Instructor Materials Chapter 1: Routing Concepts

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Instructor Materials – Chapter 1 Planning Guide

This PowerPoint deck is divided in two parts:

1. Instructor Planning Guide
   - Information to help you become familiar with the chapter
   - Teaching aids
2. Instructor Class Presentation
   - Optional slides that you can use in the classroom
   - Begins on slide # 13

Note: Remove the Planning Guide from this presentation before sharing with anyone.

cisco

Routing and Switching Essentials 6.0 Planning Guide
Chapter 1: Routing Concepts

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
1.0.1.2	Class Activity	Do We Really Need a Map?	Optional
1.1.1.7	Class Activity	Identify Router Components	-
1.1.1.8	Packet Tracer	Use Traceroute to Discover the Network	Recommended
1.1.1.9	Lab	Mapping the Internet	Optional
1.1.2.7	Syntax Checker	Configure the Management SVI on S2	-
1.1.2.8	Class Activity	Document an Addressing Scheme	-
1.1.2.9	Packet Tracer	Document the Network	Recommended
1.1.3.1	Syntax Checker	Configure Basic Settings on R2	-
1.1.3.2	Syntax Checker	Configure an IPv4 Router Interface	-
1.1.3.5	Packet Tracer	Configure IPv4 and IPv6 Interfaces	Recommended

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 1: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
1.1.4.1	Syntax Checker	Verfiy Router Interfaces (Fig.4)	-
1.1.4.1	Syntax Checker	Verify Router IP Interfaces (Fig.5)	-
1.1.4.3	Syntax Checker	Filtering Show Commands	-
1.1.4.4	Syntax Checker	Command History Feature	-
1.1.4.5	Packet Tracer	Configure and Verify a Small Network	Recommended
1.1.4.6	Lab	Configure Basic Router Settings with IOS CLI	Optional
1.2.1.6	Class Activity	Match Layer 2 and Layer 3 Addressing	-
1.2.2.5	Class Activity	Order the Steps in the Packet Forwarding Process	-
1.2.2.6	Class Activity	Match the Administrative Distance to the Route Source	-
1.3.1.4	Class Activity	Interpret the Content of a Routing Table Entry	-

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 1: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
1.3.2.3	Syntax Checker	Configure the Directly Connected Interfaces on R2	-
1.3.2.5	Packet Tracer	PT Investigating Directly Connected Routes	Recommended
1.3.3.2	Syntax Checker	Configure a Default Static Route on R1 (Fig. 3)	-
1.3.3.2	Syntax Checker	Configure Static Route on R2 (Fig. 4)	-
1.4.1.1	Class Activity	We Really Could Use a Map!	Optional

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 1: Assessment

- Students should complete Chapter 1, “Assessment” after completing Chapter 1.
- Quizzes, labs, Packet Tracers and other activities can be used to informally assess student progress.

Chapter 1: Best Practices

Prior to teaching Chapter 1, the instructor should:

- Complete Chapter 1, "Assessment."
- The objectives of this chapter are:
  - Describe the primary functions and features of a router.
  - Connect devices for a small routed network.
  - Using the CLI, configure a router to route between multiple directly connected networks.
  - Explain the encapsulation and de-encapsulation process used by routers when switching packets between interfaces.
  - Explain the path determination function of a router.
  - Compare ways in which a router builds a routing table 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.

Chapter 1: Best Practices (Cont.)

Section 1.1

- Review the OSI model and the TCP/IP protocol stack and review the process of encapsulation.
- Discuss the key Network Characteristics:
  - Topology
  - Reliability
  - Scalability
  - Availability
  - Speed
  - Cost
  - Security
- Highlight the routers position in the OSI model and the process of encapsulation.
- Emphasize that routers are specialized computers.
- Emphasize the types of memory used by routers and what is stored in each.

Chapter 1: Best Practices (Cont.)

Section 1.1 (cont.)

- Make sure students are clear on what role a router plays in a network:
  - To determine best path for packets
  - To forward packets toward their destination
  - To interconnect networks
- Discuss the three packet-forwarding mechanisms that routers use. Stressing that Cisco Express Forwarding (CEF) is the most recent and preferred method
- Ask students what addresses are required in order to connect to a network. And how they are assigned. IP address, subnet mask or prefix, and default gateway.
- Review basic configuration of a router and commands to verify configuration.
- The show command can be filtered for specific parameters to reduce the amount of output by using the pipe (|) character after the show.
  - Show ip interface brief | exclude unassigned
  - Show running config | section line vty

Chapter 1: Best Practices (Cont.)

Section 1.2

- Review encapsulation and de-encapsulation of packets. Encourage students to test their understanding using activity 1.2.1.6
- Discuss Metrics and how the best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network.
  - Have students evaluate different paths to a local destination eg via highway - further but faster or local roads –shorter but slower. Compare to routing metrics.
- Students need to be very familiar with the default Administrative Distances.
- Describe the differences between, and advantages and disadvantages of, Static and Dynamic Routing.

Section 1.3

- Stress the importance of understanding the routing table for verification that the route entries are present and correct. Routing tables contain important information used for troubleshooting.

Chapter 1: Best Practices (Cont.)

Section 1.3 (cont.)

- Provide the student with extra practice exercises interpreting entries in the routing table.
- Demonstrate and encourage the use of the Syntax Checker utility to practice CLI commands.
- Recommendation – Students should keep notes of commands especially "show commands" and the results.
- CLI resources – basic router CLI commands

  http://www.youtube.com/watch?v=-zvihHxrfzM

  http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/routconf.html

Chapter 1: Additional Help

- For additional help with teaching strategies, including lesson plans, analogies for difficult concepts, and discussion topics, visit the CCNA Community at: https://www.netacad.com/group/communities/community-home
- Best practices from around the world for teaching CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna-blog
- If you have lesson plans or resources that you would like to share, upload them to the CCNA Community in order to help other instructors.
- Students can enroll in **Packet Tracer Know How 1: Packet Tracer 101** (self-enroll)

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1: Routing Concepts

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1 - Sections & Objectives

1.1 Router Initial Configuration

- Describe the primary functions and features of a router.
- 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 the encapsulation and de-encapsulation process used by routers when switching packets between interfaces.
- Explain the path determination function of a router.

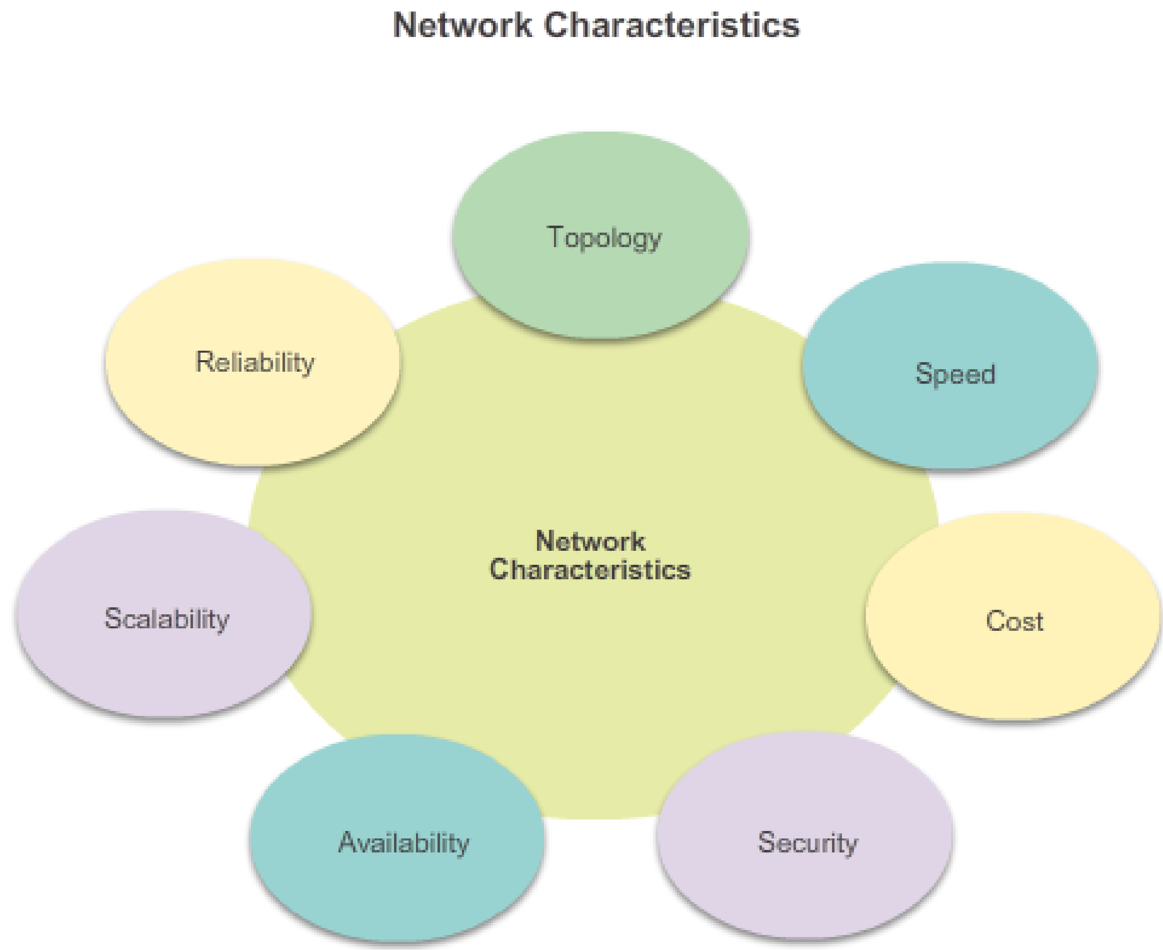
1.3 Router Operation

- 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

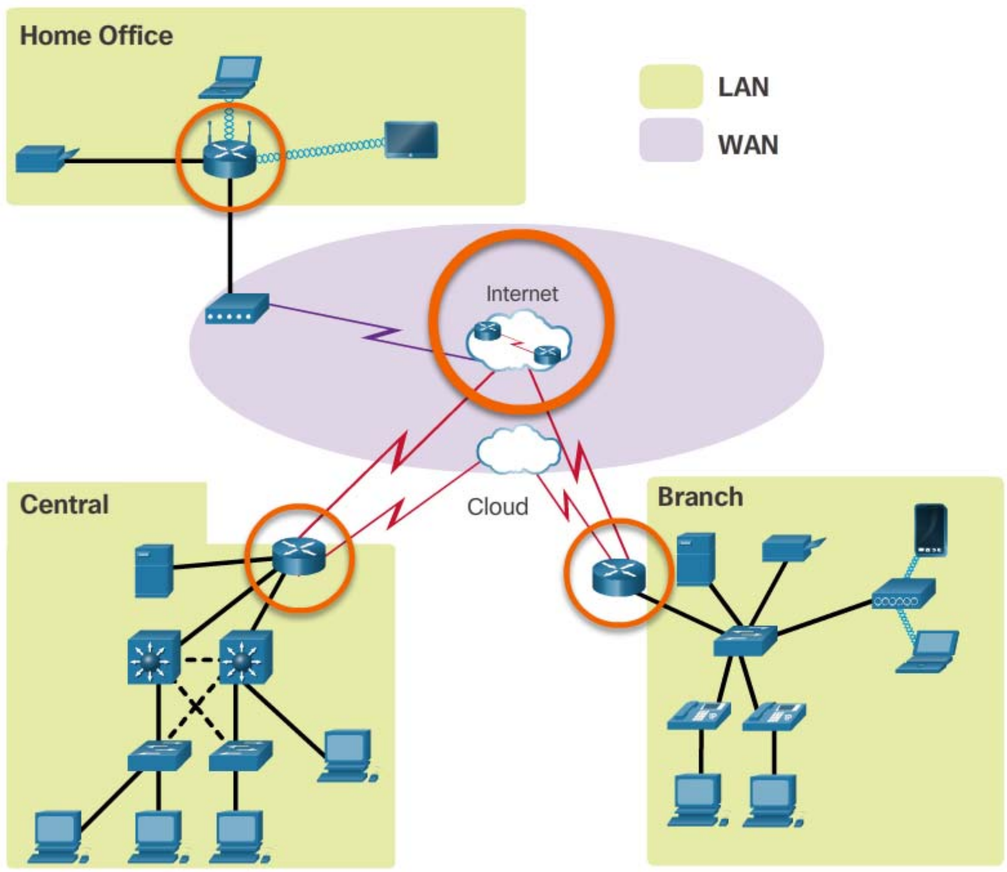
Cisco | Networking Academy®
Mind Wide Open™

Characteristics of a Network



Router Functions
Why Routing?

The router is responsible for the routing of traffic between networks.

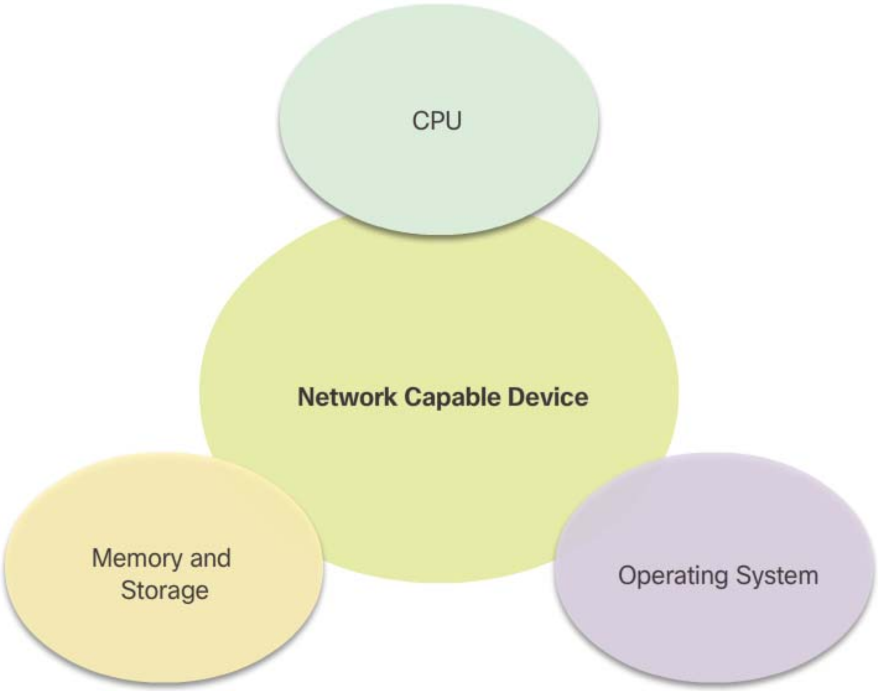


Router Functions

Routers are Computers

Routers are specialized computers containing the following required components to operate:

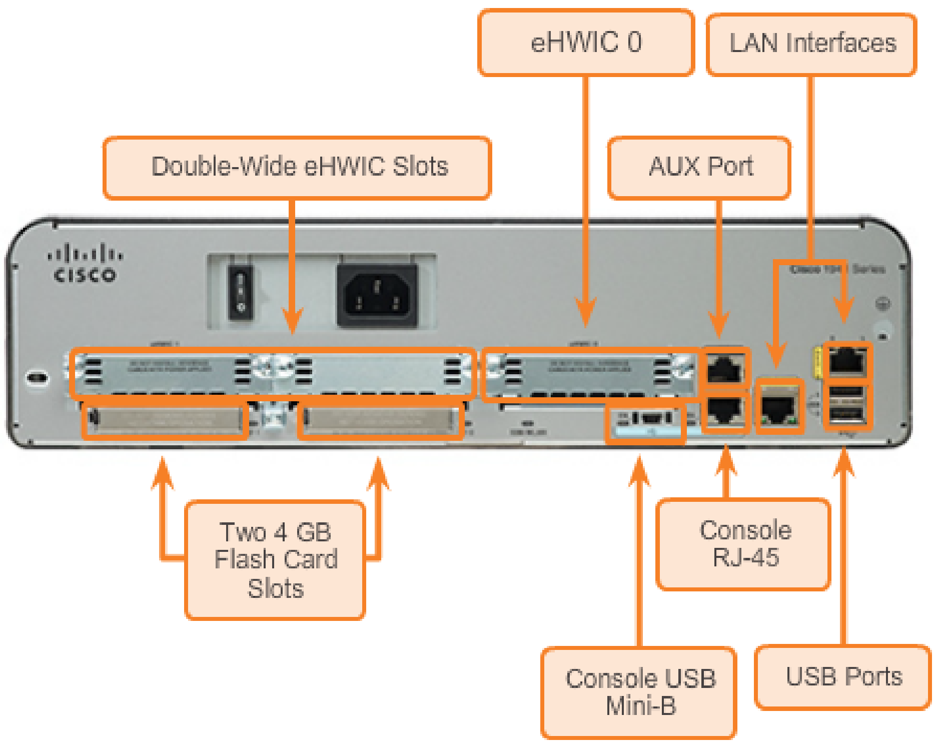
- Central processing unit (CPU)
- Operating system (OS) - Routers use Cisco IOS
- Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)



Routers are Computers (cont.)

Routers use specialized ports and network interface cards to interconnect to other networks.

Back Panel of a Router



Router Functions

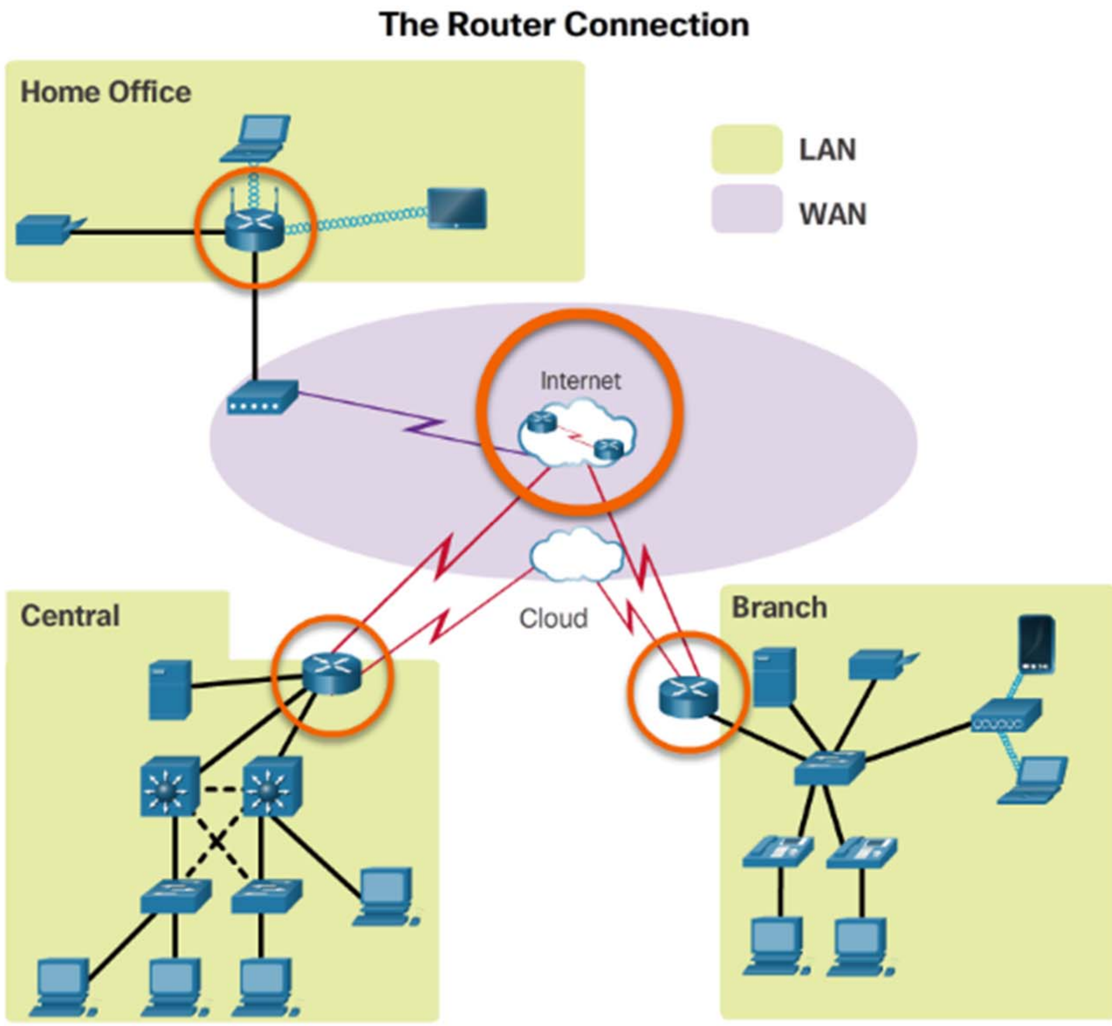
Routers are Computers

Router Memory

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

Router Functions

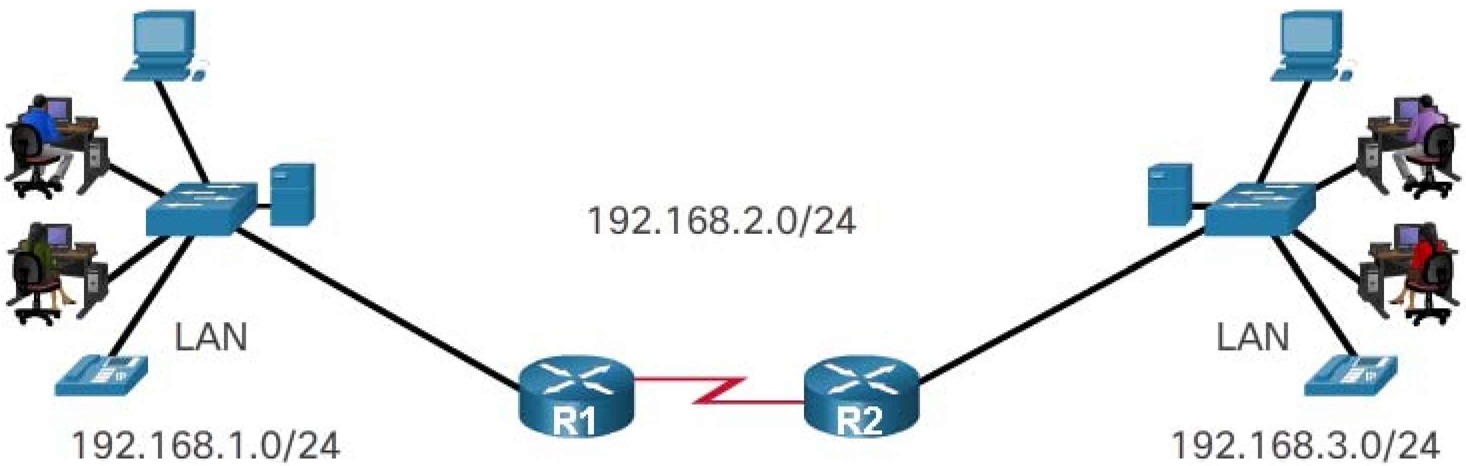
Routers Interconnect Networks



Router Functions

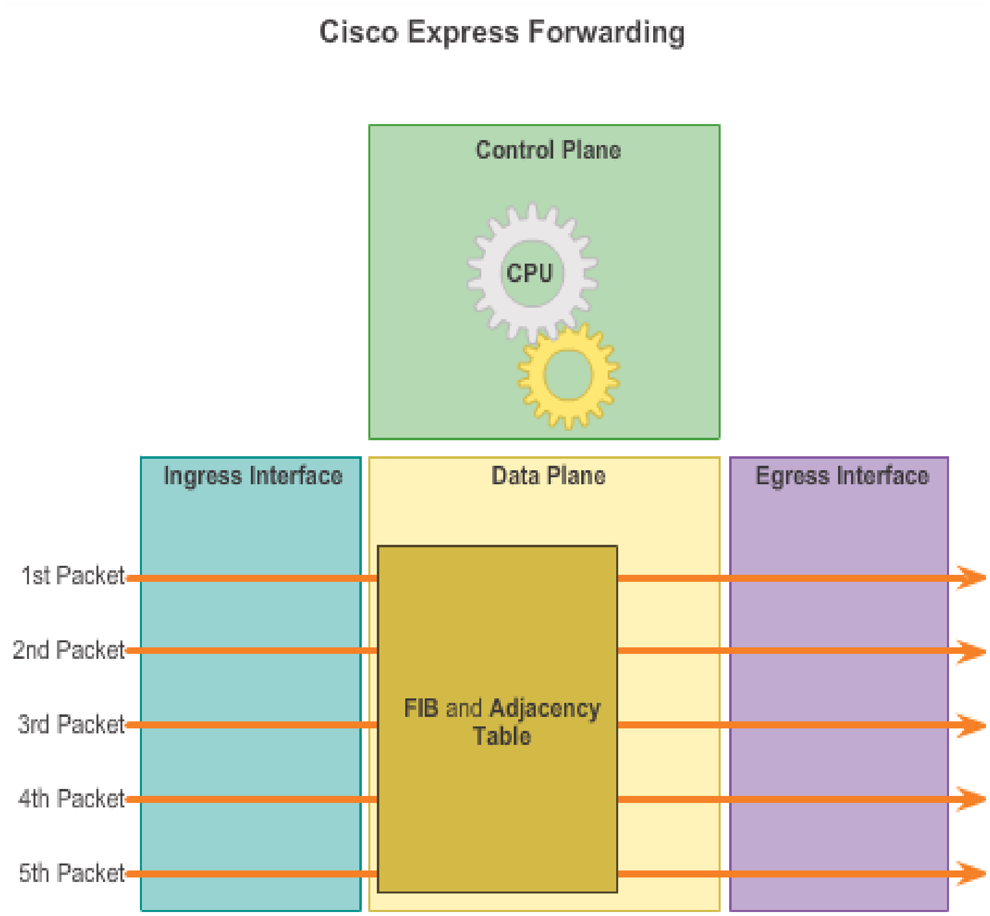
Routers Choose Best Paths

- Routers use static routes and dynamic routing protocols to learn about remote networks and build their routing tables.
- Routers use routing tables to determine the best path to send packets.
- Routers encapsulate the packet and forward it to the interface indicated in routing table.



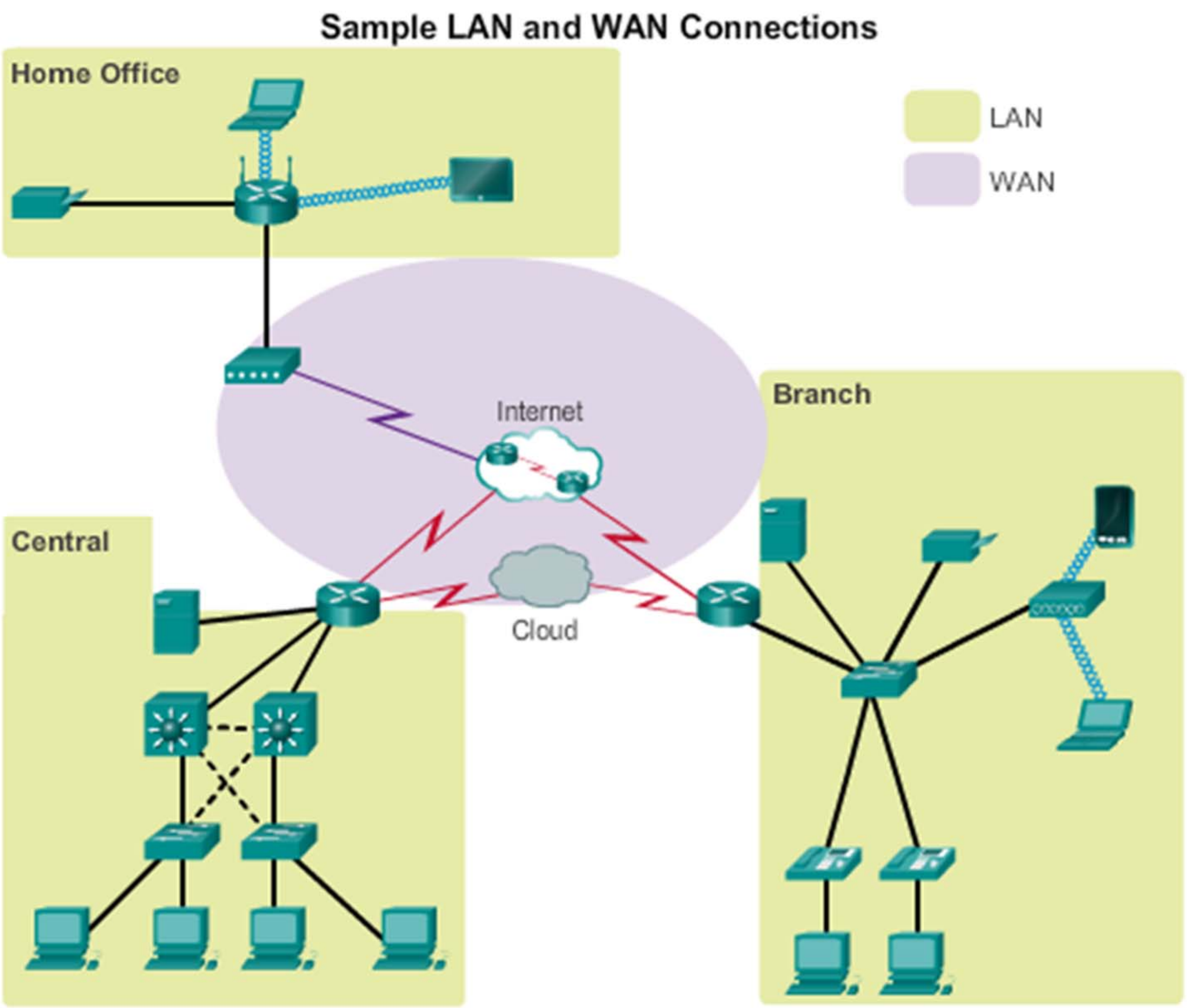
Router Functions
Packet Forwarding Methods

- **Process switching** – An older packet forwarding mechanism still available for Cisco routers.
- **Fast switching** – A common packet forwarding mechanism which uses a fast-switching cache to store next hop information.
- **Cisco Express Forwarding (CEF)** – The most recent, fastest, and preferred Cisco IOS packet-forwarding mechanism.



Connect Devices

Connect to a Network

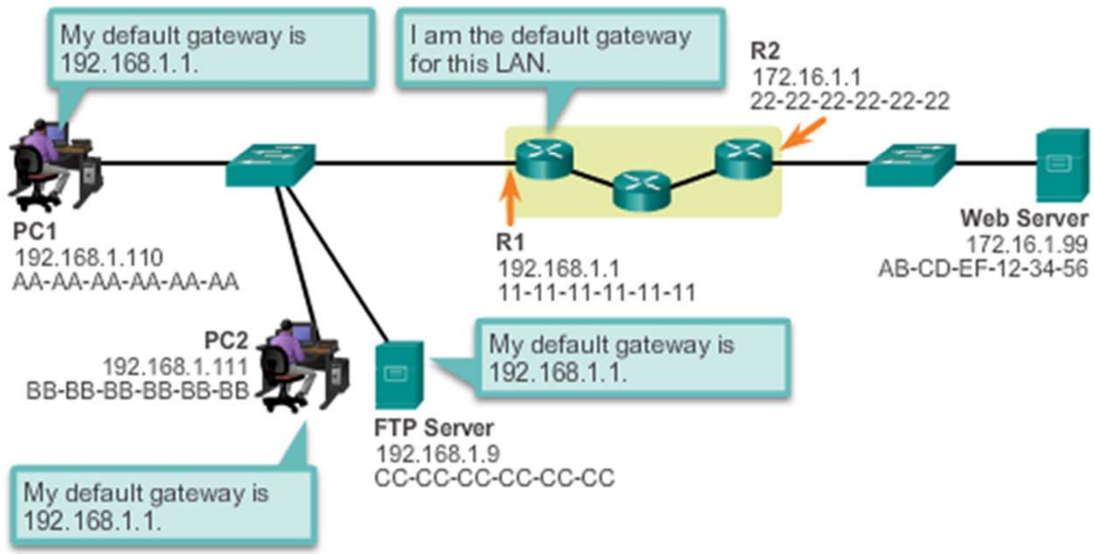


Default Gateways

To enable network access devices, must be configured with the following IP address information:

- **IP address** - Identifies a unique host on a local network.
- **Subnet mask** - Identifies the host's network subnet.
- **Default gateway** - Identifies the router a packet is sent to when the destination is not on the same local network subnet.

Destination MAC Address	Source MAC Address	Source IP Address	Destination MAC Address	Data
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	192.168.1.110	172.16.1.99	

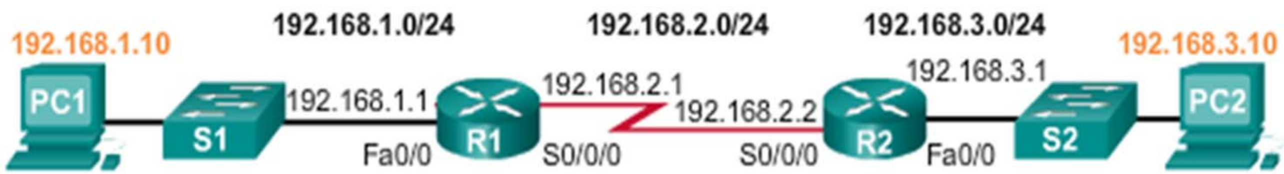


Connect Devices

Document Network Addressing

Network documentation should include at least the following in a topology diagram and addressing table:

- Device names
- Interfaces
- IP addresses and subnet masks
- Default gateways



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

Connect Devices

Enable IP on a Host

Statically Assigned IP address – The host is manually assigned an IP address, subnet mask and default gateway. A DNS server IP address can also be assigned.

- Used to identify specific network resources such as network servers and printers.
- Can be used in very small networks with few hosts.

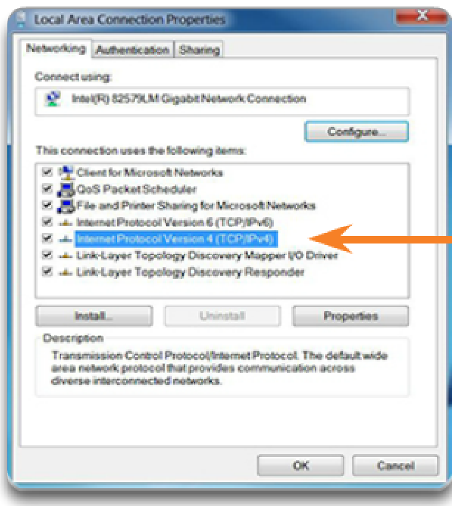
Dynamically Assigned IP Address – IP Address information is dynamically assigned by a server using Dynamic Host Configuration Protocol (DHCP).

- Most hosts acquire their IP address information through DHCP.
- DHCP services can be provided by Cisco routers.

Connect Devices

Enable IP on a Host

Statically Assigning an IP Address

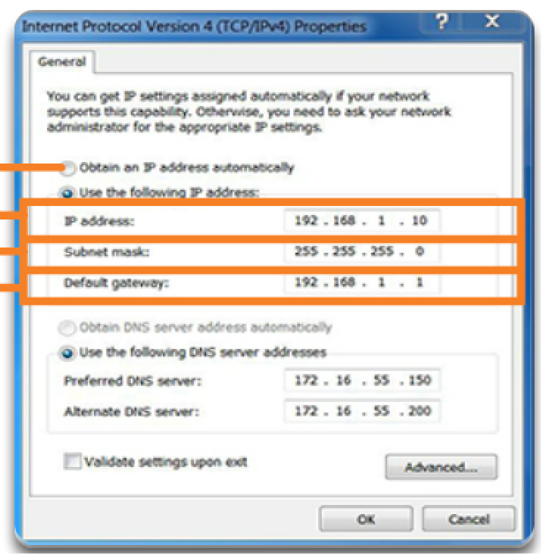


For static assignments, enter addresses:

IP Address

Subnet Mask

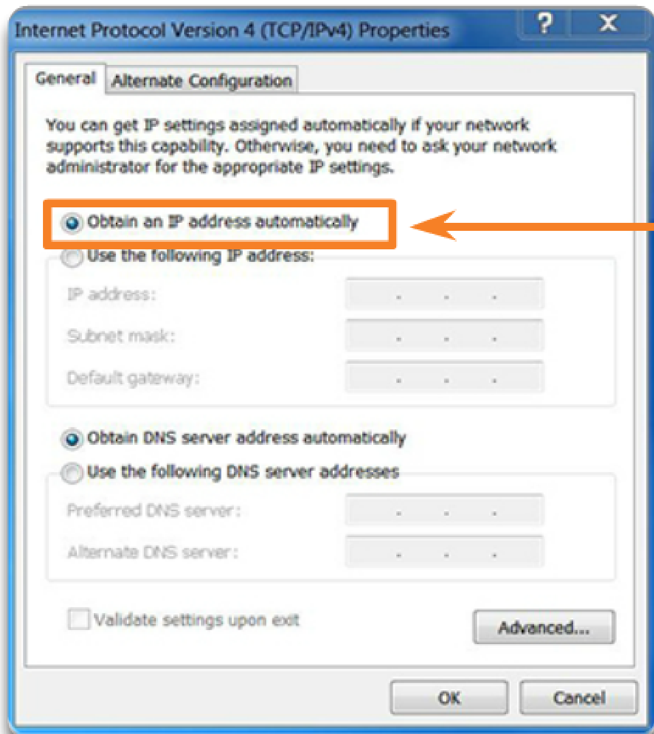
Default Gateway



Connect Devices

Enable IP on a Host

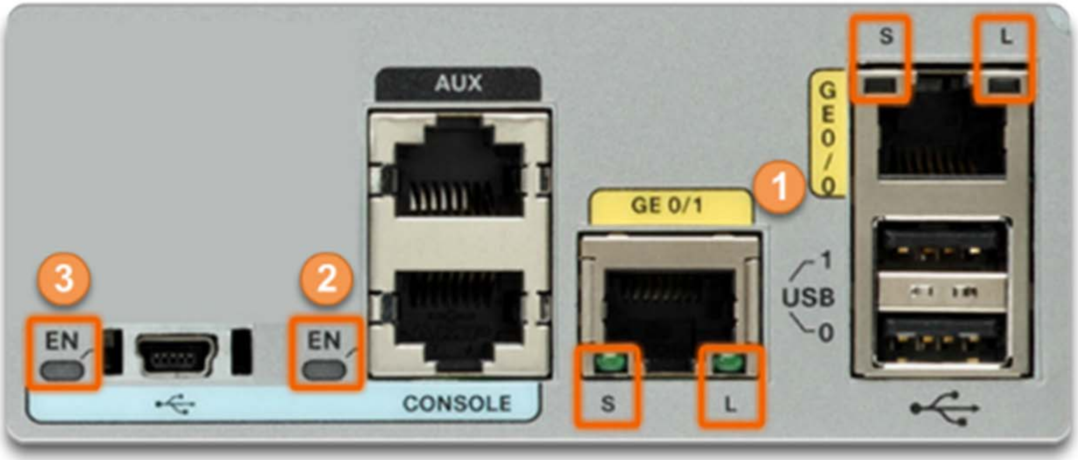
Dynamically Assigning an IP Address



This property will set the device to obtain an IP address automatically.

Device LEDs

CISCO 1941 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

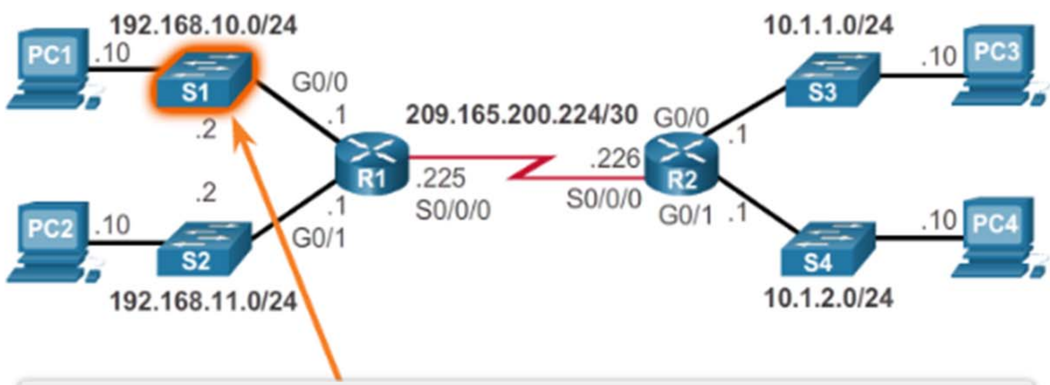
Console Access

Console Connection Requirements

Port on Computer	Cable Required	Port on ISR	Terminal Emulation
Serial Port	RJ-45-to-DB-9 Console Cable	RJ-45 Console Port	Tera Term PuTTY
USB Type-A Port	• USB-to-RS-232 compatible serial port adapter • Adapter may require a software driver • RJ-45-to-DB-9 console cable	RJ-45 Console Port	Tera Term PuTTY
USB Type-A Port	• USB Type-A to USB Type-B (Mini-B USB) • A device driver is required and available from cisco.com.	USB Type-B (Mini-B USB)	Tera Term PuTTY

Enable IP on a Switch

- Network infrastructure devices require IP addresses to enable remote management.
- On a switch, the management IP address is assigned on a virtual interface called a switched virtual interface (SVI)




```
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)#
```

Router Basic Settings

Configure Router Basic Settings

- **Name the device –** Distinguishes it from other routers
- **Secure management access –** Secures privileged EXEC, user EXEC, and Telnet access, and encrypts passwords .
- **Configure a banner –** Provides legal notification of unauthorized access.
- **Save the Configuration**

Secure Management Access


```
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)#
```

Configure an IPv4 Router Interface

To be available, a router interface must be:

- Configured with an address and subnet mask.
- Activated using **no shutdown** command. By default LAN and WAN interfaces are not activated.
- Configured with the clock rate command on the Serial cable end labeled DCE.

Optional description can be included.

Configure the G0/0 Interface


```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Jan 30 22:04:47.551: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#
```

Configure an IPv6 Router Interface

Configure interface with IPv6 address and subnet mask:

- Use the **ipv6 address** *ipv6-address*/*ipv6-length* [link-local | eui-64]interface configuration command.
- Activate using the **no shutdown** command.

Configure the R1 G0/0 Interface

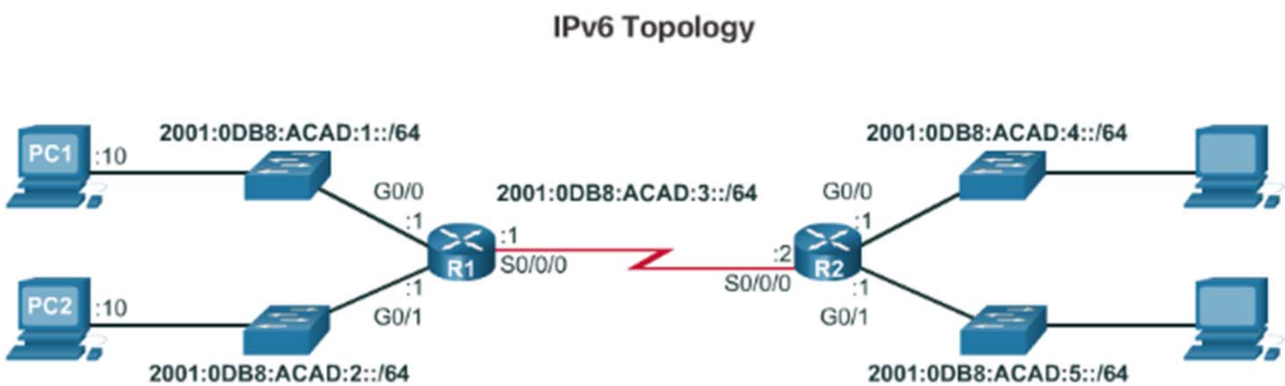

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#description Link to LAN 1
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Feb  3 21:38:37.279: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
*Feb  3 21:38:40.967: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

Router Basic Settings

Configure an IPv6 Router Interface (cont.)

IPv6 interfaces can support more than one address:

- Configure a specified global unicast – **ipv6address** *ipv6-address /ipv6-length*
- Configure a global IPv6 address with an interface identifier (ID) in the low-order 64 bits - **ipv6address** *ipv6-address /ipv6-length* eui-64
- Configure a link-local address - **ipv6address** *ipv6-address /ipv6-length* link-local



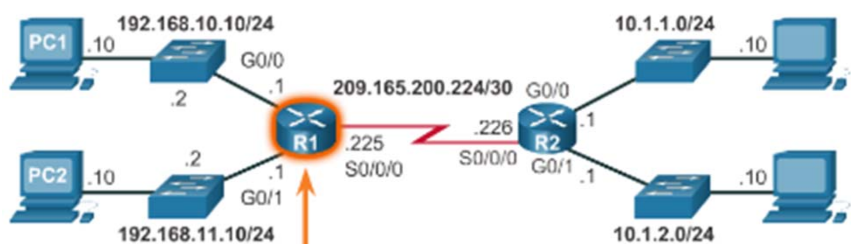
Router Basic Settings

Configure an IPv4 Loopback Interface

A loopback interface is a logical interface that is internal to the router:

- It is not assigned to a physical port, it is considered a software interface that is automatically in an UP state.
- A loopback interface is useful for testing.
- It is important in the OSPF routing process.

Configure the Loopback0 Interface




```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface loopback0,
changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface loopback0, changed state to up
```

Verify Connectivity of Directly Connected Networks
Verify Interface Settings

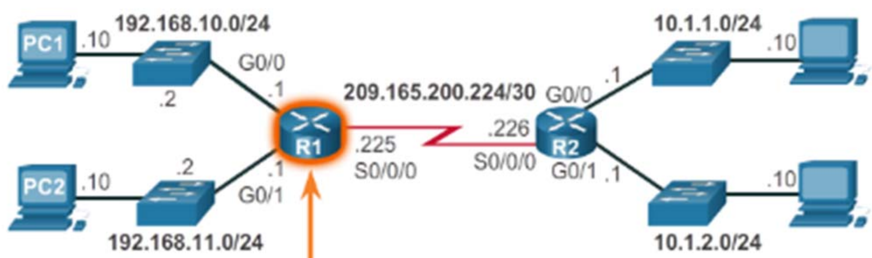
Show commands are used to verify operation and configuration of interface:

- **show ip interfaces brief**
- **show ip route**
- **show running-config**

Show commands that are used to gather more detailed interface information:

- **show interfaces**
- **show ip interfaces**

Display Interface Summaries

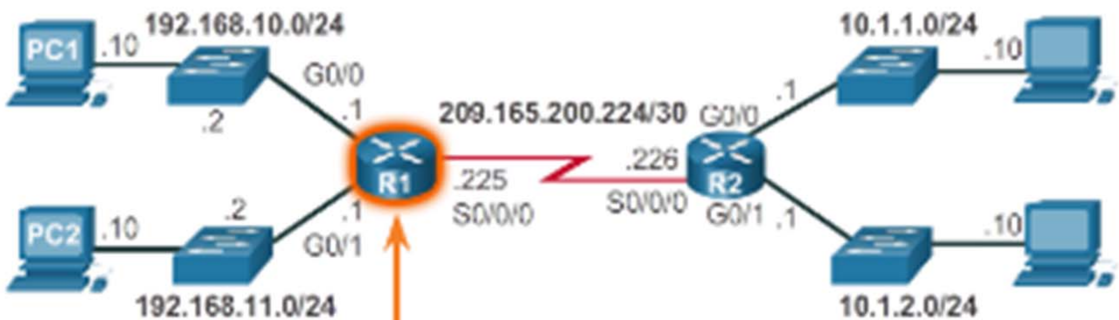



```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225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

Verify Connectivity of Directly Connected Networks

Verify Interface Settings (cont.)

Verify the Routing Table




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mo

<output omitted>

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.10.0/24 is directly connected, GigabitEther
L        192.168.10.1/32 is directly connected, GigabitEther
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.11.0/24 is directly connected, GigabitEther
L        192.168.11.1/32 is directly connected, GigabitEther
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 m
```

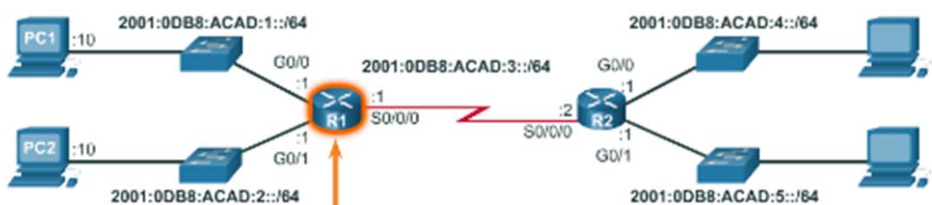
Verify Connectivity of Directly Connected Networks

Verify IPv6 Interface Settings

Common commands to verify the IPv6 interface configuration:

- **show ipv6 interface brief -** displays a summary for each of the interfaces.
- **show ipv6 interface gigabitethernet 0/0 -** displays the interface status and all the IPv6 addresses for this interface.
- **show ipv6 route -** verifies that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table.

Verify Connectivity on 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#
```

Verify Connectivity of Directly Connected Networks

Filter Show Command Output

Show command output can be managed using the following command and filters:

- Use the **terminal length** *number* command to specify the number of lines to be displayed.
- To filter specific output of commands use the **(|)pipe character** after show command. Parameters that can be used after pipe include:
  - **section, include, exclude, begin**

Filtering Show Commands

```
R1# show running-config | section line vty
line vty 0 4
 password 7 030752180500
 login
 transport input all
R1#
```

Filtering Show Commands

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ
R1#
R1# show ip interface brief | include up
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
R1#
```

Verify Connectivity of Directly Connected Networks

Command History Feature

The command history feature temporarily stores a list of executed commands for access:

- To recall commands press **Ctrl+P** or the **UP Arrow**.
- To return to more recent commands press **Ctrl+N** or the **Down Arrow**.
- By default, command history is enabled and the system captures the last 10 commands in the buffer. Use the **show history** privileged EXEC command to display the buffer contents.
- Use the **terminal history size** user EXEC command to increase or decrease size of the buffer.

