, and the destination data link address of the NIC card receiving the frame.

LAN and WAN Frames



- Layer 2 protocol used for a topology is determined by the technology.
- Data link layer protocols include:
  - Ethernet
  - 802.11 Wireless
  - Point-to-Point Protocol (PPP)
  - HDLC
  - Frame Relay

Data can be corrupted
during transmission.

Some applications require that
errors be detected and corrected.

Types of Errors

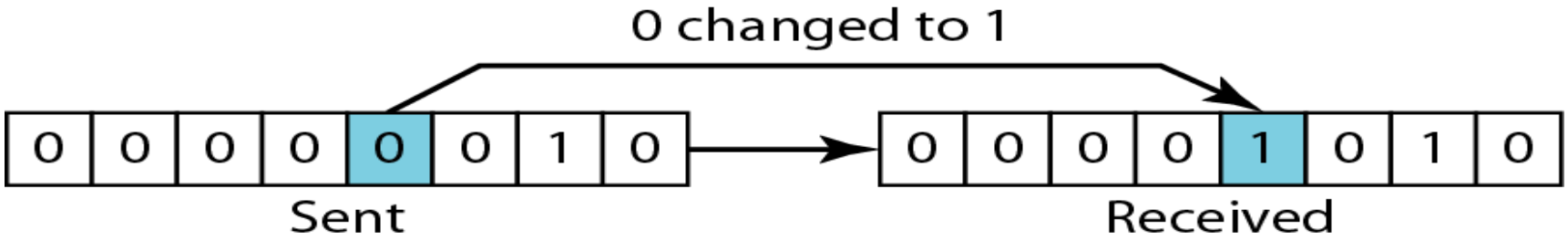
Let us discuss some issues related, directly or indirectly, to error detection and correction.

Topics discussed in this section:

Types of Errors
Redundancy
Detection Versus Correction
Forward Error Correction Versus Retransmission

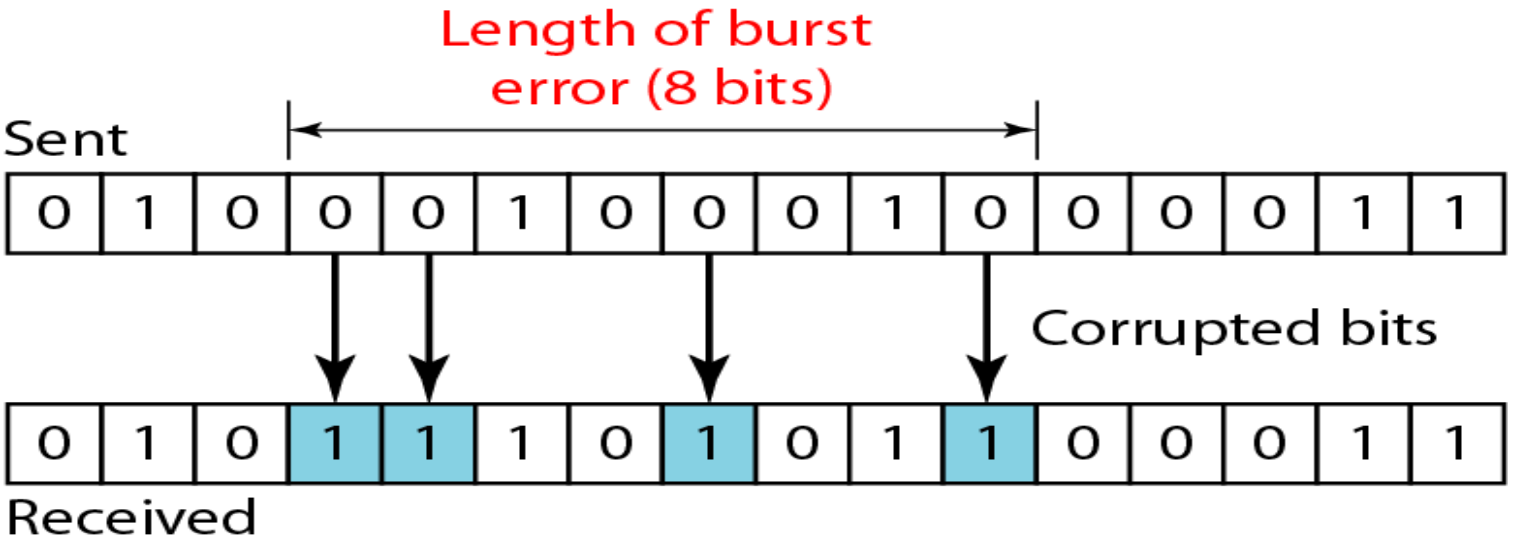
In a single-bit error, only 1 bit in the data unit has changed.

Figure. *Single-bit error*



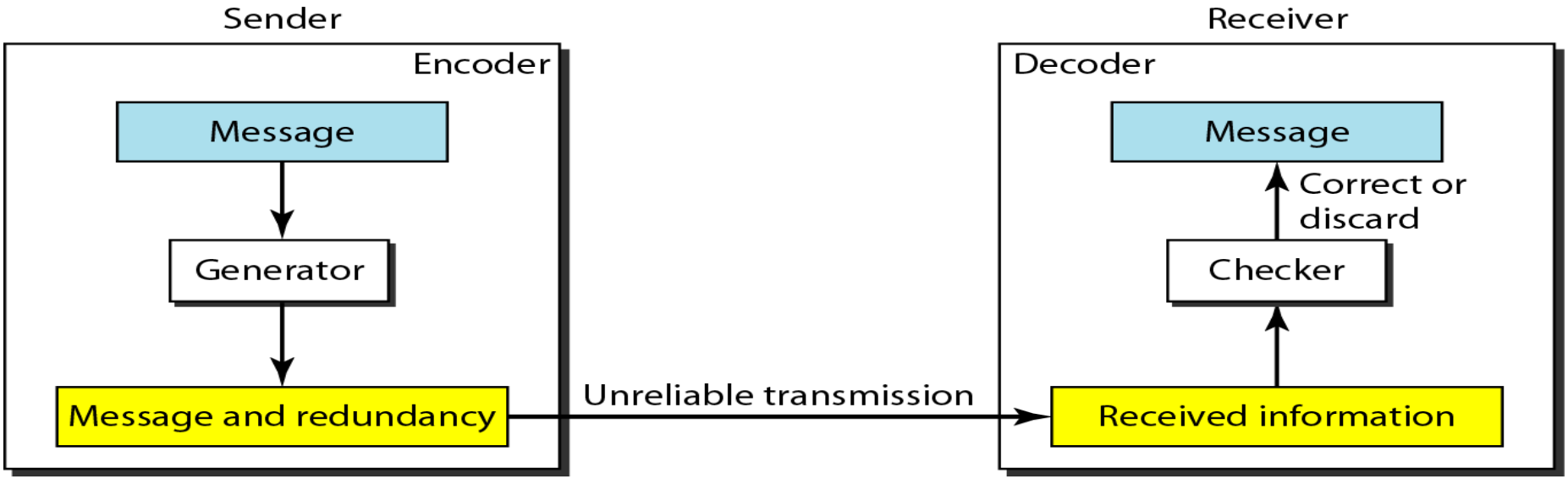
A burst error means that 2 or more bits in the data unit have changed.

Figure. *Burst error of length 8*



To detect or correct errors, we need to send extra (redundant) bits with data.

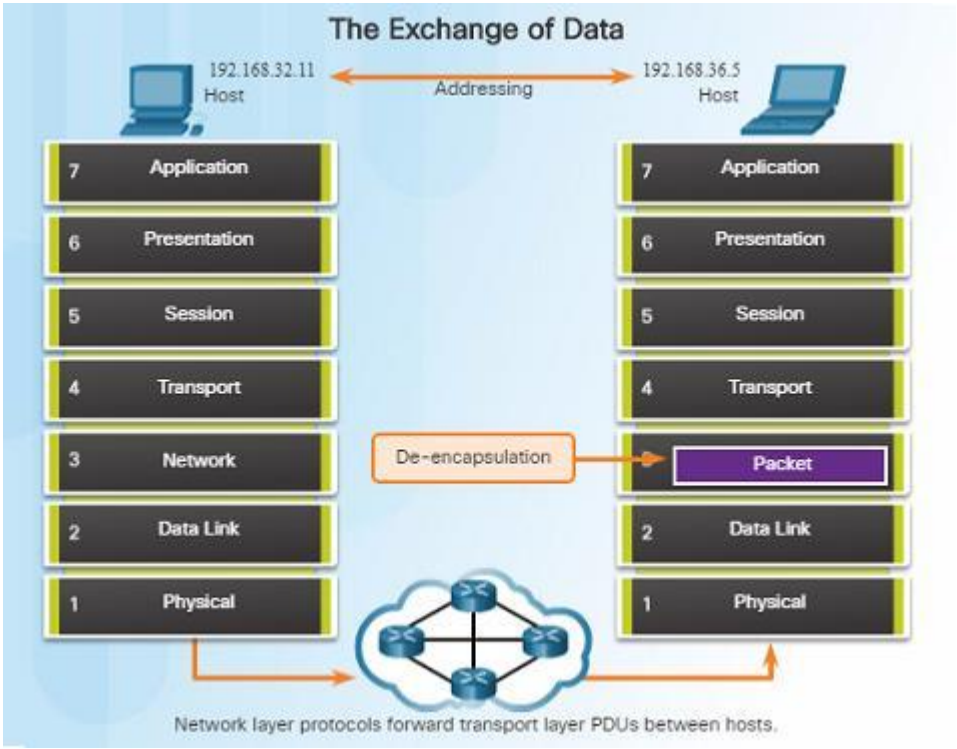
Figure. *The structure of encoder and decoder*



Network Layer Protocols

The Network Layer

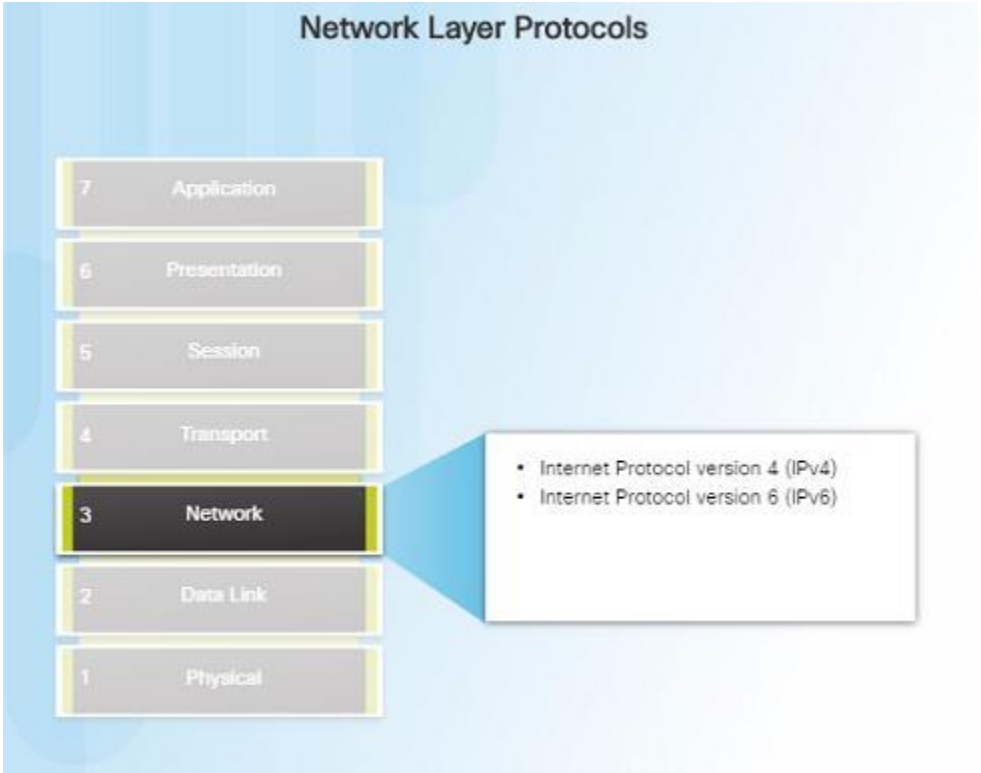
- The network layer, which resides at OSI Layer 3, provides services that allow end devices to exchange data across a network.
- The network layer uses four processes in order to provide end-to-end transport:
  - Addressing of end devices – IP addresses must be unique for identification purposes.
  - Encapsulation – The protocol data units from the transport layer are encapsulated by adding IP header information including source and destination IP addresses.
  - Routing – The network layer provides services to direct packets to other networks. Routers select the best path for a packet to take to its destination network.
  - De-encapsulation – The destination host de-encapsulates the packet to see if it matches its own.



Network Layer Protocols

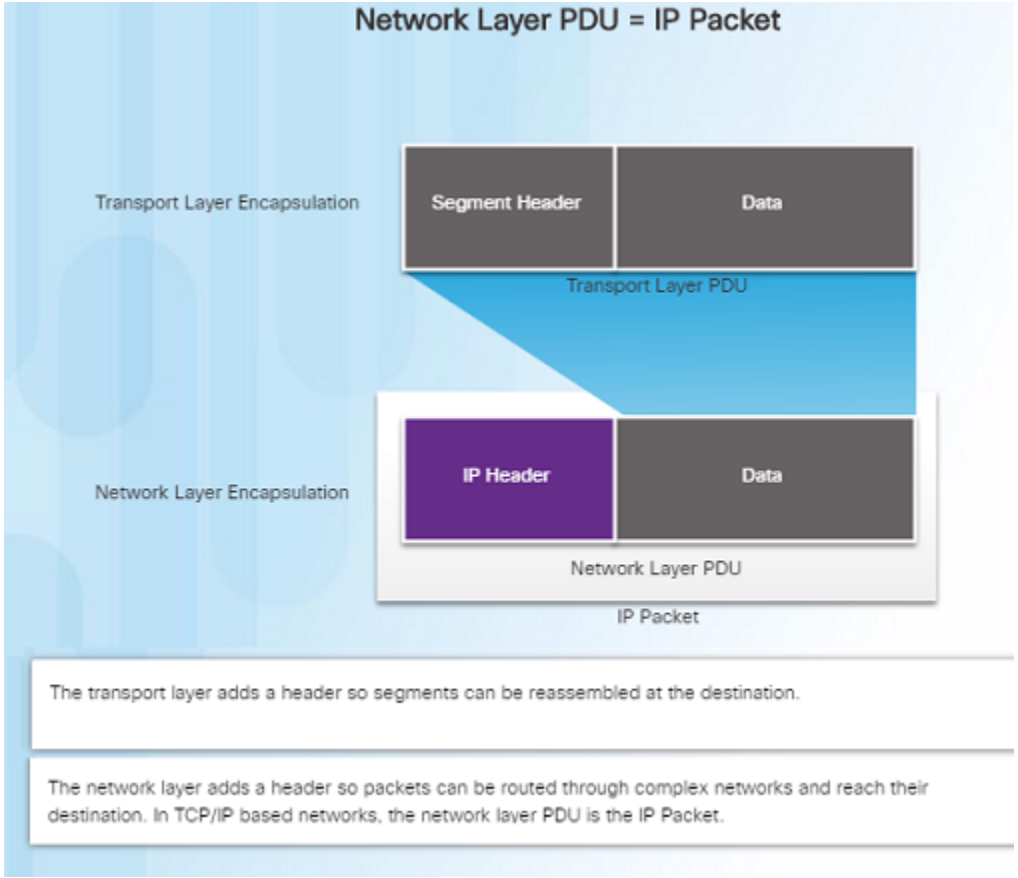
- There are several network layer protocols in existence; however, the most commonly implemented are:
  - Internet Protocol version 4 (IPv4)
  - Internet Protocol version 6 (IPv6)

Note: Legacy network layer protocols are not discussed.



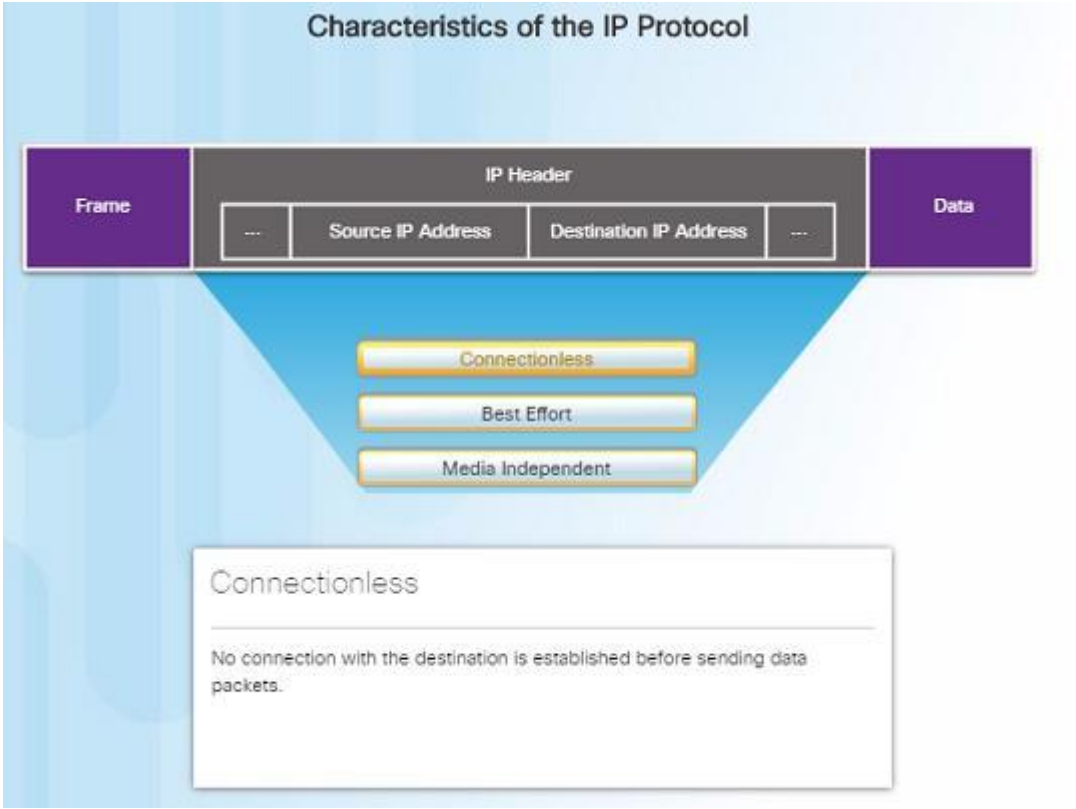
Encapsulating IP

- At the network layer, IP encapsulates the transport layer segment by adding an IP header for the purpose of delivery to the destination host.
- The IP header stays the same from the source to the destination host.
- The process of encapsulating data layer by layer enables the services at different layers to scale without affecting other layers.
- Routers implement different network layer protocols concurrently over a network and use the network layer packet header for routing.



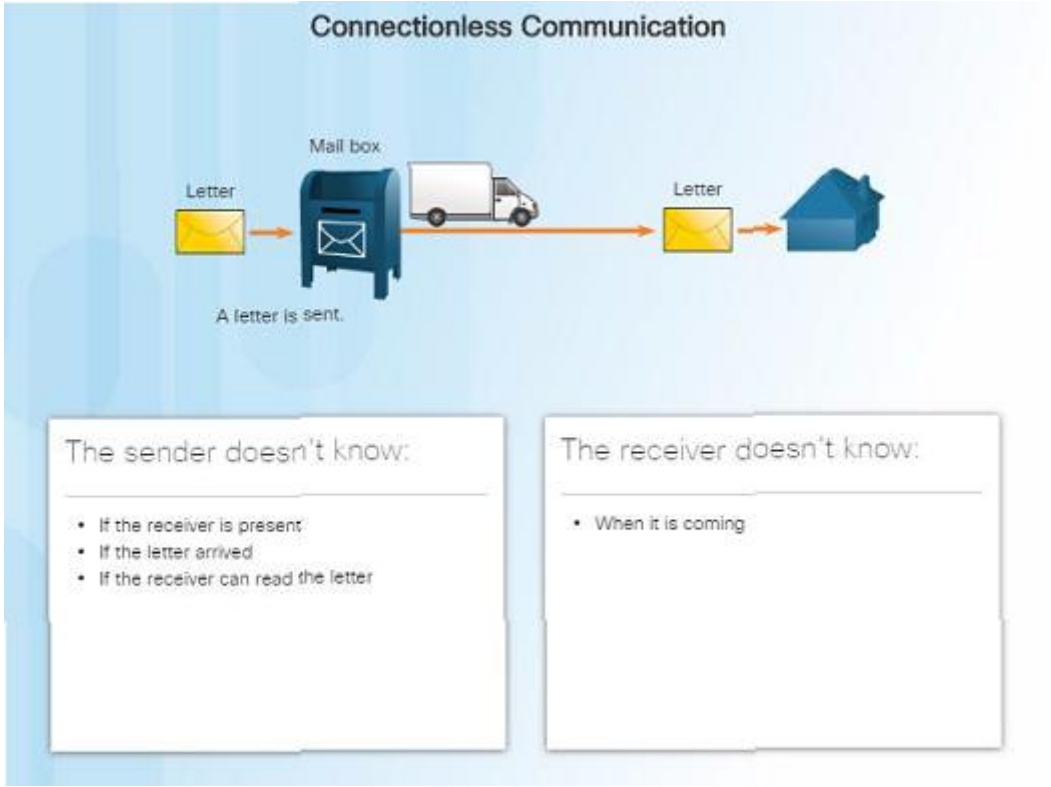
Characteristics of IP

- IP was designed as a protocol with low overhead – it provides only the functions required to deliver a packet from the source to a destination.
- An IP packet is sent to the destination without prior establishment of a connection
- IP was not designed to track and manage the flow of packets.
  - These functions, if required, are performed by other layers – primarily TCP



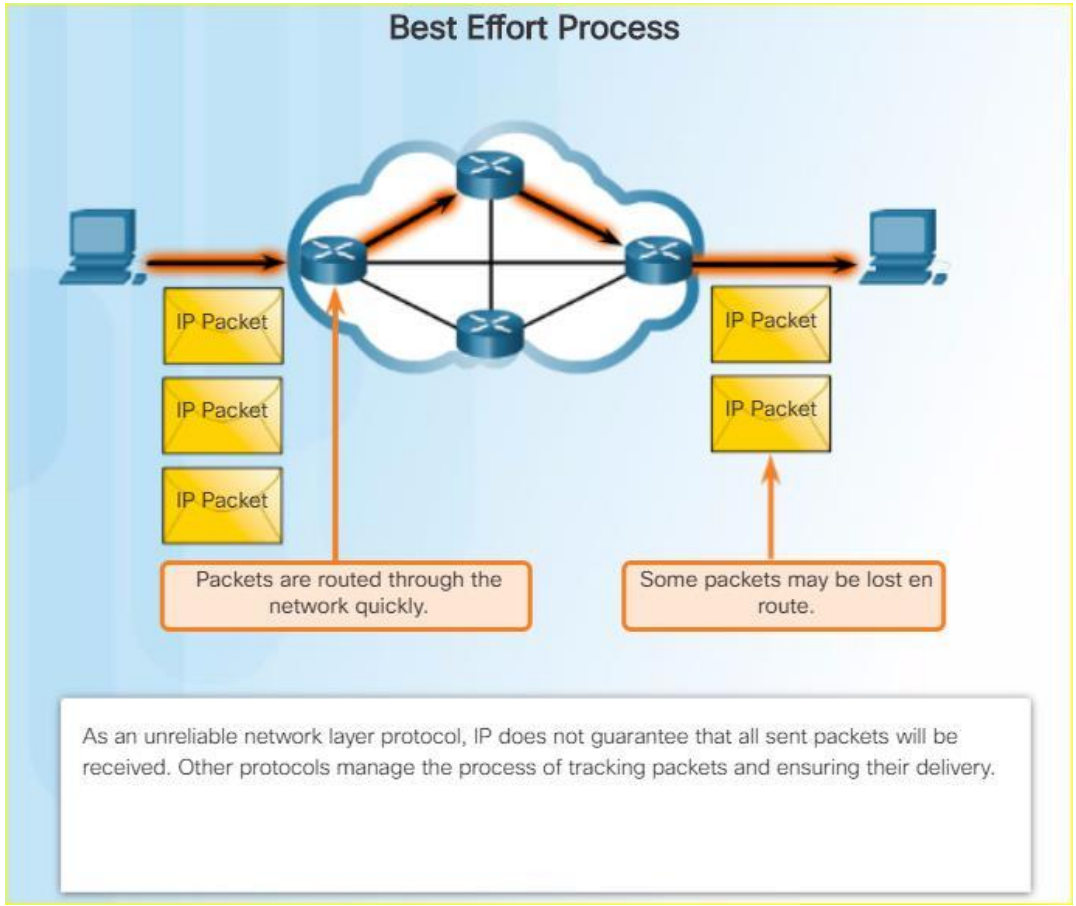
IP - Connectionless

- IP is a connectionless protocol:
  - No dedicated end-to-end connection is created before data is sent.
  - Very similar process as sending someone a letter through snail mail.
  - Senders do not know whether or not the destination is present, reachable, or functional before sending packets.
  - This feature contributes to the low overhead of IP.



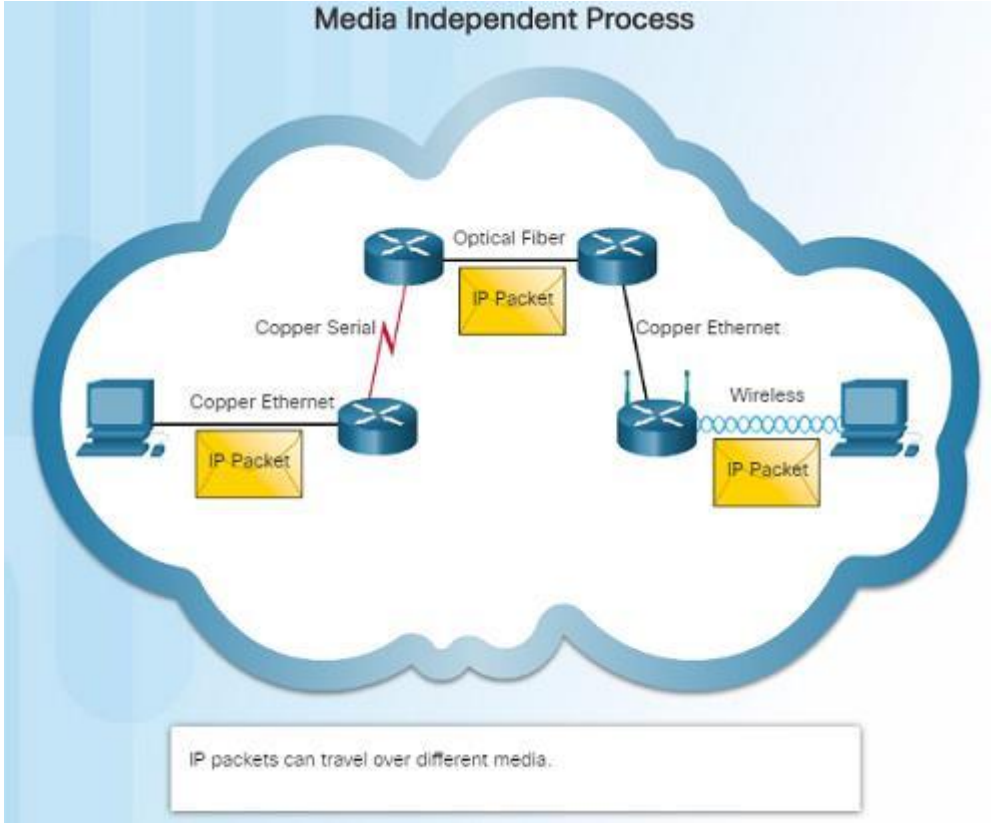
IP – Best Effort Delivery

- IP is a Best Effort Delivery protocol:
  - IP is considered “unreliable” because it does not guarantee that all packets that are sent will be received.
  - Unreliable means that IP does not have the capability to manage and recover from undelivered, corrupt, or out of sequence packets.
  - If packets are missing or not in the correct order at the destination, upper layer protocols/services must resolve these issues.



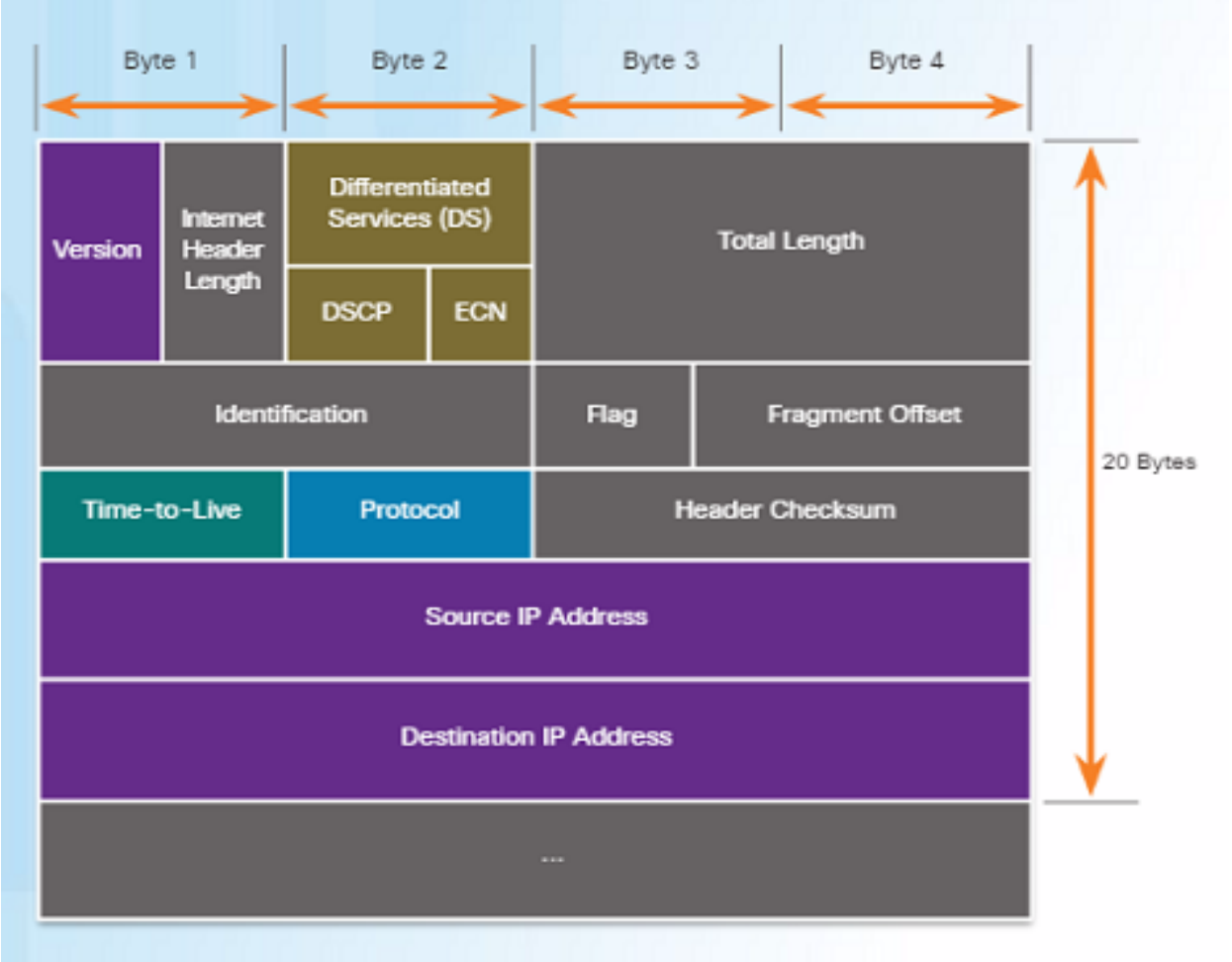
IP – Media Independent

- IP operates independently from the media that carries the data at lower layers of the protocol stack – it does not care if the media is copper cables, fiber optics or wireless.
- The OSI data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium.
- The network layer does have a maximum size of the PDU that can be transported – referred to as MTU (maximum transmission unit).
- The data link layer tells the network layer the MTU.



IPv4 Packet Header

- An IPv4 packet header consists of the fields containing binary numbers. These numbers identify various settings of the IP packet which are examined by the Layer 3 process.
- Significant fields include:
  - Version – Specifies that the packet is IP version 4
  - Differentiated Services or DiffServ (DS) – Used to determine the priority of each packet on the network.
  - Time-to-Live (TTL) – Limits the lifetime of a packet – decreased by one at each router along the way.
  - Protocol – Used to identify the next level protocol.
  - Source IPv4 Address – Source address of the packet.
  - Destination IPv4 Address – Address of destination.

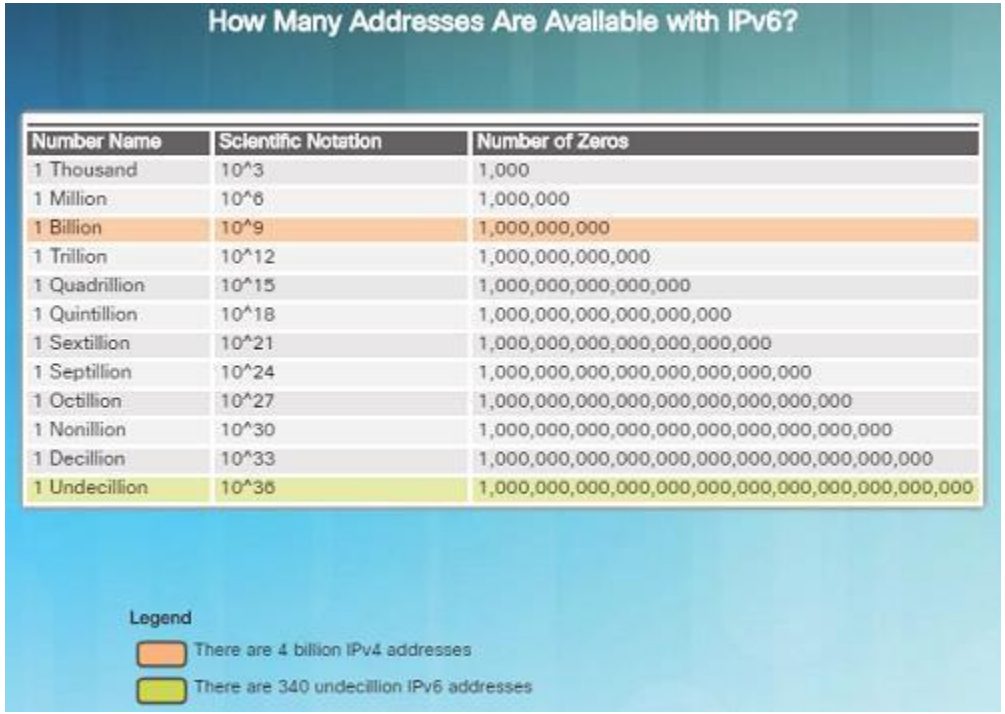


Limitations of IPv4

- IPv4 has been updated to address new challenges.
- Three major issues still exist with IPv4:
  - IP address depletion – IPv4 has a limited number of unique public IPv4 addresses available. Although there are about 4 billion IPv4 addresses, the exponential growth of new IP-enabled devices has increased the need.
  - Internet routing table expansion – A routing table contains the routes to different networks in order to make the best path determination. As more devices and servers are connected to the network, more routes are created. A large number of routes can slow down a router.
  - Lack of end-to-end connectivity – Network Address Translation (NAT) was created for devices to share a single IPv4 address. However, because they are shared, this can cause problems for technologies that require end-to-end connectivity.

