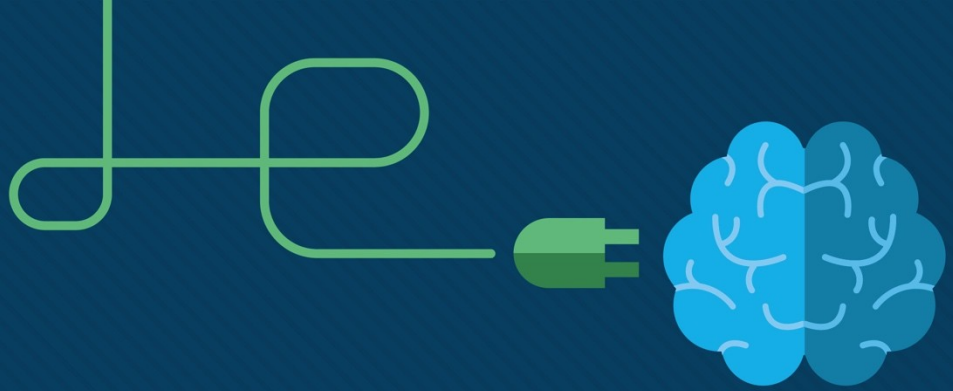


Chapter 1: Routing Concepts

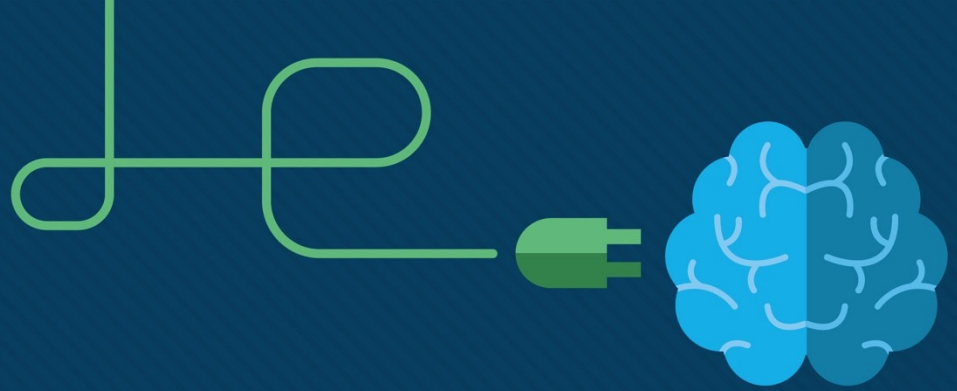
Instructor Materials

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 1: Routing Concepts

Routing and Switching Essentials 6.0 Planning Guide



Chapter 1: Routing Concepts

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 1 - Sections & Objectives

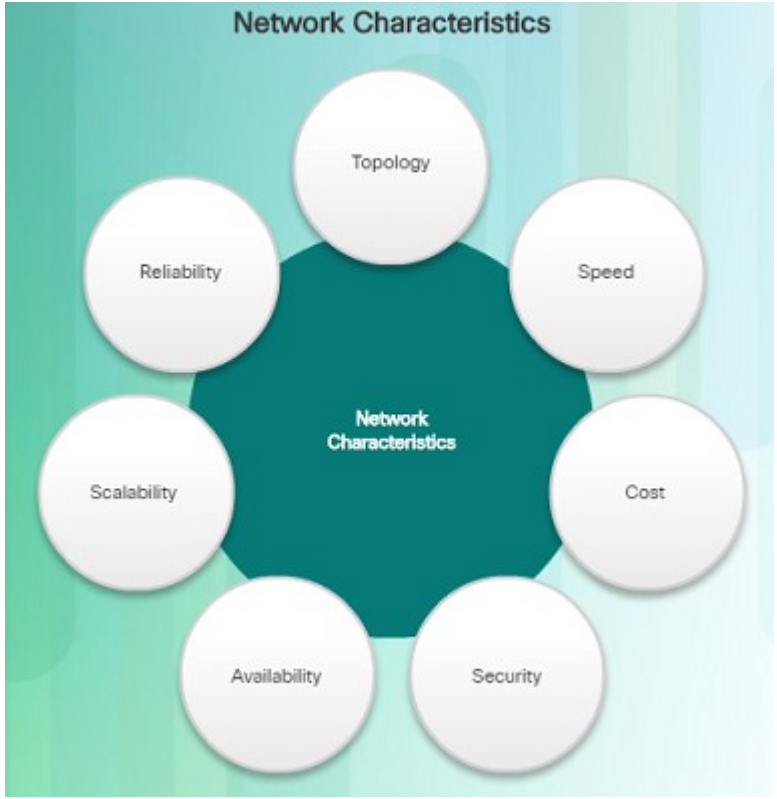
- 1.1 Router Initial Configuration
  - Configure a router to route between multiple directly-connected networks.
    - Describe the primary functions and features of a router.
    - Connect devices for a small, routed network.
    - Configure basic settings on a router to route between two directly-connected networks, using CLI.
    - Verify connectivity between two networks that are directly connected to a router.
- 1.2 Routing Decisions
  - Explain how routers use information in data packets to make forwarding decisions in a small to medium-sized business network.
    - Explain the encapsulation and de-encapsulation process used by routers when switching packets between interfaces.
    - Explain the path determination function of a router.

Chapter 1 - Sections & Objectives

- 1.3 Router Operation
  - Explain how a router learns about remote networks when operating in a small to medium-sized business network.
    - Explain routing table entries for directly connected networks.
    - Explain how a router builds a routing table of directly connected networks.
    - Explain how a router builds a routing table using static routes.
    - Explain how a router builds a routing table using a dynamic routing protocol.

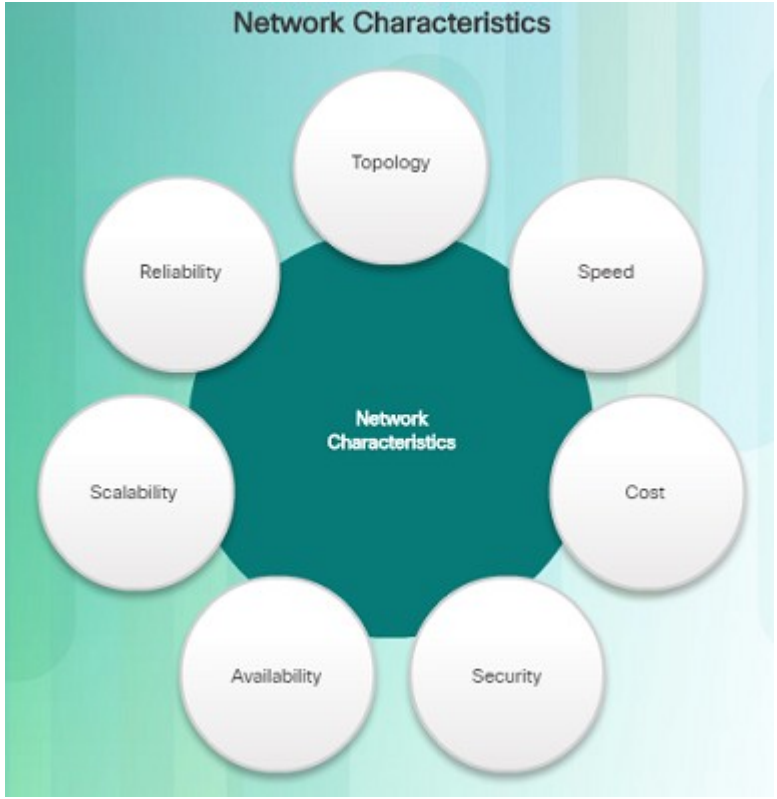
1.1 Router Initial Configuration

Characteristics of a Network



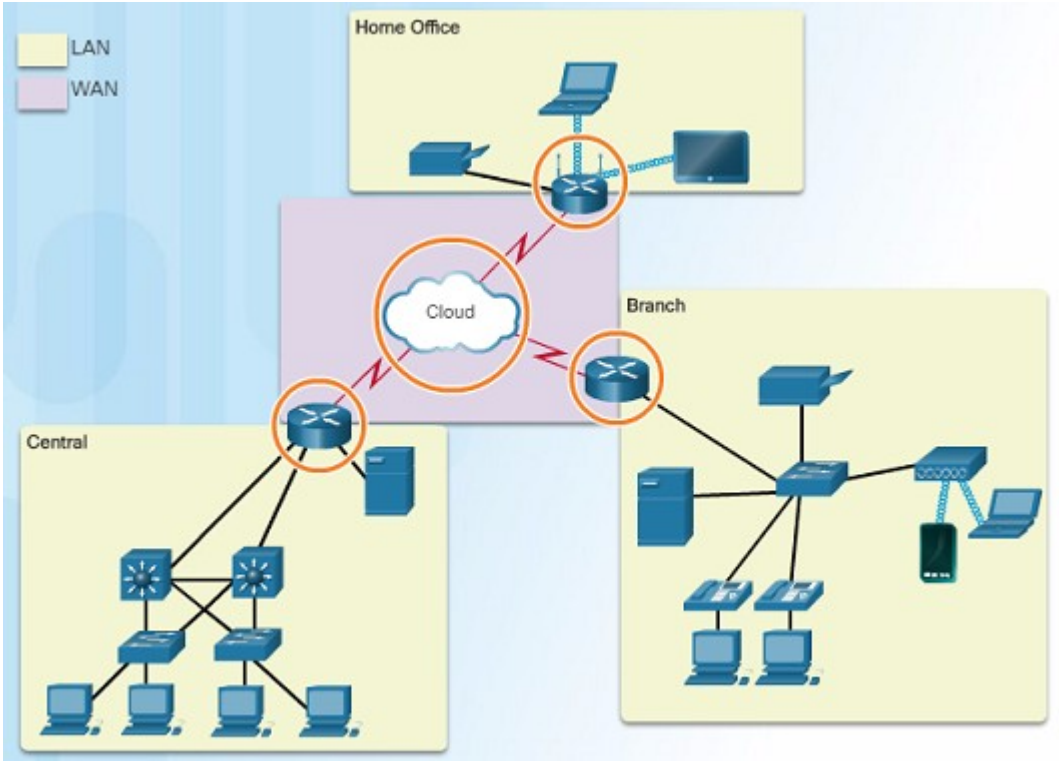
- Networks are relied on for web applications, IP telephony, video conferencing, interactive gaming, e-commerce, and much more.
- Characteristics referred to when discussing networks:
  - Topology
    - Physical topology – arrangement of the cables, network devices, and end systems; it describes how the network devices are actually interconnected with wires and cables
    - Logical topology – describes the path over which the data is transferred in a network and how the network devices appear connected to network users
  - Speed – measure of the data rate in bits per second (b/s) of a given link in the network

Characteristics of a Network (Cont.)



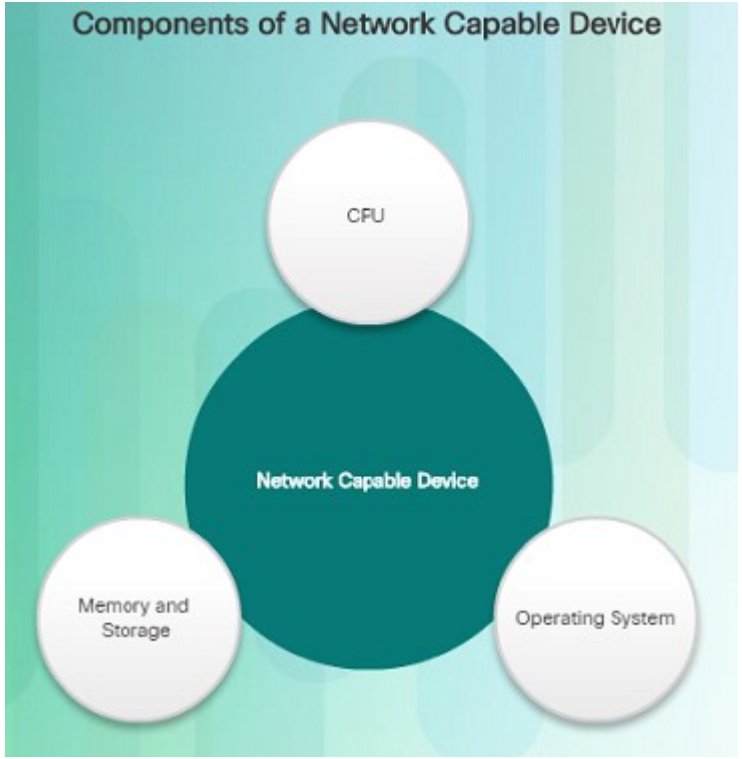
- Cost – general expense for purchasing of network components as well as installation and maintenance of the network
- Security – indicates how protected the network is, including the information that is transmitted over the network
- Availability – refers to the likelihood that the network is available for use when it is required
- Scalability – indicates how easily the network can accommodate more users and data transmission requirements as they increase
- Reliability – indicates the dependability of the components that make up the network including the routers, switches, PCs, and servers; often measured as MTBF (mean time between failures)

Why Routing?



- Router:
  - Connects one network to another network
  - Determines the best route to the destination before forwarding traffic to the next router along the path
  - Responsible for routing traffic between network
  - Routing table used to determine the most efficient path to reach the destination

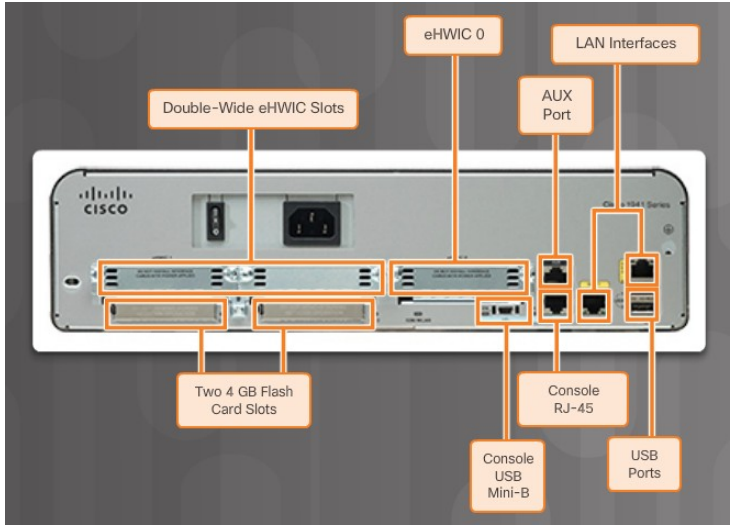
Routers Are Computers



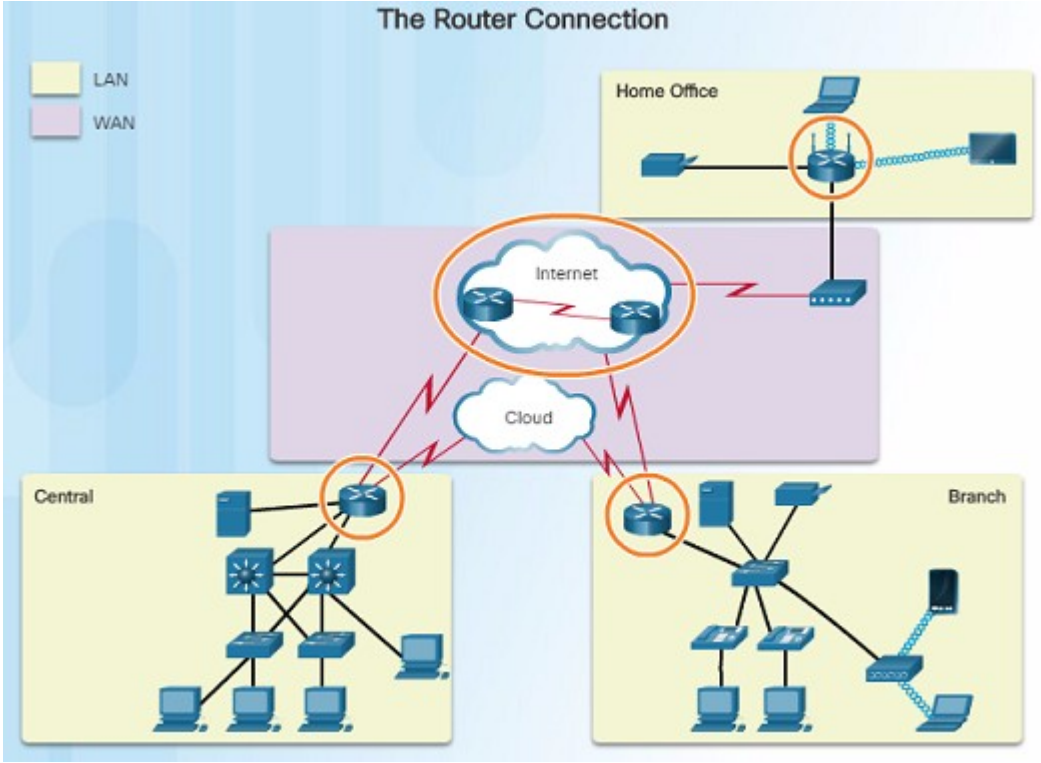
- A router is a specialized computer and requires the same components to operate as computers including:
  - Central Processing Unit (CPU)
  - Operating System (OS)
    - A desktop computer might use the Windows Operating System, but a Cisco Router uses the Cisco Internetwork Operating System (IOS).
  - Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)
    - Non-volatile vs. volatile memory
    - Which one requires constant power to retain content?
- Routers have specialized ports and network interface cards to interconnect devices to other networks

Routers Are Computers (Cont.)

Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage for: • Bootup instructions • Basic diagnostic software • Limited IOS in case the router cannot load the full featured IOS
Non-Volatile Random Access Memory (NVRAM)	Non-volatile memory that provides permanent storage for the: • Startup configuration file
Flash	Non-volatile memory that provides permament storage for: • IOS • Other system-related files

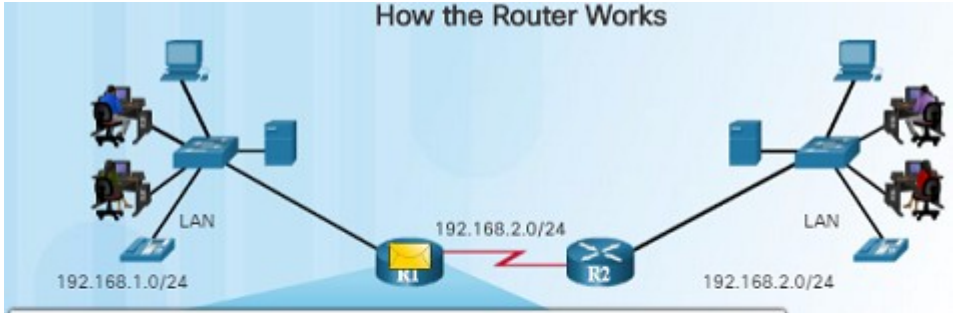


Routers Interconnect Networks



- Router is responsible for forwarding packets from network to network, from the source to the destination
- Multiple networks on a router require multiple interfaces that each belong to a different IP network
  - These interfaces are used to connect:
    - LANs – Ethernet networks that contain PCs, printers, and servers
    - WANs – used to connect networks over large geographical areas such as to an ISP
- When a packet arrives on a router's interface, the router might be the final destination, or it may have to send it to another router to reach its final destination.