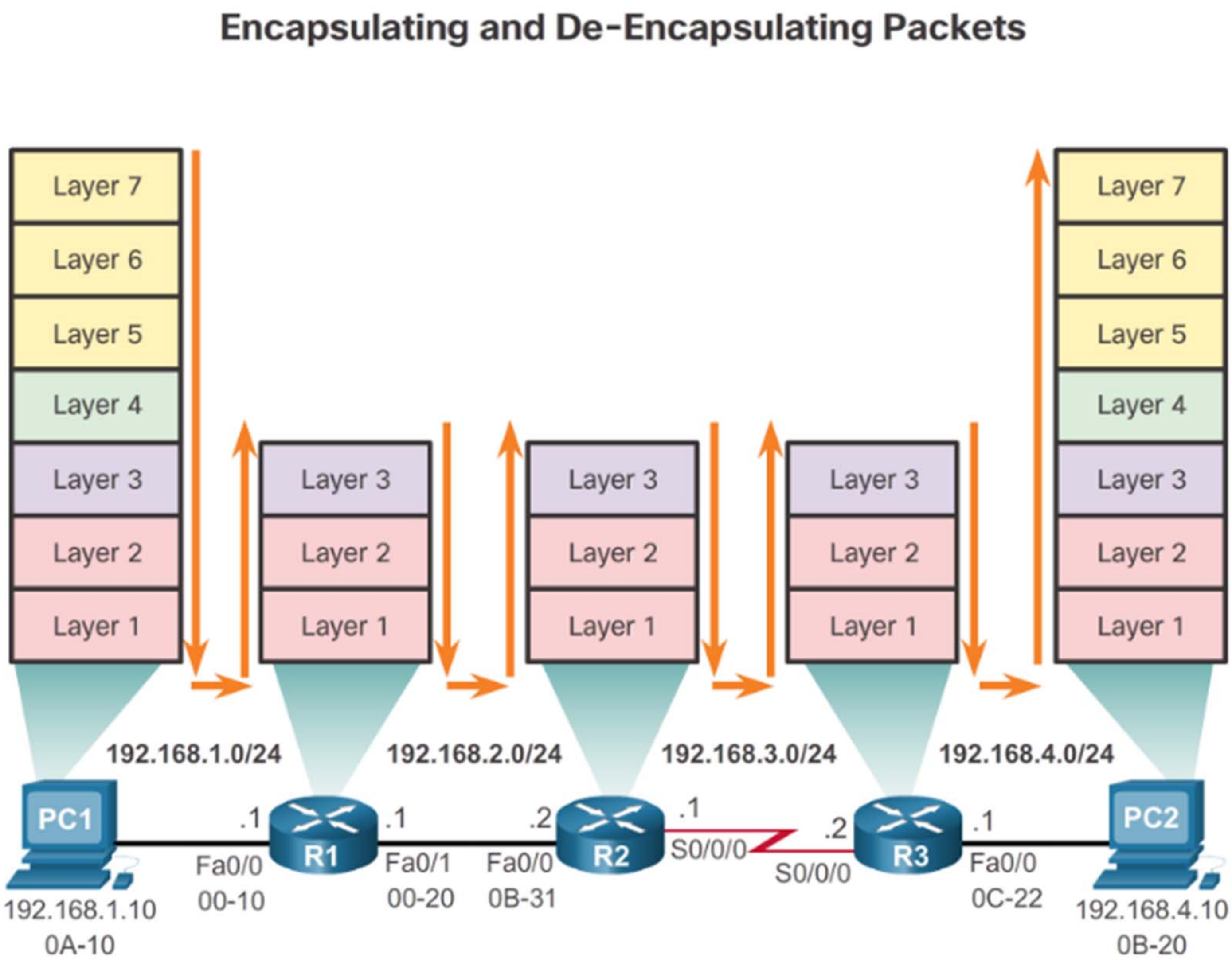
```
R1# terminal history size 200
R1#
R1# show history
  show ip interface brief
  show interface g0/0
  show ip interface g0/1
  show ip route
  show ip route 209.165.200.224
  show running-config interface s0/0/0
  terminal history size 200
  show history
R1#
```

1.2 Routing Decisions

Cisco | Networking Academy®
Mind Wide Open™

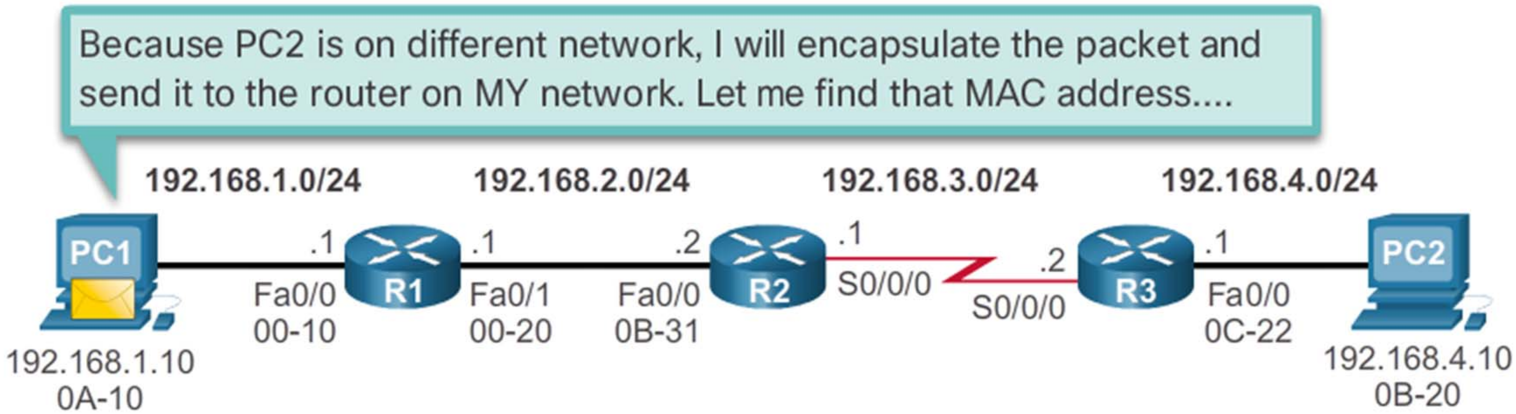
Switching Packets Between Networks

Router Switching Function



Switching Packets Between Networks
Send a Packet

PC1 Sends a Packet to PC2



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

Dest. MAC 00-10	Source MAC 0A-10	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

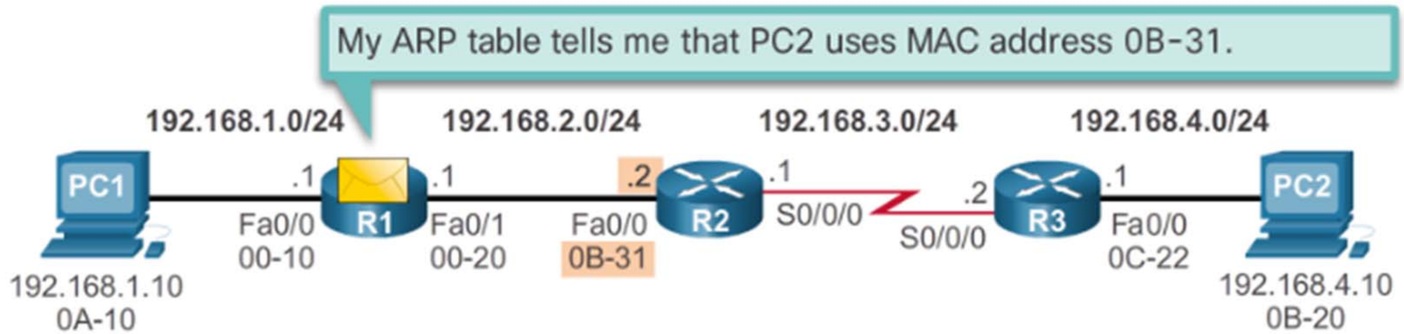
PC1's ARP Cache for R1

IP Address	MAC Address
192.168.1.1	00-10

Switching Packets Between Networks

Forward to Next Hop

R1 Forwards the Packet to PC2



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

Dest. MAC 0B-31		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R1's ARP Cache

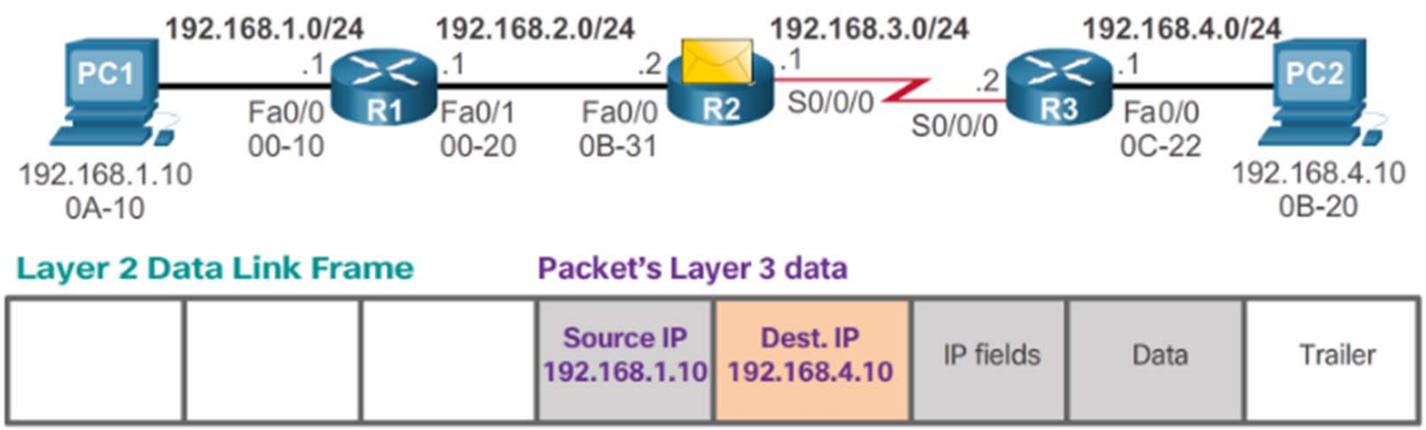
IP Address	MAC Address
192.168.2.2	0B-31

R1's Routing Table

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

Switching Packets Between Networks
Packet Routing

R2 Forwards the Packet to R3

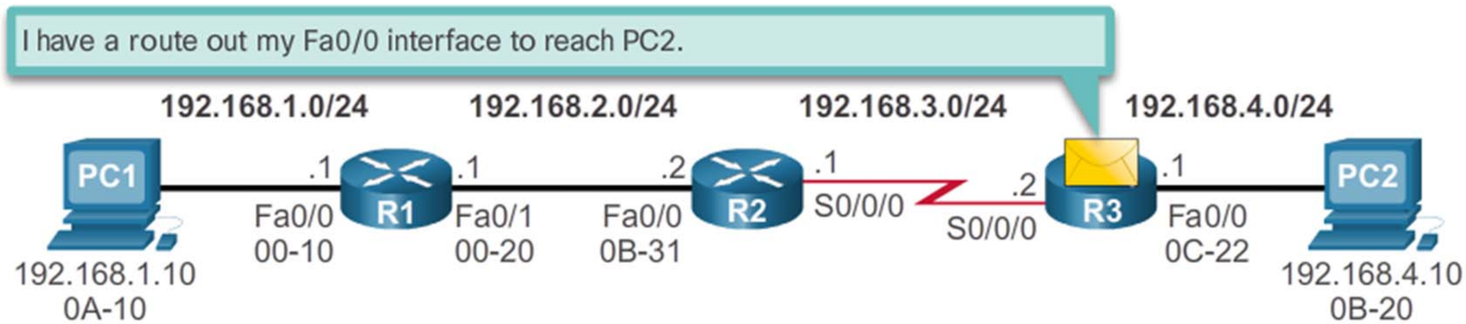


R2's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	Fa/0/0
192.168.2.0/24	0	Dir. Connect.	Fa/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.162.3.2	S0/0/0

Switching Packets Between Networks
Reach the Destination

R3 Forwards the Packet to PC2



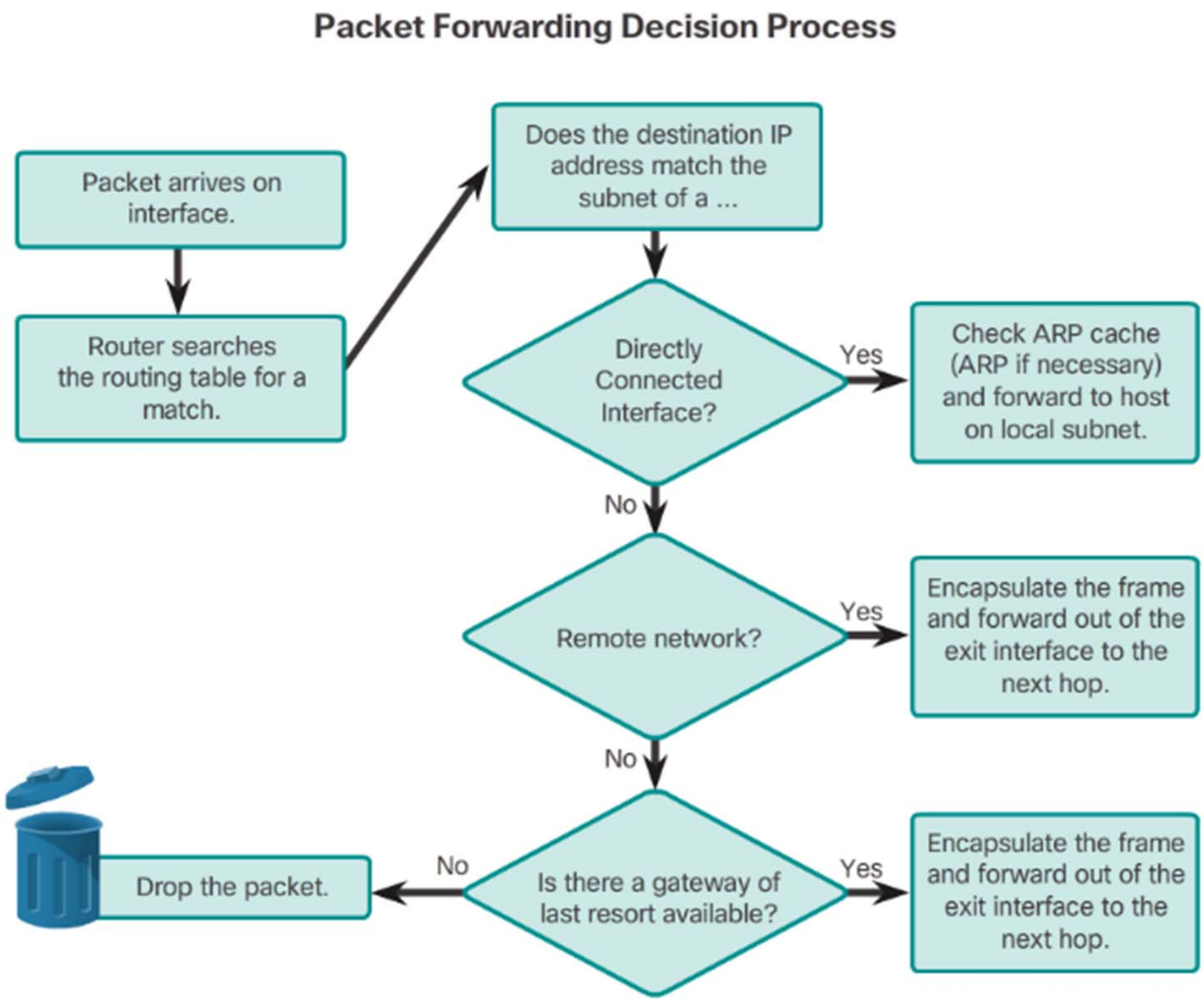
Layer 2 Data Link Frame — **Packet's Layer 3 data**

		Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	0	Dir. Connect.	Fa0/0

Path Determination
Routing Decisions



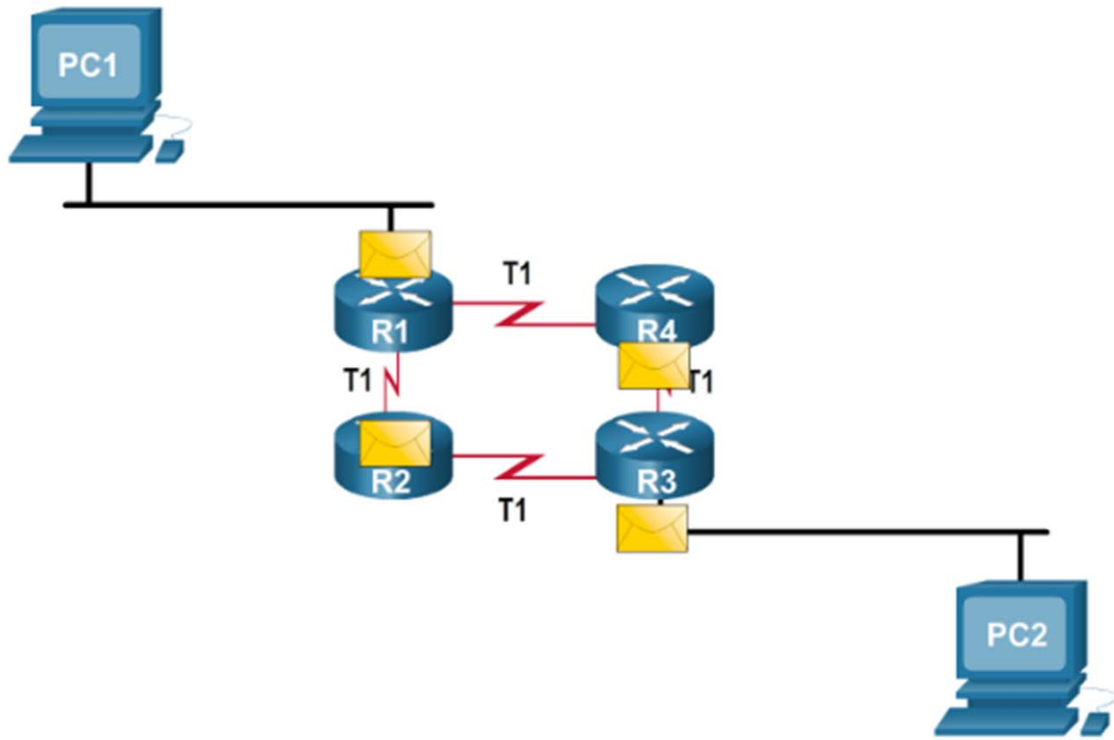
Path Determination
Best Path

- **Best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network**:
  - A metric is the value used to measure the distance to a given network.
  - Best path to a network is the path with the lowest metric.
- **Dynamic routing protocols use their own rules and metrics to build and update routing tables**:
  - Routing Information Protocol (RIP) - Hop count
  - Open Shortest Path First (OSPF) - Cost based on cumulative bandwidth from source to destination
  - Enhanced Interior Gateway Routing Protocol (EIGRP) - Bandwidth, delay, load, reliability

Path Determination

Load Balancing

- When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally:
  - o Equal cost load balancing can improve network performance.
  - o Equal cost load balancing can be configured to use both dynamic routing protocols and static routes.



Path Determination

Administrative Distance

- If multiple paths to a destination are configured on a router, the path installed in the routing table is the one with the lowest Administrative Distance (AD):
  - A static route with an AD of 1 is more reliable than an EIGRP-discovered route with an AD of 90.
  - A directly connected route with an AD of 0 is more reliable than a static route with an AD of 1.

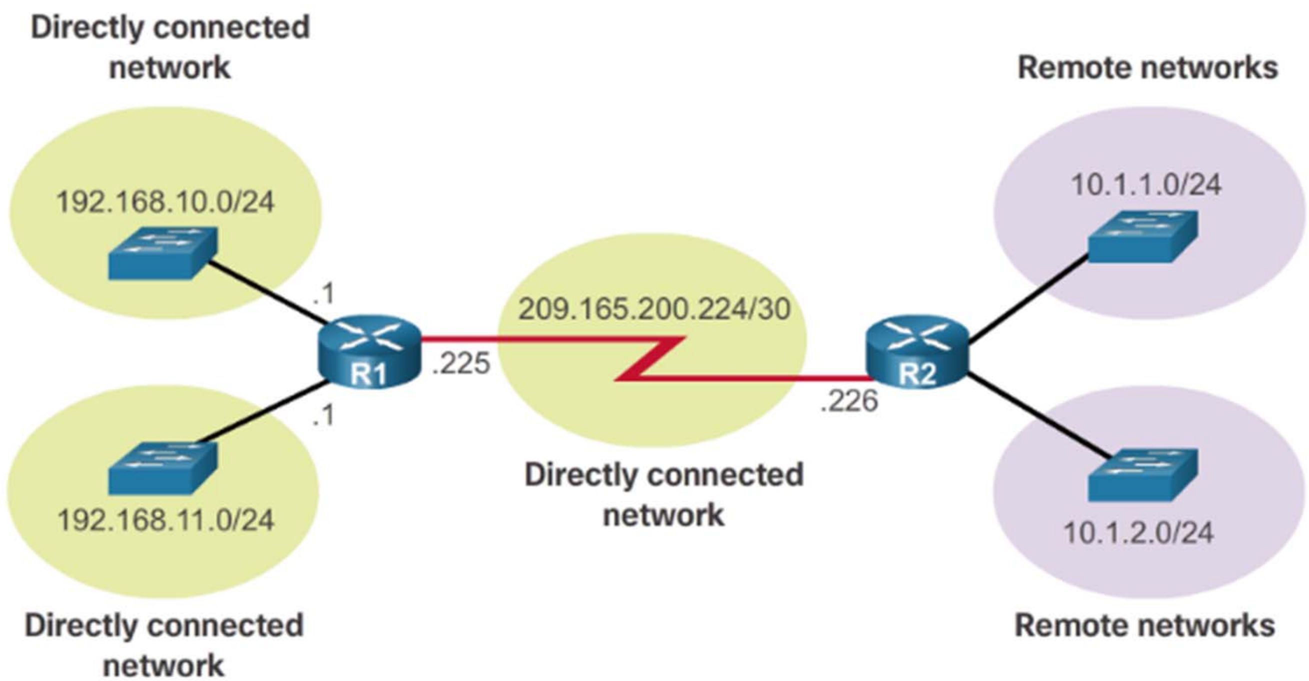
Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

1.3 Router Operation

Cisco | Networking Academy®
Mind Wide Open™

The Routing Table

- A routing table is a file stored in RAM that contains information about:
  - Directly connected routes
  - Remote routes



Routing Table Sources

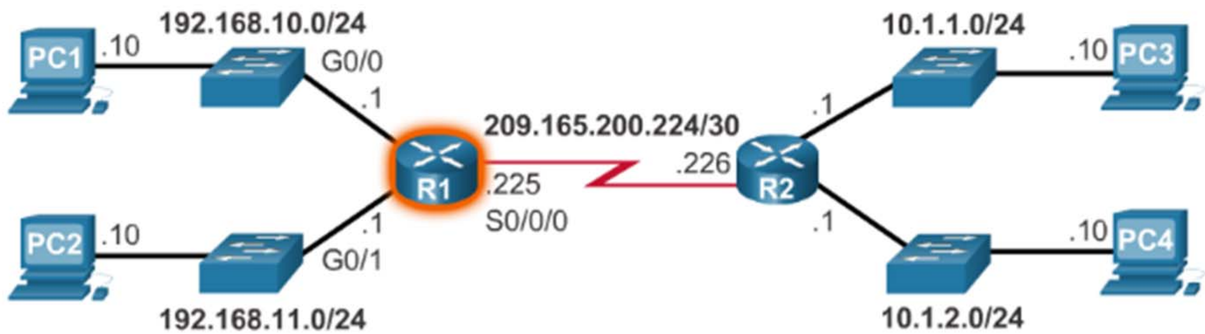
The **show ip route** command is used to display the contents of the routing table:

- **Local route interfaces -** Added to the routing table when an interface is configured. (displayed in IOS 15 or newer for IPv4 routes and all IOS releases for IPv6 routes.)
- **Directly connected interfaces -** Added to the routing table when an interface is configured and active.
- **Static routes -** Added when a route is manually configured and the exit interface is active.
- **Dynamic routing protocol -** Added when EIGRP or OSPF are implemented and networks are identified.

Analyze the Routing Table

Routing Table Sources (cont.)

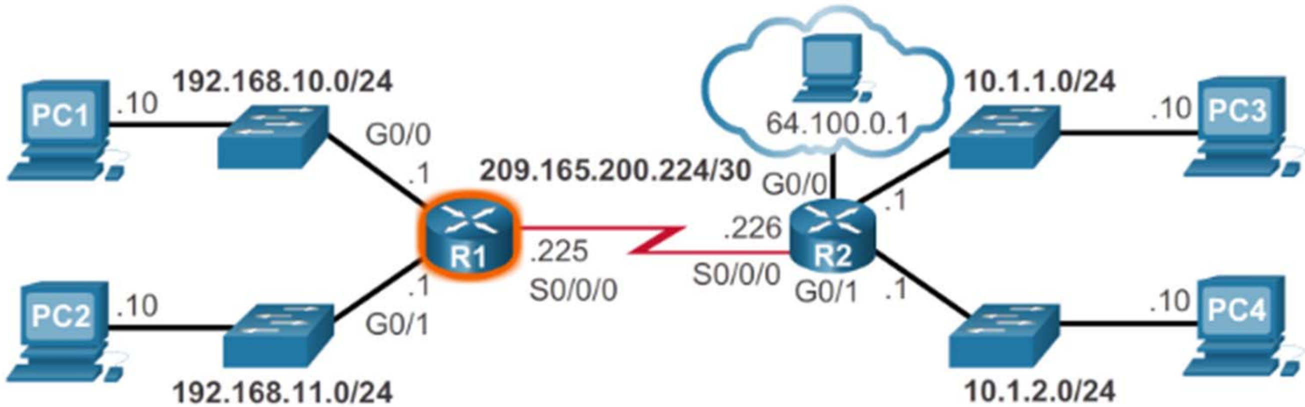
Routing Table of R1




```
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, 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
     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,
```

Remote Network Routing Entries

Interpreting the entries in the routing table



D	10.1.1.0/24	[	90	/2170112]	via	209.165.200.226,	00:00:05,	Serial0/0/0

Legend

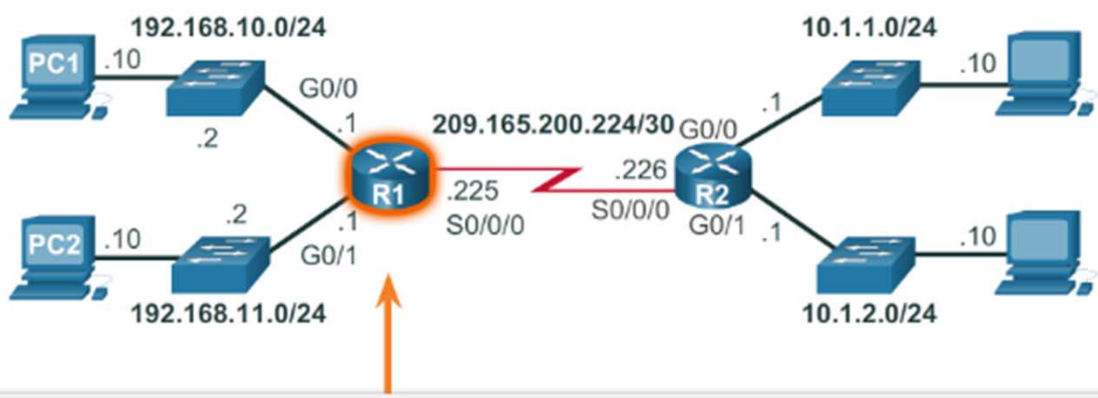
- Identifies how the network was learned by the router.
- Identifies the destination network.
- Identifies the administrative distance (trustworthiness) of the route source.
- Identifies the metric to reach the remote network.
- Identifies the next-hop IP address to reach the remote network.
- Identifies the amout of elapsed time since the network was discovered.
- Identifies the outgoing interface on the router to reach the destination network.

Directly Connected Routes

Directly Connected Interfaces

A newly deployed router, without any configured interfaces, has an empty routing table.

Empty Routing Table

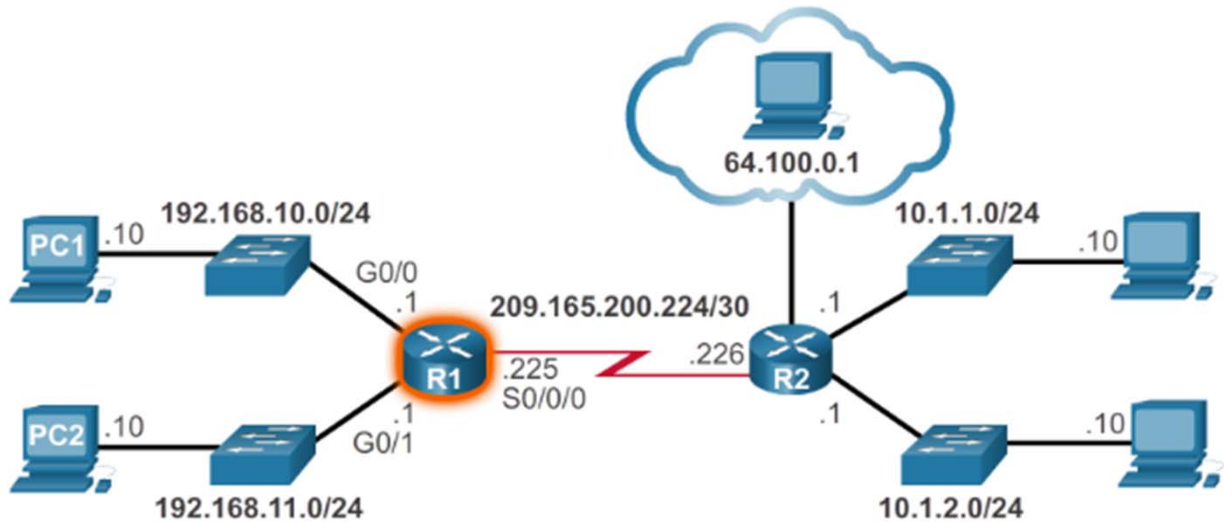



```
R1# show ip route
Codes:L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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#
```

Directly Connected Routes

Directly Connected Routing Table Entries

Directly Connected Network Entry Identifiers



A	B	C
C	192.168.10.0/24 is directly connected,	GigabitEthernet0/0
L	192.168.10.1/32 is directly connected,	GigabitEthernet0/0

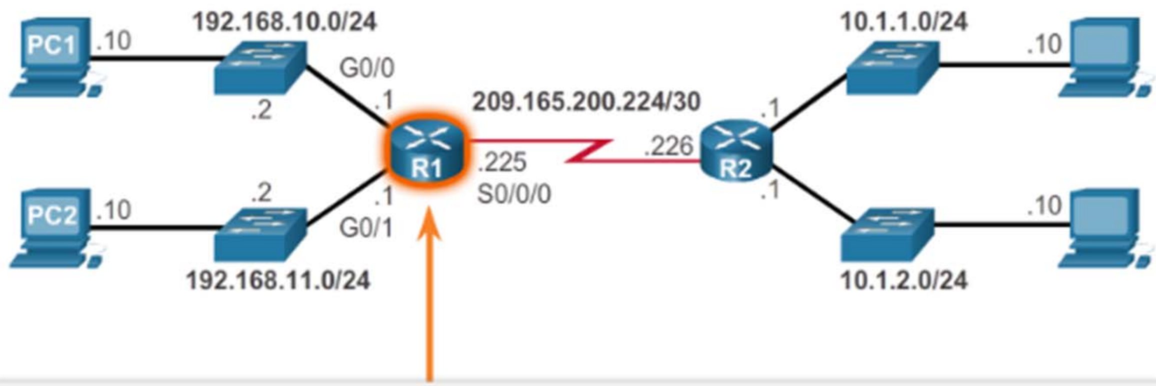
Legend

- (green) - Identifies how the network was learned by the router.
- (pink) - Identifies the destination network and how it is connected.
- (orange) - Identifies the interface on the router connected to the destination network.

Directly Connected Routes

Directly Connected Example

Verifying the Directly Connected Routing Table Entries

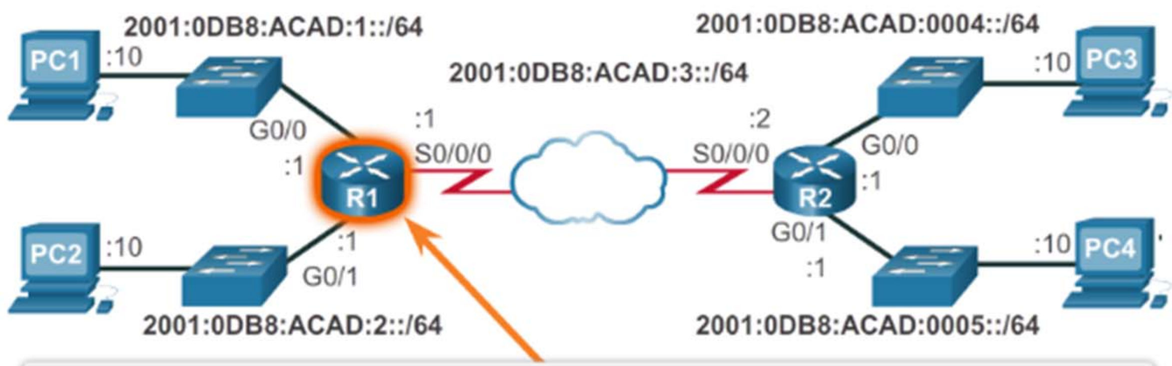



```
R1# show ip route | begin Gateway
Gateway of last resort is not set

      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
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 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#
```

Directly Connected Routes

Directly Connected IPv6 Example

Show the IPv6 Route Table




```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route, B - BGP, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default
       NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2
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
```

Static Routes

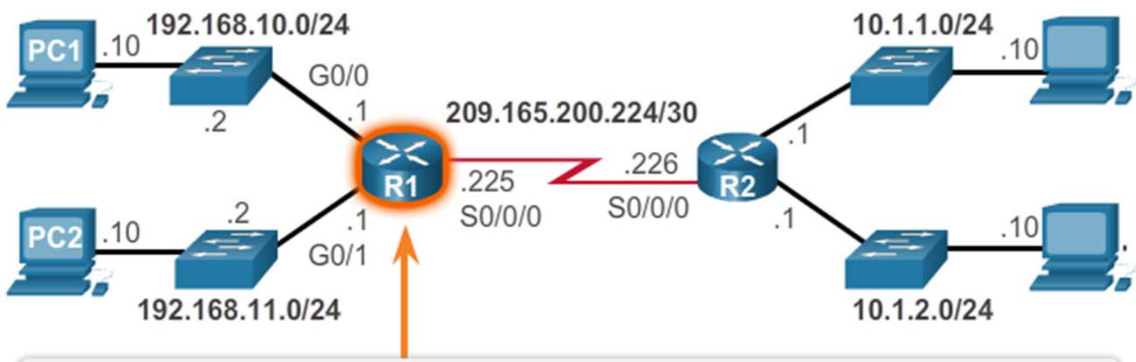
Static routes and default static routes can be implemented after directly connected interfaces are added to the routing table:

- Static routes are manually configured.
- They define an explicit path between two networking devices.
- Static routes must be manually updated if the topology changes.
- Their benefits include improved security and control of resources.
- Configure a static route to a specific network using the **ip route** *network mask* **{***next-hop-ip* **|** *exit-intf***}** command**.**
- A default static route is used when the routing table does not contain a path for a destination network.
- Configure a default static route using the **ip route** 0.0.0.0 0.0.0.0 {*exit-intf* | *next-hop-ip*} command.

Statically Learned Routes

Static Route Example

Entering and Verifying a Static Default Route

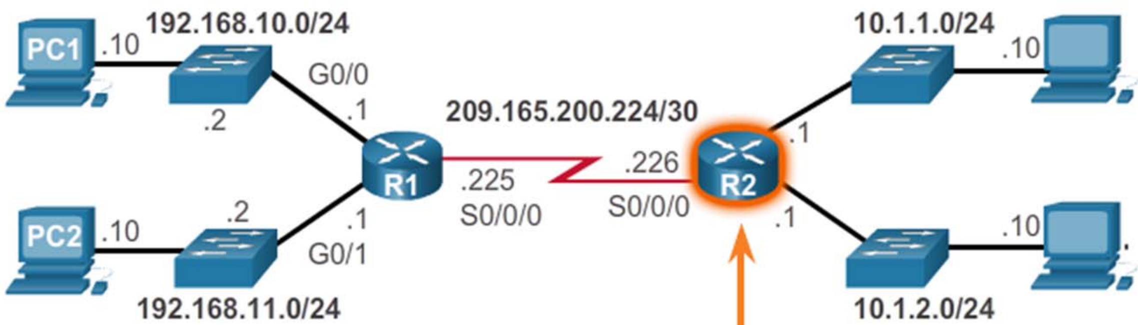



```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)# exit
R1#
*Feb  1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console
by console

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
L     192.168.11.1/32 is directly connected, GigabitEthernet0/1
```

Statically Learned Routes

Static Route Example (cont.)

Entering and Verifying a Static Route

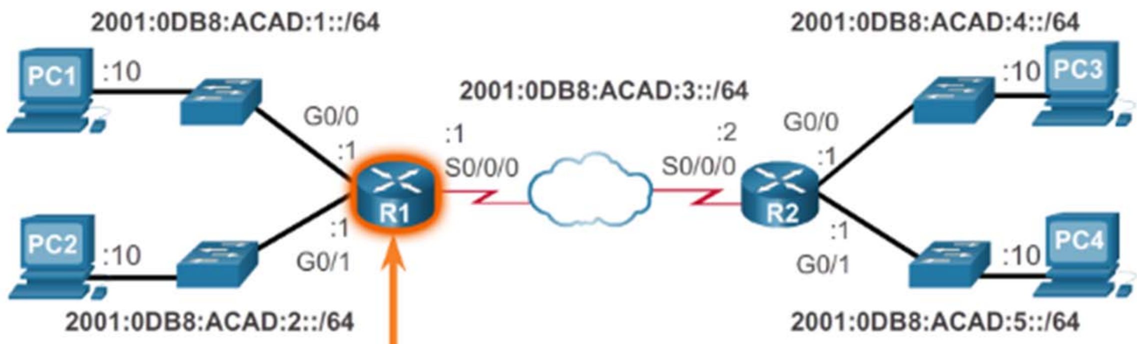



```
R2(config)# ip route 192.168.10.0 255.255.255.0 s0/0/0
R2(config)# ip route 192.168.11.0 255.255.255.0 209.165.200.225
R2(config)# exit
R2#
R2# show ip route | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C     10.1.1.0/24 is directly connected, GigabitEthernet0/0
L     10.1.1.1/32 is directly connected, GigabitEthernet0/0
C     10.1.2.0/24 is directly connected, GigabitEthernet0/1
L     10.1.2.1/32 is directly connected, GigabitEthernet0/1
S    192.168.10.0/24 is directly connected, Serial0/0/0
S    192.168.11.0/24 [1/0] via 209.165.200.225
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
```

Statically Learned Routes

Static IPv6 Route Examples

Entering and Verifying an IPv6 Static Default Route



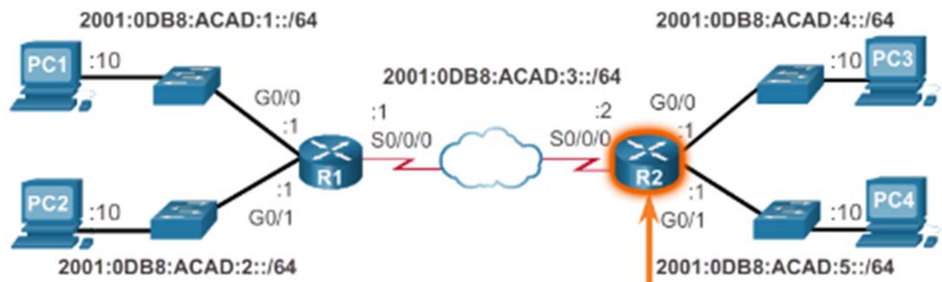

```
R1(config)# ipv6 route ::/0 s0/0/0
R1(config)# exit
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
       D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
       DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter,
       OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via Serial0/0/0, directly connected
C   2001:0DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
```

Statically Learned Routes

Static IPv6 Route Examples

Entering and Verifying IPv6 Static Routes



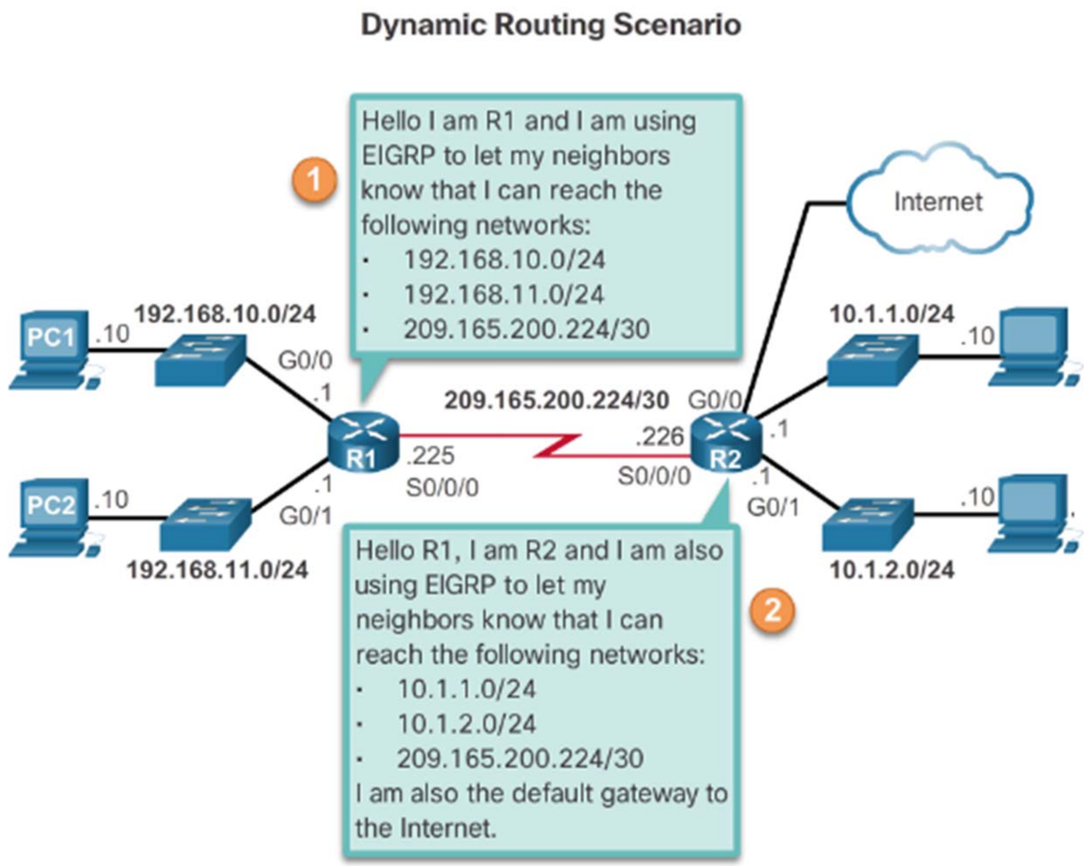

```
R2(config)# ipv6 route 2001:0DB8:ACAD:1::/64 2001:0DB8:ACAD:3::1
R2(config)# ipv6 route 2001:0DB8:ACAD:2::/64 s0/0/0
R2(config)# ^Z
R2#
```

```
R2# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
       D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
       DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter,
       OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2001:0DB8:ACAD:1::/64 [1/0]
     via 2001:DB8:ACAD:3::1
S   2001:0DB8:ACAD:2::/64 [1/0]
     via Serial0/0/0, directly connected
```

Dynamic Routing Protocols

Dynamic Routing

- Dynamic routing is used by routers to share information about the reachability and status of remote networks.
- It performs network discovery and maintains routing tables.
- Routers have converged after they have finished exchanging and updating their routing tables.



Dynamic Routing Protocols

IPv4 Routing Protocols

Cisco routers can support a variety of dynamic IPv4 routing protocols including:

- **EIGRP –** Enhanced Interior Gateway Routing Protocol
- **OSPF –** Open Shortest Path First
- **IS-IS –** Intermediate System-to-Intermediate System
- **RIP –** Routing Information Protocol

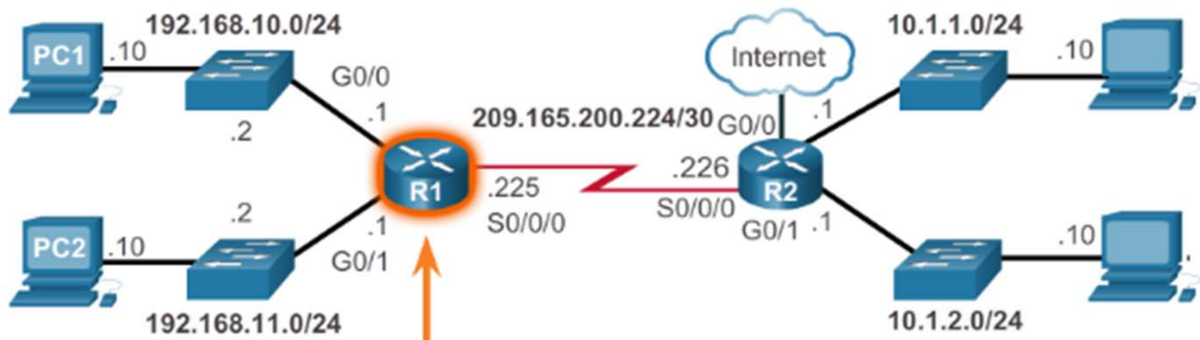
Use the **router ?** Command in global configuration mode to determine which routing protocols are supported by the IOS.

```
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
```

Dynamic Routing Protocols

IPv4 Dynamic Routing Examples

Verify Dynamic Routes




```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/2297856] via 209.165.200.226, 00:07:29, Serial0/0/0
      10.0.0.0/24 is subnetted, 2 subnets
D        10.1.1.0 [90/2172416] via 209.165.200.226, 00:07:29, Serial0/0/0
D        10.1.2.0 [90/2172416] via 209.165.200.226, 00:07:29, 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
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 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#
```

Dynamic Routing Protocols
IPv6 Routing Protocols

Cisco routers can support a variety of dynamic IPv6 routing protocols including:

- **RIPng (**RIP next generation)
- **OSPFv3**
- **EIGRP** for IPv6

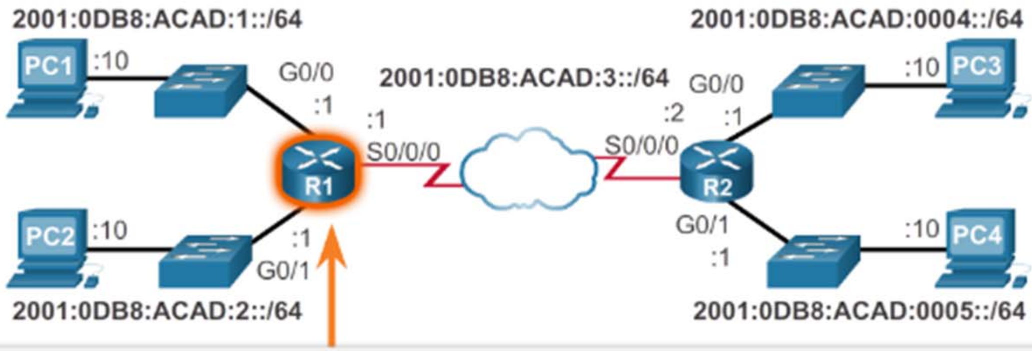
Use the **ipv6 router ?** command to determine which routing protocols are supported by the IOS

```
R1(config)# ipv6 router ?
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf       Open Shortest Path First (OSPF)
  rip        IPv6 Routing Information Protocol (RIPv6)

R1(config)# router
```

