Chapter 3
Router Concepts and Configuration

Outline

- Introduction
- Interconnected Networks
- Load Balancing
- Routing Protocols

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are the primary functions and features of a router?
- How do you connect devices for a small, routed network?
- How do you configure basic settings on a router to route between two directly connected networks, using CLI?
- How do you verify connectivity between two networks that are directly connected to a router?
- What is the encapsulation and de-encapsulation process used by routers when switching packets between interfaces?
- What is the path determination function of a router?

Objectives….

- What are the routing table entries for directly connected networks?
- How does a router build a routing table of directly connected networks?
- How does a router build a routing table using static routes?
- How does a router build a routing table using a dynamic routing protocol?

Introduction

- Networks allow people to communicate, collaborate, and interact in many ways.
- Networks are used to access web pages, talk using IP telephones, participate in video conferences, compete in interactive gaming, shop using the Internet, complete online coursework, and more.
- Ethernet switches function at the data link layer, Layer 2, and are used to forward Ethernet frames between devices within the same network.
- However, when the source and destination IP addresses are on different networks, the Ethernet frame must be sent to a router.
- A router connects one network to another network.

Introduction….

- The router uses its routing table to determine the best path to use to forward a packet.
- When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because a host device cannot communicate directly with devices outside of the local network.
- The default gateway is the intermediary device that routes traffic from the local network to devices on remote networks.
- It is often used to connect a local network to the Internet.
- Because the router can route packets between networks, devices on different networks can communicate.

Router initial configuration

- A router must be configured with specific settings before it can be deployed.
- New routers are not configured.
- They must be initially configured using the console port.

Characteristics of a Network

- **Topology**
  - There are physical and logical topologies.
- **physical topology**
  - Is the arrangement of the cables, network devices, and end systems.
  - It describes how the network devices are actually interconnected with wires and cables.
- **logical topology**
  - Is the path over which the data is transferred in a network.
  - It describes how the network devices appear connected to network users.

Characteristics of a Network

Speed

- Is a measure of the data rate in bits per second (b/s) of a given link in the network.

Cost

- Indicates the general expense for purchasing of network
- components, and installation and maintenance of the network.

Security

- Indicates how protected the network is, including the information that is transmitted over the network.
- The subject of security is important, and techniques and practices are constantly evolving.
- Consider security whenever actions are taken that affect the network.

Characteristics of a Network….

Availability

- Is the likelihood that the network is available for use when it is required.