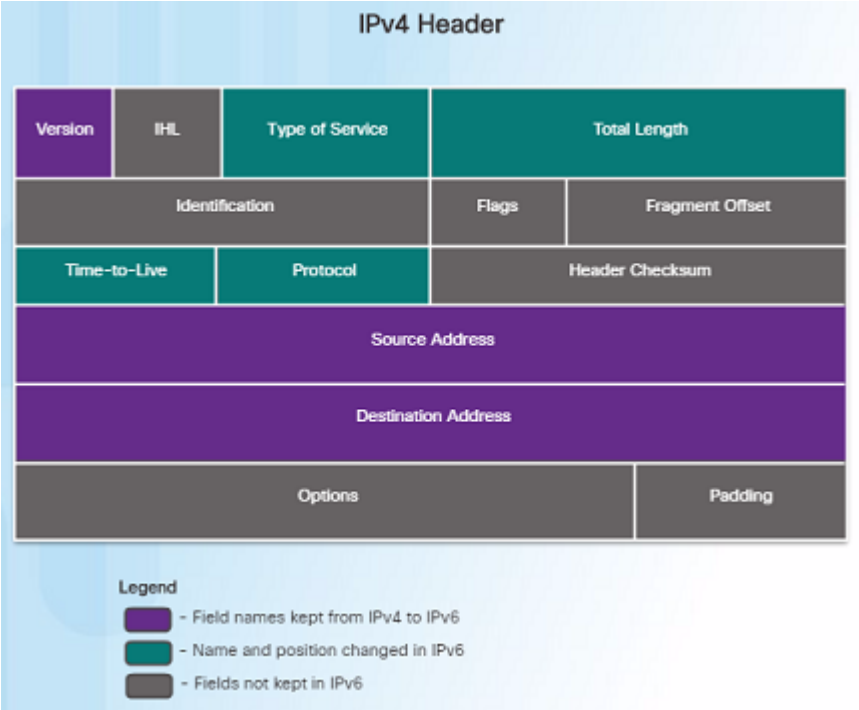
Introducing IPv6

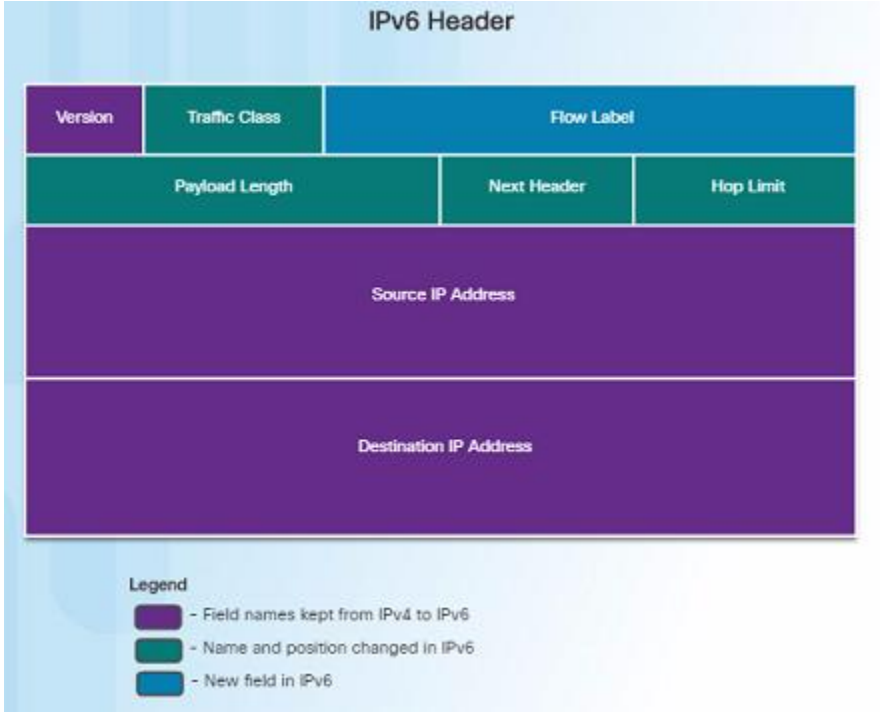
- In the early ‘90s, the IETF started looking at a replacement for IPv4 – which led to IPv6.
- Advantages of IPv6 over IPv4 include:
  - Increased address space – based on 128-bit addressing vs. 32-bit with IPv4
  - Improved packet handling – fewer fields with IPv6 than IPv4
  - Eliminates the need for NAT – no need to share addresses with IPv6
- There are roughly enough IPv6 addresses for every grain of sand on Earth.



Encapsulating IPv6

- The IPv6 header is simpler than the IPv4 header.

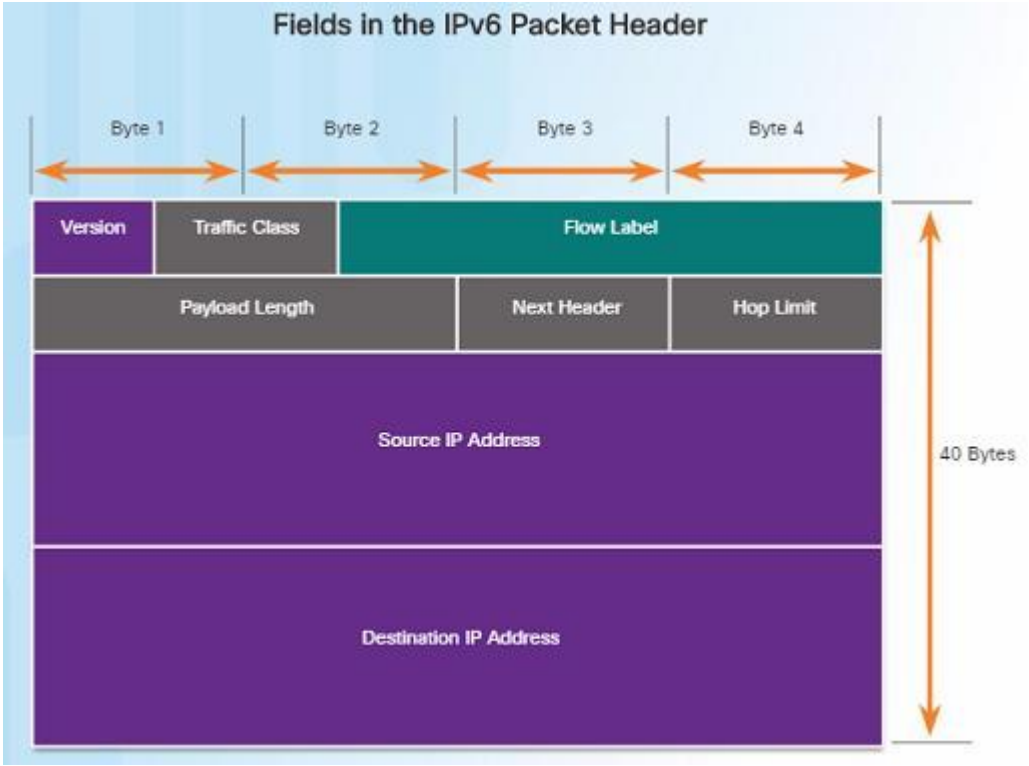




Encapsulating IPv6 (Cont.)

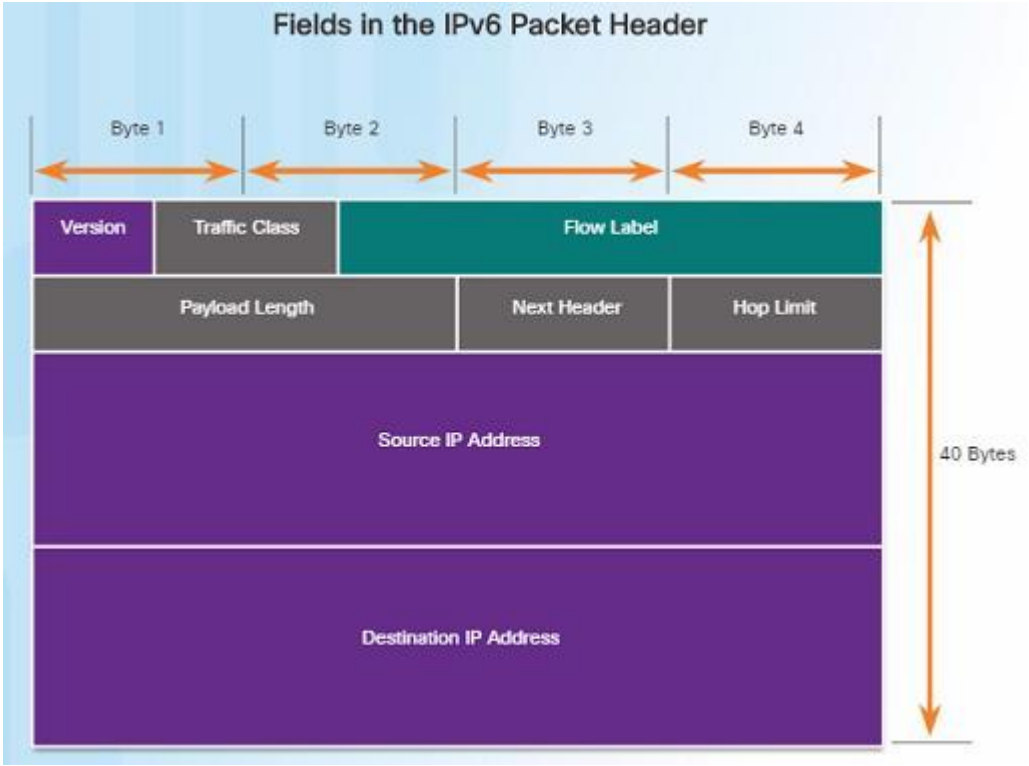
- Advantages of IPv6 over IPv4 using the simplified header:
  - Simplified header format for efficient packet handling
  - Hierarchical network architecture for routing efficiency
  - Auto-configuration for addresses
  - Elimination of need for network address translation (NAT) between private and public addresses

IPv6 Packet Header



- IPv6 packet header fields:
  - **Version** – Contains a 4-bit binary value set to 0110 that identifies it as a IPv6 packet.
  - **Traffic Class** – 8-bit field equivalent to the IPv4 Differentiated Services (DS) field.
  - **Flow Label** – 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
  - **Payload Length** – 16-bit field indicates the length of the data portion or payload of the packet.
  - **Next Header** – 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying.

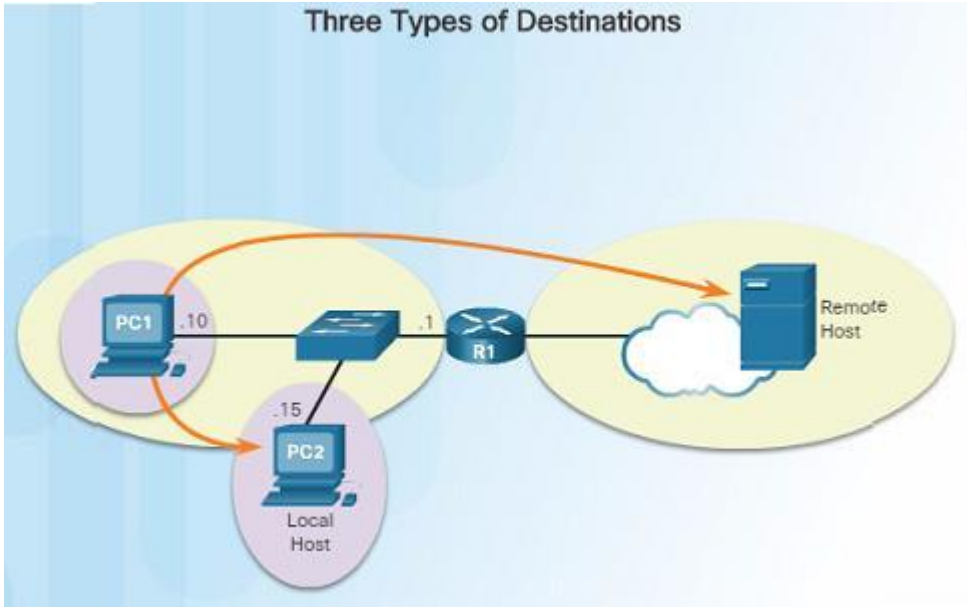
IPv6 Packet Header (Cont.)



- IPv6 packet header fields:
  - **Hop Limit** – 8-bit field replaces the IPv4 TTL field. This value is decremented by 1 as it passes through each router. When it reaches zero, the packet is discarded.
  - **Source IPv6 Address** – 128-bit field that identifies the IPv6 address of the sending host.
  - **Destination IPv6 Address** – 128-bit field that identifies the IPv6 address of the receiving host.

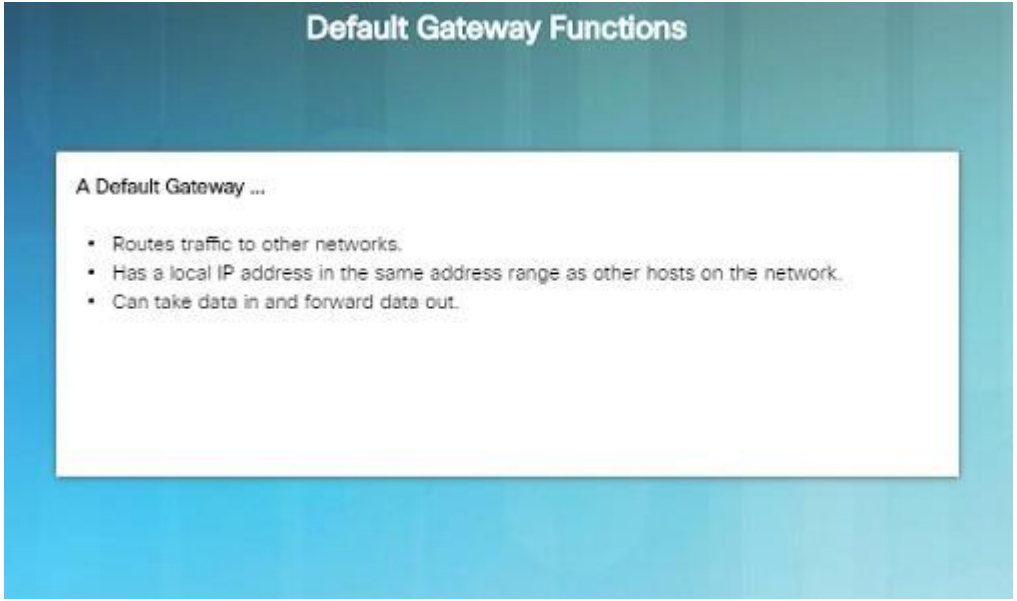
Routing

Host Forwarding Decision



- An important role of the network layer is to direct packets between hosts.
- A host can send a packet to:
  - Itself – A host can ping itself for testing purposes using 127.0.0.1 which is referred to as the loopback interface.
  - Local host – This is a host on the same local network as the sending host. The hosts share the same network address.
  - Remote host – This is a host on a remote network. The hosts do not share the same network address.
- The source IPv4 address and subnet mask is compared with the destination address and subnet mask in order to determine if the host is on the local network or remote network.

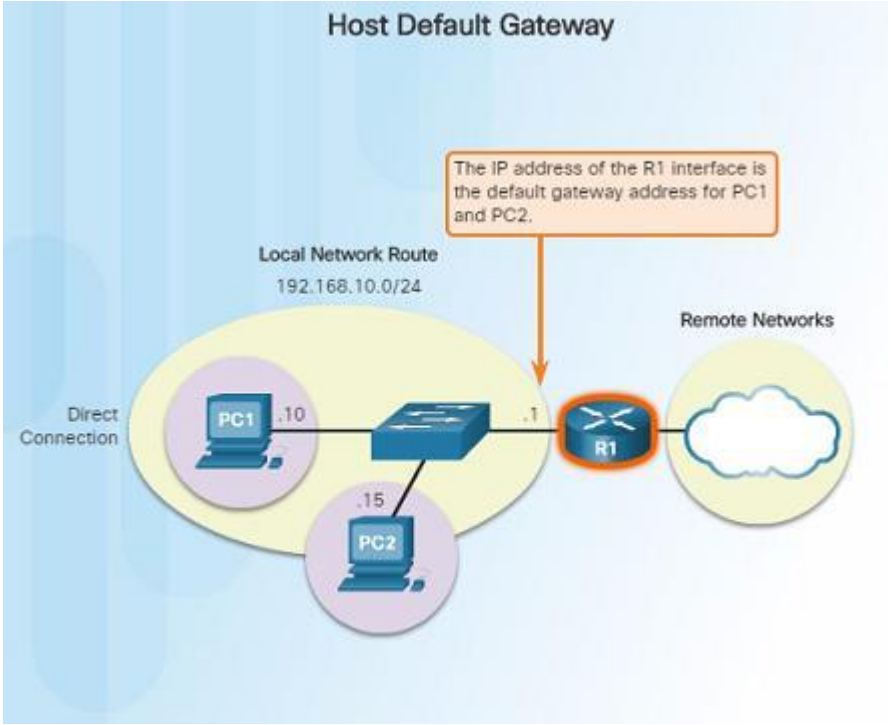
Default Gateway



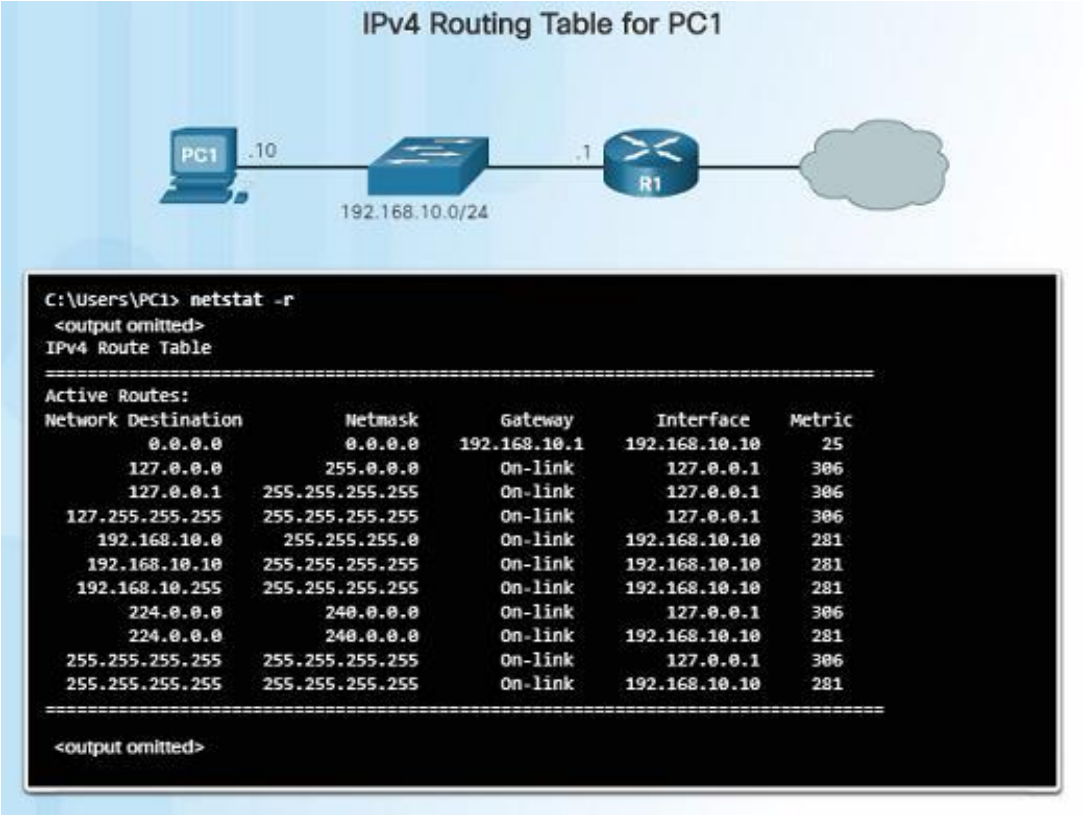
- The default gateway is the network device that can route traffic out to other networks. It is the router that routes traffic out of a local network.
- This occurs when the destination host is not on the same local network as the sending host.
- The default gateway will know where to send the packet using its routing table.
- The sending host does not need to know where to send the packet other than to the default gateway – or router.

Using the Default Gateway

- A host's routing table usually includes a default gateway address – which is the router IP address for the network that the host is on.
- The host receives the IPv4 address for the default gateway from DHCP, or it is manually configured.
- Having a default gateway configured creates a default route in the routing table of a host - which is the route the computer will send a packet to when it needs to contact a remote network.



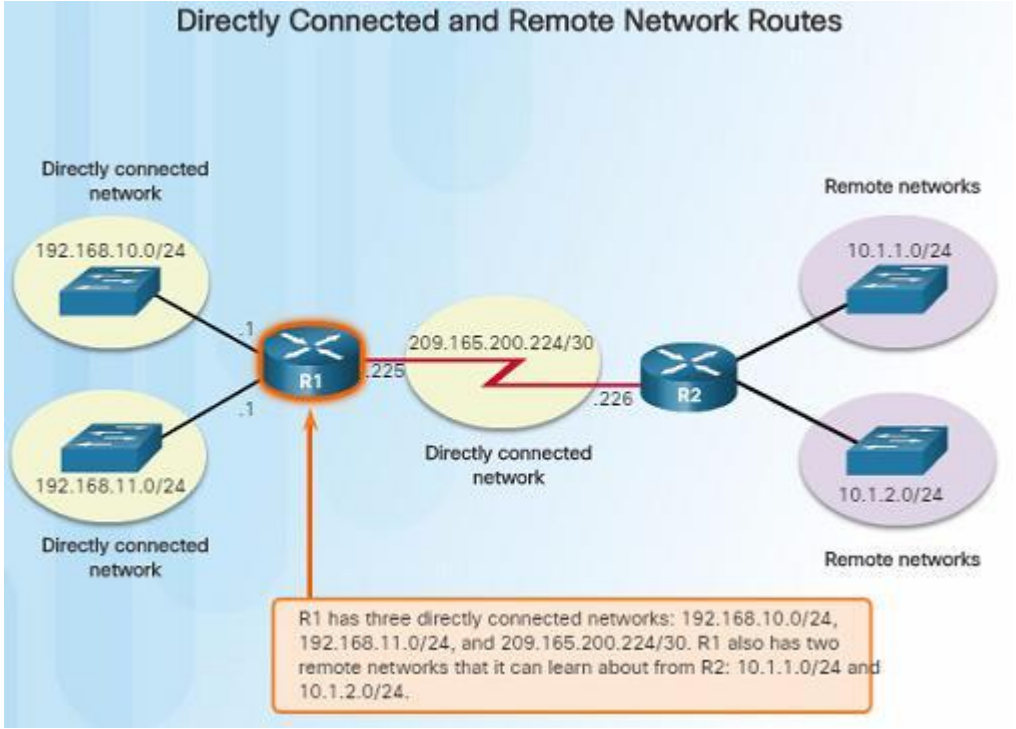
Host Routing Tables




```
C:\Users\PC1> netstat -r
 <output omitted>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
 <output omitted>
```

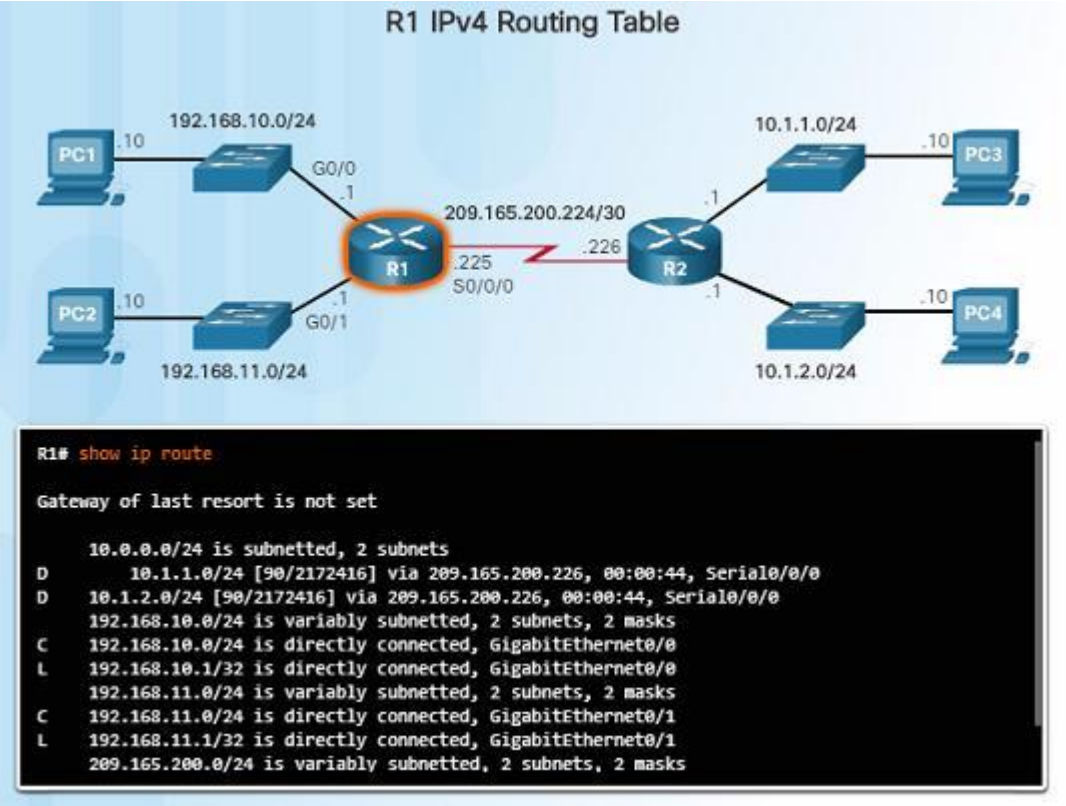
- On a Windows host, you can display the routing table using:
  - **route print**
  - **netstat -r**
- Three sections will be displayed:
  - Interface List – Lists the Media Access Control (MAC) address and assigned interface number of network interfaces on the host.
  - IPv4 Route Table – Lists all known IPv4 routes.
  - IPv6 Route Table – Lists all known IPv6 routes.

Router Packet Forwarding Decision



- When a router receives a packet destined for a remote network, the router has to look at its routing table to determine where to forward the packet.
- A router's routing table contains:
  - Directly-connected routes – These routes come from the active router interfaces configured with IP addresses.
  - Remote routes – These routes come from remote networks connected to other routers. They are either configured manually or learned through a dynamic routing protocol.
  - Default route – This is where the packet is sent when a route does not exist in the routing table.

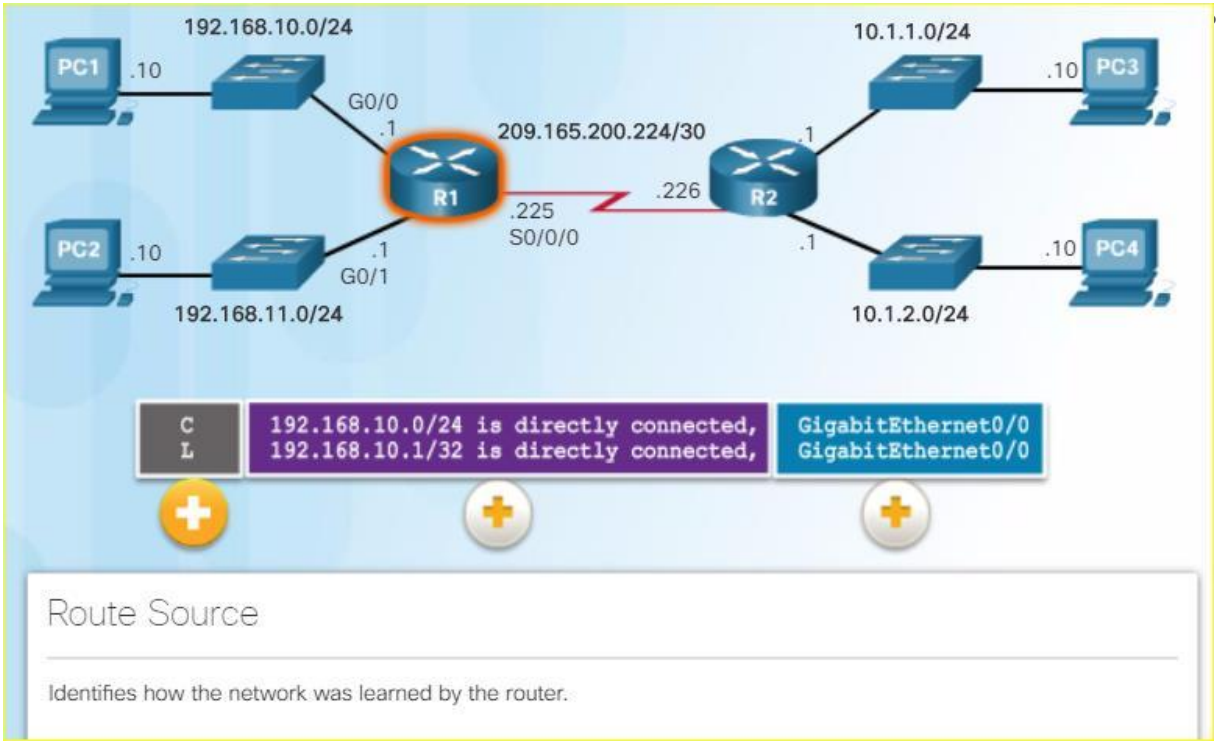
IPv4 Router Routing Table



- On a Cisco IOS router, the **show ip route** command is used to display the router's IPv4 routing table. The routing table shows:
  - Directly connected and remote routes
  - How each route was learned
  - Trustworthiness and rating of the route
  - When the route was last updated
  - Which interface is used to reach the destination

- A router examines an incoming packet's header to determine the destination network. If there's a match, the packet is forwarded using the specified information in the routing table.

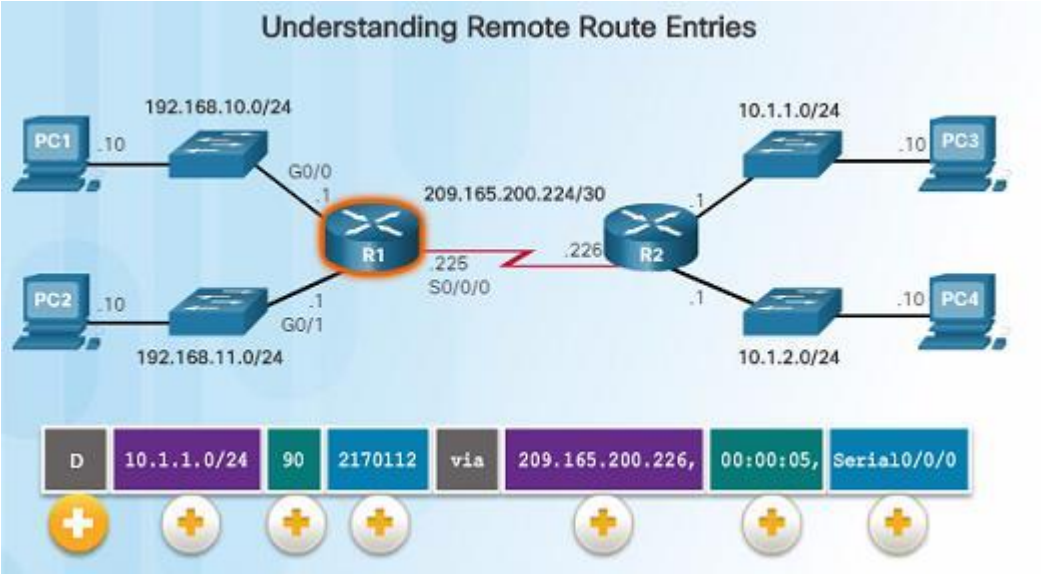
Directly Connected Routing Table Entries



When a router interface is configured and activated, the following two routing table entries are created automatically:

- **C** – Identifies that the network is directly connected and the interface is configured with an IP address and activated.
- **L** – Identifies that it is a local interface. This is the IPv4 address of the interface on the router.