Routers Choose Best Paths

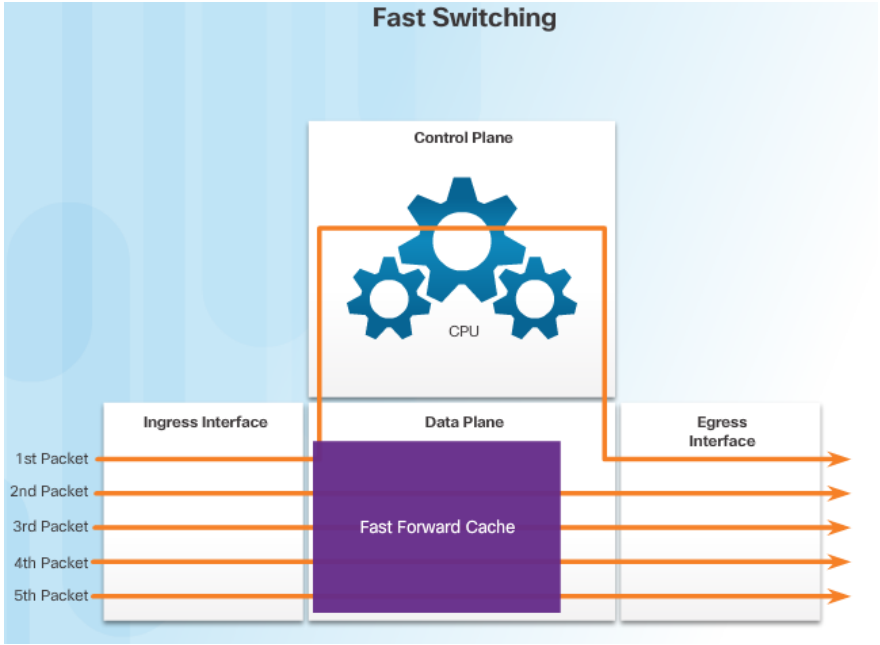



```
R1# show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS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

Gateway of last resort is not set

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

- Routers use the routing table like a map to discover the best path to a given network.

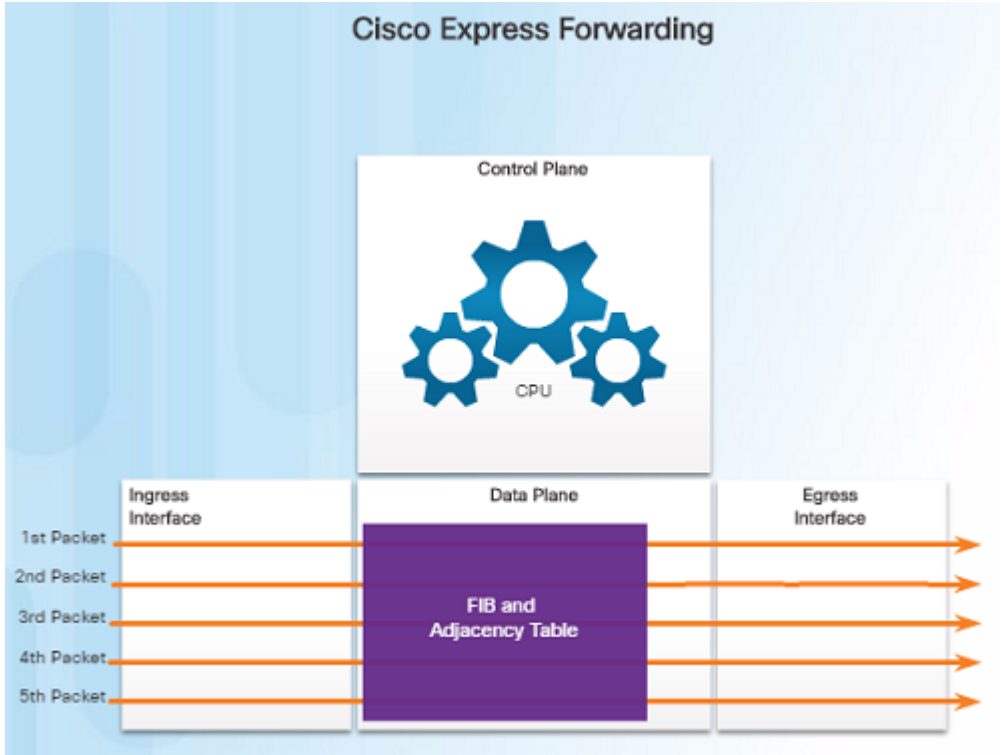
- The primary functions of a router are to:
  - Determine the best path to send packets
  - Forward packets toward their destination
- When a router receives a packet, it examines the destination address of the packet and uses the routing table to look for the best path to that network.
  - When a match is found, the router encapsulates the packet into the data link frame of the outgoing exit interface and then forwards the packet out that interface to its destination.
- A router can handle different data link layer frame encapsulations.
  - The router might receive a frame from its Ethernet interface. It will have to de-encapsulate the packet to search the routing table for a matching network. Once it finds a match, it will encapsulate it inside of the corresponding frame required for the outgoing interface, such as a PPP frame.

Packet Forwarding Mechanisms



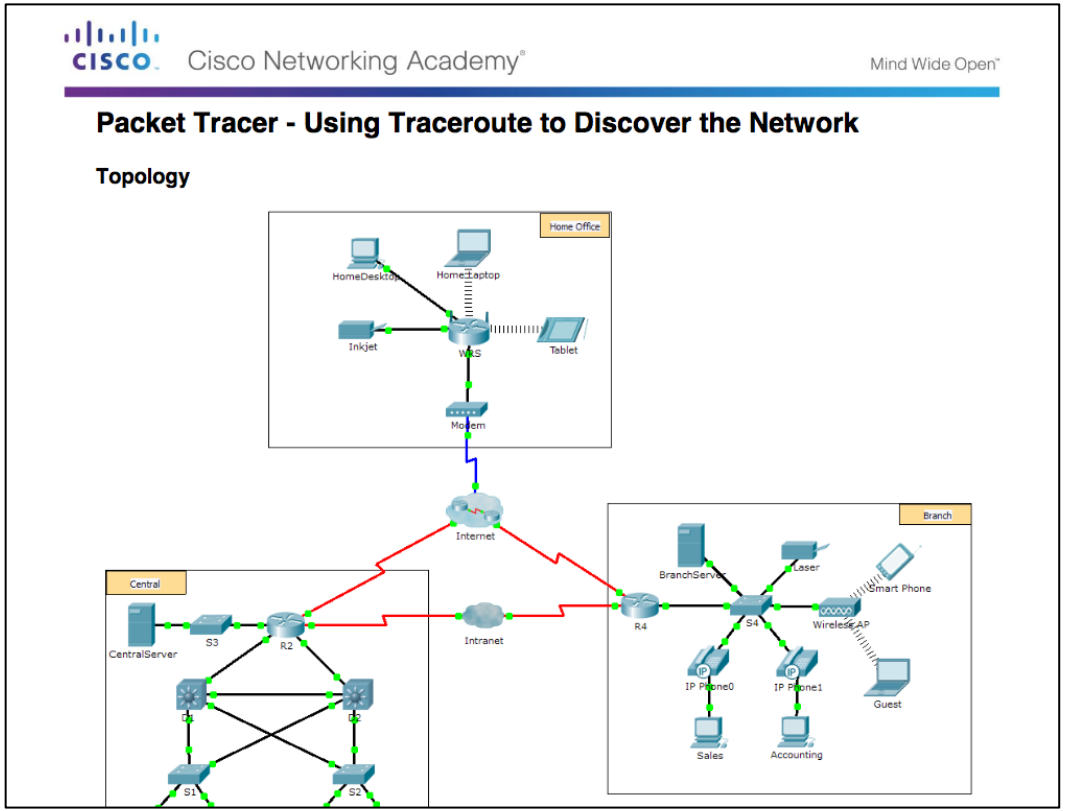
- Routers support three packet-forwarding mechanisms:
  - Process switching –
    - Slower and older packet forwarding mechanism
    - Packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table in order to determine the exit interface
    - Slow because it does this for every packet in a stream
  - Fast Switching –
    - Common packet forwarding mechanism which uses a fast-switching cache to store the next-hop information
    - Packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache
    - If no match, it is process-switched and forwarded to the exit interface
    - Packet flow information stored in the fast-switching cache for quick lookup

Packet Forwarding Mechanisms (Cont.)

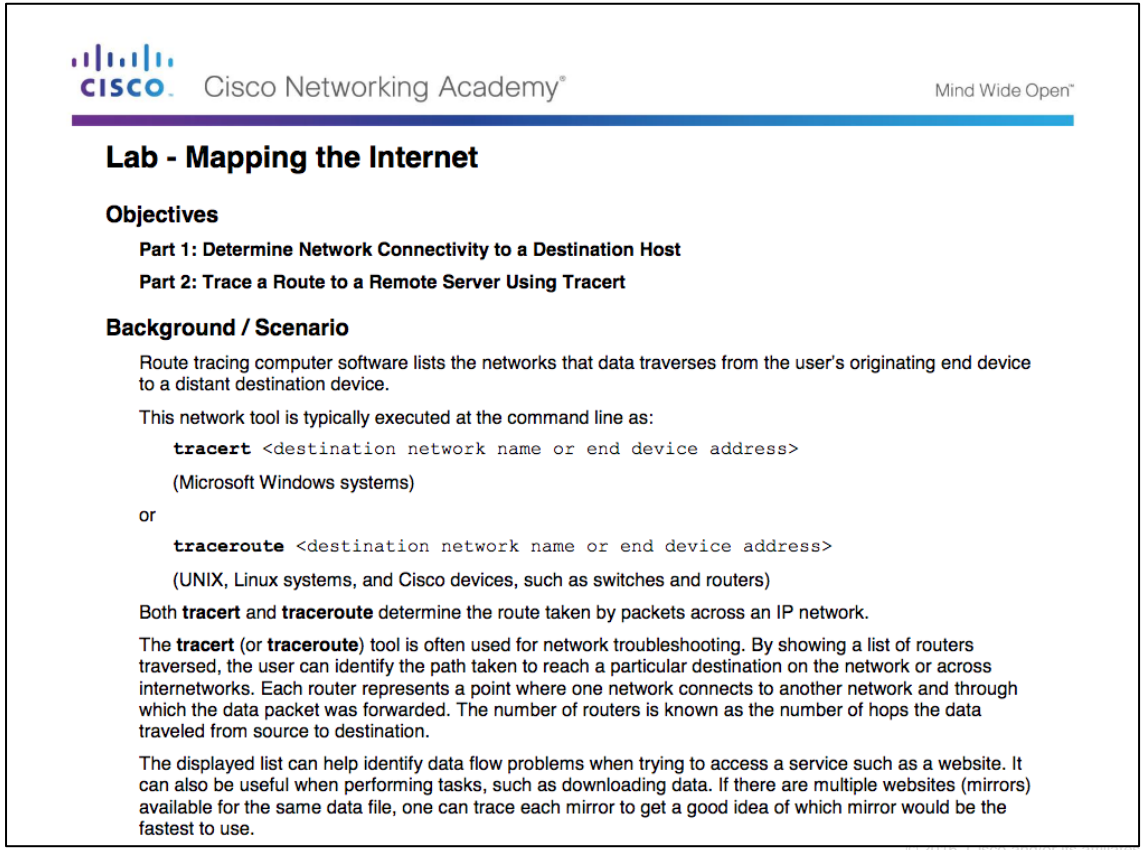


- Cisco Express Forwarding – CEF
  - Fastest, most recent, and preferred packet-forwarding mechanism
  - CEF builds a Forwarding Information Base (FIB) and an adjacency table
  - Table entries are not packet-triggered like fast switching, but change-triggered when something changes in the network topology
  - When a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet
  - FIB contains pre-computed reverse lookups, next hop information for routes including the interface and Layer 2 information

Packet Tracer – Using Traceroute to Discover the Network



Lab – Mapping the Internet



Cisco Networking Academy® Mind Wide Open™

Lab - Mapping the Internet

Objectives

Part 1: Determine Network Connectivity to a Destination Host

Part 2: Trace a Route to a Remote Server Using Tracert

Background / Scenario

Route tracing computer software lists the networks that data traverses from the user's originating end device to a distant destination device.

This network tool is typically executed at the command line as:

tracert <destination network name or end device address>

(Microsoft Windows systems)

or

traceroute <destination network name or end device address>

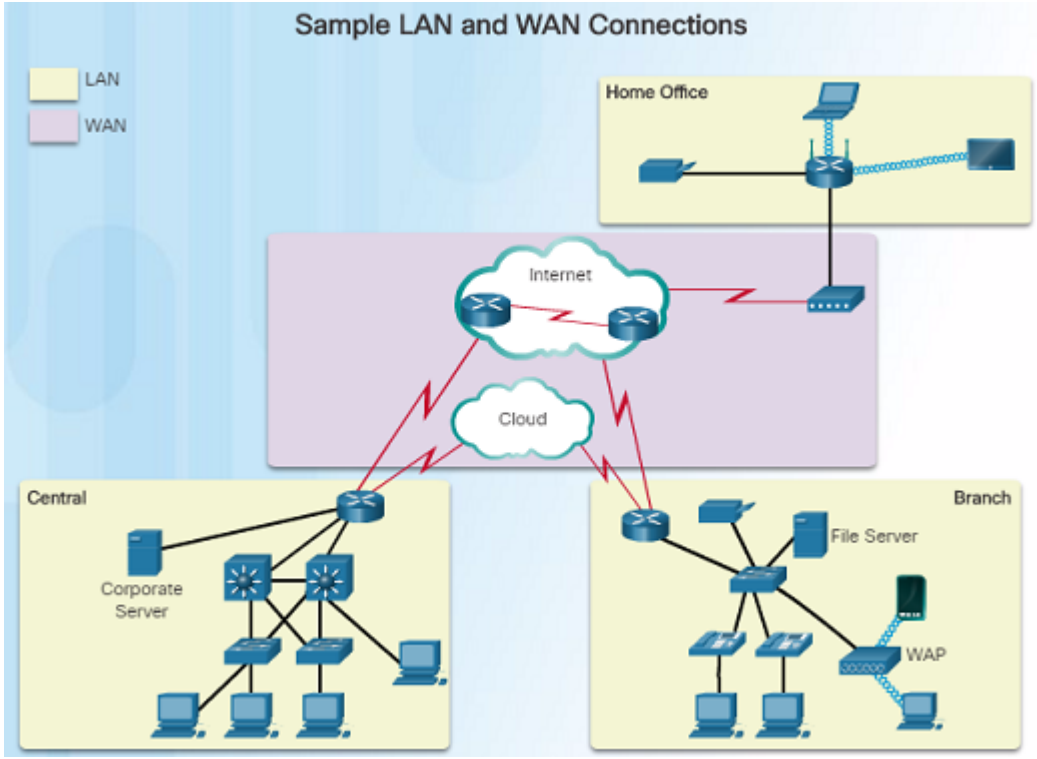
(UNIX, Linux systems, and Cisco devices, such as switches and routers)

Both **tracert** and **traceroute** determine the route taken by packets across an IP network.

The **tracert** (or **traceroute**) tool is often used for network troubleshooting. By showing a list of routers traversed, the user can identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of hops the data traveled from source to destination.

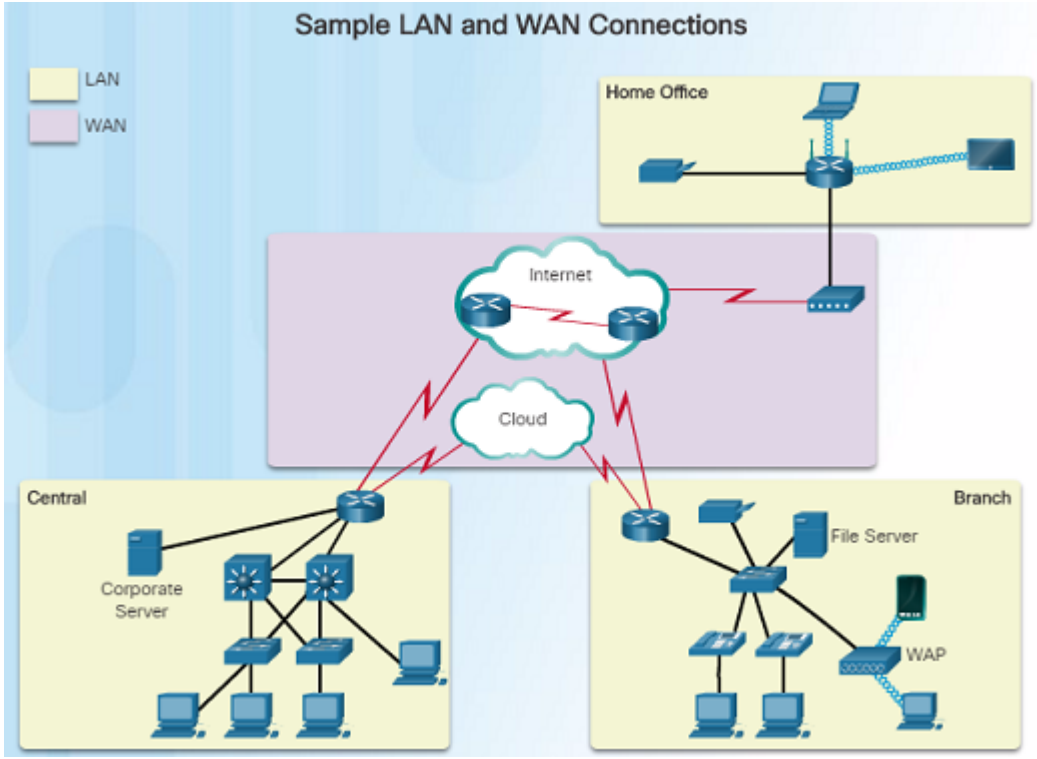
The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks, such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Connect to a Network



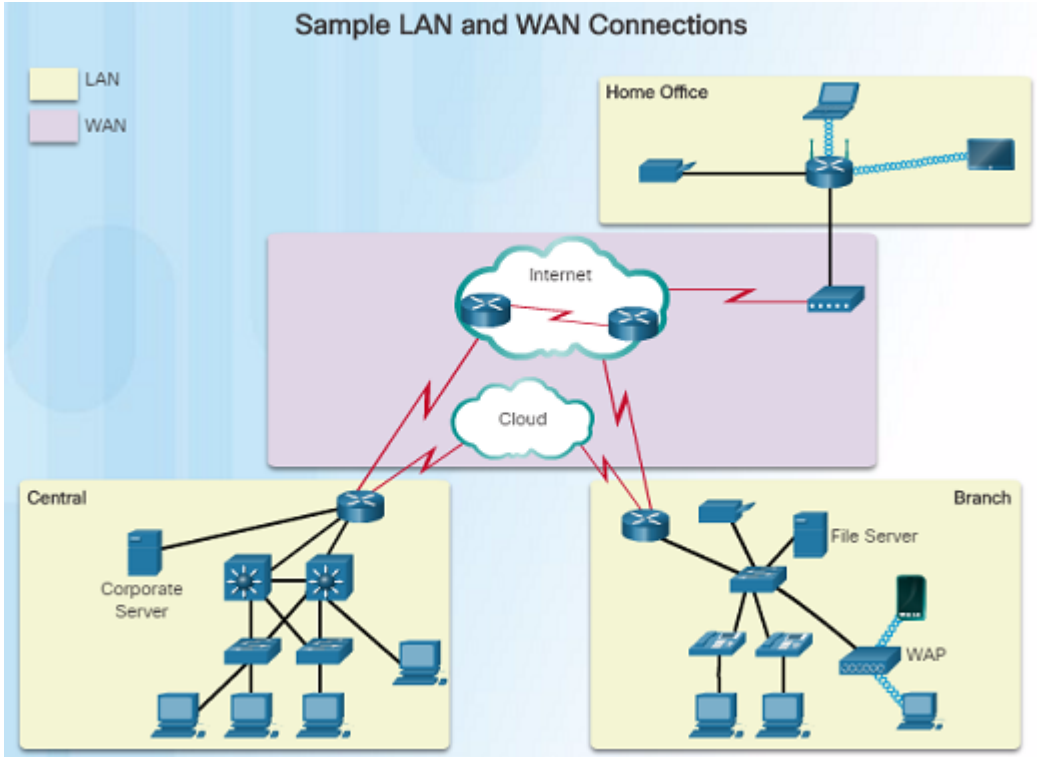
- Home Office devices might connect as follows:
  - Laptops and tablets connect wirelessly to a home router.
  - A network printer connects using an Ethernet cable to the switch port on the home router
  - The home router connects to the Internet service provider cable modem using an Ethernet cable.
  - The cable modem connects to the ISP network.

Connect to a Network (Cont.)



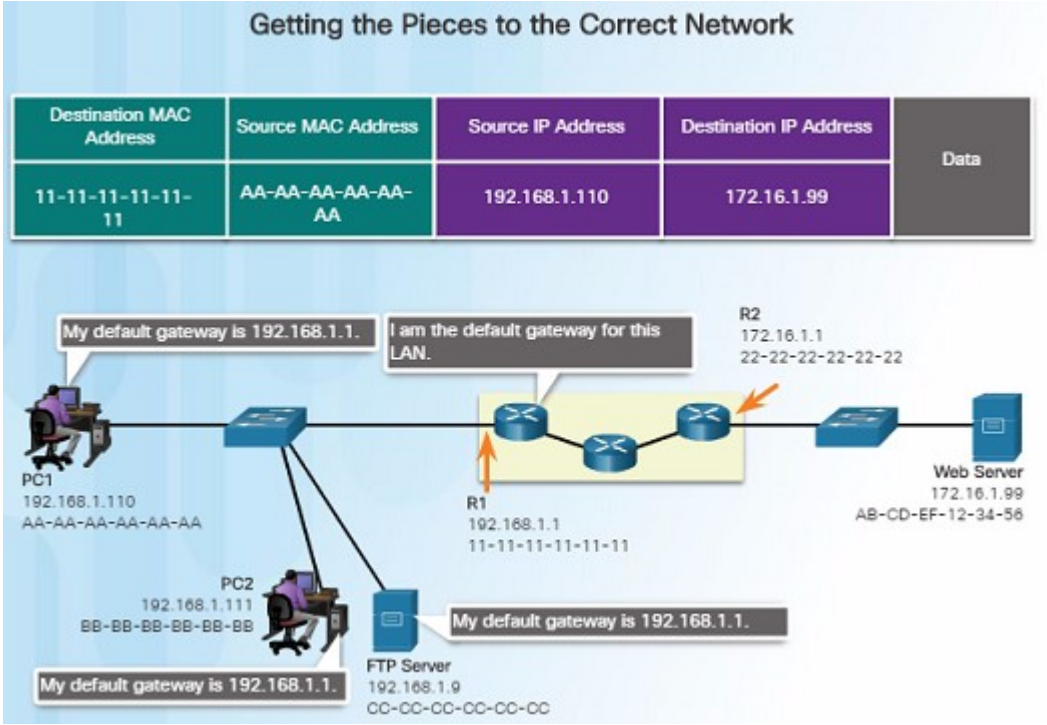
- Branch site devices might connect as follows:
  - Desktop PCs, VoIP phones, and corporate resources such as file servers and printers connect to Layer 2 switches using Ethernet cables.
  - Laptops and smartphones connect wirelessly to wireless access points (WAPs).
  - The WAPs connect to switches using Ethernet cables.
  - Layer 2 switches connect to an Ethernet interface on the edge router using Ethernet cables.
  - The edge router connects to a WAN service provider.

Connect to a Network (Cont.)



- Central site devices might connect as follows:
  - Desktop PCs and VoIP phones connect to Layer 2 switches using Ethernet cables.
  - Layer 2 switches connect redundantly to multilayer Layer 3 switches using Ethernet fiber-optic cables.
  - Layer 3 multilayer switches connect to an Ethernet interface on the edge router using Ethernet cables.
  - The corporate website server connects to the edge router interface.
  - The edge router connects to a WAN SP and also to an ISP for backup purposes.

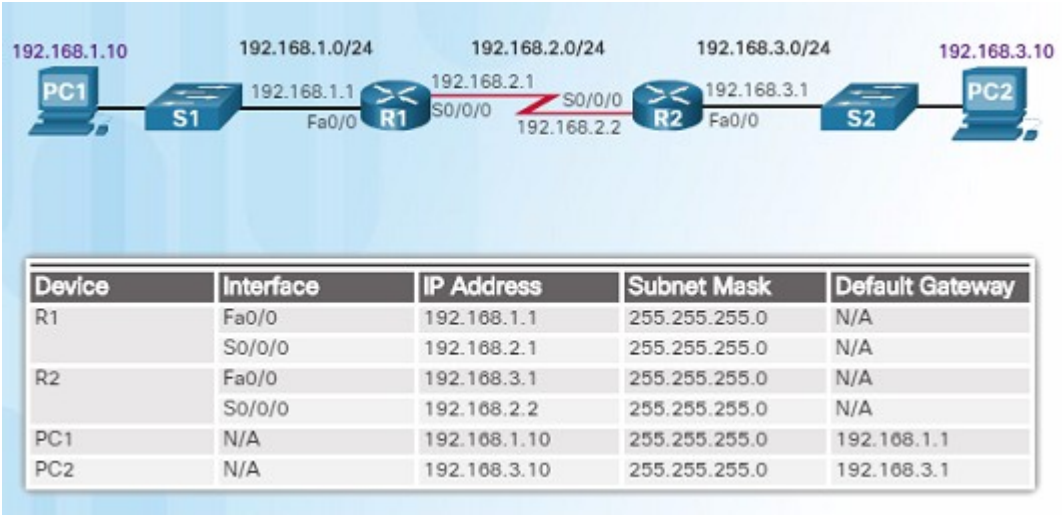
Default Gateways



- Routers are also usually configured with their own default gateway.

- Devices need the following information for network access: IP address, subnet mask, and default gateway.
- When a host sends a packet to a device that is on the same IP network, the packet is forwarded out the host interface to the destination device. The router does not need to get involved.
- When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because the host device cannot communicate with devices outside of the local network.
- The default gateway is the device that routes traffic from the local network to devices on remote networks, such as devices on the Internet.

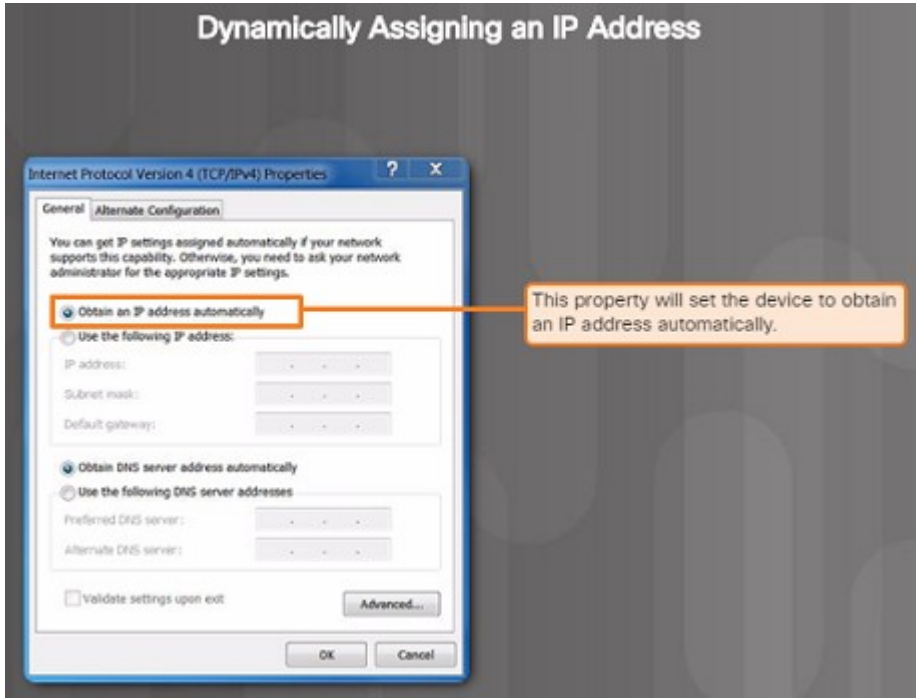
Document Network Addressing



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

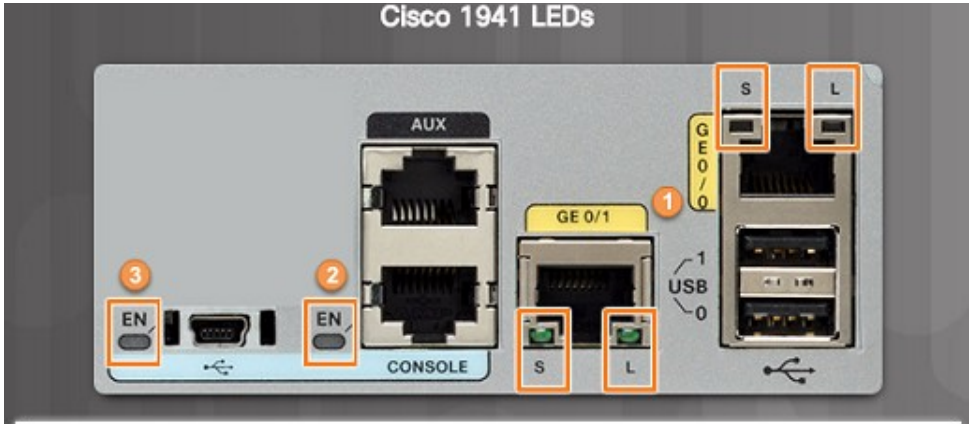
- When designing a new network or mapping an existing one, the documentation should identify:
  - Device names
  - Interfaces used in the design
  - IP addresses and subnet masks
  - Default gateway addresses
- The figure in the left shows two useful documents:
  - Topology diagram – provides a visual reference that indicates the physical and logical Layer 3 addressing.
  - An addressing table – captures device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses.

Enable IP on a Host



- A host can be assigned IP address information either:
  - Statically –
    - Manually configure the IP address, subnet mask, default gateway and probably the DNS server IP address.
    - Servers and printers commonly use static address assignment.
  - Dynamically –
    - IP address information is obtained from a Dynamic Host Configuration Protocol (DHCP) server.
    - DHCP server provides an IP address, subnet mask, default gateway and probably the DNS server information.
    - Most host devices uses DHCP.

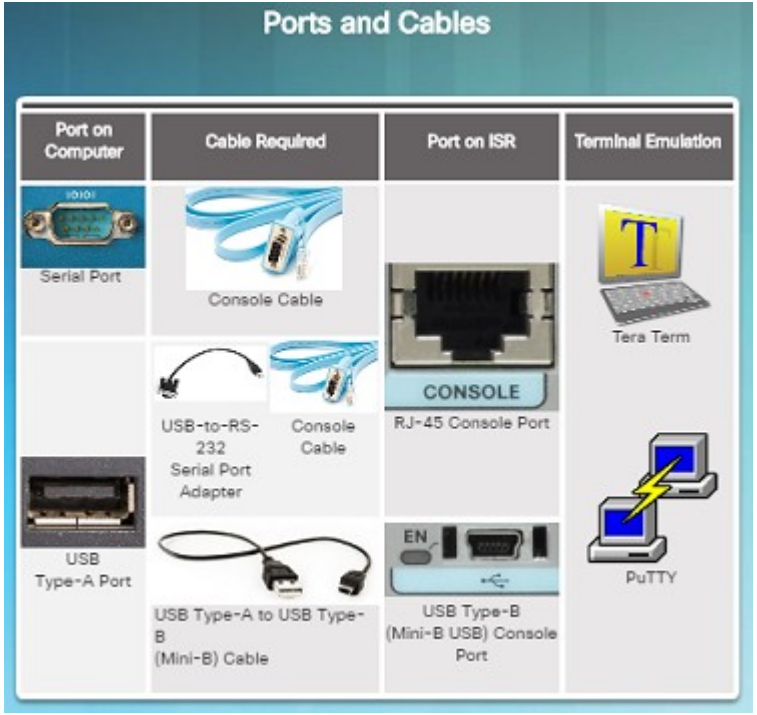
Device LEDs



#	Port	LED	Color	Description
1	GE0/0 and GE0/1	S (Speed)	1 blink + pause	Port operating at 10 Mb/s
			2 blink + pause	Port operating at 100 Mb/s
			3 blink + pause	Port operating at 1000 Mb/s
		L (Link)	Green	Link is active
			Off	Link is inactive
2	Console	EN	Green	Port is active
			Off	Port is inactive
3	USB	EN	Green	Port is active
			Off	Port is inactive

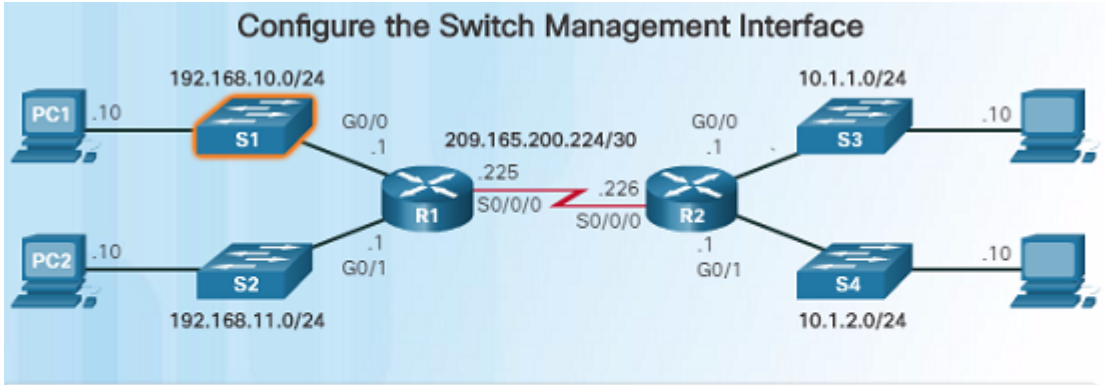
- Host computers connect to a wired network using a RJ-45 Ethernet cable.
- Most network interface cards have one or two LED indicators next to the interface.
  - Green LED indicates a good connection.
  - A blinking green indicates network activity.
  - No light indicates a problem with either the network cable or the network itself.
- Network infrastructure devices also use LEDs to provide a quick status view. For example, a Cisco Catalyst 2960 switch:
  - Green LEDs indicate a switch is functioning normally.
  - Amber LEDs indicate a malfunction.
- Cisco routers also use various LED indicators to provide status information.

Console Access



- Devices including routers and switches are commonly accessed using Secure Shell (SSH) or HyperText Transfer Protocol Secure (HTTPS).
- Console access is usually only required when initially configuring a device, or if remote access fails.
- Console access requires:
  - Console cable – RJ-45 to DB-9 serial cable or a USB serial cable.
  - Terminal emulation software – Tera Term, PuTTY, or HyperTerminal
- Cable is connected between the serial port of the host and the console port on the device.
  - If a host does not have a serial port, use the USB port and a USB-to-RS-232 adapter.

Enable IP on a Switch