Dynamic Routing Protocols

IPv6 Dynamic Routing Examples

Verify Dynamic Routes




```
R1# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

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
D   2001:DB8:ACAD:4::/64 [90/2172416]
     via FE80::D68C:B5FF:FECE:A120, Serial0/0/0
D   2001:DB8:ACAD:5::/64 [90/2172416]
     via FE80::D68C:B5FF:FECE:A120, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

1.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary

Summary

- Describe the primary functions and features of a router.
- 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.
- 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.
- Explain how a router learns about remote networks when operating in a small to medium-sized business network.
- 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.

Section 1.1

New Terms and Commands

- Topology
- Speed
- Cost
- Security
- Availability
- Scalability
- Reliability
- Point-to-Point Protocol (PPP)
- Process Switching
- Fast switching
- Cisco Express Forwarding (CEF)
- Wireless access points (WAPs)

- Edge router
- Gateway of Last Resort
- Topology diagram
- Secure Shell (SSH)
- Hypertext Transfer Protocol Secure (HTTPS)
- Console cable
- Terminal emulation software - Tera Term, PuTTY, HyperTerminal
- Secure management access
- **Ipv6 address** *ipv6-address/ipv6-length* [link-local | eui-64] interface configuration command.

- **no shutdown** command
- loopback interface
- **interface loopback** *number command*
- **show ip route** command
- **show running-config** interface*interface-id*
- **show ip interface brief** command
- **show running-config** *interface* command
- **show ip interfaces** command
- **Show ipv6 interface** command

Section 1.1 (cont.)

New Terms and Commands

- **show interfaces** command
- **show ipv6 interface brief** command
- **show ipv6 route** command
- pipe (**|**) character
- Ctrl+P
- Ctrl+N
- **show history**
- **terminal history**

Section 1.2

New Terms and Commands

- Metrics
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- load balancing
- IS-IS - Intermediate System-to-Intermediate System
- RIPng (RIP next generation)
- OSPFv3

Section 1.3

New Terms and Commands

- Administrative Distance (AD)
- Local Route interfaces
- Static routes
- Route timestamp
- Route source
- **ip route** *network mask* { *next-hop-ip* | *exit-intf* }
- **ip route 0.0.0.0 0.0.0.0** { *exit-intf* | *next-hop-ip* }
- **ipv6 unicast-routing**
- **ipv6 route ::/0** {*ipv6-address* | *interface-type interface-number*}
- **ipv6 route** *ipv6-prefix/prefix-length* {*ipv6-address*|*interface-type interface-number*}
- **Router ?** command
- **Ipv6 router ?** command

Cisco | Networking Academy®
Mind Wide Open™

Instructor Materials
Chapter 2: Static Routing

CCNA Routing and Switching

Introduction to Networks v6.0

Cisco | Networking Academy®
Mind Wide Open™

Instructor Materials – Chapter 2 Planning Guide

This PowerPoint deck is divided in two parts:

1. Instructor Planning Guide
   - Information to help you become familiar with the chapter
   - Teaching aids
2. Instructor Class Presentation
   - Optional slides that you can use in the classroom
   - Begins on slide # 15

Note: Remove the Planning Guide from this presentation before sharing with anyone.

Routing and Switching Essentials 6.0 Planning Guide
Chapter 2: Static Routing

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
2.0.1.2	Class Activity	Which Way Should We Go?	Optional
2.1.1.4	Class Activity	Identify the Advantages and Disadvantages of Static Routing	-
2.1.2.6	Class Activity	Identify the Type of Static Route	-
2.2.1.3	Syntax Checker	Configuring Next-hop Static Routes on R2 (Fig.3)	Recommended
2.2.1.3	Syntax Checker	Configuring Next-Hop Static Routes on R3 (Fig.4)	-
2.2.1.4	Syntax Checker	Configure Directly Connected Static Routes on R2 (Fig. 3)	Recommended
2.2.1.4	Syntax Checker	Configure Directly Connected Static Routes on R3 (Fig.4)	-
2.2.1.5	Syntax Checker	Configure Fully Specified Static Routes on R2 (Fig. 3)	-
2.2.1.5	Syntax Checker	Configure Fully Specified Static Routes on R3 (Fig.4)	-

Chapter 2: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
2.2.1.6	Syntax Checker	Verify the Static Routing Settings on R2 (Fig. 4)	-
2.2.1.6	Syntax Checker	Verify the Static Routing Settings on R3 (Fig. 5)	-
2.2.2.4	Packet Tracer	Configuring IPv4 Static and Default Routes	Recommended
2.2.2.5	Lab	Lab Configuring IPv4 Static and Default Routes	Optional
2.2.3.1	Syntax Checker	Enabling IPv6 Unicast Routing on R2 (Fig.3)	-
2.2.3.1	Syntax Checker	Enabling IPv6 Unicast Routing on R3 (Fig.4)	-
2.2.3.3	Syntax Checker	Configure Next-Hop Static IPv6 Routes on R2 (Fig.3)	-
2.2.3.3	Syntax Checker	Configure Next-Hop Static IPv6 Routes on R3 (Fig.4)	-
2.2.3.4	Syntax Checker	Configure Directly Connected Static IPv6 Routes on R2 (Fig.3)	-

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 2: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
2.2.3.4	Syntax Checker	Configure Directly Connected Static IPv6 Routes on R3 (Fig.4)	-
2.2.3.5	Syntax Checker	Configure a Fully Specified Static IPv6 Route on R2 (Fig.3)	-
2.2.4.4	Packet Tracer	Configuring IPv6 Static and Default Routes	Recommended
2.2.4.5	Lab	Configuring IPv6 Static and Default Routes	Optional
2.2.5.2	Syntax Checker	Configure a Floating Static Route on R3	-
2.2.5.4	Packet Tracer	Configuring Floating Static Routes	Recommended
2.2.6.2	Syntax Checker	Configure Host Static Routes (Fig.3)	-
2.3.2.3	Packet Tracer	Troubleshooting Static Routes	Recommended
2.3.2.4	Lab	Troubleshooting IPv4 and IPv6 Static Routes	Optional
2.4.1.1	Class Activity	Make It Static	Optional

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 2: Assessment

- Students should complete Chapter 2, “Assessment” after completing Chapter 2.
- Quizzes, labs, Packet Tracers, and other activities can be used to informally assess student progress.

Chapter 2: Best Practices

Prior to teaching Chapter 2, the instructor should:

- Complete Chapter 2, “Assessment.”
- The objectives of this chapter are:
  - Explain the advantages and disadvantages of static routing.
  - Explain the purpose of different types of static routes.
  - Configure IPv4 and IPv6 static routes by specifying a next-hop address.
  - Configure IPv4 and IPv6 default routes.
  - Configure a floating static route to provide a backup connection.
  - Configure IPv4 and IPv6 static host routes that direct traffic to a specific host.
  - Explain how a router processes packets when a static route is configured.
  - Troubleshoot common static and default route configuration issues.

Chapter 2: Best Practices (Cont.)

Section 2.1

- Routers learn about remote networks dynamically using routing protocols, or manually using static routes. In many cases, routers use a combination of both dynamic routing protocols and static routes. This chapter focuses on static routing.
- Static routes do not require the same amount of processing and overhead as dynamic routing protocols.
- Discuss the advantages and disadvantages of static routing.
- Point out where are and how static routes are used
  - Easy to maintain routing table in small networks that are not expected to grow.
  - Routing to and from stub networks.
  - Using a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.

Stress the advantages of static routing. It is easy for students to discount static routing in favor of dynamic.

Chapter 2: Best Practices (Cont.)

Section 2.1(cont.)

- Highlight the types of IPv4 and IPv6 static routes that will be examined in the chapter:
  - Standard static route
  - Default static route
  - Floating static route

Section 2.2

- Set up in Packet Tracer the sample topology that is used in the curriculum. Share with the students so that they can do the static route configurations “hands-on” as you demonstrate.
- Clarify the meaning of the terms next-hop and exit interface.
- Discuss the use of default routes and ask students to explain how default routes would be incorporated in their institution’s network?

Chapter 2: Best Practices (Cont.)

Section 2.2

- Encourage students to use the Syntax Checker activities to practice the new commands.
- Explain the necessity for using a fully specified static route which includes both the exit interface and the next-hop address. (Necessary with older IOS not using CEF)
- Demonstrate how to verify static routes using:
  - **show ip route**
  - **show ip route static**
  - **show ip route** *network*
  - **show ipv6 route**
  - **show ipv6 route static**
  - **show ipv6 route** *network*

Chapter 2: Best Practices (Cont.)

Section 2.2 (cont.)

- Discuss the use of Floating Static Routes as backup routes.
- Explain that the Cisco IOS automatically installs a local host route when an interface address is configured on the router. Indicated with an "L". Show this as it happens using Packet Tracer.
- Have students examine routing table output and identify the Static, Default and Local Host routes.

Section 2.3

- Demonstrate methodical troubleshooting of static routes using **ping**, **traceroute**, **show ip route**, **show ip interface brief** and **show cdp neighbors detail.**
- Provide students with as many opportunities as possible to hone their troubleshooting skills.

Chapter 2: Additional Help

- For additional help with teaching strategies, including lesson plans, analogies for difficult concepts, and discussion topics, visit the CCNA Community at: https://www.netacad.com/group/communities/community-home
- Best practices from around the world for teaching CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna-blog
- If you have lesson plans or resources that you would like to share, upload them to the CCNA Community in order to help other instructors.
- Students can enroll in **Packet Tracer Know How 1: Packet Tracer 101** (self-enroll)

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2: Static Routing

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2 - Sections & Objectives

2.1 Static Routing Implementation

- Explain the advantages and disadvantages of static routing.
- Explain the purpose of different types of static routes.

2.2 Configure Static and Default Routes

- Configure IPv4 and IPv6 static routes by specifying a next-hop address.
- Configure IPv4 and IPv6 default routes.
- Configure a floating static route to provide a backup connection.
- Configure IPv4 and IPv6 static host routes that direct traffic to a specific host

2.3 Troubleshoot Static and Default Route Issues

- Explain how a router processes packets when a static route is configured.
- Troubleshoot common static and default route configuration issues.

2.1 Static Routing Implementation

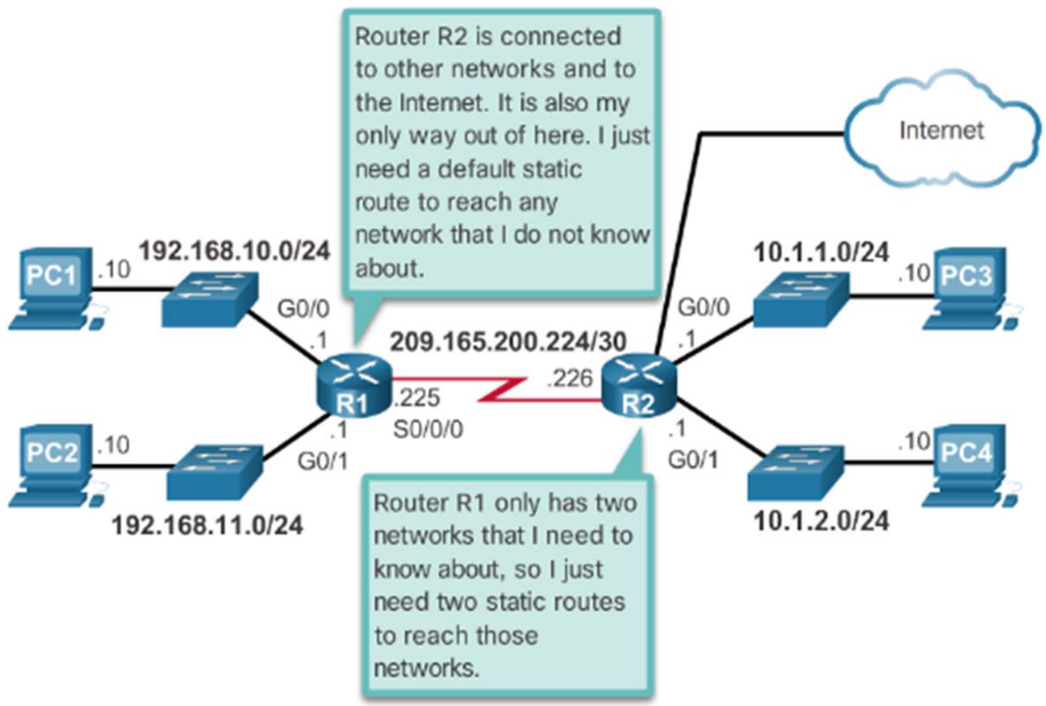
Cisco | Networking Academy®
Mind Wide Open™

Static Routing
Reach Remote Networks

A router can learn about remote networks in one of two ways:

- **Manually** - Remote networks are manually entered into the route table using static routes.
- **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

Static and Default Route Scenario



Static Routing

Why Use Static Routing?

Static routing provides some advantages over dynamic routing, including:

- Static routes are not advertised over the network, resulting in better security.
- Static routes use less bandwidth than dynamic routing protocols, no CPU cycles are used to calculate and communicate routes.
- The path a static route uses to send data is known.

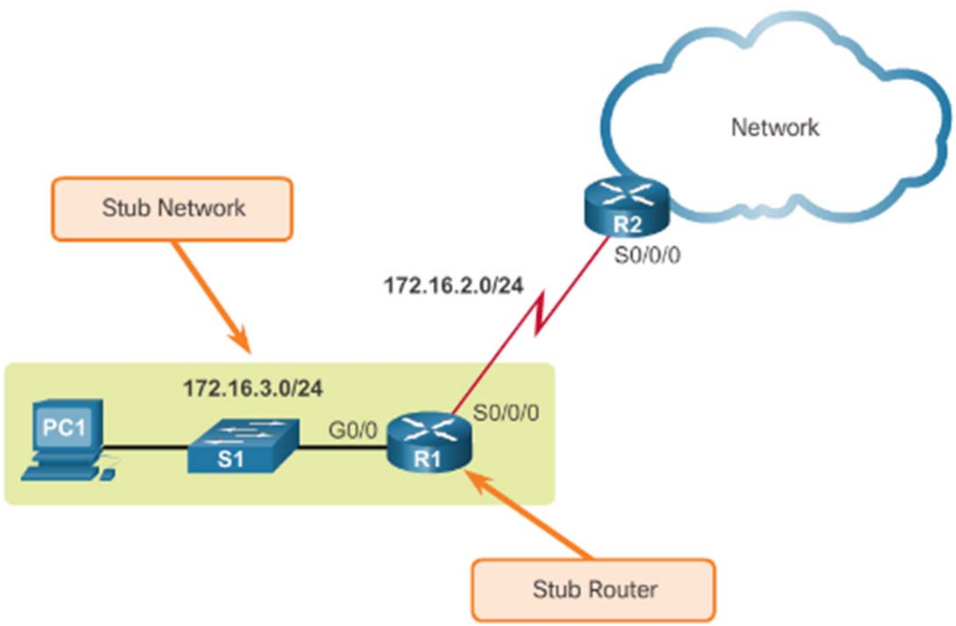
	Dynamic Routing	Static Routing
Configuration Complexity	Generally independent of the network size	Increases with network size
Topology Changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource Usage	Uses CPU, memory, link bandwith	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

Static Routing

When to Use Static Routes

Static routing has three primary uses:

- Providing ease of routing table maintenance in smaller networks.
- Routing to and from stub networks. A stub network is a network accessed by a single route, and the router has no other neighbors.
- Using a single default route to represent a path to any network that does not have a more specific match with another route in the routing table.



Types of Static Routes

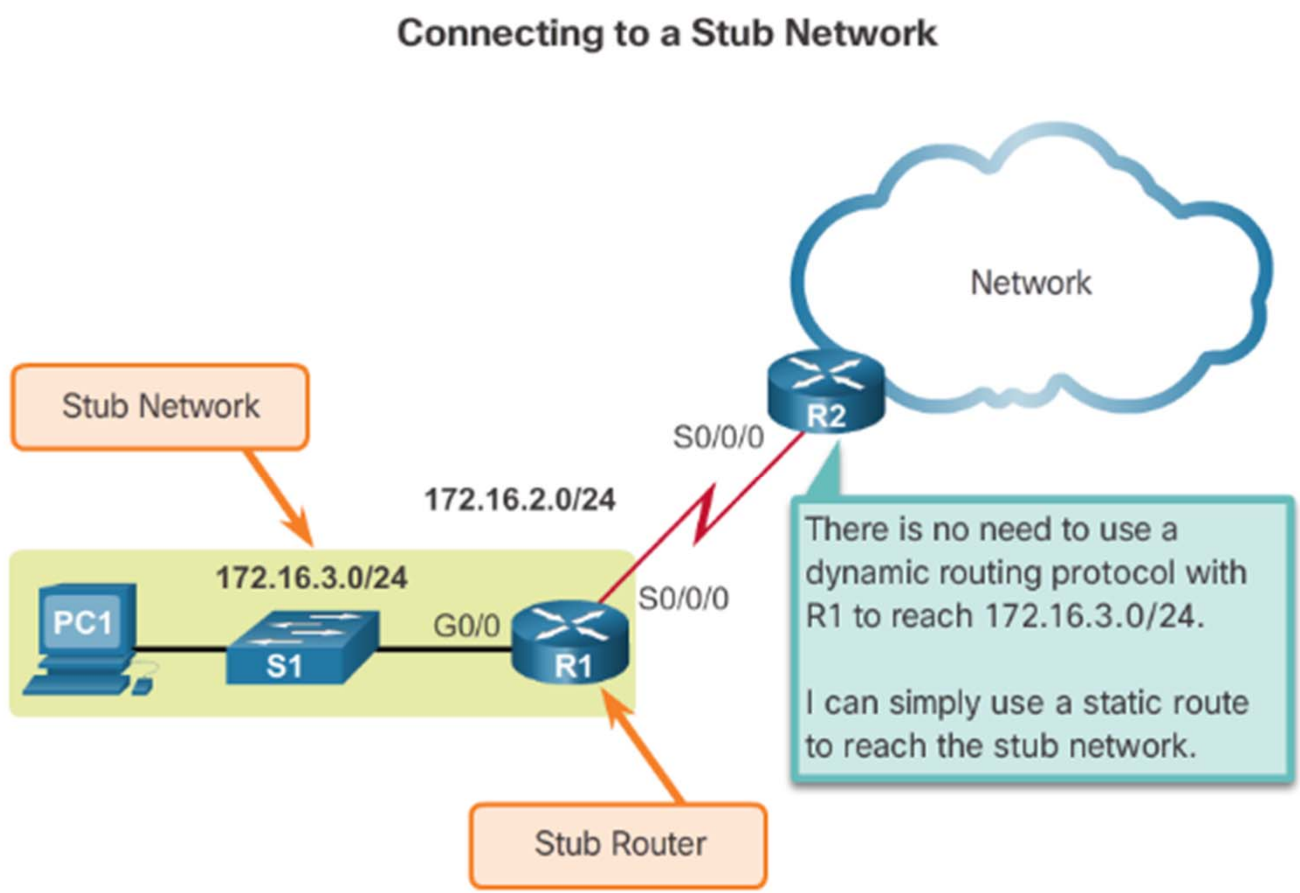
Static Route Applications

Static Routes are often used to:

- Connect to a specific network.
- Provide a Gateway of Last Resort for a stub network.
- Reduce the number of routes advertised by summarizing several contiguous networks as one static route.
- Create a backup route in case a primary route link fails.

Types of Static Routes

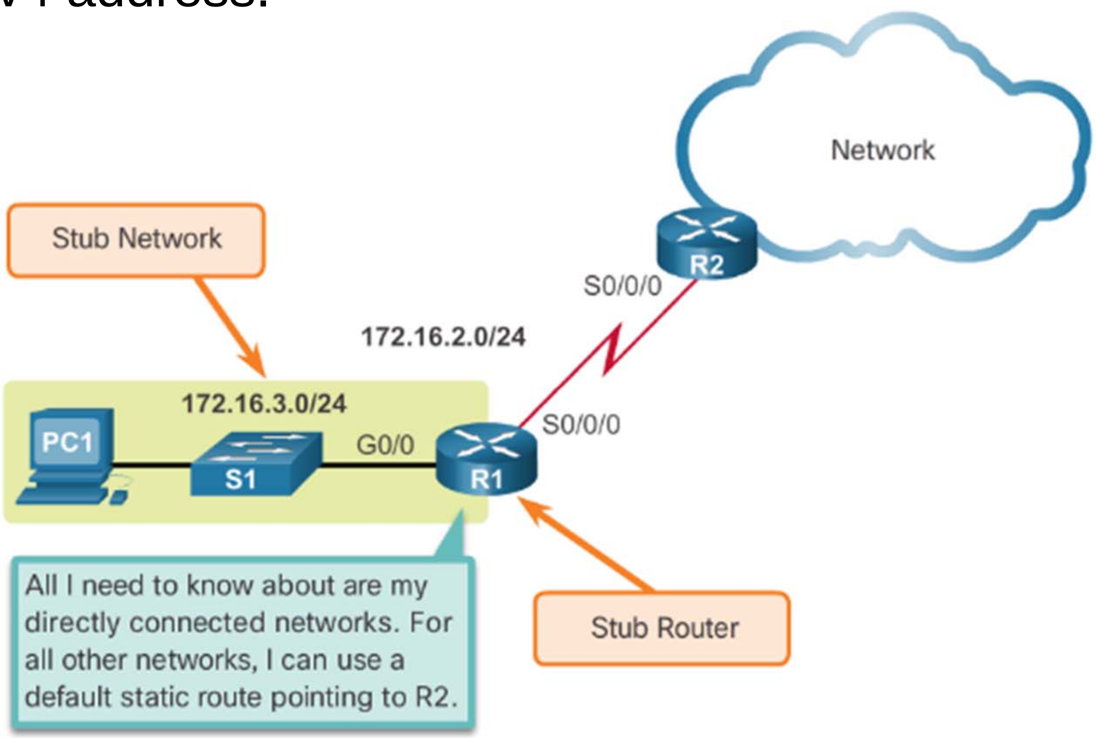
Standard Static Route



Types of Static Routes

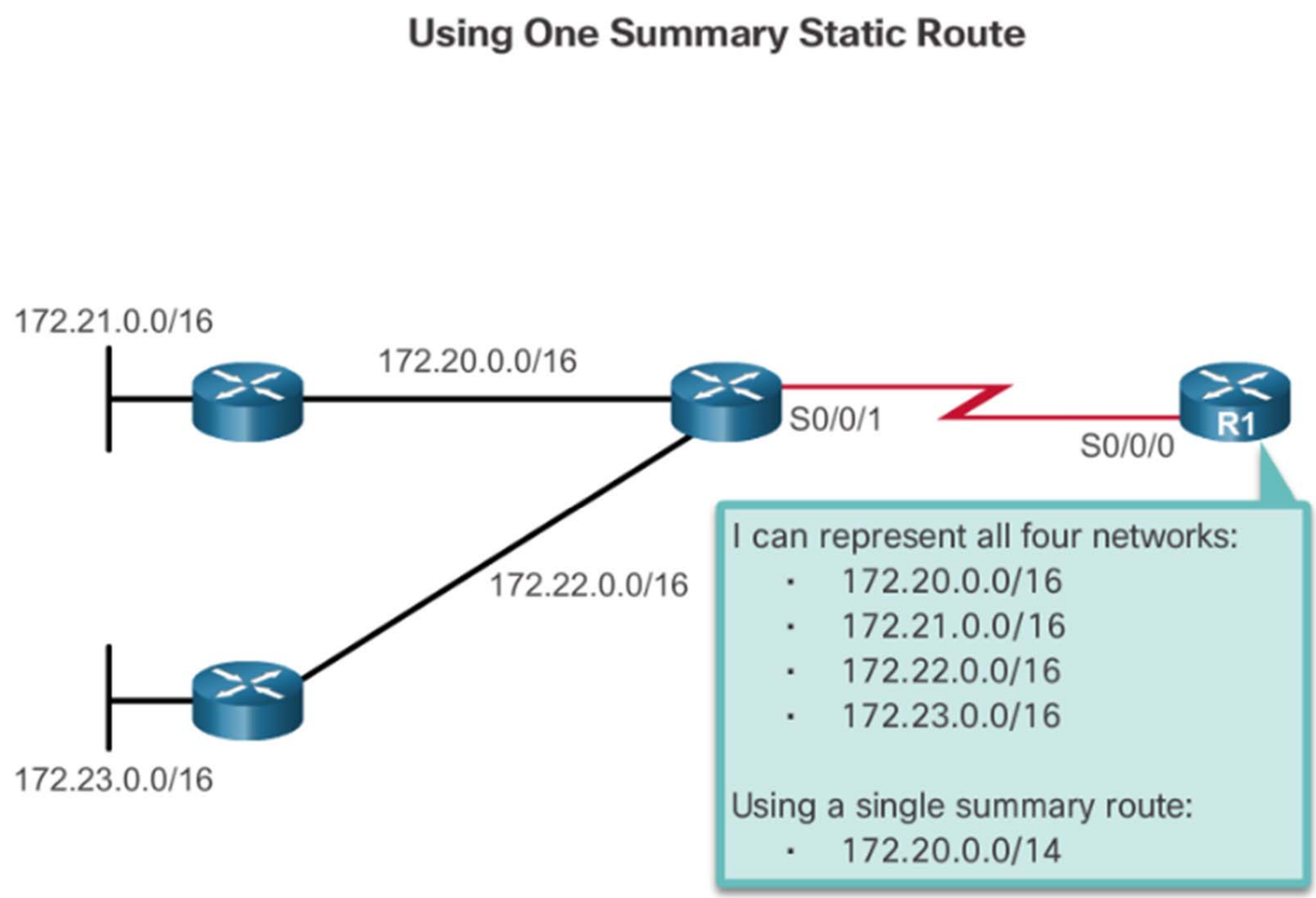
Default Static Route

- A default static route is a route that matches all packets.
- A default route identifies the gateway IP address to which the router sends all IP packets that it does not have a learned or static route.
- A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address.



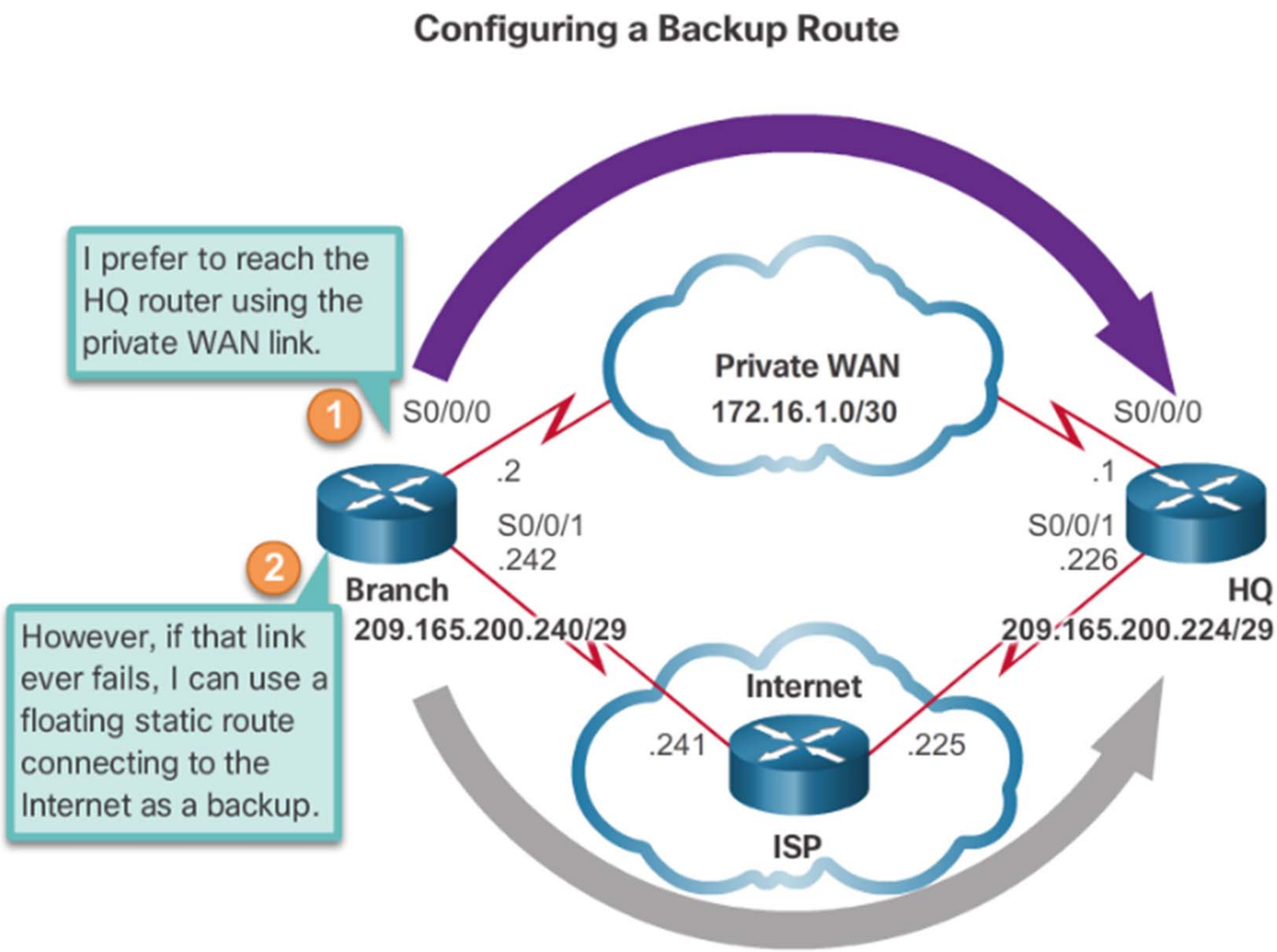
Types of Static Routes

Summary Static Route



Types of Static Routes

Floating Static Route



6.2 Configure Static and Default Routes

Cisco | Networking Academy®
Mind Wide Open™

Configure IPv4 Static Routes

ip route Command

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table
subnet-mask	• Subnet mask of the remote network to be added to the routing table • The subnet mask can be modified to summarize a group of networks
ip-address	• Commonly referred to as the next-hop router's IP address • Typically used when connecting to a broadcast media (i.e., Ethernet) • Commonly creates a recursive lookup
exit-intf	• Use the outgoing interface to forward packets to the destination network • Also referred to as a directly attached static route • Typically used when connecting in a point-to-point configuration
distance	• (Optional) Configures an administrative distance • Typically used to configure a floating static route

Configure IPv4 Static Routes
Next-Hop Options

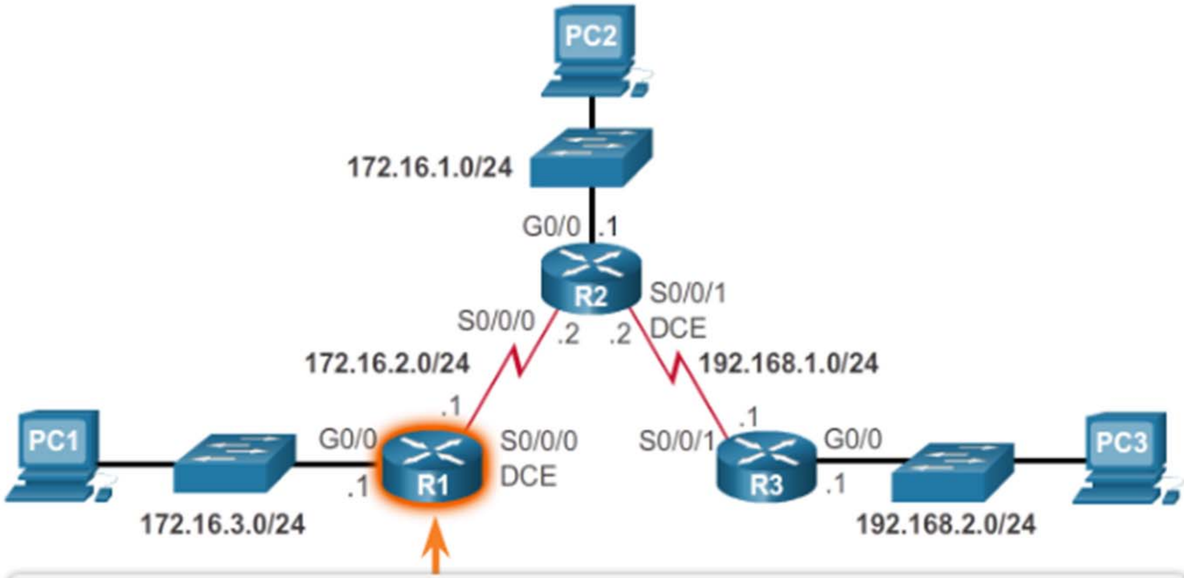
The next hop can be identified by an IP address, exit interface, or both. How the destination is specified creates one of the three following route types:

- **Next-hop route** - Only the next-hop IP address is specified.
- **Directly connected static route** - Only the router exit interface is specified.
- **Fully specified static route** - The next-hop IP address and exit interface are specified.

Configure IPv4 Static Routes

Configure a Next-Hop Static Route

Configuring Next-Hop Static Routes on R1

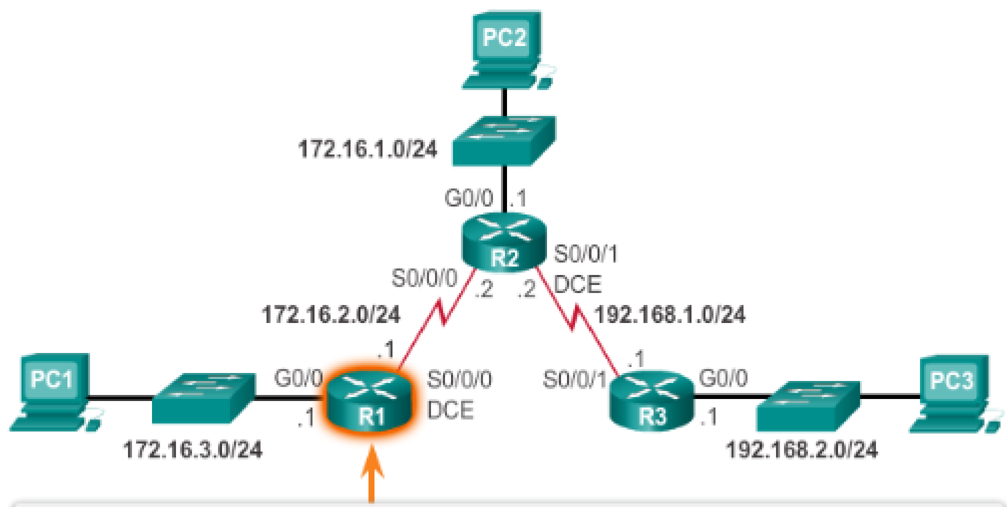



```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#
```

Configure IPv4 Static Routes

Configure Directly Connected Static Route

Configure Directly Attached Static Routes on R1

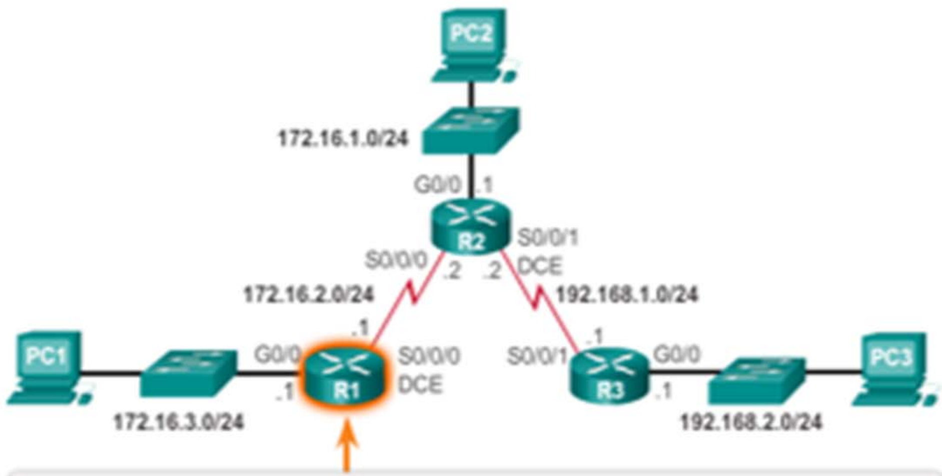



```
R1(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.2.0 255.255.255.0 s0/0/0
R1(config)#
```

```
S       172.16.1.0/24 is directly connected, Serial0/0/0
C       172.16.2.0/24 is directly connected, Serial0/0/0
L       172.16.2.1/32 is directly connected, Serial0/0/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
R1#
```

Configure a Fully Specified Static Route

Configure Directly Attached Static Routes on R1

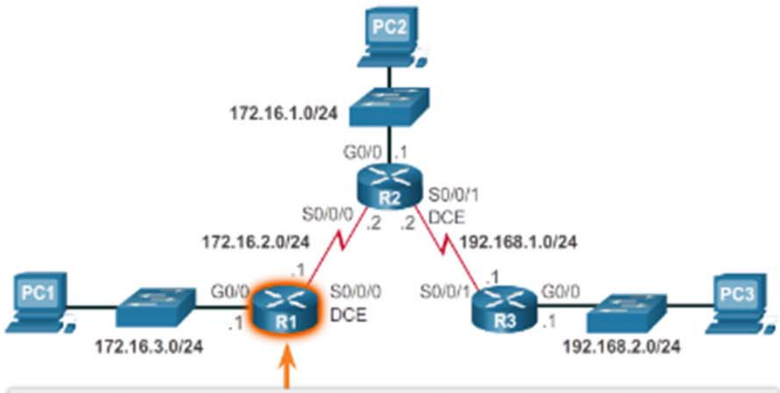



```
R1(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.1.0 255.255.255.0 s0/0/0
R1(config)#ip route 192.168.2.0 255.255.255.0 s0/0/0
R1(config)#
```

```
S        172.16.1.0/24 is directly connected, Serial0/0/0
C        172.16.2.0/24 is directly connected, Serial0/0/0
L        172.16.2.1/32 is directly connected, Serial0/0/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0
S     192.168.1.0/24 is directly connected, Serial0/0/0
S     192.168.2.0/24 is directly connected, Serial0/0/0
R1#
```

Configure IPv4 Static Routes

Verify a Static Route




```
R1# show ip route static | begin Gateway
Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

```
R1# show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 172.16.2.2
      Route metric is 0, traffic share count is 1
R1#
```

```
R1# show running-config | section ip route
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1#
```

Configure IPv4 Static Routes

Default Static Route

Default Static Route Syntax

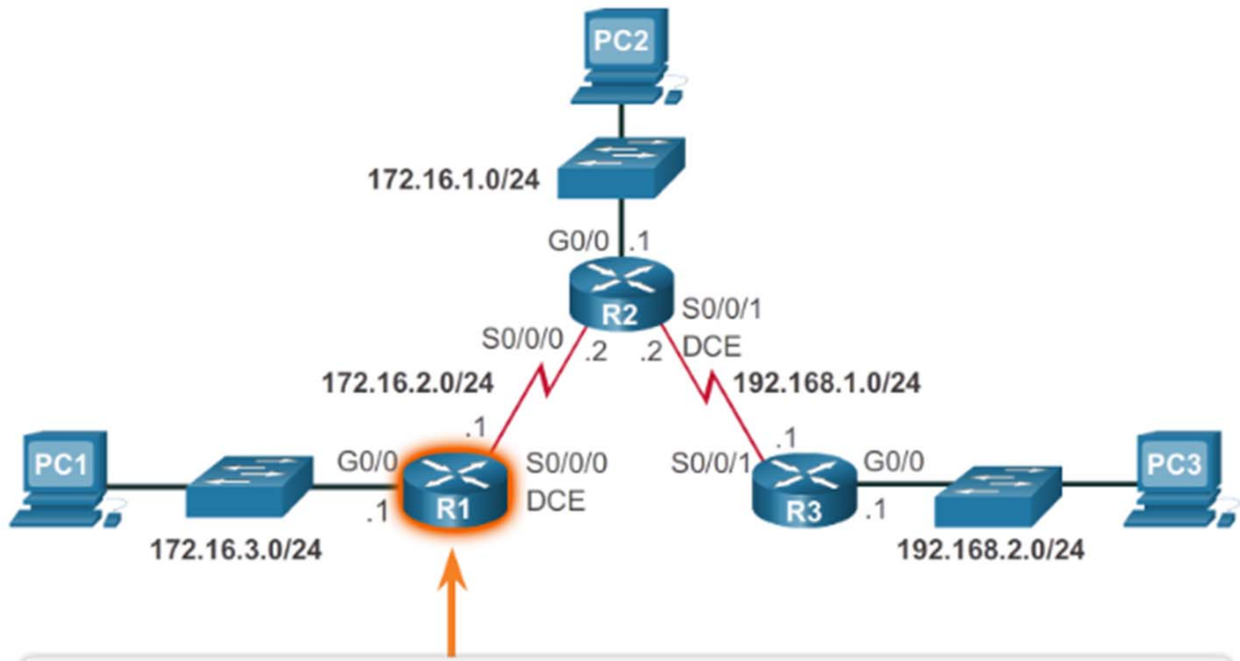
```
Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

Parameter	Description
0.0.0.0 0.0.0.0	Matches any network address.
ip-address	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

Configure IPv4 Static Routes

Configure a Default Static Route

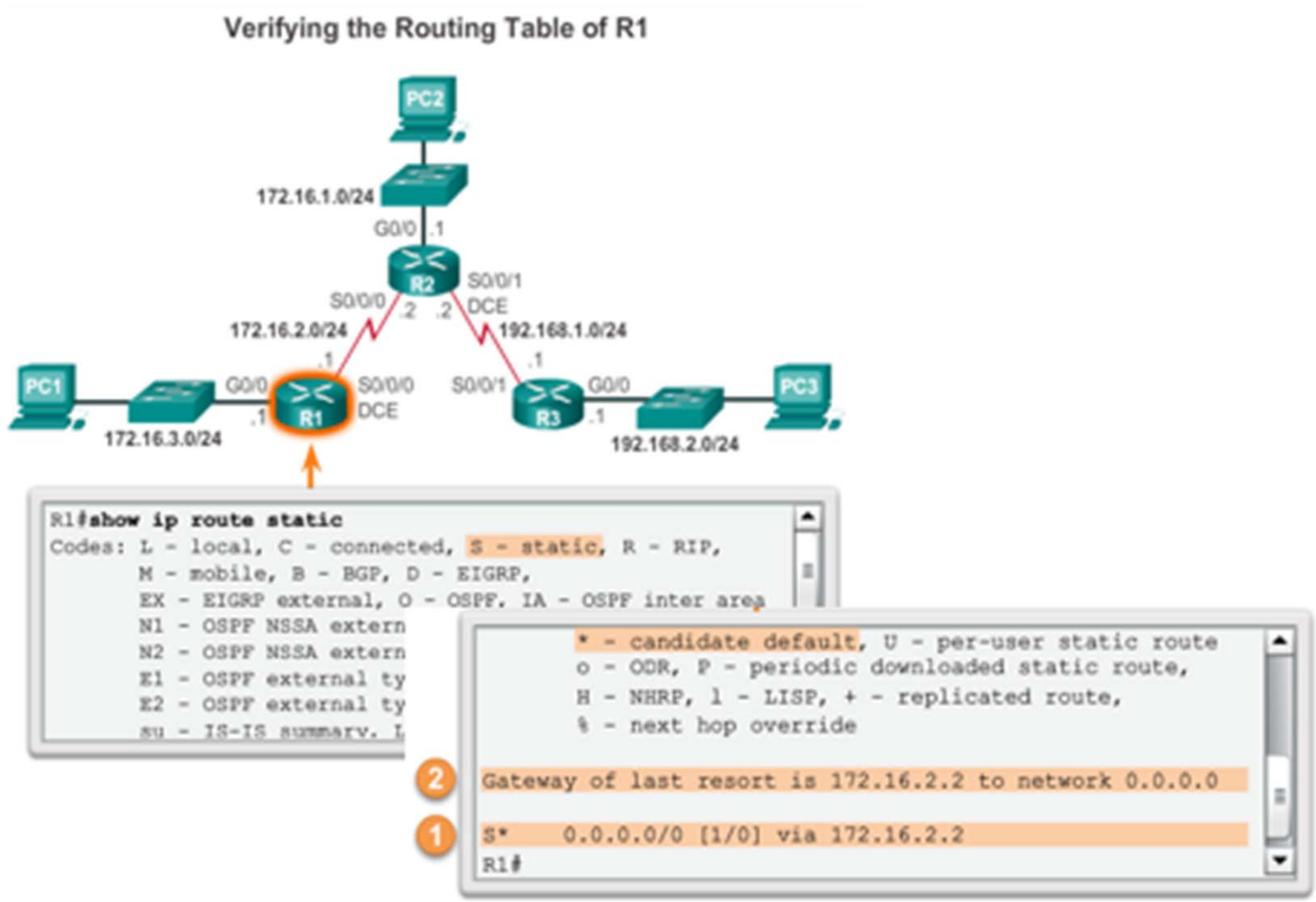
Configuring a Default Static Route




```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)#
```

Configure IPv4 Static Routes

Verify a Default Static Route



The `ipv6 route` Command

IPv6 Command Syntax

```
Router(config)# ipv6 route ipv6-prefix/prefix-length
{ipv6-address | exit-intf}
```

Parameter	Description
`ipv6-prefix`	Destination network address of the remote network to be added to the routing table.
`prefix-length`	Prefix length of the remote network to be added to the routing table.
`ipv6-address`	• Commonly referred to as the next-hop router's IP address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
`exit-intf`	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

Configure IPv6 Static Routes

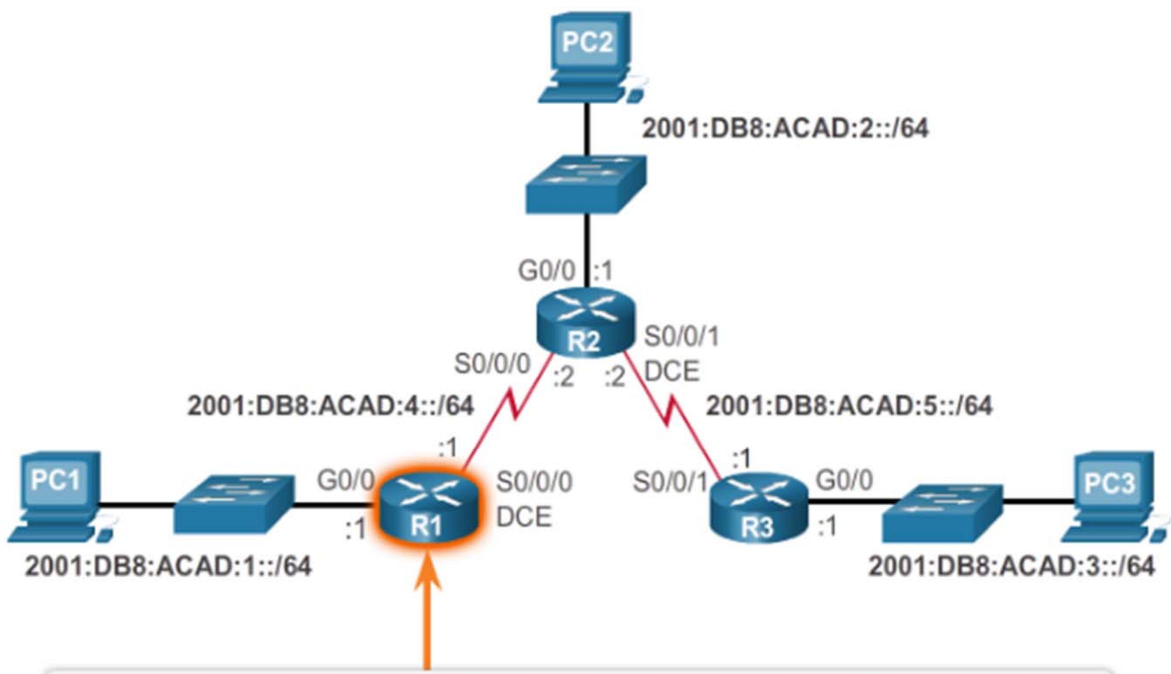
Next-Hop Options

- **Next-hop static IPv6 route** - Only the next-hop IPv6 address is specified
- **Directly connected static IPv6 route** - Only the router exit interface is specified
- **Fully specified static IPv6 route** - The next-hop IPv6 address and exit interface are specified

Configure IPv6 Static Routes

Configure a Next-Hop Static IPv6 Route

Configure Next-Hop Static IPv6 Routes

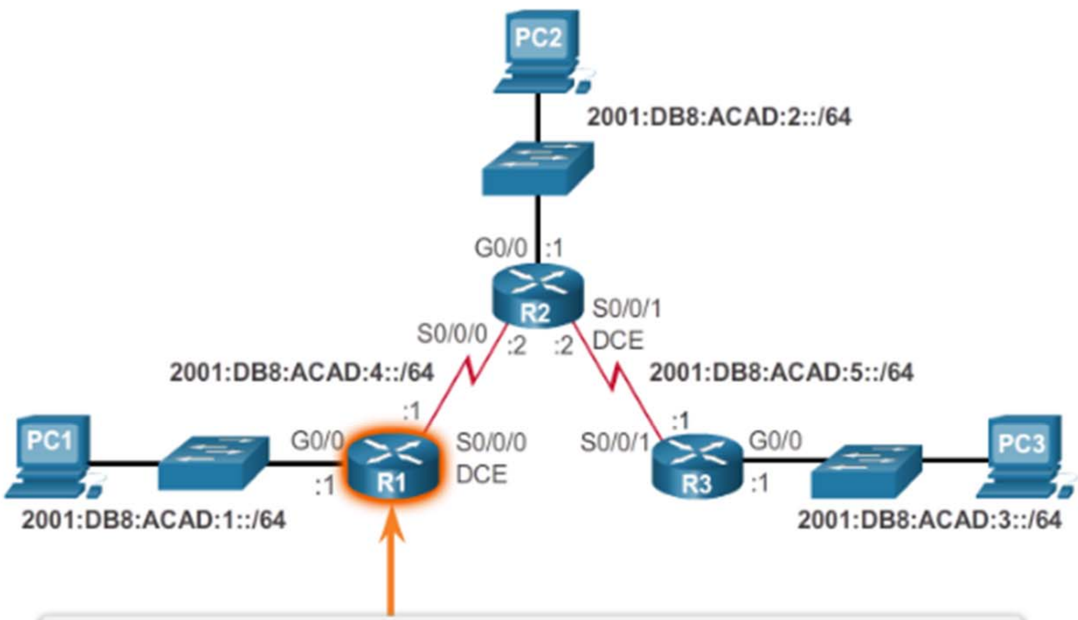



```
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:DB8:ACAD:4::2
R1(config)# ipv6 route 2001:DB8:ACAD:5::/64 2001:DB8:ACAD:4::2
R1(config)# ipv6 route 2001:DB8:ACAD:3::/64 2001:DB8:ACAD:4::2
R1(config)#
```

Configure IPv6 Static Routes

Directly Connected Static IPv6 Route

Configure Directly Connected Static IPv6 Routes on R1




```
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 s0/0/0
R1(config)# ipv6 route 2001:DB8:ACAD:5::/64 s0/0/0
R1(config)# ipv6 route 2001:DB8:ACAD:3::/64 s0/0/0
R1(config)#
R1#
```

Configure IPv6 Static Routes

Fully Specified Static IPv6 Route

Configure Fully Specified Static IPv6 Routes on R1


```
R1(config)# ipv6 route 2001:db8:acad:2::/64 fe80::2
% Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2
R1(config)#
```

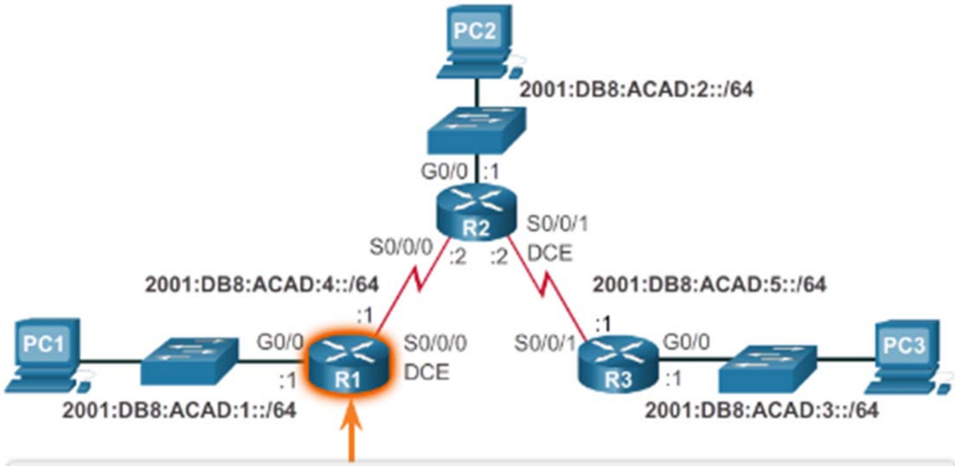
Configure IPv6 Static Routes

Verify IPv6 Static Routes

In addition to **`ping`** and **`traceroute`**, commands to verify static routes include:

- **`show ipv6 route`**
- **`show ipv6 route static`**
- **`show ipv6 route`** *`network`*

Verify a Specific Entry in the Routing Table




```
R1# show ipv6 route 2001:db8:acad:3::
Routing entry for 2001:DB8:ACAD:3::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:ACAD:4::2
      Last updated 00:19:11 ago
R1#
```

Configure IPv6 Default Routes

Default Static IPv6 Route

Default Static IPv6 Route Syntax

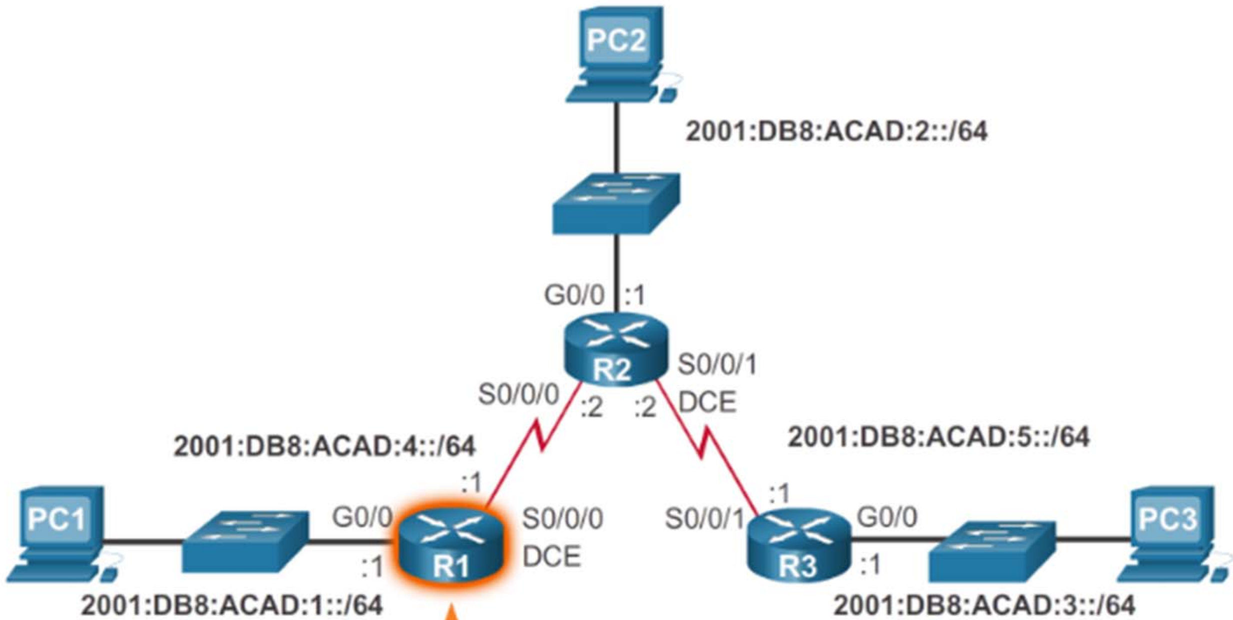
```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```

Parameter	Description
::/0	Matches any IPv6 prefix regardless of prefix length.
ipv6-address	• Commonly referred to as the next-hop router's IPv6 address. • Typically used when connecting to a broadcast media (i.e., Ethernet). • Commonly creates a recursive lookup.
exit-intf	• Use the outgoing interface to forward packets to the destination network. • Also referred to as a directly attached static route. • Typically used when connecting in a point-to-point configuration.

Configure IPv6 Default Routes

Configure a Default Static IPv6 Route

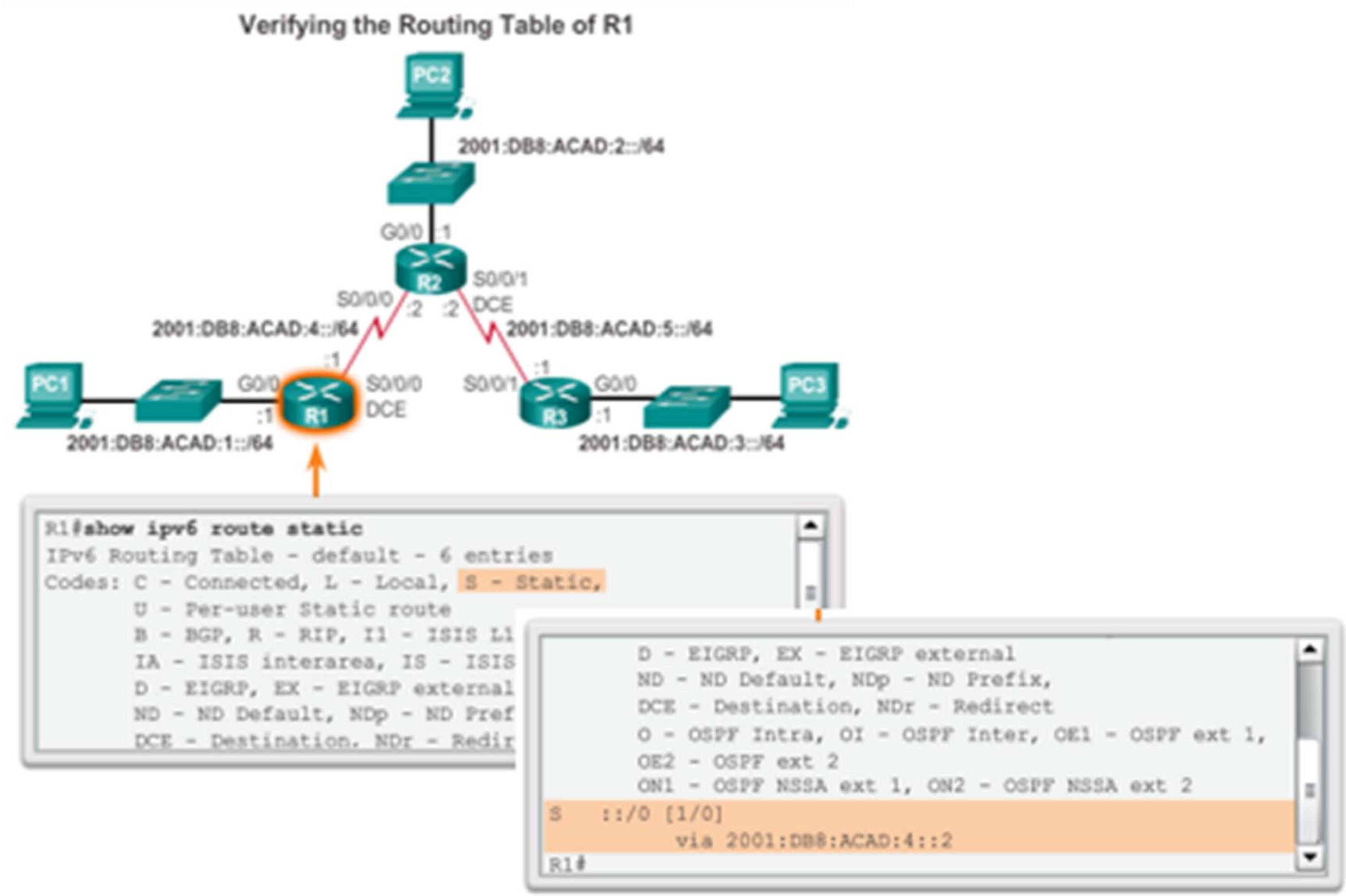
Configuring a Default Static IPv6 Route




```
R1(config)# ipv6 route ::/0 2001:DB8:ACAD:4::2
R1(config)#
```

Configure IPv6 Default Routes

Verify a Default IPv6 Static Route

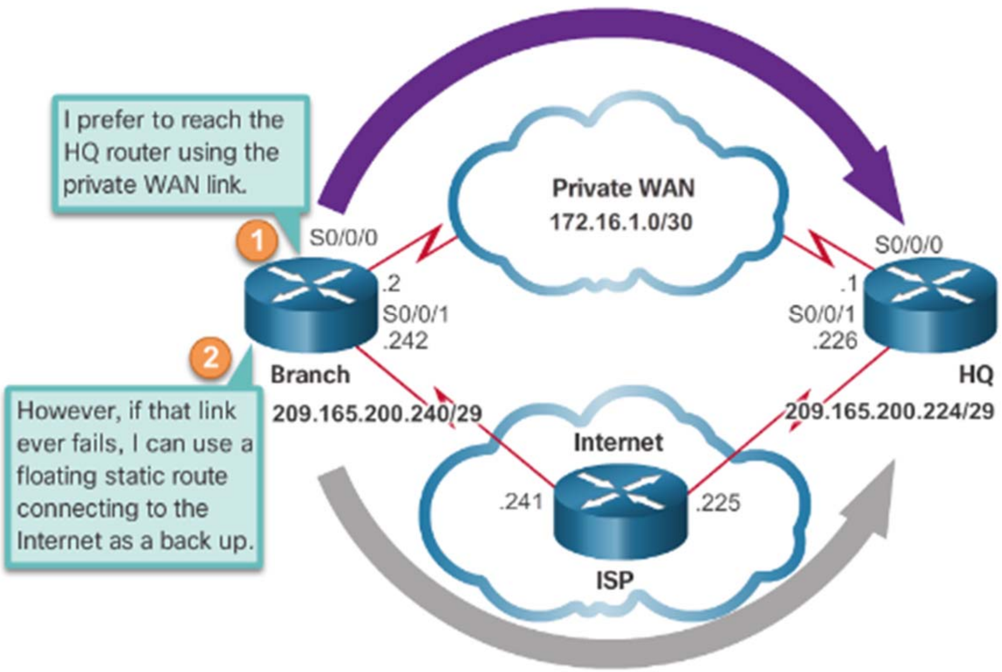


Floating Static Routes

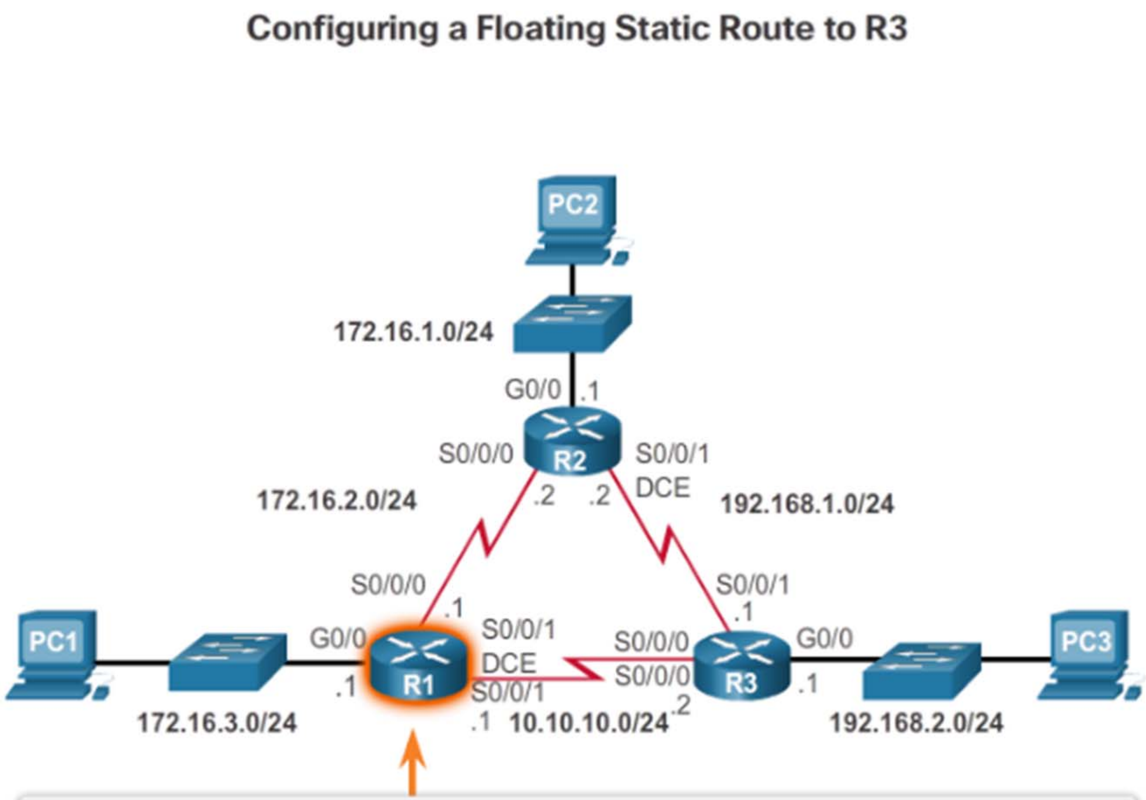
Floating static routes have an administrative distance greater than the administrative distance of another static route or dynamic routes.

- The static route “floats” and is not used when the route with the better administrative distance is active.
- If the preferred route is lost the floating static route can take over.

Why Configure a Floating Static Route?



Configure an IPv4 Floating Static Route




```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)#
```

Configure IPv6 Default Routes

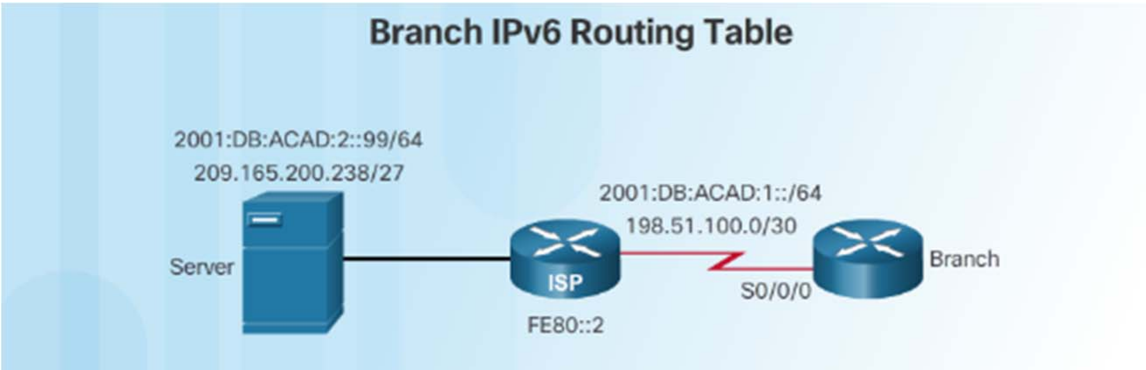
Test the IPv4 Floating Static Route

To test a floating static route:

- Use the **`show ip route`** command to verify that the routing table is using the default static route.
- Use the **`traceroute`** command to follow the traffic flow out the primary route.
- Disconnect the link or shutdown the primary interface(s). In the curriculum example the serial interfaces on R2 are shutdown.
- Use a **`show ip route`** command to verify that the routing table is using the floating static route.
- Use a **`traceroute`** command to follow the traffic flow out the backup route.

Configure Static Host Routes

Automatically Installed Host Routes




```
Branch# show ipv6 route
IPv6 Routing Table - default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
C   2001:DB8:ACAD:1::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
Branch#
```

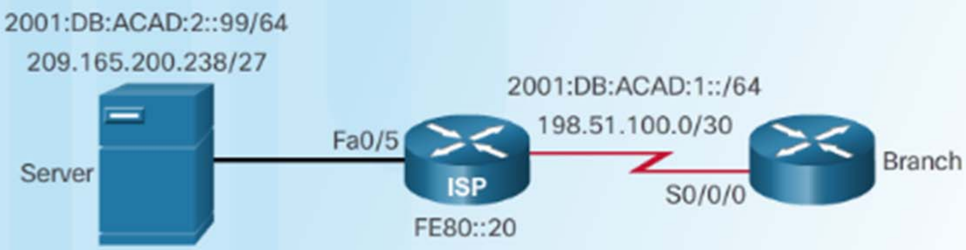
A host route is an IPv4 address with a 32-bit mask or an IPv6 address with a 128-bit mask.

- Automatically installed when an IP address is configured on the router.
- The local routes are marked with “L” in the output of the routing table.