Scalability

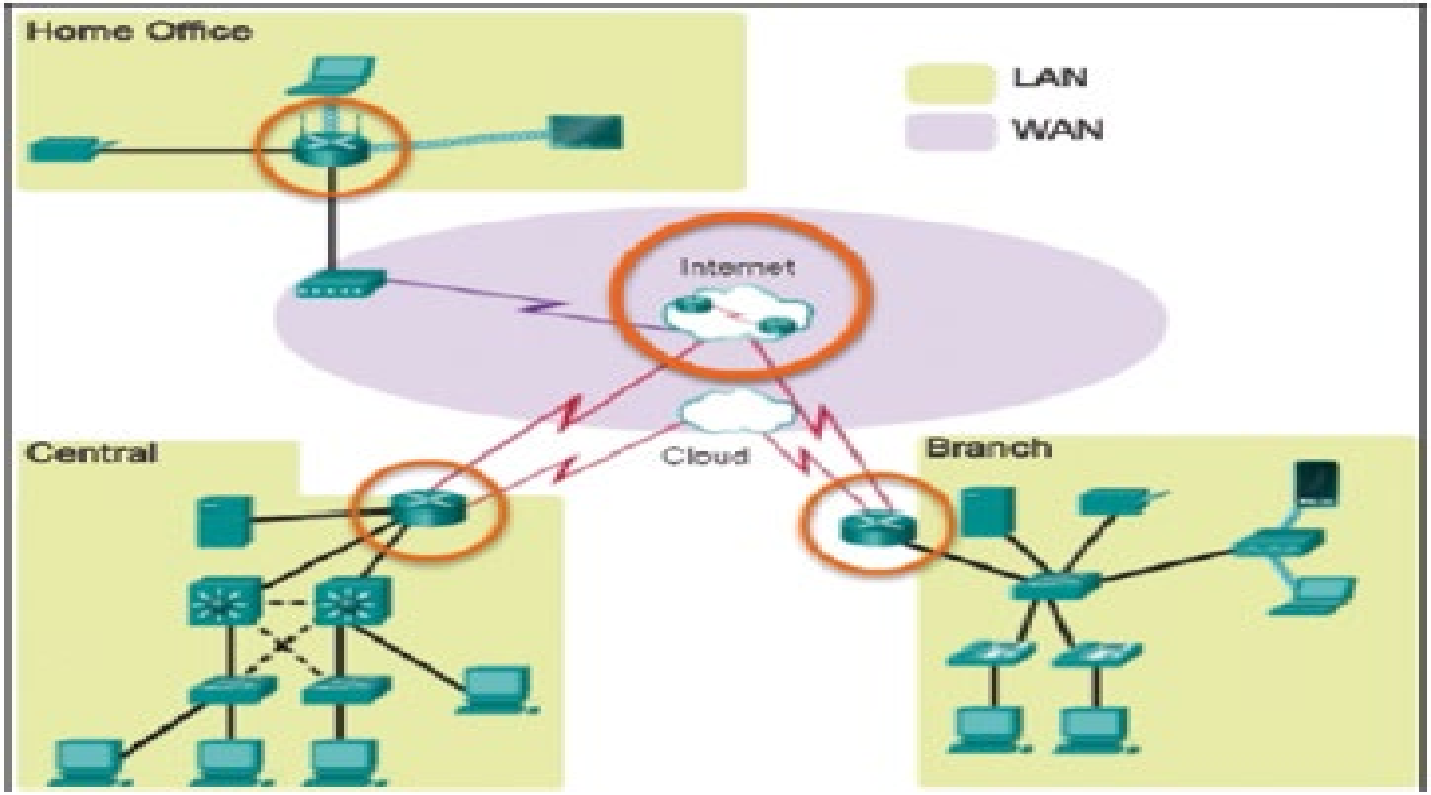
- Indicates how easily the network can accommodate more users and data transmission requirements.
- If a network design is optimized to only meet current requirements, it can be very difficult and expensive to meet new needs when the network grows.

Reliability

- Indicates the dependability of the components that make up the network, such as the routers, switches, PCs, and servers.
- Reliability is often measured as a probability of failure or as the ***mean time between failures (MTBF)***.

Why Routing?

- Communication between networks would not be possible without a router determining the best path to the destination and forwarding traffic to the next router along that path.
- Router is responsible for the routing of traffic between networks.