```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.10.2 255.255.255.0
S1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
S1(config-if)# exit
S1(config)#
S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

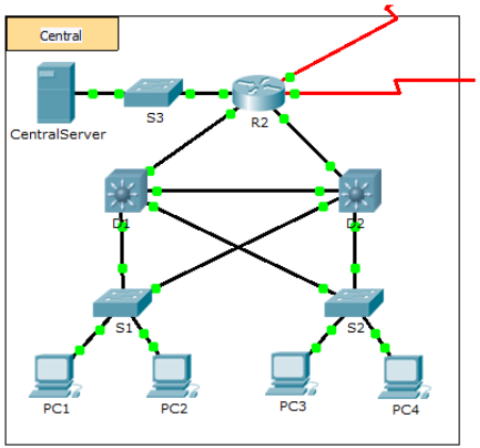
- Network devices require IP addresses in order for the network administrator to connect to the devices using Telnet, SSH, HTTP, or HTTPS.
- A switch requires an IP address to be configured on a virtual interface, called the switched virtual interface (SVI).
- Commands in the figure to the left should be used to configure the IP address on vlan 1 and also the default-gateway information.

Packet Tracer – Documenting the Network

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Documenting the Network

Topology

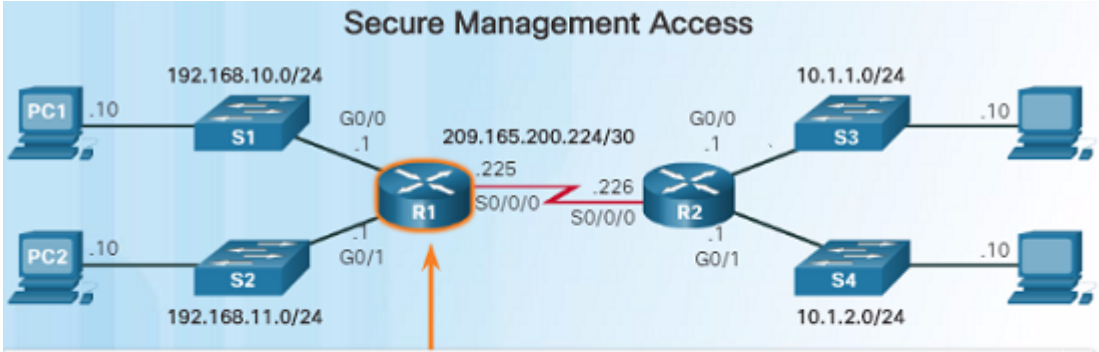


Background

In this activity, your job is to document the addressing scheme and connections used in the Central portion of the network. You must use a variety of commands to gather the required information.

Note: The user EXEC password is **cisco**. The privileged EXEC password is **class**.

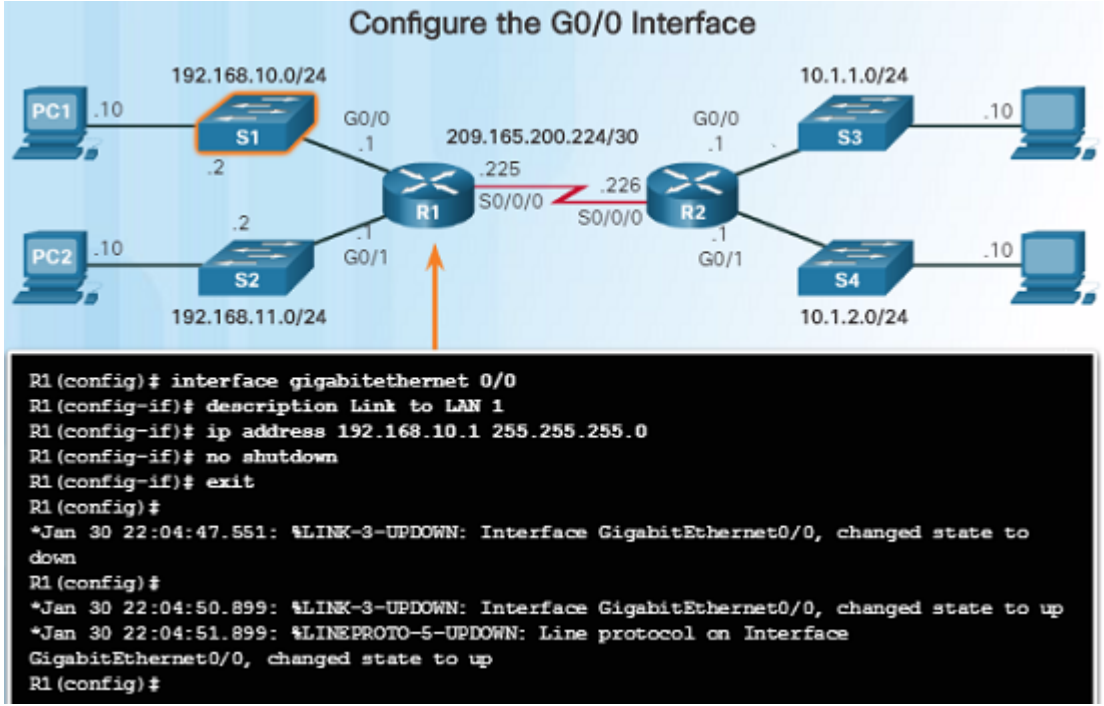
Configure Basic Router Settings




```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

- Cisco routers and switches have similar initial configuration steps:
  - Name the device in order to distinguish it from other devices in the network using the **hostname** command in global config mode.
  - Secure management access as shown in the figure to the left in order to secure privileged EXEC, user EXEC, and remote access.
  - Configure a banner to provide legal notification of unauthorized access in global config mode: **banner motd ** Authorized Access Only! ****
- Always save your configuration changes and verify your settings: **R1# copy running-config startup-config**

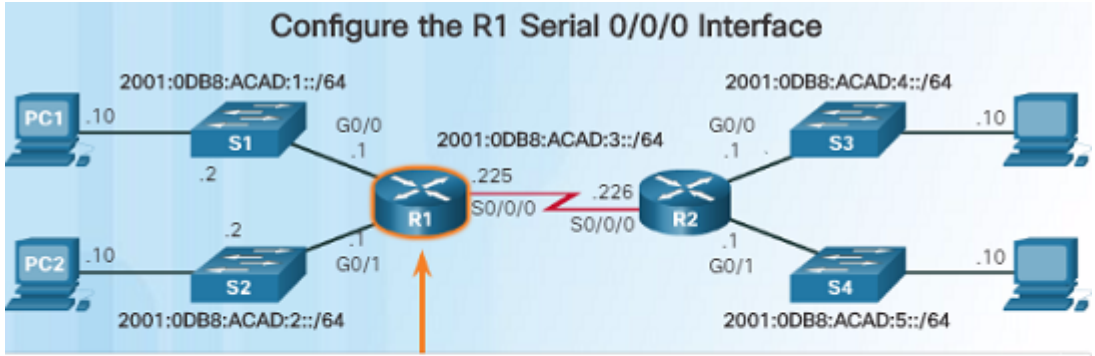
Configure an IPv4 Router Interface



- Layer 2 switches support LANs and have multiple FastEthernet or Gigabit Ethernet ports.
- Routers support LANs and WANs and have many types of interfaces including Gigabit Ethernet and High-Speed WAN Interface Card (HWIC) slots to support WAN connections.
- As shown in the figure to the left, an interface must be configured with an IP address, subnet mask, and activated with the **no shutdown** command.

Note: In a lab environment, the serial interface with the cable end labeled DCE needs to be configured with a **clock rate** command.

Configure an IPv6 Router Interface

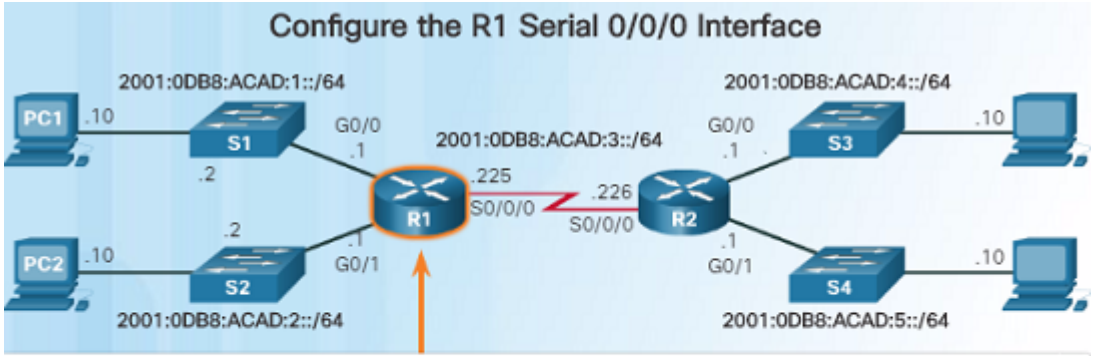



```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#
*Feb  3 21:39:43.307: %LINK-3-UPDOWN: Interface
Serial0/0/0, changed state to down
R1(config-if)#
```

- The **clock rate 128000** command was used since this is being configured in a lab environment.

- To configure host PC1, statically assign an IPv6 address to the host under Internet Control Protocol Version 6 (TCP/IPv6) Properties.
- Configuring an IPv6 interface is very similar to configuring an IPv4 interface, use the **ipv6 address** command.
- As shown in the figure, configure the interface with an IPv6 address and subnet mask prefix.
- Activate the interface with the **no shutdown** command.
- An interface can generate its own IPv6 link-local address without having a global unicast address by using the **ipv6 enable** interface config command.

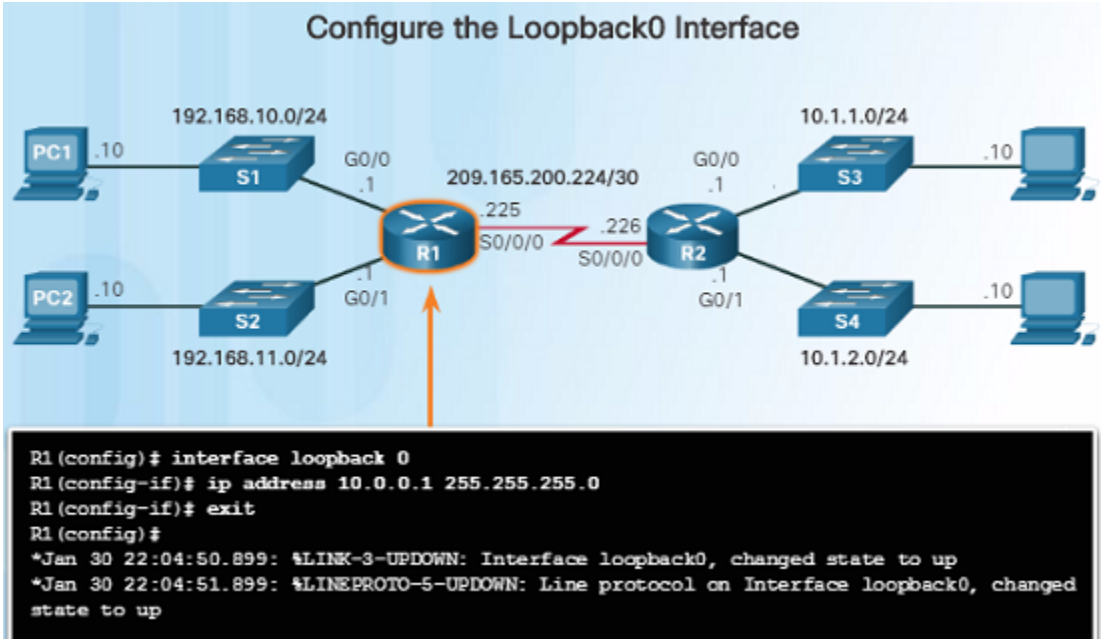
Configure an IPv6 Router Interface (Cont.)