Configure Static Host Routes

Configure IPv4 and IPv6 Static Host Routes

IPv4 and IPv6 Host Route Configuration and Verification

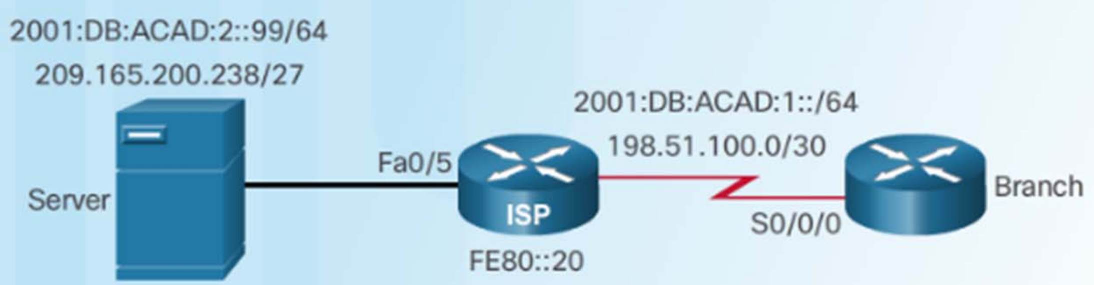



```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2
Branch(config)# ipv6 route 2001:db8:acad:2::99/128 2001:db8:acad:1::2
Branch(config)# end
Branch# show ip route | begin Gateway
Gateway of last resort is not set

      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, Serial0/0/0
L        198.51.100.1/32 is directly connected, Serial0/0/0
      209.165.200.0/32 is subnetted, 1 subnets
S        209.165.200.38 [1/0] via 198.51.100.2
Branch# show ipv6 route
<output omitted>
C    2001:DB8:ACAD:1::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:ACAD:1::1/128 [0/0]
      via Serial0/0/0, receive
S    2001:DB8:ACAD:2::99/128 [1/0]
      via 2001:DB8:ACAD:1::2
L    FF00::/8 [0/0]
      via Null0, receive
Branch#
```

Configure Static Host Routes

Configure IPv4 and IPv6 Static Host Routes

Fully Specified IPv6 Host Route with the Next-Hop Link-Local Address

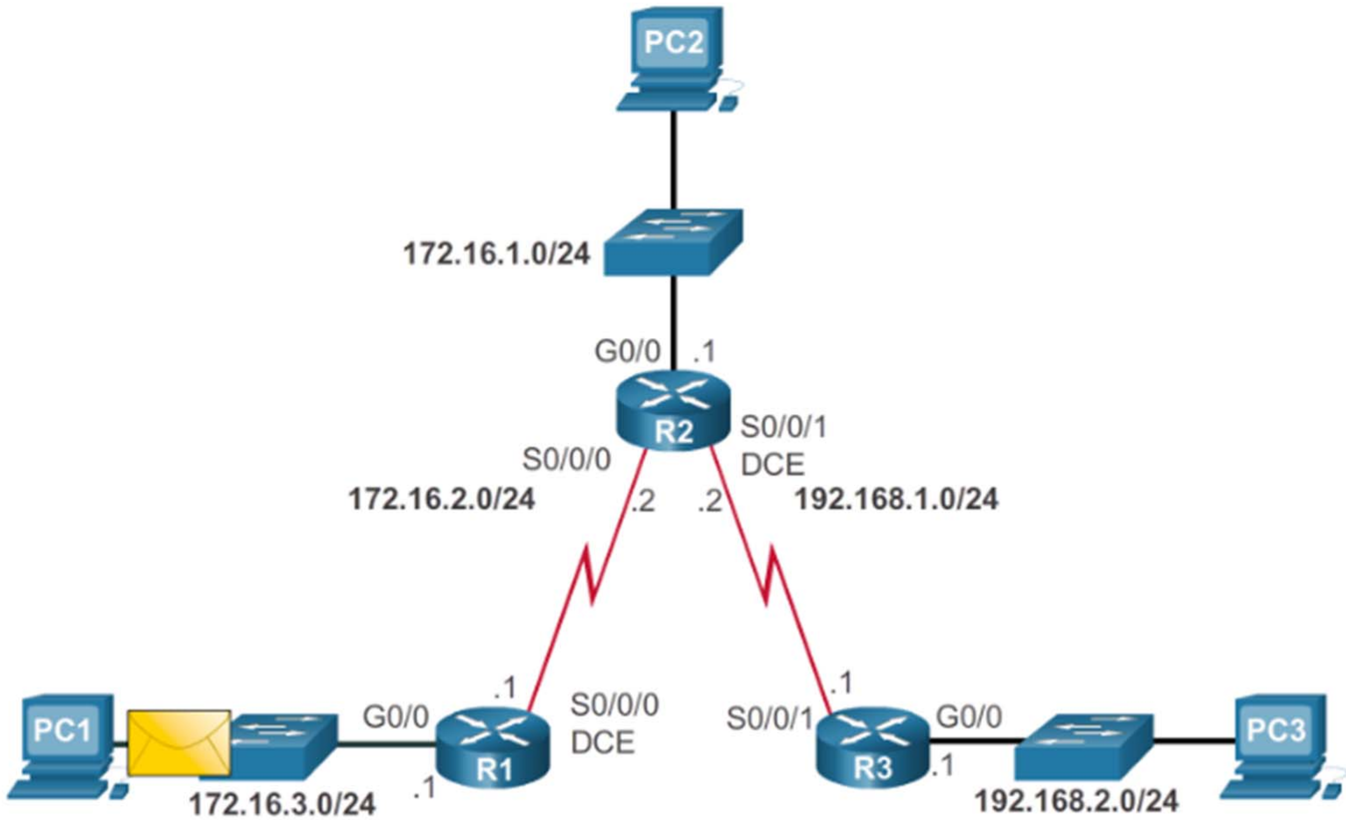



```
Branch(config)# no ipv6 route 2001:db8:acad:2::99/128 2001:db8:acad:1::2
Branch(config)# ipv6 route 2001:db8:acad:2::99/128 serial 0/0/0 fe80::2
Branch(config)# end
Branch# show ipv6 route
 <output omitted>

S    ::/0 [1/0]
      via 2001:DB8:ACAD:1::2
C    2001:DB8:ACAD:1::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:ACAD:1::1/128 [0/0]
      via Serial0/0/0, receive
S    2001:DB8:ACAD:2::99/128 [1/0]
      via FE80::2, Serial0/0/0
L    FF00::/8 [0/0]
      via Null0, receive
Branch#
```

6.2 Troubleshoot Static and Default Route Issues

Packet Processing with Static Routes

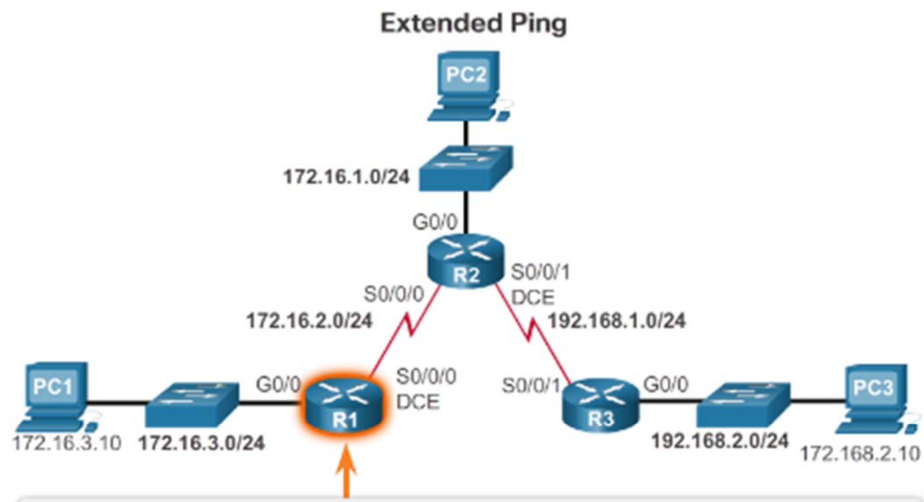
Static Routes and Packet Forwarding



Troubleshoot a Missing Route

IOS troubleshooting commands include:

- **`ping`**
- Extended **ping** enables you to specify the source IP address for the ping packets.
- **`traceroute`**
- **`show ip route`**
- **`show ip interface brief`**
- **`show cdp neighbors detail`**




```
R1# ping 192.168.2.1 source 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28
ms
R1#
```

Solve a Connectivity Problem

- Finding a missing (or misconfigured) route requires using the right tools in a methodical manner.
- Use the **ping** command to confirm the destination can't be reached.
- A **traceroute** would also reveal the closest router (or hop) that fails to respond as expected. In this case, the router would then send an Internet Control Message Protocol (ICMP) destination unreachable message back to the source.
- The next step is to investigate the routing table using the **show ip route** command. Look for missing or misconfigured routes.
- Incorrect static routes are a common cause of routing problems.

2.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary
Summary

- Explain the advantages and disadvantages of static routing.
- Explain the purpose of different types of static routes.
- Configure IPv4 and IPv6 static routes by specifying a next-hop address.
- Configure IPv4 and IPv6 default routes.
- Configure a floating static route to provide a backup connection.
- Configure IPv4 and IPv6 static host routes that direct traffic to a specific host.
- Explain how a router processes packets when a static route is configured.
- Troubleshoot common static and default route configuration issues.

Section 2.1
Terms and Commands

- static route
- administrative distance (AD)
- stub network
- default route
- 0.0.0.0/0
- default static route
- Gateway of Last Resort
- more specific match
- summary static route
- floating static route

Section 2.2
Terms and Commands

- exit-intf
- next hop
- recursive static route
- recursive lookup
- directly connected static route
- CEF (Cisco Express Forwarding)
- FIB (Forwarding Information Base)
- fully specified static route
- edge router
- stub router
- quad-zero route
- ::/0
- destination network
- **Ipv6 route** command
- Fully specified static IPv6 route
- **show ipv6 route**
- **show ipv6 route static**
- **show ipv6 route network**
- IPv4 Static Host Routes
- IPv6 Static Host Routes

Section 2.3
Terms and Commands

- Extended ping

Cisco | Networking Academy®
Mind Wide Open™

Instructor Materials Chapter 3: Dynamic Routing

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Instructor Materials – Chapter 3 Planning Guide

This PowerPoint deck is divided in two parts:

1. Instructor Planning Guide
   - Information to help you become familiar with the chapter
   - Teaching aids
2. Instructor Class Presentation
   - Optional slides that you can use in the classroom
   - Begins on slide # 15

Note: Remove the Planning Guide from this presentation before sharing with anyone.

Routing and Switching Essentials v6.0 Planning Guide
Chapter 3: Dynamic Routing

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
3.0.1.2	Class Activity	How Much Does This Cost	Optional
3.1.2.5	Activity	Compare Static and Dynamic Routing	-
3.2.1.2	Syntax Checker	Advertising the R2 and R3 Networks	-
3.2.1.3	Syntax Checker	Verifying RIP Settings and Routes on R2 and R3 Networks	-
3.2.1.4	Syntax Checker	Enable and Verify RIPv2 on R2 and R3	-
3.2.1.5	Syntax Checker	Disable Automatic Summarization on R2 and R3	-

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 3: Activities

What activities are associated with this chapter?

Page #	Activity Type	Activity Name	Optional?
3.2.1.6	Syntax Checker	Configuring and Verifying a Passive Interface on R2 and R3	-
3.2.1.7	Syntax Checker	Verifying the Gateway of Last Resort on R2 and R3	-
3.2.1.8	Packet Tracer	Configuring RIPv2	Recommended
3.2.1.9	Lab	Configuring RIPv2	Optional
3.3.1.4	Activity	Identify Parts of an IPv4 Routing Table Entry	-
3.3.2.6	Activity	Identify Parent and Child IPv4 Routes	-
3.3.3.3	Activity	Determine the Longest Match Route	-
3.3.4.4	Activity	Identify Parts of an IPv6 Routing Table Entry	-
3.4.1.1	Class Activity	IPv6, Details, Details…	Optional

The password used in the Packet Tracer activities in this chapter is: **PT_ccna5**

Chapter 3: Assessment

- Students should complete Chapter 3, “Assessment” after completing Chapter 3.
- Quizzes, labs, Packet Tracers and other activities can be used to informally assess student progress.

Chapter 3: Best Practices

Prior to teaching Chapter 3, the instructor should:

- Complete Chapter 3, “Assessment.”
- The objectives of this chapter are:
  - Explain the purpose of dynamic routing protocols.
  - Explain the use of dynamic routing and static routing.
  - Configure the RIPv2 routing protocol.
  - Explain the components of an IPv4 routing table entry for a given route.
  - Explain the parent/child relationship in a dynamically built routing table.
  - Determine which route will be used to forward a IPv4 packet.
  - Determine which route will be used to forward a IPv6 packet.

Chapter 3: Best Practices (Cont.)

Section 3.1

- Create topologies in Packet Tracer similar to the topologies in the chapter and demonstrate static versus dynamic routing. Stress the advantages and disadvantages of static and dynamic routing.
- During this chapter, consider setting up a large network as a Packet Tracer demonstration to allow students to see size and complexity.
- Discuss with students the advantages and disadvantages of using routing protocols rather than static routing. Introduce terms such as metrics, convergence, distance vector, link state, classless, classful, IGP, and EGP.

Chapter 3: Best Practices (Cont.)

Section 3.2

- Demonstrate each RIP command using Packet Tracer. Follow-up with the recommended lab, 3.2.1.8 Configuring RIPv2.
- Syntax checkers in this section can be used to assist student in memorizing commands and interpreting error commands.

Chapter 3: Best Practices (Cont.)

Section 3.3

- Reading routing tables is crucial in troubleshooting. Provide many examples of pre-configured topologies for practice.

Chapter 3: Best Practices (Cont.)

Discussion Questions

1. When do we need to use static routing?
2. When do we need to use dynamic routing?
3. What are the advantages and disadvantages of static and dynamic routing?
4. Compare and contrast the distance vector and link-state routing protocols.
5. What is the advantage of classless routing protocols over classful routing protocols?
6. Why do we want to have convergence in the shortest possible time after a change in a network?
7. Why do we need to have multiple metrics?
8. What affects the speed of convergence?

Chapter 3: Best Practices (Cont.)

Story for Chapter 3

When two companies join forces, their networks too must unite. Our customer had purchased one of its competitors and we were asked to integrate these two very different and very large networks. Each company's remote offices needed access to all of the existing company networks as well as those of the new company. The static routing statements on each company's core routers had grown as they each added remote offices. With the merger of these two companies' networks, the number of static routes had doubled. For this merger to work, a simple answer to a complex problem had to be found. Because these networks were all managed by Cisco routers, a very simple EIGRP network schema was installed on all interconnected routers. This new dynamically routed network eliminated the need to maintain static routes on any of the core or remote office routers. In addition, it allowed for easy future expansion of any additional networks. With only a few hours of consulting time and a basic knowledge of dynamic routing, the network merger went through without a problem.

Chapter 3: Additional Help

- For additional help with teaching strategies, including lesson plans, analogies for difficult concepts, and discussion topics, visit the CCNA Community at: https://www.netacad.com/group/communities/community-home
- Best practices from around the world for teaching CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna-blog
- If you have lesson plans or resources that you would like to share, upload them to the CCNA Community in order to help other instructors.
- Students can enroll in **Packet Tracer Know How 1: Packet Tracer 101** (self-enroll)

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3: Dynamic Routing

Routing and Switching Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3 - Sections & Objectives

3.1 Dynamic Routing Protocols

- Explain the purpose of dynamic routing protocols.
- Explain the use of dynamic routing and static routing

3.2 RIPv2

- Configure the RIPv2 routing protocol.

3.3 The Routing Table

- Explain the components of an IPv4 routing table entry for a given route.
- Explain the parent/child relationship in a dynamically built routing table.
- Determine which route will be used to forward a IPv4 packet.
- Determine which route will be used to forward a IPv6 packet.

3.4 Summary

3.1 Dynamic Routing Protocols

Cisco | Networking Academy®
Mind Wide Open™

Dynamic Routing Protocol Overview
Dynamic Routing Protocol Evolution

- Dynamic routing protocols have been used in networks since the late 1980s.
- Newer versions support the communication based on IPv6.

Routing Protocols Classification

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Dynamic Routing Protocol Overview

Dynamic Routing Protocols Components

Routing Protocols are used to facilitate the exchange of routing information between routers.

The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Dynamic Routing Protocols Components (cont.)

Main components of dynamic routing protocols include:

- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** Routing protocols use algorithms for facilitating routing information for best path determination.

Dynamic versus Static Routing
Static Routing Uses

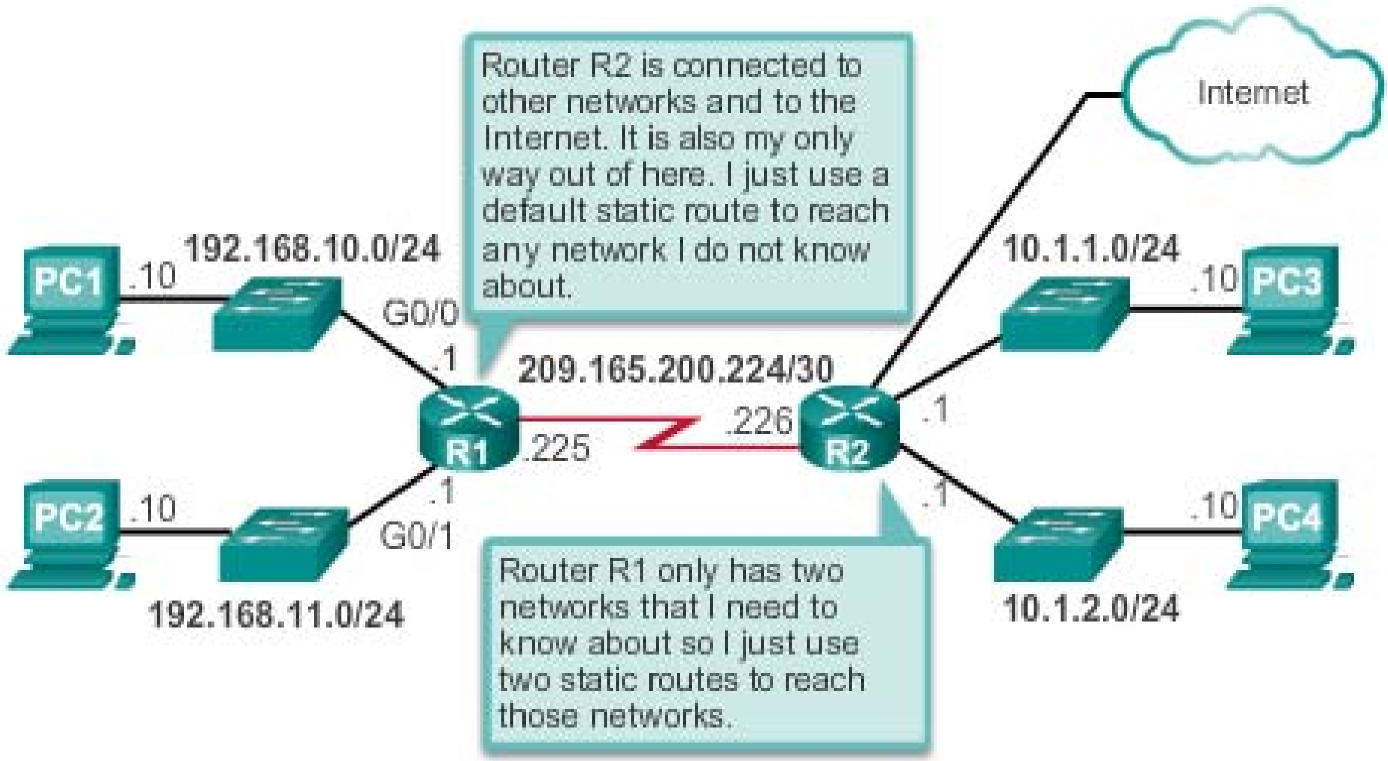
Networks typically use a combination of both static and dynamic routing.

Static routing has several primary uses:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from a stub network. A network with only one default route out and no knowledge of any remote networks.
- Accessing a single default router. This is used to represent a path to any network that does not have a match in the routing table.

Dynamic verses Static Routing

Static Routing Uses (cont.)



Static Routing Advantages and Disadvantages

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	Configuration complexity increases dramatically as network grows.
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	

Dynamic verses Static Routing

Dynamic Routing Advantages & Disadvantages

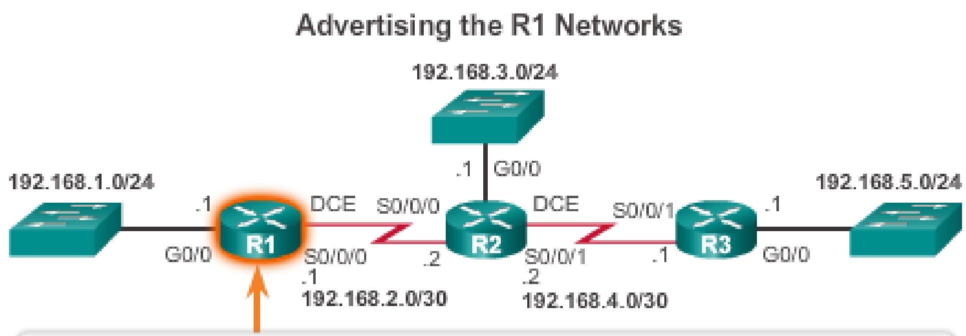
Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.

3.2 RIPv2

Configuring the RIP Protocol

Router RIP Configuration Mode

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```




```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#
```

Verify RIP Routing

Verifying RIP Settings on R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip

  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0    1     1 2
    Serial0/0/0           1     1 2

  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:15
  Distance: (default is 120)

R1#
```

Verifying RIP Routes on R1

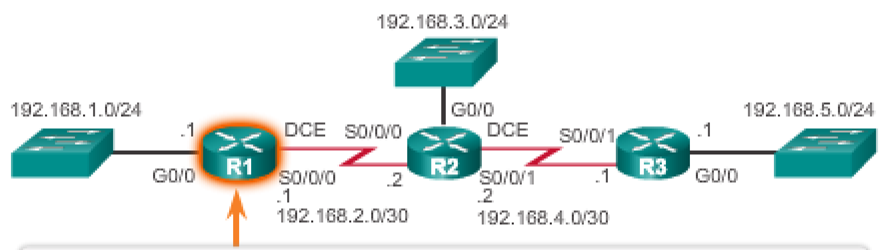
```
R1# show ip route | begin Gateway
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R     192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R     192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R     192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:24, Serial0/0/0
R1#
```

Configuring the RIP Protocol
Enable and Verify RIPv2

Verifying RIP Settings on R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not
set
  Incoming update filter list for all interfaces is not
set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after
240
  Redistributing: rip
  Default version control: send version 1, receive any
version
    Interface             Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0    1     1 2
    Serial0/0/0           1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway          Distance       Last Update
```

Enable and Verify RIPv2 on R1




```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# ^Z
R1#
R1# show ip protocols | section Default
  Default version control: send version 2, receive version 2
    Interface           Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0   2     2
    Serial0/0/0          2     2
R1#
```

Configuring the RIP Protocol

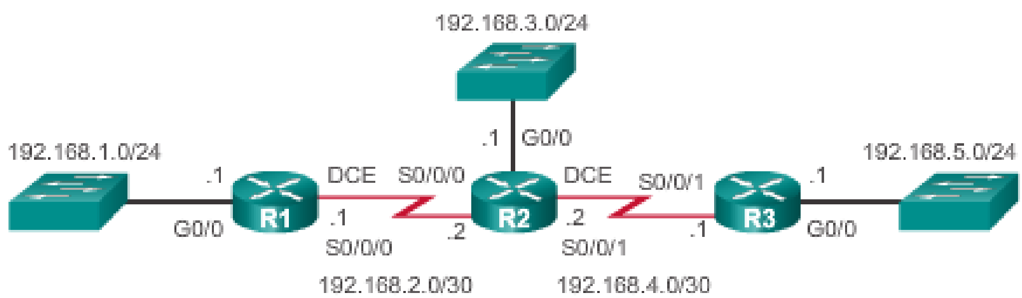
Disable Auto Summarization

- Similarly to RIPv1, RIPv2 automatically summarizes networks at major network boundaries by default.
- To modify the default RIPv2 behavior of automatic summarization, use the **`no auto-summary`** router configuration mode command.
- This command has no effect when using RIPv1.
- When automatic summarization has been disabled, RIPv2 no longer summarizes networks to their classful address at boundary routers. RIPv2 now includes all subnets and their appropriate masks in its routing updates.
- The **`show ip protocols`** now states that automatic network summarization is not in effect.

Configuring the RIP Protocol

Configuring Passive Interfaces

Configuring Passive Interfaces on R1



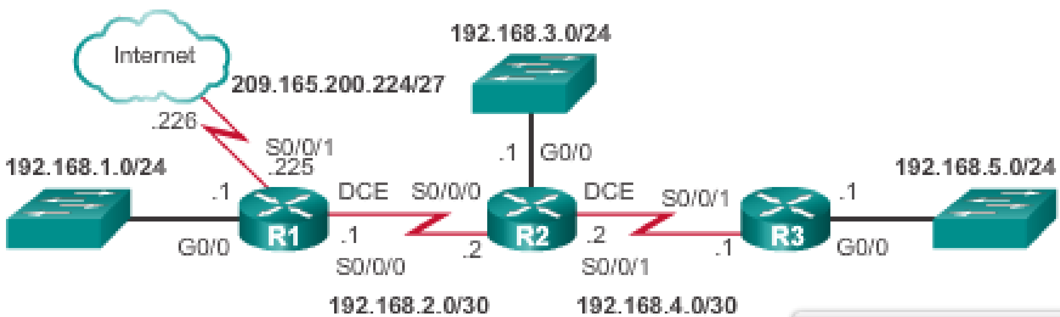
Sending out unneeded updates on a LAN impacts the network in three ways:

- Wasted Bandwidth
- Wasted Resources
- Security Risk

```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
R1# show ip protocols | begin Default
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0           2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:06
  Distance: (default is 120)

R1#
```

Propagate a Default Route

Propagating a Default Route on R1



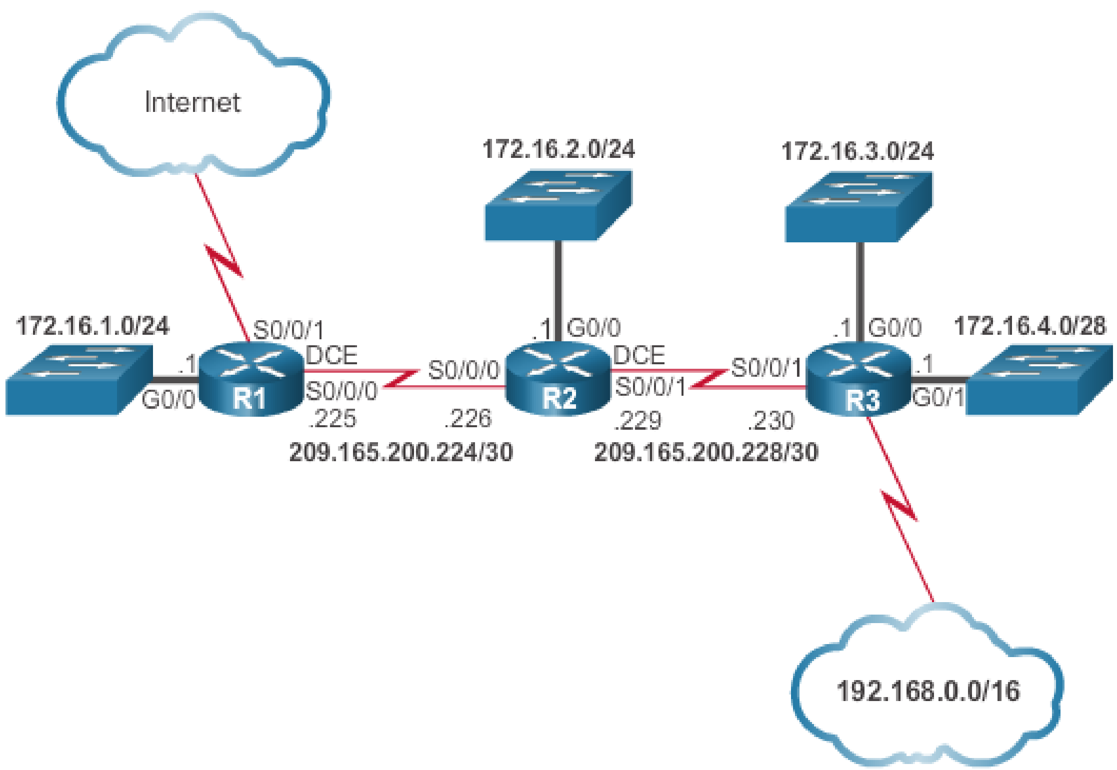

```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^Z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from
console by console
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.226, Serial0/0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0
L        192.168.1.1/32 is directly connected,
GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R     192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
```

3.3 The Routing Table

Cisco | Networking Academy®
Mind Wide Open™

Parts of an IPv4 Route Entry
Routing Table Entries

Reference Topology



Parts of an IPv4 Route Entry

Routing Table Entries

Routing Table of R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                     is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R  192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 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
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
                    Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

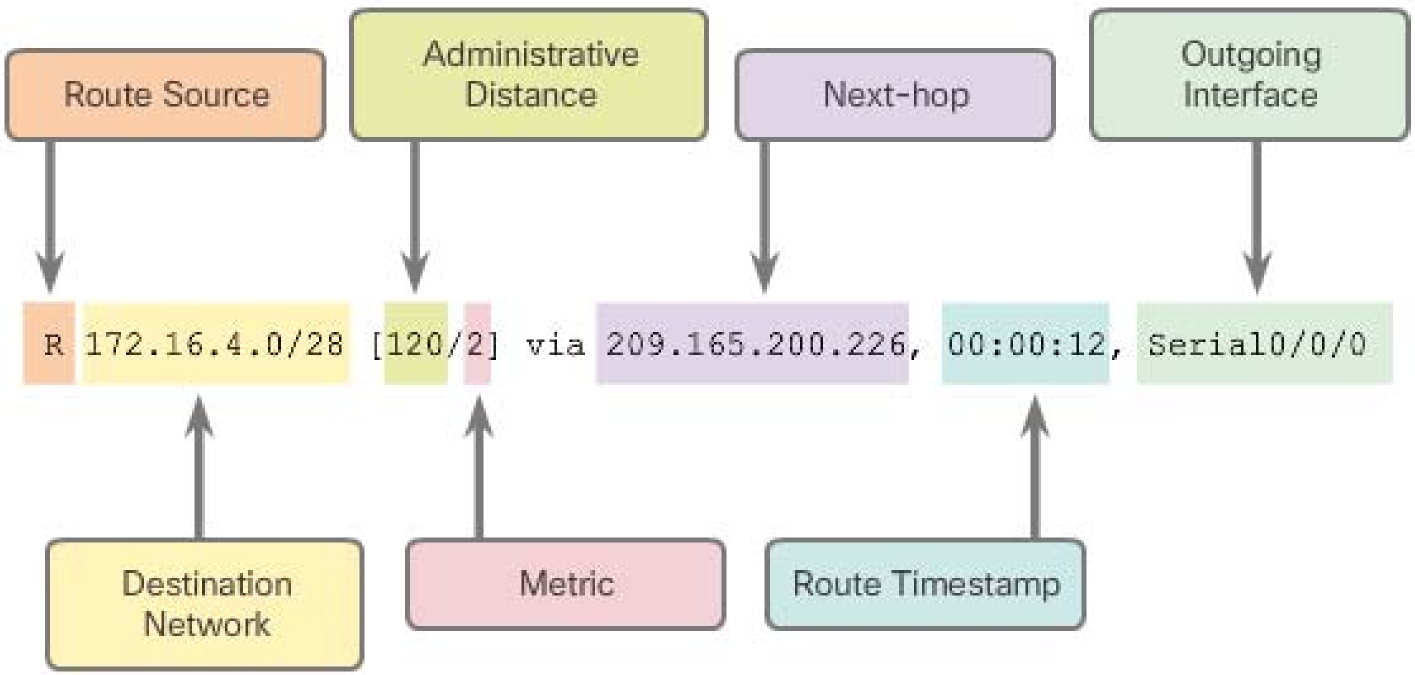
Parts of an IPv4 Route Entry
Directly Connected Entries

Route Source	Destination Network	Outgoing Interface
C	172.16.1.0/24 is directly connected,	GigabitEthernet0/0
L	172.16.1.1/32 is directly connected,	GigabitEthernet0/0

Directly Connected Interfaces of R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226,00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 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
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Parts of an IPv4 Route Entry
Remote Network Entries



Dynamically Learned IPv4 Routes
Routing Table Terms

Routes are discussed in terms of:

- Ultimate route
- Level 1 route
- Level 1 parent route
- Level 2 child routes

Routing Table of R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 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
R        209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
C        209.165.200.232/30 is directly connected, Serial0/0/1
L        209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Dynamically Learned IPv4 Routes

Ultimate Route

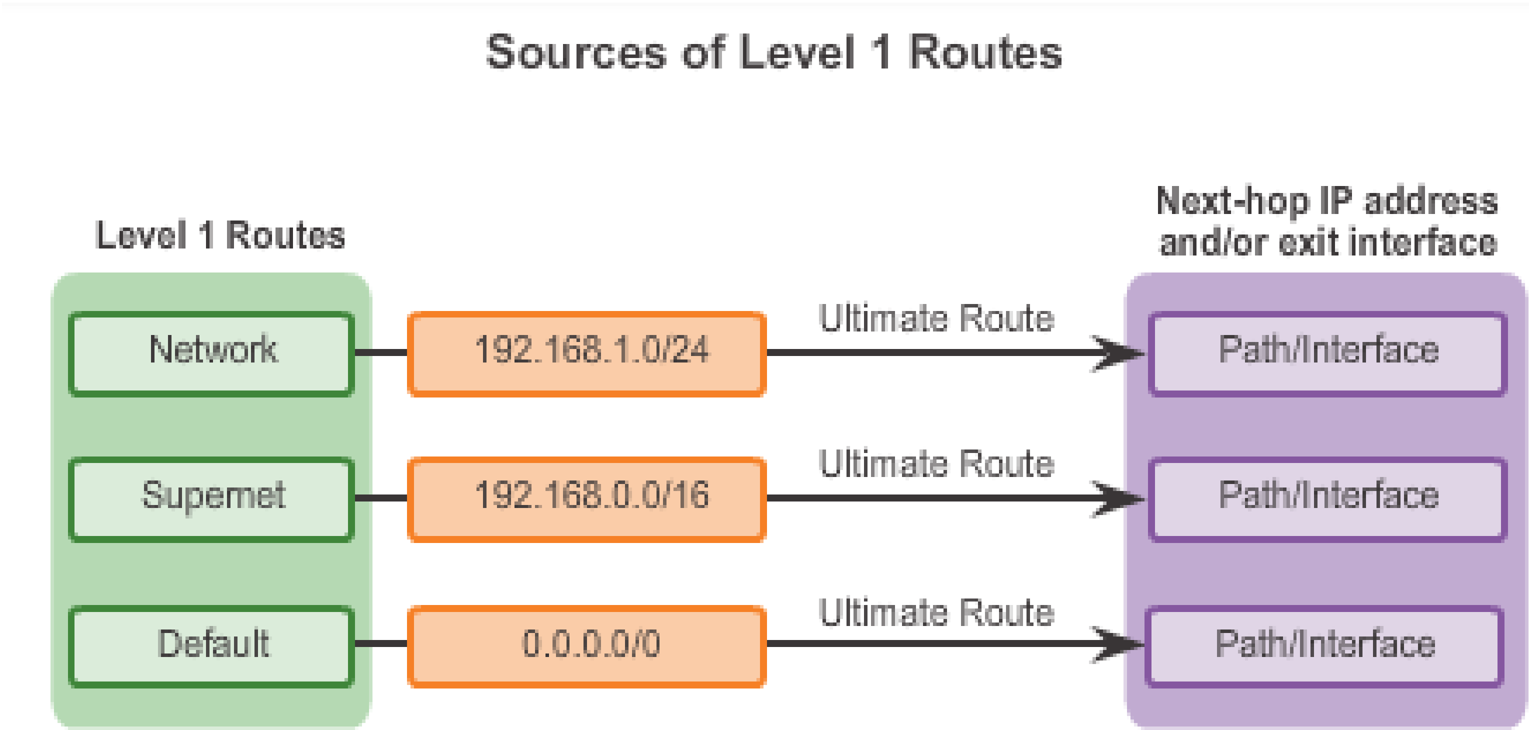
An ultimate route is a routing table entry that contains either a next-hop IP address or an exit interface.

Directly connected, dynamically learned, and link local routes are ultimate routes.

Ultimate Routes of R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
          Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 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
R        209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
C        209.165.200.232/30 is directly connected, Serial0/0/1
L        209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Dynamically Learned IPv4 Routes
Level 1 Route



Dynamically Learned IPv4 Routes
Level 1 Parent Route

Level 1 Parent Routes of R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C        209.165.200.224/30 is directly connected,
Serial0/0/0
```

Dynamically Learned IPv4 Routes
Level 2 Child Route

Example of Level 2 Child Routes

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*     0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                 is directly connected, Serial0/0/1
       172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C         172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L         172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R         172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R         172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R         172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R      192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
       209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C         209.165.200.224/30 is directly connected,
Serial0/0/0
```

The IPv4 Route Lookup Process

Route Lookup Process

1. If the best match is a level 1 ultimate route, then this route is used to forward the packet.
2. If the best match is a level 1 parent route, proceed to the next step.
3. The router examines child routes (the subnet routes) of the parent route for a best match.
4. If there is a match with a level 2 child route, that subnet is used to forward the packet.
5. If there is not a match with any of the level 2 child routes, proceed to the next step.

The Ipv4 Route Lookup Process

Route Lookup Process (cont.)

6. The router continues searching level 1 supernet routes in the routing table for a match, including the default route, if there is one.
7. If there is now a lesser match with a level 1 supernet or default routes, the router uses that route to forward the packet.
8. If there is not a match with any route in the routing table, the router drops the packet.

The IPv4 Route Lookup Process

Best Route = Longest Match

Matches for Packet Destined to 172.16.0.10

IP Packet Destination	172.16.0.10	10101100.00010000.00000000.00001010

Route 1	172.16.0.0/12	10101100.00010000.00000000.00000000
Route 2	172.16.0.0/18	10101100.00010000.00000000.00000000
Route 3	172.16.0.0/26	10101100.00010000.00000000.00000000

Longest Match to IP Packet Destination

The IPv4 Route Lookup Process

IPv6 Routing Table Entries

- Components of the IPv6 routing table are very similar to the IPv4 routing table (directly connected interfaces, static routes, and dynamically learned routes).
- IPv6 is classless by design, all routes are effectively level 1 ultimate routes. There is no level 1 parent of level 2 child routes.

Analyze an IPVv6 Routing Table

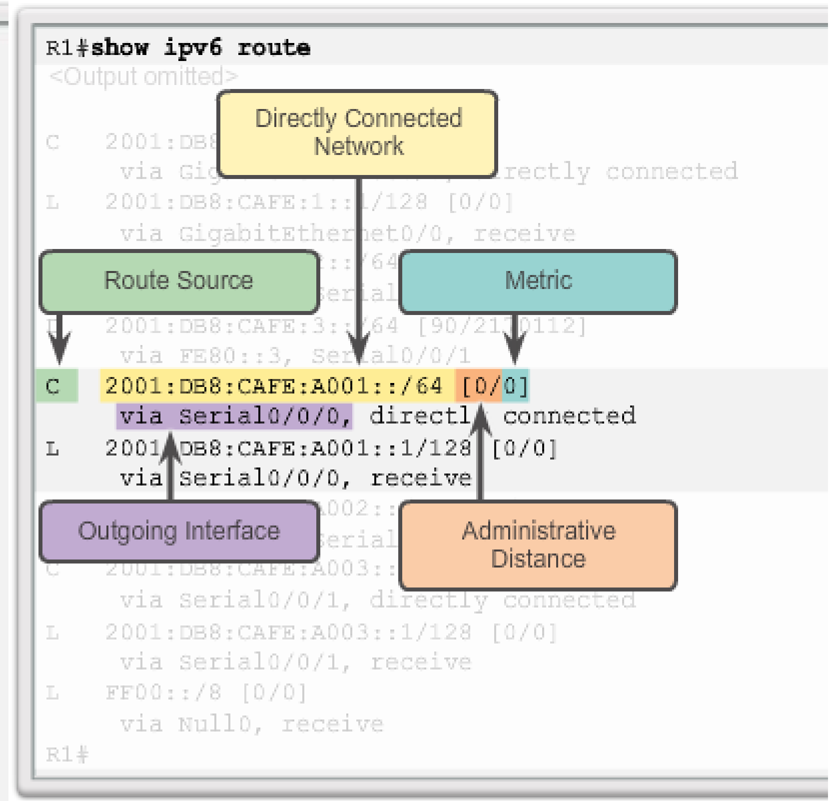
Directly Connected Entries

IPv6 Routing Table of R1

JG13

```
R1#show ipv6 route
<Output omitted>

C    2001:DB8:CAFE:1::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:CAFE:1::1/128 [0/0]
      via GigabitEthernet0/0, receive
D    2001:DB8:CAFE:2::/64 [90/3524096]
      via FE80::3, Serial0/0/1
D    2001:DB8:CAFE:3::/64 [90/2170112]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A001::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:CAFE:A001::1/128 [0/0]
      via Serial0/0/0, receive
D    2001:DB8:CAFE:A002::/64 [90/3523840]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A003::/64 [0/0]
      via Serial0/0/1, directly connected
L    2001:DB8:CAFE:A003::1/128 [0/0]
      via Serial0/0/1, receive
L    FF00::/8 [0/0]
      via Null0, receive
R1#
```

Directly Connected Routes on R1



Slide 46

JG13 I suggest using the Fig 2 router output instead of the Fig 1 (on the left)

Jane Gibbons, 10/12/2013

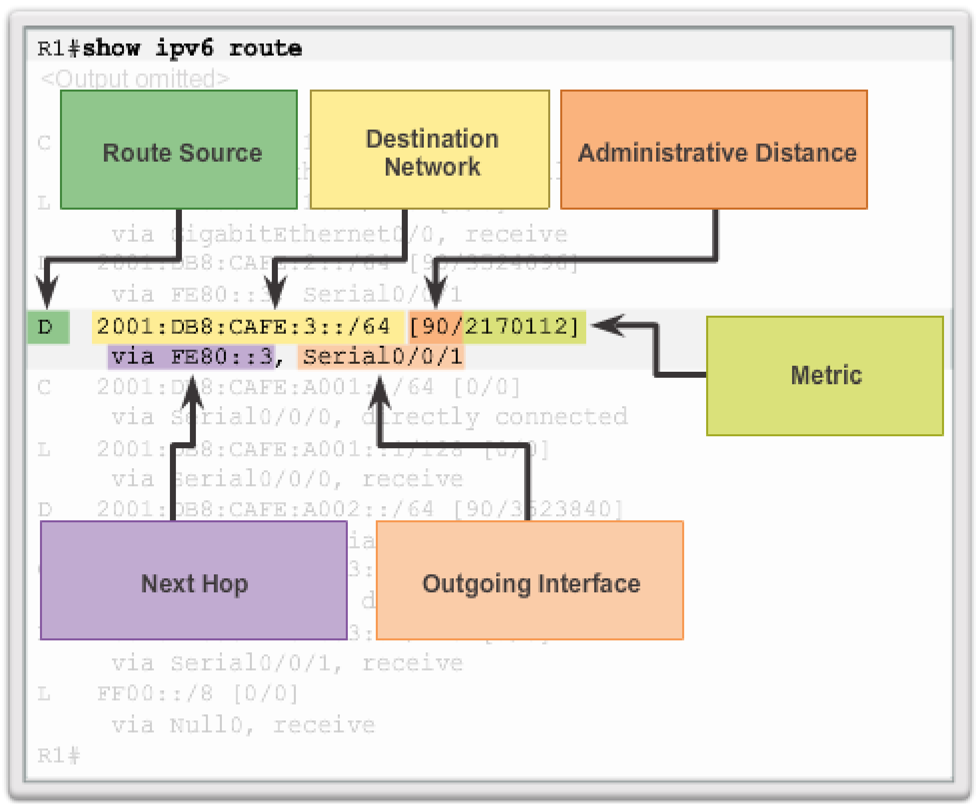
Analyze an IPVv6 Routing Table

Remote IPv6 Network Entries

Remote Network Entries on R1

```
R1#show ipv6 route
<Output omitted>

C    2001:DB8:CAFE:1::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:CAFE:1::1/128 [0/0]
      via GigabitEthernet0/0, receive
D    2001:DB8:CAFE:2::/64 [90/3524096]
      via FE80::3, Serial0/0/1
D    2001:DB8:CAFE:3::/64 [90/2170112]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A001::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:CAFE:A001::1/128 [0/0]
      via Serial0/0/0, receive
D    2001:DB8:CAFE:A002::/64 [90/3523840]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A003::/64 [0/0]
      via Serial0/0/1, directly connected
L    2001:DB8:CAFE:A003::1/128 [0/0]
      via Serial0/0/1, receive
L    FF00::/8 [0/0]
      via Null0, receive
R1#
```

Remote Network Entries on R1



3.4 Summary

Chapter 3: Summary

Dynamic routing protocols:

- Used by routers to automatically learn about remote networks from other routers.
- Purpose includes: discovery of remote networks, maintaining up-to-date routing information, choosing the best path to destination networks, and ability to find a new best path if the current path is no longer available.
- Best choice for large networks but static routing is better for stub networks.
- Function to inform other routers about changes.

Chapter 3: Summary (cont.)

Dynamic routing protocols:

- Responsible for discovering remote networks, as well as maintaining accurate network information.
- Upon a change in the topology routing protocols propagate that information throughout the routing domain.
- Convergence: The process of bringing all routing tables to a state of consistency, where all of the routers in the same routing domain, or area, have complete and accurate information about the network. Some routing protocols converge faster than others.

Chapter 3: Summary (cont.)

Dynamic routing protocols:

- Cisco routers use the administrative distance value to determine which routing source to use.
- Each dynamic routing protocol has a unique administrative value, along with static routes and directly connected networks.
- Directly connected networks are preferred source, followed by static routes and then various dynamic routing protocols.

Chapter 3: Summary (cont.)

Dynamic routing protocols:

- Each dynamic routing protocol has a unique administrative value, along with static routes and directly connected networks. The lower the administrative value, the more preferred the route source.
- A directly connected network is always the preferred source, followed by static routes and then various dynamic routing protocols.
- Routing table entries contain a route source, a destination network, and an outgoing interface.
- Route sources can be either connected, local, static, or from a dynamic routing protocol.
- IPv4 routing tables can contain four types of routes: ultimate routes, level 1 routes, level 1 parent routes, and level 2 child routes.
- Because IPv6 is classless by design, all routes are effectively level 1 ultimate routes. There is no level 1 parent of level 2 child routes.

Section 3.1

Terms and Commands

- Static routing
- Dynamic routing
- RIPv1
- RIPv2
- OSPF
- IS-IS
- IGRP
- EIGRP
- BGP
- Routing table
- Stub network
- Update messages

Section 3.2
Terms and Commands

- `router rip`
- `no router rip`
- `network` *network-address*
- `show ip protocols`
- `show ip route`
- `version 2`
- `no version`
- `no auto-summary`
- `passive-interface`
- `passive-interface default`
- `no passive-interface`
- `ip route 0.0.0.0 0.0.0.0`
- `default-information originate`

Section 3.3
Terms and Commands

- Classful routing
- Classless addressing
- Route source (C and L)
- Destination network
- Outgoing interface
- Administrative distance (AD)
- Metric
- Route timestamp
- Ultimate route
- Level 1 route
- Level 1 parent route
- Level 2 child route
- Network route
- Supernet route
- Default route

Cisco | Networking Academy®
Mind Wide Open™

Chapter 4: Enhanced Interior Gateway Protocol (EIGRP)

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 4

Chapter 4: Objectives

- Describe the features and operation of EIGRP.
- Examine the different EIGRP packet formats.
- Calculate the composite metric used by the Diffusing Update Algorithm (DUAL).
- Describe the concepts and operation of DUAL.
- Examine the commands to configure and verify basic EIGRP operations for IPv4 and IPv6.

4.1 Characteristics of EIGRP

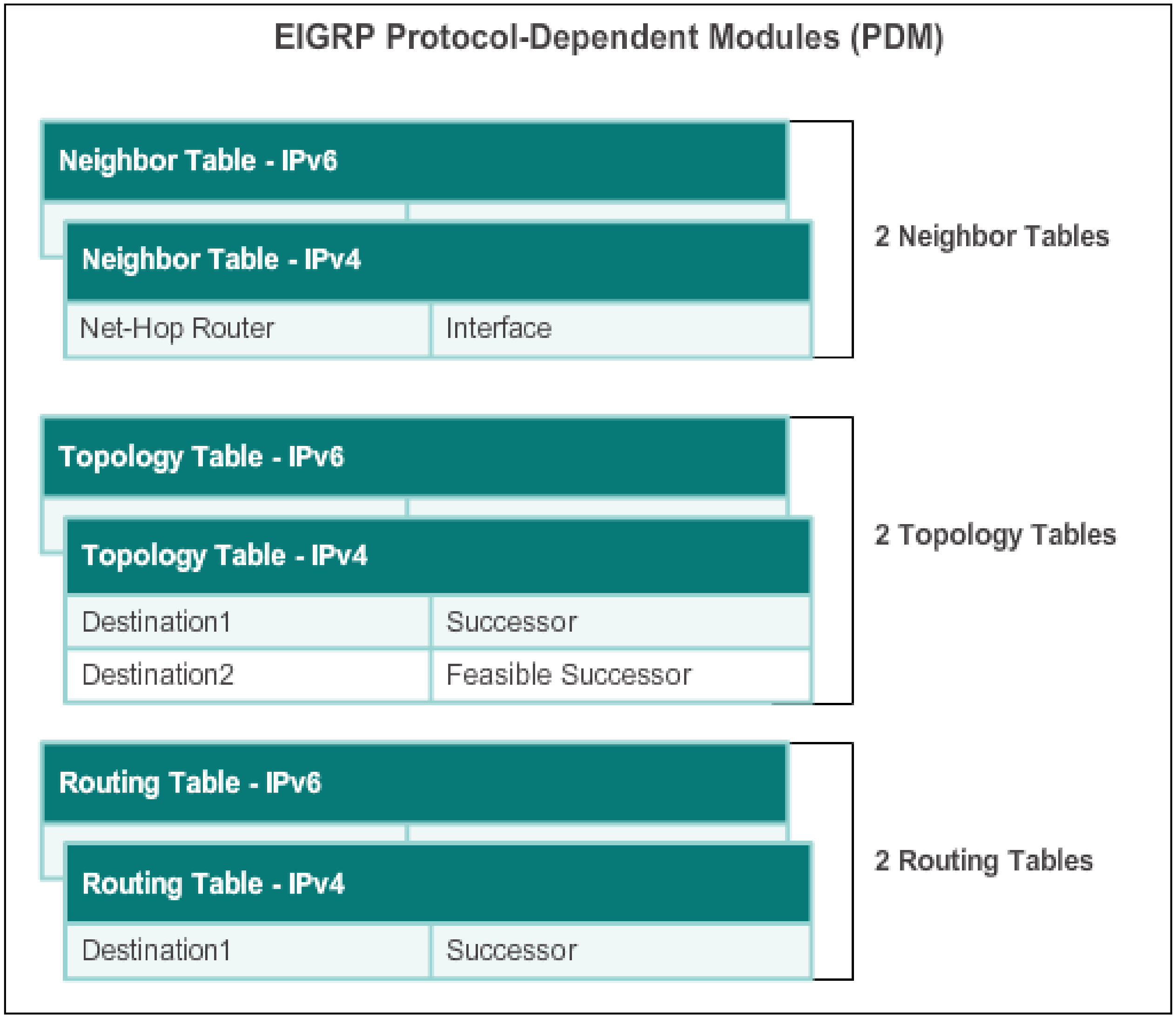
Cisco | Networking Academy®
Mind Wide Open™

Basic Features of EIGRP

Features of EIGRP

- Released in 1992 as a Cisco proprietary protocol.
- 2013 basic functionality of EIGRP released as an open standard.
- Advanced Distance Vector routing protocol.
- Uses the Diffusing Update Algorithm (DUAL) to calculate paths and back-up paths.
- Establishes Neighbor Adjacencies.
- Uses the Reliable Transport Protocol to provide delivery of EIGRP packets to neighbors.
- Partial and Bounded Updates. Send updates only when there is a change and only to the routers that need the information.
- Supports Equal and Unequal Cost Load Balancing.