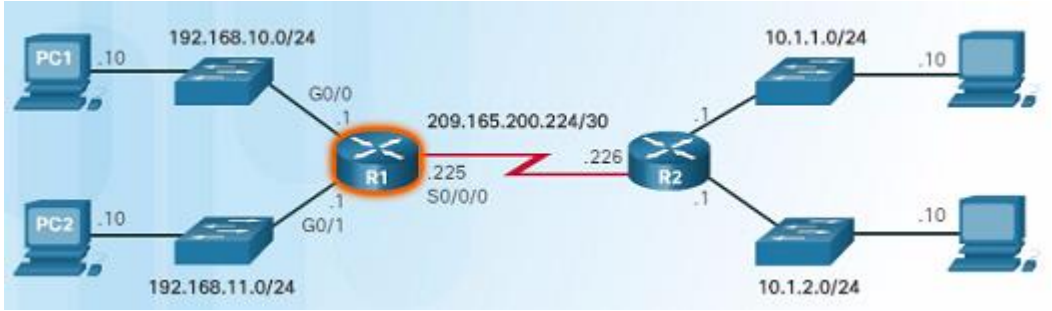
Understanding Remote Route Entries



- The **D** represents the Route Source which is how the network was learned by the router. **D** identifies the route as an EIGRP route or (Enhanced Interior Gateway Routing Protocol)

- **10.1.1.0/24** identifies the destination network.
- **90** is the administrative distance for the corresponding network – or the trustworthiness of the route. The lower the number, the more trustworthy it is.
- **2170112** – represents the metric or value assigned to reach the remote network. Lower values indicate preferred routes.
- **209.165.200.226** – Next-hop or IP address of the next router to forward the packet.
- **00:00:05** - Route Timestamp identifies when the router was last heard from.
- **Serial/0/0/0** – Outgoing Interface

Next-Hop Address




```
R1# show ip route
<output omitted>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D     10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
      Serial0/0/0
D     10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
      Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0
L     192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C     192.168.11.0/24 is directly connected, GigabitEthernet0/1
L     192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

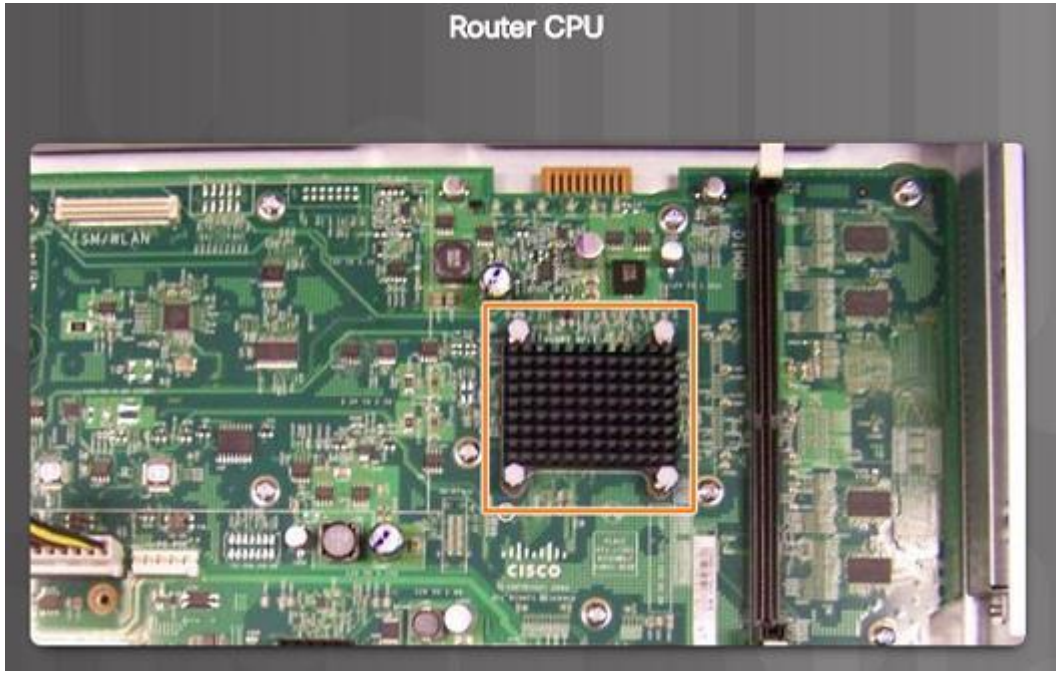
- When a packet arrives at a router destined for a remote network, it will send the packet to the next hop address corresponding to the destination network address in its routing table.
- For example, if the R1 router in the figure to the left receives a packet destined for a device on the 10.1.1.0/24 network, it will send it to the next hop address of 209.165.200.226.
- Notice in the routing table, a default gateway address is not set – if the router receives a packet for a network that isn't in the routing table, it will be dropped.

Routers

A Router is a Computer

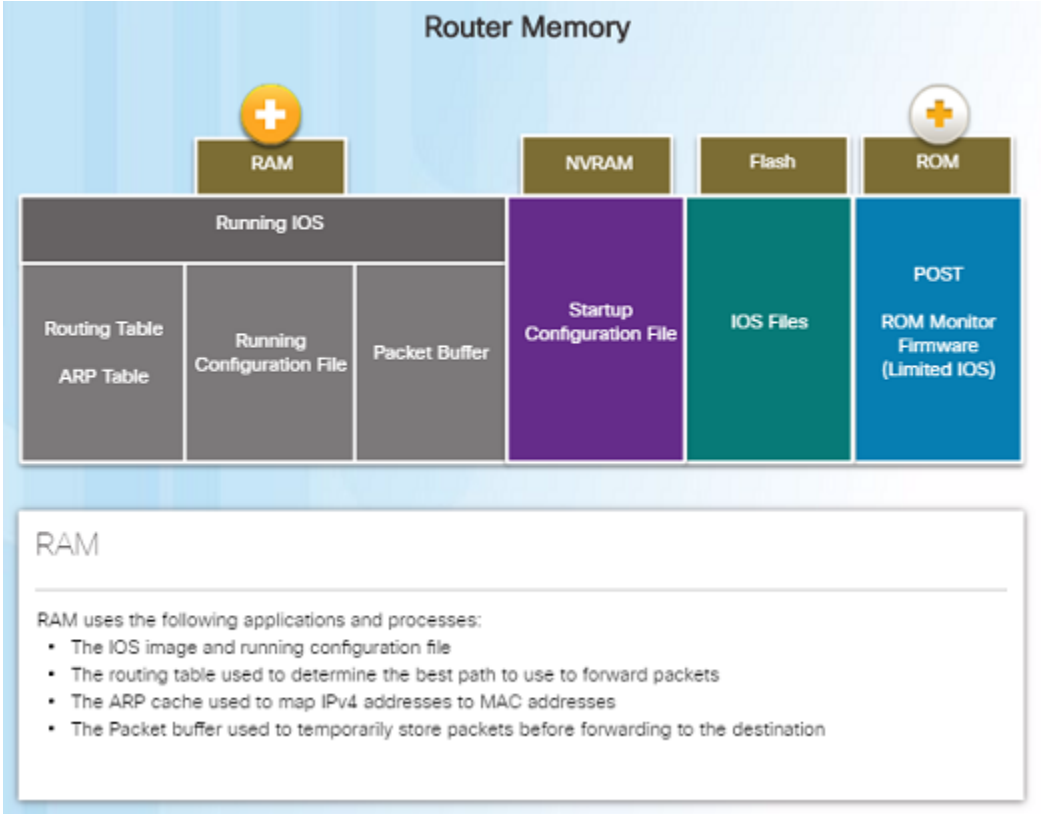
- A router is a computer. Like computers, a router requires a CPU, an operating system, and memory.
- Cisco routers are designed to meet the needs of wide variety of businesses and networks:
  - Branch – Teleworkers, small businesses, and medium-size branch sites.
  - WAN – Large businesses, organizations and enterprises.
  - Service Provider – Large service providers.
- The focus of the CCNA certification is on the branch family of routers.

Router CPU and OS



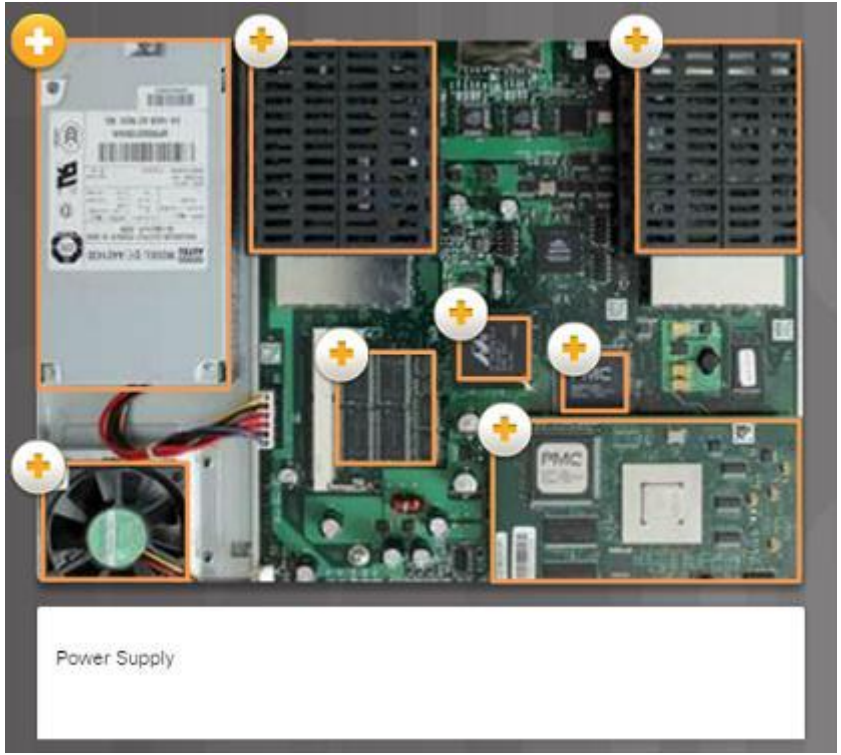
- Like computers, Cisco routers require a CPU to execute OS instructions including system initialization, routing functions and switching functions.
- The component highlighted in the figure to the left is the CPU of a Cisco 1941 with the heatsink attached. A heatsink is used to dissipate the heat from the CPU for cooling purposes.
- The CPU requires an operating system to provide routing and switching functions. Most Cisco devices use the Cisco Internetwork Operating System (IOS).

Router Memory



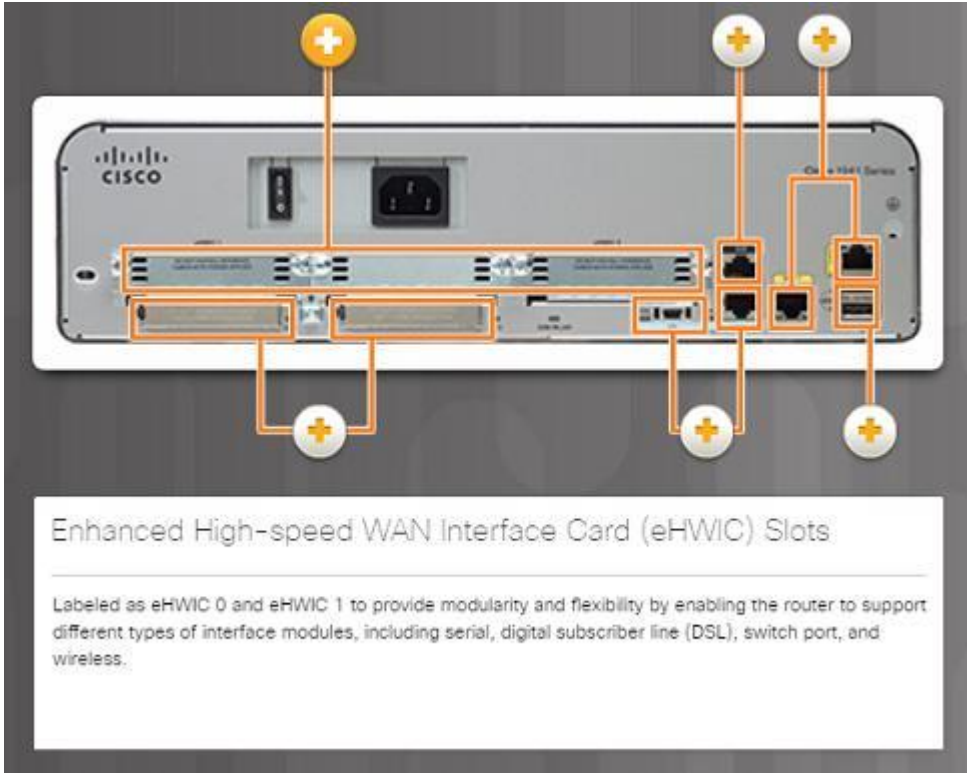
- Volatile memory – requires continual power to store information.
- Non-volatile memory – does not require continual power.
- A router uses four types of memory:
  - RAM – Volatile memory used to store applications, processes, and data needed to be executed by the CPU.
  - ROM – Non-volatile memory used to store crucial operational instructions and a limited IOS. ROM is firmware embedded on an integrated circuit inside of the router.
  - NVRAM – Non-volatile memory used as permanent storage for the startup configuration file (startup-config).
  - Flash – Non-volatile memory used as permanent storage for the IOS and other operating system files such as log or backup files.

Inside a Router



- There are numerous types and models of routers, however, they all have the same general hardware components:
  - Power supply
  - Cooling fan
  - SDRAM - Synchronous Dynamic RAM
  - Non-volatile RAM (NVRAM)
  - CPU
  - Heat shields
  - Advanced Integration Module (AIM)

Connect to a Router



- Cisco devices, routers, and switches typically interconnect many devices. The Cisco 1941 router backplane includes the following ports and connections:
  - Enhanced High-speed WAN Interface Card (eHWIC) Slots
  - Auxiliary (AUX) – RJ-45 port for remote management.
  - Console Port – Used for initial configuration and Command Line Interface access – RJ-45 or USB Type-B (mini-B USB)
  - Gigabit Ethernet used to provide LAN access by connecting to switches, users, or to other routers.
  - Compact Flash Slots – Labeled as CF0 and CF1 and used to provide increased storage flash space upgradable to 4GB.
  - USB port – used to provide additional storage space.

LAN and WAN Interfaces

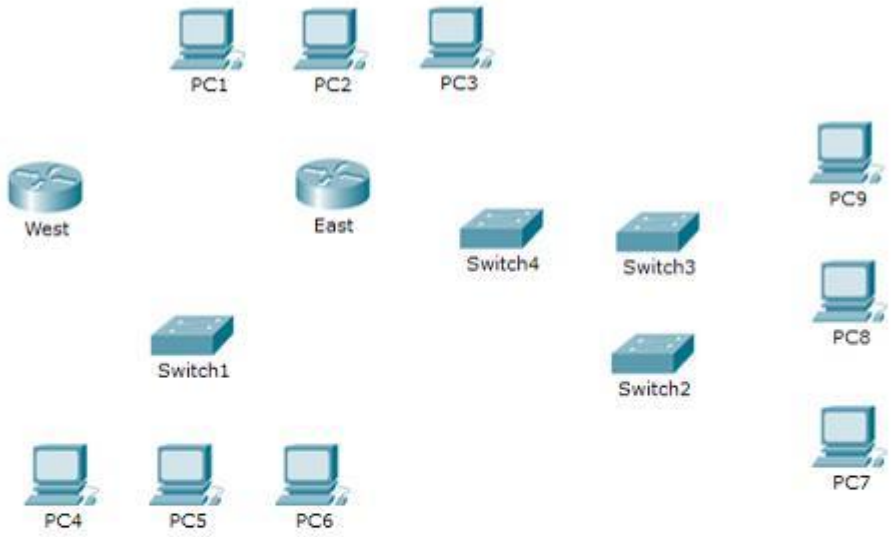
- Cisco router connections can be classified in two categories:
  - In-band router interfaces – LAN and WAN interfaces
  - Management ports – Console and AUX ports

- The most common ways to access user EXEC mode in the CLI environment on a Cisco router:
  - Console – This is a physical management port that provides out-of-band access to the Cisco router. Out-of-band means that it is dedicated and does not require network services to be configured on the router.
  - Secure Shell (SSH) – This is a secure method of remotely establishing a CLI connection over a network. SSH does require active networking services configured.
  - Telnet – Telnet is an insecure method of remotely establishing a CLI session through a virtual interface over a network. The connection is not encrypted.

Packet Tracer – Exploring Internetworking Devices

- In this Packet Tracer activity, you will explore different options available on internetworking devices.
- You will be required to determine which options provide the necessary connectivity when connecting multiple devices.

Topology



Objectives

Part 1: Identify Physical Characteristics of Internetworking Devices

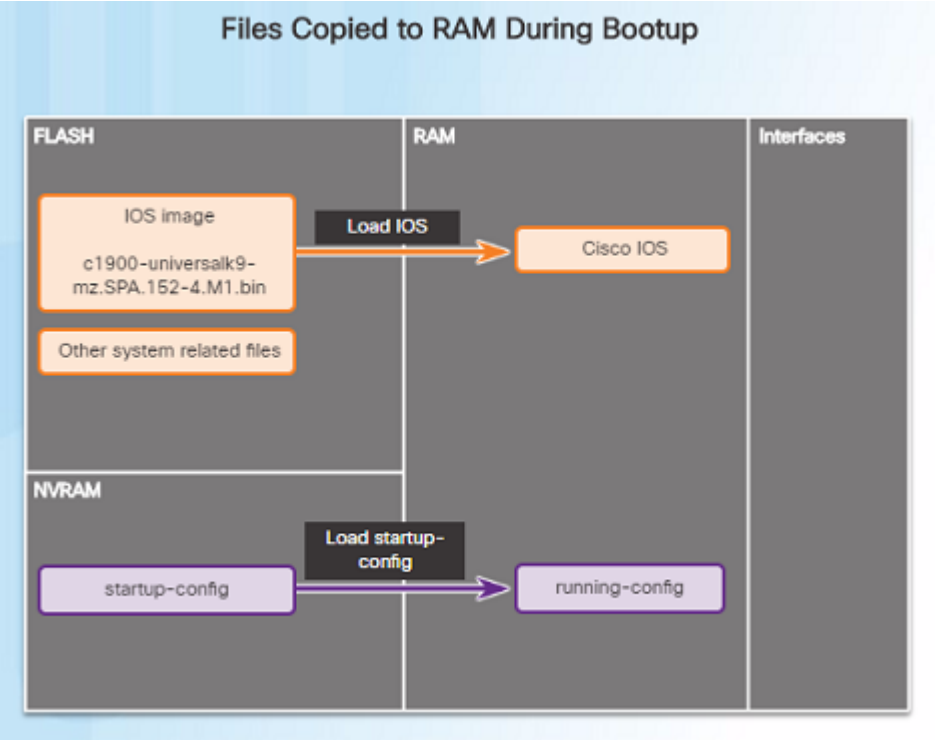
Part 2: Select Correct Modules for Connectivity

Part 3: Connect Devices

Background

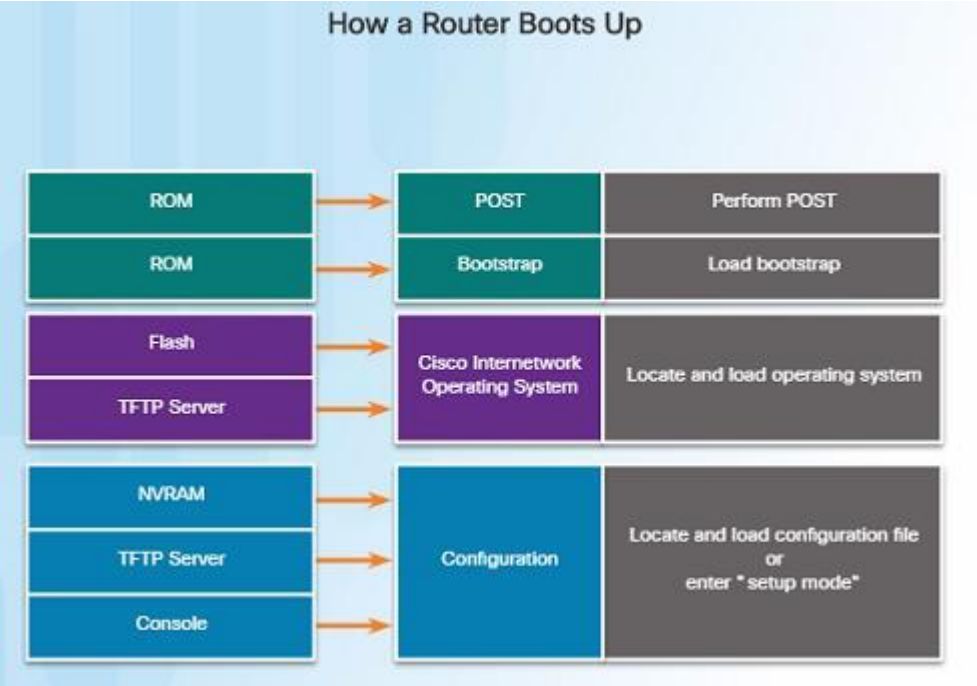
In this activity, you will explore the different options available on internetworking devices. You will also be required to determine which options provide the necessary connectivity when connecting multiple devices. Finally, you will add the correct modules and connect the devices.

Bootset Files



- Cisco routers and switches load the IOS image and startup configuration file into RAM when they are booted.
- The running configuration is modified when the network administrator makes any changes. These changes should be saved to the startup configuration file in NVRAM in order for them to take effect on the next reboot of the router or during in the event of a power loss.

Router Bootup Process



- Three major phases to the bootup process of a router:
  - Perform the POST and load the bootstrap program – During the Power-on Self-Test, the router executes diagnostics from ROM on various hardware components. After the POST, the bootstrap program is copied from ROM into RAM and its job is to locate the Cisco IOS and load it into RAM.
  - Locate and load the Cisco IOS software – Typically, the IOS is stored in flash memory and is copied into RAM for execution by the CPU.
  - Locate and load the startup configuration file or enter setup mode – The bootstrap program then copies the startup config file from NVRAM into RAM and becomes the running configuration.

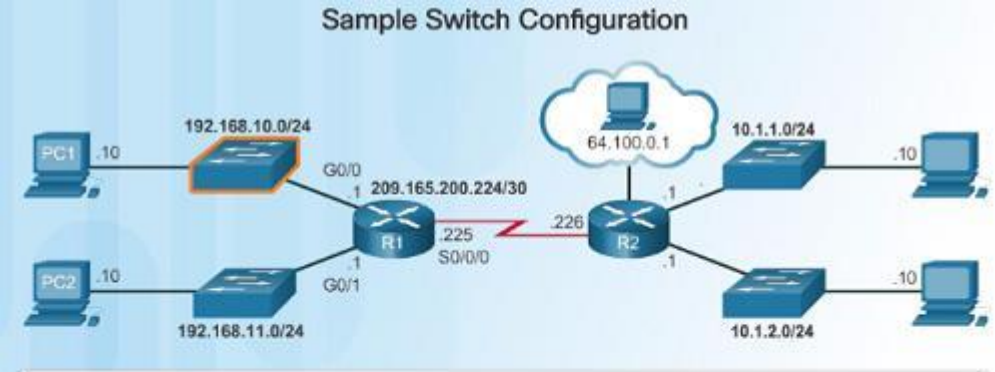
Show Version Output

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15,
RELEASE SOFTWARE (fc1)

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is
"flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on


<output omitted>


Cisco CISCO1941/K9 (revision 1.0)
with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
```

- The **show version** command displays information about the version of the Cisco IOS software running on the router as well as:
  - The version of the bootstrap program
  - Information about the hardware configuration
  - Amount of system memory

Configure a Cisco Router

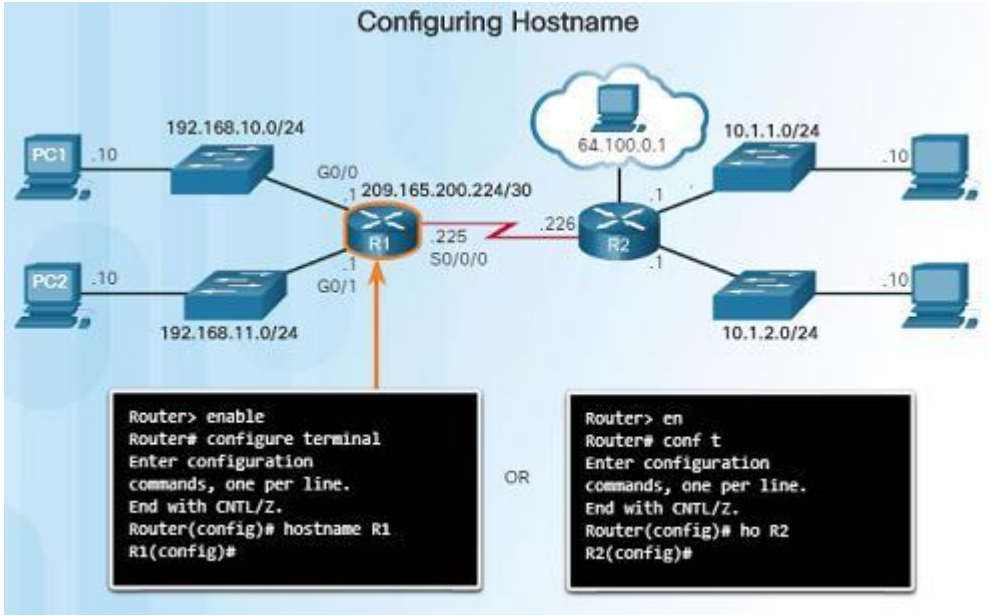
Basic Switch Configuration Steps




```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.10.50 255.255.255.0
S1(config-if)# no shutdown
```

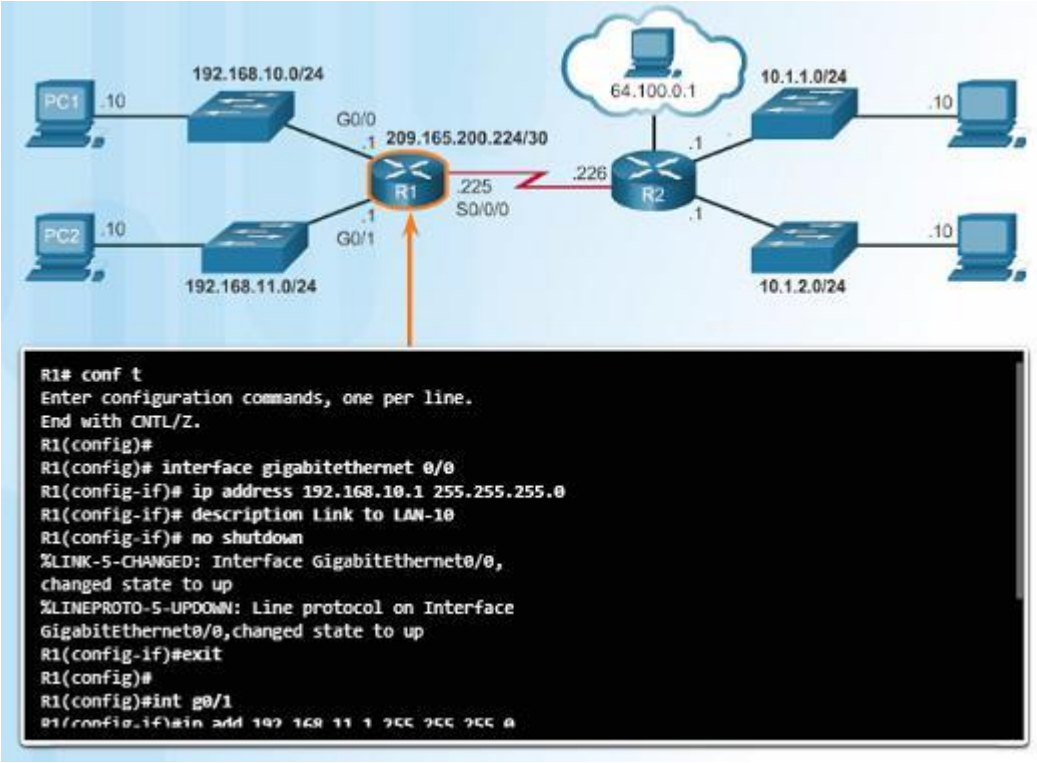
- Cisco routers and switches have many similarities in regards to their configuration:
  - Support a similar operating system.
  - Support similar command structure.
  - Support many of the same commands.
  - They also have identical initial configuration steps when implemented in a network.
- The commands on the left display a sample configuration of a switch.

Basic Router Configuration Steps



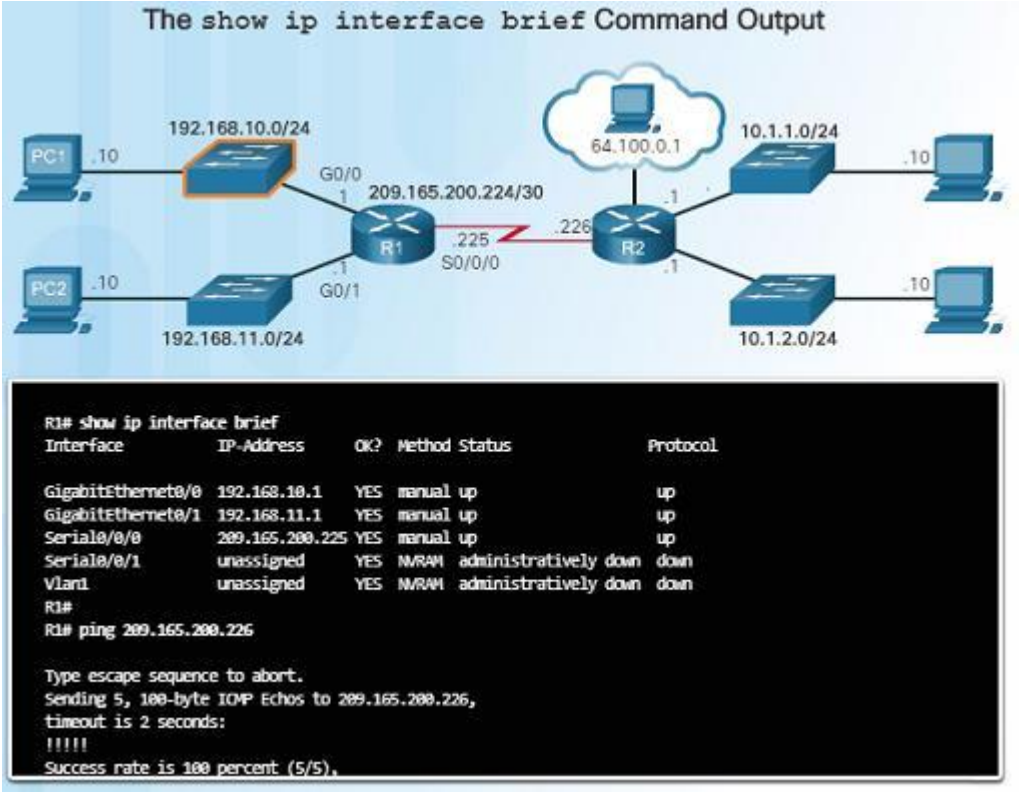
- Similar to the configuration of a switch on the previous slide, the initial configuration should include:
  - Configure the router's device name
  - Secure the user EXEC mode
  - Secure remote Telnet and SSH access
  - Secure privileged EXEC mode
  - Secure all passwords in the config file
  - Provide legal notification – Authorized access only
  - Save the configuration

Configure Router Interfaces



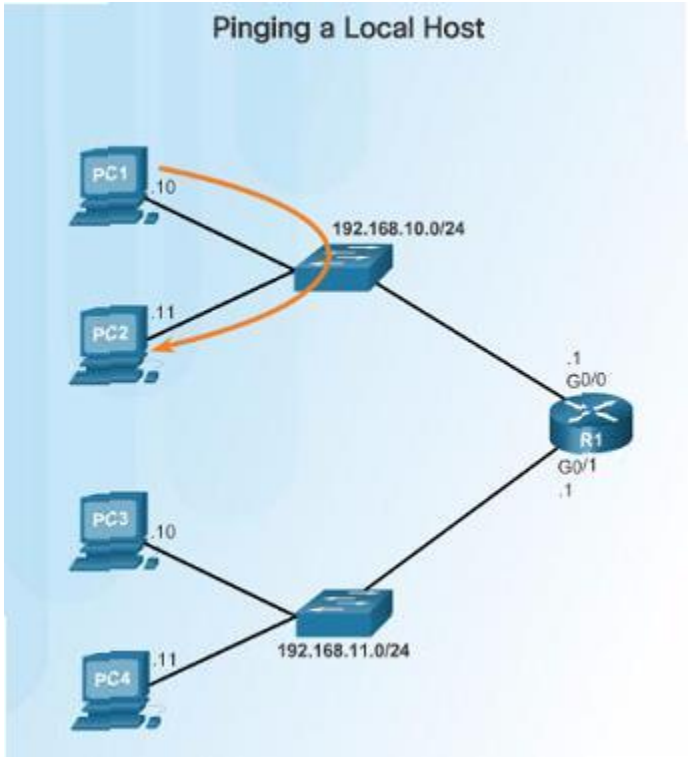
- For routers to be reachable by other devices in the network, the in-band interfaces must be configured. For example, a Cisco 1941 router has four in-band interfaces:
  - Two Gigabit Ethernet Interfaces – G0/0 and G0/1
  - One serial WAN Interface card with two interfaces – S 0/0/0 and S0/0/1
- The commands in the figure to the left provide an example of how to configure a router's interface to provide network connectivity.
- It is important that you use the command **no shutdown** when you are ready to make the interface active.

Verify Interface Configuration



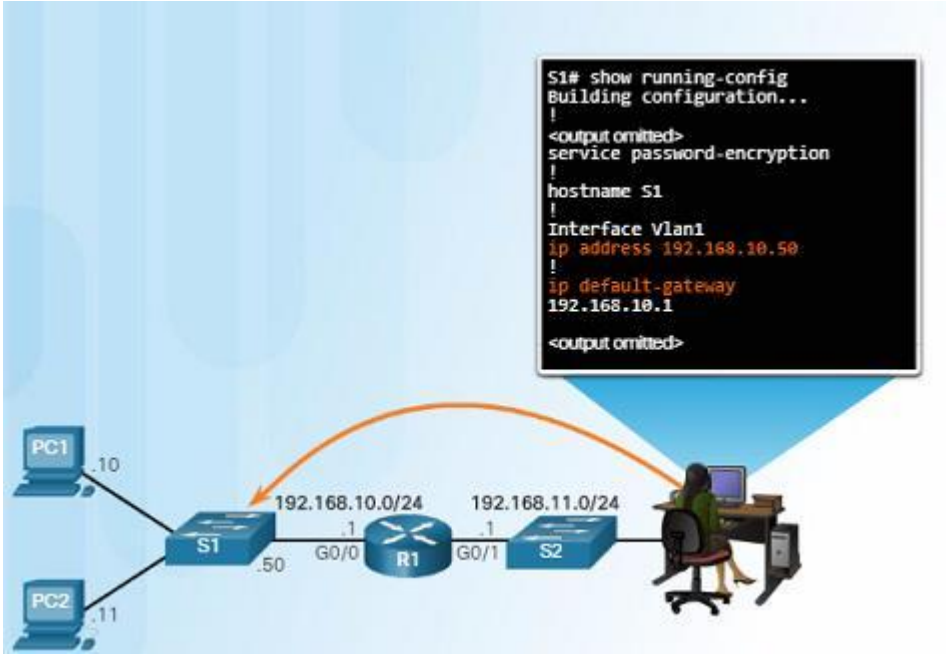
- After configuring an interface, or for troubleshooting purposes, there are several commands that can be used:
  - **show ip interface brief** – Provides you a summarized view of all interfaces to verify if they are activated and operational. Look for Status of “up” and Protocol of “up”.
  - **show ip route** – Displays the contents of the IPv4 routing table stored in RAM.
  - **show interfaces** – Displays the IPv4 statistics for all interfaces on a router.
- Remember to save your configuration changes with the **copy running-config startup-config** command.

Default Gateway for a Host



- For an end device or a host to communicate over the network, it must be configured with the correct IP address information including the default gateway address.
- The default gateway is only used when the host wants to send a packet to a device on another network – if the device is on the same network, it can send it directly to that device.
- If PC1 needs to send a packet to PC3 which is on a different network, it must send it to the default gateway address of 192.168.10.1 on router R1's G0/0 interface.

Default Gateway for a Switch

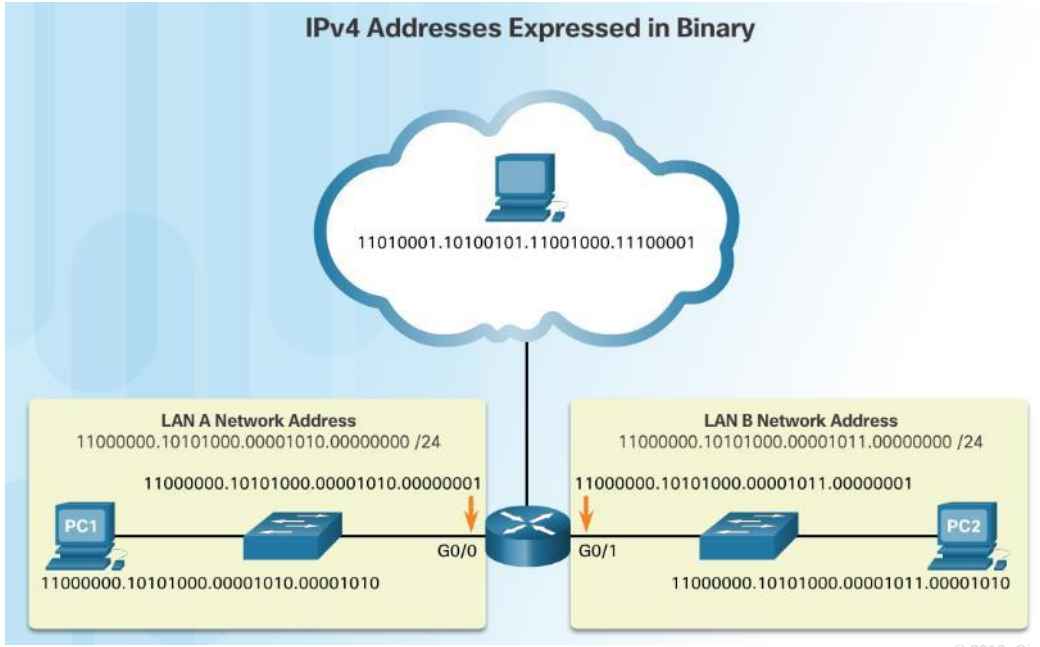


- Normally, a Layer 2 device, such as a switch, does not require an IP address to function.
- An IP address, subnet mask, and default gateway address are required in order to connect to it remotely (via SSH or Telnet) for configuration or administrative purposes.
- Use the command **ip default-gateway** global configuration command to configure the default gateway on a switch.
- It is important to note that a switch does not use the default gateway address to forward packets to from hosts on its local network to remote networks.