```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#
*Feb  3 21:39:43.307: %LINK-3-UPDOWN: Interface
Serial0/0/0, changed state to down
R1(config-if)#
```

- Unlike IPv4, IPv6 interfaces will typically have more than one IPv6 address.
- An IPv6 device must have an IPv6 link-local address but will most likely also have an IPv6 global unicast address.
- An interface can also have multiple IPv6 global unicast addresses from the same subnet.
- These commands can be used to create a global unicast or link-local IPv6 address:
  - **ipv6 address** ipv6-address/prefix-length
  - **ipv6 address** ipv6-address/prefix-length **eui-64**
  - **ipv6 address** ipv6-address/prefix-length **link-local**

Configure an IPv4 Loopback Interface



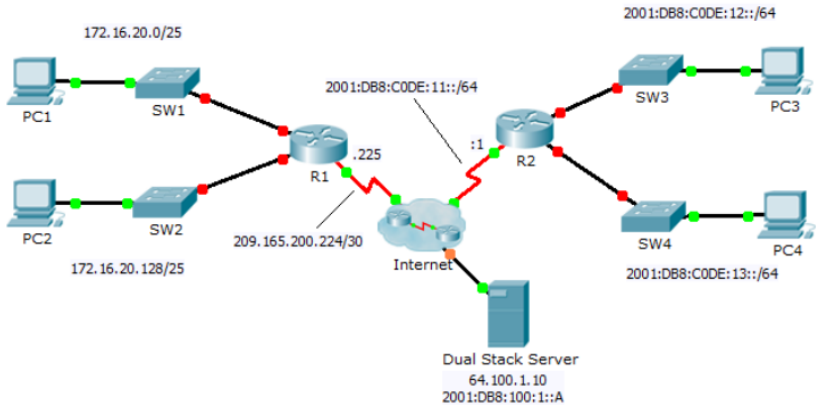
- An IPv4 loopback interface is typically configured on a router for testing and management purposes.
- A loopback interface is a logical interface internal to the router.
  - It is not assigned to a physical port and can not be connected to any other device.
  - It is a software interface that is automatically placed in an “up” state as long as the router is functioning.
- Some routing protocols such as OSPF require an address for identification, the loopback address can be used rather than an interface address which might go down on occasion, disrupting OSPF routing.

Packet Tracer – Configuring IPv4 and IPv6 Interfaces

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Configuring IPv4 and IPv6 Interfaces

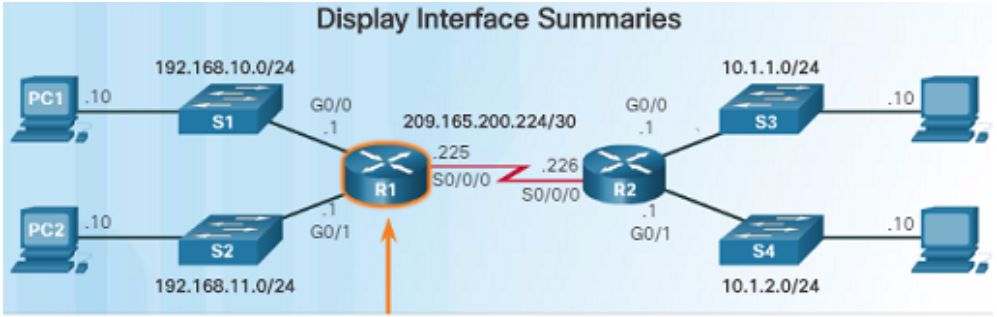
Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
	G0/0	172.16.20.1	255.255.255.128	N/A

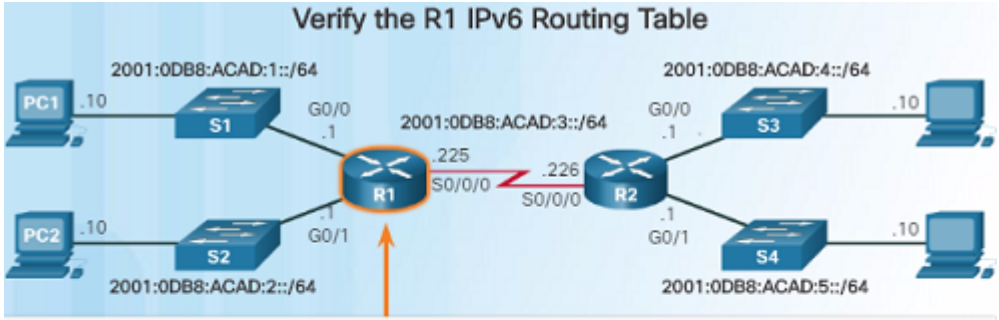
Verify Interface Settings




```
R1# show ip interfaces brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         192.168.11.1    YES manual up                    up
Serial0/0/0                209.165.200.225 YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
R1#
```

- The following commands are used to verify the operation and configuration of an interface:
  - **show ip interface brief** – Displays a summary for all interfaces including the IPv4 address of the interface as well as the current operational status.
  - **show ip route** – Displays the contents of the IPv4 routing table.
  - **show running-config interface** *interface-id* – Displays the commands configured on the specified interface.
- The following commands can be used to gather more detailed interface information:
  - **show interfaces** – Displays interface information and packet flow counts.
  - **show ip interface** – Displays the IPv4 related information for all interfaces on a router.

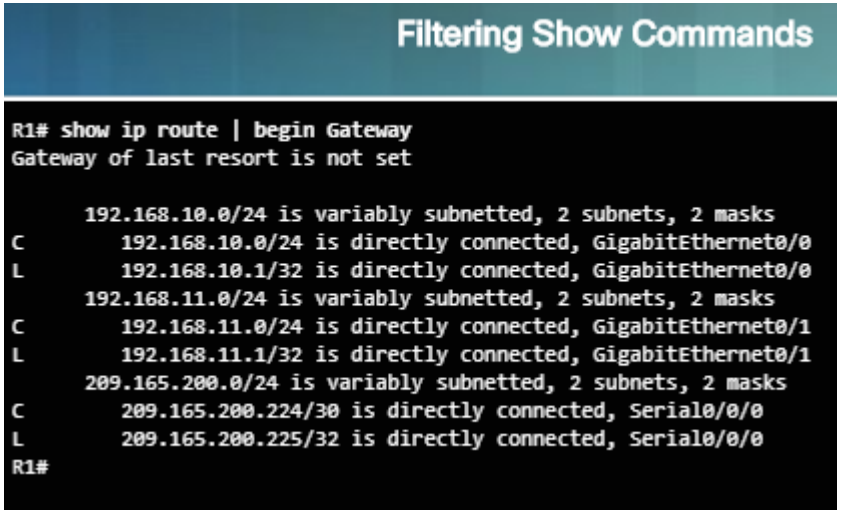
Verify IPv6 Interface Settings




```
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
```

- IPv6 commands used for interface configuration verification are similar to IPv4.
  - **show ipv6 interface brief** – If the output shows up/up, this shows that Layers 1 and 2 are operational
  - **show ipv6 interface** *interface-id* – Shows the interface status and all of the IPv6 addresses that belong to the interface.
  - **show ipv6 route** – Verifies that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table.
- As shown in the figure to the left, a ‘C’ next to a route indicates that this is a directly connected network.
  - When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix length is added to the IPv6 routing table as a connected route.

Filter Show Command Output



- Commands that generate multiple screens of output are, by default, paused after 24 lines.
  - The spacebar allows you to see the next set of lines, while the ENTER key will display the next line.
  - Use the terminal length command to change the number of lines to be displayed.
- Another useful feature that makes it easier to view show output is by filtering the output. To enable the filtering command, use the pipe character, "|". For example:
  - **show running-config | section line con** – shows the section that starts with "line con"
  - **show ip interface brief | include down** – includes all output that matches "down"
  - **show ip interface brief | exclude up** – "excludes all output that matches up"
  - **show running-config | begin line** – shows all the remaining output starting with "line"

Command History Feature

```
Enter the command to set the number of lines in command history to 200.
R1# terminal history size 200

Enter the command to display command history.
R1# show history
  show ip interface brief
  show interface g0/0
  show ip interface g0/1
  show ip route
  show ip route 209.165.200.224
  show running-config interface s0/0/0
  terminal history size 200
  show history
R1#