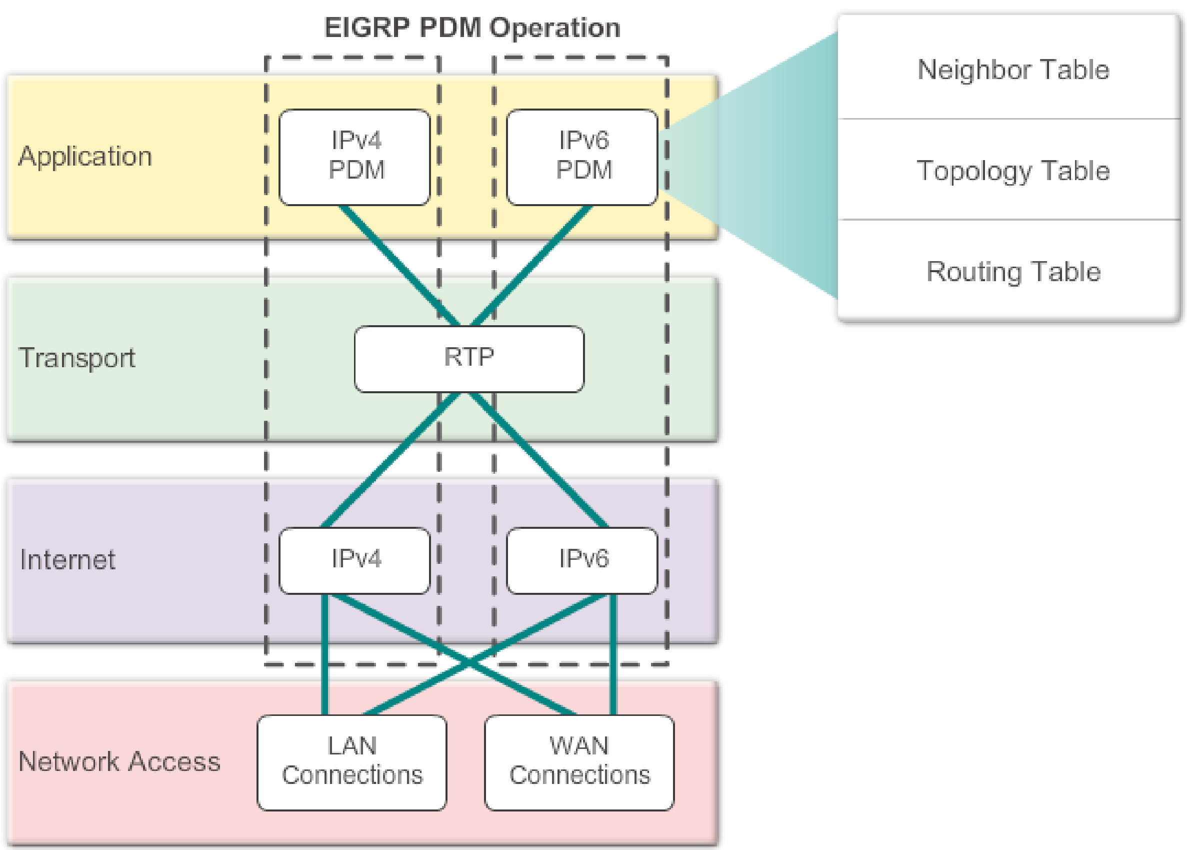
Basic Features of EIGRP
Protocol Dependent Modules



Basic Features of EIGRP

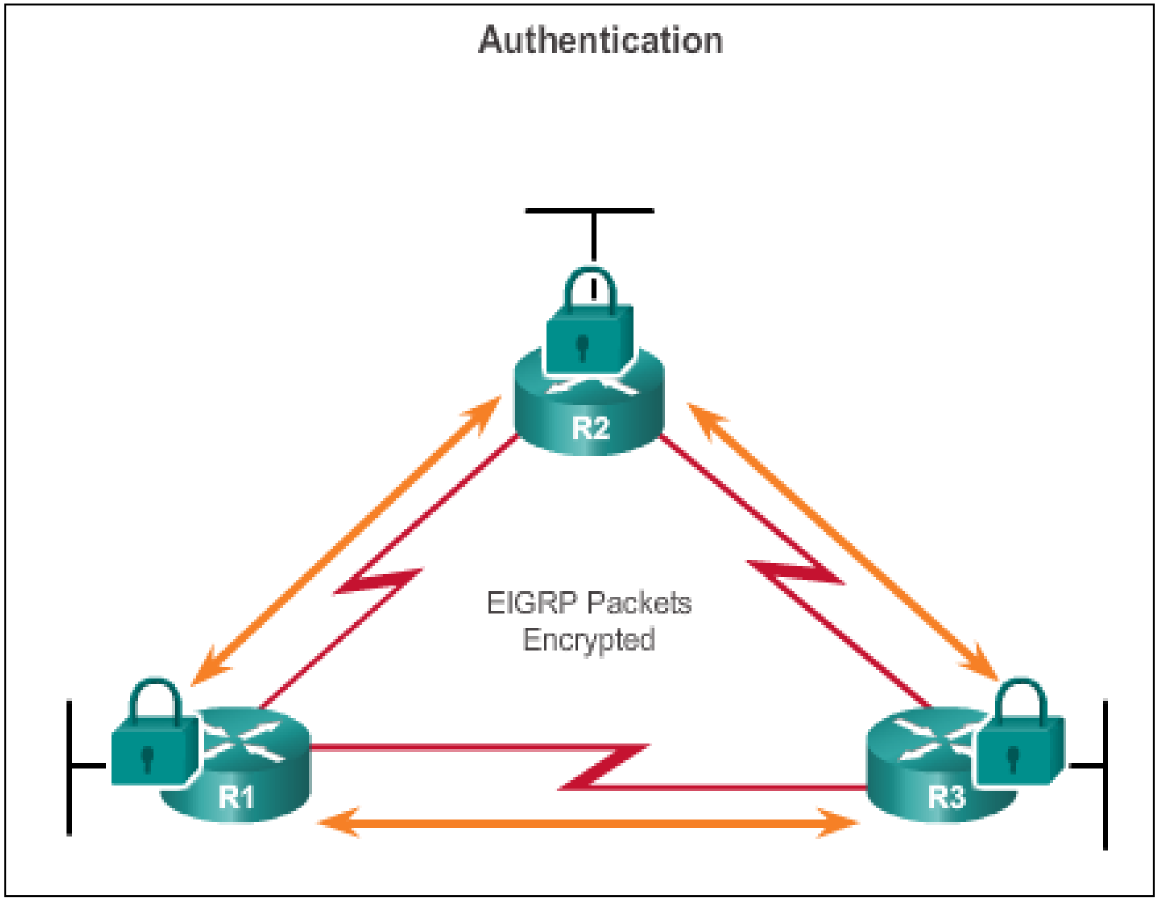
Reliable Transport Protocol

EIGRP Replaces TCP with RTP



Basic Features of EIGRP
Authentication

- EIGRP can be configured to authenticate routing information.
- Ensures routers only accept updates from routers that have been configured with the correct authentication information.



Types of EIGRP Packets
EIGRP Packet Types

Packet Type	Description
Hello	Used to discover other EIGRP routers in the network.
Acknowledgement	Used to acknowledge the receipt of any EIGRP packet.
Update	Convey routing information to known destinations.
Query	Used to request specific information from a neighbor router.
Reply	Used to respond to a query.

Types of EIGRP Packets

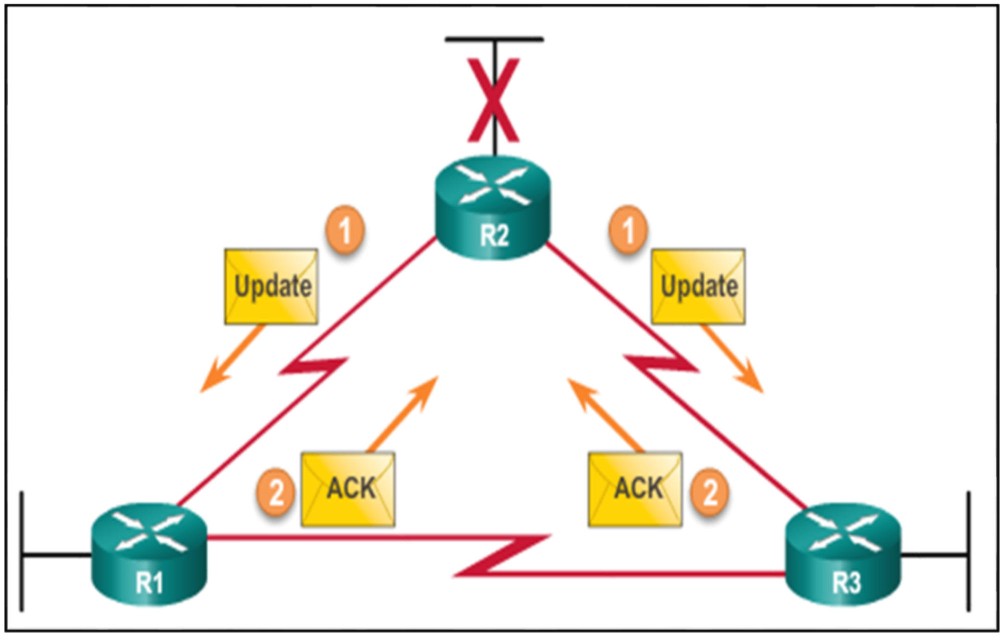
EIGRP Hello Packets

- Used to discover EIGRP neighbors.
- Used to form and maintain EIGRP neighbor adjacencies.
- Sent as IPv4 or IPv6 multicasts.
- IPv4 multicast address 224.0.0.10.
- IPv6 multicast address FF02::A.
- Unreliable delivery.
- Sent every 5 seconds (every 60 seconds on low-speed NBMA networks).
- EIGRP uses a default Hold timer of three times the Hello interval before declaring neighbor unreachable.

Types of EIGRP Packets

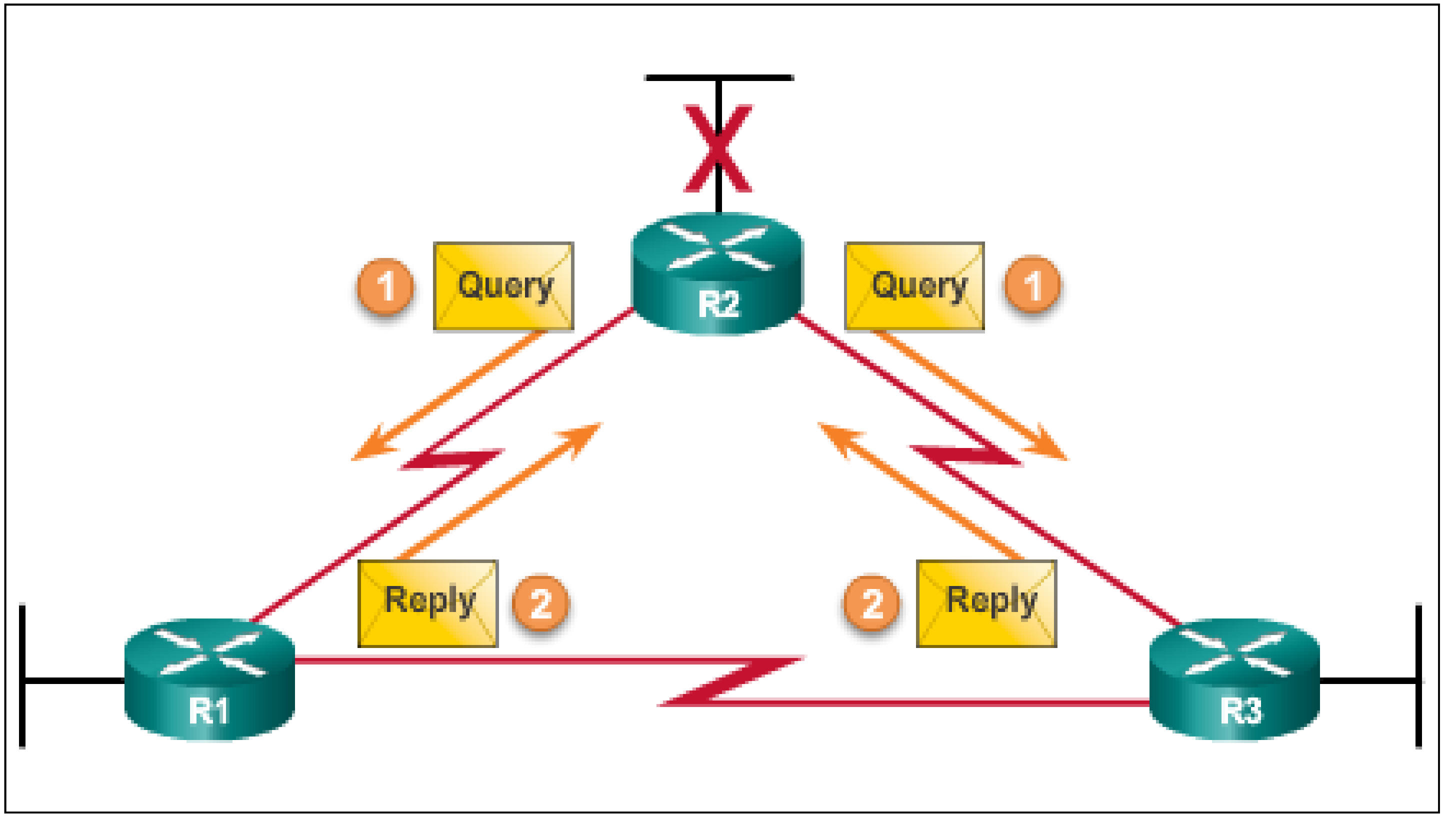
EIGRP Update & Acknowledgement Packets

- Update packets are sent to propagate routing information, only when necessary.
- Sends **Partial** updates – only contains information about route changes.
- Sends **Bounded** updates- sent only to routers affected by the change.
- Updates use reliable delivery, therefore, require an **acknowledgement**.



EIGRP Query and Reply Packets

- Used when searching for networks.
- Queries use reliable delivery, which can be multicast or unicast.
- Replies use reliable delivery.



EIGRP Messages

Encapsulating EIGRP Messages

Type/Length/Values Types

Data Link Frame Header	IP Packet Header	EIGRP Packet Header	TLV Types

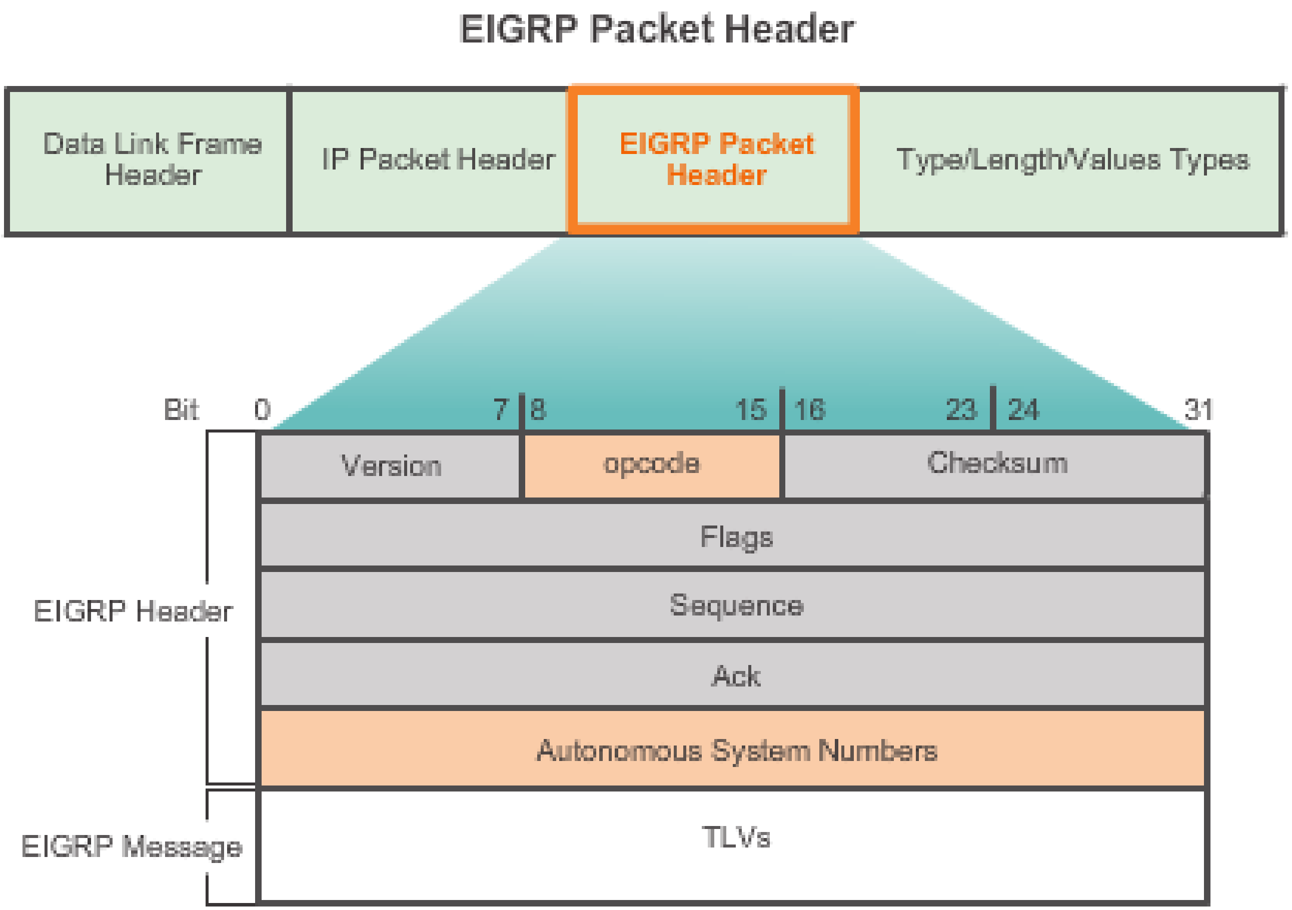
Data Link Frame
MAC Source Address = Address of sending interface
MAC Destination Address = Multicast: 01-00-5E-00-00-0A

IP Packet
IPv4 Source Address = Address of sending interface
IPv4 Destination Address = Multicast: 224.0.0.10
Protocol field = 88 for EIGRP

EIGRP Packet Header
Opcode for EIGRP packet type
Autonomous System Number

TLV Types
Some types include:
0x0001 EIGRP Parameters
0x0102 IP Internal Routes
0x0103 IP External Routes

EIGRP Packet Header and TLV



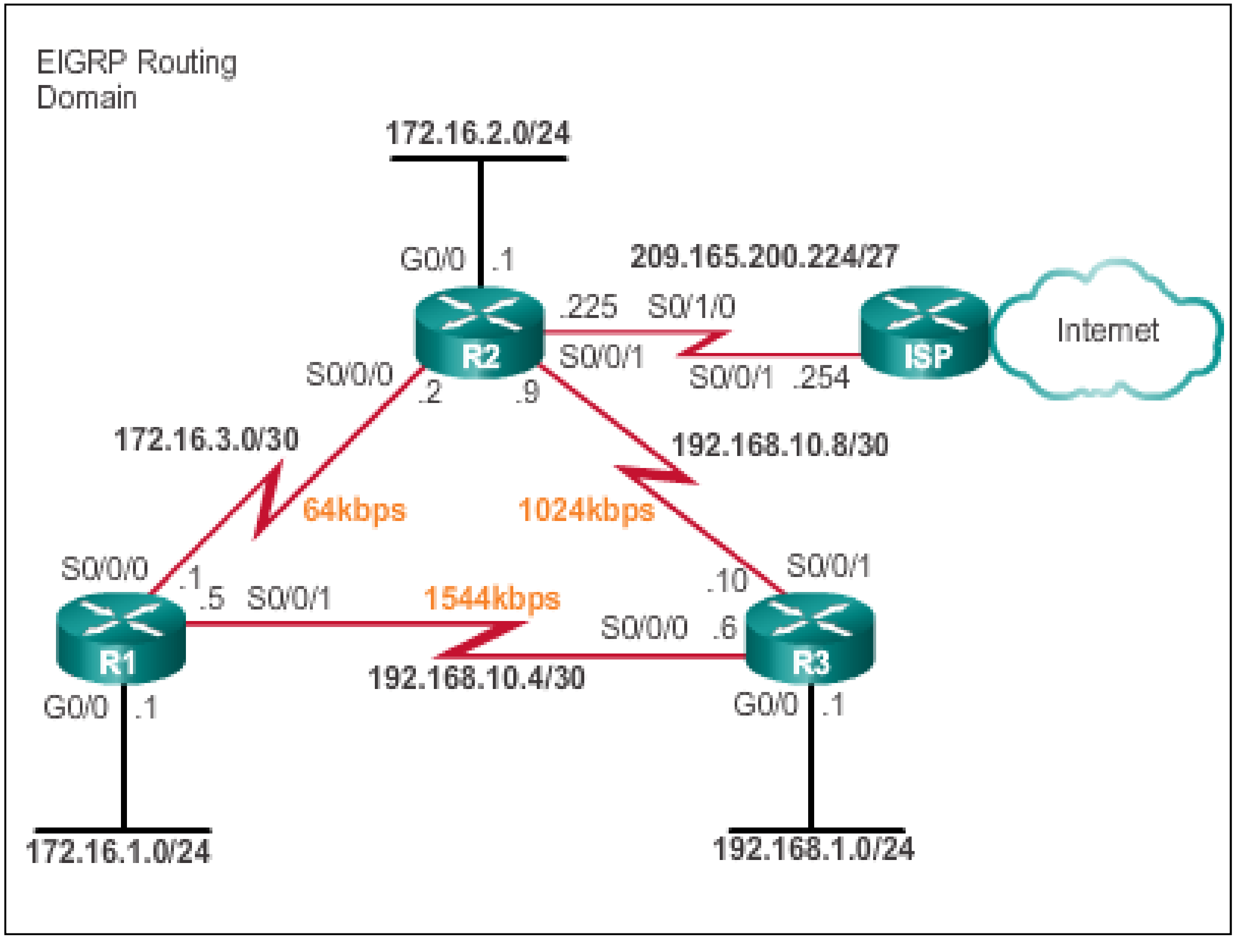
- **Opcode:** EIGRP Packet Type: Update (1), Query (3), Reply(4), Hello (5)
- **Autonomous System Number:** ID for this EIGRP routing process

4.2 Configuring EIGRP for IPv4

Cisco | Networking Academy®
Mind Wide Open™

EIGRP Network Topology

This course uses the topology that configures EIGRP with IPv4.



Configuring EIGRP with IPv4

Autonomous System Numbers

- The **`router eigrp`** *`autonomous-system`* command enables the EIGRP process.
- The autonomous system number is only significant to the EIGRP routing domain.
- The EIGRP autonomous system number is not associated with the Internet Assigned Numbers Authority (IANA) globally assigned autonomous system numbers used by external routing protocols.
- Internet Service Providers (ISPs) require an autonomous system number from IANA.
- ISPs often use the Border Gateway Protocol (BGP), which does use the IANA autonomous system number in its configuration.

Configuring EIGRP with IPv4

Router EIGRP Command

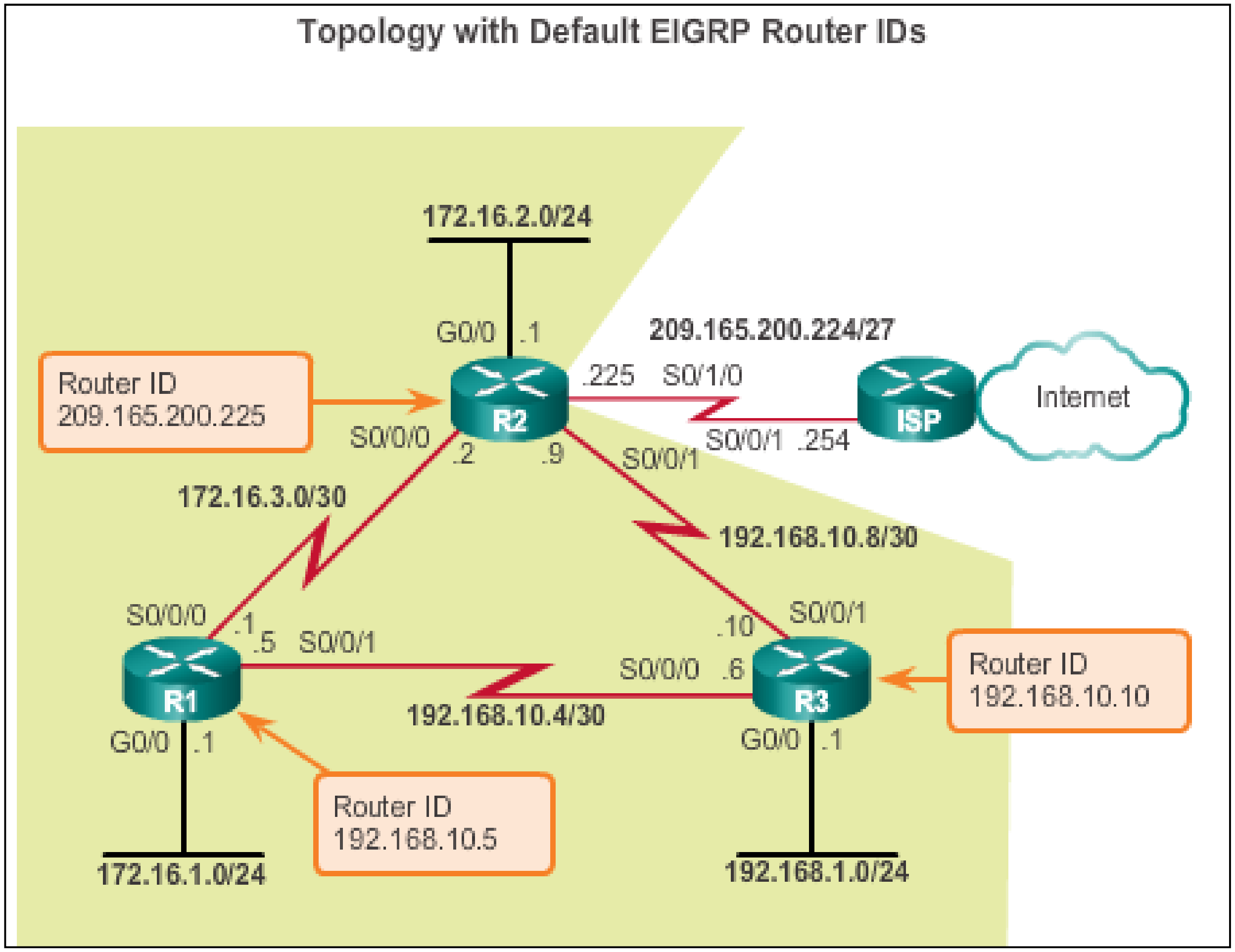
Router(config)# **router eigrp** *autonomous-system*

```
R1(config)#router eigrp 1
R1(config-router)#
```

To completely remove the EIGRP routing process from a device, use the **no router eigrp** *autonomous-system* command.

EIGRP Router ID

Used in both EIGRP and OSPF routing protocols, the router ID's role is more significant in OSPF.



Configuring the EIGRP Router ID

- Configuring the EIGRP router ID

```
Router(config)# router eigrp autonomous-system
Router(config-router)# eigrp router-id ipv4-address
```

- The IPv4 loopback address can be used as the router ID.
- If the **eigrp** *router-id* value is not configured, the highest loopback address is selected as the router ID.
- Configuring a loopback interface

```
Router(config)# interface loopback number
Router(config-if)# ip addressipv4-address subnet-mask
```

Configuring EIGRP with IPv4

Network Command

- Enables any interface on this router that matches the network address in the **`network`** router configuration mode command to send and receive EIGRP updates.
- These networks are included in EIGRP routing updates.

Enables EIGRP for the interfaces on subnets in 172.16.1.0/24 and 172.16.3.0/30.

```
R1(config)# router eigrp 1
R1(config-router)# network 172.16.0.0
R1(config-router)# network 192.168.10.0
R1(config-router)#
```

Enables EIGRP for the interfaces on subnet 192.168.10.4/30.

Configuring EIGRP with IPv4

Network Command

The **`eigrp log-neighbor-changes`** router configuration mode

- On by default
- Displays changes in neighbor adjacencies
- Verifies neighbor adjacencies during configuration
- Indicates when any adjacencies have been removed

Configuring EIGRP with IPv4

The Network Command and Wildcard Mask

- To configure EIGRP to advertise specific subnets only, use the *wildcard-mask* option with the **`network`** command.

  Router(config-router)# **network** *network address* [*wildcard-mask*]

- The wildcard mask is the inverse of the subnet mask.
- To calculate the wildcard mask, subtract the subnet mask from 255.255.255.255:

```
      255.255.255.255
   -- 255.255.255.252
        0.  0.  0.  3   wildcard mask
```

- **Note**: Some IOS versions also let you enter the subnet mask instead of a wildcard mask.

Passive Interface

- Use the `passive-interface` command to:
  - Prevent neighbor adjacencies
  - Suppress unnecessary update traffic
  - Increase security controls, such as preventing unknown rogue routing devices from receiving EIGRP updates
- To configure:

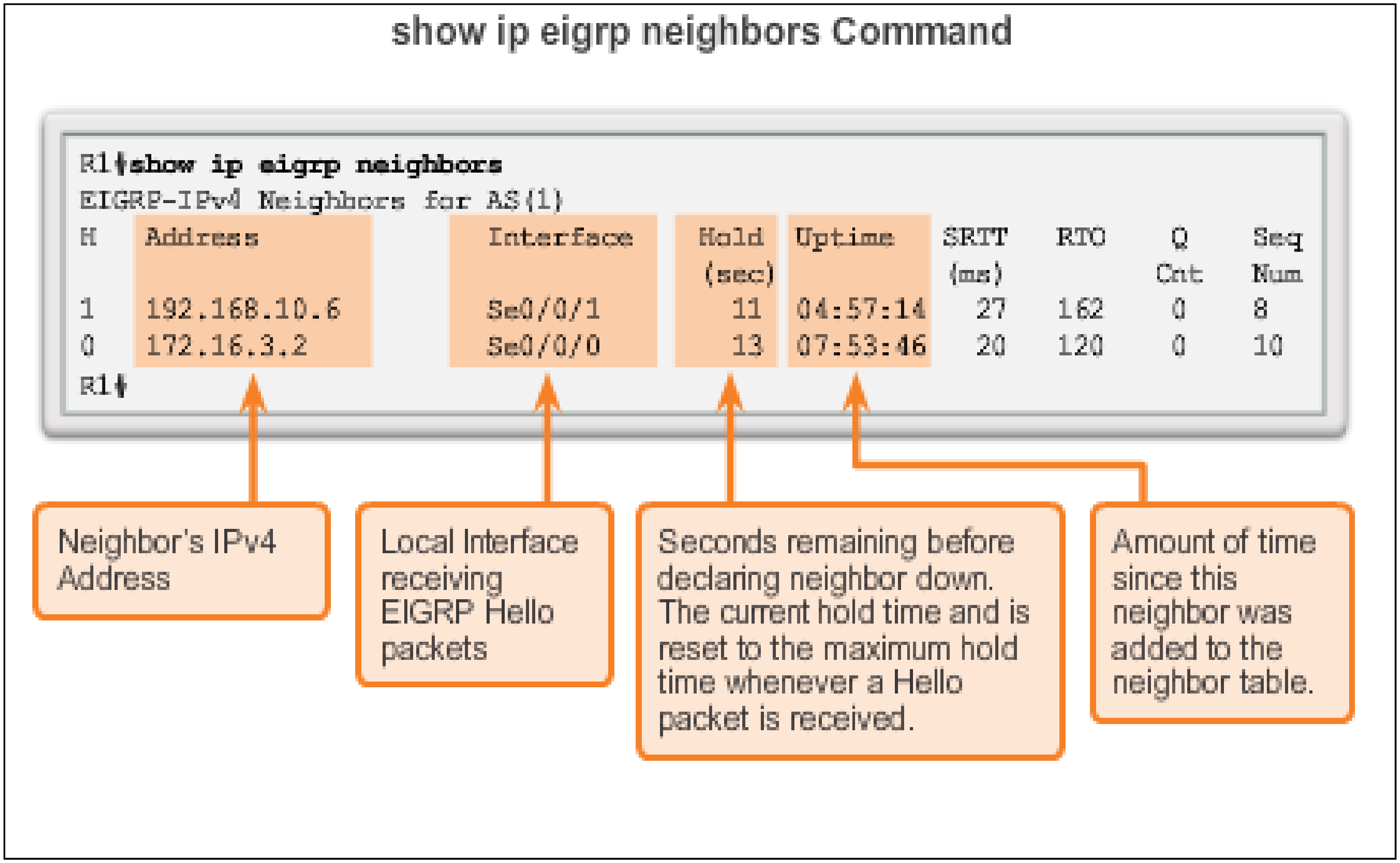
```
Router(config)# router eigrp as-number
Router(config-router)# passive-
interface interface-type interface-number
```

- To verify:

```
Router# show ip protocols
```

Configuring EIGRP with IPv4

Verifying EIGRP: Examining Neighbors




```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address          Interface     Hold  Uptime    SRTT  RTO   Q    Seq
                                   (sec)           (ms)        Cnt  Num
1   192.168.10.6     Se0/0/1        11   04:57:14   27   162   0    8
0   172.16.3.2       Se0/0/0        13   07:53:46   20   120   0    10
R1#
```

Configuring EIGRP with IPv4

Verifying EIGRP: `show ip protocols` Command

`show ip protocols` Command

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.6          90      00:40:20
    172.16.3.2            90      00:40:20
  Distance: internal 90 external 170

R1#
```

1. Routing protocol and Process ID (AS Number)
2. EIGRP Router ID
3. EIGRP Administrative Distances
4. EIGRP Automatic Summarization is disabled.
5. EIGRP Routing Information Sources lists all the EIGRP routing sources the IOS uses to build its IPv4 routing table.

Configuring EIGRP with IPv4

Verifying EIGRP: Examine the IPv4 Routing Table

R1's IPv4 Routing Table

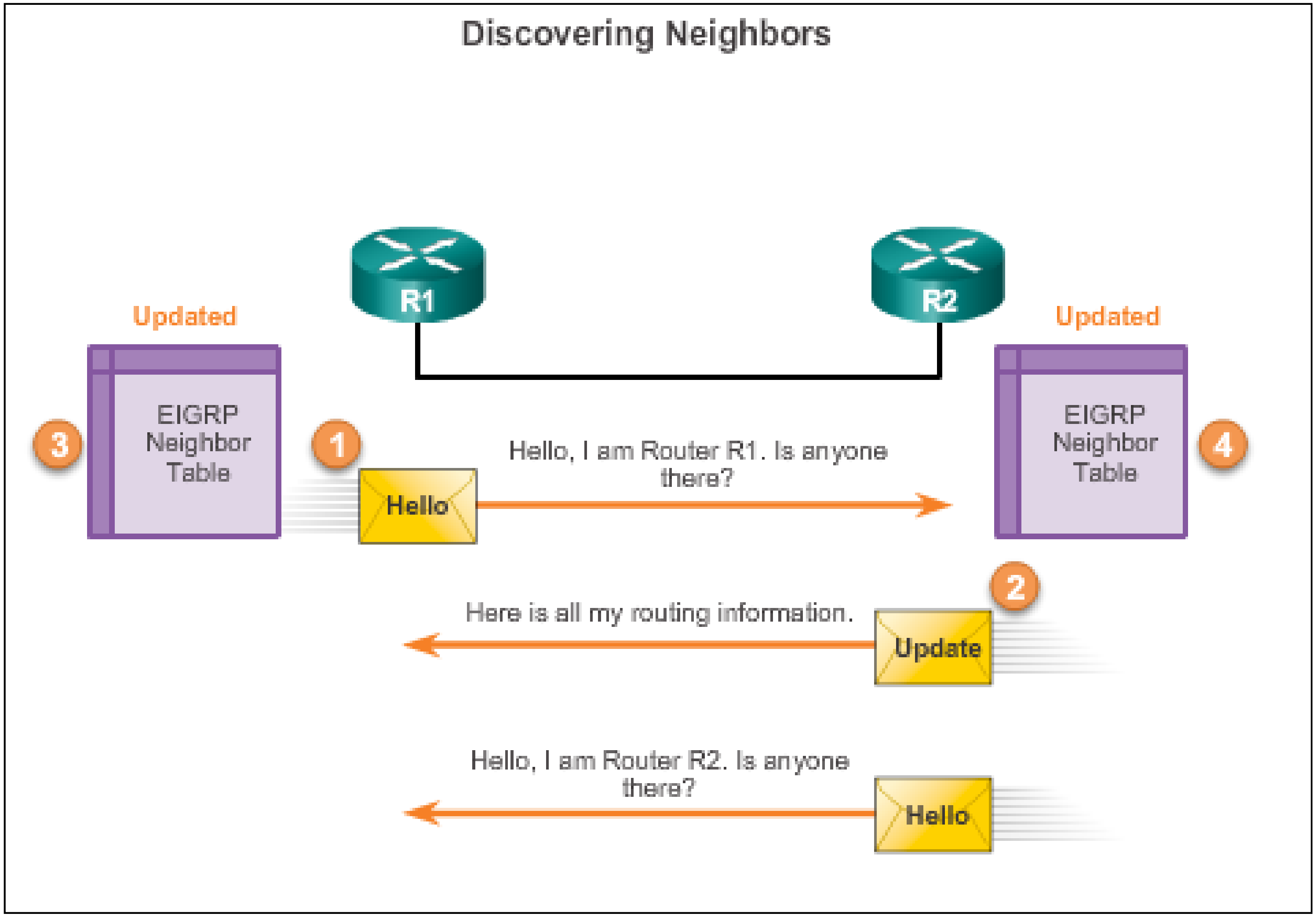
```
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
D        172.16.2.0/24 [90/2170112] via 172.16.3.2,
00:14:35, Serial0/0/0
C        172.16.3.0/30 is directly connected, Serial0/0/0
L        172.16.3.1/32 is directly connected, Serial0/0/0
D     192.168.1.0/24 [90/2170112] via 192.168.10.6,
00:13:57, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2
masks
C        192.168.10.4/30 is directly connected,
Serial0/0/1
L        192.168.10.5/32 is directly connected,
Serial0/0/1
D        192.168.10.8/30 [90/2681856] via 192.168.10.6,
00:50:42, Serial0/0/1
                         [90/2681856] via 172.16.3.2,
00:50:42, Serial0/0/0
R1#
```

4.3 Operation of EIGRP

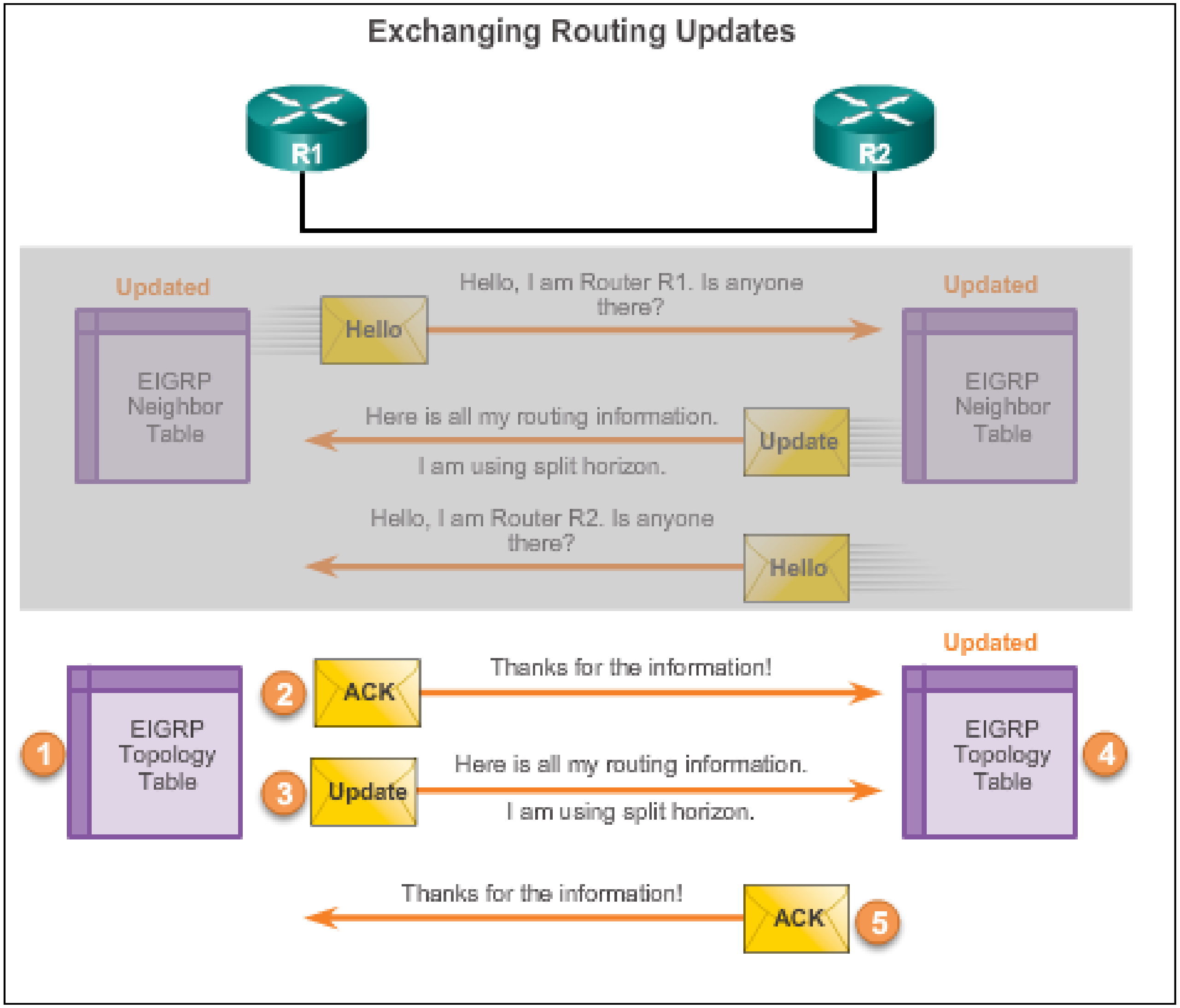
Cisco | Networking Academy®
Mind Wide Open™

EIGRP Initial Route Discovery

EIGRP Neighbor Adjacency



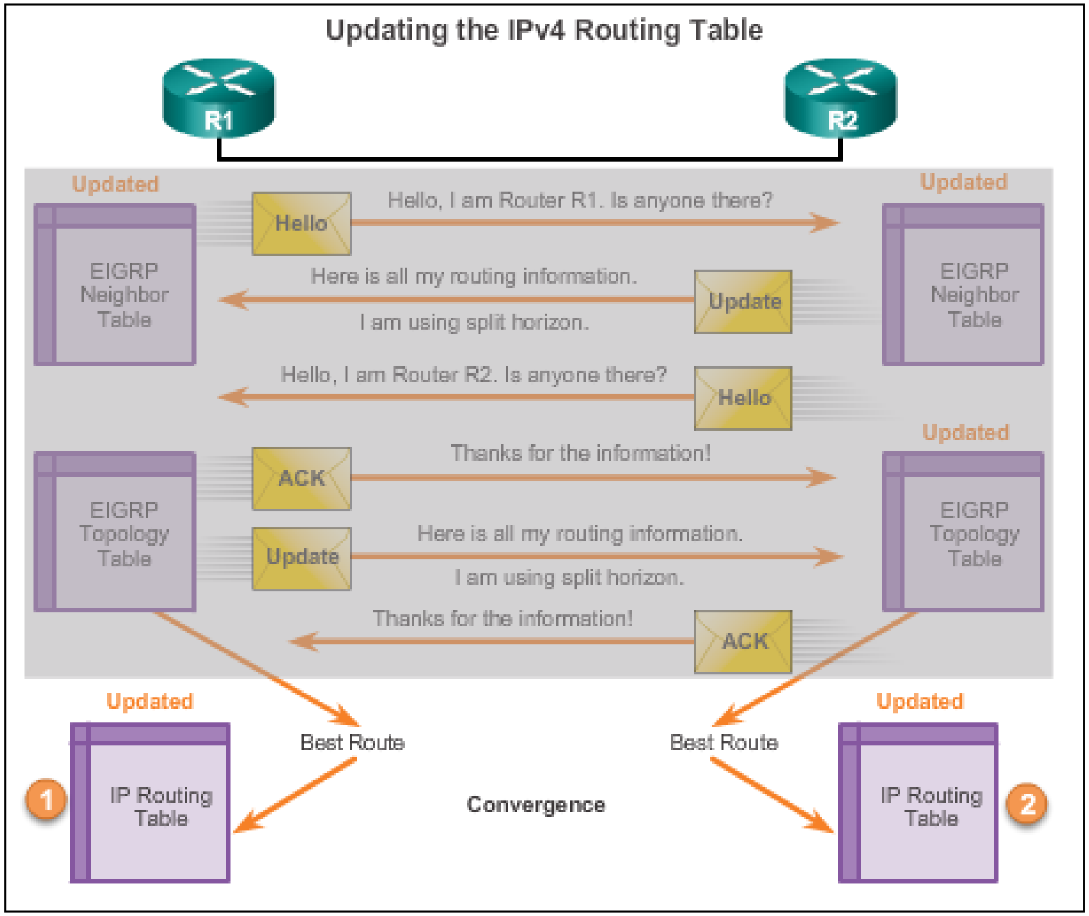
EIGRP Initial Route Discovery
EIGRP Topology Table

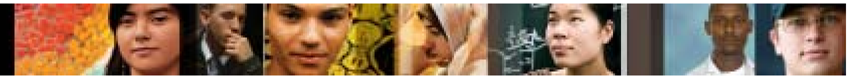


EIGRP Initial Route Discovery

EIGRP Convergence

Convergence – All routers have the correct, most up-to-date information about the network.





Metrics

EIGRP Composite Metric

EIGRP Composite Metric

Default Composite Formula:
metric = **[K1*bandwidth + K3*delay]**

Complete Composite Formula:
metric = **[K1*bandwidth + (K2*bandwidth)/(256 - load)+K3*delay] * [K5/(reliability + K4)]**

(Not used if "K" values are 0)

Note: This is a conditional formula. If K5 = 0, the last term is replaced by 1 and the formula becomes: Metric = [K1 * bandwidth + (K2 * bandwidth)/(256 load) + K3 * delay]

Default values:
K1 (bandwidth) = 1
K2 (load) = 0
K3 (delay) = 1
K4 (reliability) = 0
K5 (reliability) = 0

"K" values can be changed with the **metric weights** command

```
Router(config-router)# metric weights tos k1 k2 k3 k4 k5
```

Examining Interface Values

- BW – Bandwidth of the interface (in Kilobits per second).
- DLY – Delay of the interface (microseconds).
- Reliability – Reliability of interface; by default, the value is not included in the computing metric.
- Txload, Rxload – By default, the value is not included in the computing metric.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
<Output omitted>
R1#

R1#show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0 (bia
fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<Output omitted>
R1#
```

Metrics

Bandwidth Metric

- Use the **`show interfaces`** command to verify bandwidth.
- Most serial bandwidths are set to 1,544 kb/s (default).
- A correct value for bandwidth is very important in order to calculate the correct metric (both sides of link must have same bandwidth).

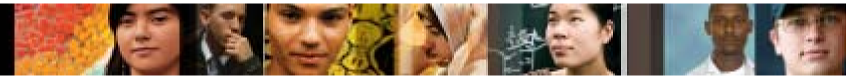
```
R1(config)# interface s 0/0/0
R1(config-if)# bandwidth 64
```

```
R1# show interface s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<Output omitted>
```

Delay Metric

Interface Delay Values

Media	Delay
Ethernet	1,000
Fast Ethernet	100
Gigabit Ethernet	10
16M Token Ring	630
FDDI	100
T1 (Serial Default)	20,000
DS0 (64 Kbps)	20,000
1024 Kbps	20,000
56 Kbps	20,000



Metrics

Calculating the EIGRP Metric

Step 1. Determine the link with the slowest bandwidth. Use that value to calculate bandwidth (10,000,000/bandwidth).

Step 2. Determine the delay value for each outgoing interface on the way to the destination. Add the delay values and divide by 10 (sum of delay/10).

Step 3. Add the computed values for bandwidth and delay, and multiply the sum by 256 to obtain the EIGRP metric.

[K1 * bandwidth + K3 * delay] * 256 = Metric

Since K1 and K3 both equal 1, the formula simplifies to:

(Bandwidth + Delay) * 256 = Metric

((10,000,000 / bandwidth) + (sum of delay / 10)) * 256 = Metric

```
R2# show ip route

D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:12:32, Serial0/0/1
```

DUAL and the Topology Table

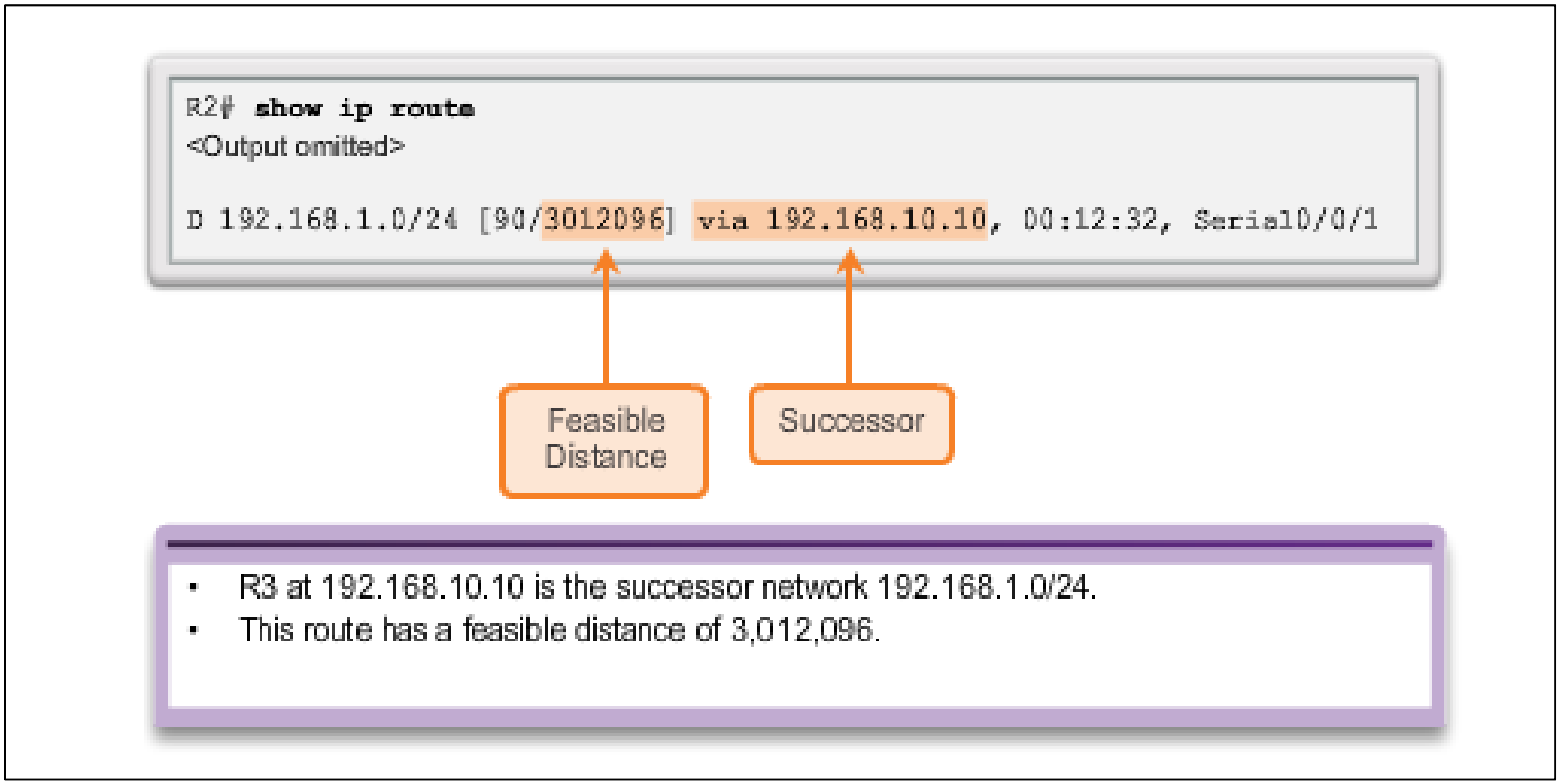
DUAL Concepts

- **Diffusing Update ALgorithm (DUAL)** provides the following:
  - Loop-free paths and loop-free backup paths
  - Fast convergence
  - Minimum bandwidth usage with bounded updates
- The decision process for all route computations is done by the **DUAL Finite State Machine (FSM)**
  - DUAL FSM tracks all routes.
  - Uses EIGRP metrics to select efficient, loop-free paths.
  - Identifies the routes with the least-cost path to be inserted into the routing table.
- EIGRP maintains a list of backup routes that DUAL has already determined that can be used immediately if the primary path fails.

DUAL and the Topology Table

Successor and Feasible Distance

- The **Successor** is the least-cost route to the destination network.
- The **Feasible Distance** (FD) is the lowest calculated metric to reach the destination network.



Feasible Successors, Feasibility Condition, and Reported Distance

- **Feasible Successor** (FS) is a neighbor that has a loop-free backup path to the same network as the successor, and it satisfies the Feasibility Condition (FC).
- **Feasibility Condition** (FC) is met when a neighbor's Reported Distance (RD) to a network is less than the local router's feasible distance to the same destination network.
- **Reported Distance** (RD) is an EIGRP neighbor's feasible distance to the same destination network.