IPv4 Network Addresses

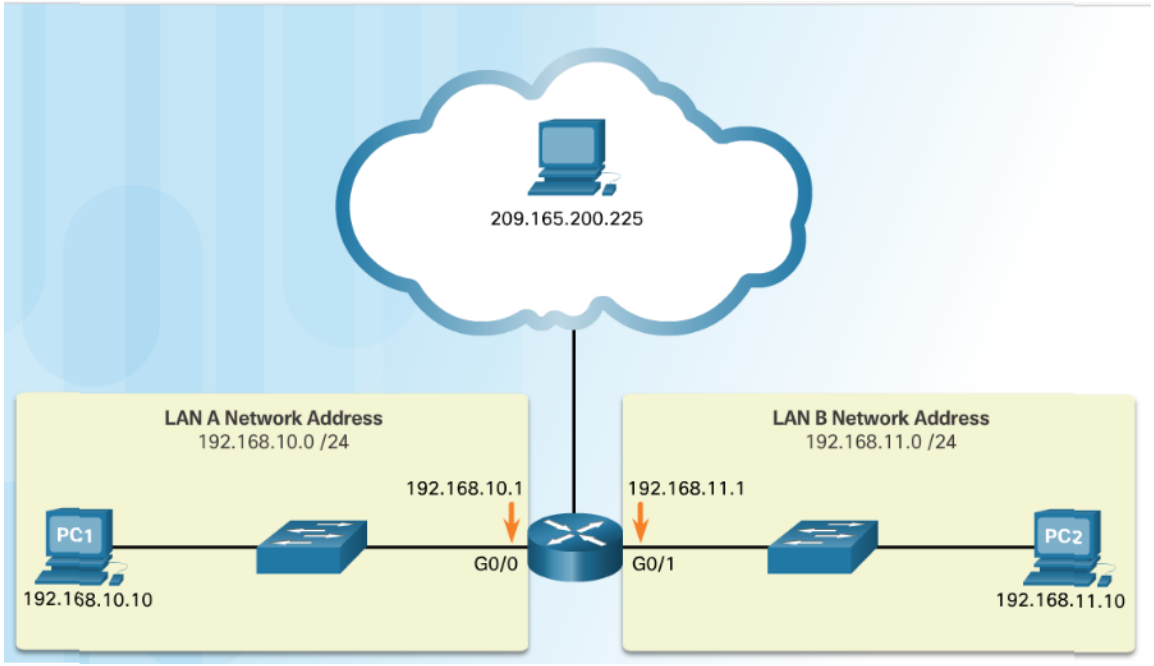
IPv4 Addresses

- Binary numbering system consists of the numbers 0 and 1 called bits
  - IPv4 addresses are expressed in 32 binary bits divided into 4 8-bit octets



IPv4 Addresses (Cont.)

- IPv4 addresses are commonly expressed in dotted decimal notation



Positional Notation

- The first row identifies the number base or radix. Decimal is 10. Binary is based on 2, therefore radix will be 2
- The 2nd row considers the position of the number starting with 0. These numbers also represent the exponential value that will be used to calculate the positional value (4th row).
- The 3rd row calculates the positional value by taking the radix and raising it by the exponential value of its position. Note: n^0 is always = 1.
- The positional value is listed in the fourth row.

Decimal Positional Notation

Radix	10	10	10	10
Position in Number	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Positional Value	1000	100	10	1

Applying decimal positional notation

	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number (1234)	1	2	3	4
Calculate	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up ...	1000	+ 200	+ 30	+ 4
Result	1,234			

Positional Notation (Cont.)

Binary Positional Notation

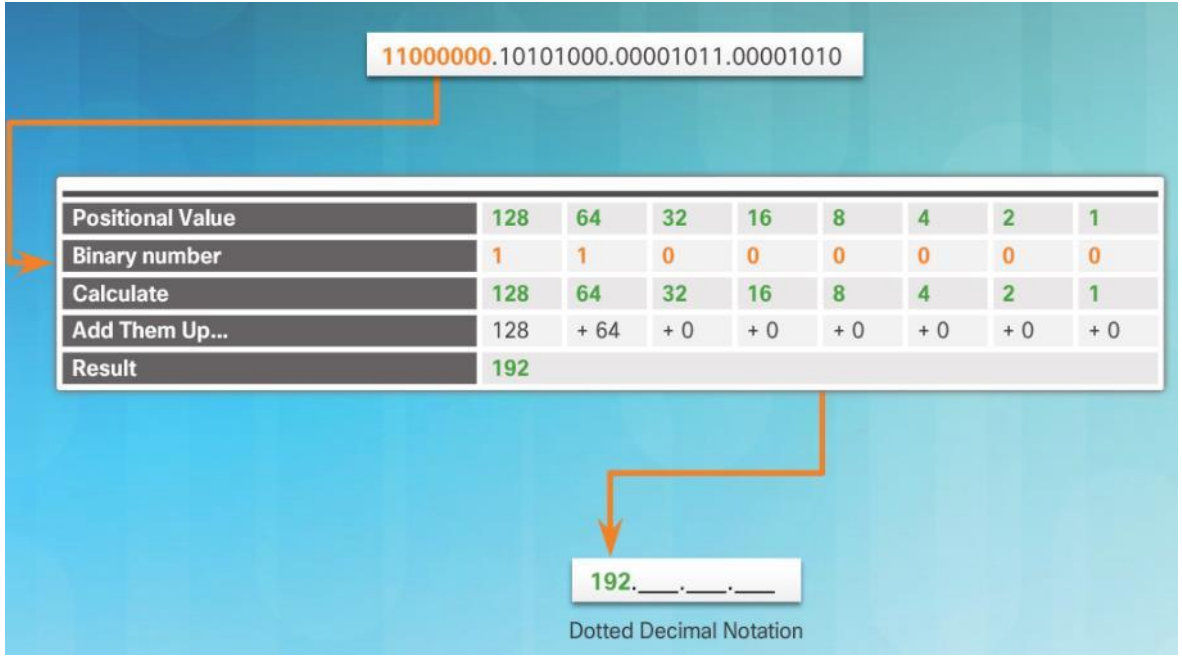
Radix	2	2	2	2	2	2	2	2
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Positional Value	128	64	32	16	8	4	2	1

- Applying binary positional notation.

Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add Them Up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

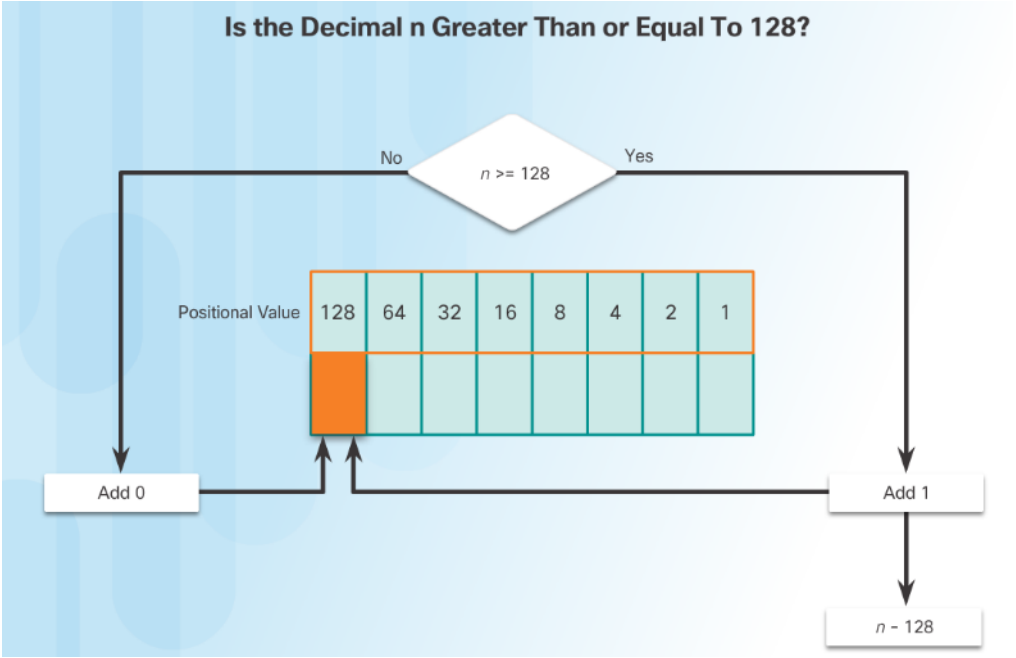
Binary to Decimal Conversion

- To convert a binary IPv4 address to decimal enter the 8-bit binary number of each octet under the positional value of row 1 and then calculate to produce the decimal.



Decimal to Binary Conversion

- To convert a decimal IPv4address to binary use the positional chart and check first if the number is greater than the 128 bit. If no a 0 is placed in this position. If yes then a 1 is placed in this position.
- 128 is subtracted from the original number and the remainder is then checked against the next position (64) If it is less than 64 a 0 is placed in this position. If it is greater, a 1 is placed in this position and 64 is subtracted.
- The process repeats until all positional values have been entered.



Decimal to Binary Conversion Examples

Example: 192.168.10.11

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000 . _____ . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0

11000000 . 10101000 . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	0

11000000 . 10101000 . 00001010 . _____

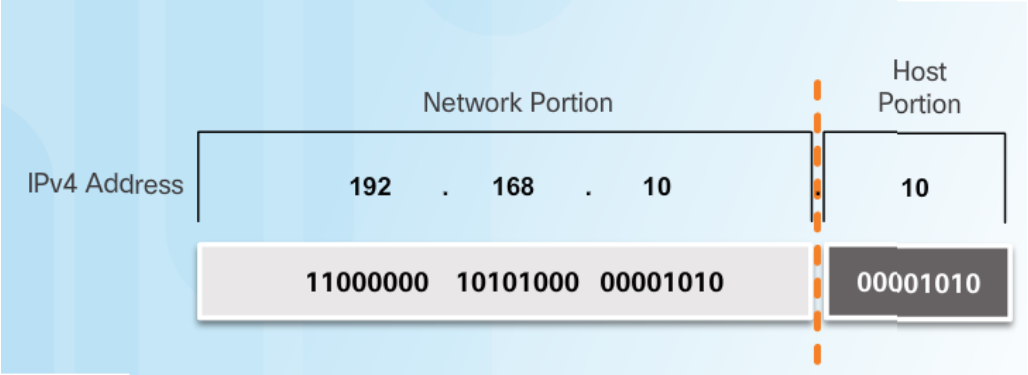
Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	1

11000000 . 10101000 . 00001010 . 00001011

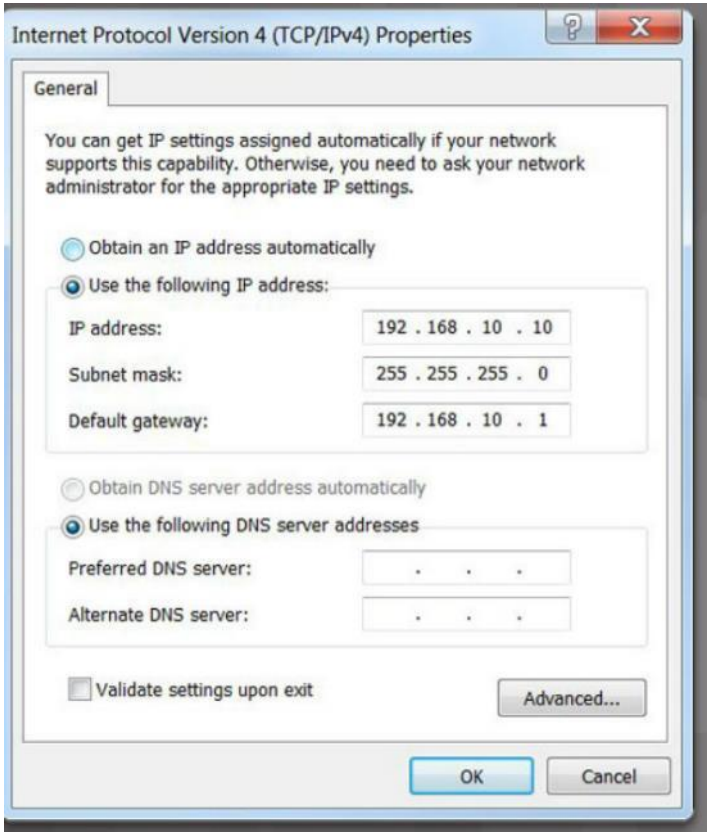
Network and Host Portions

- An IPv4 address is hierarchical.
  - Composed of a Network portion and Host portion.
- All devices on the same network must have the identical network portion.
- The Subnet Mask helps devices identify the network portion and host portion.



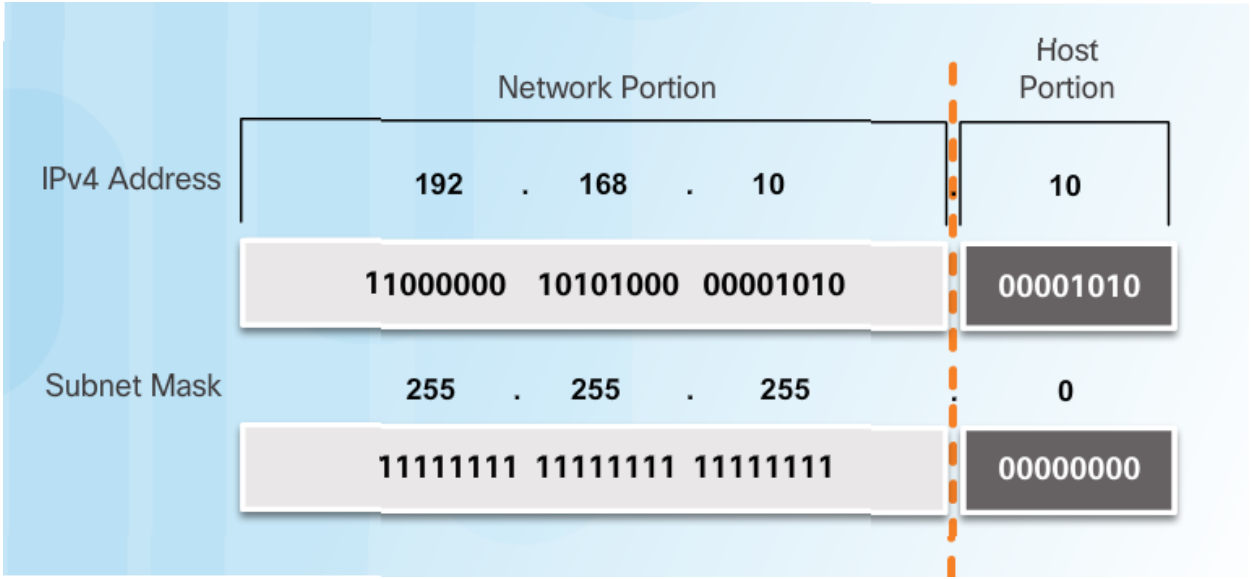
The Subnet Mask

- Three IPv4 addresses must be configured on a host:
  - Unique IPv4 address of the host.
  - Subnet mask - identifies the network/host portion of the IPv4 address.
  - Default gateway -IP address of the local router interface.



The Subnet Mask (Cont.)

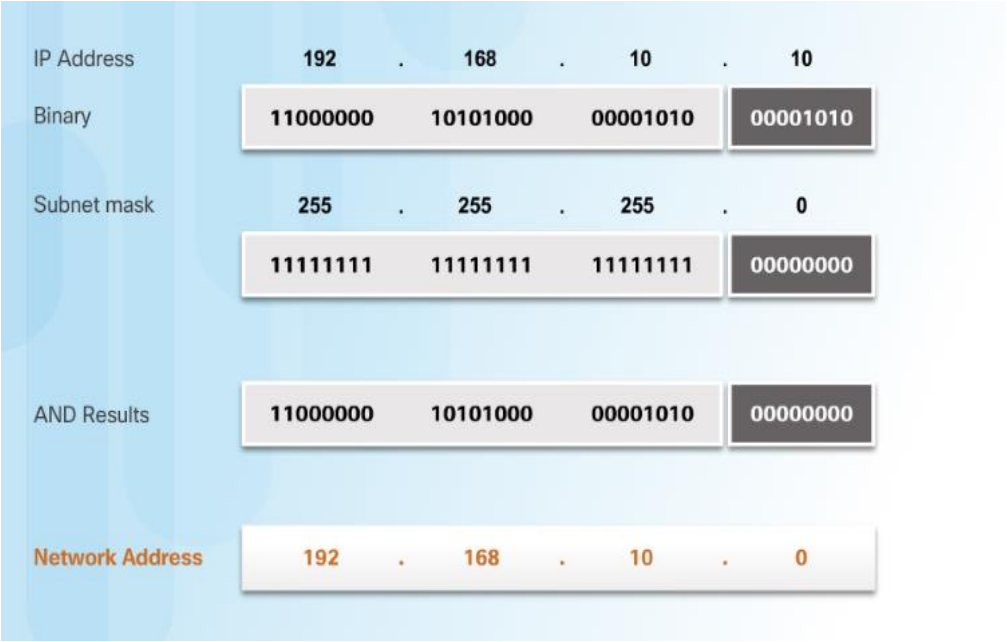
- The IPv4 address is compared to the subnet mask bit by bit, from left to right.
- A 1 in the subnet mask indicates that the corresponding bit in the IPv4 address is a network bit.



Logical AND

- A logical AND is one of three basic binary operations used in digital logic.
- Used to determine the Network Address
- The Logical AND of two bits yields the following results:

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0



The Prefix Length

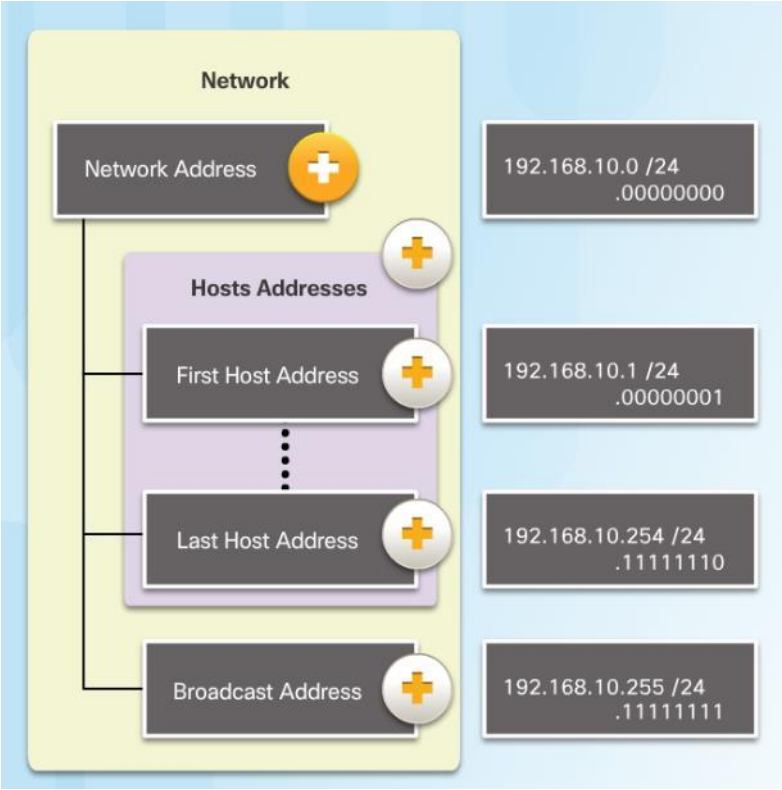
Comparing the Subnet Mask and Prefix Length

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

The Prefix Length:

- Shorthand method of expressing the subnet mask.
- Equals the number of bits in the subnet mask set to 1.
- Written in slash notation, / followed by the number of network bits.

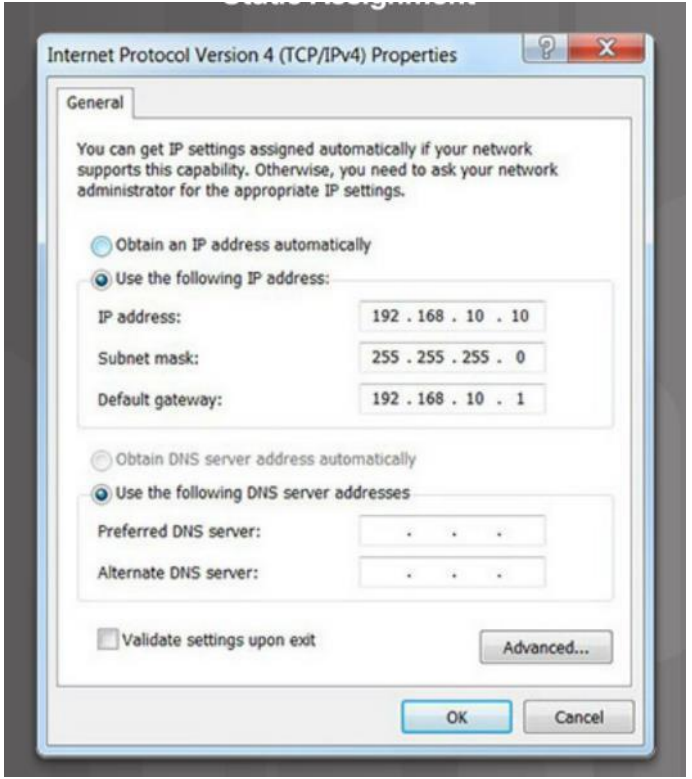
Network, Host, and Broadcast Addresses



- Types of Addresses in Network 192.168.10.0/24
  - Network Address - host portion is all 0s (.00000000)
  - First Host address - host portion is all 0s and ends with a 1 (.00000001)
  - Last Host address - host portion is all 1s and ends with a 0 (.11111110)
  - Broadcast Address - host portion is all 1s (.11111111)

Static IPv4 Address Assignment to a Host

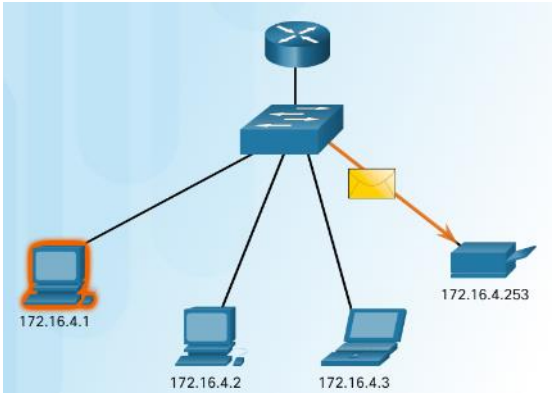
- Some devices like printers, servers and network devices require a fixed IP address.
- Hosts in a small network can also be configured with static addresses.



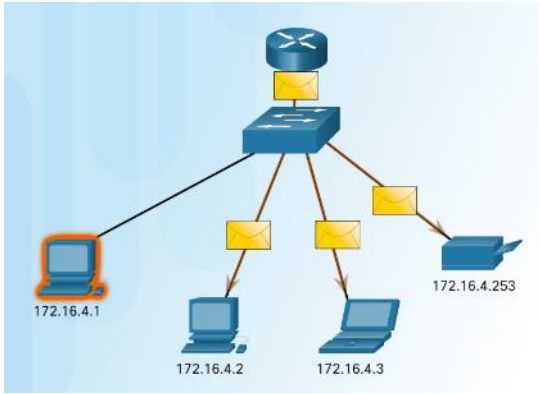
Dynamic IPv4 Address Assignment to a Host

- Most networks use Dynamic Host Configuration Protocol (DHCP) to assign IPv4 addresses dynamically.
- The DHCP server provides an IPv4 address, subnet mask, default gateway, and other configuration information.
- DHCP leases the addresses to hosts for a certain length of time.
- If the host is powered down or taken off the network, the address is returned to the pool for reuse.

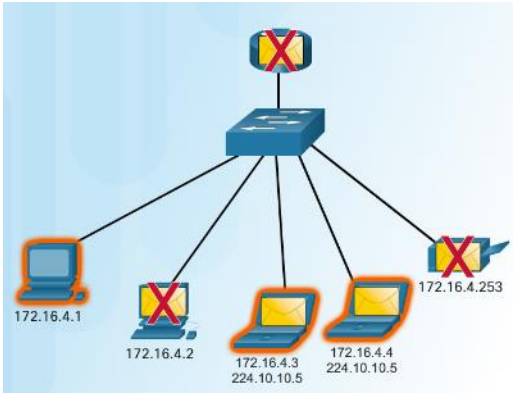
IPv4 Communication



- Unicast – one to one communication.



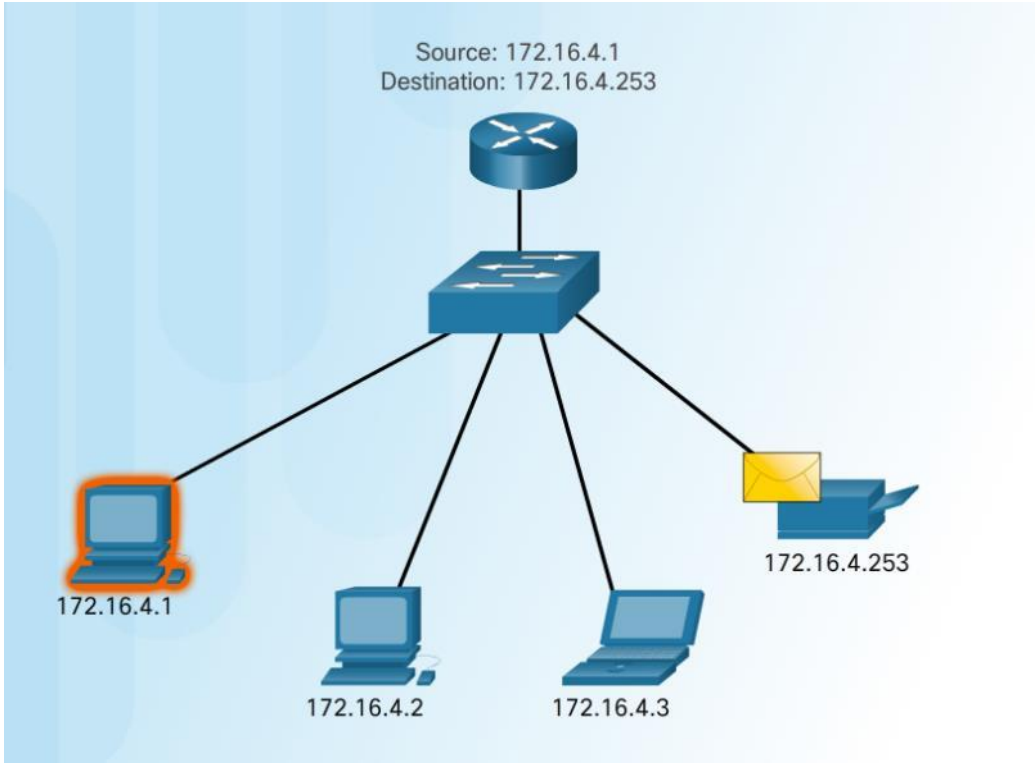
- Broadcast– one to all.



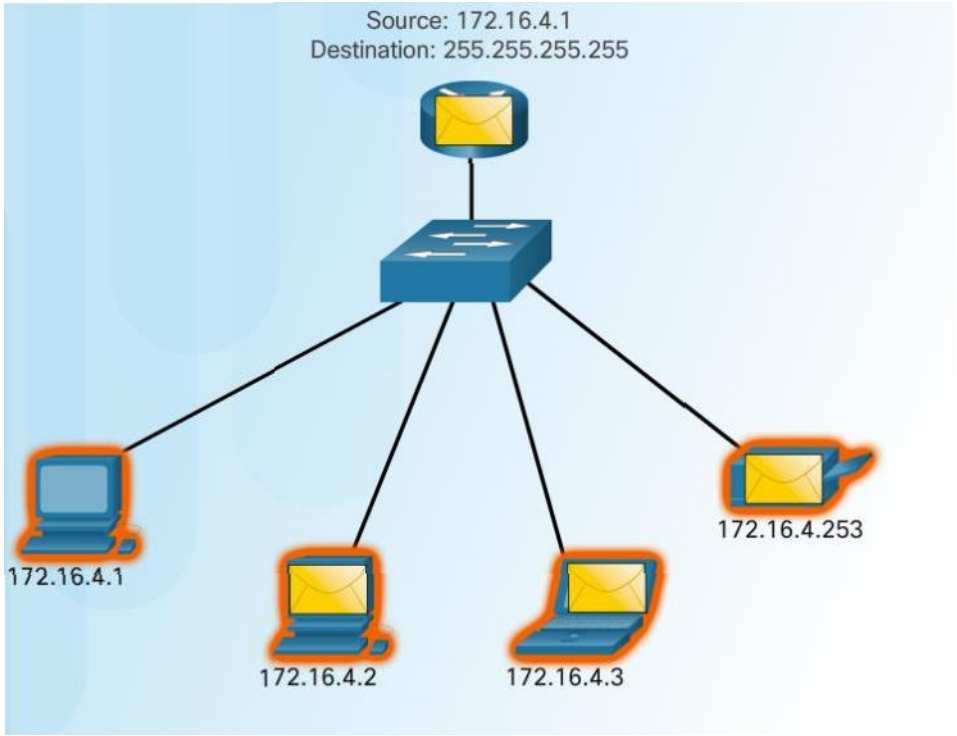
- Multicast – one to a select group.

Unicast Transmission

- Unicast – one to one communication.
  - Use the address of the destination device as the destination address.

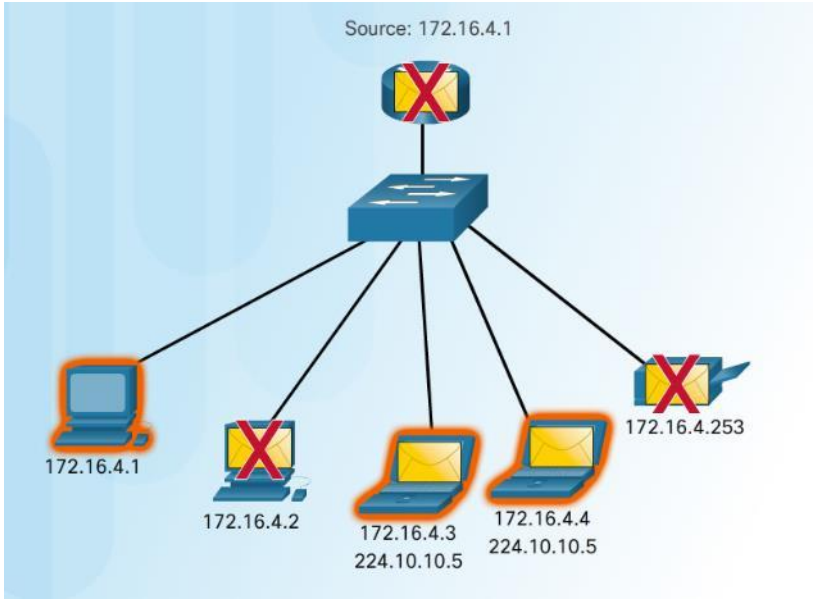


Broadcast Transmission



- Broadcast– one to all
  - Message sent to everyone in the LAN (broadcast domain.)
  - destination IPv4 address has all ones (1s) in the host portion.

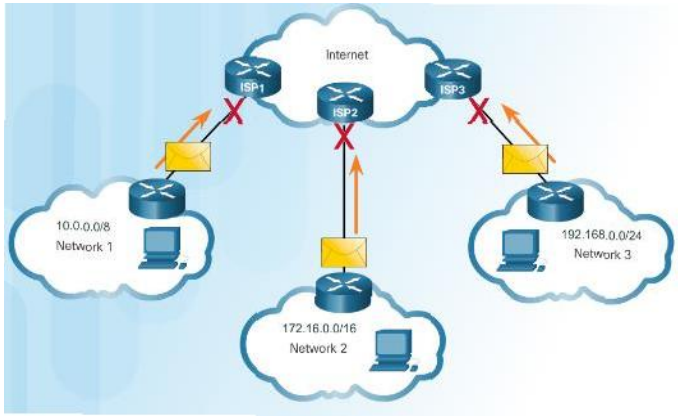
Multicast Transmission



- Multicast– one to a select group.
  - 224.0.0.0 to 239.255.255.255 addresses reserved for multicast.
  - routing protocols use multicast transmission to exchange routing information.

Public and Private IPv4 Addresses

- Private Addresses
  - Not routable
  - Introduced in mid 1990s due to depletion of IPv4 addresses
  - Used only in internal networks.
  - Must be translated to a public IPv4 to be routable.
  - Defined by RFC 1918
- Private Address Blocks
  - 10.0.0.0 /8 or 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255



Special User IPv4 Addresses

Pinging the Loopback Interface

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Loopback addresses (127.0.0.0 /8 or 127.0.0.1)
  - Used on a host to test if the TCP/IP configuration is operational.
- Link-Local addresses (169.254.0.0 /16 or 169.254.0.1)
  - Commonly known as Automatic Private IP Addressing (APIPA) addresses.
  - Used by Windows client to self configure if no DHCP server available.
- TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255)
  - Used for teaching and learning.

Legacy Classful Addressing

Class A Specifics	
Address Block	0.0.0.0 - 127.0.0.0
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Class B Specifics	
Address Block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Class C Specifics	
Address Block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

- In 1981, Internet IPv4 addresses were assigned using classful addressing (RFC 790)
- Network addresses were based on 3 classes:
  - **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
  - **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support the needs of moderate to large size networks up to approximately 65,000 host addresses.
  - **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.

Legacy Classful Addressing

- Network addresses were based on 3 classes:
  - **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.

Class A Specifics	
Address Block	0.0.0.0 – 127.0.0.0
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Legacy Classful Addressing

- Network addresses were based on 3 classes:
  - **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support the needs of moderate to large size networks up to approximately 65,000 host addresses.

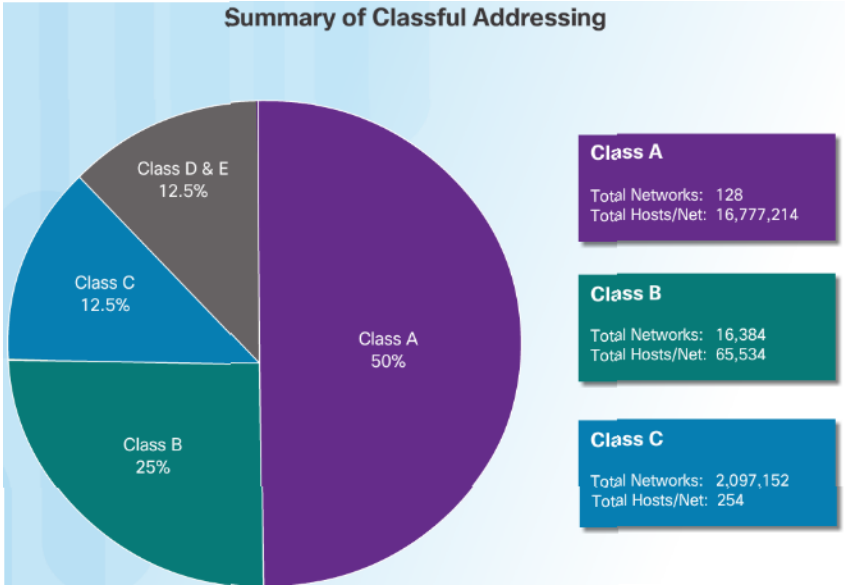
Class B Specifics	
Address Block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Legacy Classful Addressing

- Network addresses were based on 3 classes:
  - **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.