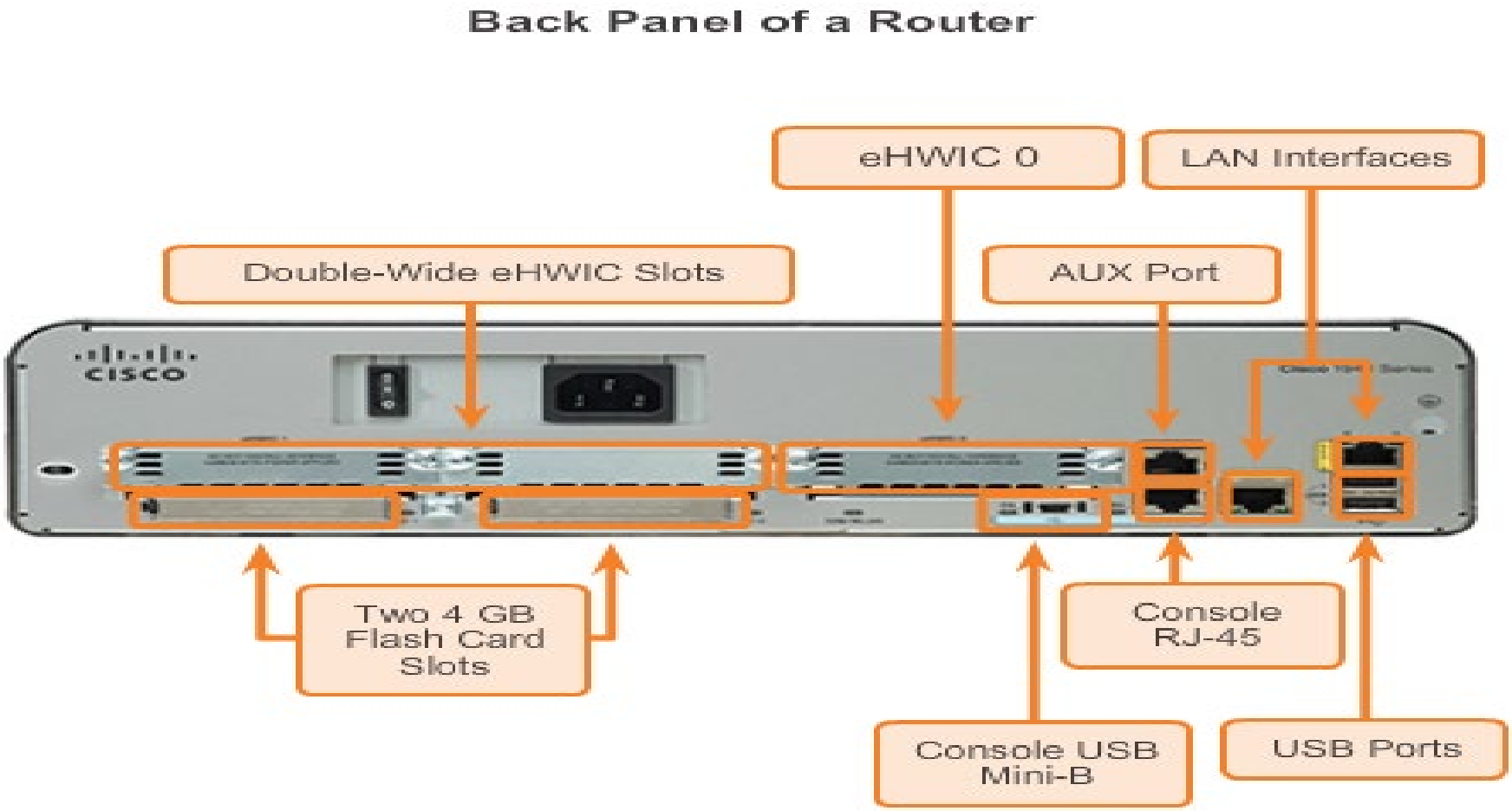
Routers are Computers

- Routers are specialized computers containing the following required components to operate:
  - CPU
  - OS - Routers use Cisco IOS
  - Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)
- Routers utilize the following memory:

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system files

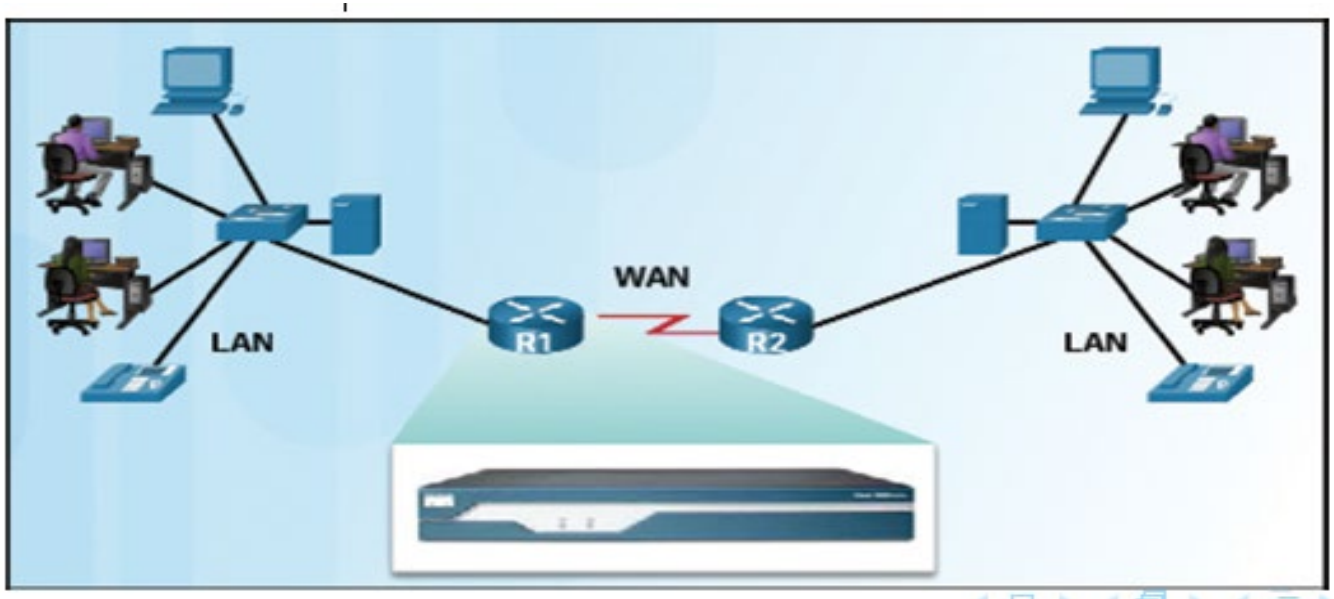
Routers are Computers…

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



Routers Interconnect Networks

- Routers can connect multiple networks.
  - Routers have multiple interfaces that each belong to a different IP network.
- Each network that a router connects to typically requires a separate interface.
- These interfaces are used to connect a combination of both LANs and WANs.



Routers Choose Best Paths

- Determine the best path to send packets.
  - Uses its routing table to determine path.
- Forward packets toward their destination.
  - Forwards packet to interface indicated in routing table.
- Encapsulates the packet and forwards out toward destination.
- Routers use **static routes** and **dynamic routing** protocols to learn about remote networks and build their routing tables.
  - **Static Routing**
    - routes are described by fixed paths through a data network.
    - the routes are entered by system administrator.
  - **Dynamic Routing**
    - Protocols and algorithms are used to automatically propagate routing information.
    - Routers will communicate the adjacent routers which informs the network to which each router is connected.
    - These routers adjusts automatically in a network when traffic changes.