You successfully set and displayed command history.
```

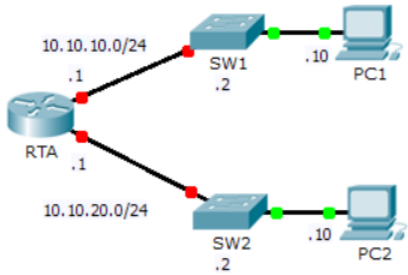
- The command history feature shows previously executed commands when recalled.
- Press **Ctrl+P** or the **Up Arrow** key to recall commands in the history buffer.
  - The most recent commands are displayed first
  - Keep pressing Up Arrow to recall the commands in the history buffer.
- By default, command history is enabled and the last 10 commands are stored in the history buffer.
- Use the **terminal history size** user EXEC command to change this number.
- Use the **show history** privileged EXEC command to display the contents of the buffer.

Packet Tracer – Configuring and Verifying a Small Network

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Configuring and Verifying a Small Network

Topology



Addressing Table

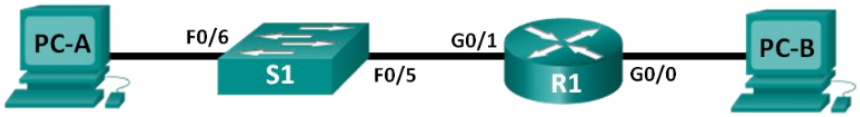
Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
	G0/1	10.10.20.1	255.255.255.0	N/A
SW1	VLAN1	10.10.10.2	255.255.255.0	10.10.10.1
SW2	VLAN1	10.10.20.2	255.255.255.0	10.10.20.1
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.1

Lab – Configuring Basic Router Settings with IOS CLI

Cisco Networking Academy® Mind Wide Open™

Lab – Configuring Basic Router Settings with IOS CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

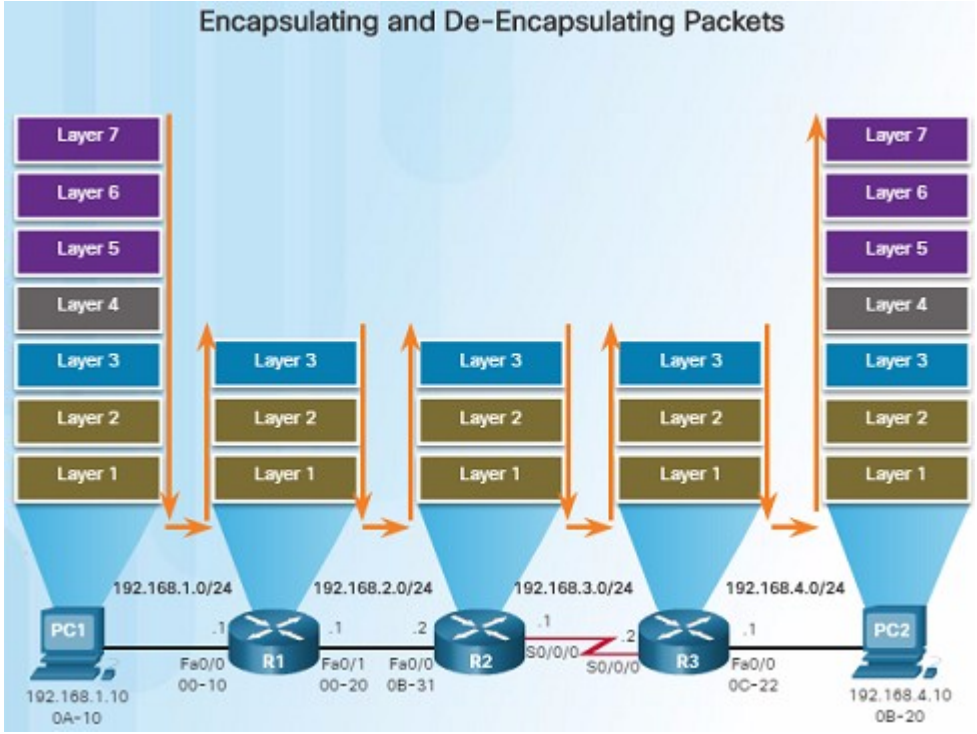
- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 information to the PC interfaces.

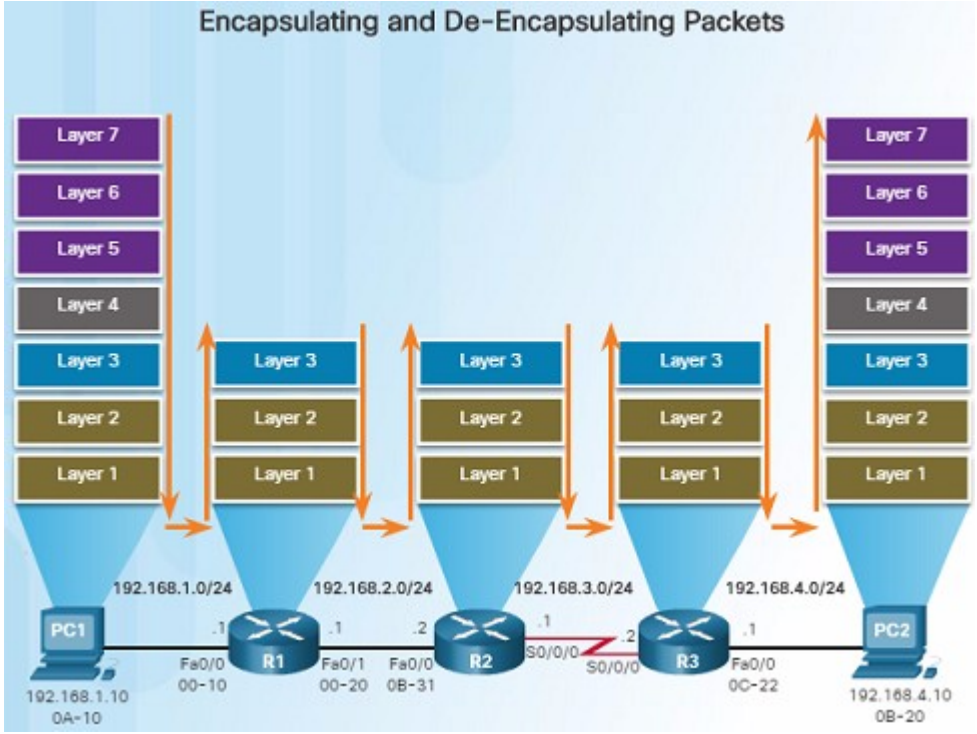
1.2 Routing Decisions

Router Switching Function



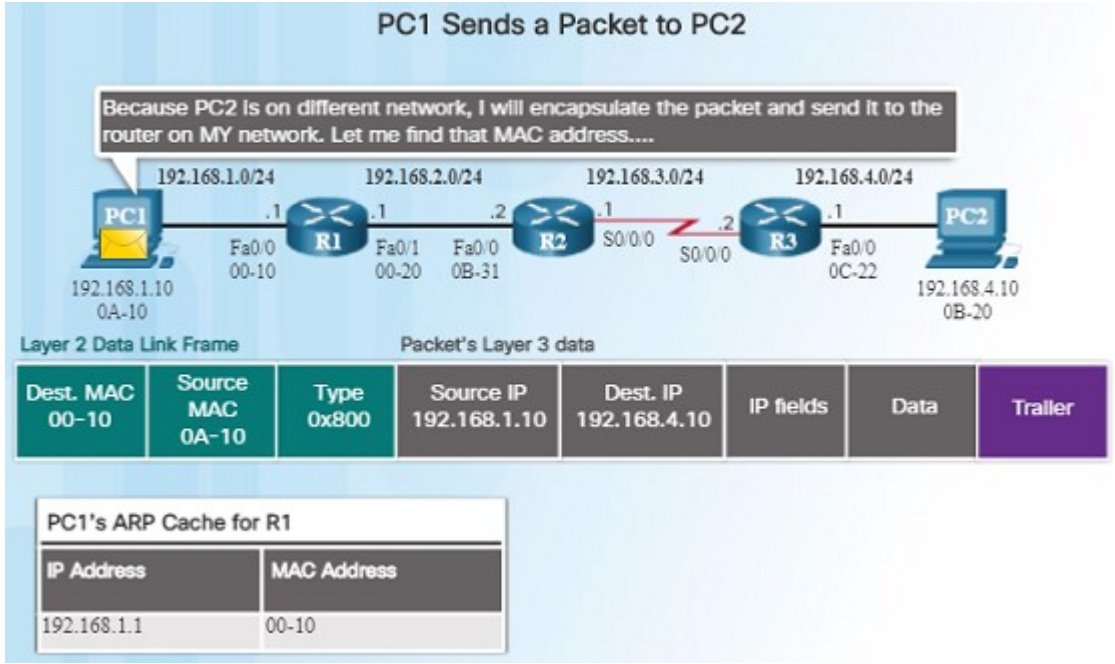
- The primary function of a router is to forward packets toward their destination.
  - Uses a switching function which is a process that accepts a packet on one interface and forwards it out of another interface. This is not to be confused with the function of a Layer 2 switch.
  - The switching function also encapsulates the packets in the appropriate data link frame type for the outgoing interface.

Router Switching Function (Cont.)



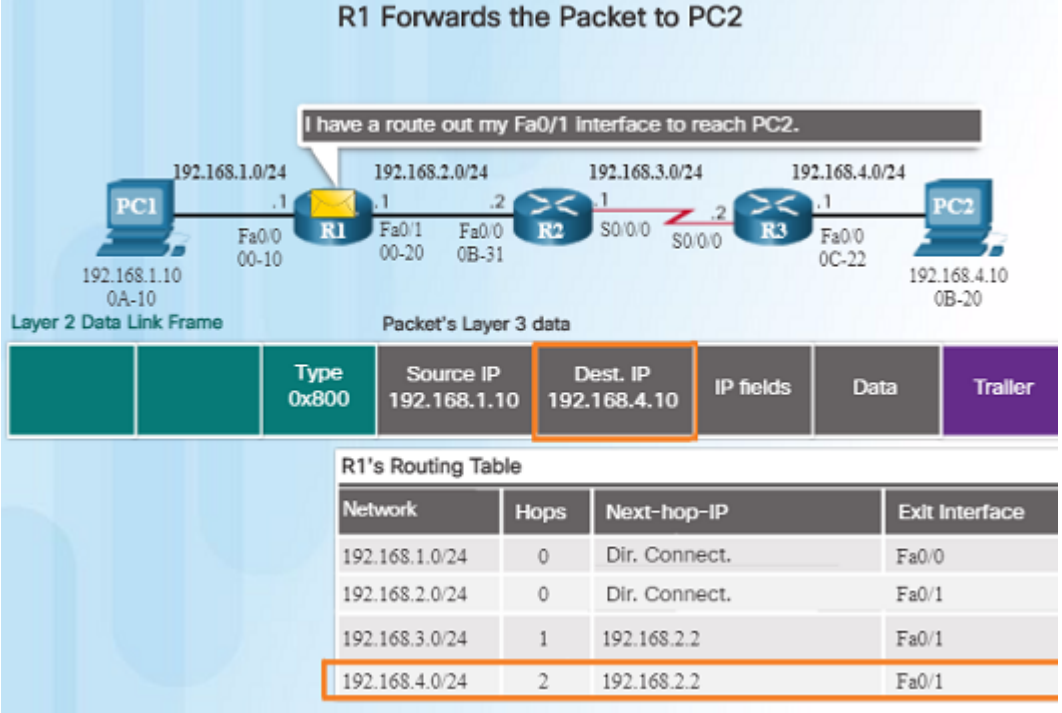
- When a router receives a packet from one network that is destined for another network, the router performs the following three steps:
  - Step 1. De-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet.
  - Step 2. Examines the destination IP address of the IP packet to find the best path in the routing table.
  - Step 3. If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface.
- As a packet travels from the source device to the destination device, the Layer 3 IP addresses do not change. However, the Layer 2 data link addresses change at every hop as it is de-encapsulated and re-encapsulated.

Send a Packet



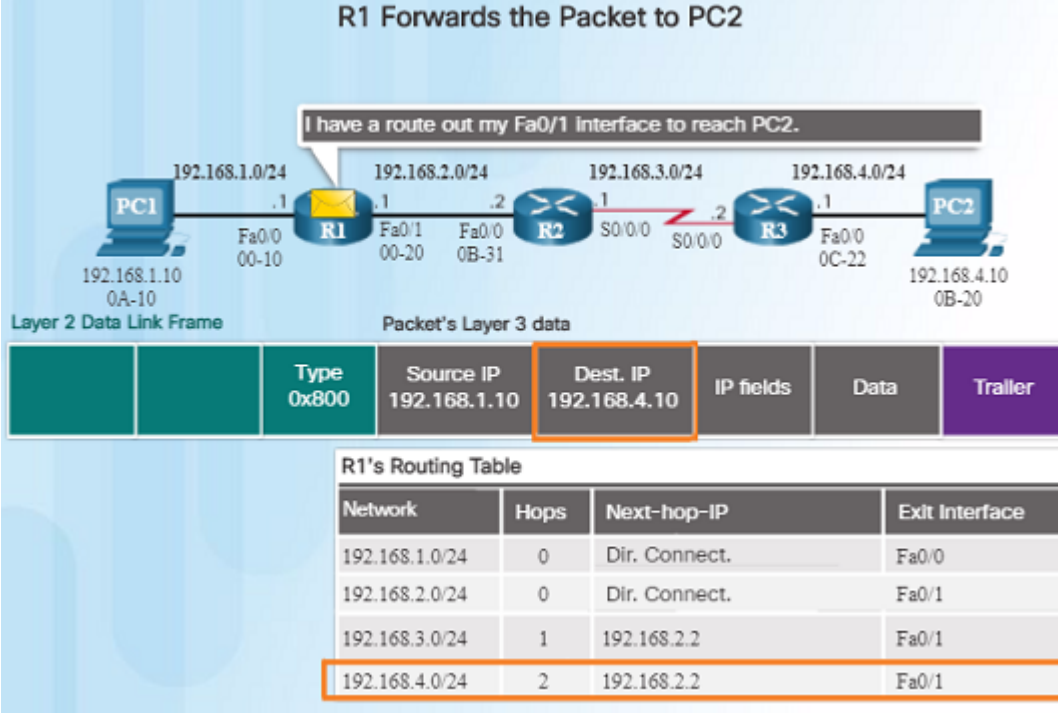
- For PC1 to send a packet to PC2, the following occurs:
  - PC1 must determine if the destination IPv4 address is on the same network. If it is on the same network, PC1 will obtain the destination MAC address from its ARP cache or use an ARP request.
  - Because the destination network is on a different network, PC1 forwards the packet to its default gateway.
  - To determine the MAC address of the default gateway, PC1 checks its ARP table for the IPv4 address of the default gateway and its corresponding MAC address. An ARP request is sent if it is not found.
  - When PC1 has the MAC address of Router R1, it can forward the packet.

Forward to the Next Hop



- When R1 receives the Ethernet frame from PC1, the following occurs:
  - R1 examines the destination MAC address which matches the MAC address of the receiving interface and copies the frame into its buffer.
  - R1 identifies the Ethernet Type field as 0x800 which indicates that the Ethernet frame contains an IPv4 packet in the data portion of the frame.
  - R1 de-encapsulates the Ethernet frame.
  - Because the destination IPv4 address of the packet, 192.168.4.10, does not match any of the directly connected networks on R1, R1 searches the routing table for a corresponding route.
    - R1's Routing Table has a route for the 192.168.4.0/24 network.

Forward to the Next Hop (Cont.)

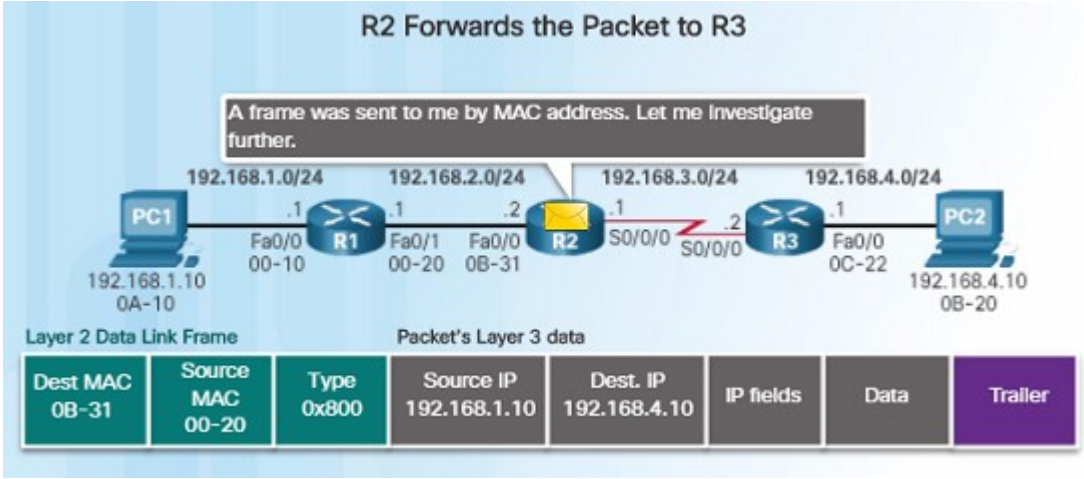


R1's Routing Table

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

- When R1 receives the Ethernet frame from PC1, the following occurs:
  - The route that R1 finds to the 192.168.4.0/24 network has a next-hop address of 192.168.2.2 and an exit interface of FastEthernet 0/1.
  - This will require that the IPv4 packet be encapsulated in a new Ethernet frame with the destination MAC address of the IPv4 address of the next-hop router, 192.168.2.2
  - Because the exit interface is on an Ethernet network, R1 must resolve the next-hop IPv4 address with a destination MAC address using ARP, assuming it is not in its ARP cache.
  - When R1 has the MAC address for the next-hop, the Ethernet frame is forwarded out of the FastEthernet 0/1 interface of R1.

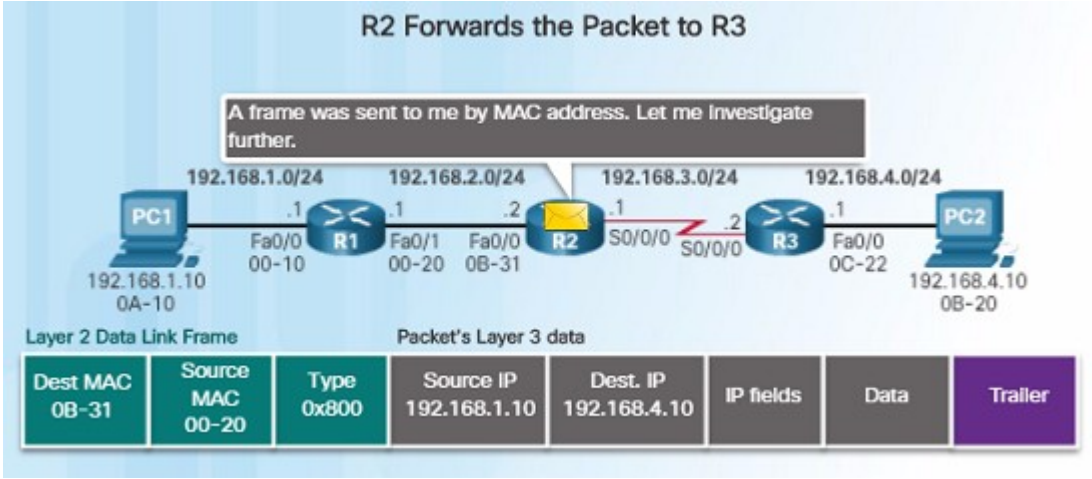
Packet Routing



- The process outlined to the right describes what happens when router R2 receives a frame on its FA0/0 interface that needs to be forwarded to router R3.

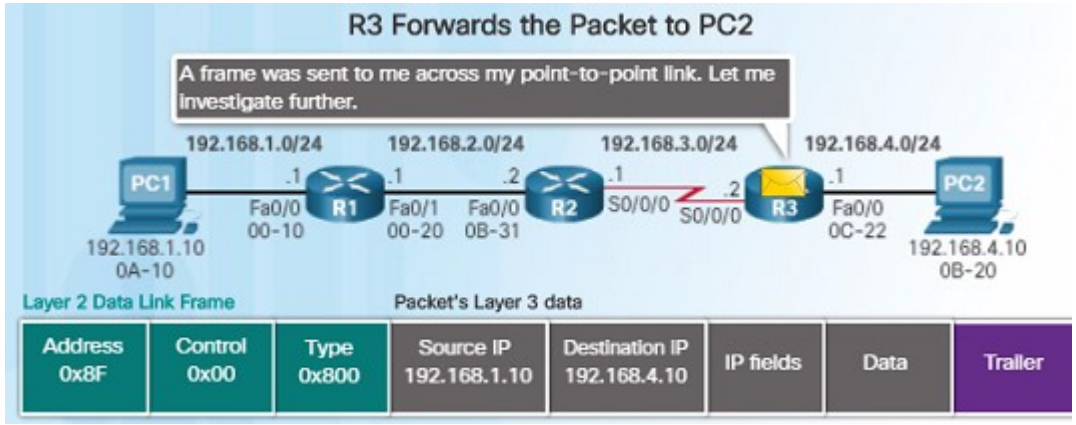
- R2 examines the destination MAC address. Because it matches the MAC address of its receiving interface, R2 copies the frame into its buffer.
- R2 determines that that frame contains an IPv4 packet in the data portion of the frame.
- R2 de-encapsulates the Ethernet frame.
- Because the destination IP address is on a different network, the routing table is searched to find a corresponding route for the destination IPv4 address.

Packet Routing (Cont.)



- The routing table of R2 has a route to the 192.168.4.0/24 network with a next-hop IPv4 address of 192.168.3.2 and an exit interface of Serial 0/0/0.
- Because the exit interface is not Ethernet, R2 does not have to resolve the next-hop IP-v4 address with a destination MAC address.
- The IPv4 packet is encapsulated into a new data link frame used by the exit interface and sent out the Serial 0/0/0 exit interface.
- Because there are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of a broadcast.

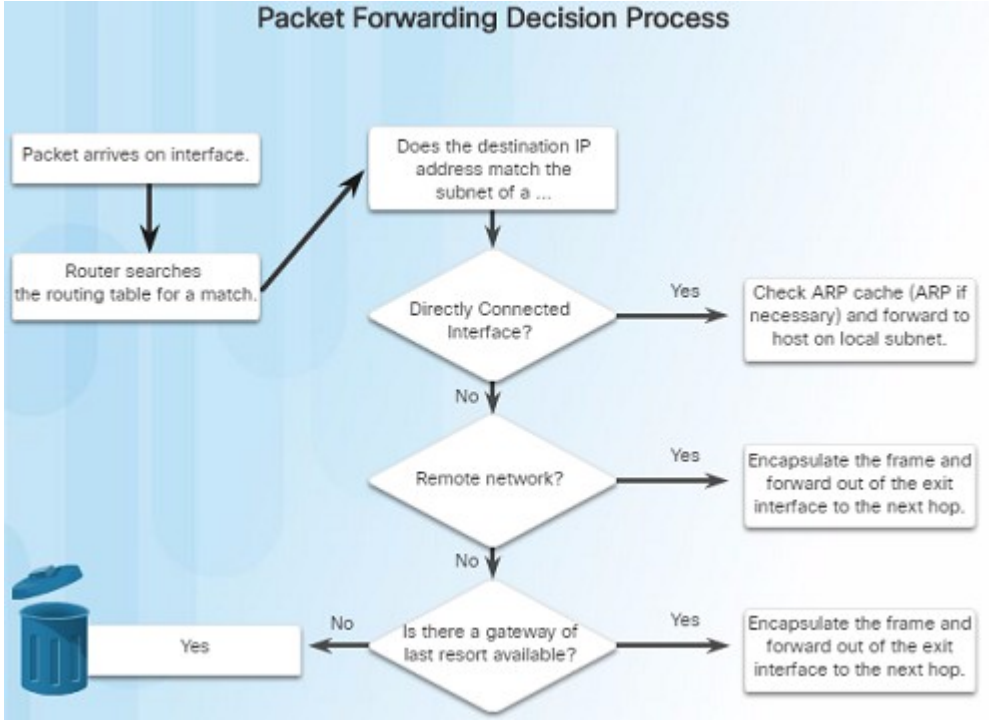
Reach the Destination



- The process outlined on the right describes what takes place when R3 receives a frame on its serial interface.

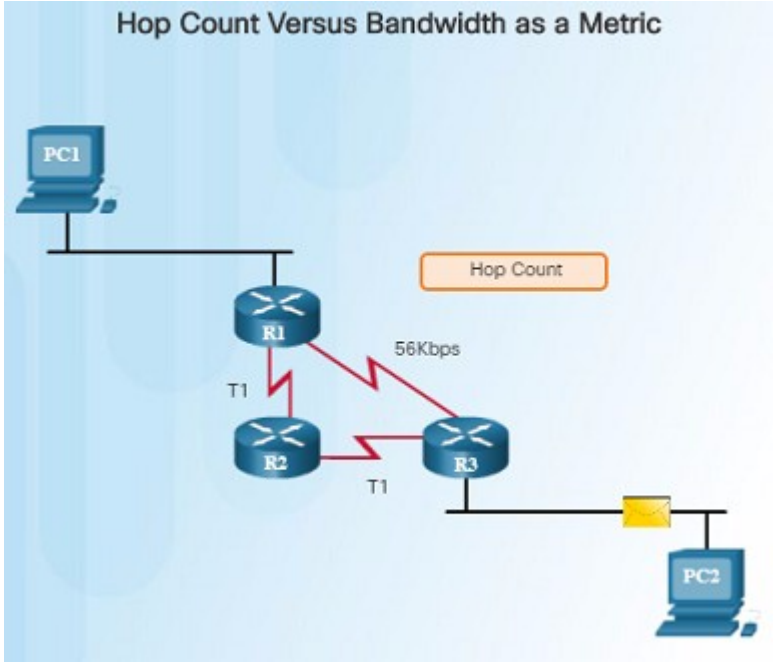
- R3 copies the data link PPP frame into its buffer.
- R3 de-encapsulates the data link PPP frame.
- R3 searches the routing table for the destination IPv4 address of the packet.
- Because the destination network is on R3's directly connected network, the packet can be sent directly and does not need to be sent to another router.
- Because the exit interface is a directly connected Ethernet network, R3 must resolve the destination IPv4 address of the packet with a destination MAC address by either finding it in its ARP cache or send out an ARP request.

Routing Decisions



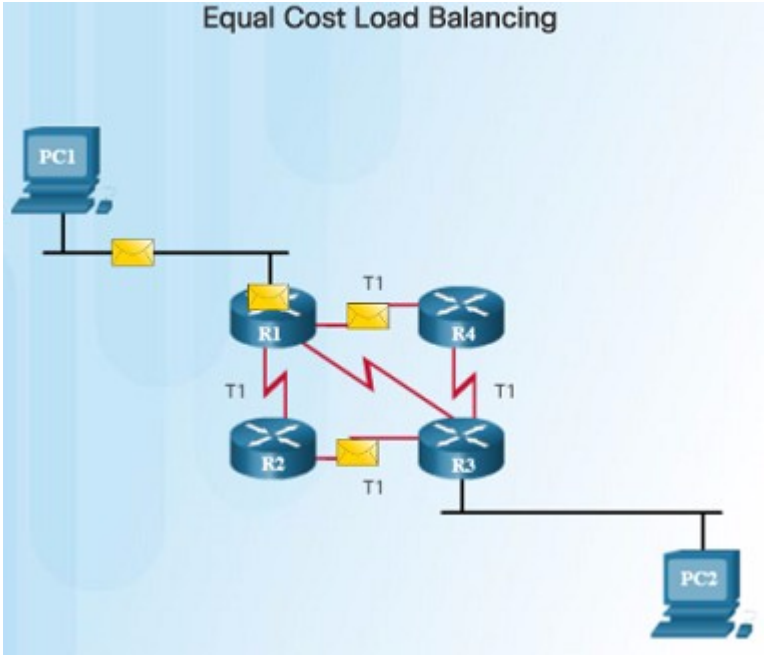
- The primary function of a router is to determine the best path to send packets.
- A routing table search results in one of three path determinations:
  - Directly connected network – If the destination IP address belongs to a network that is directly connected to the router, the packet is forwarded out of that interface.
  - Remote network – If the destination IP address of the packet belongs to a remote network, the packet is forwarded to another router.
  - No route determined – If the destination IP address does not belong to a connected network or is in the routing table, the packet is sent to Gateway of Last Resort.

Best Path



- Determining the best path to a destination network involves the evaluation of multiple paths and selecting the optimum or shortest path to reach that network.
- The best path is selected based on the metric or value that is used by the routing protocol.
- The best path to a network is the path with the lowest metric. A metric is a value that is used to measure the distance to a given network.
- Each dynamic routing protocols has their own rules and metrics to build and update routing tables. For example:
  - Routing Information Protocol (RIP) – Hop count
  - Open Shortest Path First (OSPF) – Cisco's cost based cumulative bandwidth from source to destination
  - Enhanced Interior Gateway Routing Protocol (EIGRP) – Bandwidth, delay, load, reliability

Load Balancing



- If a router has two or more paths with identical metrics to the same destination network, the router will forward the packets using both paths equally.
- The routing table contains a single destination network, but has multiple exit interfaces – one for each equal cost path. This is referred to as equal cost load balancing.
- If configured correctly, load balancing can increase the effectiveness and performance of the network.
- Equal cost load balancing can be configured to use both dynamic routing protocols and static routes.
- EIGRP supports unequal cost load balancing.

Administrative Distance

Default Administrative Distances

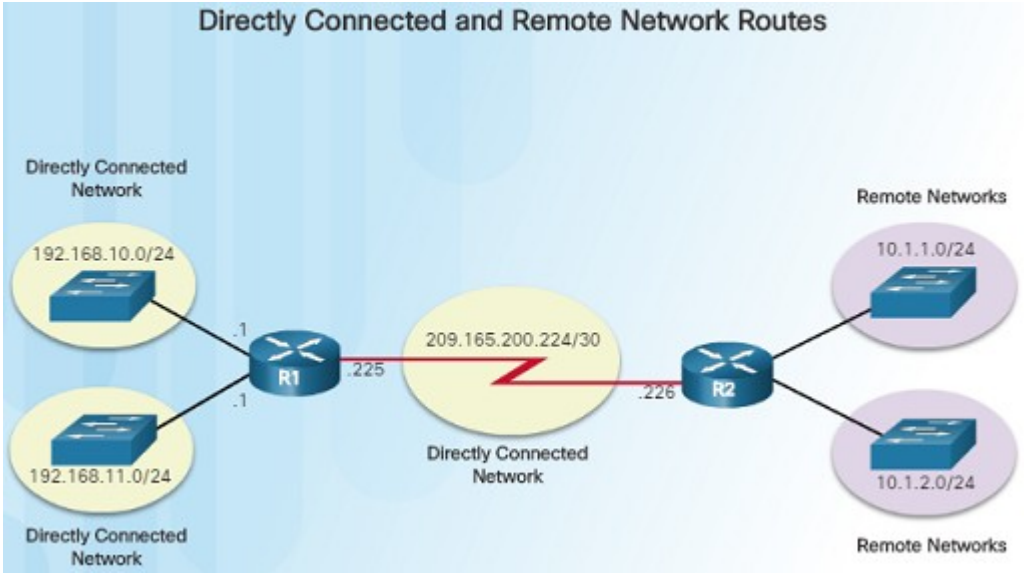
Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

- Which route source is more trustworthy, Internal EIGRP or OSPF?

- If a router has multiple routing protocols configured and static routes, it is possible that the routing table might have more than one route source for the same destination network.
- Each routing protocol might prefer a different path to reach the same destination. How does the router know which path to choose?
- The Cisco IOS uses what is known as the administrative distance (AD) to determine which route to install in the routing table.
- The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy.

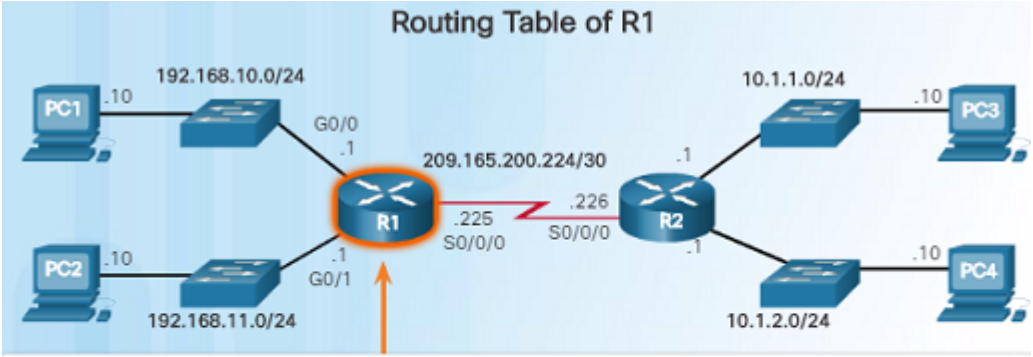
1.3 Router Operation

The Routing Table



- The routing table of a router stores information about:
  - Directly connected routes – Obtained from the active router interfaces.
  - Remote routes – These are remote networks connected to other routers that are learned from dynamic routing protocols or are statically configured.
- A routing table is a data file in RAM that is used to store information about directly connected and remote networks.
- The routing table contains next hop associations for remote networks. The association tells the router what the next hop is for a destination network.

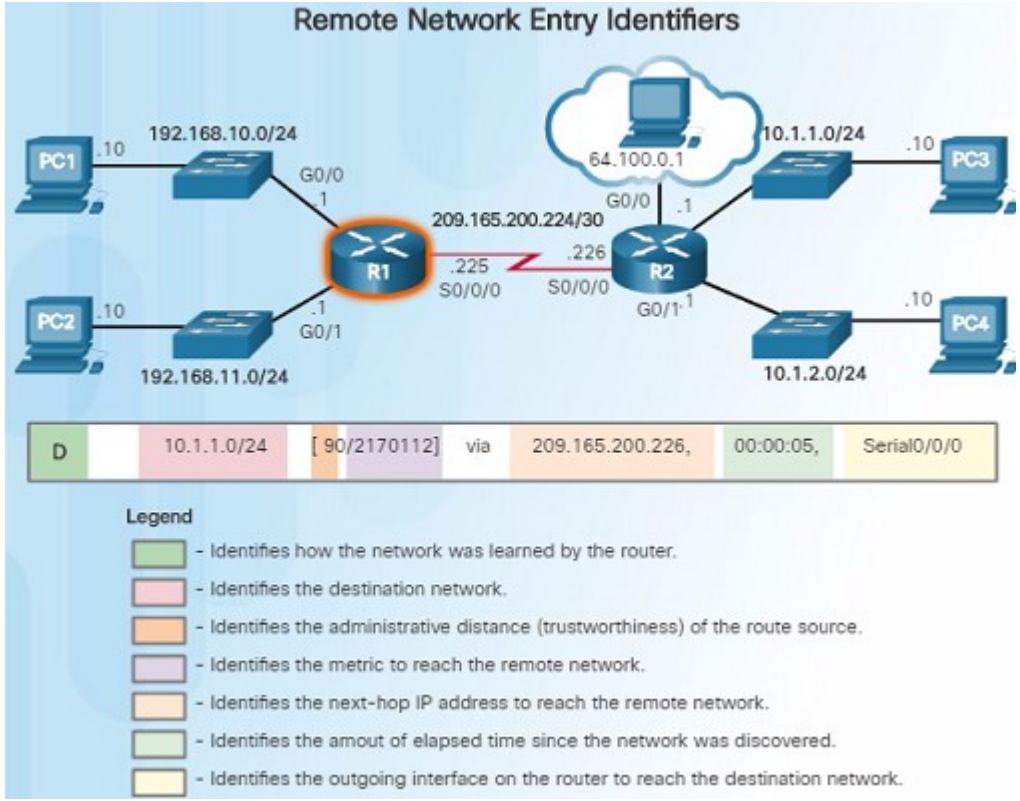
Routing Table Sources