Class C Specifics	
Address Block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

Classless Addressing



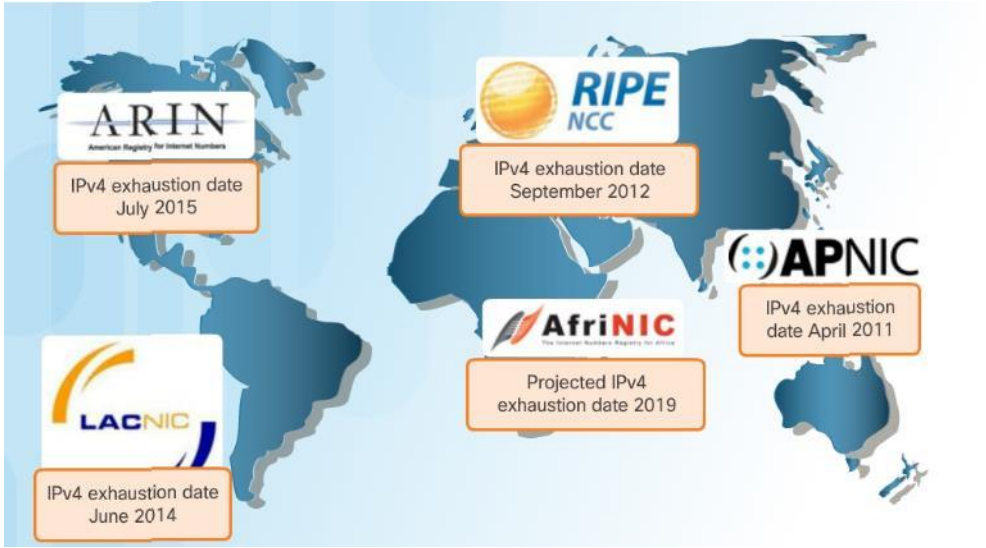
- Classful Addressing wasted addresses and exhausted the availability of IPv4 addresses.
- Classless Addressing Introduced in the 1990s
  - Classless Inter-Domain Routing (CIDR, pronounced “cider”)
  - Allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C.

Assignment of IP Addresses

- The following organizations manage and maintain IPv4 and IPv6 addresses for the various regions.
  - American Registry for Internet Numbers (ARIN)- North America.
  - Réseaux IP Europeans (RIPE) - Europe, the Middle East, and Central Asia
  - Asia Pacific Network Information Centre (APNIC) - Asia and Pacific regions
  - African Network Information Centre (AfriNIC) – Africa
  - Regional Latin-American and Caribbean IP Address Registry (LACNIC) - Latin America and some Caribbean islands

IPv6 Network Addresses

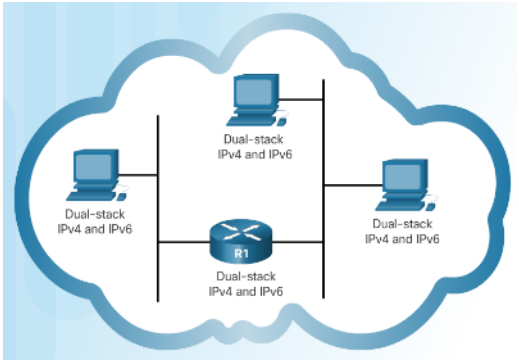
The Need for IPv6



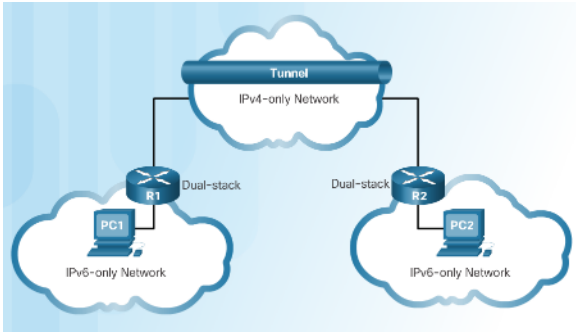
- IPv6 versus IPv4:
  - Has a larger 128-bit address space
  - 340 undecillion addresses
  - Solves limitations with IPv4
  - Adds enhancement like address auto-configuration.
- Why IPv6 is needed:
  - Rapidly increasing Internet population
  - Depletion of IPv4
  - Issues with NAT
  - Internet of Things

IPv4 and IPv6 Coexistence

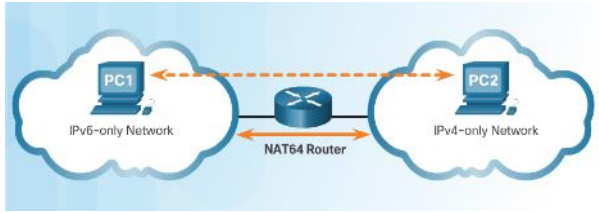
- Migration from IPv4 to IPv6 Techniques



Dual stack - Devices run both IPv4 and IPv6 protocol stacks simultaneously.



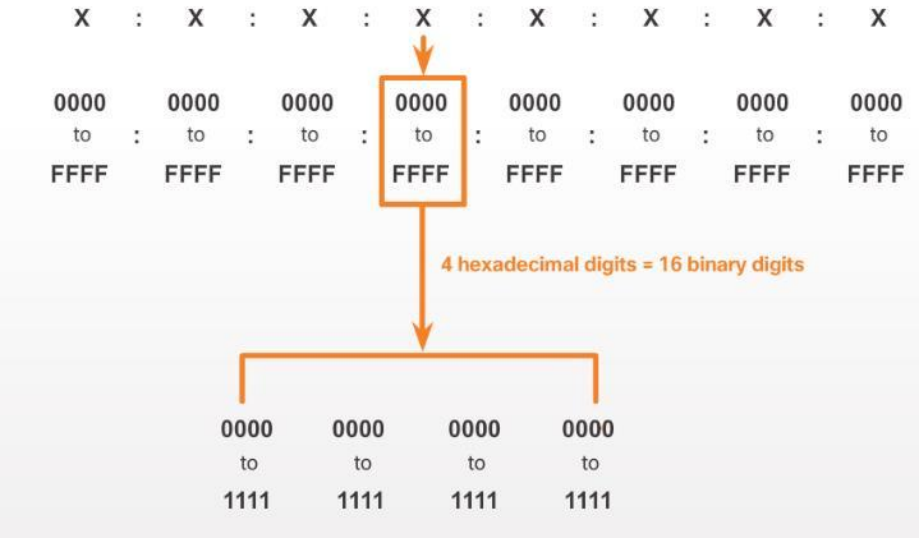
Tunneling - The IPv6 packet is encapsulated inside an IPv4 packet.



Translation - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4 devices.

IPv6 Address Representation

- IPv6 Addresses:
  - 128 bits in length
  - Every 4 bits is represented by a single hexadecimal digit
  - Hextet - unofficial term referring to a segment of 16 bits or four hexadecimal values.



IPv6 Address Representation (Cont.)

- Preferred format for IPv6 representation

2001	0DB8	0000	1111	0000	0000	0000	0200
2001	0DB8	0000	00A3	ABCD	0000	0000	1234
2001	0DB8	000A	0001	0000	0000	0000	0100
2001	0DB8	AAAA	0001	0000	0000	0000	0200
FE80	0000	0000	0000	0123	4567	89AB	CDEF
FE80	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0001	FF00	0200
0000	0000	0000	0000	0000	0000	0000	0001
0000	0000	0000	0000	0000	0000	0000	0000

Rule 1 – Omit Leading 0s

- In order to reduce or compress IPv6
  - First rule is to omit leading zeros in any hextet.

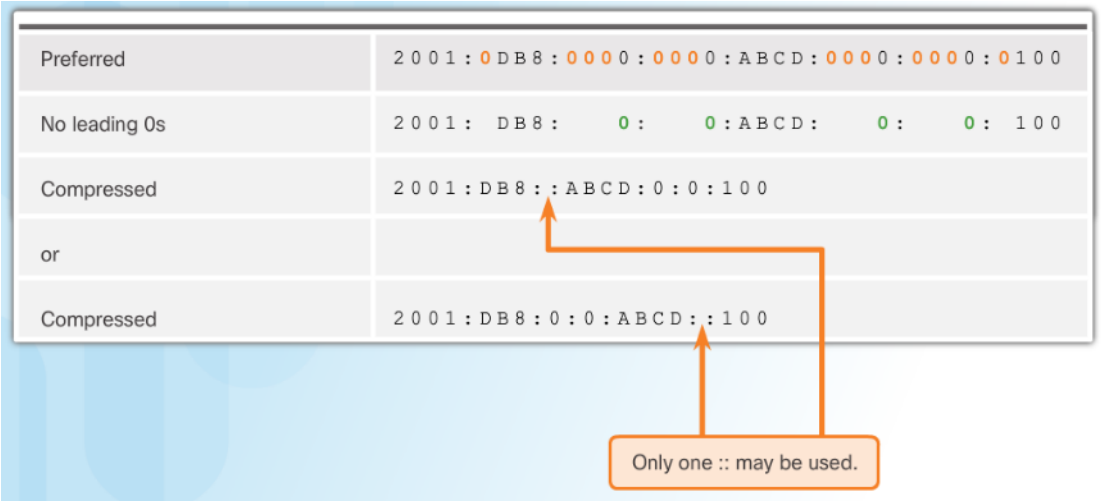
Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001:DB8:0:1111:0:0:0:200

Preferred	2001:0DB8:000A:1000:0000:0000:0000:0100
No leading 0s	2001:DB8:A:1000:0:0:0:100

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0:0:0:0:0:0:0:0

Rule 2 – Omit All 0 Segments

- Rule 2 – Omit All 0 Segments
  - A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.



Rule 2 – Omit All 0 Segments (Cont.)

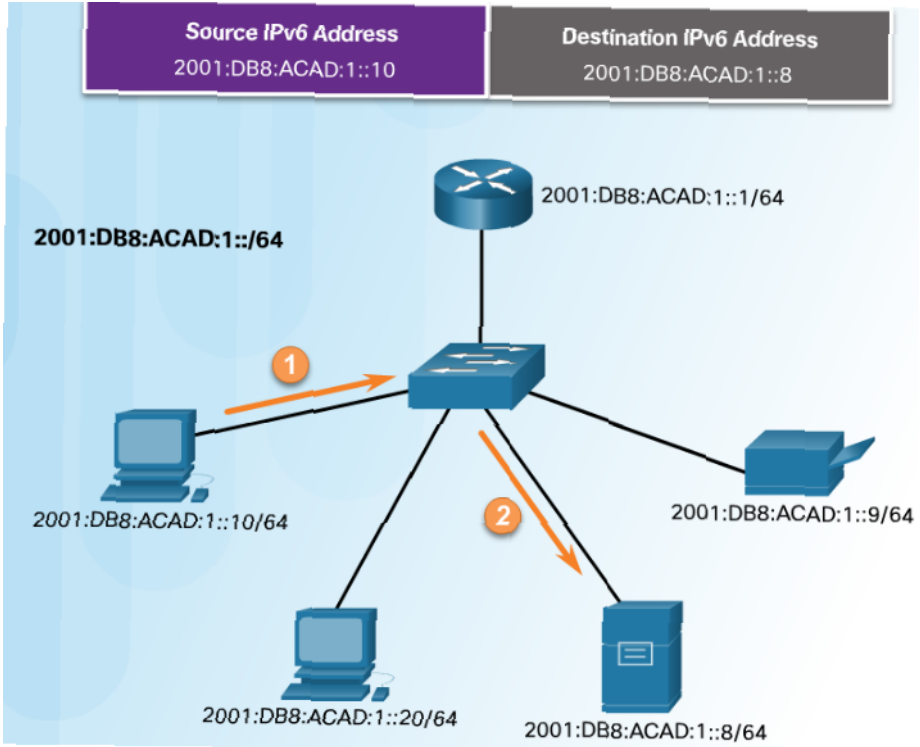
- Rule 2 – Omit All 0 Segments
  - A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

Preferred	FF02:0000:0000:0000:0000:0000:0000:0001
No leading 0s	FF02: 0: 0: 0: 0: 0: 0: 1
Compressed	FF02::1

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0: 0: 0: 0: 0: 0: 0: 0
Compressed	::

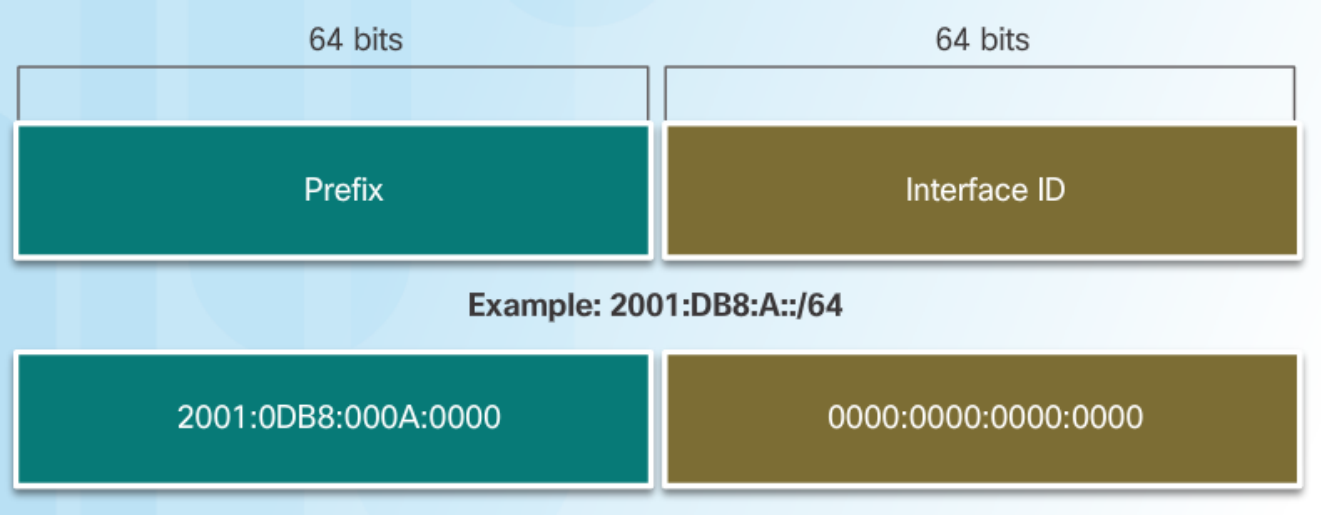
IPv6 Address Types

- Three types of IPv6 addresses:
  - **Unicast**- Single source IPv6 address.
  - **Multicast** - An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
  - **Anycast** - An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices.



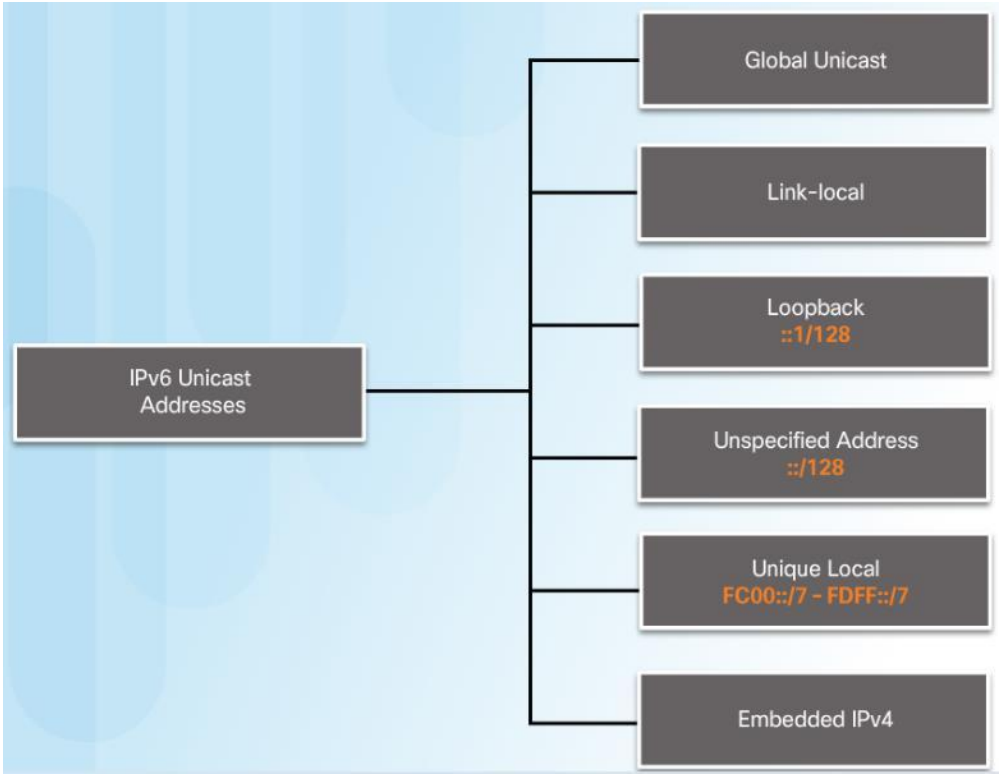
IPv6 Prefix Length

- The IPv6 prefix length is used to indicate the network portion of an IPv6 address:
  - The prefix length can range from 0 to 128.
  - Typical IPv6 prefix length for most LANs is /64



IPv6 Unicast Addresses

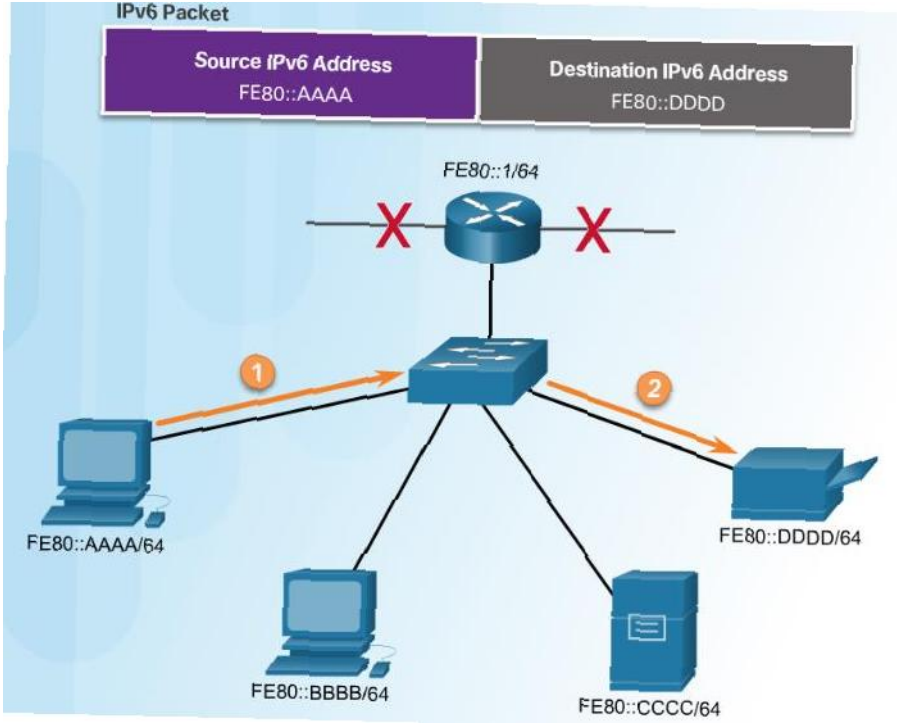
- **Global Unicast** - These are globally unique, Internet routable addresses.
- **Link-local** - used to communicate with other devices on the same local link. Confined to a single link.
- **Unique Local** - used for local addressing within a site or between a limited number of sites.



IPv6 Link-Local Unicast Addresses

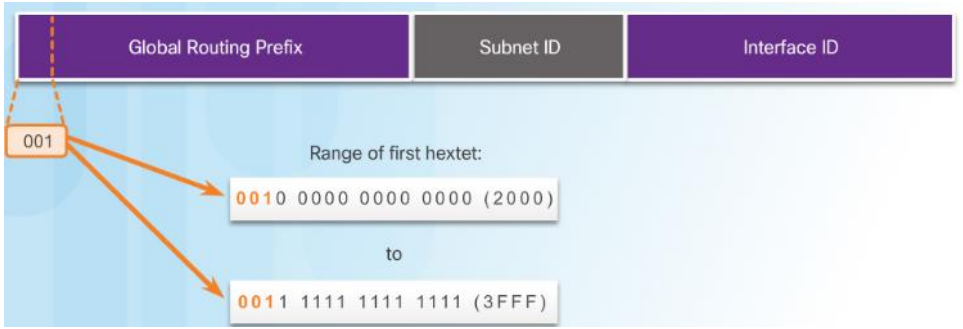
- IPv6 link-local addresses:
  - Enable a device to communicate with other IPv6-enabled devices on the same link only.
    - Are created even if the device has not been assigned a global unicast IPv6 address.
  - Are in the FE80::/10 range.

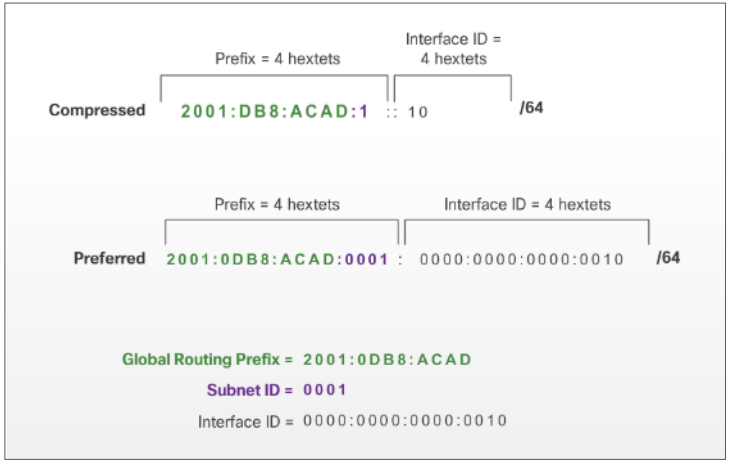
Note: Typically, it is the link-local address of the router that is used as the default gateway for other devices on the link.



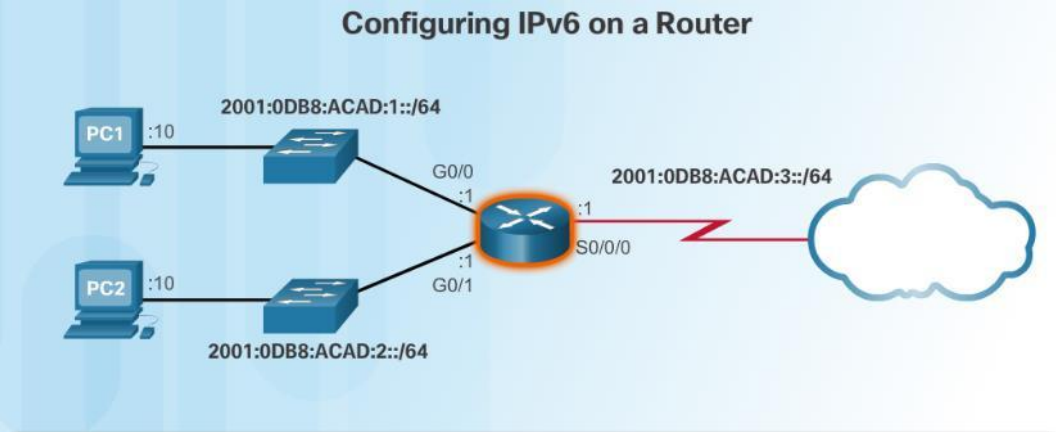
Structure of an IPv6 Global Unicast Address

- Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned
- A global unicast address has three parts:
  - **Global routing prefix** - network, portion of the address that is assigned by the provider. Typically /48.
  - **Subnet ID –** Used to subnet within an organization.
  - **Interface ID** - equivalent to the host portion of an IPv4 address.





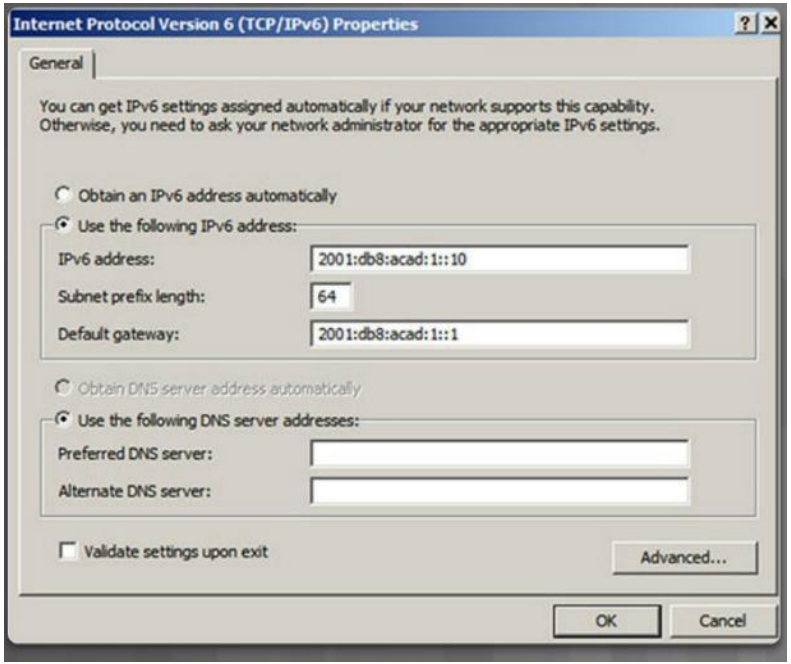
Static Configuration of a Global Unicast Address




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 56000
R1(config-if)# no shutdown
```

- Router Configuration:
  - Similar commands to IPv4, replace IPv4 with IPv6
  - Command to configure andIPv6 global unicast on an interface is **ipv6 address** *ipv6-address/prefix-length*

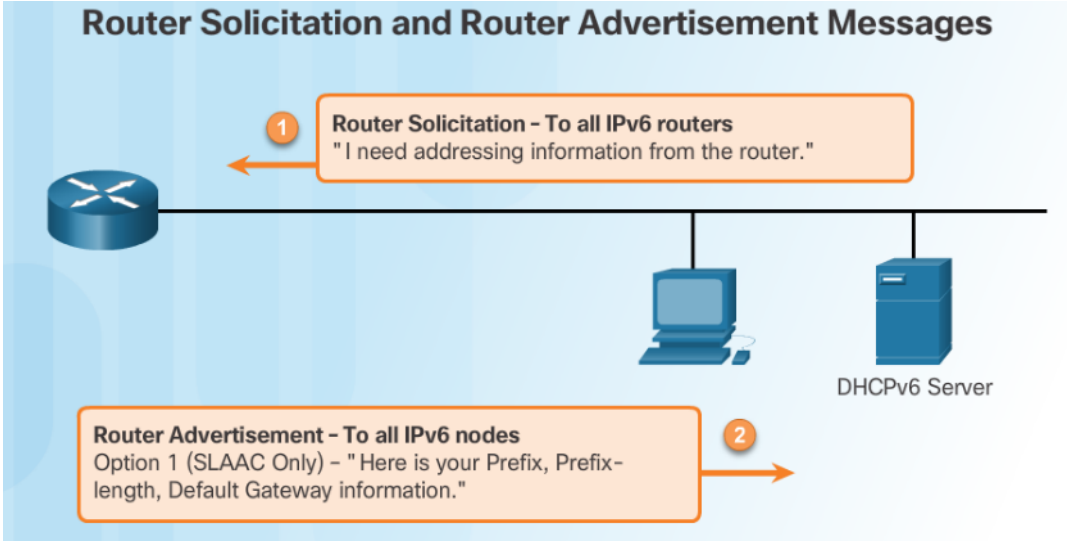
Static Configuration of a Global Unicast Address (Cont.)



- Host Configuration:
  - Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address
  - Default gateway address can be configured to match the link-local or global unicast address of the Gigabit Ethernet interface.
- Dynamic assignment of IPv6 addresses:
  - Stateless Address Autoconfiguration (SLAAC)
  - Stateful DHCPv6

Dynamic Configuration - SLAAC

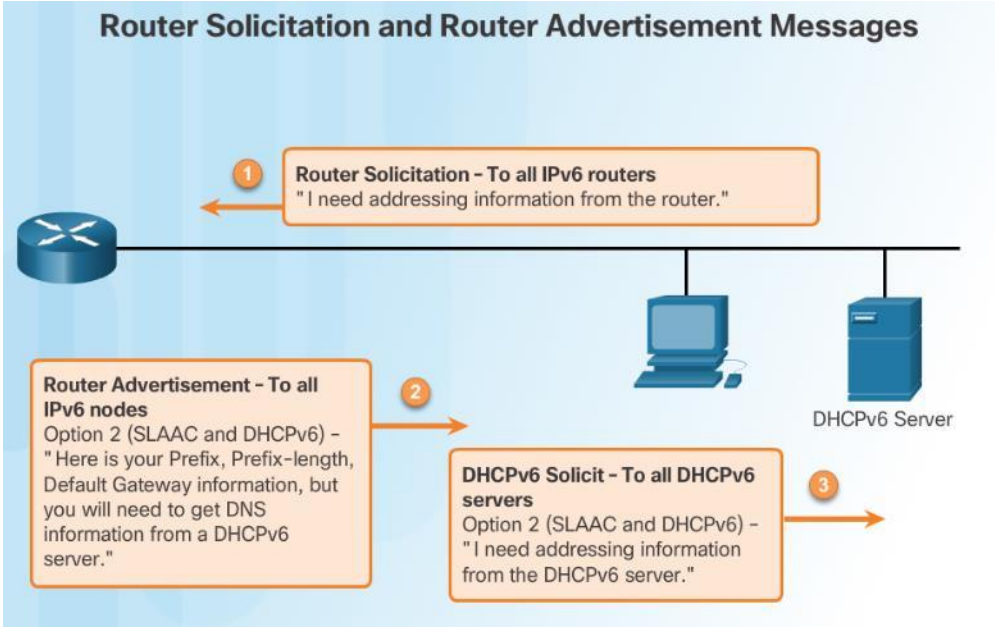
- Stateless Address Autoconfiguration (SLAAC):
  - A device can obtain its prefix, prefix length, default gateway address, and other information from an IPv6 router.
  - Uses the local router's ICMPv6 Router Advertisement (RA) messages
- ICMPv6 RA messages sent every 200 seconds to all IPv6-enabled devices on the network.



Option 1 (SLAAC Only) – "I'm everything you need (Prefix, Prefix-length, Default Gateway)"
Option 2 (SLAAC and DHCPv6) – "Here is my information but you need to get other information such as DNS addresses from a DHCPv6 server."
Option 3 (DHCPv6 Only) – "I can't help you. Ask a DHCPv6 server for all your information."

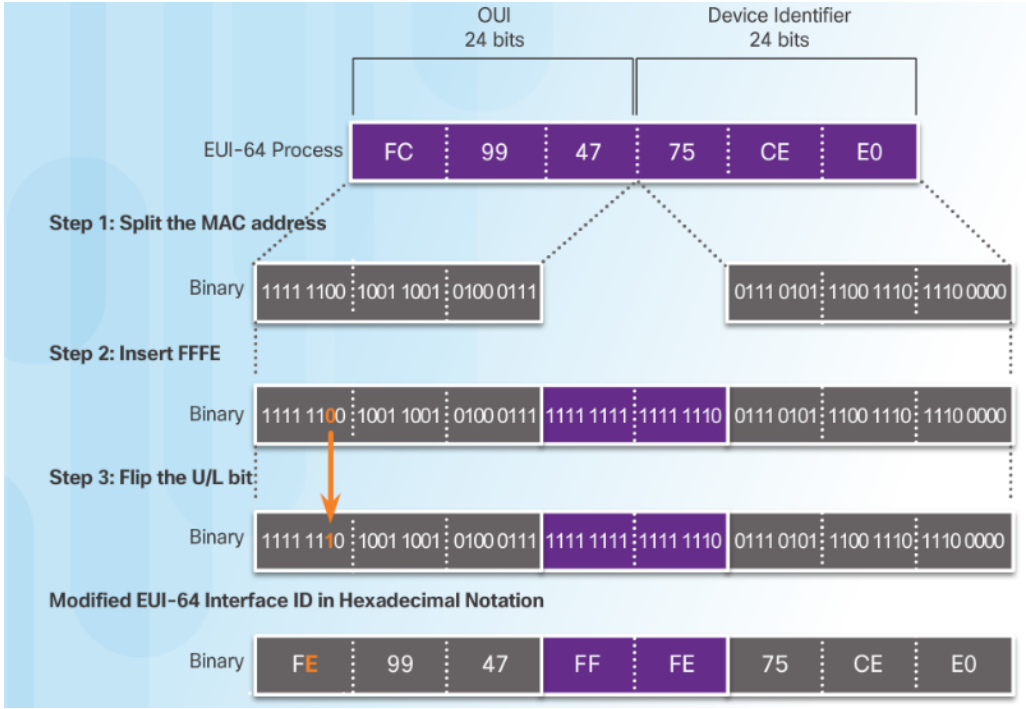
Dynamic Configuration – DHCPv6

- The RA Option 1: SLAAC only (this is the default)
- RA Option 2: SLAAC and Stateless DHCPv6:
  - Uses SLAAC for IPv6 global unicast address and default gateway.
  - Uses a stateless DHCPv6 server for other information.
- RA Option 3: Stateful DHCPv6
  - Uses the Routers link-local address for the default gateway.
  - Uses DHCPv6 for all other information.



EUI-64 Process and Randomly Generated

- When the RA message is SLAAC or SLAAC with stateless DHCPv6, the client must generate its own Interface ID
  - The Interface ID can be created using the EUI-64 process or a randomly generated 64-bit number
- An EUI-64 Interface ID is represented in binary and is made up of three parts:
  - 24-bit OUI from the client MAC address, but the 7th bit (the Universally/Locally (U/L) bit) is reversed.
  - The inserted 16-bit value FFFE (in hexadecimal).
  - 24-bit Device Identifier from the client MAC address.



EUI-64 Process and Randomly Generated (Cont.)

- Randomly Generated Interface IDs
  - Windows uses a randomly generated Interface ID

Dynamic Link-Local Addresses

- Link-local address can be established dynamically or configured manually.
- Cisco IOS routers use EUI-64 to generate the Interface ID for all link-local address on IPv6 interfaces.
- Drawback to using the dynamically assigned link-local address is the long interface ID, therefore they are often configured statically.

Static Link-Local Addresses

- Manual Configuration of the link-local address allows the creation of a simple, easy to remember address.