DUAL and the Topology Table

Topology Table: show ip eigrp Command

```
R2#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.2.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
        via 192.168.10.10 (3523840/2169856), Serial0/0/1
        via 172.16.3.1 (41024000/2169856), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3012096
        via 192.168.10.10 (3012096/2816), Serial0/0/1
        via 172.16.3.1 (41024256/2170112), Serial0/0/0
```

```
R2#show ip eigrp topology
<Output omitted>

P 192.168.1.0/24, 1 successors, FD is 3012096
        via 192.168.10.10 (3012096/2816), Serial0/0/1
        via 172.16.3.1 (41024256/2170112), Serial0/0/0
```

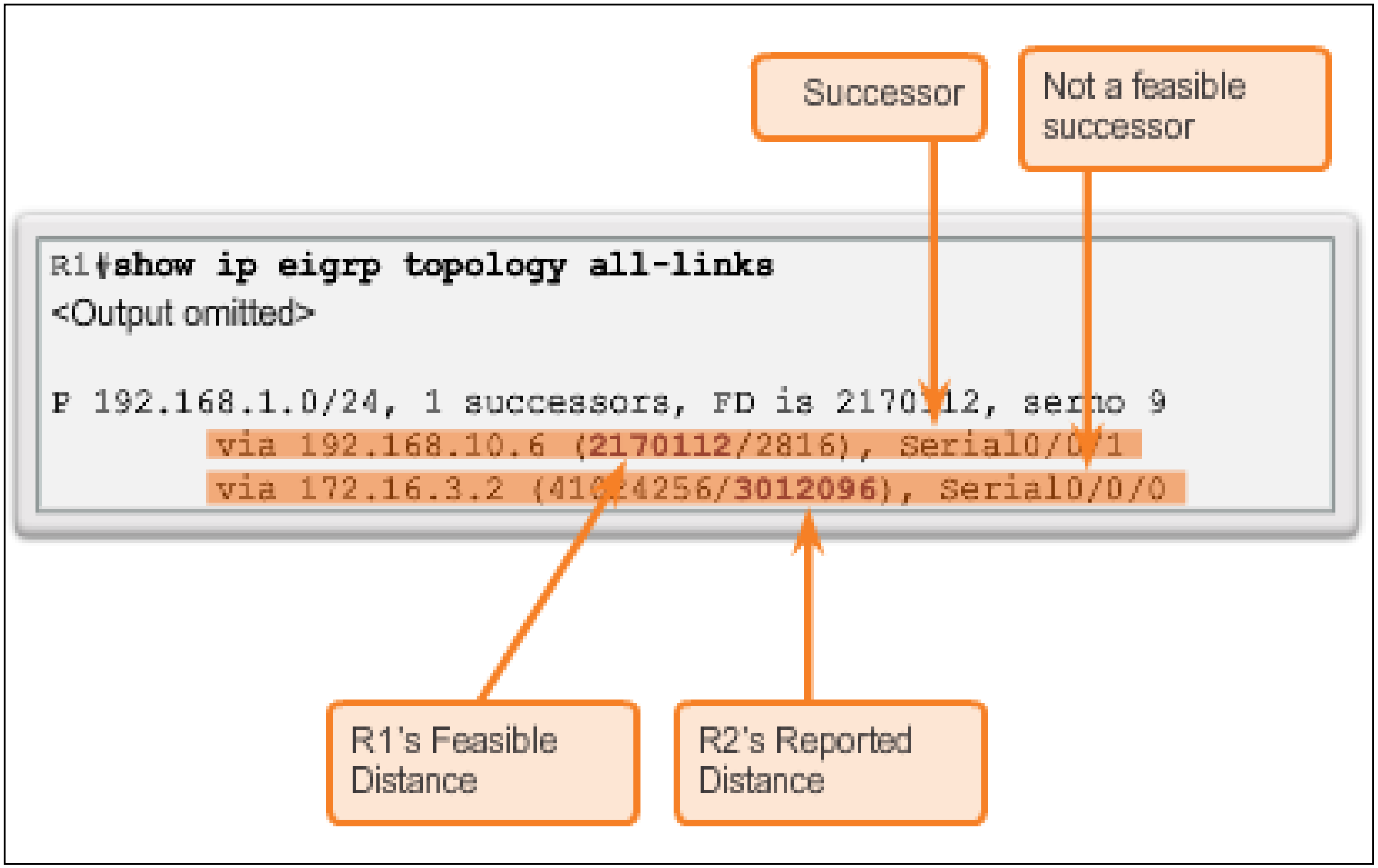
- Next hop address of the successor
- Feasible distance
- Successor's (R3) Reported Distance
- Outbound interface to reach this network

```
R2#show ip eigrp topology
<Output omitted>

P 192.168.1.0/24, 1 successors, FD is 3012096
        via 192.168.10.10 (3012096/2816), Serial0/0/1
        via 172.16.3.1 (41024256/2170112), Serial0/0/0
```

- Next hop address of the feasible successor (R1)
- Feasible distance if the feasible successor (R1) was the successor
- Feasible Successor's (R1) Reported Distance
- Outbound interface to reach this network

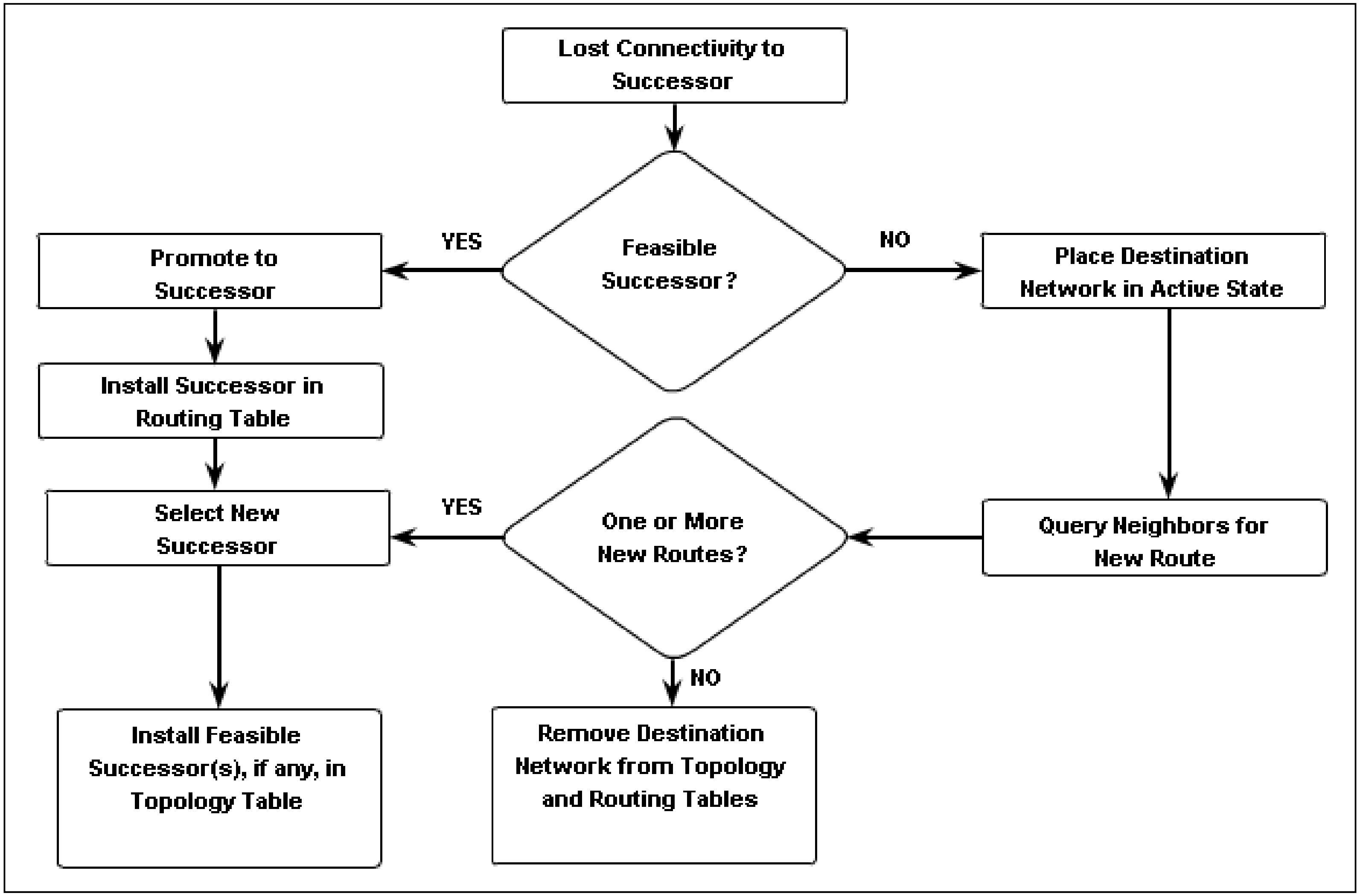
DUAL and the Topology Table

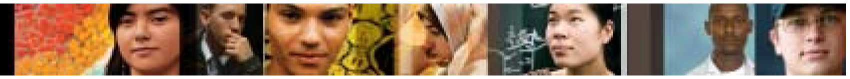
Topology Table: No Feasible Successor



DUAL and Convergence

DUAL Finite State Machine (FSM)





DUAL and Convergence

DUAL: Feasible Successor

```
R2#debug eigrp fsm
EIGRP Finite State Machine debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface s 0/0/1
R2(config-if)#shutdown
<Output omitted>
EIGRP-IPv4(1):Find FS for dest 192.168.1.0/24. FD is 3012096,
RD is 3012096 on tid 0
DUAL: AS(1) Removing dest 172.16.1.0/24, nexthop 192.168.10.10
DUAL: AS(1) RT installed 172.16.1.0/24 via 172.16.3.1
<Output omitted>
R2(config-if)#end
R2#undebug all
```

```
R2#show ip route
<Output omitted>

D 192.168.1.0/24 [90/41024256] via 172.16.3.1, 00:15:51,
Serial0/0/0
```

New Successor (R1)

DUAL and Convergence

DUAL: No Feasible Successor

```
R1#show ip eigrp topology
<Output omitted>

P 192.168.1.0/24, 1 successors, FD is 2170112
        via 192.168.10.6 (2170112/2816), Serial0/0/1
```

Successor (R3)

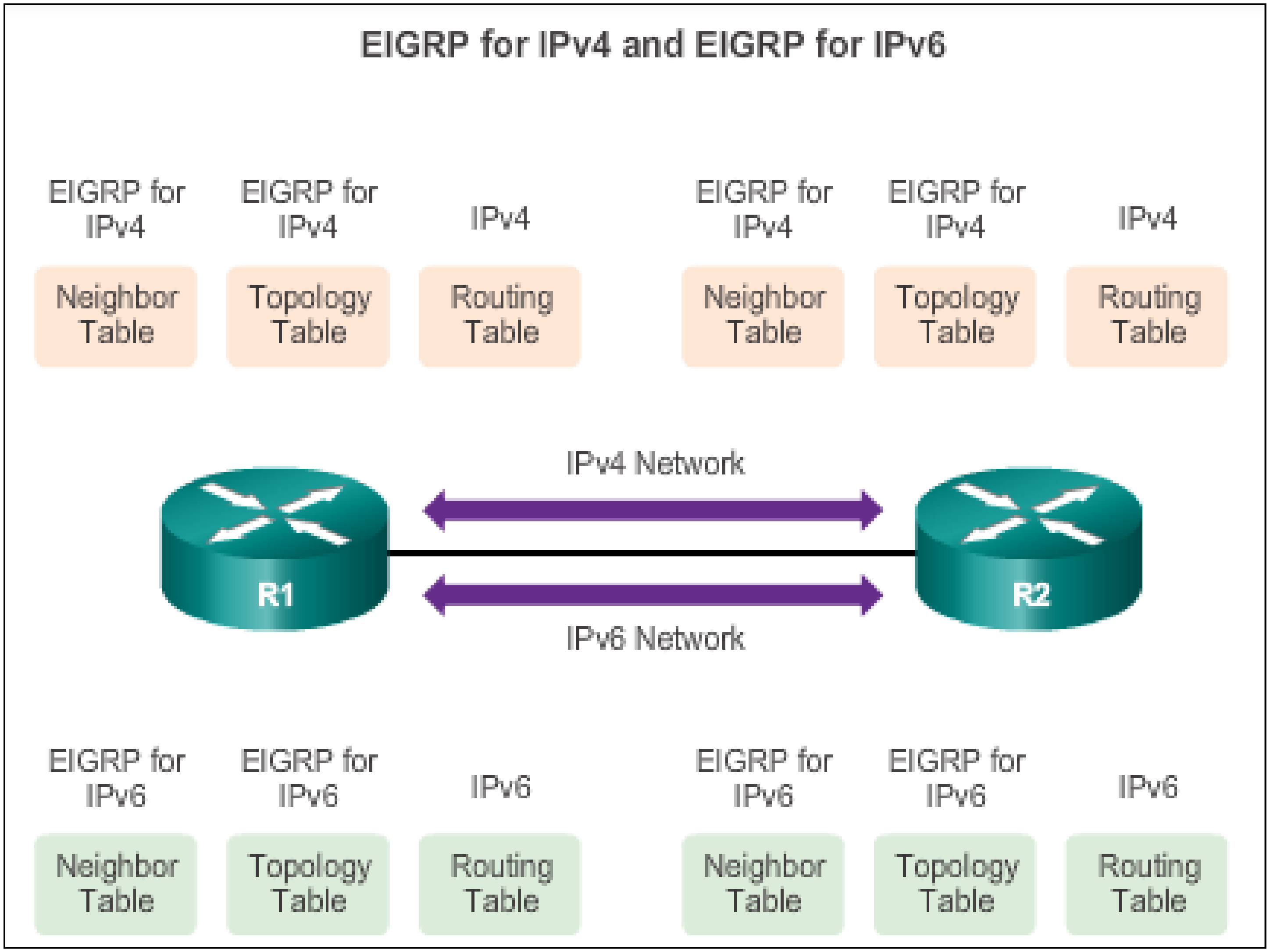
No feasible successor

```
R1#debug eigrp fsm
EIGRP Finite State Machine debugging is on
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s 0/0/1
R1(config-if)#shutdown
<Output omitted>
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is 2170112,
RD is 2170112
DUAL: AS(1) Dest 192.168.1.0/24 entering active state for tid
0.
EIGRP-IPv4(1): dest(192.168.1.0/24) active
EIGRP-IPv4(1): rcvreply: 192.168.1.0/24 via 172.16.3.2 metric
41024256/3012096 EIGRP-IPv4(1): reply count is 1
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is
72057594037927935, RD is 72057594037927935
DUAL: AS(1) Removing dest 192.168.1.0/24, nexthop 192.168.10.6
DUAL: AS(1) RT installed 192.168.1.0/24 via 172.16.3.2
<Output omitted>
R1(config-if)#end
R1#undebug all
```

4.4 Configuration of EIGRP for IPv6

Cisco | Networking Academy®
Mind Wide Open™

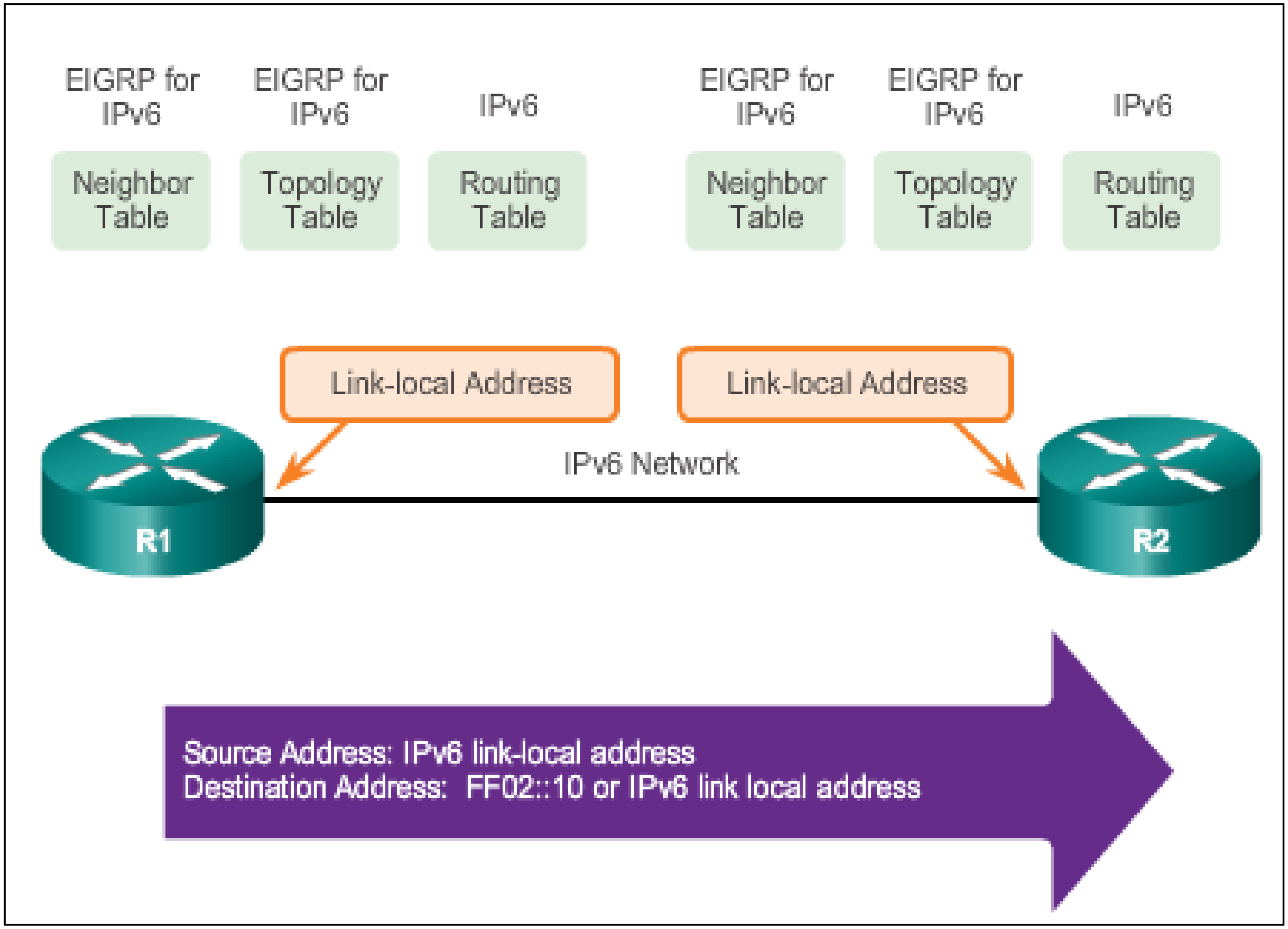
EIGRP for IPv6



Comparing EIGRP for IPv4 and IPv6

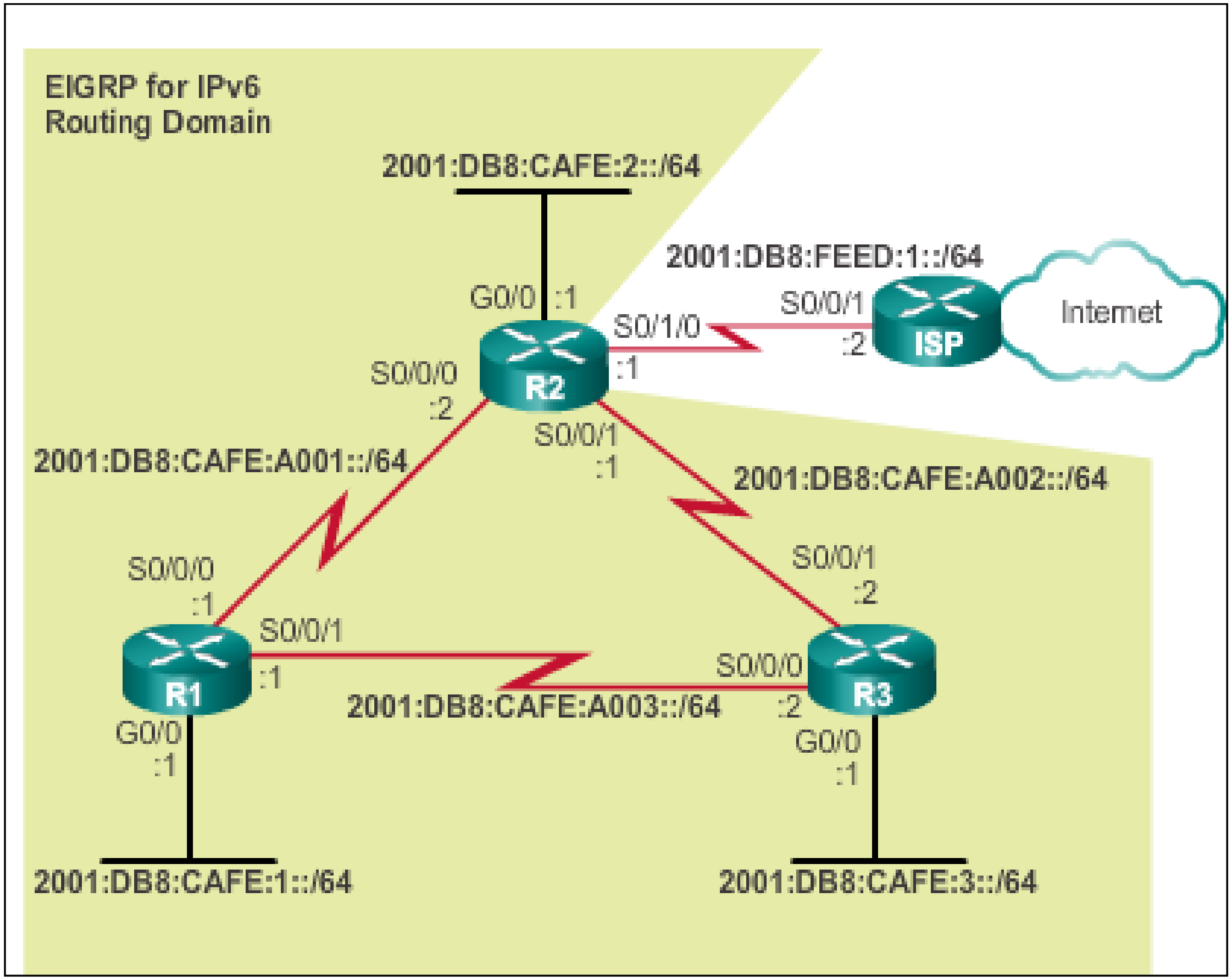
	EIGRP for IPv4	EIGRP for IPv6
Advertised routes	IPv4 networks	IPv6 prefixes
Distance vector	Yes	Yes
Convergence technology	DUAL	DUAL
Metric	Bandwidth and delay by default, reliability and load are optional	Bandwidth and delay by default, reliability and load are optional
Transport protocol	RTP	RTP
Update messages	Incremental, partial and bounded updates	Incremental, partial and bounded updates
Neighbor discovery	Hello packets	Hello packets
Source and destination addresses	IPv4 source address and 224.0.0.10 IPv4 multicast destination address	IPv6 link-local source address and FF02::10 IPv6 multicast destination address
Authentication	Plain text and MD5	MD5
Router ID	32-bit router ID	32-bit router ID

EIGRP for IPv4 vs. IPv6
IPv6 Link-local Addresses



Configuring EIGRP for IPv6

EIGRP for IPv6 Network Topology



Configuring IPv6 Link-Local Addresses

Manually configuring link-local addresses

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

Verifying link-local addresses

```
R1#show ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::1
    2001:DB8:CAFE:1::1
Serial0/0/0                [up/up]
    FE80::1
    2001:DB8:CAFE:A001::1
Serial0/0/1                [up/up]
    FE80::1
    2001:DB8:CAFE:A003::1
R1#
```

Same IPv6 link-local address is configured on all interfaces.

Configuring EIGRP for the IPv6 Routing Process

- The **`ipv6 unicast-routing`** global configuration mode command is required to enable any IPv6 routing protocol.
- Configuring EIGRP for IPv6

```
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router eigrp 2
R2(config-rtr)#eigrp router-id 2.0.0.0
R2(config-rtr)#no shutdown
R2(config-rtr)#
```

- The **`no shutdown`** command and a router ID are required for the router to form neighbor adjacencies.

Configuring EIGRP for IPv6

ipv6 eigrp interface Command

Enabling EIGRP of IPv6 on an Interface

```
R1(config)#interface g0/0
R1(config-if)#ipv6 eigrp 2
R1(config-if)#exit
R1(config)#interface s 0/0/0
R1(config-if)#ipv6 eigrp 2
R1(config-if)#exit
R1(config)#interface s 0/0/1
R1(config-if)#ipv6 eigrp 2
R1(config-if)#
```

```
R2(config)#interface g 0/0
R2(config-if)#ipv6 eigrp 2
R2(config-if)#exit
R2(config)#interface s 0/0/0
R2(config-if)#ipv6 eigrp 2
R2(config-if)#exit
%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1
(Serial0/0/0) is up: new adjacency
R2(config)#interface s 0/0/1
R2(config-if)#ipv6 eigrp 2
R2(config-if)#
```

Verifying EIGRP for IPv6

Verifying EIGRP for IPv6: Examining Neighbors

show ipv6 eigrp neighbors Command

```
R1# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(2)
H   Address                  Interface   Hold   Uptime     SRTT   RTO   Q    Seq
                                         (sec)             (ms)         Cnt  Num
1   Link-local address:       Se0/0/1     13    00:37:17    45     270   0    8
    FE80::3
0   Link-local address:       Se0/0/0     14    00:53:16    32    2370   0    8
    FE80::2
R1#
```

Neighbor's IPv6 Link-local Address

Local Interface receiving EIGRP for IPv6 Hello packets

Amount of time since this neighbor was added to the neighbor table.

Seconds remaining before declaring neighbor down.

The current hold time and is reset to the maximum hold time whenever a Hello packet is received.

Verifying EIGRP for IPv6

Verifying EIGRP for IPv6: show ip protocols Command

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 2"
EIGRP-IPv6 Protocol for AS(2)
```

1. Routing protocol and Process ID (AS Number)

```
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

2. K values used in composite metric

```
  NSF-aware route hold timer is 240
  Router-ID: 1.0.0.0
```

3. EIGRP Router ID

```
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
```

4. EIGRP Administrative Distances

```
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

  Interfaces:
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
```

5. Interfaces enabled for this EIGRP for IPv6.

```
  Redistribution:
    None
R1#
```

Verifying EIGRP for IPv6: Examine the Routing Table

Use the **show ipv6 route** command to examine the IPv6 routing table.

```
R1#show ipv6 route
 <Output omitted>
C    2001:DB8:CAFE:1::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:CAFE:1::1/128 [0/0]
      via GigabitEthernet0/0, receive
D    2001:DB8:CAFE:2::/64 [90/3524096]
      via FE80::3, Serial0/0/1
D    2001:DB8:CAFE:3::/64 [90/2170112]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A001::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:CAFE:A001::1/128 [0/0]
      via Serial0/0/0, receive
D    2001:DB8:CAFE:A002::/64 [90/3523840]
      via FE80::3, Serial0/0/1
C    2001:DB8:CAFE:A003::/64 [0/0]
      via Serial0/0/1, directly connected
L    2001:DB8:CAFE:A003::1/128 [0/0]
      via Serial0/0/1, receive
L    FF00::/8 [0/0]
      via Null0, receive
R1#
```

Chapter 4: Summary

- EIGRP is a classless, advanced distance vector routing protocol.
- EIGRP uses the source code of “D” for DUAL in the routing table.
- The default administrative distance of 90 is used for internal routes and 170 for routes imported from an external source.
- Advanced features include DUAL, establishing neighbor adjacencies, RTP, partial and bounded updates, and equal and unequal cost load balancing.
- PDMs give EIGRP the capability to support different Layer 3 protocols.
- EIGRP Hello packets are used to discover neighbors.
- The **`show ip eigrp neighbors`** command is used to view neighbor table and verify adjacencies.

Chapter 4: Summary (cont.)

- EIGRP sends partial bounded updates when a change occurs on network.
- EIGRP composite metric uses bandwidth, delay, reliability and load to determine the best path (by default, only bandwidth and delay are used).
- DUAL FSM is used to determine best path; Successor and potential backup path, FS to every destination network.

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5: EIGRP Advanced Configurations and Troubleshooting

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 5

5.1 Advanced EIGRP Configurations

5.2 Troubleshooting EIGRP

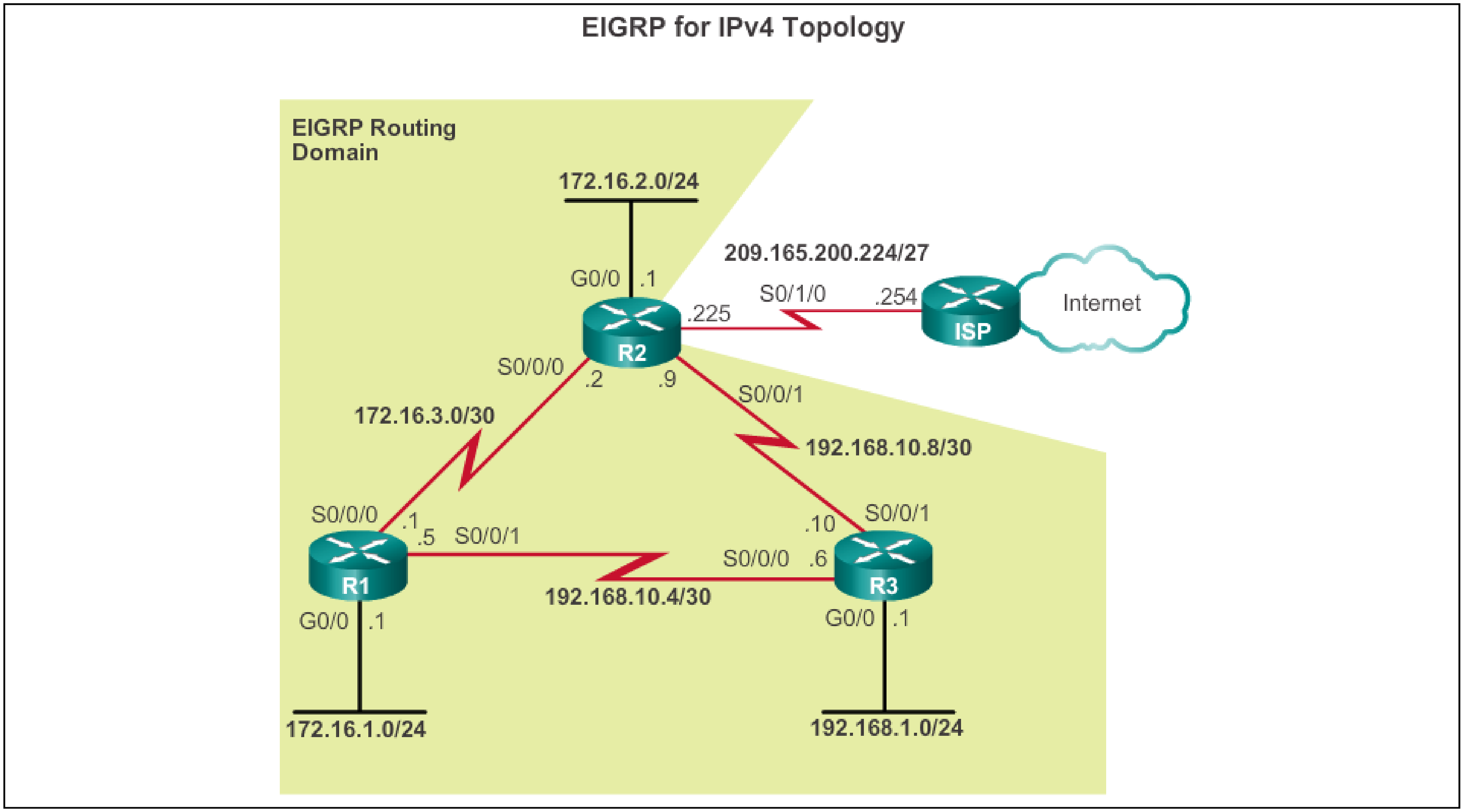
5.3 Summary

Chapter 5: Objectives

After completing this chapter, you will be able to:

- Configure EIGRP automatic summarization.
- Configure EIGRP manual summarization.
- Configure a router to propagate a default route in an EIGRP network.
- Modify EIGRP interface settings to improve network performance.
- Configure EIGRP authentication to ensure secure routing updates.
- Explain the process and tools used to troubleshoot an EIGRP network.
- Troubleshoot neighbor adjacency issues in an EIGRP network.
- Troubleshoot missing route entries in an EIGRP routing table.

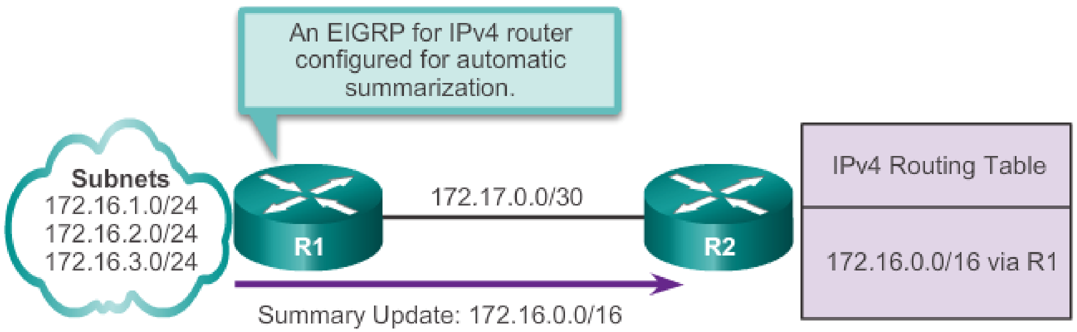
Network Technology



Automatic Summarization

EIGRP Automatic Summarization

Automatic Summarization at Classful Network Boundary



Classful Networks

Class A: 0.0.0.0 to 127.255.255.255	Default Mask: 255.0.0.0 or /8
Class B: 128.0.0.0 to 191.255.255.255	Default Mask: 255.255.0.0 or /16
Class C: 192.0.0.0 to 223.255.255.255	Default Mask: 255.255.255.0 or /24

Configuring EIGRP Automatic Summarization

- EIGRP for IPv4 automatic summarization is disabled, by default, beginning with Cisco IOS Release 15.0(1)M and 12.2(33). Prior to this, automatic summarization was enabled, by default.
- To enable automatic summarization for EIGRP, use the **auto-summary** command in router configuration mode.

  R1(config)# **router eigrp** *autonomous-system*

  R1(config-router)# **auto-summary**

- Use the **no** form of this command to disable autosummarization.

  R1(config)# **router eigrp** *autonomous-system*

  R1(config-router)# **no auto-summary**

Autosummarization

Verifying Autosummarization: show ip protocols

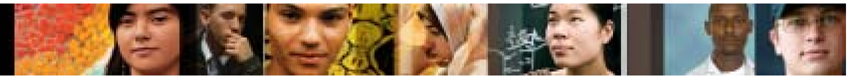
Verifying Automatic Summarization is Enabled

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
<Output omitted>

Automatic Summarization: enabled
    192.168.10.0/24 for Gi0/0, Se0/0/0
      Summarizing 2 components with metric 2169856
    172.16.0.0/16 for Se0/0/1
      Summarizing 3 components with metric 2816
<Output omitted>
```

Autosummarization

Verifying Autosummarization: Topology Table

```
R3# show ip eigrp topology all-links

P 172.16.0.0/16, 1 successors, FD is 2170112, serno 9
        via 192.168.10.5 (2170112/2816), Serial0/0/0
        via 192.168.10.9 (3012096/2816), Serial0/0/1

<Output omitted>
```



Autosummarization

Verifying Autosummarization: Routing Table

Verifying Summary Route in Routing Table

Automatic Summarization Disabled

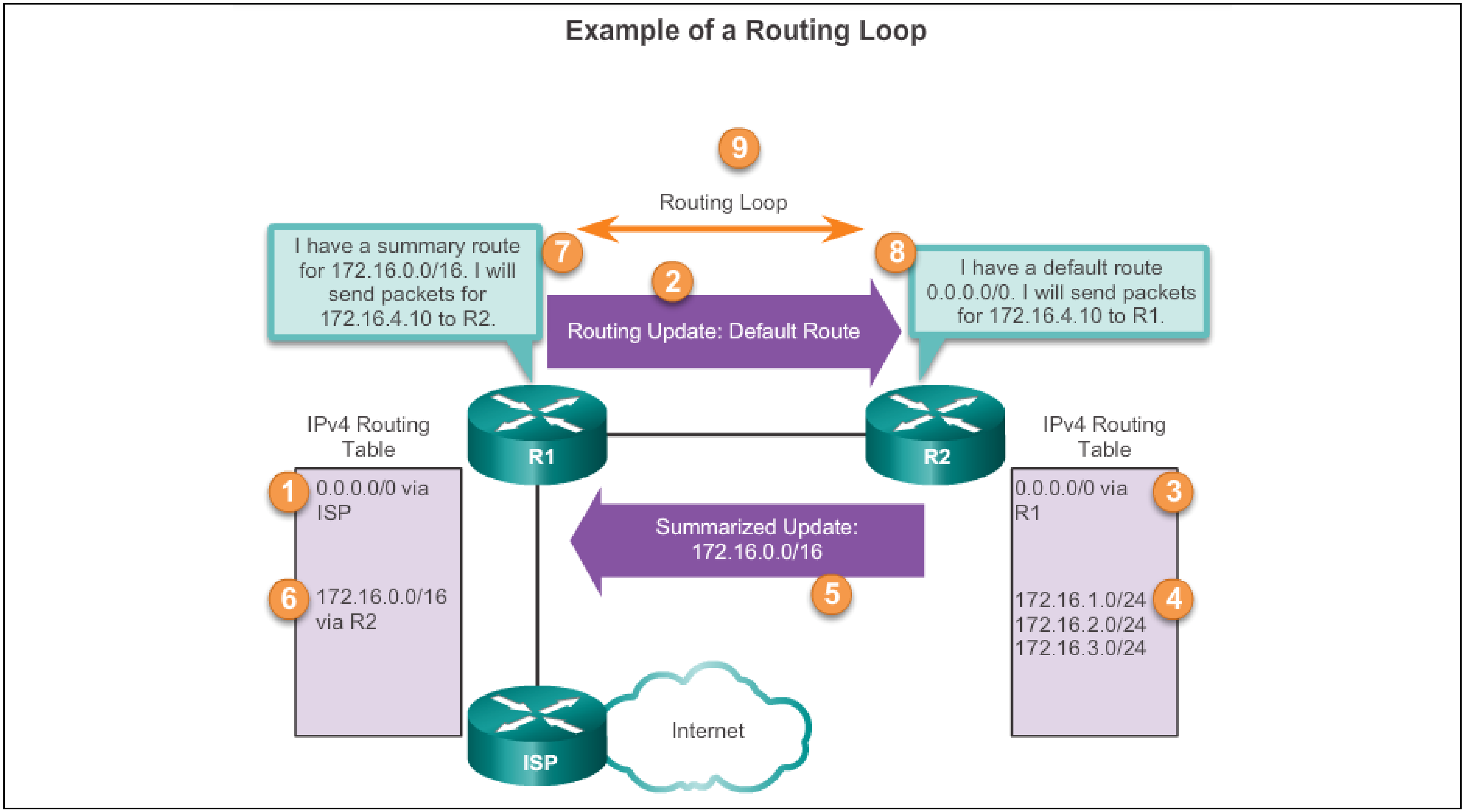
```
R3# show ip route eigrp
<Output omitted>

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D     172.16.1.0/24 [90/2170112] via 192.168.10.5,
                     02:21:10, Serial0/0/0
D     172.16.2.0/24 [90/3012096] via 192.168.10.9,
                     02:21:10, Serial0/0/1
D     172.16.3.0/30 [90/41024000] via 192.168.10.9,
                     02:21:10, Serial0/0/1
```

Automatic Summarization Enabled

```
R3# show ip route eigrp
<Output omitted>

D    172.16.0.0/16 [90/2170112] via 192.168.10.5, 00:12:05,
     Serial0/0/0
     192.168.10.0/24 is variably subnetted, 5 subnets, 3
     masks
D    192.168.10.0/24 is a summary, 00:11:43, Null0
R3#
```

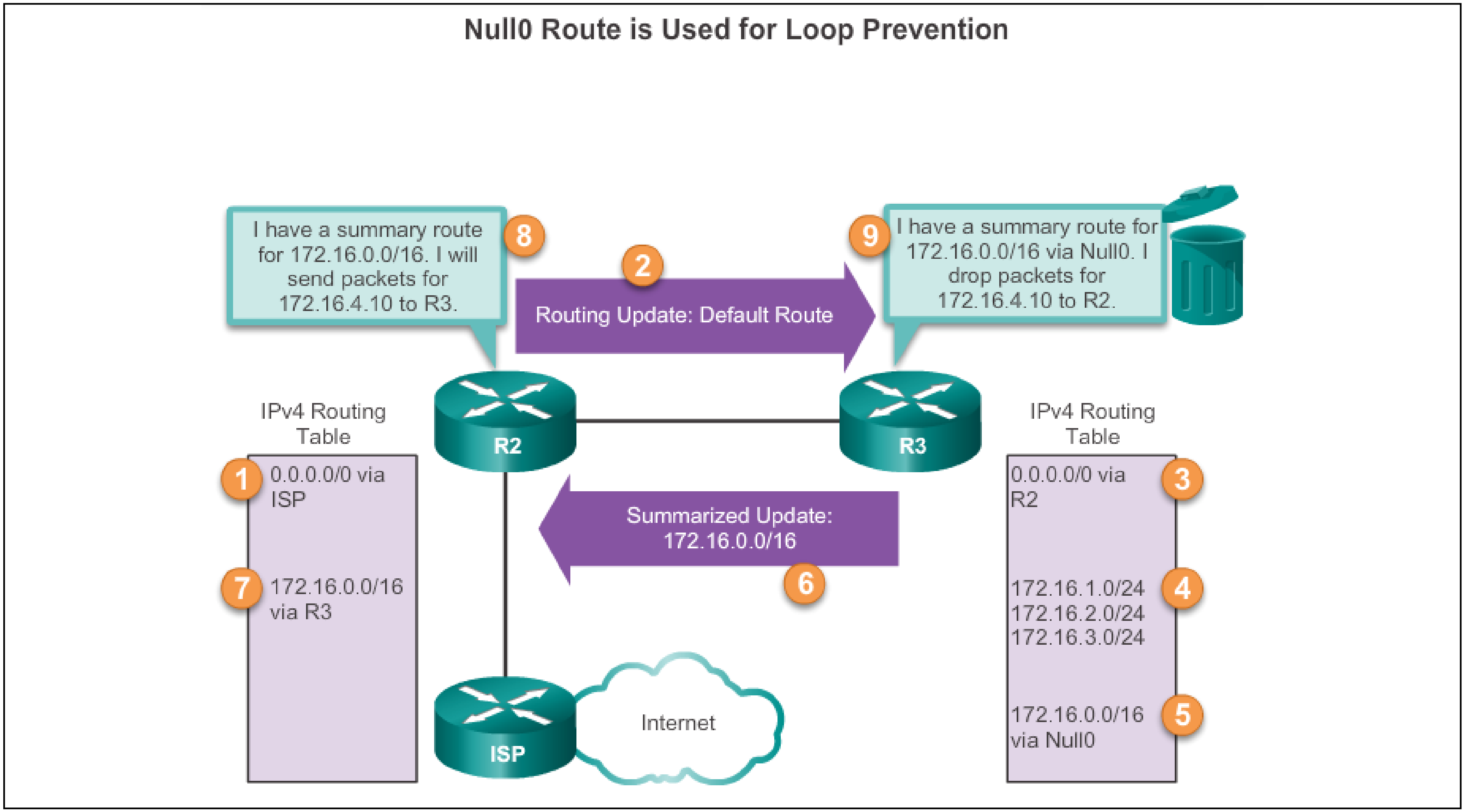
Autosummarization

Summary Route



Autosummarization

Summary Route (cont.)



Manual Summarization

Manual Summary Routes

- EIGRP can be configured to summarize routes, whether or not autosummarization is enabled.
- Because EIGRP is a classless routing protocol and includes the subnet mask in the routing updates, manual summarization can include supernet routes.
- A supernet is an aggregation of multiple major classful network addresses.

Manual Summarization

Configuring EIGRP Manual Summary Routes

Calculating a Summary Route

```
192.168.1.0:  11000000 . 10101000 . 00000001 . 00000000
192.168.2.0:  11000000 . 10101000 . 00000010 . 00000000
192.168.3.0:  11000000 . 10101000 . 00000011 . 00000000
```

22 matching bits

22 matching bits = a/22 subnet mask or 255.255.252.0

```
R3(config)# interface serial 0/0/0
R3(config-if)# ip summary-address eigrp 1 192.168.0.0
255.255.252.0
R3(config-if)#
```

Configure the summary route on all interfaces that send EIGRP packets.

Verifying Manual Summary Routes

Verifying Summary Route Received on R1 and R2

```
R1# show ip route
<Output omitted>

D 192.168.0.0/22 [90/2170112] via 192.168.10.6, 01:53:19, Serial0/0/1
R1#
```

```
R2# show ip route
<Output omitted>

D 192.168.0.0/22 [90/3012096] via 192.168.10.10, 01:53:33, Serial0/0/1
R2#
```

Manual Summarization

EIGRP for IPv6: Manual Summary Routes

IPv6 Manually Summary Configuration on R3

```
R3(config)# interface serial 0/0/0
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# end

R3# show ipv6 route

D   2001:DB8:ACAD::/48 [5/128256]
     via Null0, directly connected

<Output omitted>
```

Default Route Propagation

Propagating a Default Static Route

- Using a static route to 0.0.0.0/0 as a default route is not routing protocol-dependent.
- The quad zero static default route can be used with any currently supported routing protocols.
- The static default route is usually configured on the router that has a connection to a network outside the EIGRP routing domain, for example, to an ISP.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1/0
R2(config)# router eigrp 1
R2(config-router)# redistribute static
```

Default Route Propagation

Verifying the Propagated Default Route

The entry for the EIGRP-learned default route is identified by the following:

- **D** – This route was learned from an EIGRP routing update.
- ***** – The route is a candidate for a default route.
- **EX** – The route is an external EIGRP route; in this case, a static route outside of the EIGRP routing domain.
- **170** – This is the administrative distance of an external EIGRP route.

```
R1# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:25:23,
Serial0/0/1
R1#
```

Default Route Propagation

EIGRP for IPv6- Default Route

```
R2(config)# ipv6 route ::/0 serial 0/1/0
R2(config)# ipv6 router eigrp 2
R2(config-router)# redistribute static
```

Note: Some IOSs may require that the **redistribute static** command include the EIGRP metric parameters and maximum transmission unit (MTU) before the static route can be redistributed. These parameters may vary, but an example for this scenario would be:

```
R2(config)# ipv6 router eigrp 2
R2(config-router)# redistribute static metric 64 2000
255 1 1500
```

Fine-tuning EIGRP Interfaces

EIGRP Bandwidth Utilization

EIGRP Bandwidth for IPv4

- By default, EIGRP uses only up to 50% of an interface's bandwidth for EIGRP information, which prevents the EIGRP process from overutilizing a link and not allowing enough bandwidth for the routing of normal traffic.
- The **ip bandwidth-percent eigrp** command can be used to configure the percentage of bandwidth that may be used by EIGRP on an interface.

```
Router(config-if)# ip bandwidth-percent eigrp as-number
percent
```

Fine-tuning EIGRP Interfaces

EIGRP Bandwidth Utilization (cont.)

EIGRP Bandwidth for IPv6

To configure the percentage of bandwidth that may be used by EIGRP for IPv6 on an interface, use the **ipv6 bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
Router(config-if)# ipv6 bandwidth-percent eigrp as-number percent
```

Fine-tuning EIGRP Interfaces

Hello and Hold Timers

Configuring EIGRP for IPv4 Hello and Hold Timers

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip hello-interval eigrp 1 60
R1(config-if)# ip hold-time eigrp 1 180
```

Default Hello Intervals and Hold Times for EIGRP

Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

Fine-tuning EIGRP Interfaces
Load Balancing IPv4

- Equal-cost load balancing is the ability of a router to distribute outbound traffic using all interfaces that have the same metric from the destination address.
- The Cisco IOS will, by default, allow load balancing using up to four equal-cost paths; however, this can be modified. Using the **maximum-paths** router configuration mode command, up to 32 equal-cost routes can be kept in the routing table.

```
Router(config-router)# maximum-paths value
```

- If the value is set to 1, load balancing is disabled.

Fine-tuning EIGRP Interfaces

Load Balancing IPv6

R3's IPv6 Routing Table

```
R3# show ipv6 route eigrp
<Output omitted>

EX   ::/0 [170/3011840]
      via FE80::2, Serial0/0/1
D    2001:DB8:ACAD::/48 [5/128256]
      via Null0, directly connected
D    2001:DB8:CAFE:1::/64 [90/2170112]
      via FE80::1, Serial0/0/0
D    2001:DB8:CAFE:2::/64 [90/3012096]
      via FE80::2, Serial0/0/1
D    2001:DB8:CAFE:A001::/64 [90/41024000]
      via FE80::2, Serial0/0/1
      via FE80::1, Serial0/0/0
R3#
```

Secure EIGRP

Routing Protocol Authentication Overview

- Network administrators must be aware that routers are at risk from attack just as much as end-user devices. Anyone with a packet sniffer, such as Wireshark, can read information propagating between routers.
- A method to protect routing information on the network is to authenticate routing protocol packets using the Message Digest 5 (MD5) algorithm.
- Routing protocols, such as RIPv2, EIGRP, OSPF, IS-IS, and BGP all support various forms of MD5 authentication.

Secure EIGRP

Configuring EIGRP with MD5 Authentication

EIGRP Authentication with MD5

Step 1: Create a Keychain

```
Router(config)# key chain name-of-chain
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string key-string-text
```

Step 2: Configure EIGRP Authentication Using Keychain and Key

```
Router(config)# interface type number
Router(config-if)# ip authentication mode eigrp as-number md5
Router(config-if)# ip authentication key-chain eigrp as-number
name-of-chain
```

EIGRP Authentication Example

Configuring EIGRP MD5 Authentication on R1

```
R1(config)# key chain EIGRP_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# end
R1#
```

Secure EIGRP

EIGRP Authentication Example (cont.)

Configuring EIGRP for IPv6 MD5 Authentication on R1

```
R1(config)# key chain EIGRP_IPV6_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
                EIGRP_IPV6_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
                EIGRP_IPV6_KEY
R1(config-if)#
```

Secure EIGRP

Verifying Authentication

- Adjacencies are only formed when both connecting devices have authentication configured.
- To verify that the correct EIGRP adjacencies were formed after being configured for authentication, use the **show ip eigrp neighbors** command on each router.
- To verify the neighbor adjacencies EIGRP for IPv6, use the **show ipv6 eigrp neighbors** command.

5.2 Troubleshooting EIGRP

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Basic EIGRP Troubleshooting Commands

EIGRP for IPv4

- `Router#` **`show ip eigrp neighbors`**
- `Router#` **`show ip route`**
- `Router#` **`show ip protocols`**

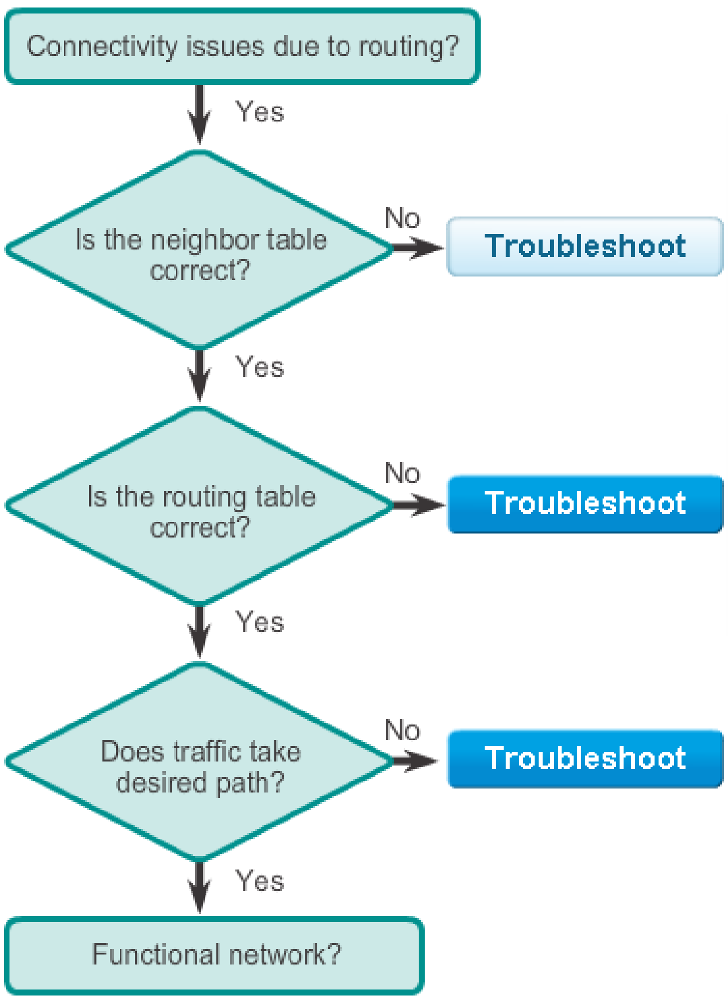
EIGRP for IPv6

- `Router#` **`show ipv6 eigrp neighbors`**
- `Router#` **`show ipv6 route`**
- `Router#` **`show ipv6 protocols`**

Components of Troubleshooting EIGRP

Components

Diagnosing EIGRP Connectivity Issues



Troubleshoot

- Are the interfaces operational?
- Are the interfaces enabled for EIGRP?
- Does the EIGRP AS match?
- Is there an interface that is configured as passive?

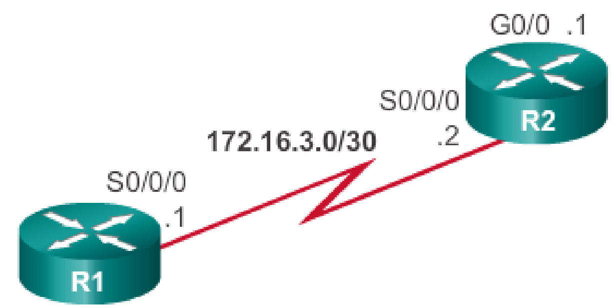
Show commands

```
show ip eigrp neighbors
show ip interface brief
show ip eigrp interface
```

Troubleshoot EIGRP Neighbor Issues

Layer 3 Connectivity

A prerequisite for a neighbor adjacency to form between two directly connected routers is Layer 3 connectivity.




```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0         172.16.1.1      YES manual up          up
Serial0/0/0                172.16.3.1      YES manual up          up
Serial0/0/1                192.168.10.5    YES manual up          up
R1# ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
28/28/28 ms
R1#
```

Troubleshoot EIGRP Neighbor Issues

EIGRP Parameters

When troubleshooting an EIGRP network, one of the first things to verify is that all routers that are participating in the EIGRP network are configured with the same autonomous system number.

EIGRP for IPv4

- `Router#` **`show ip protocols`**

EIGRP for IPv6

- `Router#` **`show ipv6 protocols`**

EIGRP Interfaces

- In addition to verifying the autonomous system number, it is necessary to verify that all interfaces are participating in the EIGRP network.
- The **network** command that is configured under the EIGRP routing process indicates which router interfaces participate in EIGRP.

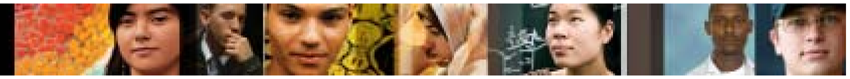
```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
                    Xmit Queue   PeerQ        Mean   Pacing Time
Interface    Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable
Gi0/1          0        0/0          0/0         0       0/0
Se0/0/0        1        0/0          0/0      1295       0/23
Se0/0/1        1        0/0          0/0      1044       0/15
R1#
```

Troubleshoot EIGRP Routing Table Issues

Passive Interface

- One reason that route tables may not reflect the correct routes is due to the **`passive-interface`** command.
- The show ip protocols can be used to check if an interface is configured as passive.

```
R2# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"
 <output omitted>
Routing for Networks:
    172.16.0.0
    192.168.10.8/30
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance       Last Update
    192.168.10.10          90       00:08:59
    172.16.3.1             90       00:08:59
  Distance: internal 90 external 170
R2#
```



Troubleshoot EIGRP Routing Table Issues

Passive Interface

- With EIGRP running on a network, the **`passive-interface`** command stops both outgoing and incoming routing updates. For this reason, routers do not become neighbors.

Configuring Network to ISP as a Passive Interface

```
R2(config)# router eigrp 1
R2(config-router)# network 209.165.200.0
R2(config-router)# passive-interface serial 0/1/0
R2(config-router)# end
R2# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address         Interface   Hold Uptime    SRTT  RTO  Q   Seq
                                (sec)          (ms)       Cnt Num
1   172.16.3.1       Se0/0/0    175 01:09:18    80   2340 0   16
0   192.168.10.10    Se0/0/1    11  01:09:33   1037  5000 0   17
R2#
```

Missing Network Statement

10.10.10.0/24 Unreachable from R3

```
R3# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
R3#
```

Troubleshoot EIGRP Routing Table Issues

Missing Network Statement (cont.)

10.10.10.0/24 R1 Updates

```
R1# show ip protocols | begin Routing for Networks
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.6          90      01:34:19
    172.16.3.2            90      01:34:19
  Distance: internal 90 external 170

R1#
```

Troubleshoot EIGRP Routing Table Issues

Missing Network Statement (cont.)

Add Missing Network Statement

```
R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0
```

Troubleshooting EIGRP Routing Table Issues
Autosummarization

- Another issue that may create problems for the network administrator is EIGRP autosummarization.
- EIGRP for IPv4 can be configured to automatically summarize routes at classful boundaries. If there are discontiguous networks, autosummarization causes inconsistent routing.
- Classful networks do not exist in IPv6; therefore, EIGRP for IPv6 does not support autosummarization. All summarization must be accomplished using EIGRP manual summary routes.

Chapter 5: Summary

- EIGRP is one of the routing protocols commonly used in large enterprise networks.
- Modifying EIGRP features and troubleshooting problems is one of the most essential skills for a network engineer involved in the implementation and maintenance of large, routed enterprise networks that use EIGRP.
- Summarization decreases the number of entries in routing updates and lowers the number of entries in local routing tables. It also reduces bandwidth utilization for routing updates and results in faster routing table lookups.
- EIGRP for IPv4 autosummarization is disabled, by default, beginning with Cisco IOS Release 15.0(1)M and 12.2(33). Prior to this, autosummarization was enabled, by default.

Cisco | Networking Academy®

Mind Wide Open™

Chapter 6: Single-Area OSPF

Routing Protocols

Cisco | Networking Academy®
Mind Wide Open™

Chapter 6

6.1 Characteristics of OSPF

6.2 Configuring Single-area OSPFv2

6.3 Configure Single-area OSPFv3

Chapter 6: Objectives

After completing this chapter, you will be able to:

- Explain the process by which link-state routers learn about other networks.
- Describe the types of packets used by Cisco IOS routers to establish and maintain an OSPF network.
- Explain how Cisco IOS routers achieve convergence in an OSPF network.
- Configure an OSPF router ID.
- Configure single-area OSPFv2 in a small, routed IPv4 network.
- Explain how OSPF uses cost to determine best path.
- Verify single-area OSPFv2 in a small, routed network.
- Compare the characteristics and operations of OSPFv2 to OSPFv3.
- Configure single-area OSPFv3 in a small, routed network.
- Verify single-area OSPFv3 in a small, routed network.