```
R1# show running-config
<output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface GigabitEthernet0/0
```

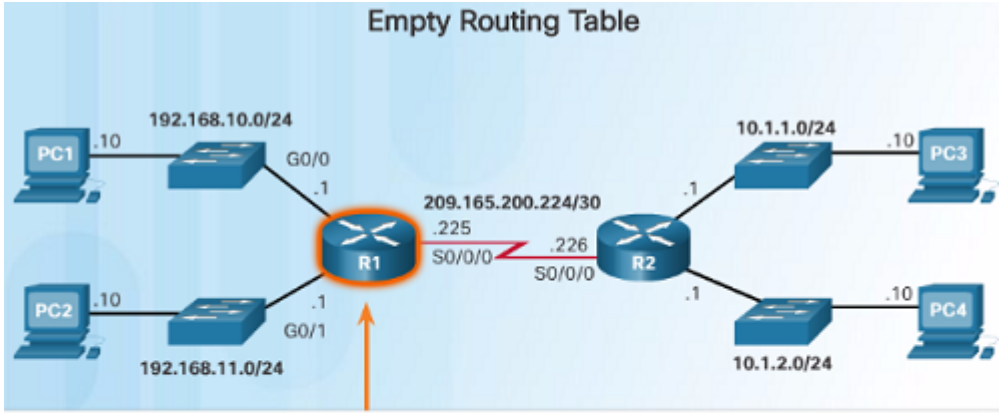
- On a Cisco router, the **show ip route** command can be used to display the IPv4 routing table.
- Additional route information is provided in the routing table including: how the route was learned, how long the route has been in the table, and which interface to send out of to reach a destination.
- Sources of the routing table entries are identified by a code:
  - L - Local Route interfaces
  - C - Directly connected interfaces
  - S - Static routes
  - D – Learned dynamically from another router using the EIGRP routing protocol.
  - O – Learned dynamically from another router using the OSPF routing protocol.

Remote Network Routing Entries



- You must know how to interpret the content of IPv4 and IPv6 routing tables. The figure to the left highlights the details for the route to the remote network 10.1.1.0:
  - Route source – how the route was learned
  - Destination network – address of the remote network
  - Administrative distance – trustworthiness of the route
  - Metric – value assigned to reach the remote network; lower the better
  - Next-hop – the IPv4 address of the next router to forward the packet to
  - Route timestamp – how much time has passed since the route was learned
  - Outgoing interface – exit interface to forward packet out of

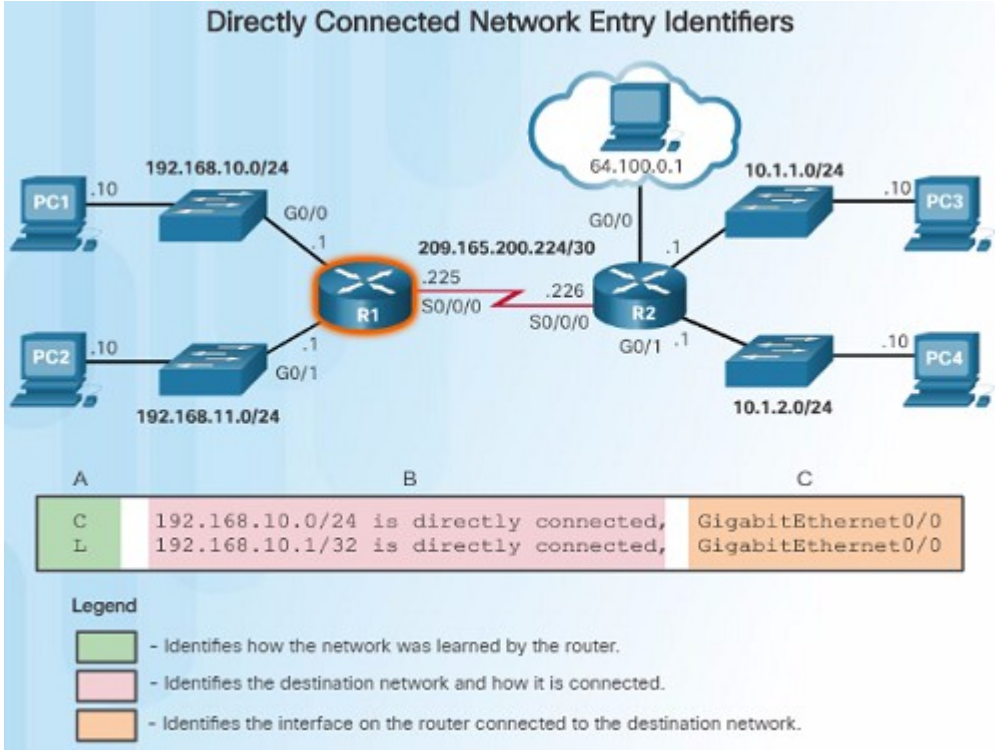
Directly Connected Interfaces




```
R1# show ip route
Codes:L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is not set
R1#
```

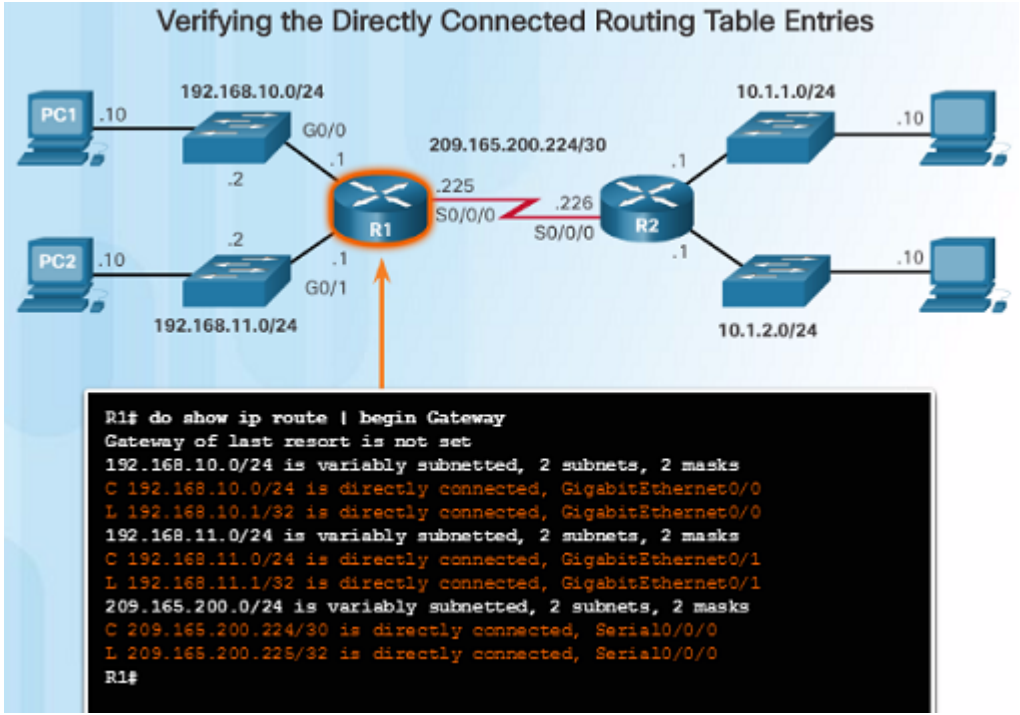
- A new router without any configured interfaces will have an empty routing table – as shown in the figure.
- Before the interface state is considered up/up and added to the IPv4 routing table, the interface must:
  - Be assigned a valid IPv4 or IPv6 address
  - Be activated with the no shutdown command
  - Receive a carrier signal from another device such as a router, switch, or host.
- When the interface is up, the network of that interface is added to the routing table as a directly connected route.

Directly Connected Routing Table Entries



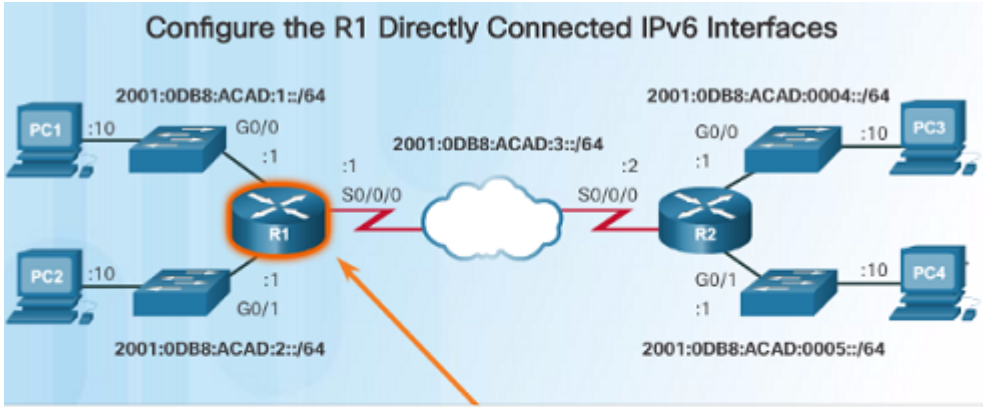
- With IOS version 15 and later, an active directly connected interface creates two routing table entries as shown in the figure:
  - The route source “C” identifies the route as a directly connected network.
  - The route source “L” identifies the IPv4 address assigned to the router’s interface.
- The routing table entry shows the destination network as well as the outgoing interface to use when forwarding packets to the destination network.

Directly Connected Examples



- When the interfaces are configured with an appropriate IP address, subnetmask, and activated with the **no shutdown** command, they will be automatically added to the routing table as shown in the figure to the left.
- As each interface is added, the routing table automatically adds the connected (‘C’) and local (‘L’) entries.

Directly Connected IPv6 Example




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb  3 21:38:37.279: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
*Feb  3 21:38:40.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Feb  3 21:38:41.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
```