```
Router(config-if)#
ipv6 address link-local-address link-local
```

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Verifying IPv6 Address Configuration

- The commands to verify IPv6 configuration are similar to IPv4
  - show ipv6 interface brief
  - show ipv6 route
- The ping command for IPv6 is identical to the command used with IPv4, except that an IPv6 address is used.

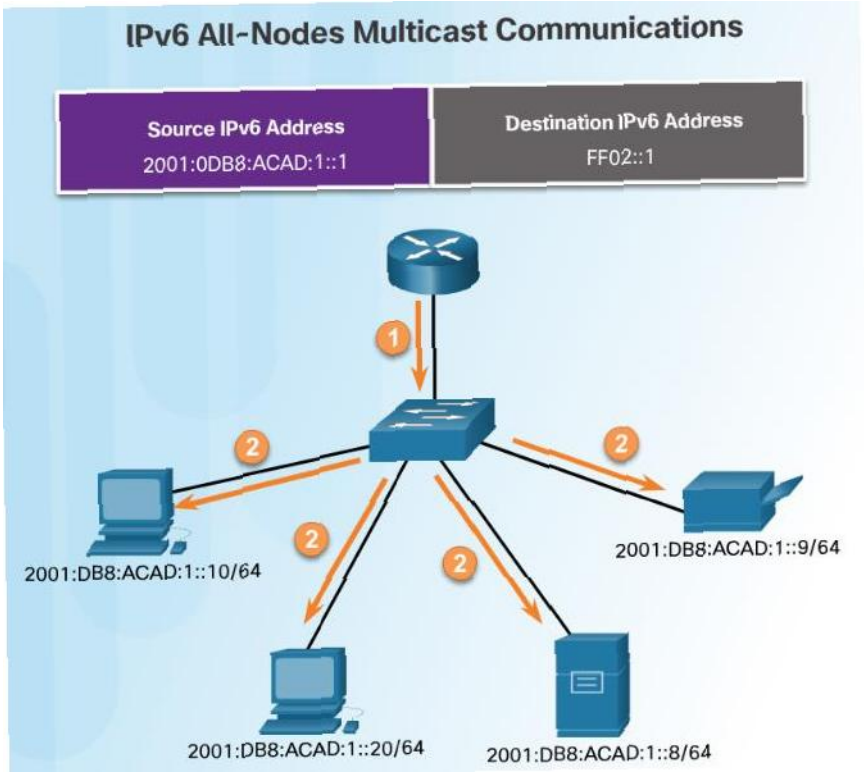
```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static



C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

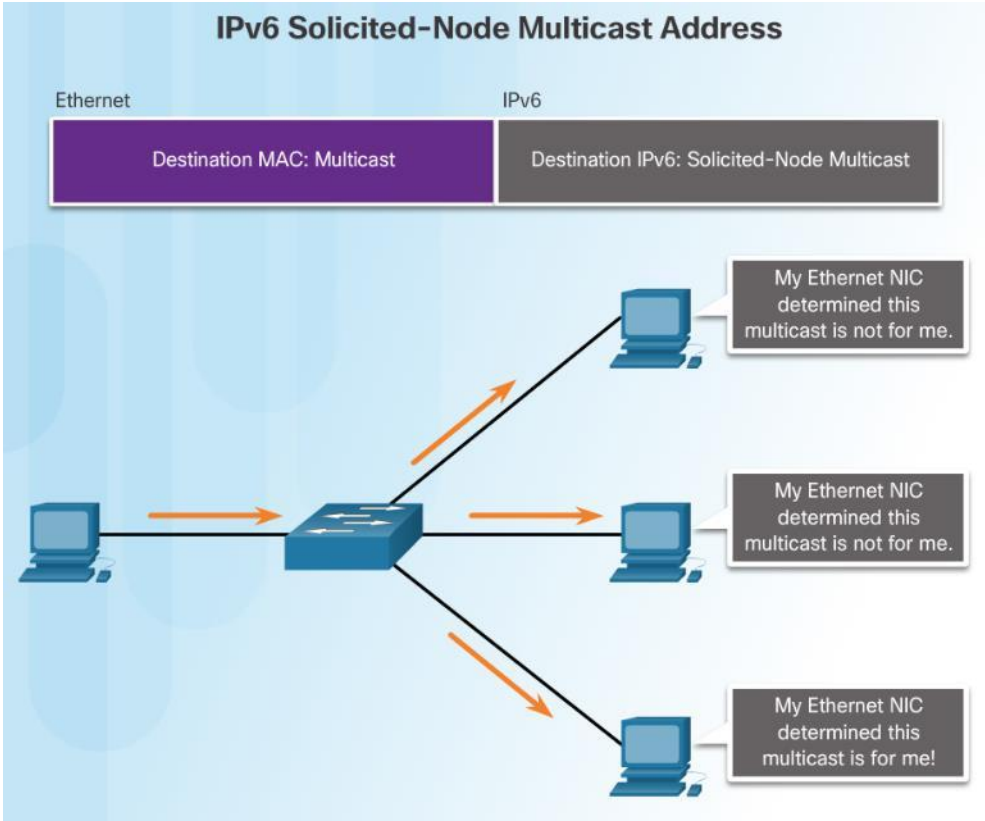
Assigned IPv6 Multicast Addresses

- There are two types of IPv6 multicast addresses:
  - Assigned multicast - reserved multicast addresses for predefined groups of devices
  - Solicited node multicast
- Two common IPv6 assigned multicast groups:
  - FF02::1 All-nodes multicast group – This is a multicast group that all IPv6-enabled devices join. Similar to a broadcast in IPv4
  - FF02::2 All-routers multicast group – This is a multicast group that all IPv6 routers join.



Solicited-Node IPv6 Multicast Addresses

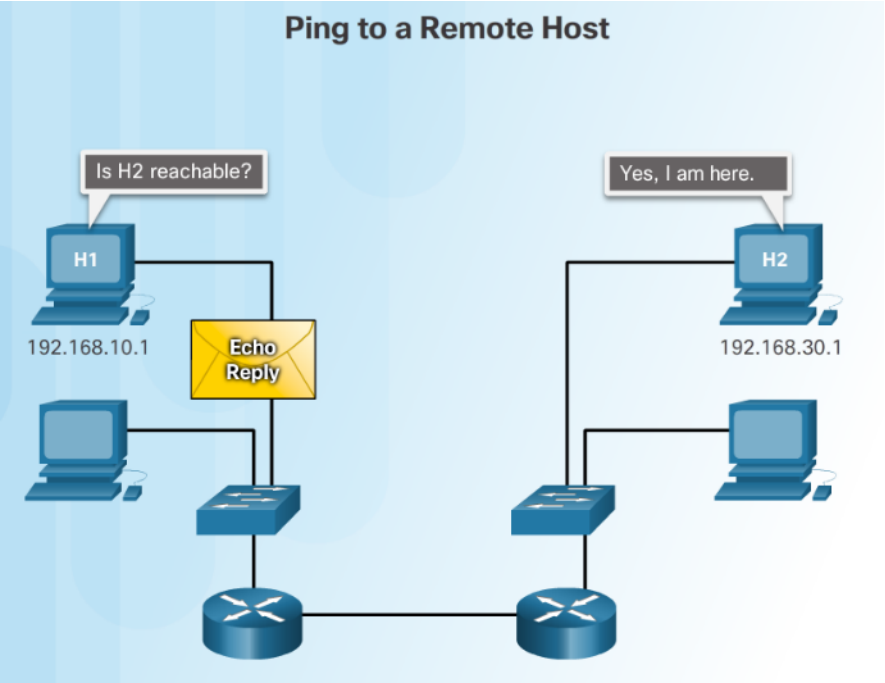
- Solicited-node multicast address:
  - Mapped to .a special Ethernet multicast address
  - Allows Ethernet NIC to filter frame on destination MAC.



Connectivity Verification

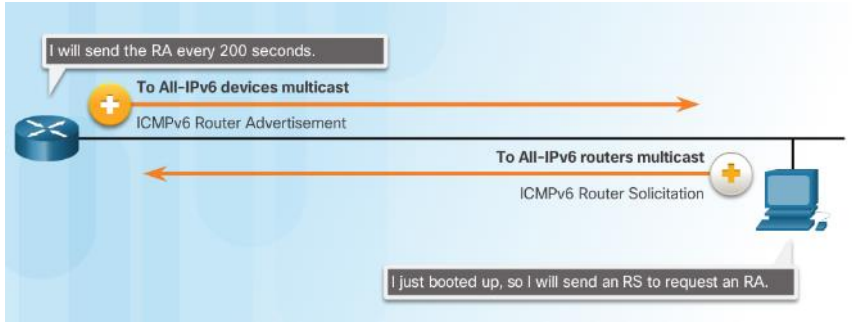
ICMPv4 and ICMPv6

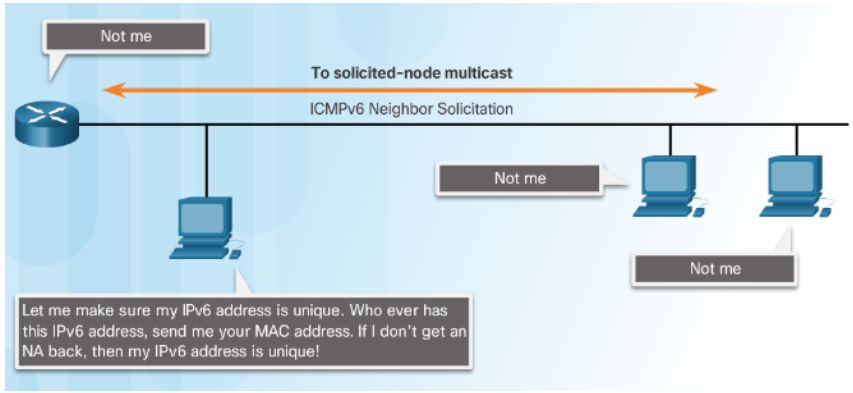
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6
- ICMP messages common to both include:
  - Host confirmation
  - Destination or Service Unreachable
  - Time exceeded
  - Route redirection



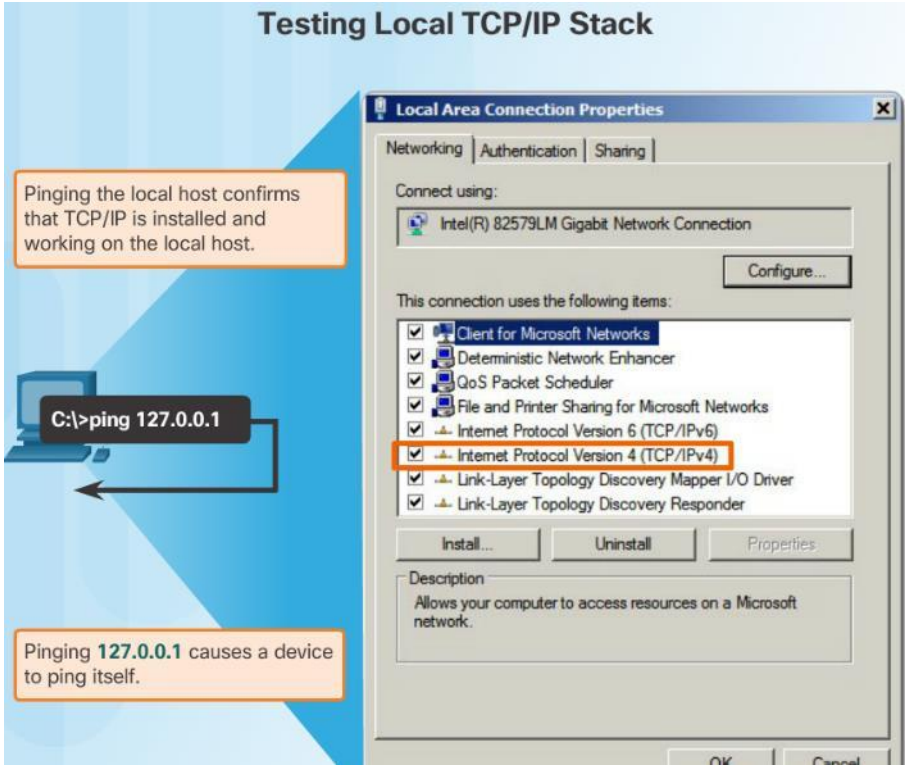
ICMPv6 Router Solicitation and Router Advertisement Messages

- ICMPv6 includes four new protocols as part of the Neighbor Discovery Protocol (ND or NDP)
  - Router Solicitation (RS) message
  - Router Advertisement (RA) message
- RA messages used to provide addressing information to hosts
  - Neighbor Solicitation (NS) message
  - Neighbor Advertisement (NA) message
- Neighbor Solicitation and Neighbor Advertisement messages are used for Address resolution and Duplicate Address Detection (DAD).



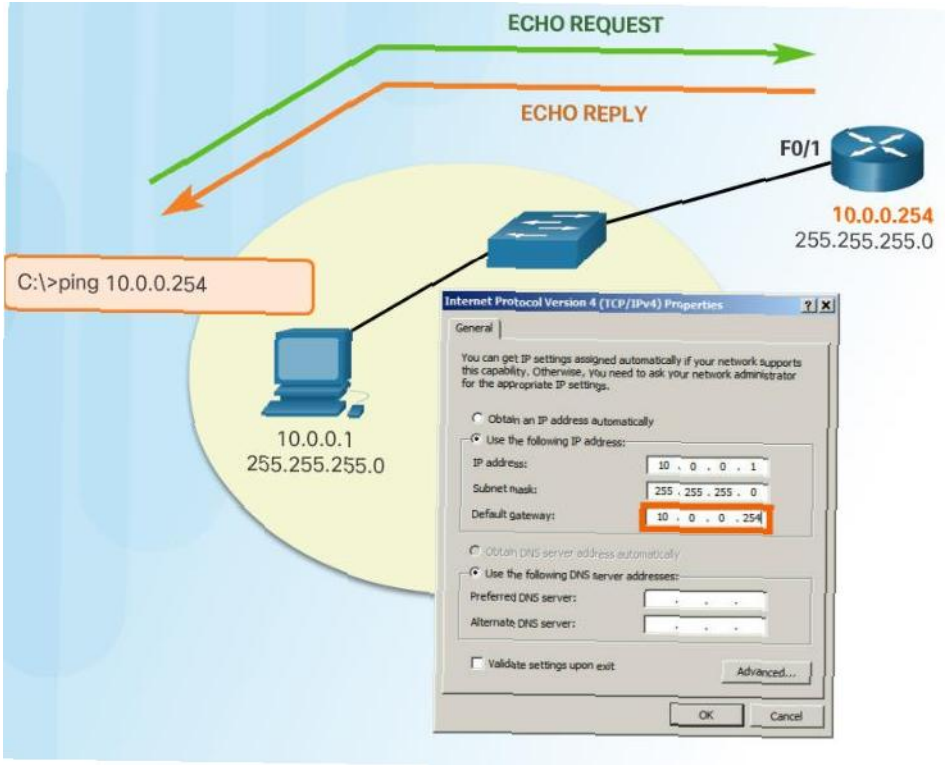


Ping - Testing the Local Stack



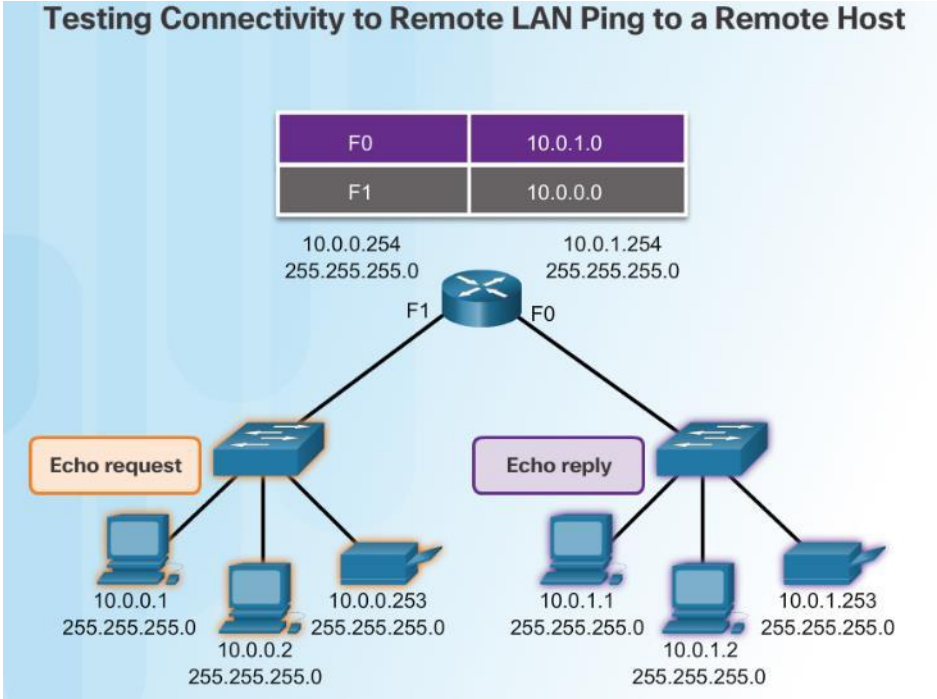
- Ping the local loopback address of 127.0.0.1 for IPv4 or ::1 for IPv6 to verify that IP is properly installed on the host.

Ping – Testing Connectivity to the Local LAN



- Use ping to test the ability of a host to communicate on the local network.

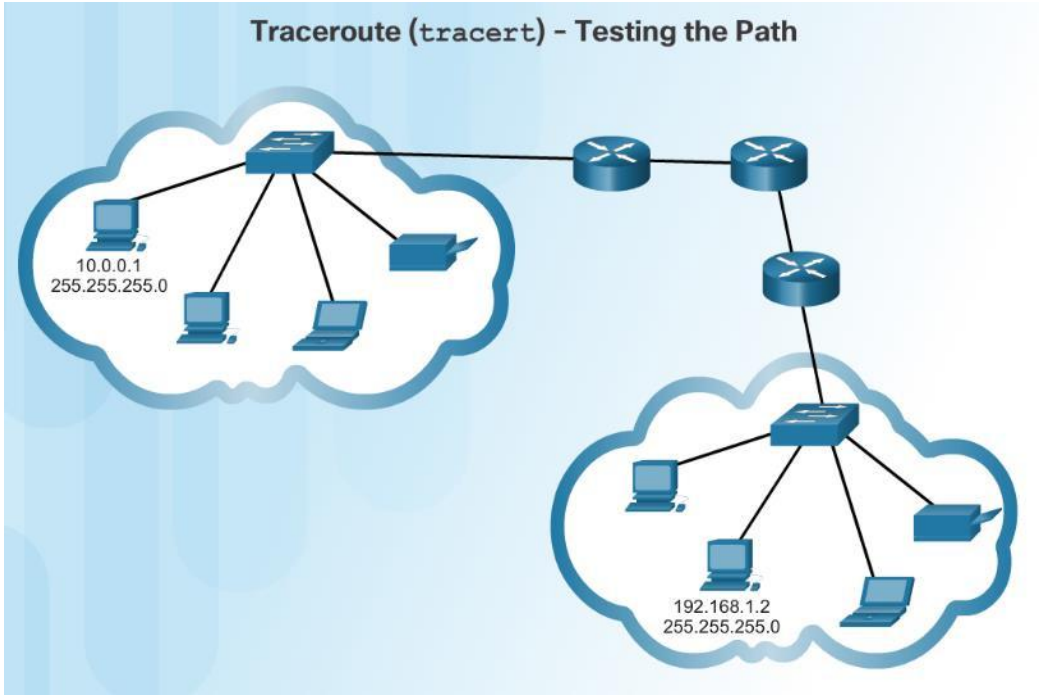
Ping – Testing Connectivity to a Remote Host



- Use ping to test the ability of a host to communicate across an internetwork.

Traceroute – Testing the Path

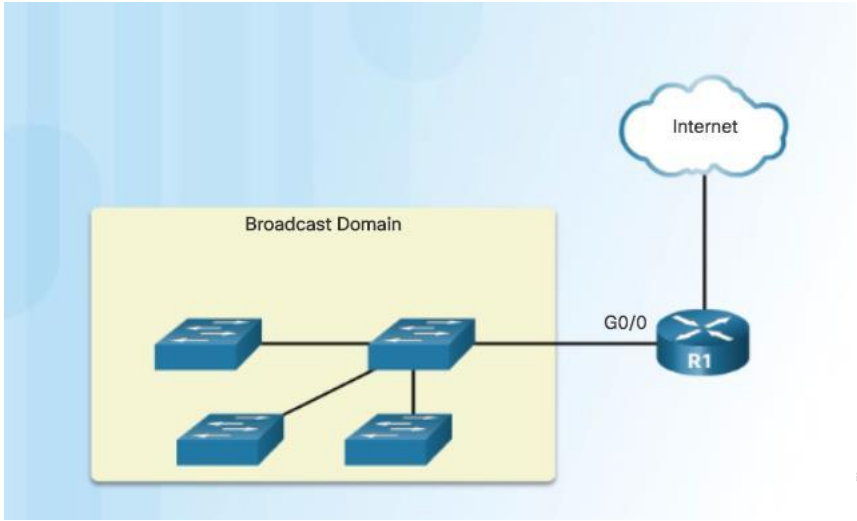
- Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path.
  - Round Trip Time (RTT) – Time it takes the packet to reach the remote host and for the response from the host to return.
  - Asterisk (*) is used to indicate a lost packet.



Subnetting an IPv4 Network

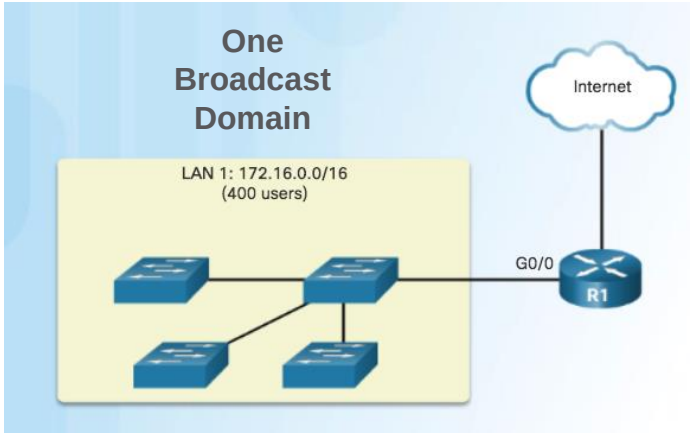
Broadcast Domains

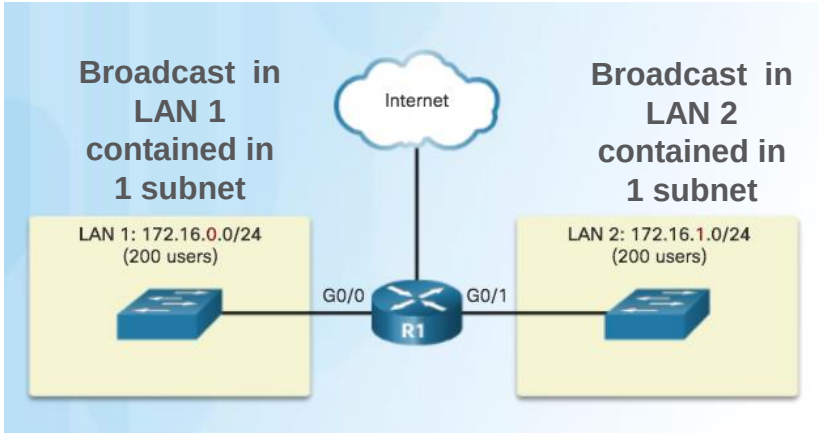
- Devices use broadcasts in an Ethernet LAN to locate:
  - **Other devices** - Address Resolution Protocol (ARP) which sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address.
  - **Services –** Dynamic Host Configuration Protocol (DHCP) which sends broadcasts on the local network to locate a DHCP server.
- Switches propagate broadcasts out all interfaces except the interface on which it was received.



Problems with Large Broadcast Domains

- Hosts can generate excessive broadcasts and negatively affect the network.
  - Slow network operations due to the significant amount of traffic it can cause.
  - Slow device operations because a device must accept and process each broadcast packet.
- Solution: Reduce the size of the network to create smaller broadcast domains. These smaller network spaces are called *subnets*.

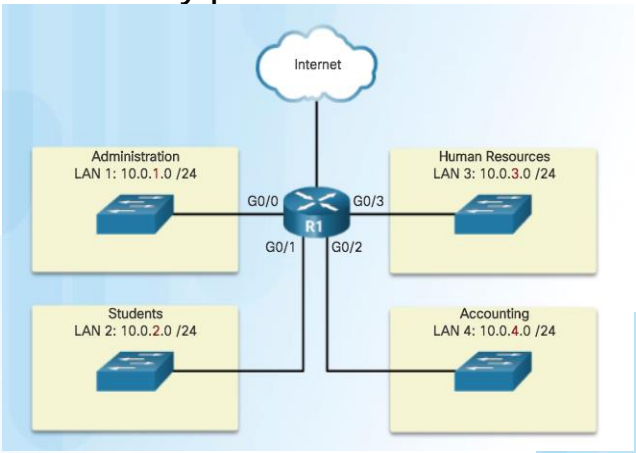




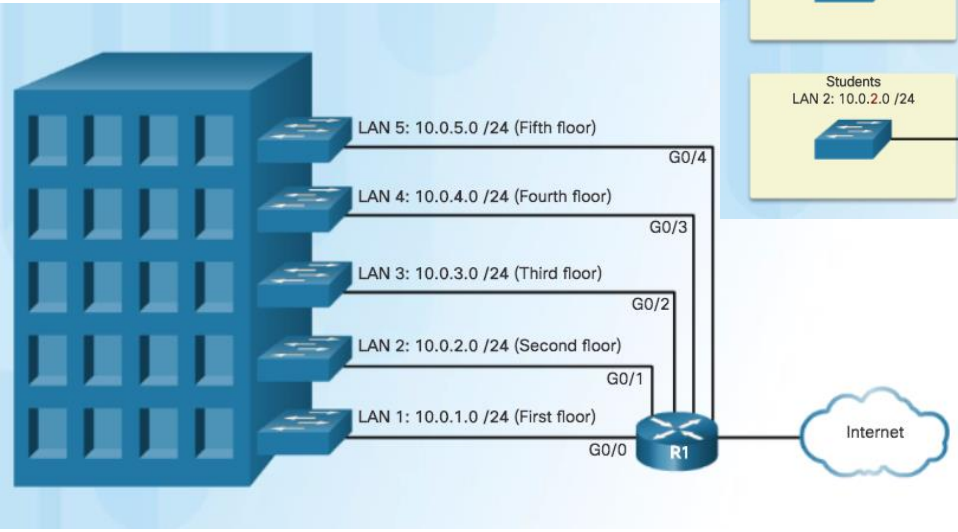
Reasons for Subnetting

- Reduces overall network traffic and improves network performance.
- Enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together.

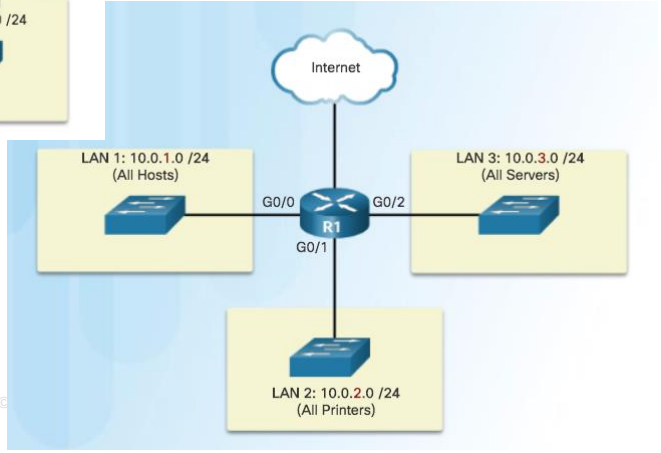
Communicating between Networks



Subnetting by Location



Subnetting by Device Type



Octet Boundaries

Networks are most easily subnetted at the octet boundary of /8, /16, and /24

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

- Prefix length and the subnet mask are different ways of identifying the network portion of an address.
- Subnets are created by borrowing host bits for network bits.
- More host bits borrowed, the more subnets that can be defined.

Subnetting on the Octet Boundary

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/16	10.0.0.1 – 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 – 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 – 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 – 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 – 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 – 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 – 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 – 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 – 10.255.255.254	10.255.255.255

- Subnetting Network 10.x.0.0/16
- Define up to 256 subnets with each subnet capable of connecting 65,534 hosts.
- First two octets identify the network portion while the last two octets are for host IP addresses.

Subnetting on the Octet Boundary (Cont.)

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/24	10.0.0.1 – 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 – 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 – 10.0.2.254	10.0.1.255
...	...	...
10.0.255.0/24	10.0.255.1 – 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 – 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 – 10.1.1.254	1.1.1.0.255
10.1.2.0/24	10.1.2.1 – 10.1.2.254	10.1.2.0.255
...	...	...
10.100.0.0/24	10.100.0.1 – 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 – 10.255.255.254	10.255.255.255

- Subnetting Network 10.x.x.0/24
- Define 65,536 subnets each capable of connecting 254 hosts.
- /24 boundary is very popular in subnetting because of number of hosts.

Classless Subnetting

Subnetting a /24 Network

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Subnets can borrow bits from *any* host bit position to create other masks.

Video Demonstration – The Subnet Mask

Subnetting in Binary

- ANDING
  - Convert IP address and Subnet Mask to Binary (line up vertically like an addition problem)
  - Logically AND (1 and 1 = 1, all other combinations = 0)
  - Result is network address for original IP address
- Classful Subnetting
  - Class A /8 255.0.0.0
  - Class B /16 255.255.0.0
  - Class C /24 255.255.255.0

Video Demonstration – The Subnet Mask (Cont.)

Subnetting 192.168.1.0/24

192	168	1	0
255	255	255	128
11000000	10101000	00000001	00000000
11111111	11111111	11111111	10000000
N	N	N	SN H

Subnet bits = $2^1 = 2$

Host bits = $2^7 = 128\text{-}2 = 126$

Subnetworks = 2

Subnetting 192.168.1.0/24

192	168	1	68
255	255	255	128
11000000	10101000	00000001	01000100
11111111	11111111	11111111	10000000
11000000	10101000	00000001	00000000
192	168	1	0

192.168.1.0 /25 ------> 192.168.1.127 /25

192.168.1.128 /25 -----> 192.168.1.255 /25

Video Demonstration – Subnetting with the Magic Number

- Magic number technique used to calculate subnets
- Magic number is simply the place value of the last one in the subnet mask
- /25 11111111.11111111.11111111.10000000 magic number = 128
- /26 11111111.11111111.11111111.11000000 magic number = 64
- /27 11111111.11111111.11111111.11100000 magic number = 32

Video Demonstration – Subnetting with the Magic Number (Cont.)

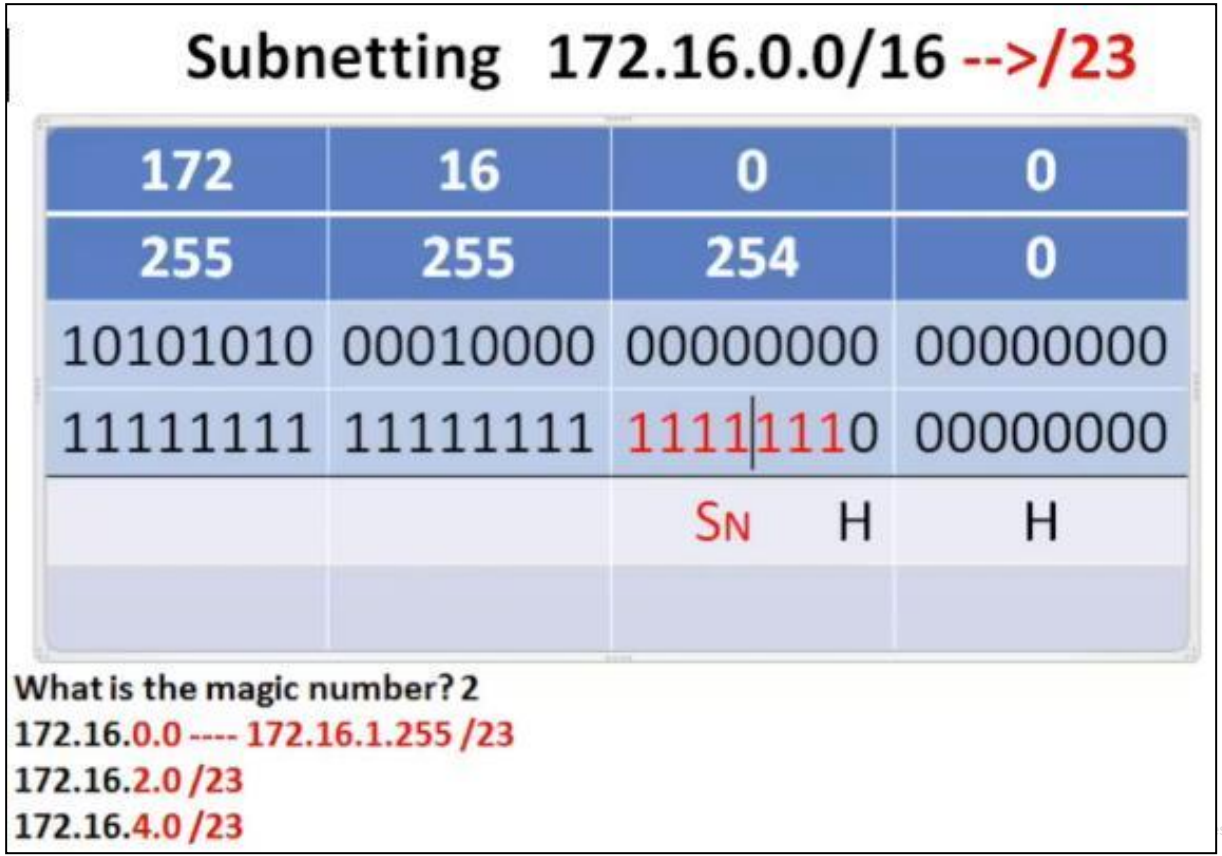
The Magic Number is the last 1 in Binary

192	168	1	0
255	255	255	224
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11100000
			SN H

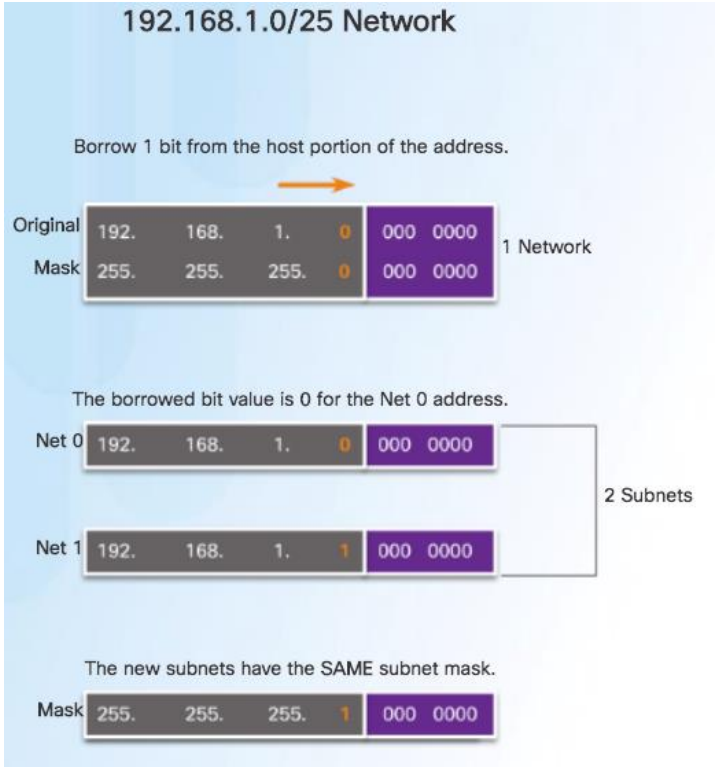
The Magic Number is? 32

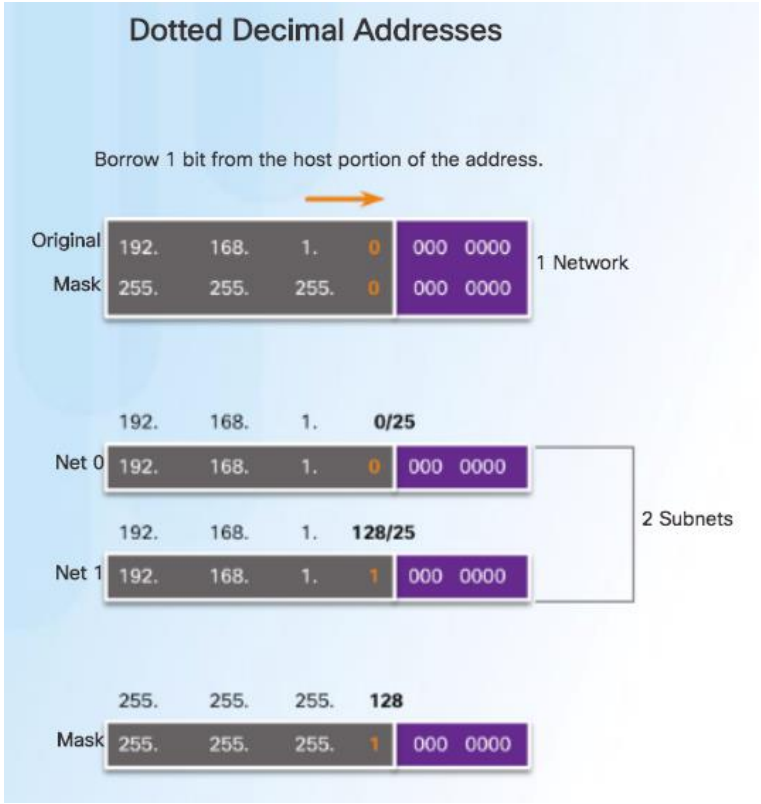
192.168.1.0 /27
192.168.1.32 /27
192.168.1.64 /27
192.168.1.96 /27
192.168.1.128 /27
192.168.1.160 /27
192.168.1.192 /27
192.168.1.224 /27

Video Demonstration – Subnetting with the Magic Number (Cont.)