Open Shortest Path First
Evolution of OSPF

Interior Gateway Protocols

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

1988

1989
updated in
2008

Features of OSPF

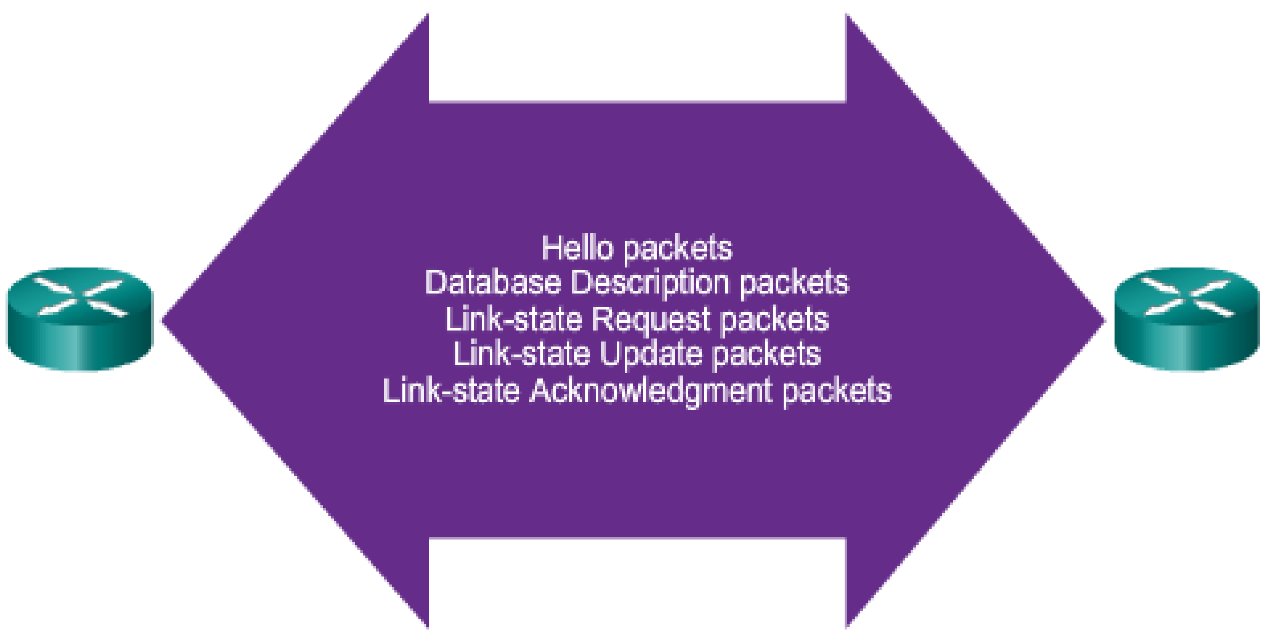
Open Shortest Path First
Components of OSPF

OSPF Data Structures

Database	Table	Description
Adjacency Database	Neighbor Table	• List of all neighbor routers to which a router has established bidirectional communication. • This table is unique for each router. • Can be viewed using the **`show ip ospf neighbor`** command.
Link-state Database (LSDB)	Topology Table	• Lists information about all other routers in the network. • The database shows the network topology. • All routers within an area have identical LSDB. • Can be viewed using the **`show ip ospf database`** command.
Forwarding Database	Routing Table	• List of routes generated when an algorithm is run on the link-state database. • Each router's routing table is unique and contains information on how and where to send packets to other routers. • Can be viewed using the **`show ip route`** command.

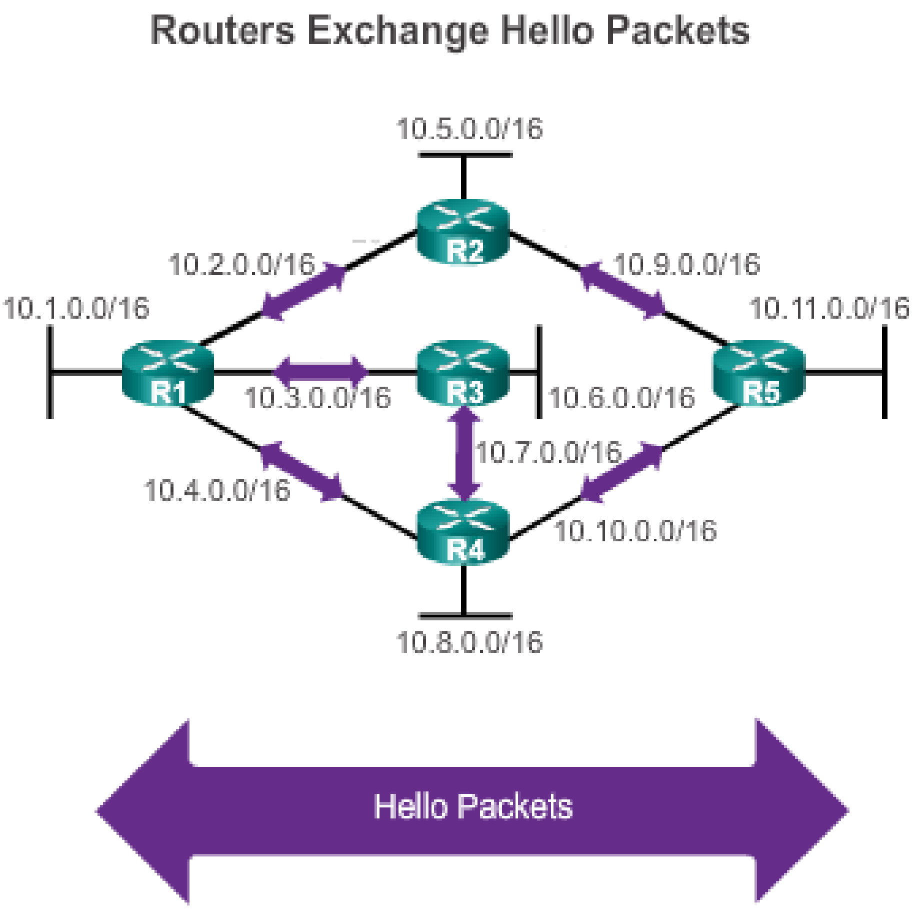
Open Shortest Path First
Components of OSPF (cont.)

OSPF Routers Exchange Packets - These packets are used to discover neighboring routers and also to exchange routing information to maintain accurate information about the network.



Open Shortest Path First

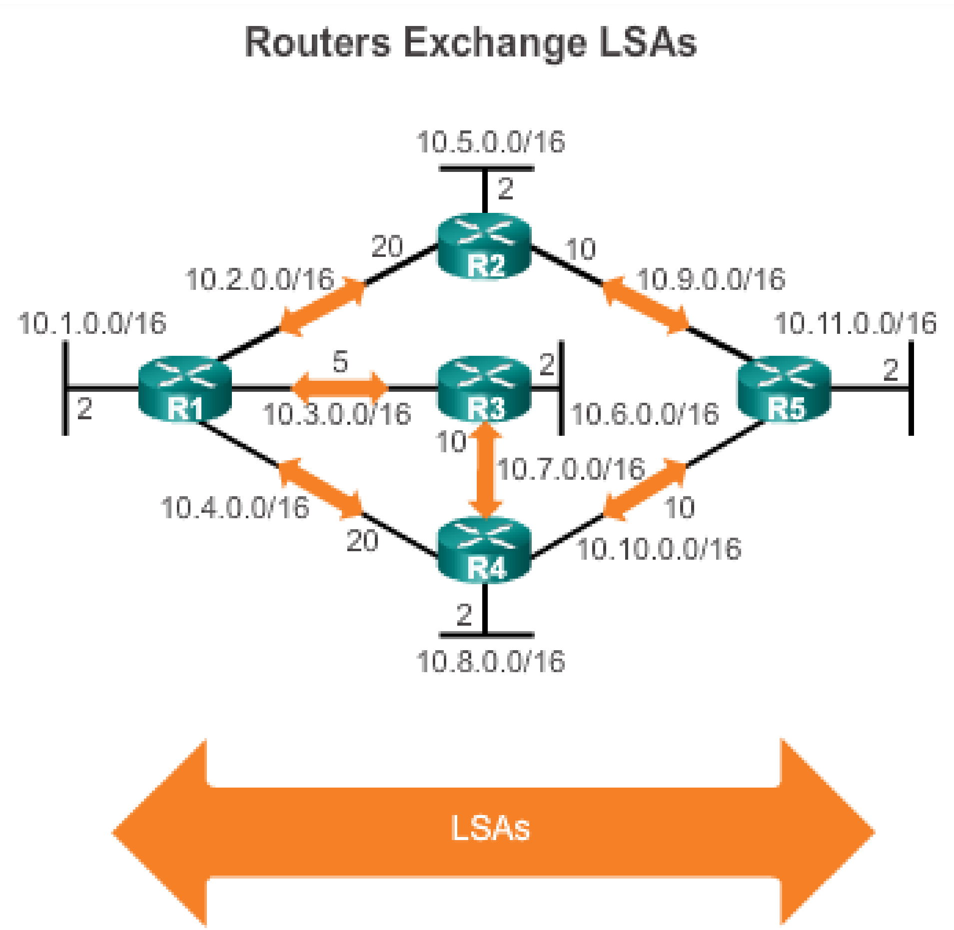
Link-State Operation



If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor

Open Shortest Path First

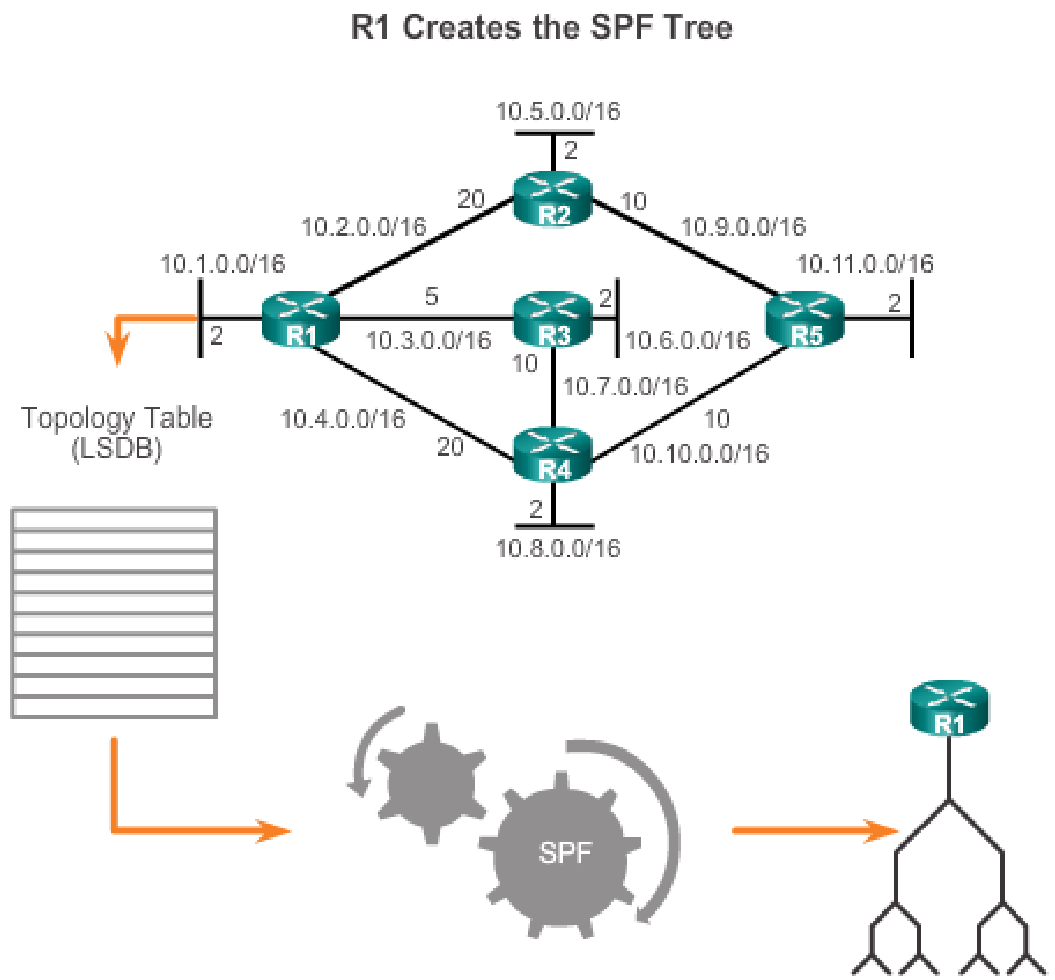
Link-State Operation (cont.)



- LSAs contain the state and cost of each directly connected link.
- Routers flood their LSAs to adjacent neighbors.
- Adjacent neighbors receiving the LSA immediately flood the LSA to other directly connected neighbors, until all routers in the area have all LSAs.

Open Shortest Path First

Link-State Operation

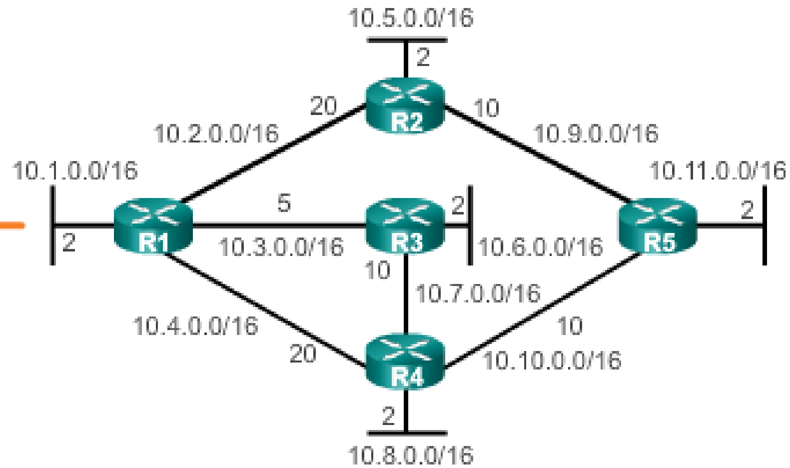


- Build the topology table based on the received LSAs.
- This database eventually holds all the information about the topology of the network.
- Execute the SPF Algorithm.

Open Shortest Path First

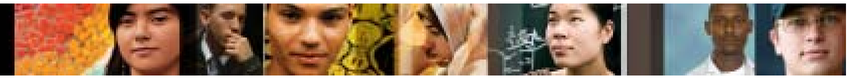
Link-State Operation (cont.)

Content of the R1 SPF Tree



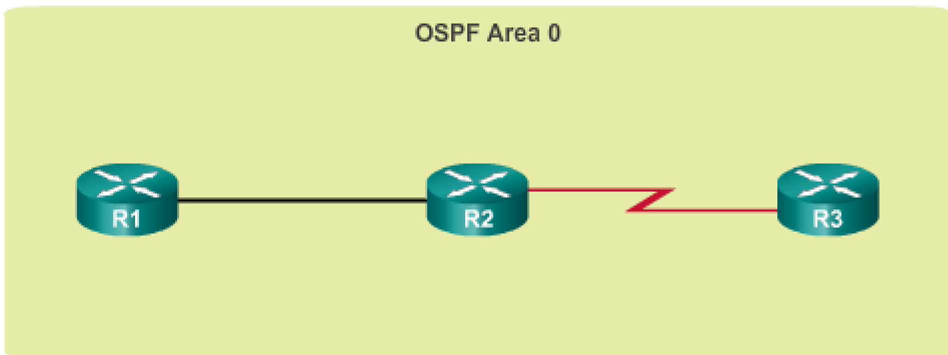
Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

From the SPF tree, the best paths are inserted into the routing table.



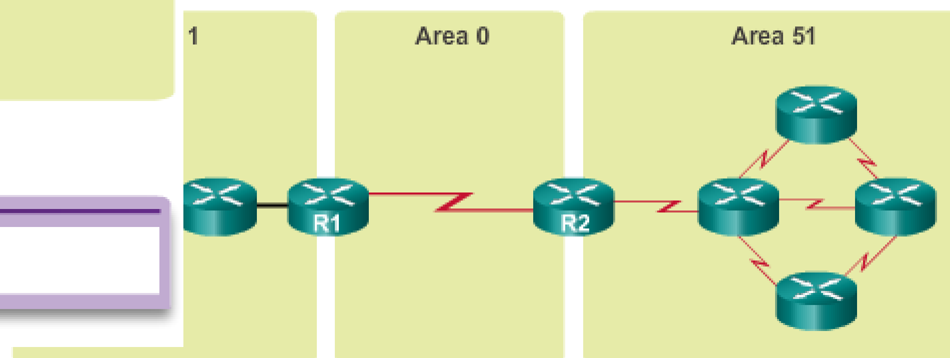
Open Shortest Path First
Single-area and Multiarea OSPF

Single-Area OSPF



- Area 0 is also called the backbone area.
- Single-area OSPF is useful in smaller networks with few routers.

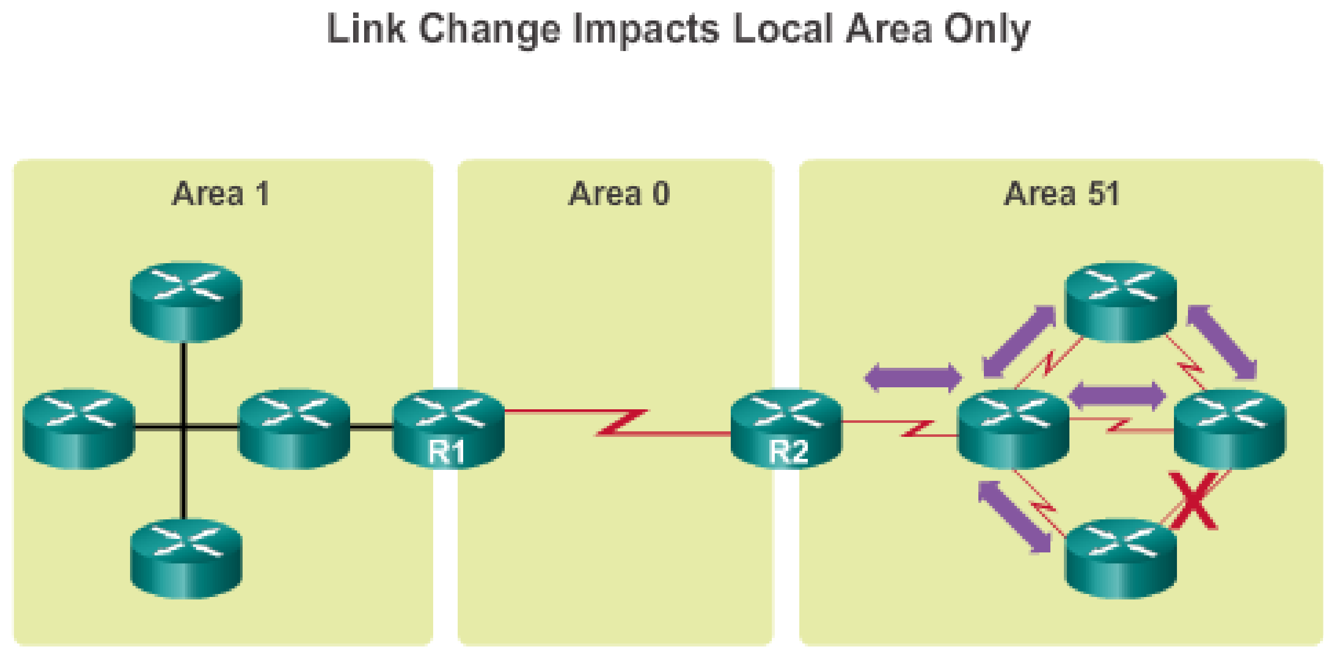
Multiarea OSPF



- Implemented using a two-layer area hierarchy as all areas must connect to the backbone area (area 0).
- Interconnecting routers are called Area Border Routers (ABR).
- Useful in larger network deployments to reduce processing and memory overhead.

Open Shortest Path First

Single-area and Multiarea OSPF (cont.)



- Link failure affects the local area only (area 51).
- The ABR (R2) isolates the fault to area 51 only.
- Routers in areas 0 and 1 do not need the run the SPF algorithm.

OSPF Messages
Encapsulating OSPF Messages

OSPF IPv4 Header Fields

Data Link Frame Header	IP Packet Header	OSPF Packet Header	OSPF Packet Type-Specific Database

Data Link Frame (Ethernet Fields shown here)
MAC Destination Address = Multicast: 01-00-5E-00-00-05 or 01-00-5E-00-00-06
MAC Source Address = Address of sending interface

IP Packet
IP Source Address = Address of sending interface
IP Destination Address = Multicast: 224.0.0.5 or 224.0.0.6
Protocol field = 89 for OSPF

OSPF Packet Header
Type code for OSPF Packet type
Router ID and Area Id

OSPF Packet types
0x01 Hello
0x02 Database Description (DD)
0X03 Link State Request
0X04 Link State Update
0X05 Link State Acknowledgment

OSPF Messages

Types of OSPF Packets

OSPF Packet Descriptions

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

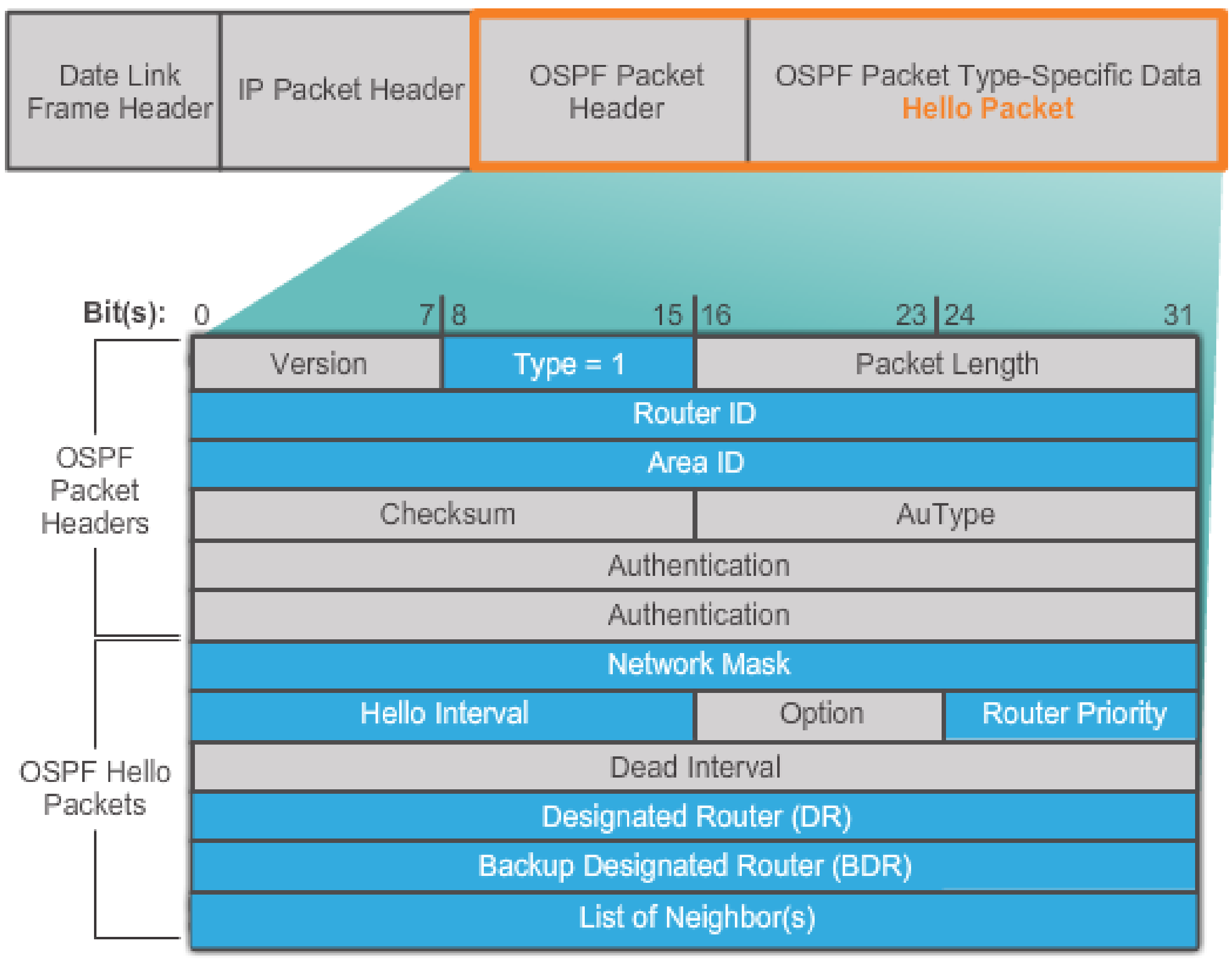
OSPF Messages
Hello Packet

OSPF Type 1 packet = Hello packet:

- Discover OSPF neighbors and establish neighbor adjacencies.
- Advertise parameters on which two routers must agree to become neighbors.
- Elect the Designated Router (DR) and Backup Designated Router (BDR) on multiaccess networks like Ethernet and Frame Relay.

OSPF Messages
Hello Packet (cont.)

OSPF Hello Packet Content



OSPF Messages
Hello Packet Intervals

OSPF Hello packets are transmitted:

- To 224.0.0.5 in IPv4 and FF02::5 in IPv6 (all OSPF routers)
- Every 10 seconds (default on multiaccess and point-to-point networks)
- Every 30 seconds (default on non-broadcast multiaccess [NBMA] networks)
- Dead interval is the period that the router waits to receive a Hello packet before declaring the neighbor down
- Router floods the LSDB with information about down neighbors out all OSPF enabled interfaces
- Cisco's default is 4 times the Hello interval

OSPF Messages

Link-State Updates

LSUs Contain LSAs

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between router
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

- An LSU contains one or more LSAs.
- LSAs contain route information for destination networks.

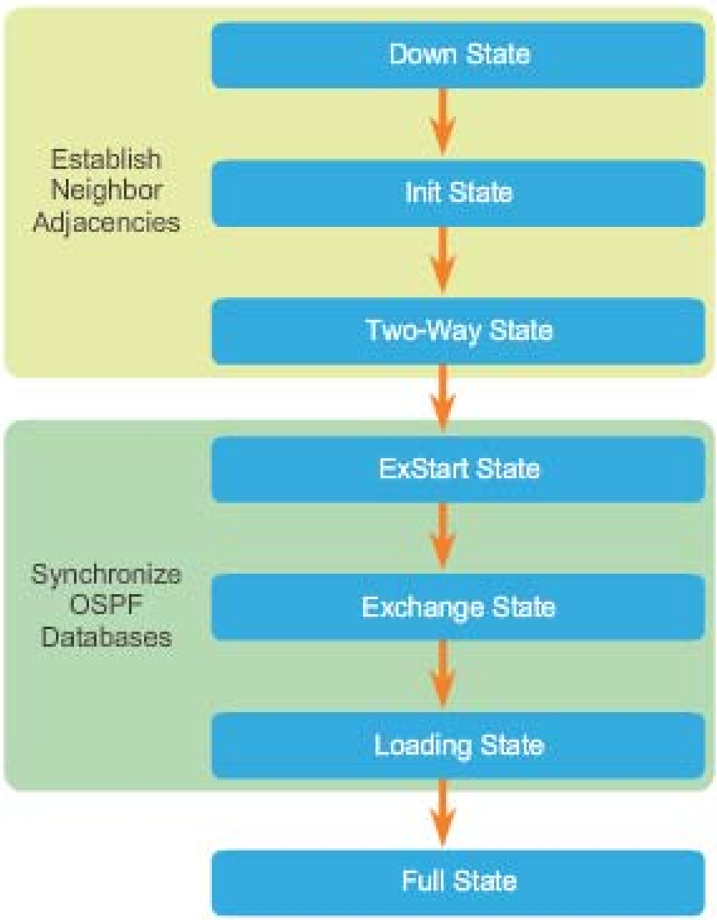
LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9,10,11	Opaque LSAs

OSPF Operation

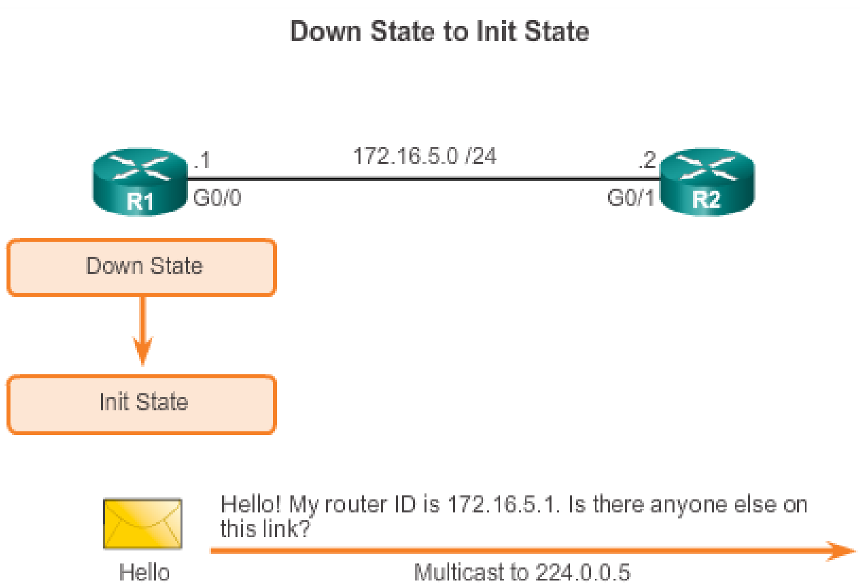
OSPF Operational States

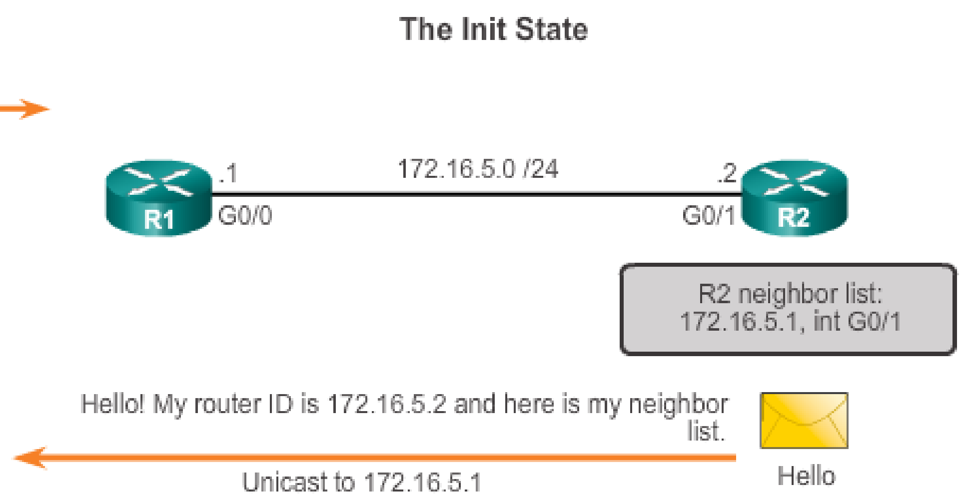
When an OSPF router is initially connected to a network, it attempts to:

- Create adjacencies with neighbors
- Exchange routing information
- Calculate the best routes
- Reach convergence
- OSPF progresses through several states while attempting to reach convergence.



OSPF Operation
Establish Neighbor Adjacencies

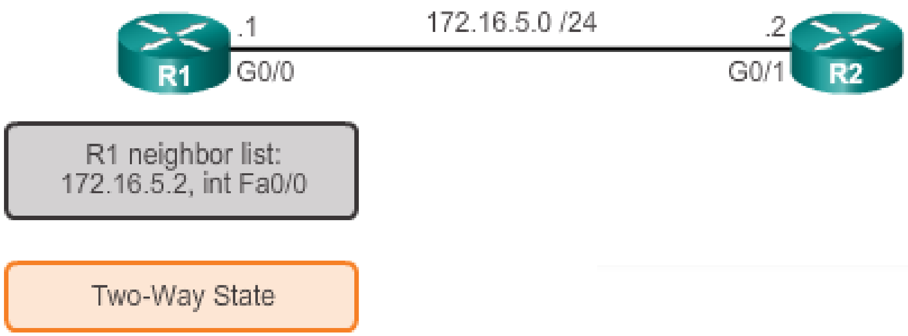




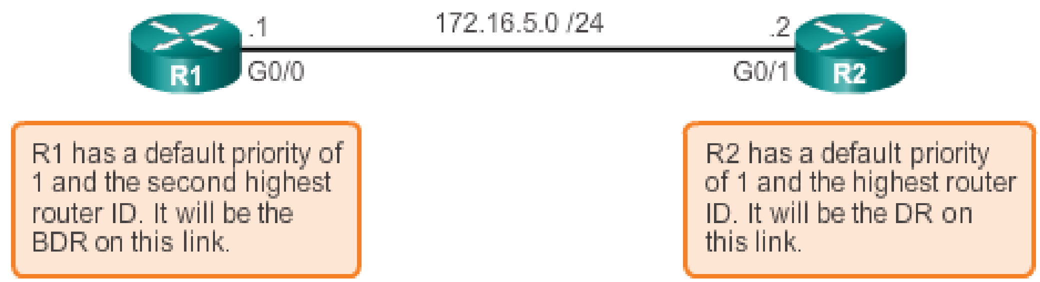
OSPF Operation

Establish Neighbor Adjacencies (cont.)

Two-Way State



Elect the DR and BDR

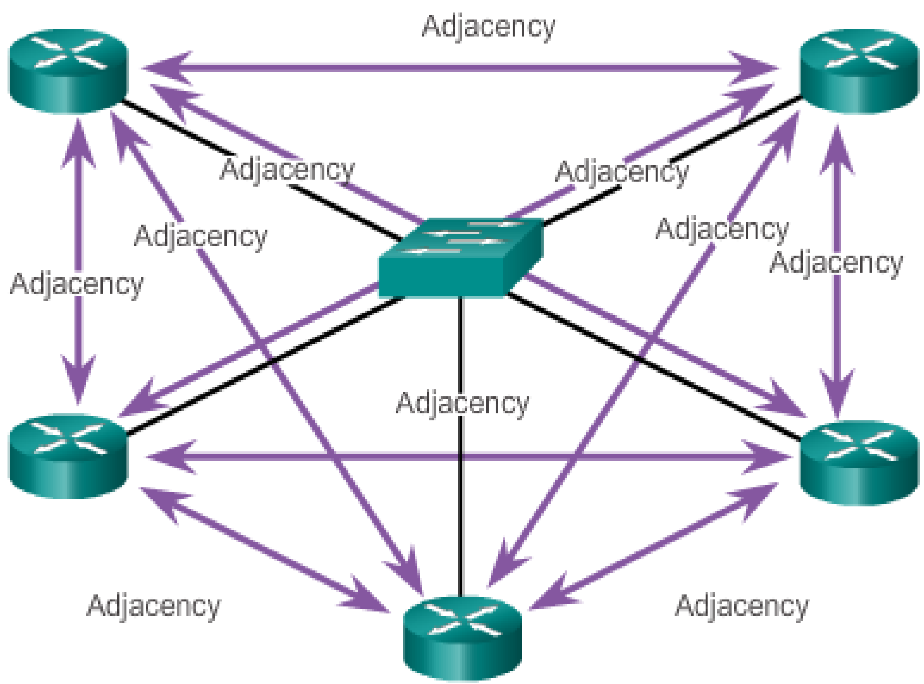


DR and BDR election only occurs on multi-access networks such as Ethernet LANs.

OSPF Operation

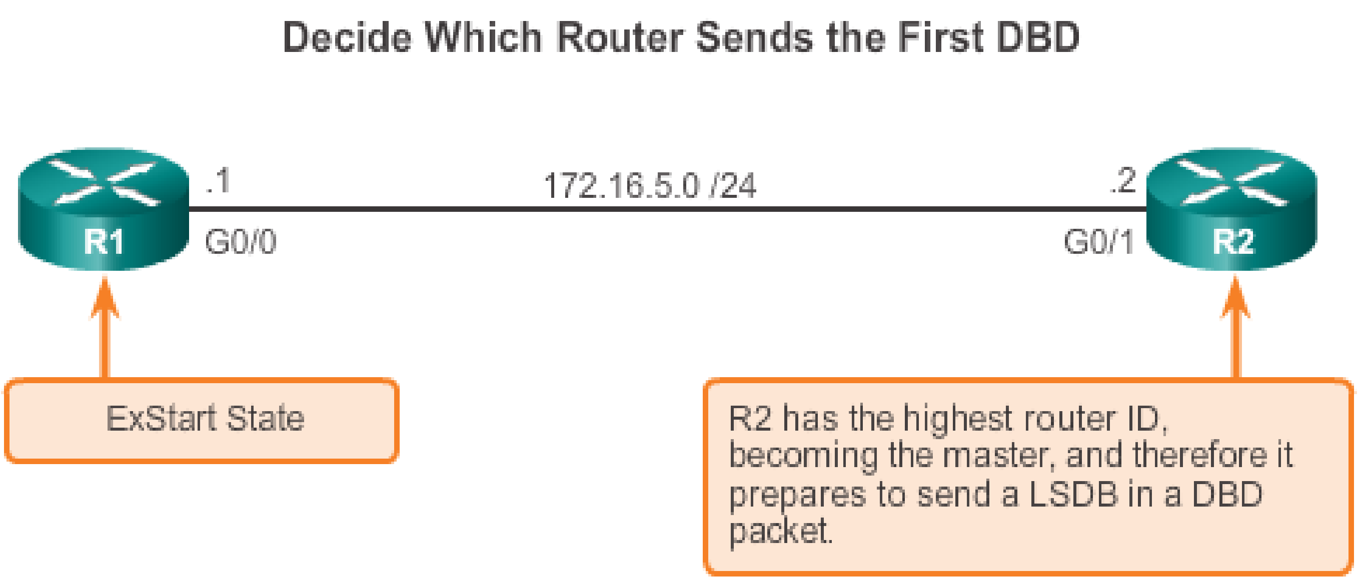
OSPF DR and BDR

Creating Adjacencies With Every Neighbor



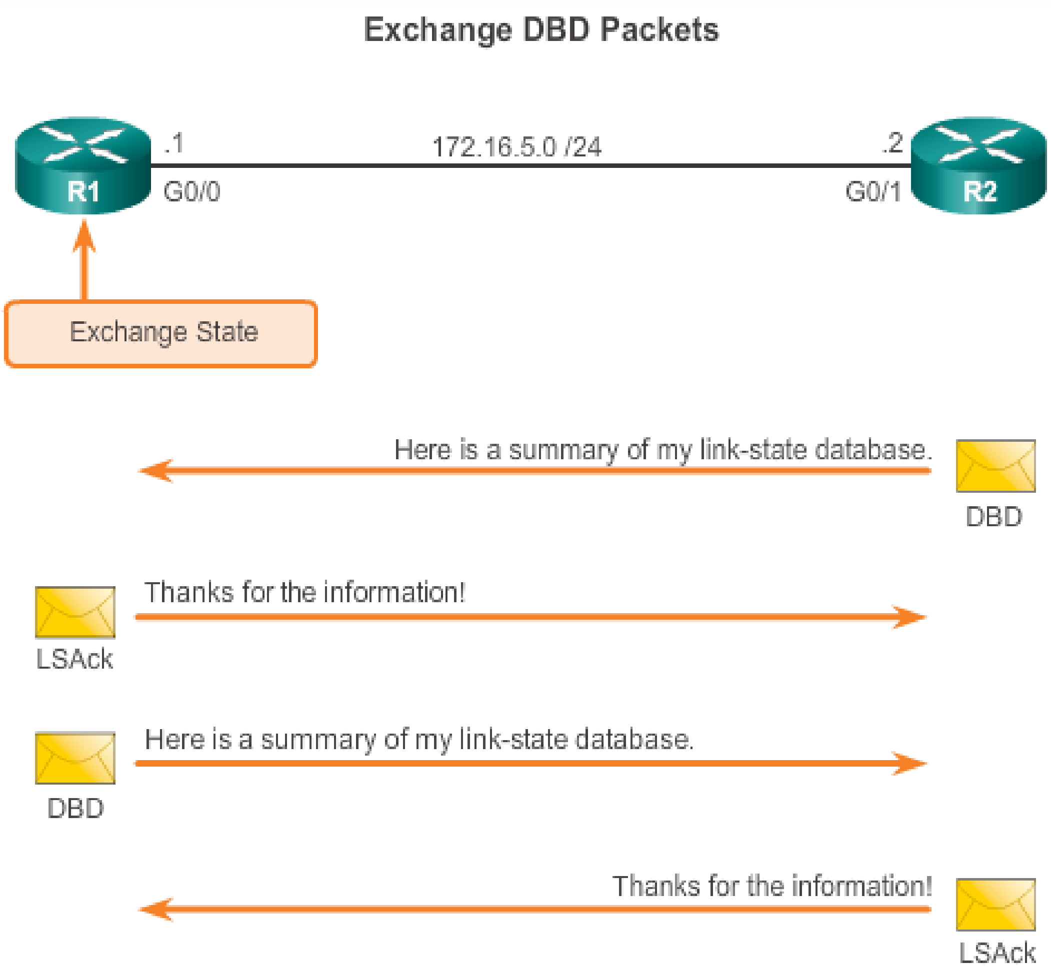
Number of Adjacencies=n(n-1)/2
n=number of routers
Example:5 routers (5-1)/2=10 adjacencies

OSPF Operation
Synchronizing OSPF Database



OSPF Operation

Synchronizing OSPF Database (cont.)



OSPF Router ID

OSPF Network Topology

Entering Router OSPF Configuration Mode on R1

```
R1(config)# router ospf 10
R1(config-router)# ?
Router configuration commands:
  auto-cost               Calculate OSPF interface cost
                          according to bandwidth
  network                 Enable routing on an IP network
  no                      Negate a command or set its defaults
  passive-interface       Suppress routing updates on an
                          interface
  priority                OSPF topology priority
  router-id               router-id for this OSPF process
```

Note: Output has been altered to display only the commands that will be used in this chapter.

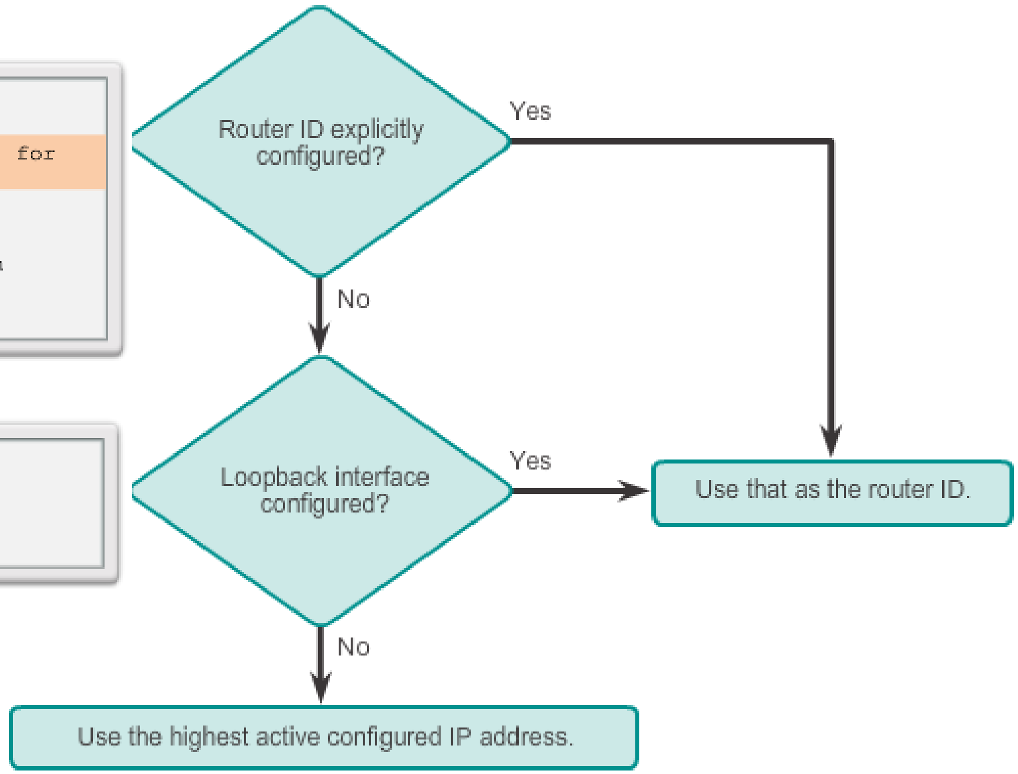
OSPF Router ID

Router IDs

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for
this to take effect
R1(config-router)# end
R1#
*Mar 25 19:46:09.711: %SYS-5-CONFIG_I: Configured from
console by console
```

```
R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1#
```

Router ID Order of Precedence



Clearing the OSPF Process

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1#
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down:
Interface down or detached
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached
```

Configure Single-area OSPFv2

The network Command

Assigning Interfaces to an OSPF Area

```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1#
```

Assigning Interfaces to an OSPF Area with a Quad Zero

```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.1 0.0.0.0 area 0
R1(config-router)# network 172.16.3.1 0.0.0.0 area 0
R1(config-router)# network 192.168.10.5 0.0.0.0 area 0
R1(config-router)#
R1#
```

Configure Single-Area OSPFv2

Passive Interface

- By default, OSPF messages are forwarded out all OSPF-enabled interfaces. However, these messages really only need to be sent out interfaces connecting to other OSPF-enabled routers.
- Sending out unneeded messages on a LAN affects the network in three ways:
  - Inefficient Use of Bandwidth
  - Inefficient Use of Resources
  - Increased Security Risk
- The Passive Interface feature helps limiting the scope of routing updates advertisements.

Configure Single-area OSPFv2

Configuring Passive Interfaces

Configuring a Passive Interface on R1

```
R1(config)# router ospf 10
R1(config-router)# passive-interface GigabitEthernet 0/0
R1(config-router)# end
R1#
```

Use the **passive-interface** router configuration mode command to prevent the transmission of routing messages through a router interface, but still allow that network to be advertised to other routers.

OSPF Cost

OSPF Metric = Cost

Cost = *reference bandwidth* / *interface bandwidth*
(default reference bandwidth is 10^8)
Cost = 100,000,000 bps / *interface bandwidth in bps*

Default Cisco OSPF Cost Values

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	10
Serial 1.544 Mbps	100,000,000	÷	1,544,000	64
Serial 128 kbps	100,000,000	÷	128,000	781
Serial 64 kbps	100,000,000	÷	64,000	1562

Same Cos
due to
reference
bandwidtl

OSPF Cost

OSPF Accumulates Costs

Cost of an OSPF route is the accumulated value from one router to the destination network.

```
R1# show ip route | include 172.16.2.0
O        172.16.2.0/24 [110/65] via 172.16.3.2, 03:39:07,
         Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 65, type intra
  area
  Last update from 172.16.3.2 on Serial0/0/0, 03:39:15 ago
  Routing Descriptor Blocks:
  * 172.16.3.2, from 2.2.2.2, 03:39:15 ago, via Serial0/0/0
      Route metric is 65, traffic share count is 1
R1#
```

OSPF Cost

Adjusting the Reference Bandwidth

- Use the **command - auto-cost reference-bandwidth**
- Must be configured on every router in the OSPF domain
- Notice that the value is expressed in Mb/s:
  - **Gigabit Ethernet** - **auto-cost reference-bandwidth 1000**
  - **10 Gigabit Ethernet** - **auto-cost reference-bandwidth 10000**

Verifying the S0/0/0 Link Cost

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
 Internet Address 172.16.3.1/30,Area 0,Attached via Network Statement
 Process ID 10,Router ID 1.1.1.1,Network Type POINT_TO_POINT,Cost:647
 Topology-MTID    Cost    Disabled    Shutdown     Topol
        0          647       no          no           B
 Transmit Delay is 1 sec, State POINT_TO_POINT
 Timer intervals configured, Hello 10, Dead 40, Wait 40,
   oob-resync timeout 40
   Hello due in 00:00:01
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 3/3, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
R1#
```

Verifying the Metric to the R2 LAN

```
R1# show ip route | include 172.16.2.0
O       172.16.2.0/24 [110/648] via 172.16.3.2, 00:06:03, Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 648, type intra area
  Last update from 172.16.3.2 on Serial0/0/0, 00:06:17 ago
  Routing Descriptor Blocks:
  * 172.16.3.2, from 2.2.2.2, 00:06:17 ago, via Serial0/0/0
      Route metric is 648, traffic share count is 1
R1#
R1#
```

OSPF Cost

Default Interface Bandwidths

On Cisco routers, the default bandwidth on most serial interfaces is set to 1.544 Mb/s.

Verifying the Default Bandwidth Settings of R1 Serial 0/0/0

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: Link to R2
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
```

OSPF Cost

Adjusting the Interface Bandwidths

Adjusting the R1 Serial 0/0/1 Interface

```
R1(config)# int s0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# end
R1#
*Mar 27 10:10:07.735: %SYS-5-CONFIG_I: Configured from console by c
R1#
R1# show interfaces serial 0/0/1 | include BW
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
R1#
R1# show ip ospf interface serial 0/0/1 | include Cost:
  Process ID 10, Router ID 1.1.1.1, Network Type
  POINT_TO_POINT, Cost: 15625
R1#
```

OSPF Cost

Manually Setting the OSPF Cost

Both the **bandwidth** interface command and the **ip ospf cost** interface command achieve the same result, which is to provide an accurate value for use by OSPF in determining the best route.

```
R1(config)# int s0/0/1
R1(config-if)# no bandwidth 64
R1(config-if)# ip ospf cost 15625
R1(config-if)# end
R1#
R1# show interface serial 0/0/1 | include BW
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
R1#
R1# show ip ospf interface serial 0/0/1 | include Cost:
    Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
    Cost: 15625
R1#
```

Verify OSPF Neighbors

Verify that the router has formed an adjacency with its neighboring routers.

```
R1# show ip ospf neighbor

Neighbor ID   Pri   State     Dead Time  Address         Interface
3.3.3.3       0     FULL/-    00:00:37   192.168.10.6    Serial0/0/1
2.2.2.2       0     FULL/-    00:00:30   172.16.3.2      Serial0/0/0
R1#
```

Verify OSPF

Verify OSPF Protocol Settings

Verifying R1's OSPF Neighbors

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not
  set
  Incoming update filter list for all interfaces is not
  set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2              110      00:17:18
    3.3.3.3              110      00:14:49
  Distance: (default is 110)

R1#
```

Verify OSPF

Verify OSPF Process Information

Verifying R1's OSPF Process

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 01:37:15.156, Time elapsed: 01:32:57.776
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode:
cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
```

Verify OSPF

Verify OSPF Interface Settings

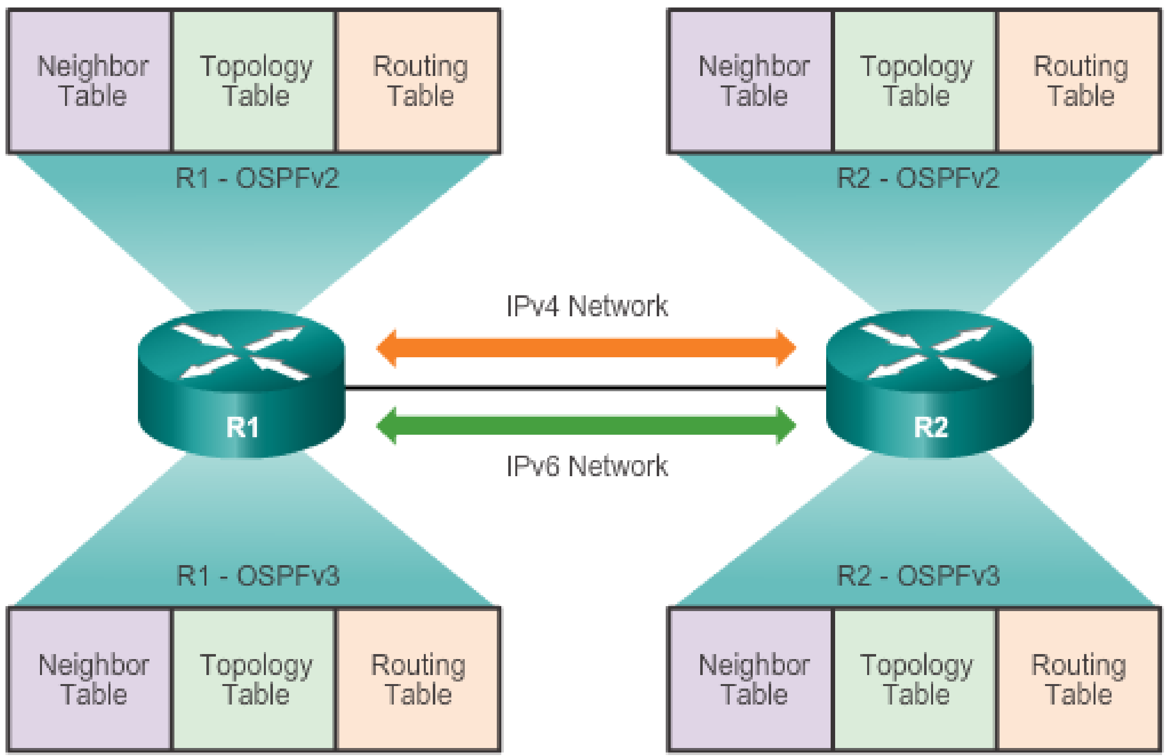
Verifying R1's OSPF Interfaces

```
R1# show ip ospf interface brief
Interface    PID   Area   IP Address/Mask    Cost   State   Nbrs F/C
Se0/0/1      10    0      192.168.10.5/30    15625  P2P     1/1
Se0/0/0      10    0      172.16.3.1/30      647    P2P     1/1
Gi0/0        10    0      172.16.1.1/24      1      DR      0/0
R1#
```

OSPFv2 vs. OSPFv3

OSPFv3

OSPFv2 and OSPFv3 Data Structures



OSPFv2 vs. OSPFv3

Similarities Between OSPFv2 to OSPFv3

OSPFv2 and OSPFv3	
Link-State	Yes
Routing Algorithm	SPF
Metric	Cost
Areas	Supports the same two-level hierarchy
Packet Types	Same Hello, DBD, LSR, LSU and LSAck packets
Neighbor Discovery	Transitions through the same states using Hello packets
DR and BDR	Function and election process is the same
Router ID	32-bit router ID: determined by the same process in both protocols

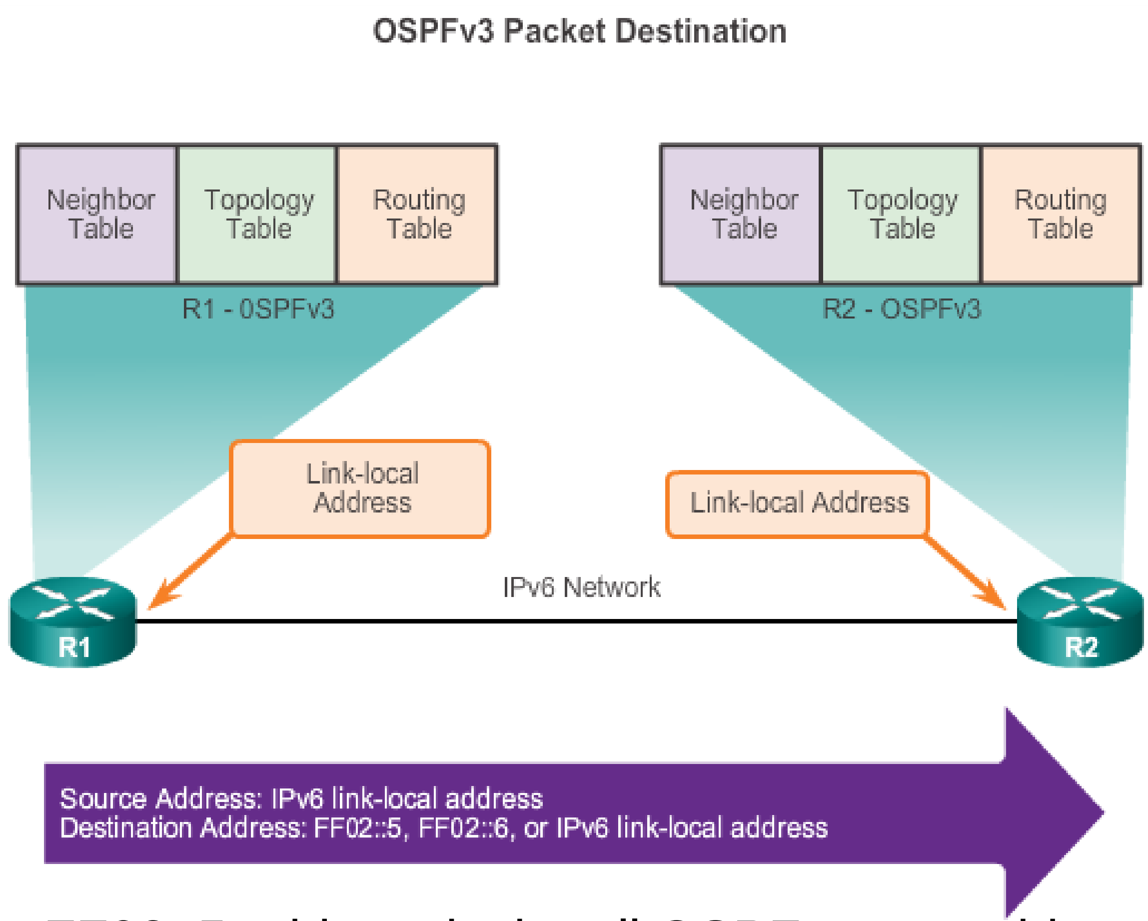
OSPFv2 vs. OSPFv3

Differences Between OSPFv2 to OSPFv3

	OSPFv2	OSPFv3
Advertises	IPv4 networks	IPv6 prefixes
Source Address	IPv4 source address	IPv6 link-local address
Destination Address	Choice of: • Neighbor IPv4 unicast address • 224.0.0.5 all-OSPF-routers multicast address • 224.0.0.6 DR/BDR multicast address	Choice of: • Neighbor IPv6 link-local address • FF02::5 all-OSPFv3-routers multicast address • FF02::6 DR/BDR multicast address
Advertise Networks	Configured using the **`network`** router configuration command	Configured using the **`ipv6 ospf process-id area-id`** interface configuration command
IP Unicast Routing	IPv4 unicast routing is enabled by default.	IPv6 unicast forwarding is not enabled by default. The **`ipv6 unicast-routing`** global configuration command must be configured.
Authentication	Plain text and MD5	IPv6 authentication

OSPFv2 vs. OSPFv3

Link-Local Addresses



FF02::5 address is the all OSPF router address
FF02::6 is the DR/BDR multicast address

Configuring OSFPv3

OSPFv3 Network Topology

Configuring Global-Unicast Addresses on R1

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# description R1 LAN
R1(config-if)# ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)# no shut
R1(config-if)# end
R1#
```

Configuring OSFPv3

OSPFv3 Network Topology (cont.)

Steps to Configure OSPFv3

Step 1: Enable IPv6 unicast routing: **`ipv6 unicast-routing`**.

Step 2: (Optional) Configure link-local addresses.

Step 3: Configure a 32-bit router ID in OSPFv3 router configuration mode using the **`router-id`** `rid` command.

Step 4: Configure optional routing specifics such as adjusting the reference bandwidth.

Step 5: (Optional) Configure OSPFv3 interface specific settings. For example, adjust the interface bandwidth.

Step 6: Enable IPv6 routing by using the **`ipv6 ospf area`** command.

Configuring OSFPv3

Link-Local Addresses

```
R1# show ipv6 interface brief
Em0/0                     [administratively down/down]
    unassigned
GigabitEthernet0/0        [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:1::1
GigabitEthernet0/1        [administratively down/down]
    unassigned
Serial0/0/0               [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:A001::1
Serial0/0/1               [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:A003::1
R1#
```

- Link-local addresses are automatically created when an IPv6 global unicast address is assigned to the interface (required).
- Global unicast addresses are not required.
- Cisco routers create the link-local address using FE80::/10 prefix and the EUI-64 process unless the router is configured manually,
- EUI-64 involves using the 48-bit Ethernet MAC address, inserting FFFE in the middle and flipping the seventh bit. For serial interfaces, Cisco uses the MAC address of an Ethernet interface.
- Notice in the figure that all three interfaces are using the same link-local address.

Configuring OSFPv3

Assigning Link-Local Addresses

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

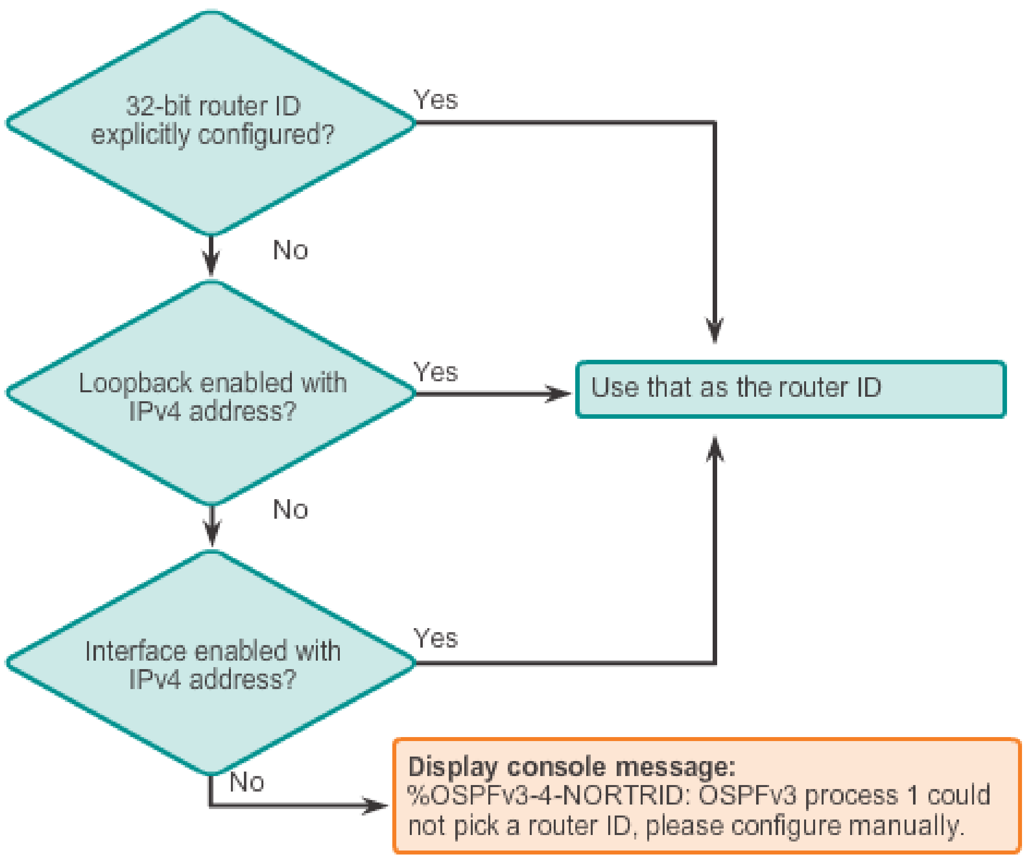
Manually configuring the link-local address provides the ability to create an address that is recognizable and easier to remember.

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    FE80::1
    2001:DB8:CAFE:1::1
GigabitEthernet0/1     [administratively down/down]
    unassigned
Serial0/0/0            [up/up]
    FE80::1
    2001:DB8:CAFE:A001::1
Serial0/0/1            [up/up]
    FE80::1
    2001:DB8:CAFE:A003::1
R1#
```

Configuring OSPFv3

Configuring the OSPFv3 Router ID

Router ID Order of Precedence



Configuring OSFPv3

Configuring the OSPFv3 Router ID (cont.)