Packet Forwarding Methods

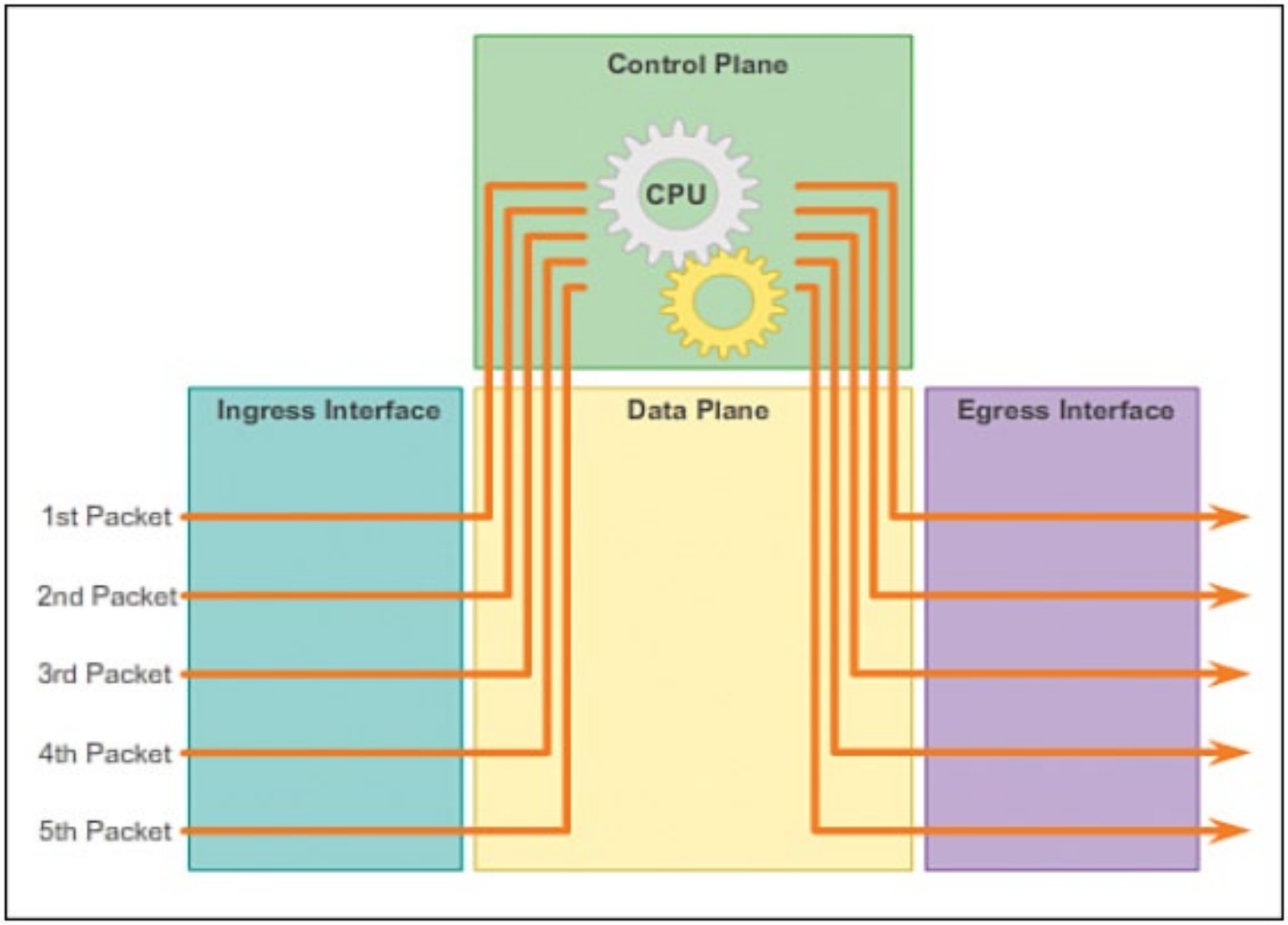
Routers support three packet-forwarding mechanisms:

1. Process Switching

- An older packet forwarding mechanism still available for Cisco routers.
- When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then it determines the exit interface and forwards the packet.
- It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets.
- Is slow and rarely implemented in modern networks.