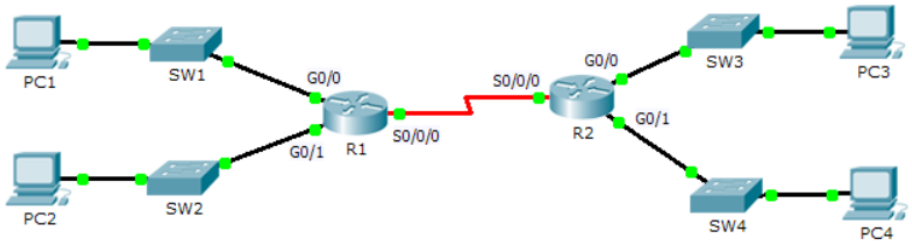
- The figure to the left shows the configuration steps for the directly connected interfaces of R1 with the indicated IPv6 addresses.
- The **show ipv6 route** command is used to verify that the IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table.
  - A ‘C’ indicates that it is a directly connected route.
  - An ‘L’ indicates it is a local route, but with IPv6, it has a /128 prefix.
- The ping command can be used to verify connectivity. For example:
  - ping 2001:db8:acad:3::2

Packet Tracer – Investigating Directly Connected Routes

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Investigating Directly Connected Routes

Topology



Objectives

Part 1: Investigate IPv4 Directly Connected Routes

Part 2: Investigate IPv6 Directly Connected Routes

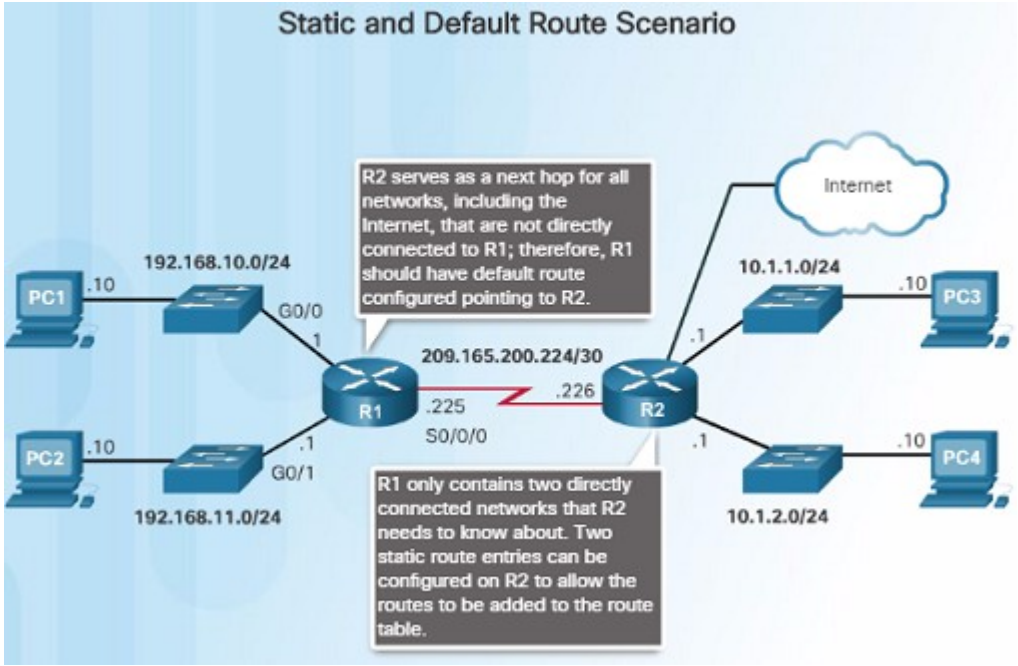
Background

The network in the activity is already configured. You will log in to the routers and use **show** commands to discover and answer the questions below about the directly connected routes.

Note: The user EXEC password is **cisco** and the privileged exec password is **class.**

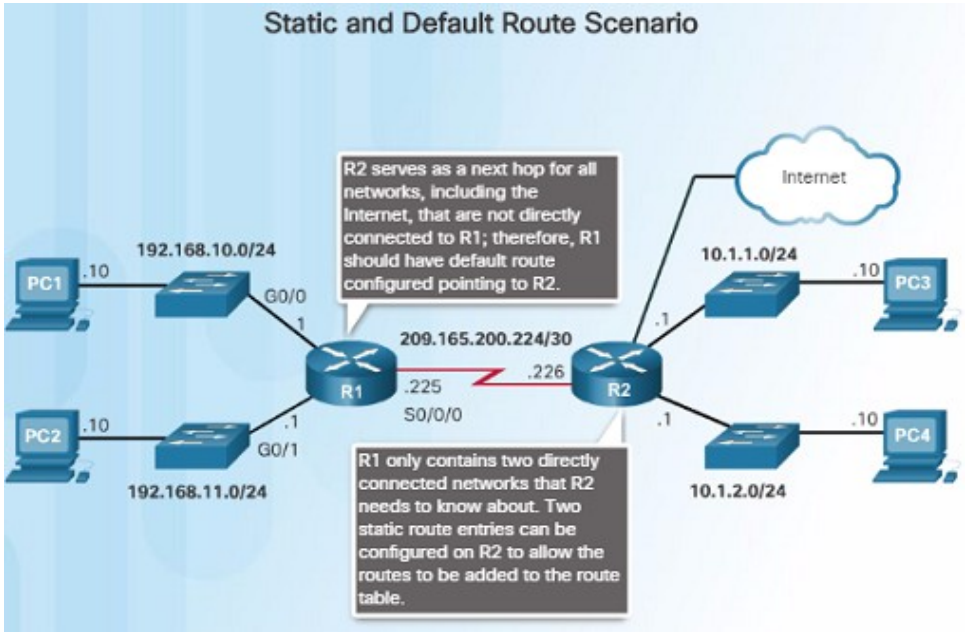
Part 1: Investigate IPv4 Directly Connected Routes

Static Routes



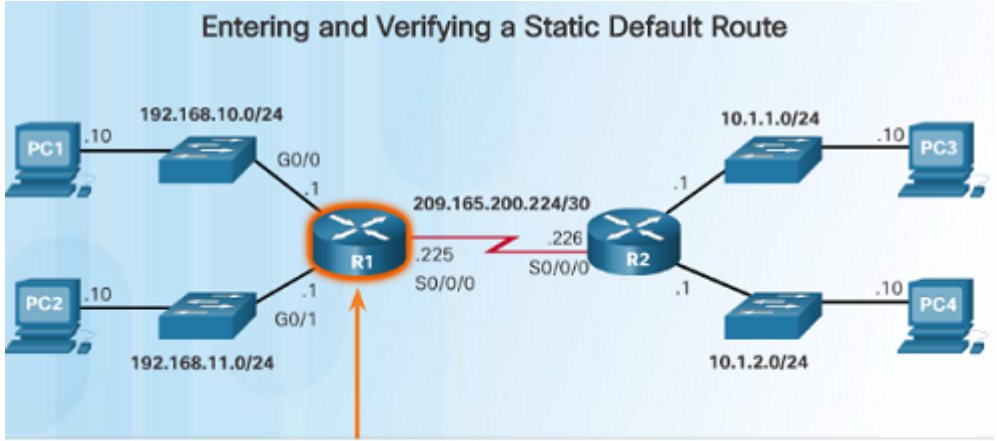
- After directly connected interfaces are configured and added to the routing table, then static or dynamic routing can be configured.
- Static routes are manually configured and define an explicit path between two networking devices.
- If the network topology changes, static routes must manually be reconfigured.
- Benefits of static routes include:
  - Improved security
  - Resource efficiency – less bandwidth usage and no CPU cycles are used to calculate and communicate route

Static Routes (Cont.)



- There are two main types of static routes in the routing table:
  - Static route to a specific network
  - Default static route
- IPv4 static routes are configured using the following command:
  - **ip route** network mask { *next-hop-ip* | *exit-intf* }
- A static route appears in the routing table with the code ‘S’.
- A default static route is similar to a default gateway on a PC or host. The default static route specifies the exit point to use when the routing table does not have a path for the destination network. Use the command:
  - **ip route** 0.0.0.0 0.0.0.0 { exit-intf | next-hop-ip }

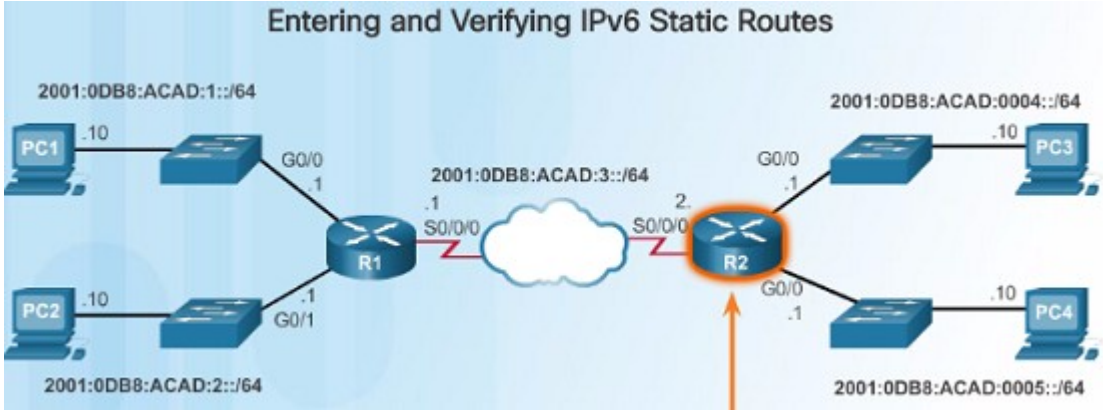
Static Route Examples




```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)# exit
R1#
*Feb 1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console
by console

R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial0/0/0
   192.168.10.0/24 is variably subnetted, 2 subnets, 2 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, 2 masks
C     192.168.11.0/24 is directly connected, GigabitEthernet0/1
```

- The figure to the left shows the configuration of an IPv4 default static route on R1 to the Serial 0/0/0 interface.
  - The ‘S’ indicates that it is a static route
  - The asterisk (*) identifies this as a possible candidate to be the default route.
  - Notice that this route was chosen to be the Gateway of last resort (default route).
- Here are two static route configurations from R2 to reach the two LANs on R1:
  - **ip route** 192.168.10.0 255.255.255.0 s0/0/0
  - **ip route** 192.168.11.0 255.255.255.0 209.165.200.225
- Which route was configured to use the exit interface?
- Will they send packets for these networks to the same router?

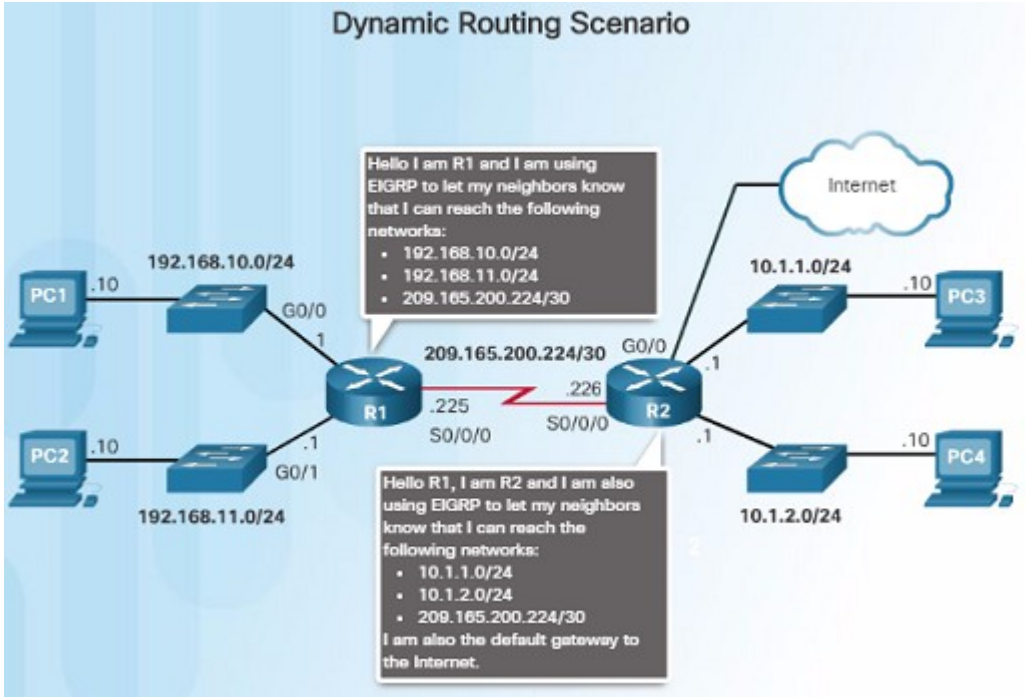
Static IPv6 Route Examples



- Like IPv4, static routes are explicitly configured to reach a specific remote network. For example:
  - **ipv6 route** 2001:0DB8:ACAD:1::/64 2001:0Db8:ACAD:3::1
  - **ipv6 route** 2001:0DB8:ACAD:2::/64 s0/0/0
- Notice that one of these routes uses an exit interface while the other uses a next hop address.

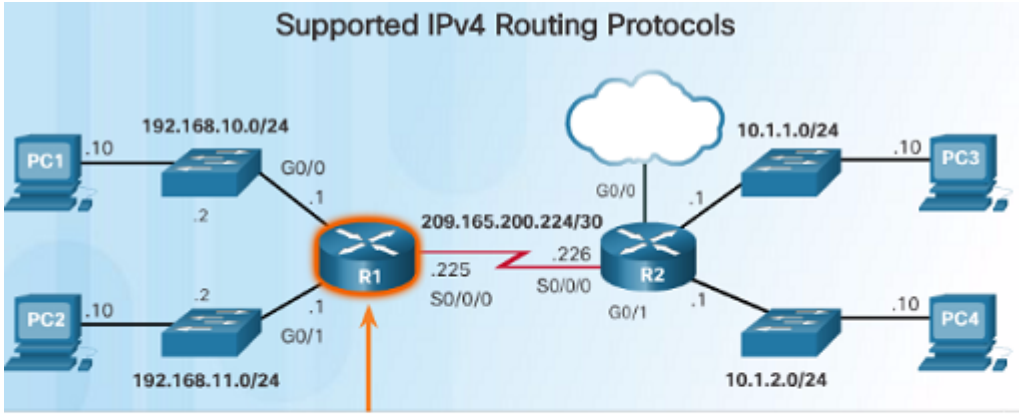
- To configure a default IPv6 static route, use the **ipv6 route ::/0** [ipv6-address | interface-type interface-number} global configuration command:
  - **ipv6 route ::/0 s0/0/0**
  - Unlike the IPv4 static route, there is no asterisk (*) or Gateway of Last Resort explicitly identified in the routing table.
- Use the **show ipv6 route** command to verify the static routes were installed.
- Use ping to verify remote network connectivity from R1:
  - **ping** 2001:0DB8:ACAD:4::1

Dynamic Routing



- Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks.
- Rather than manually configuring static routes, dynamic routing protocols use network discovery to share information about the networks that it knows about with other routers that are using the same routing protocol.
  - Routers automatically learn about remote networks from other routers
  - These networks and the best path to each are added to the routing table of the router.
- Routers have converged after they have finished exchanging and updating their routing tables. Routers then maintain the networks in their routing tables.

IPv4 Routing Protocols




```
R1(config)# router ?
  bgp       Border Gateway Protocol (BGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  ospfv3    OSPFv3
  rip       Routing Information Protocol (RIP)

R1(config)# router
```

- One of the major advantages of dynamic routing protocols over static routes - determine a new best path if the initial path becomes unusable.
- Dynamic routing protocols can adjust to topology changes without involving the network administrator.
- Cisco routers support a variety of IPv4 routing protocols including:
  - EIGRP
  - OSPF
  - IS-IS
  - RIP
  - Use **router ?** in global config mode to see the complete list.

1.4 Summary

Chapter 2: Routing Concepts

- Configure a router to route between multiple directly connected networks.
- Explain how routers use information in data packets to make forwarding decisions in a small to medium-sized business network
- Explain how a router learns about remote networks when operating in a small to medium-sized business network.


CISCO