Assigning a Router ID to R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manually
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6: Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
R1(config-rtr)#
R1(config-rtr)# end
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
R1#
```

Configuring OSFPv3

Modifying an OSPFv3 Router ID

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# end
R1#
```

```
R1# clear ipv6 ospf process
Reset selected OSPFv3 processes? [no]: y
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
R1#
```

Enabling OSPFv3 on Interfaces

Instead of using the **network** router configuration mode command to specify matching interface addresses, OSPFv3 is configured directly on the interface.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface   PID   Area      Intf ID   Cost    State   Nbrs F/C
Se0/0/1     10     0          7       15625   P2P     0/0
Se0/0/0     10     0          6       647     P2P     0/0
Gi0/0       10     0          3        1      WAIT    0/0
R1#
```

Verify OSPFv3 Neighbors/Protocol Settings

```
R1# show ipv6 ospf neighbor

OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

Neighbor ID   Pri   State       Dead Time   Interface ID Interface
3.3.3.3         0   FULL/  -    00:00:39    6            Serial0/0/1
2.2.2.2         0   FULL/  -    00:00:36    6            Serial0/0/0
R1#
```

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

Verify OSPFv3

Verify OSPFv3 Interfaces

```
R1# show ipv6 ospf interface brief
Interface     PID   Area             Intf ID    Cost   State Nbrs F/C
Se0/0/1       10    0                7          15625  P2P   1/1
Se0/0/0       10    0                6          647    P2P   1/1
Gi0/0         10    0                3          1      DR    0/0
R1#
```

Verify OSPFv3

Verify IPv6 Routing Table

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND
Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter,
OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
NSSA ext 2
O   2001:DB8:CAFE:2::/64 [110/657]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:3::/64 [110/1304]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Chapter 6: Summary

OSPF:

- For IPv4 is OSPFv2
- For IPv6 is OSPFv3
- Classless, link-state routing protocol with a default administrative distance of 110, and is denoted in the routing table with a route source code of **O**
- OSPFv2 is enabled with the **router ospf** *process-id* global configuration mode command. The *process-id* value is locally significant, which means that it does not need to match other OSPF routers to establish adjacencies with those neighbors.
- **Network** command uses the *wildcard-mask* value which is the inverse of the subnet mask, and the *area-id* value

Chapter 6: Summary (cont.)

OSPF:

- By default, OSPF Hello packets are sent every 10 seconds on multiaccess and point-to-point segments and every 30 seconds on NBMA segments (Frame Relay, X.25, ATM), and are used by OSPF to establish neighbor adjacencies. The Dead interval is four times the Hello interval, by default.
- For routers to become adjacent, their Hello interval, Dead interval, network types, and subnet masks must match. Use the **show ip ospf neighbors**command to verify OSPF adjacencies.
- In a multiaccess network, OSPF elects a DR to act as collection and distribution point for LSAs sent and received. A BDR is elected to assume the role of the DR should the DR fail. All other routers are known as DROTHERs. All routers send their LSAs to the DR, which then floods the LSA to all other routers in the multiaccess network.

Chapter 6: Summary (cont.)

OSPF:

- In multiaccess networks, the router with the highest router ID is the DR, and the router with the second highest router ID is the BDR. This can be superseded by the **ip ospf** *priority* command on that interface. The router with the highest priority value is the DR, and next-highest the BDR.
- The **show ip protocols** command is used to verify important OSPF configuration information, including the OSPF process ID, the router ID, and the networks the router is advertising.
- OSPFv3 is enabled on an interface and not under router configuration mode. OSPFv3 needs link-local addresses to be configured. IPv6 Unicast routing must be enabled for OSPFv3. A 32-bit router-ID is required before an interface can be enabled for OSPFv3.

Chapter 6: Summary (cont.)

OSPF:

- The **show ip protocols** command is used to verify important OSPFv2 configuration information, including the OSPF process ID, the router ID, and the networks the router is advertising.
- OSPFv3
  - Enabled on an interface and not under router configuration mode
  - Needs link-local addresses to be configured. IPv6
  - Unicast routing must be enabled for OSPFv3
  - 32-bit router-ID is required before an interface can be enabled for OSPFv3
  - **show ipv6 protocols** command is a quick way to verify configuration information (OSPF process ID, the router ID, and the interfaces enabled for OSPFv3)

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7: Adjust and Troubleshoot Single-Area OSPF

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7

JG1

Chapter 7: Objectives

After completing this chapter, you will be able to:

- Modify the OSPF interface priority to influence the DR/BDR election.
- Configure a router to propagate a default route in an OSPF network.
- Modify OSPF interface settings to improve network performance.
- Configure OSPF authentication to ensure secure routing updates.
- Explain the process and tools used to troubleshoot a single-area OSPF network.
- Troubleshoot missing route entries in a single-area OSPFv2 route table.
- Troubleshoot missing route entries in a single-area OSPFv3 route table.

Slide 3

JG1 from Vittoria: vittoria deloulay 9/24/2013
I think this would look better if it was in the slide format, not as a graphic. (see corresponding planning guide)
Jane Gibbons, 9/25/2013

7.1 Advanced Single-Area OSPF Configurations

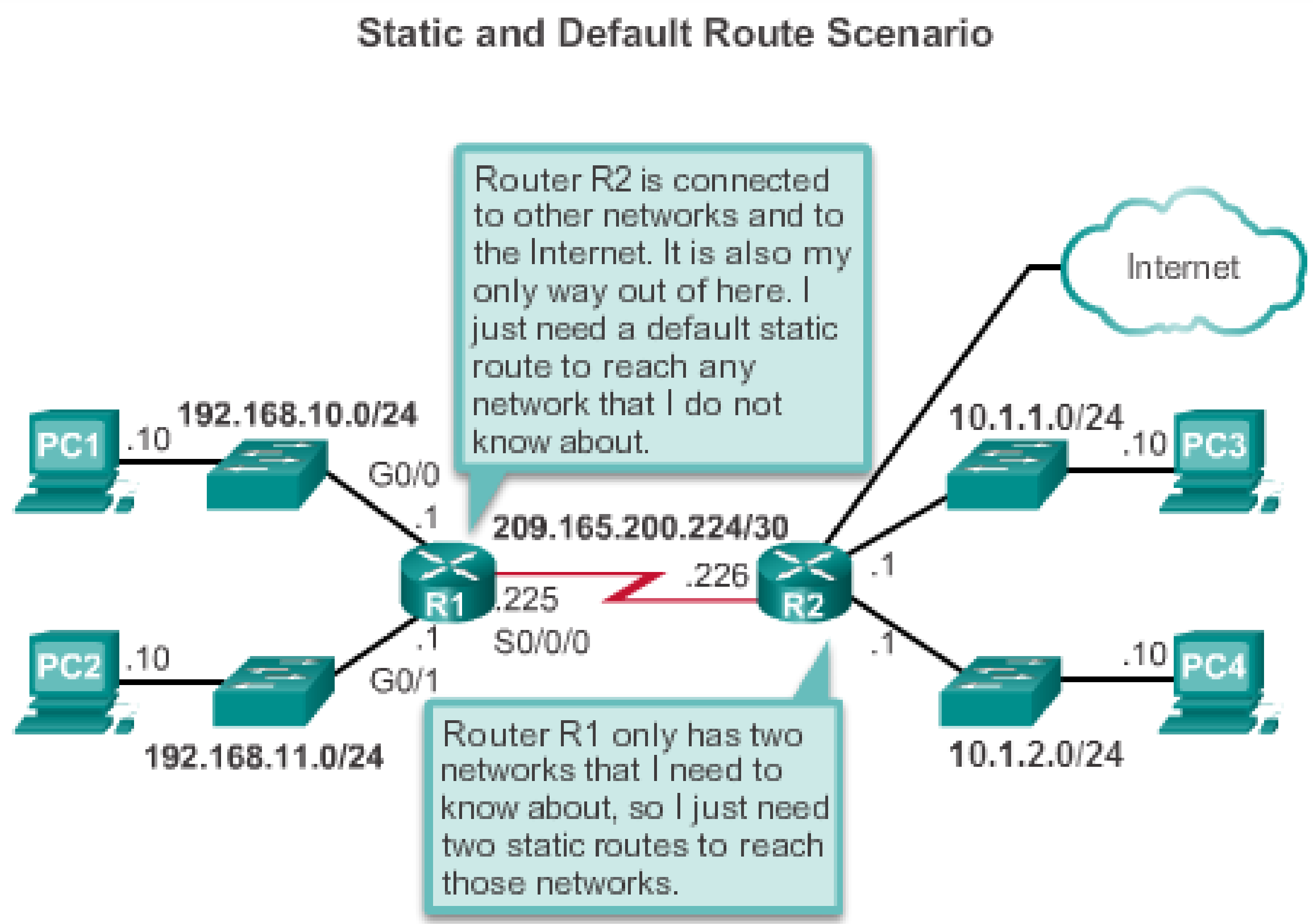
Cisco | Networking Academy®
Mind Wide Open™

Routing in the Distribution and Core Layers

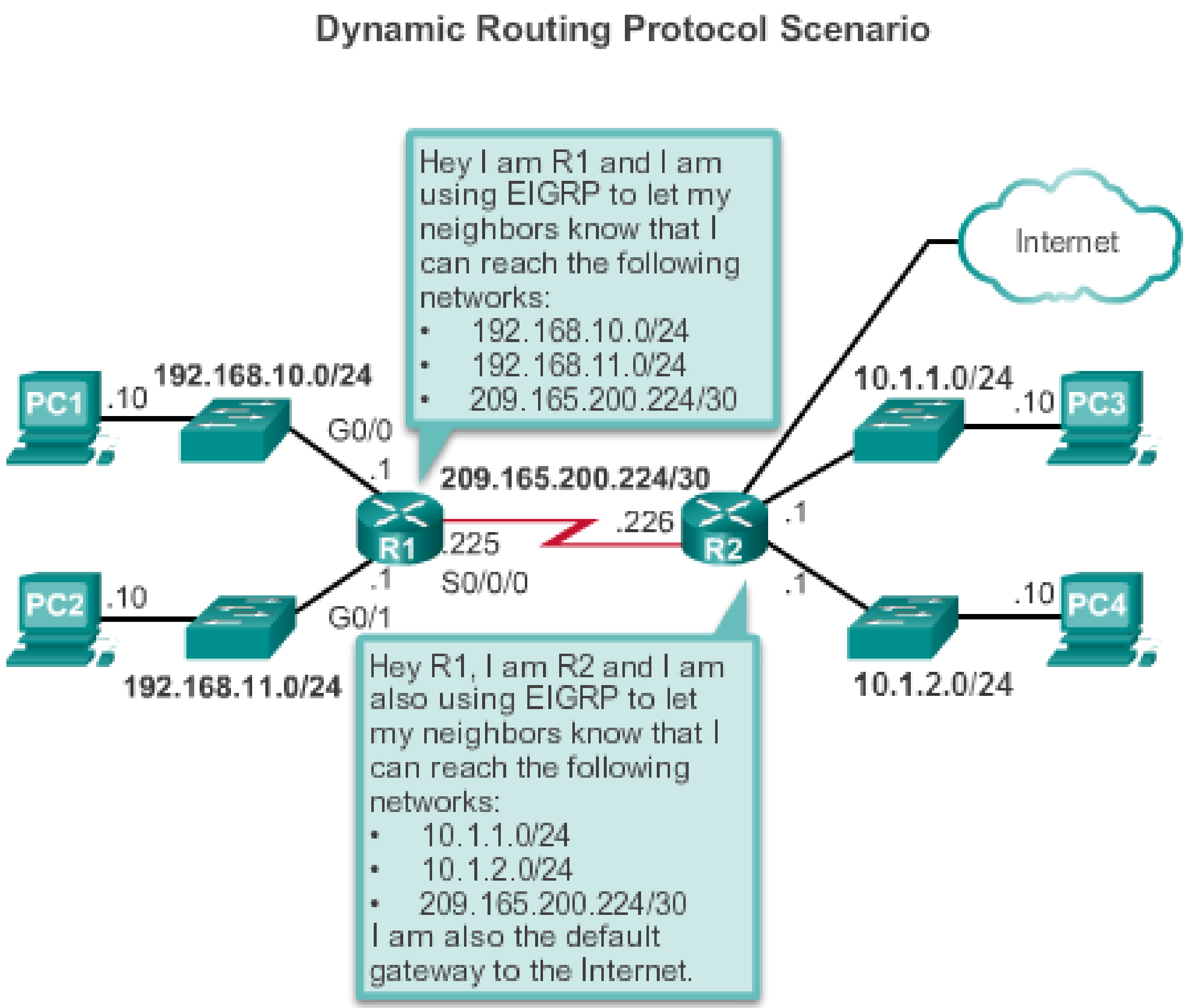
Routing versus Switching

- Switches, link aggregation, LAN redundancy and wireless LANs are all technologies that provide or enhance user access to network resources.
- Scalable networks also require optimal reachability between sites. Remote network reachability is provided by routers and Layer 3 switches which operate in the distribution and core layers.

Routing in the Distribution and Core Layers
Static Routing

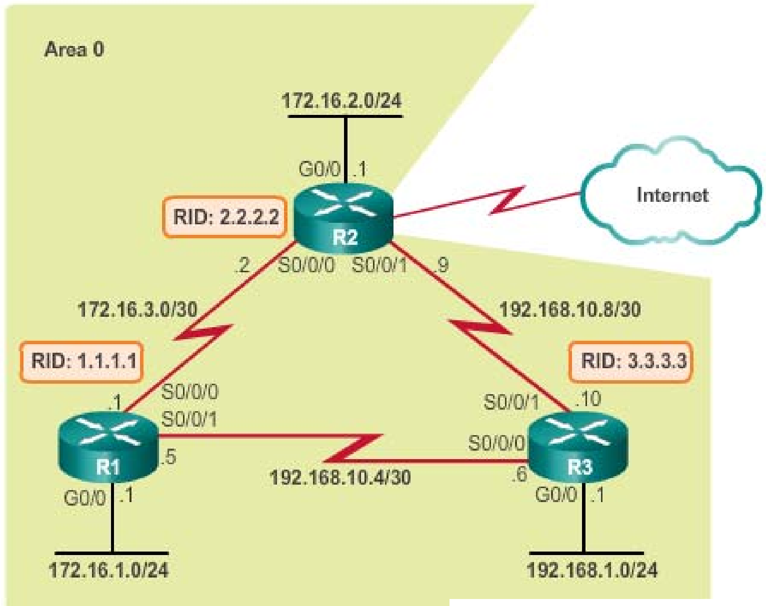


Dynamic Routing Protocols



Routing in the Distribution and Core Layers

Configuring Single-Area OSPF




```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1(config-router)# passive-interface g0/0
R1(config-router)#
```

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R2(config-router)# network 172.16.2.1 0.0.0.0 area 0
R2(config-router)# network 172.16.3.2 0.0.0.0 area 0
R2(config-router)# network 192.168.10.9 0.0.0.0 area 0
R2(config-router)#
R2(config-router)# passive-interface g0/0
R2(config-router)#
```

Routing in the Distribution and Core Layers

Verifying Single-Area OSPF

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State       Dead Time    Address         Interface
3.3.3.3         0     FULL/  -    00:00:32     192.168.10.6    Serial0/0/1
2.2.2.2         0     FULL/  -    00:00:38     172.16.3.2      Serial0/0/0
R1#
```

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance       Last Update
    3.3.3.3               110       00:12:14
    2.2.2.2               110       00:12:46
  Distance: (default is 110)

R1#v
```

Verifying Single-Area OSPF (cont.)

```
R1# show ip ospf
 Routing Process "ospf 10" with ID 1.1.1.1
 Start time: 00:06:18.952, Time elapsed: 00:39:56.400

 <Output omitted>

 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 1000 mbps
 Area BACKBONE(0)
        Number of interfaces in this area is 3
Area has no authentication
SPF algorithm last executed 00:15:21.436 ago
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x023523
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#
```

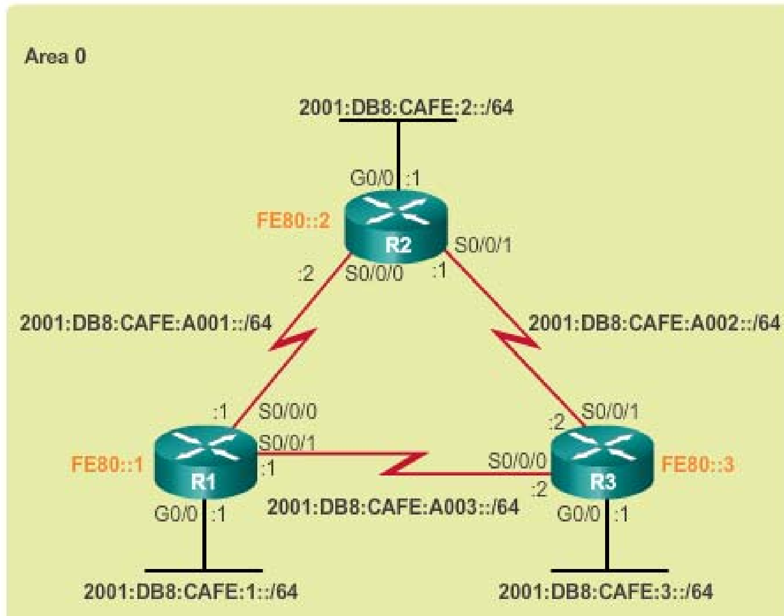
Verifying Single-Area OSPF (cont.)

```
R1# show ip ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown     Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 172.16.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.10.5/30, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
Cost: 647

<Output omitted>
```

```
R1# show ip ospf interface brief
Interface    PID   Area     IP Address/Mask    Cost  State Nbrs F/C
Gi0/0        10    0        172.16.1.1/24      1     DR    0/0
Se0/0/1      10    0        192.168.10.5/30    647   P2P   1/1
Se0/0/0      10    0        172.16.3.1/30      647   P2P   1/1
R1#
```

Routing in the Distribution and Core Layers

Configuring Single-Area OSPFv3



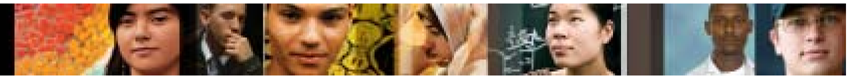

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6:  Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
R1(config-rtr)#
R1(config-rtr)# interface GigabitEthernet 0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

```
R2(config)# ipv6 router ospf 10
R2(config-rtr)# router-id 2.2.2.2
R2(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6:  Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
R2(config-rtr)#
R2(config-rtr)# interface GigabitEthernet 0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/0
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/1
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# end
R2#
```

Verifying Single-Area OSPFv3

```
R1# show ipv6 ospf neighbor

            OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

Neighbor ID Pri State        Dead Time Interface ID Interface
3.3.3.3       0  FULL/  -      00:00:31  6            Serial0/0/1
2.2.2.2       0  FULL/  -      00:00:37  6            Serial0/0/0
2.2.2.2       1  FULL/BDR      00:00:38  3            GigabitEthernet0/0
3.3.3.3       1  FULL/DROTHER  00:00:32  3            GigabitEthernet0/0
R1#
```

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```



Routing in the Distribution and Core Layers

Verifying Single-Area OSPFv3 (cont.)

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
       D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
       DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter,
       OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1,
       ON2 - OSPF NSSA ext 2
O   2001:DB8:CAFE:2::/64 [110/1]
     via GigabitEthernet0/0, directly connected
O   2001:DB8:CAFE:3::/64 [110/1]
     via GigabitEthernet0/0, directly connected
O   2001:DB8:CAFE:A002::/64 [110/648]
     via FE80::2, GigabitEthernet0/0
     via FE80::3, GigabitEthernet0/0
R1#
```

```
R1# show ipv6 ospf interface brief
Interface     PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0/1       10    0               7          647   P2P   1/1
Se0/0/0       10    0               6          647   P2P   1/1
Gi0/0         10    0               3          1     DR    2/2
R1#
```

OSPF in Multiaccess Networks

OSPF Network Types

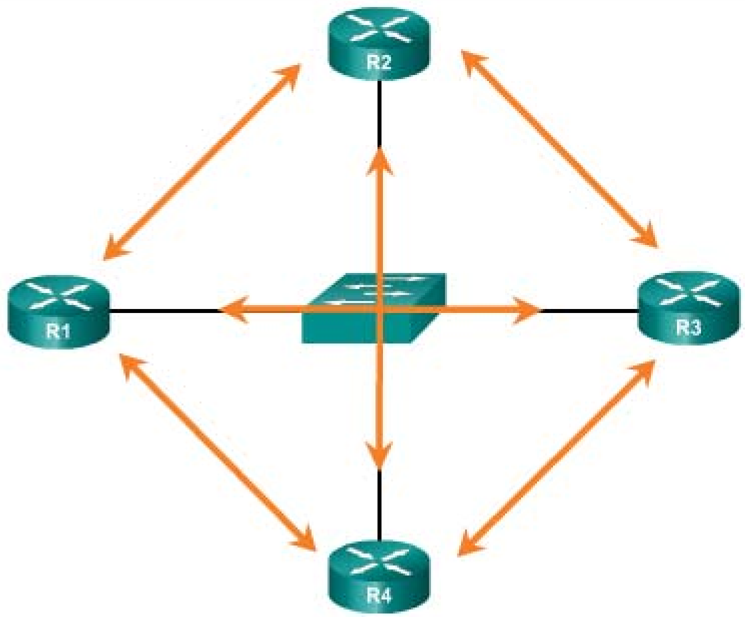
- **Point-to-point** – Two routers interconnected over a common link. Often the configuration in WAN links.
- **Broadcast Multiaccess** – Multiple routers interconnected over an Ethernet network.
- **Non-broadcast Multiaccess (NBMA)** – Multiple routers interconnected in a network that does not allow broadcasts, such as Frame Relay.
- **Point-to-multipoint** – Multiple routers interconnected in a hub-and-spoke topology over an NBMA network.
- **Virtual links** – Special OSPF network used to interconnect distant OSPF areas to the backbone area.

OSPF in Multiaccess Networks
Challenges in Multiaccess Networks

Multiaccess networks can create two challenges for OSPF:

- **Creation of multiple adjacencies** – creating adjacencies with multiple routers would lead to an excessive number of LSAs being exchanged.
- **Extensive flooding of LSAs** – Link-state routers flood the network when OSPF is initialized or when there is a change.

- Formula used to calculate the number of required adjacencies n(n-1)/2
- A topology of 4 routers would result in 4(4-1)/2 = 6

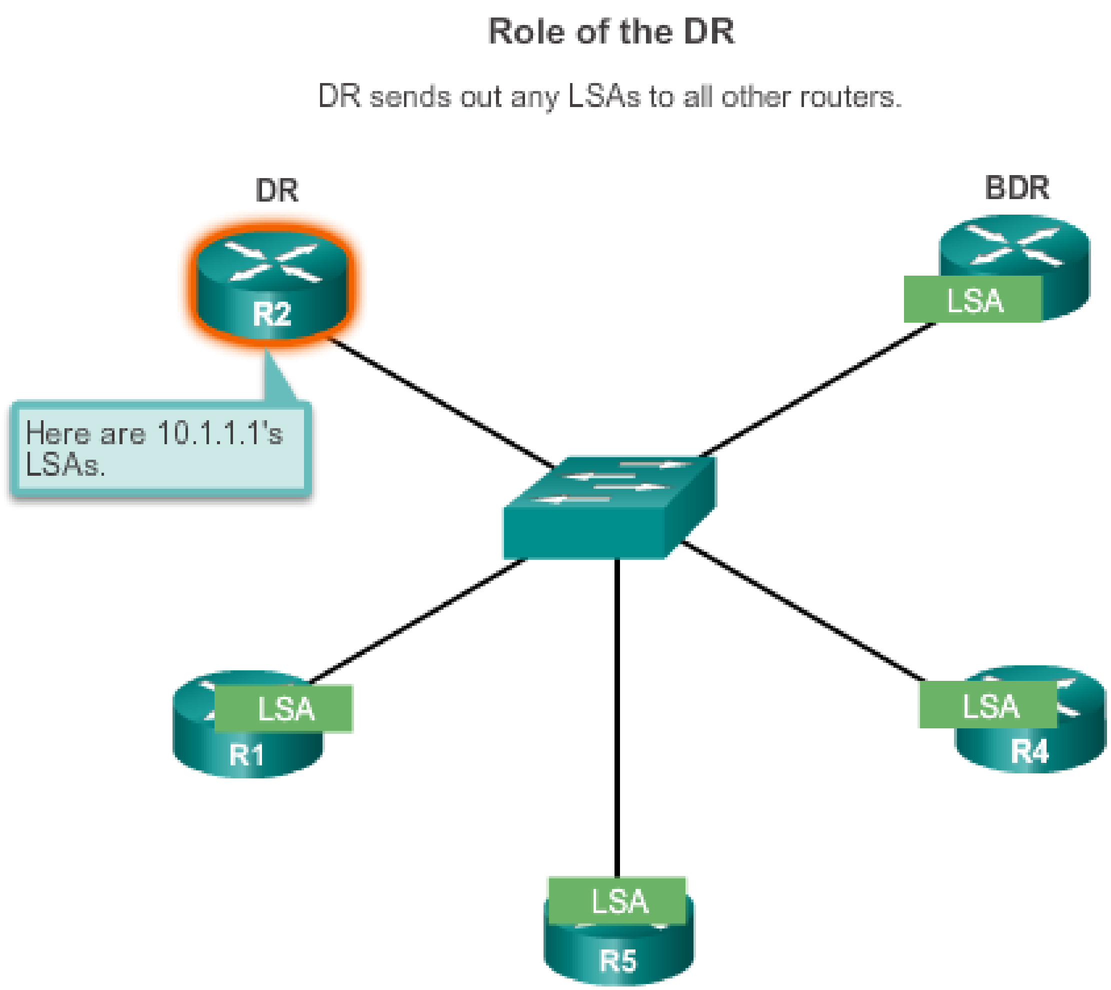


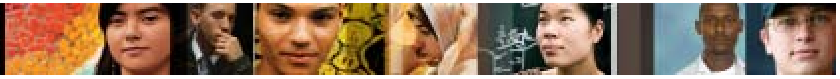
OSPF Designated Router

- The designated router (DR) is the solution to managing adjacencies and flooding of LSAs on a multiaccess network.
- The backup designated router (BDR) is elected in case the DR fails.
- All other non-DR and non-BDR routers become DROTHERs. DROTHERs only form adjacencies with the DR and BDR.
- DROTHERs only send their LSAs to the DR and BDR using the multicast address 224.0.0.6.
- DR uses the multicast address 224.0.0.5 to send LSAs to all other routers. DR only router flooding LSAs.
- DR/BDR Elections only necessary on multiaccess networks.

OSPF in Multiaccess Networks

OSPF Designated Router (cont.)





OSPF in Multiaccess Networks

Verifying DR/BDR Roles

Verifying the Role of R1

```
R1# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet Address 192.168.1.1/28,Area 0,Attached via Network Statement
 Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Topology-MTID     Cost     Disabled     Shutdown      Topology Name
       0            1          no           no             Base
 Transmit Delay is 1 sec, State DROTHER, Priority 1
 Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
 Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   oob-resync timeout 40
   Hello due in 00:00:06
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 2, Adjacent neighbor count is 2
   Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
   Adjacent with neighbor 3.3.3.3  (Designated Router)
 Suppress hello for 0 neighbor(s)
R1#
```

OSPF in Multiaccess Networks

Verifying DR/BDR Adjacencies

State of neighbors in multiaccess networks can be:

- **FULL/DROTHER** – This is a DR or BDR router that is fully adjacent with a non-DR or BDR router.
- **FULL/DR** – The router is fully adjacent with the indicated DR neighbor.
- **FULL/BDR** – The router is fully adjacent with the indicated BDR neighbor.
- **2-WAY/DROTHER** – The non-DR or BDR router has a neighbor adjacency with another non-DR or BDR router.

```
R1# show ip ospf neighbor

Neighbor ID Pri State         Dead Time  Address      Interface

1 2.2.2.2     1   FULL/BDR      00:00:36   192.168.1.2 GigabitEthernet0/0

2 3.3.3.3     1   FULL/DR       0:00:35    192.168.1.3 GigabitEthernet0/0

R1#
```

OSPF in Multiaccess Networks

Default DR/BDR Election Process

- The router with the highest interface priority is elected as the DR.
- The router with the second highest interface priority is elected as the BDR.
- Priority can be configured between 0-255. (Priority of 0 - router cannot become the DR. 0
- If interface priorities are equal, then the router with highest router ID is elected DR and second highest the BDR
- Three ways to determine router ID:
    - Router ID can be manually configured.
    - If not configured, the ID determined by the highest loopback IP address.
    - If no loopbacks, the ID is determined by the highest active IPv4 address.
- In an IPv6 network, the router ID must be configured manually.

OSPF in Multiaccess Networks

DR/BDR Election Process

DR remains the DR until one of the following occurs:

- The DR fails.
- The OSPF process on the DR fails or is stopped.
- The multiaccess interface on the DR fails or is shutdown.

If the DR fails, the BDR is automatically promoted to DR.

- There is then a new BDR election and the DROTHER with the higher priority or router ID is elected as the new BDR.

The OSPF Priority

- Instead of setting the router ID on all routers, it is better to control the election by setting interface priorities.
  - To change the priority, use one of the following commands:

    ip ospf priority *value* (OSPFv2 interface command)

    ipv6 ospf priority *value* (OSPFv3 interface command)

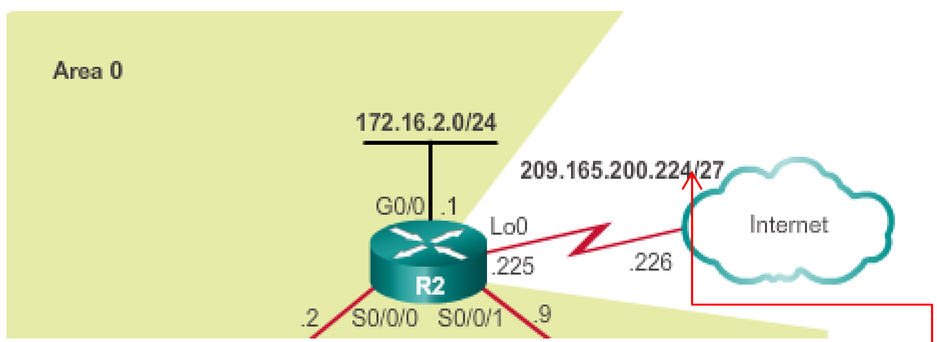
- To begin another OSPF election, use one of the following methods:
  - Shutdown the router interfaces and then re-enable them starting with the DR, then the BDR, and then all other routers.
  - Reset the OSPF process using the **clear ip ospf process** privileged EXEC mode command on all routers.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#
```

Default Route Propagation

Propagating a Default Static Route in OSPFv2

The router connected to the Internet that is used to propagate a default route is often called the edge, entrance or gateway router. In an OSPF network, it may also be call the autonomous system boundary router (ASBR).




```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Default Route Propagation

Verifying the Propagated Default Route

```
R2# show ip route | begin Gateway

Gateway of last resort is 209.165.200.226 to network
0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.226, Loopback0
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O  172.16.1.0/24 [110/65] via 172.16.3.1, 00:01:44,
   Serial0/0/0
C  172.16.2.0/24 is directly connected, GigabitEthernet0/0
L  172.16.2.1/32 is directly connected, GigabitEthernet0/0
C  172.16.3.0/30 is directly connected, Serial0/0/0
L  172.16.3.2/32 is directly connected, Serial0/0/0
O  192.168.1.0/24 [110/65] via 192.168.10.10, 00:01:12,
   Serial0/0/1
   192.168.10.0/24 is variably subnetted, 3 subnets, 2
    masks
O  192.168.10.4/30 [110/128] via 192.168.10.10, 00:01:12,
   Serial0/0/1
           [110/128] via 172.16.3.1, 00:01:12, Serial0/0/0
C  192.168.10.8/30 is directly connected, Serial0/0/1
L  192.168.10.9/32 is directly connected, Serial0/0/1
   209.165.200.0/24 is variably subnetted, 2 subnets, 2
    masks
```

Default Route Propagation

Propagating a Default Static Route in OSPFv3

Enabling OSPFv3 on the R1 Interfaces

```
R2(config)# ipv6 route ::/0 2001:DB8:FEED:1::2
R2(config)#
R2(config)# ipv6 router ospf 10
R2(config-rtr)# default-information originate
R2(config-rtr)# end
R2#
*Apr 10 11:36:21.995: %SYS-5-CONFIG_I: Configured from console by
console
R2#
```

Verifying the propagated IPv6 default Route

```
R2# show ipv6 route static
IPv6 Routing Table - default - 12 entries
Codes:C -Connected, L - Local, S - Static, U - Per-user Static route
      B -BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 -ISIS L2, IA - ISIS interarea, IS-ISIS summary,D-EIGRP
      EX -EIGRP external, ND-ND Default,NDp-ND Prefix,DCE-Destination
      NDr -Redirect, O - OSPF Intra,OI-OSPF Inter,OE1-OSPF ext 1
      OE2 -OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:DB8:FEED:1::2, Loopback0
R2#
```

OSPF Hello and Dead Intervals

OSPF Hello and Dead intervals must match, or a neighbor adjacency will not occur.

Verifying the OSPF Intervals on R1

```
R1# show ip ospf interface serial 0/0/0 | include Timer
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
R1#
```

Verifying OSPF Timer Activity

```
R1# show ip ospf neighbor

Neighbor ID  Pri  State    Dead Time  Address       Interface
3.3.3.3      0    FULL/-   00:00:35   192.168.10.6  Serial0/0/1
2.2.2.2      0    FULL/-   00:00:33   172.16.3.2    Serial0/0/0
R1#
```

Fine-tuning OSPF Interfaces

Modifying OSPF Intervals

- Modifying OSPFv2 Intervals

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)# end
R1#
```

- Modifying OSPFv3 Intervals

```
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 ospf hello-interval 5
R1(config-if)# ipv6 ospf dead-interval 20
R1(config-if)# end
R1#
```

- Verifying the OSPFv3 interface intervals

```
R2# show ipv6 ospf interface s0/0/0 | include Timer
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
R2#
R2# show ipv6 ospf neighbor

            OSPFv3 Router with ID (2.2.2.2) (Process ID 10)

Neighbor ID  Pri  State    Dead Time   Interface ID  Interface
3.3.3.3        0  FULL/-   00:00:38    7             Serial0/0/1
1.1.1.1        0  FULL/-   00:00:19    6             Serial0/0/0
R2#
```

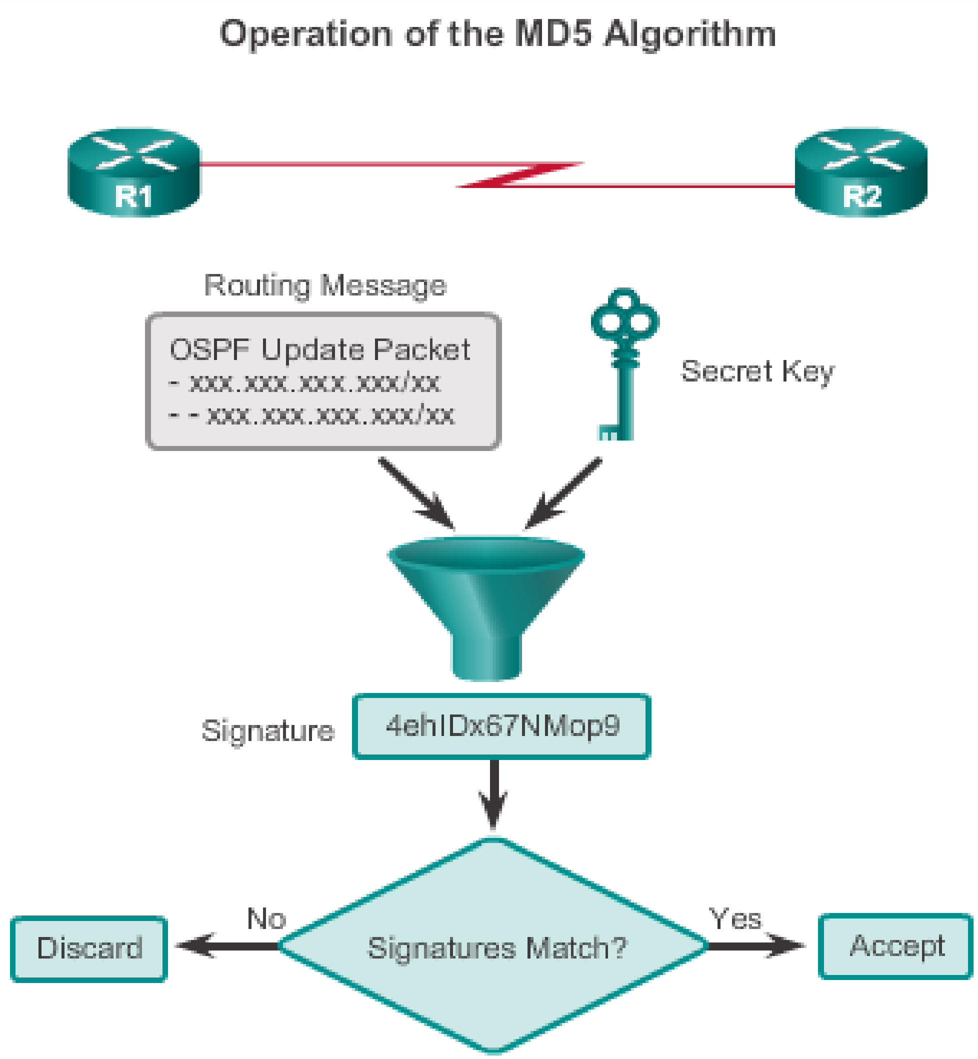
Secure OSPF

Secure Routing Updates

- When neighbor authentication has been configured on a router, the router authenticates the source of each routing update packet that it receives.
- An authenticating key that is known to both the sending and the receiving route is exchanged.
- OSPF supports three types of authentication:
  - **Null** – no authentication.
  - **Simple password authentication** – the password in the update is sent in plaintext over the network (outdated method).
  - **MD5 authentication** – Most secure and recommended method of authentication. Password is calculated using the MD5 algorithm.

Secure OSPF

MD5 Authentication



Configuring OSPF MD5 Authentication

- MD5 authentication can be enabled globally for all interfaces or on a per-interface basis.
- To enable OSPF MD5 authentication globally, configure:
  - **`ip ospf message-digest-key`** *key* **`md5`** *password* (interface configuration command)
  - **`area`** *area-id* **`authentication message-digest`** (router configuration command)
- To enable MD5 authentication on a per-interface basis, configure:
  - **`ip ospf message-digest-key`** *key* **`md5`** *password* (interface configuration command)
  - **`ip ospf authentication message-digest`** (interface configuration command)

Secure OSPF

OSPF MD5 Authentication Example

```
R1(config)# router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-router)# exit
R1(config)#
*Apr  8 09:58:09.899: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 09:58:28.627: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)#
```

continued

Secure OSPF

OSPF MD5 Authentication Example (cont.)

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
*Apr  8 10:20:10.647: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 10:20:50.007: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
```

Secure OSPF

Verifying OSPF MD5 Authentication

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 64
Topology-MTID    Cost   Disabled   Shutdown     Topology Name
      0           64       no         no             Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
R1#
R1# show ip ospf interface | include Message
  Message digest authentication enabled
  Message digest authentication enabled
  Message digest authentication enabled
R1#
```

Secure OSPF

Verifying OSPF MD5 Authentication (cont.)

Verify the Routing Table on R1

```
R1# show ip route ospf
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 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O        172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17, Serial0/0/0
O     192.168.1.0/24 [110/65] via 192.168.10.6, 00:30:43, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O        192.168.10.8/30 [110/128] via 192.168.10.6, 00:30:43, Serial0/0/1
                         [110/128] via 172.16.3.2, 00:33:17, Serial0/0/0
R1#
```

7.2 Troubleshooting Single-Area OSPF Implementations

Cisco | Networking Academy®
Mind Wide Open™

Components of Troubleshooting Single-Area OSPF

Forming OSPF Adjacencies

OSPF Adjacencies

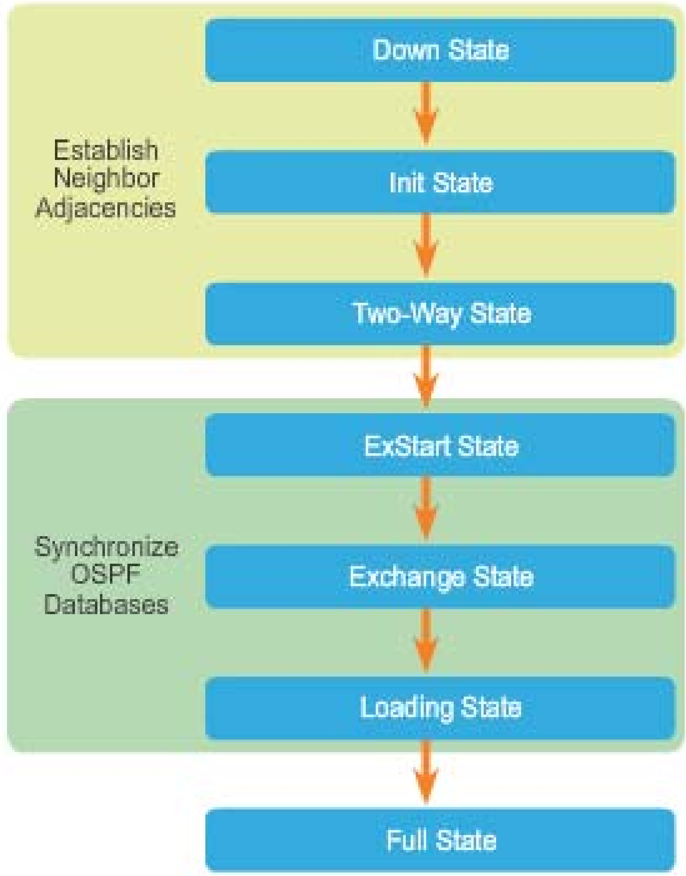
OSPF Adjacencies will not form if:

- The interfaces are not on the same network.
- OSPF network types do not match.
- OSPF Hello or Dead Timers do not match.
- Interface to neighbor is incorrectly configured as passive.
- There is a missing or incorrect OSPF network command.
- Authentication is misconfigured.

Components of Troubleshooting Single-Area OSPF

Transitioning via OSPF States

The router should not remain in any states other than FULL or 2Way for extended periods of time.

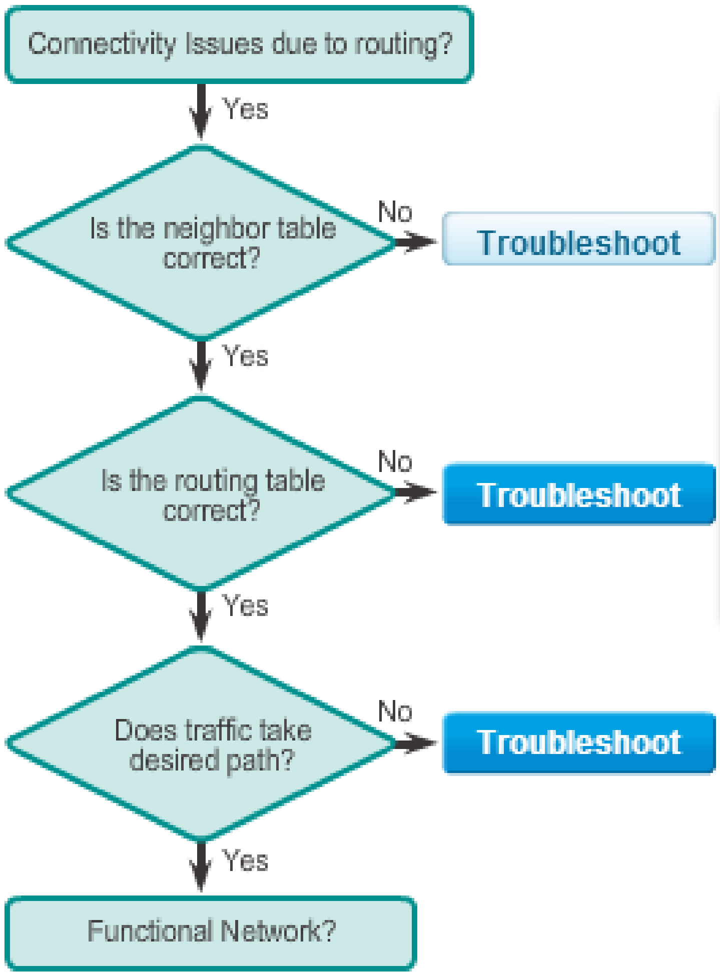


OSPF Troubleshooting Commands

- **`show ip protocols`** – Verifies vital OSPF configuration information.
- **`show ip ospf neighbor`** – Verifies that the router has formed an adjacency with its neighboring routers.
- **`show ip ospf interface`** – Displays the OSPF parameters configured on an interface, such as the OSPF process ID.
- **`show ip ospf`** – Examines the OSPF process ID and router ID.
- **`show ip route ospf`** – Displays only the OSPF learned routes in the routing table.
- **`clear ip ospf [process-id] process`** – Resets the OSPFv2 neighbor adjacencies.

Components of Troubleshooting Single-Area OSPF

Components of Troubleshooting OSPF



Troubleshoot

- Are the interfaces operational?
- Are the interfaces enabled for OSPF?
- Does the OSPF area match?
- Is there an interface that is configured as passive?

Show commands

```
show ip ospf neighbors
show ip interface brief
show ip ospf interface
```

Troubleshooting Neighbor Issues

- Verify active OSPF interfaces using the **`show ip ospf interface`** command.
- Verify the OSPF settings using the **`show ip protocols`** command.
- Disable the interface as passive using the **`no passive-interface`** command.
- Verify routes using the **`show ip route`** command.

```
Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:18,
Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
O       172.16.2.0/24 [110/65] via 172.16.3.2, 00:00:18,
        Serial0/0/0
O      192.168.1.0/24 [110/129] via 172.16.3.2, 00:00:18,
       Serial0/0/0
       192.168.10.0/30 is subnetted, 1 subnets
O         192.168.10.8 [110/128] via 172.16.3.2, 00:00:18,
          Serial0/0/0
```

Troubleshooting OSPF Routing Table Issues

- The **show ip protocols** command verifies networks that are advertised in OSPF.

```
R3# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
```

- For an interface to be enabled for OSPF, a matching **network** command must be configured under the OSPF routing process.

```
R3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# router ospf 10
R3(config-router)# network 192.168.1.0 0.0.0.255 area 0
R3(config-router)# end
```

- Use the **show ip route** command to verify routes in a routing table.
- Use the **show ip protocols** command to verify that a route is being advertised.

Troubleshoot Single-Area OSPFv3 Routing Issues

OSPFv3 Troubleshooting Commands

- **`show ipv6 protocols`** – Verifies vital OSPFv3 configuration information.
- **`show ipv6 ospf neighbor`** – Verifies that the router has formed an adjacency with its neighboring routers.
- **`show ipv6 ospf interface`** – Displays the OSPFv3 parameters configured on an interface.
- **`show ipv6 ospf`** – Examines the OSPFv3 process ID and router ID.
- **`show ipv6 route ospf`** – Displays only the OSPFv3 learned routes in the routing table.
- **`clear ipv6 ospf [`*`process-id`*`] process`** – Resets the OSPFv3 neighbor adjacencies.

Chapter 7: Summary

- OSPF defines five network types: point-to-point, broadcast multiaccess, NBMA, point-to-multipoint, and virtual links.
- The DR and BDR are elected to overcome challenges of flooding in an OSPF network.
- The routers in the network elect the router with the highest interface priority as DR. The router with the second highest interface priority is elected as the BDR.
- If all priorities are equal, the router with the highest ID is elected DR and the second highest ID becomes the BDR.
- To propagate a default route in OSPF, the ASBR must be configured with a default static route and the **default-information originate** command.
- Verify routes with the **`show ip route`** or **`show ipv6 route`** command.

Chapter 7: Summary (cont.)

- For OSPF to make a correct path determination, it may be necessary to adjust the default interface bandwidth.
- To adjust the reference bandwidth, use the auto-cost reference-bandwidth Mbps router configuration mode command.
- To adjust the interface bandwidth, use the bandwidth kilobits interface configuration mode command.
- The OSPF Hello and Dead intervals must match or a neighbor adjacency does not occur.
- OSPF supports three types of authentication: null, simple password authentication, and MD5 authentication.
- When troubleshooting OSPF neighbors, be aware that the FULL or 2WAY states are normal.

Chapter 7: Summary (cont.)

- Troubleshooting commands: **show ip protocols**, **show ip ospf neighbor**, **show ip ospf interface**, **show ip ospf**
- Troubleshooting OSPFv3 commands: **show ipv6 protocols**, **show ipv6 ospf neighbor**, **show ipv6 ospf interface**, **show ipv6 ospf**, **show ipv6 route ospf**, and **clear ipv6 ospf** [***process-id***] **process**

Cisco | Networking Academy®
Mind Wide Open™