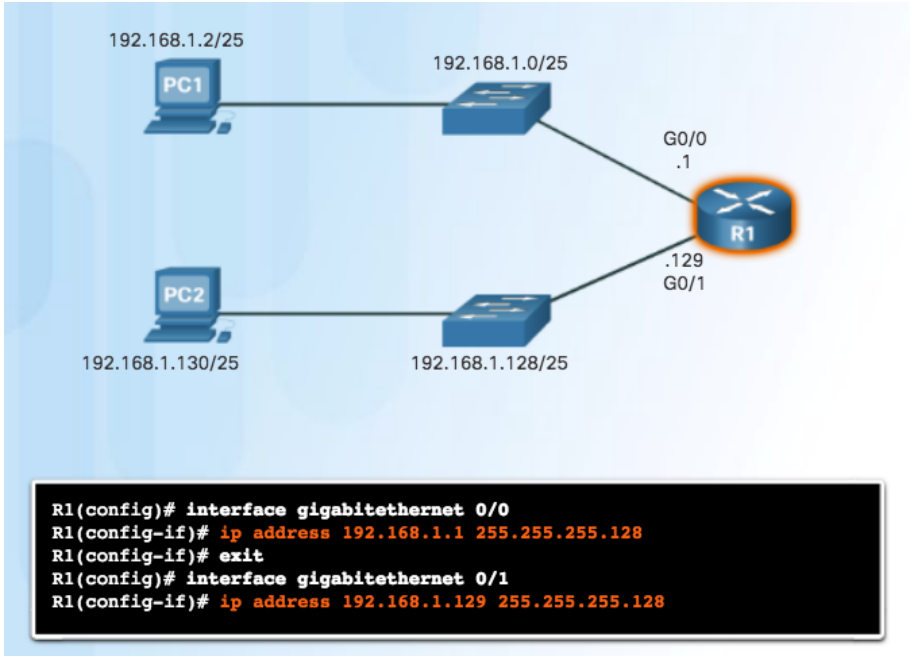
Classless Subnetting Example



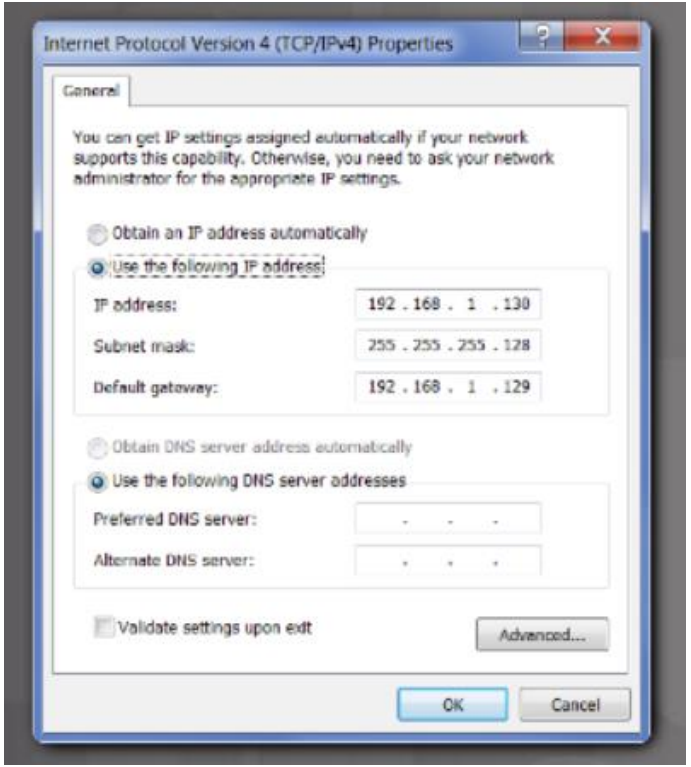


Creating 2 Subnets

- /25 Subnetting Topology




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.128
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ip address 192.168.1.129 255.255.255.128
```



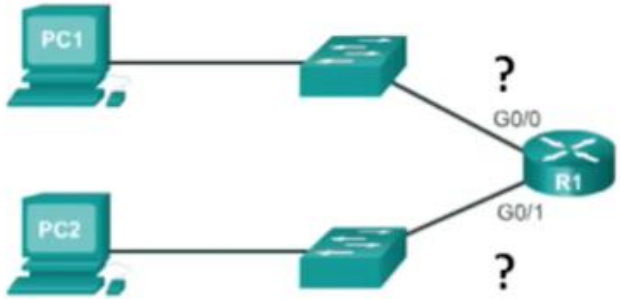
Video Demonstration – Creating Two Equal-sized Subnets (/25)

Create 2 Equal-sized Subnets from 192.168.1.0 /24

- **Subnet Mask** - 11111111.11111111.11111111.10000000

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

- Magic Number = 128
- 192.168.1.0 /25 (start at 0)
- 192.168.1.128 /25 (Add 128)



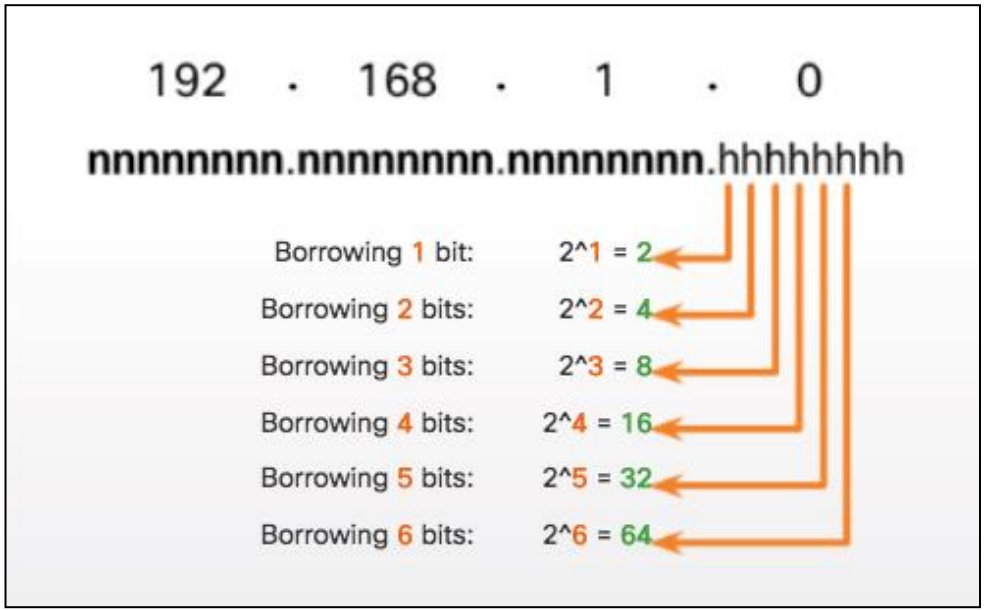
Subnetting Formulas

Calculate Number of Subnets Formula

2^n

n =bits borrowed

Subnetting a /24 Network



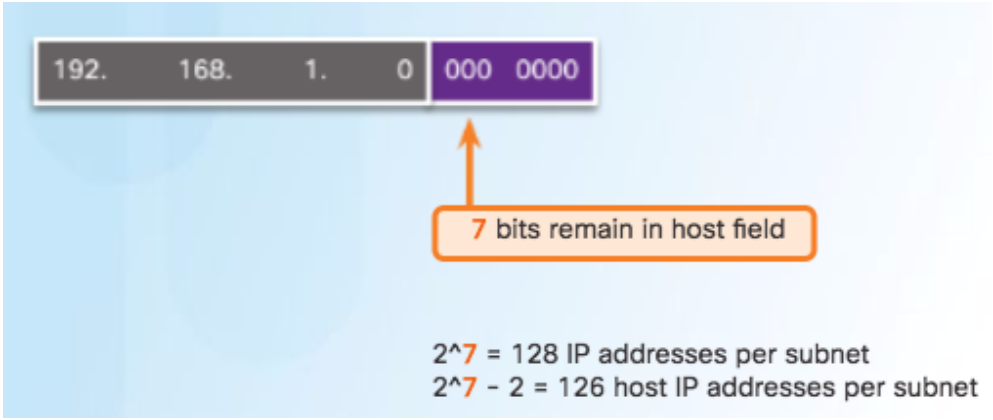
Subnetting Formulas (Cont.)

Calculate Number of Hosts Formula

2^n-2

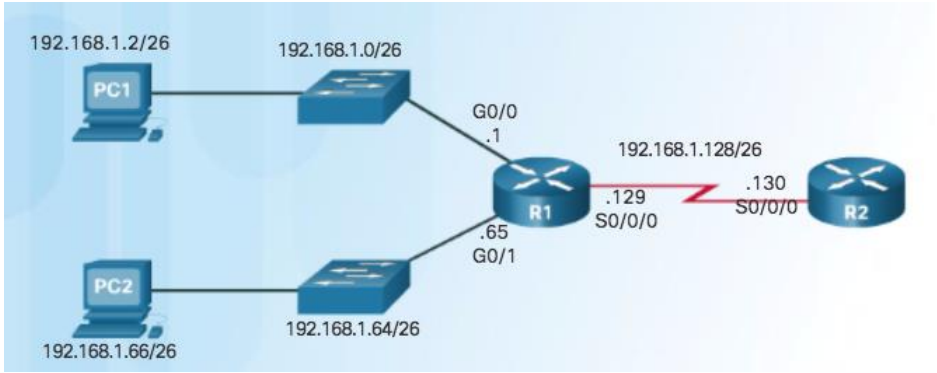
n = the number of bits remaining in the host field

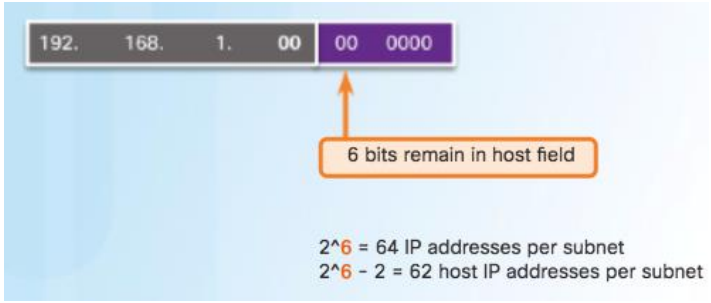
Calculating the Number of Hosts

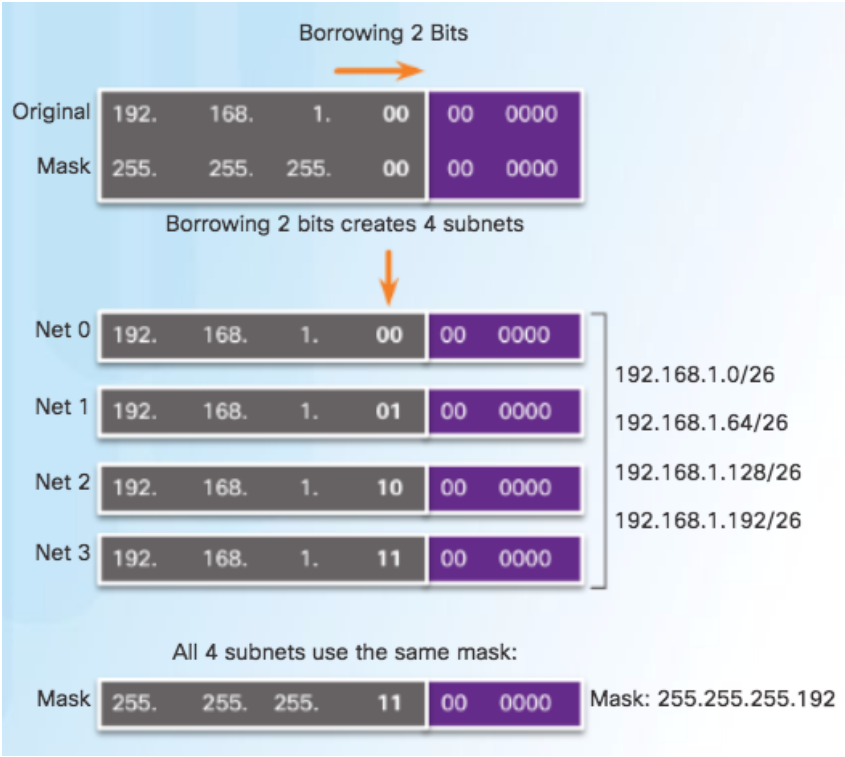


Creating 4 Subnets

- /26 Subnetting Topology







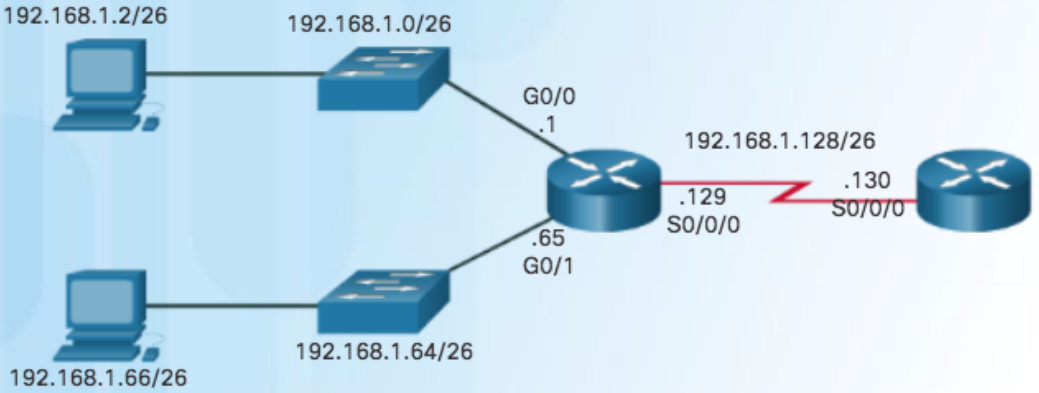
Creating 4 Subnets (Cont.)

- /26 Subnetting Topology

Net 0	Network	192.	168.	1.	00	00	0000	192.168.1.0
	First	192.	168.	1.	00	00	0001	192.168.1.1
	Last	192.	168.	1.	00	11	1110	192.168.1.62
	Broadcast	192.	168.	1.	00	11	1111	192.168.1.63
Net 1	Network	192.	168.	1.	01	00	0000	192.168.1.64
	First	192.	168.	1.	01	00	0001	192.168.1.65
	Last	192.	168.	1.	01	11	1110	192.168.1.126
	Broadcast	192.	168.	1.	01	11	1111	192.168.1.127
Net 2	Network	192.	168.	1.	10	00	0000	192.168.1.128
	First	192.	168.	1.	10	00	0001	192.168.1.129
	Last	192.	168.	1.	10	11	1110	192.168.1.190
	Broadcast	192.	168.	1.	10	11	1111	192.168.1.191

Creating 4 Subnets (Cont.)

- /26 Subnetting Topology

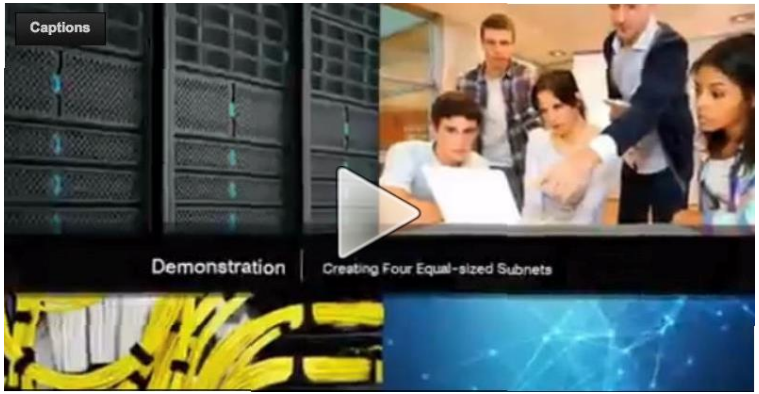



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.192
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.1.65 255.255.255.192
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.129 255.255.255.192
```

Video Demonstration – Creating Four Equal-sized Subnets (/26)

Create 4 Equal-sized Subnets from 192.168.1.0 /24

- Subnet Mask in Binary – 11111111.11111111.11111111.11000000
- 2^2 = 4 Subnets
- Magic Number = 64
- 192.168.1.0 /26
- 192.168.1.64 /26
- 192.168.1.128 /26
- 192.168.1.192 /26



Video Demonstration – Creating Eight Equal-sized Subnets (/27)

Create 8 Equal-sized Subnets from 192.168.1.0 /24

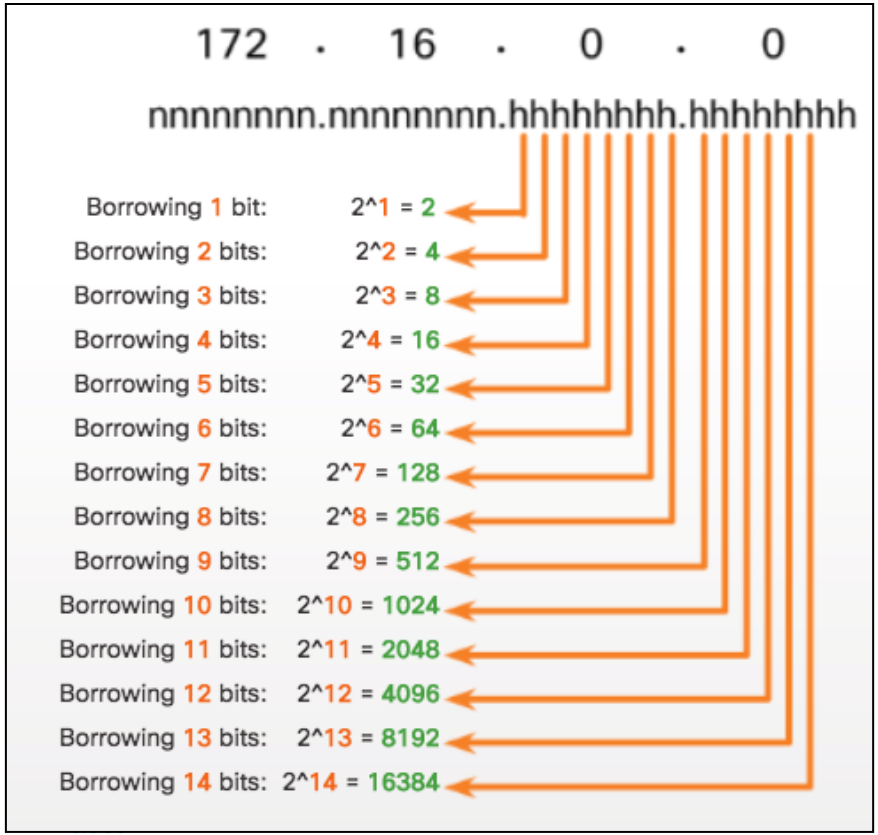
- Borrow 3 bits – 11111111.11111111.11111111.11100000
- Magic Number = 32
- 192.168.1.0 /27 (Start at 0)
- 192.168.1.32 /27 (Add 32 to previous network)
- 192.168.1.64 /27 (Add 32)
- 192.168.1.96 /27 (Add 32)
- 192.168.1.128 /27 (Add 32)
- 192.168.1.160 /27 (Add 32)
- 192.168.1.192 /27 (Add 32)
- 192.168.1.224 /27 (Add 32)

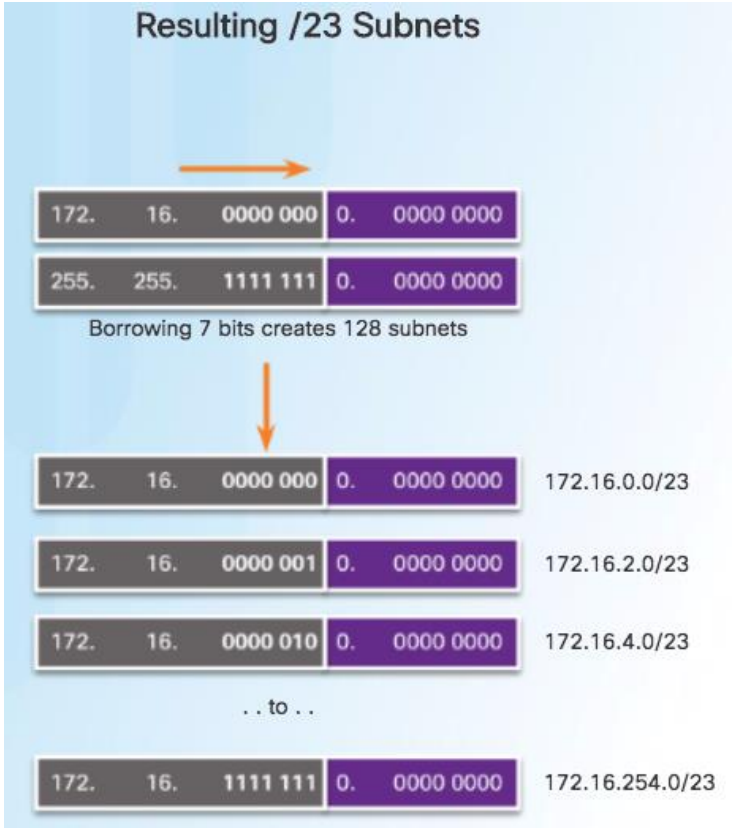
Creating Subnets with a /16 prefix

Subnetting a /16 Network

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022

Creating 100 Subnets with a /16 prefix





Subnetting a /16 and /8 Prefix

Calculating the Hosts

Hosts = 2^n
(where n = host bits remaining)

172.	16.	00 00 00 0	0.	0000 0000

9 bits remain in host field

2^9 = 512 IP addresses per subnet
2^9 - 2 = 510 host IP addresses per subnet

Address Range for 172.16.0.0/23 Subnet

Network Address

172.	16.	00 00 00 0	0.	0000 0000	= 172.16.0.0/23

First Host Address

172.	16.	00 00 00 0	0.	0000 0001	= 172.16.0.1/23

Last Host Address

172.	16.	00 00 00 0	1.	1111 1110	= 172.16.1.254/23

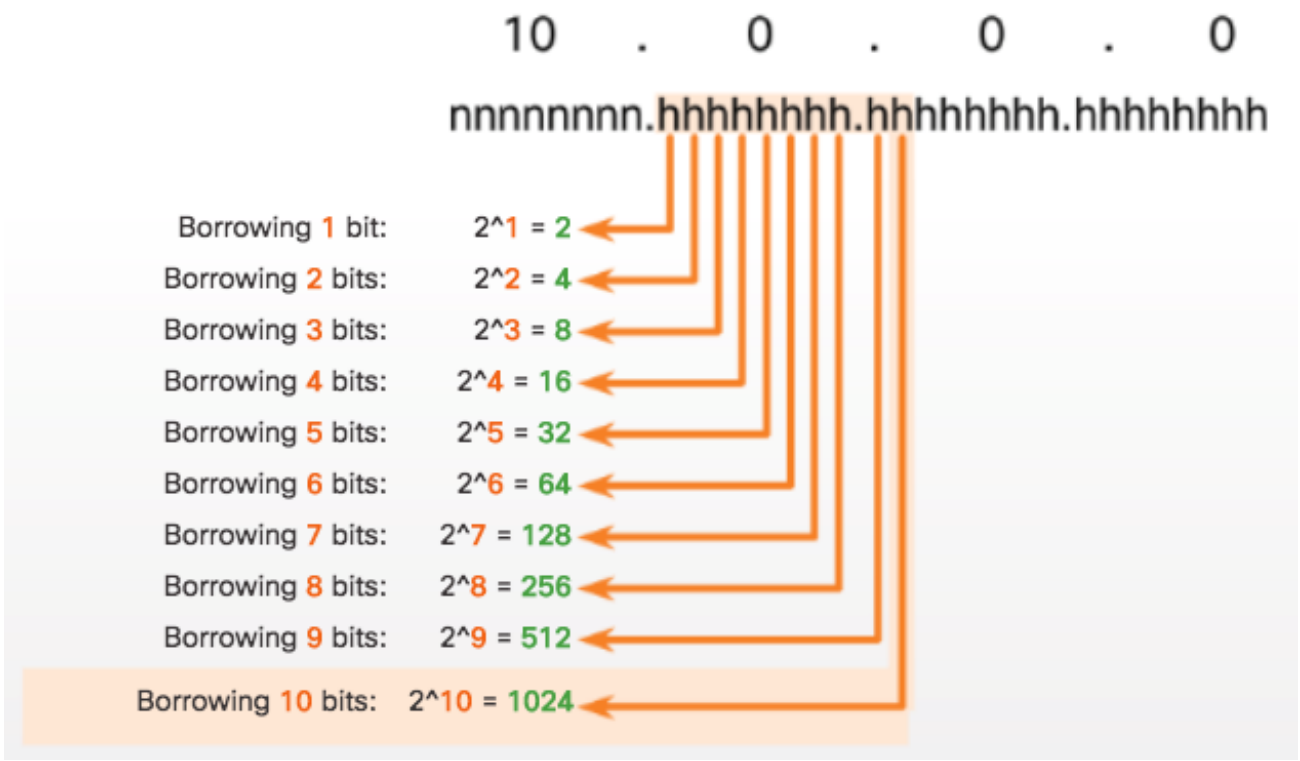
Broadcast Address

172.	16.	00 00 00 0	1.	1111 1111	= 172.16.1.255/23

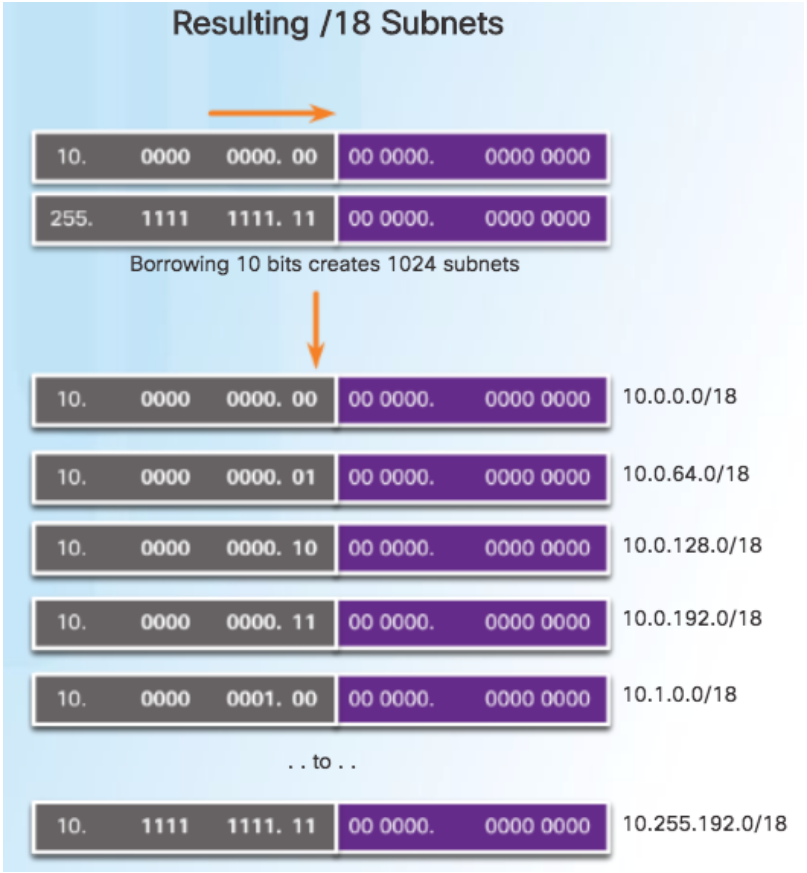
Video Demonstration – Creating One Hundred Equal-sized Subnets

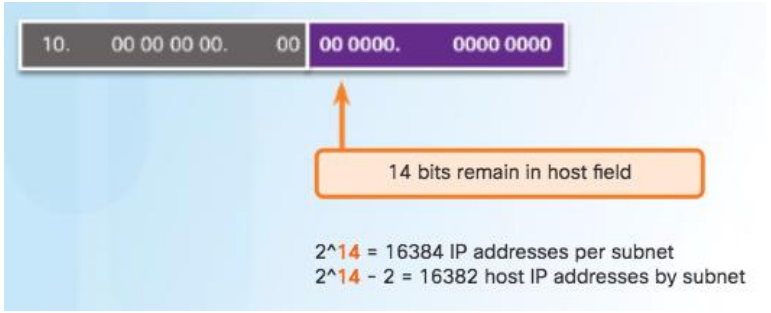
- An enterprise network requires 100 equal-sized subnets starting from 172.16.0.0/16
  - New Subnet Mask
    - 11111111.11111111.1111111**0**.00000000
  - 2^7 = 128 Subnets
  - 2^9 = 512 hosts per subnet
  - Magic Number = **2**
  - 172.16.**0**.0 /23
  - 172.16.**2**.0 /23
  - 172.16.**4**.0 /23
  - 172.16.**6**.0 /23
  - …
  - 172.16.**254**.0 /23

Creating 1000 Subnets with a /8 Network



Creating 1000 Subnets with a /8 Network (Cont.)





Video Demonstration – Subnetting Across Multiple Octets

The Magic Number is the last 1 in Binary

10	0	0	0
255	0	0	0
00001010	00000000	00000000	00000000
11111111	11100000	00000000	00000000
	SN H	H	H

The Magic Number is? 32

10.0.0.0 /11 10.128.0.0 /11
10.32.0.0 /11 10.160.0.0 /11
10.64.0.0 /11 10.192.0.0 – 10.223.255.255 /11
10.96.0.0 /11 10.224.0.0 /11

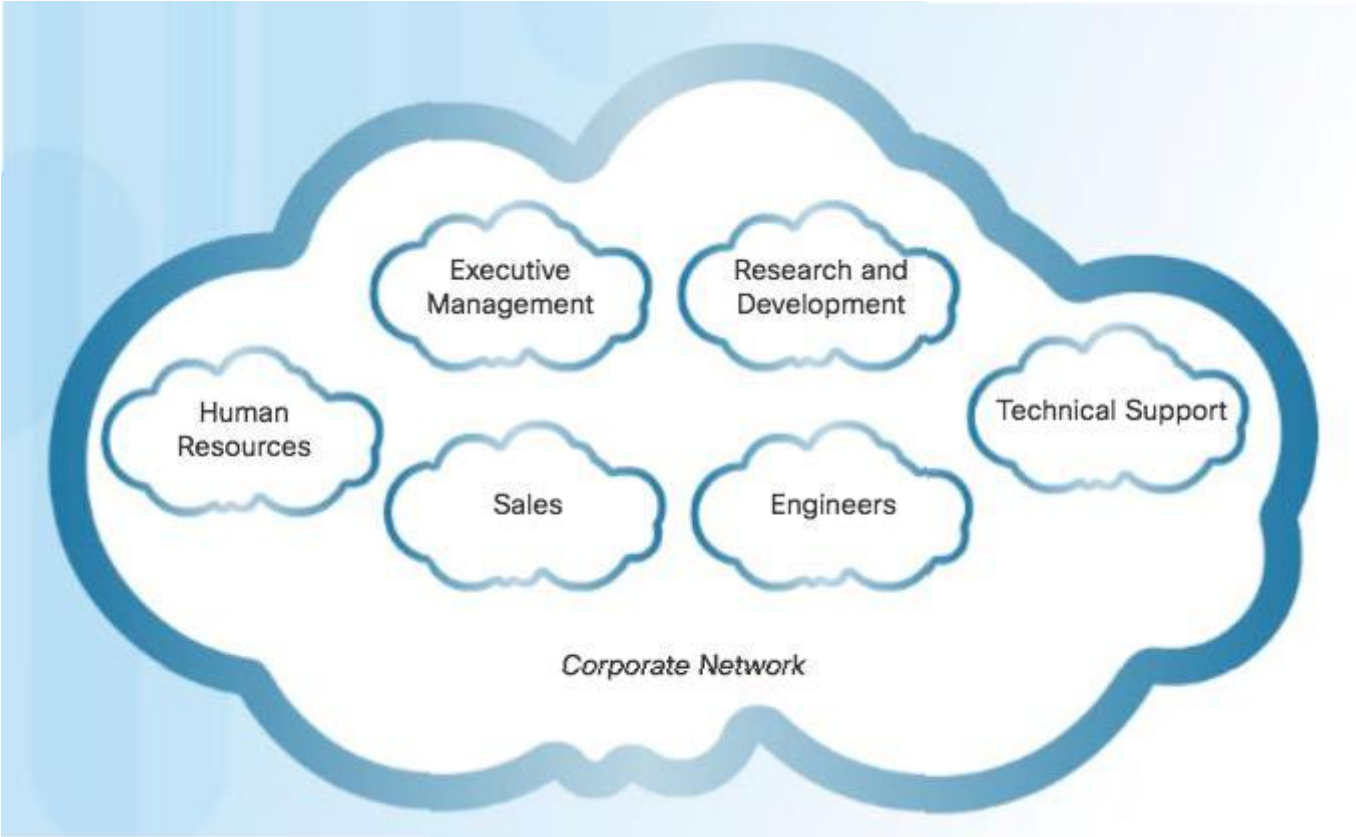
New Challenge Problem: Create over 300 Equal-sized Subnets of 20,000 Hosts each starting from 10.0.0.0/8

Subnetting Based on Host Requirements

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14

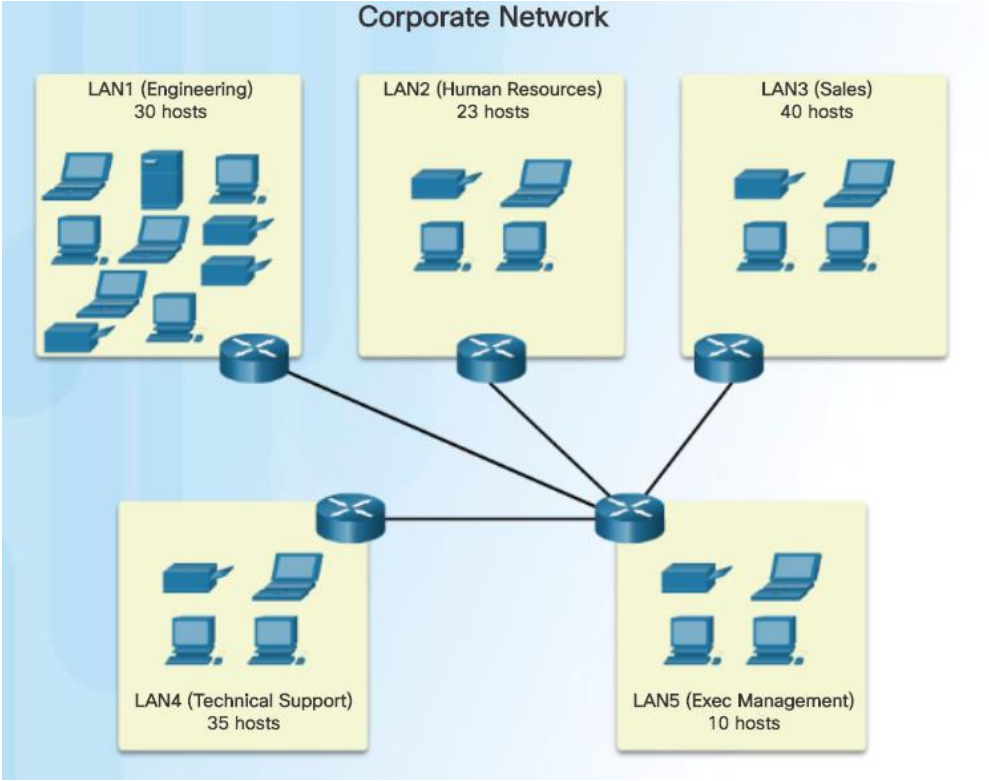
Subnetting Based On Network Requirements

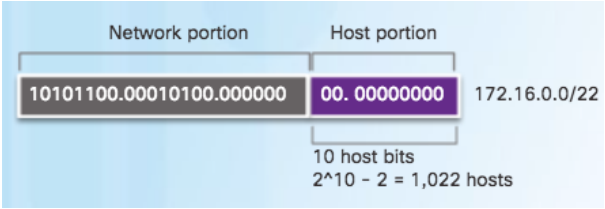
Host devices used by employees in the Engineering department in one network and Management in a separate network.