Packet Forwarding Methods

Process Switching



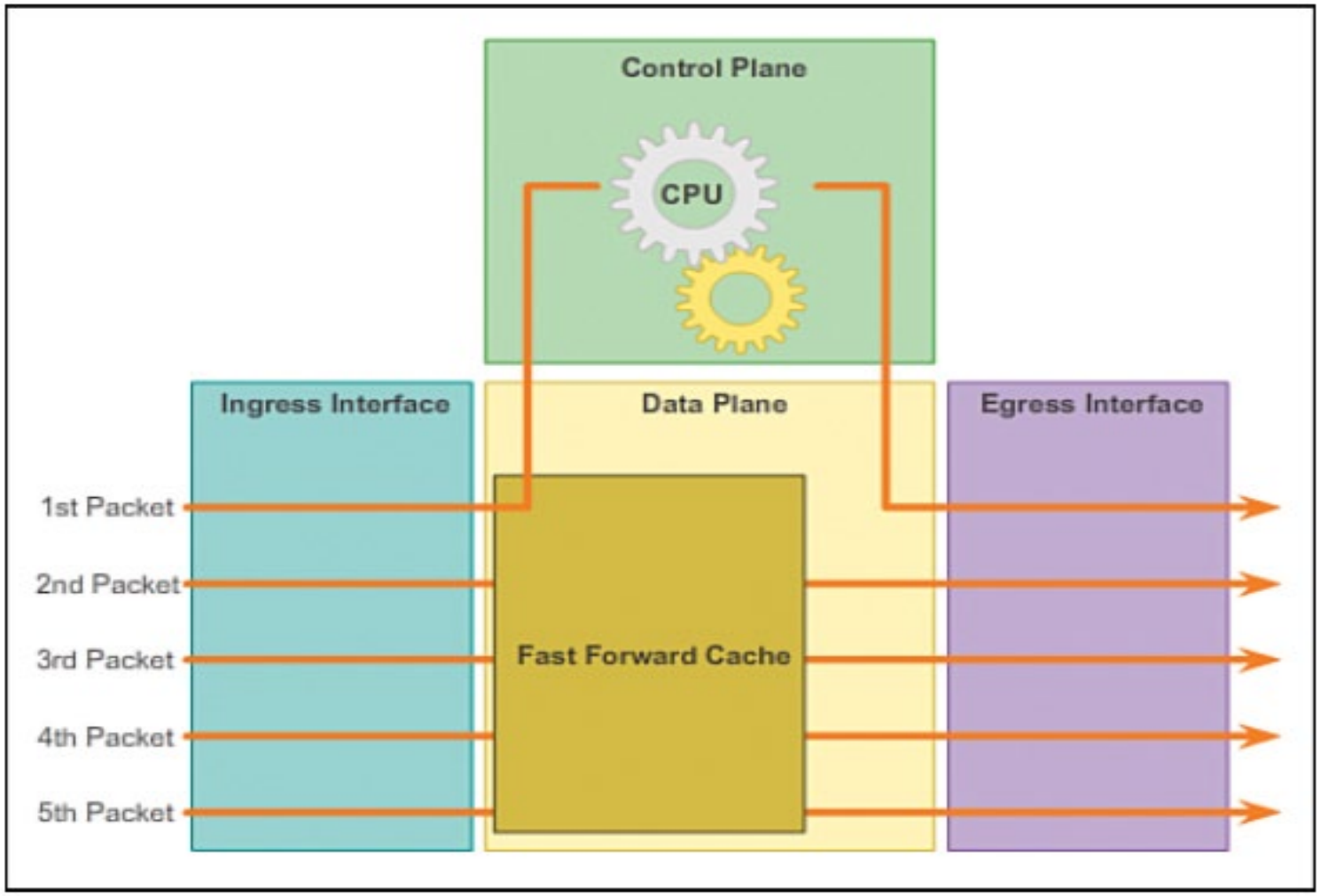
Packet Forwarding Methods…

2. Fast Switching

- A common packet forwarding mechanism that uses a fast-switching cache to store next hop information.
- When a packet arrives on an interface, it is forwarded to the control plane, where the CPU searches for a match in the fast-switching cache.
- If it is not there, it is process-switched and forwarded to the exit interface.
- The flow information for the packet is also stored in the fast-switching cache.
- If another packet going to the same destination arrives on an interface, the next-hop information in the cache is reused without CPU intervention.