Subnetting to Meet Requirements

Network Requirement Example





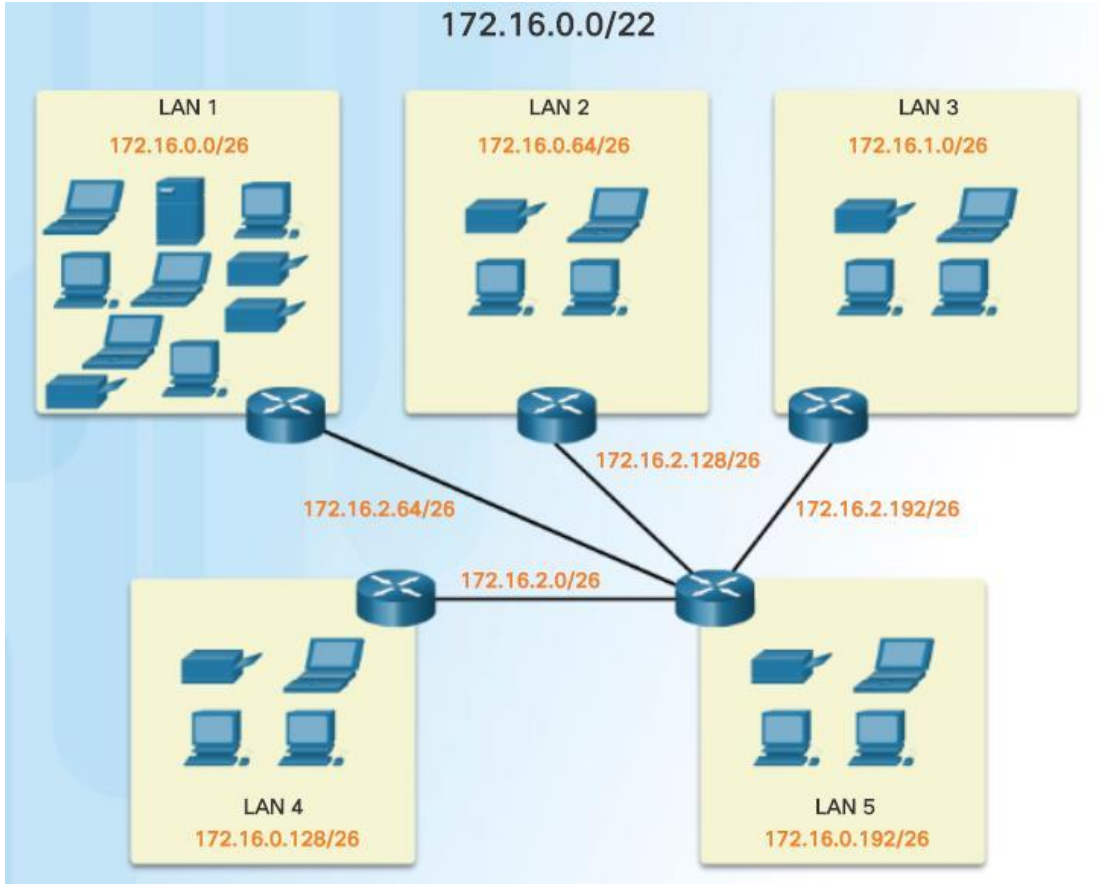
	Network Portion	Host Portion		Dotted Decimal
	10101100.00010000.000000	00.00	000000	172.16.0.0/22
0	10101100.00010000.000000	00.00	000000	172.16.0.0/26
1	10101100.00010000.000000	00.01	000000	172.16.0.64/26
2	10101100.00010000.000000	00.10	000000	172.16.0.128/26
3	10101100.00010000.000000	00.11	000000	172.16.0.192/26
4	10101100.00010000.000000	01.00	000000	172.16.1.0/26
5	10101100.00010000.000000	01.01	000000	172.16.1.64/26
6	10101100.00010000.000000	01.10	000000	172.16.1.128/26

Nets 7 – 13 not shown

14	10101100.00010000.000000	11.10	000000	172.16.3.128/26
15	10101100.00010000.000000	11.11	000000	172.16.3.192/26

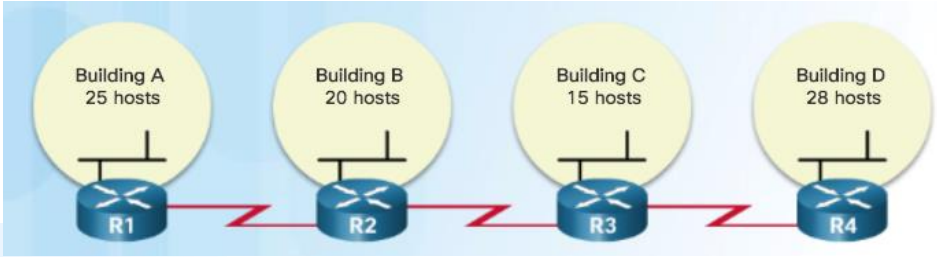
4 bits borrowed from host portion to create subnets

Network Requirement Example (Cont.)



Benefits of Variable Length Subnet Masking

Traditional Subnetting Wastes Addresses



	Network Portion	Host Portion		
	11000000.10101000.00010100	.000	00000	192.168.20.0/24
0	11000000.10101000.00010100	.000	00000	192.168.20.0/27
1	11000000.10101000.00010100	.001	00000	192.168.20.32/27
2	11000000.10101000.00010100	.010	00000	192.168.20.64/27
3	11000000.10101000.00010100	.011	00000	192.168.20.96/27
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27

Building LANs A, B, C, and D

Site to Site WANs

Unused / Available

Subnet portion
2^3 = 8 subnets

Host portion
2^5 – 2 = 30 host IP addresses per subnet

	Network Portion	Host Portion		Dotted Decimal
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27

Host portion
2^5 – 2 = 30 host IP addresses per subnet

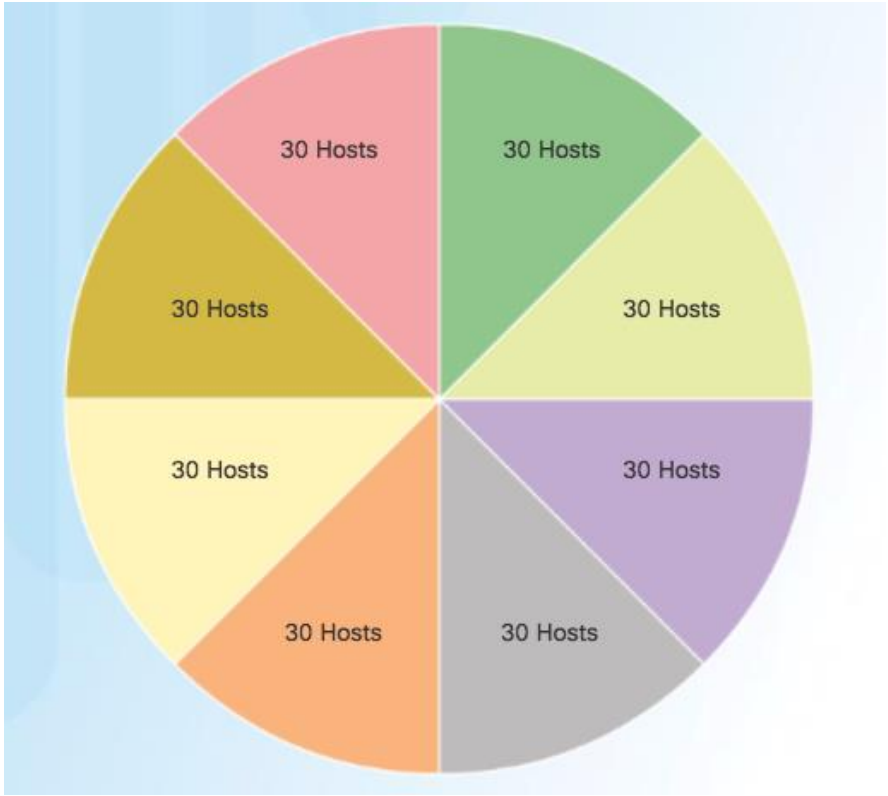
30 – 2 = 28
Each WAN subnet wastes 28 addresses

28 x 3 = 84
84 addresses are unused

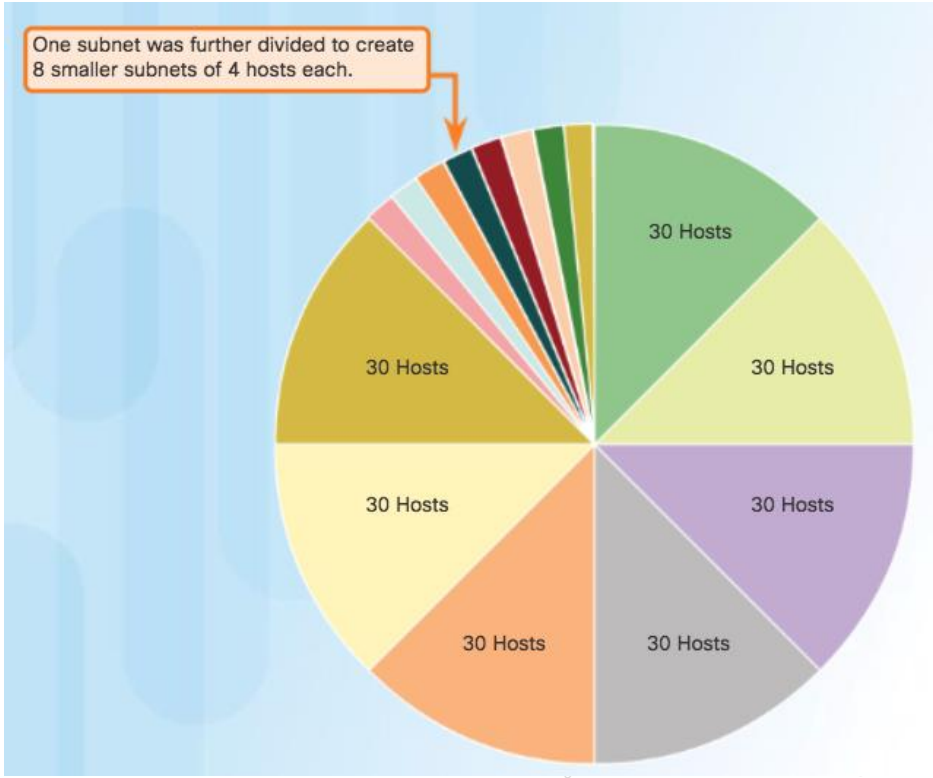
Benefits of Variable Length Subnet Masking

Variable Length Subnet Masks (VLSM)

Traditional



Subnets of Varying Sizes



Benefits of Variable Length Subnet Masking

Basic VLSM

Basic Subnetting

	Network portion	Host portion		Dotted Decimal	
	11000000.10101000.00010100	.00000000		192.168.20.0/24	
0	11000000.10101000.00010100	.000	00000	192.168.20.0/27	LANs A, B, C, D
1	11000000.10101000.00010100	.001	00000	192.168.20.32/27	
2	11000000.10101000.00010100	.010	00000	192.168.20.64/27	
3	11000000.10101000.00010100	.011	00000	192.168.20.96/27	
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27	Unused / Available
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27	
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	

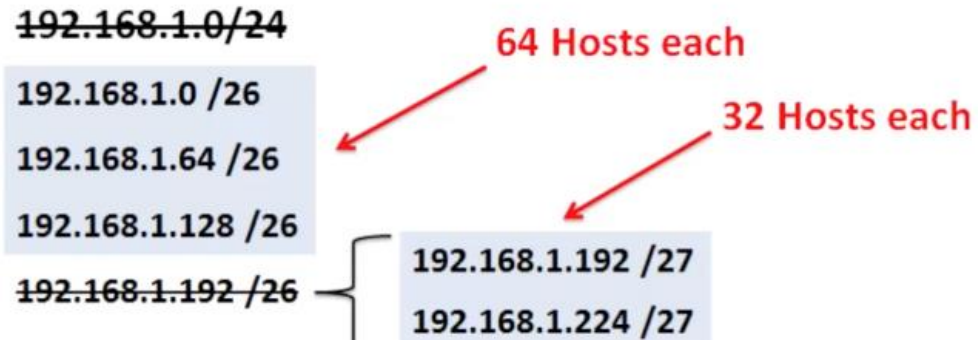
Subnet 7 will be subnetted further.

	Network portion	Host portion		Dotted Decimal	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	
	3 more bits borrowed from subnet 7				
7:0	11000000.10101000.00010100	.111000	00	192.168.20.224/30	WANs
7:1	11000000.10101000.00010100	.111001	00	192.168.20.228/30	
7:2	11000000.10101000.00010100	.111010	00	192.168.20.232/30	
7:3	11000000.10101000.00010100	.111011	00	192.168.20.236/30	Unused / Available
7:4	11000000.10101000.00010100	.111100	00	192.168.20.240/30	
7:5	11000000.10101000.00010100	.111101	00	192.168.20.244/30	
7:6	11000000.10101000.00010100	.111110	00	192.168.20.248/30	
7:7	11000000.10101000.00010100	.111111	00	192.168.20.252/30	

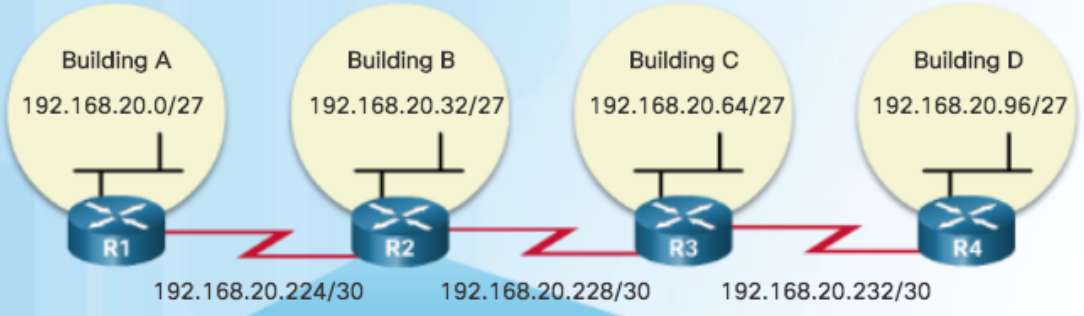
Subnetting a subnet

Video Demonstration – VLSM Basics

- Basic VLSM
  - Subnets do not have to be equal sizes, as long as their address ranges do not overlap.
  - When creating subnets it is easier to work from larger to smaller.

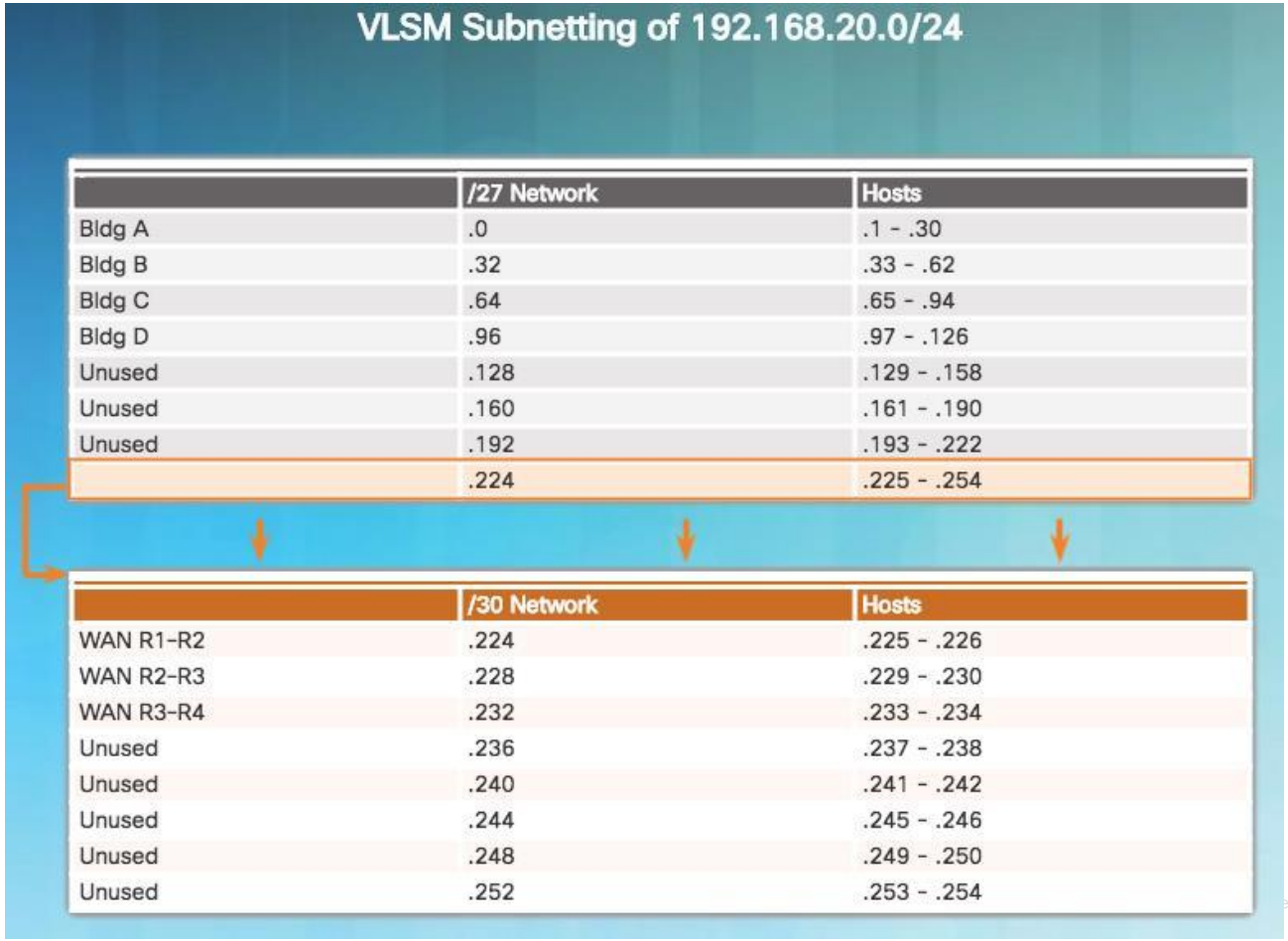


VLSM in Practice




```
R2(config)# interface gigabitethernet 0/0
R2(config-if)# ip address 192.168.20.33 255.255.255.224
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.20.226 255.255.255.252
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config)# ip address 192.168.20.229 255.255.255.252
R2(config-if)# end
R2#
```

VLSM Chart



	/27 Network	Hosts
Bldg A	.0	.1 - .30
Bldg B	.32	.33 - .62
Bldg C	.64	.65 - .94
Bldg D	.96	.97 - .126
Unused	.128	.129 - .158
Unused	.160	.161 - .190
Unused	.192	.193 - .222
	.224	.225 - .254

	/30 Network	Hosts
WAN R1-R2	.224	.225 - .226
WAN R2-R3	.228	.229 - .230
WAN R3-R4	.232	.233 - .234
Unused	.236	.237 - .238
Unused	.240	.241 - .242
Unused	.244	.245 - .246
Unused	.248	.249 - .250
Unused	.252	.253 - .254

Video Demonstration – VLSM Example

- Given the network 172.16.0.0 /23 creates subnets:
  - 1 network for 200 hosts - 256
  - 1 network for 100 hosts - 128
  - 1 network for 50 hosts - 64
  - 1 network for 25 hosts - 32
  - 1 network for 10 hosts - 16
  - 4 point-to-point networks for 2 hosts each – 4x4 = 16

/23 = 2^9 hosts = 512
256+128+64+32+16+16 = 512 hosts needed
Address range 172.16.0.0 – 172.16.1.255

~~172.16.0.0 /23~~

172.16.0.0 /24 (256)

~~172.16.1.0 /24~~

172.16.1.0 /25 (128)

~~172.16.1.128 /25~~

172.16.1.128 /26 (64)

~~172.16.1.192 /26~~

172.16.1.192 /27 (32)

~~172.16.1.224 /27~~

172.16.1.224 /28 (16)

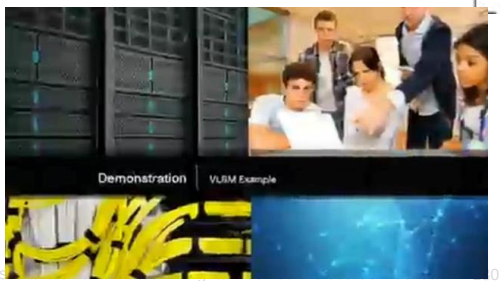
~~172.16.1.240 /28~~

172.16.1.240 /30 (4)

172.16.1.244 /30 (4)

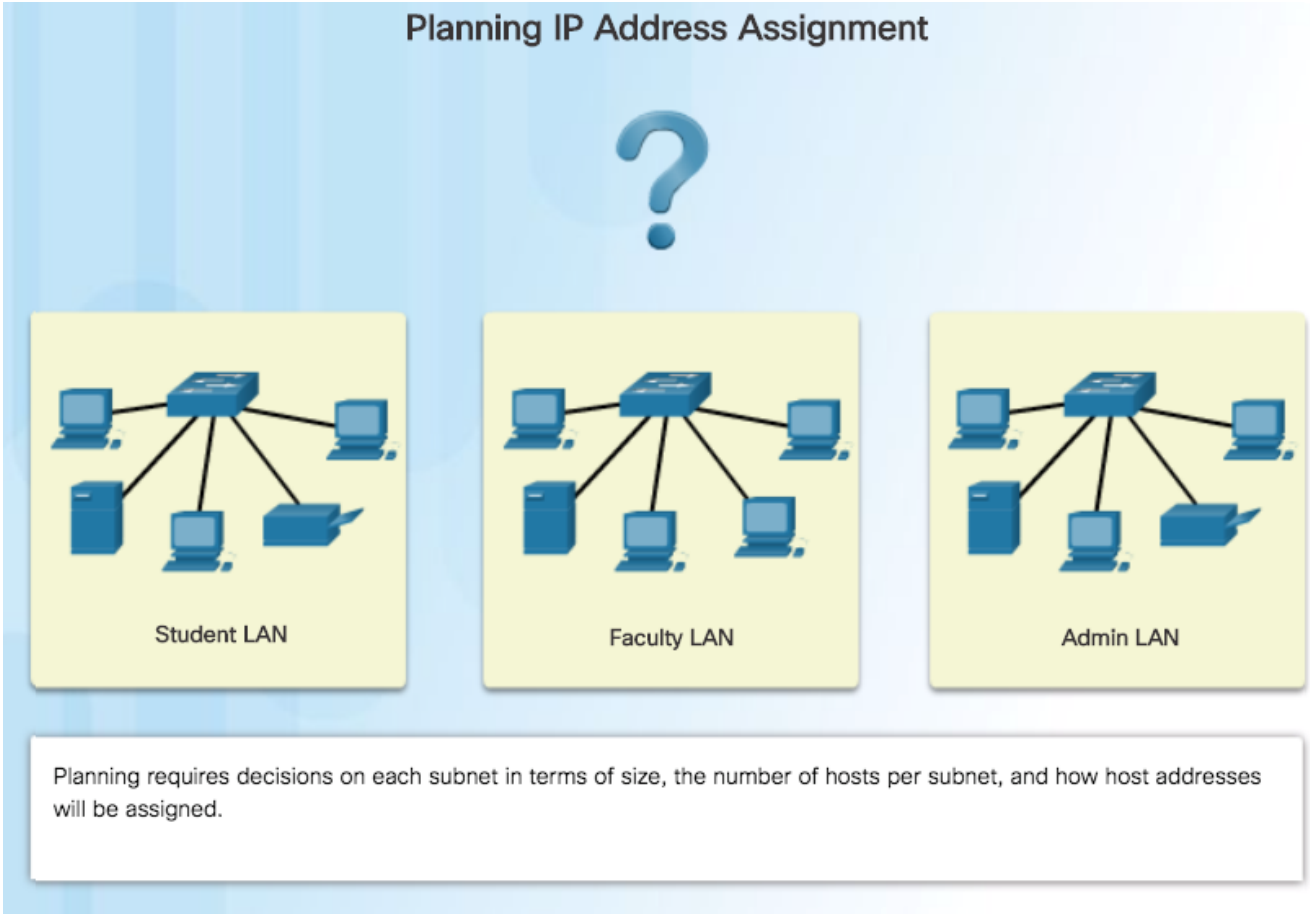
172.16.1.248 /30 (4)

172.16.1.252 /30 (4)



Addressing Schemes

Network Address Planning



Planning to Address the Network

- Each host in an internetwork must have a unique address.
- Need proper planning & documentation.
- Must provide & control access to servers from internal hosts and external hosts.
- Layer 3 STATIC address assigned to a server can be used to control access to that server.
- Monitoring security and performance of hosts means network traffic is examined for source IP addresses that are generating or receiving excessive packets.

Assigning Addresses to Devices

- Devices that require addresses:
  - **End user clients**
  - Can be set for DHCP to save time and manual errors.
  - A change in the subnetting scheme requires reconfiguration of DHCP server. IPv6 clients use DHCPv6/SLAAC.
  - **Servers**
    - Configured with static addresses.
    - Private addresses translated to public addresses if accessible from the Internet.
  - **Intermediary devices**
    - Set with static addresses for remote management.
  - **Gateway**
    - Router interface used to exit the network.

Network: 192.168.1.0/24

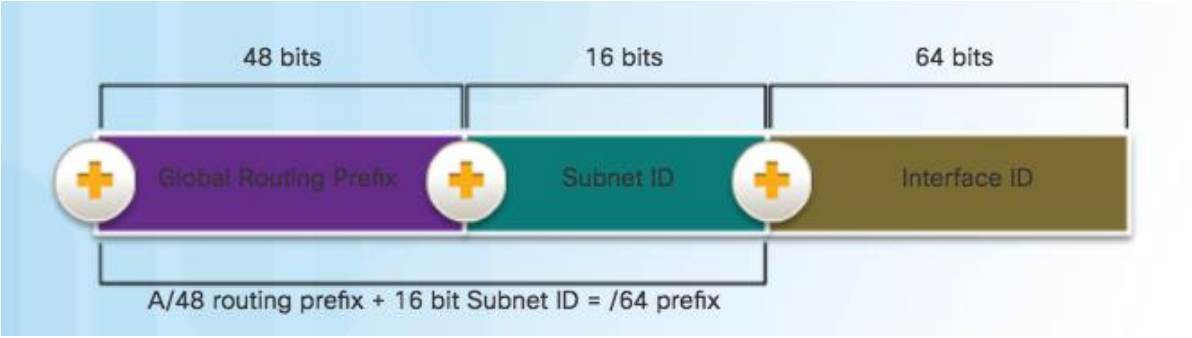
Use	First	Last
Host Devices	.1	.229
Servers	.230	.239
Printers	.240	.249
Intermediary Devices	.250	.253
Gateway (router LAN interface)	.254	

Design Considerations for IPv6

The IPv6 Global Unicast Address

- IPv6 subnetting is not concerned with conserving address space.
- IPv6 subnetting is about building an addressing hierarchy based on the number of subnetworks needed.
- IPv6 link-local address is never subnetted.
- IPv6 global unicast address can be subnetted.
- IPv6 global unicast address normally consists of a /48 global routing prefix, a 16 bit subnet ID, and a 64 bit interface ID.

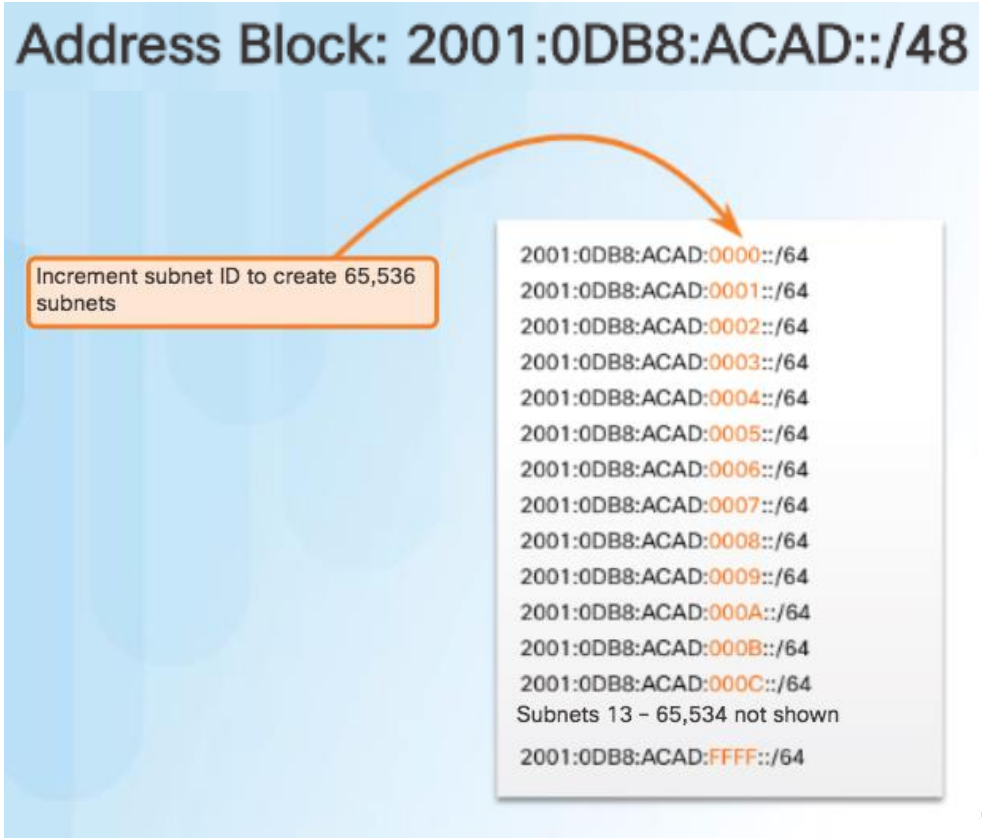
Structure



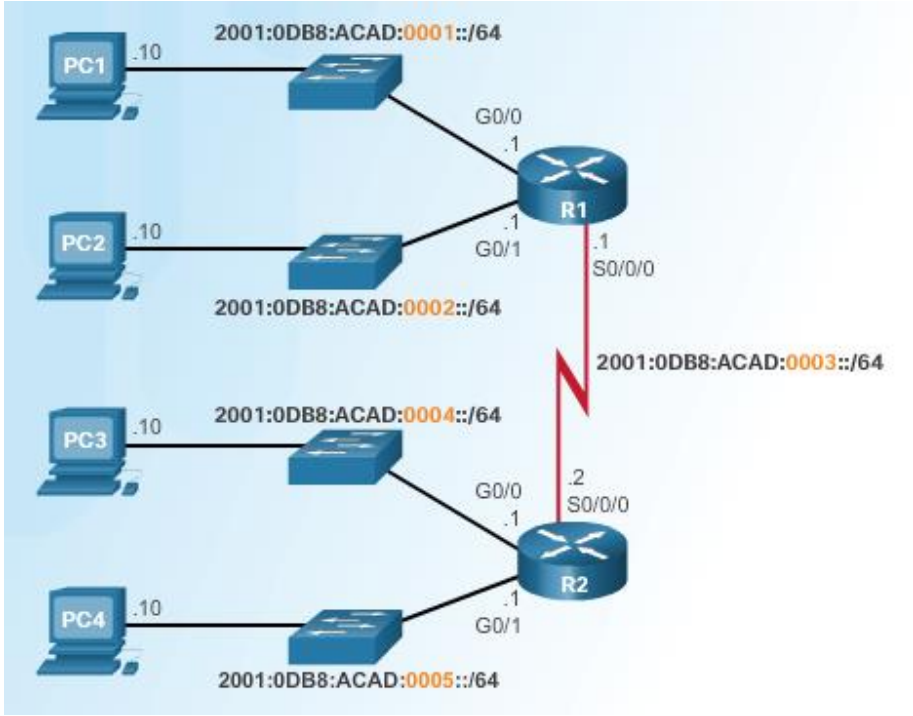
Global Routing Prefix

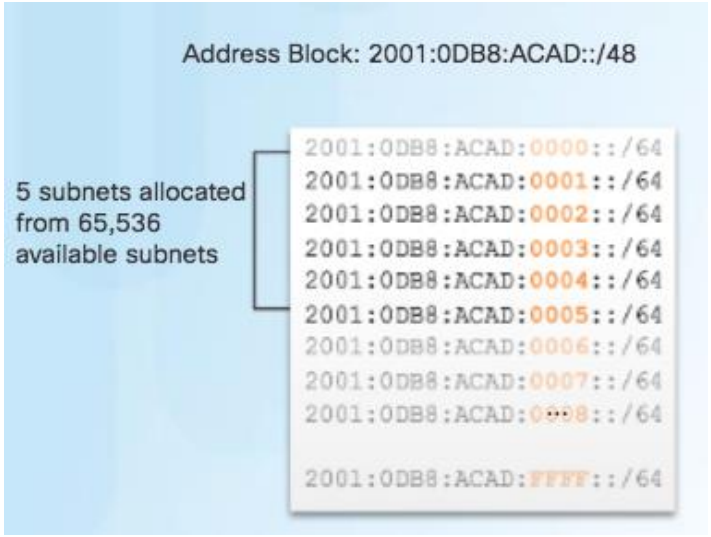
This is the prefix, or network, portion of the address that is assigned by the provider. Typically, Regional Internet Registries (RIRs) assign a /48 global routing prefix to ISPs and customers.

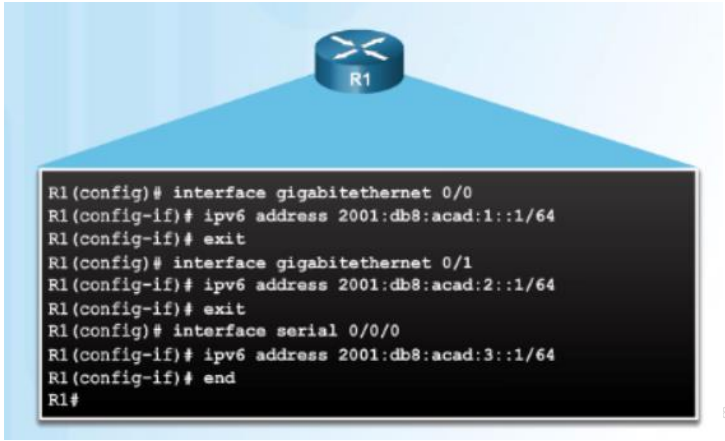
Subnetting Using the Subnet ID



IPv6 Subnet Allocation








CISCO