Packet Forwarding Methods

Fast Switching



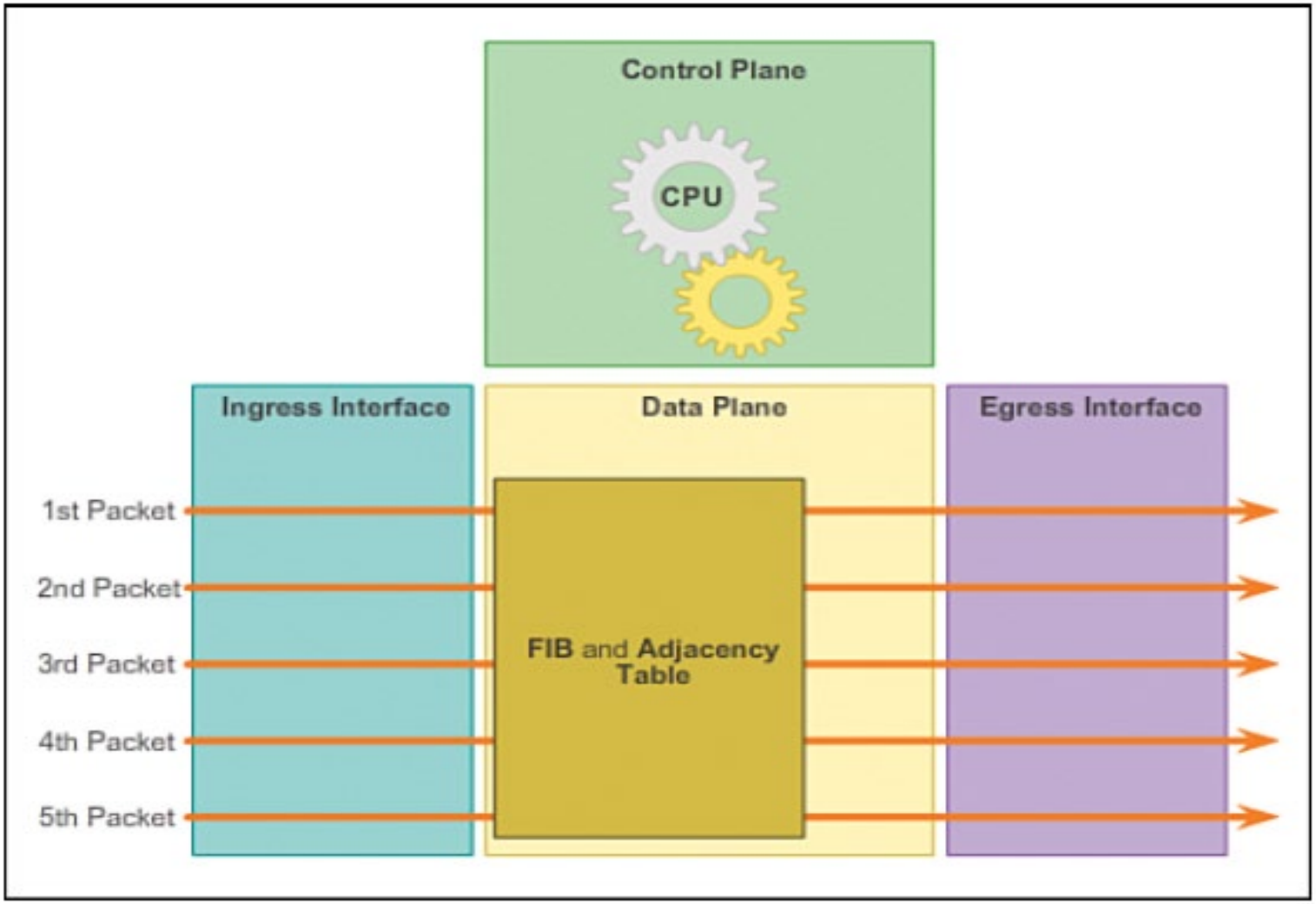
Packet Forwarding Methods…

3. Cisco Express Forwarding (CEF)

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

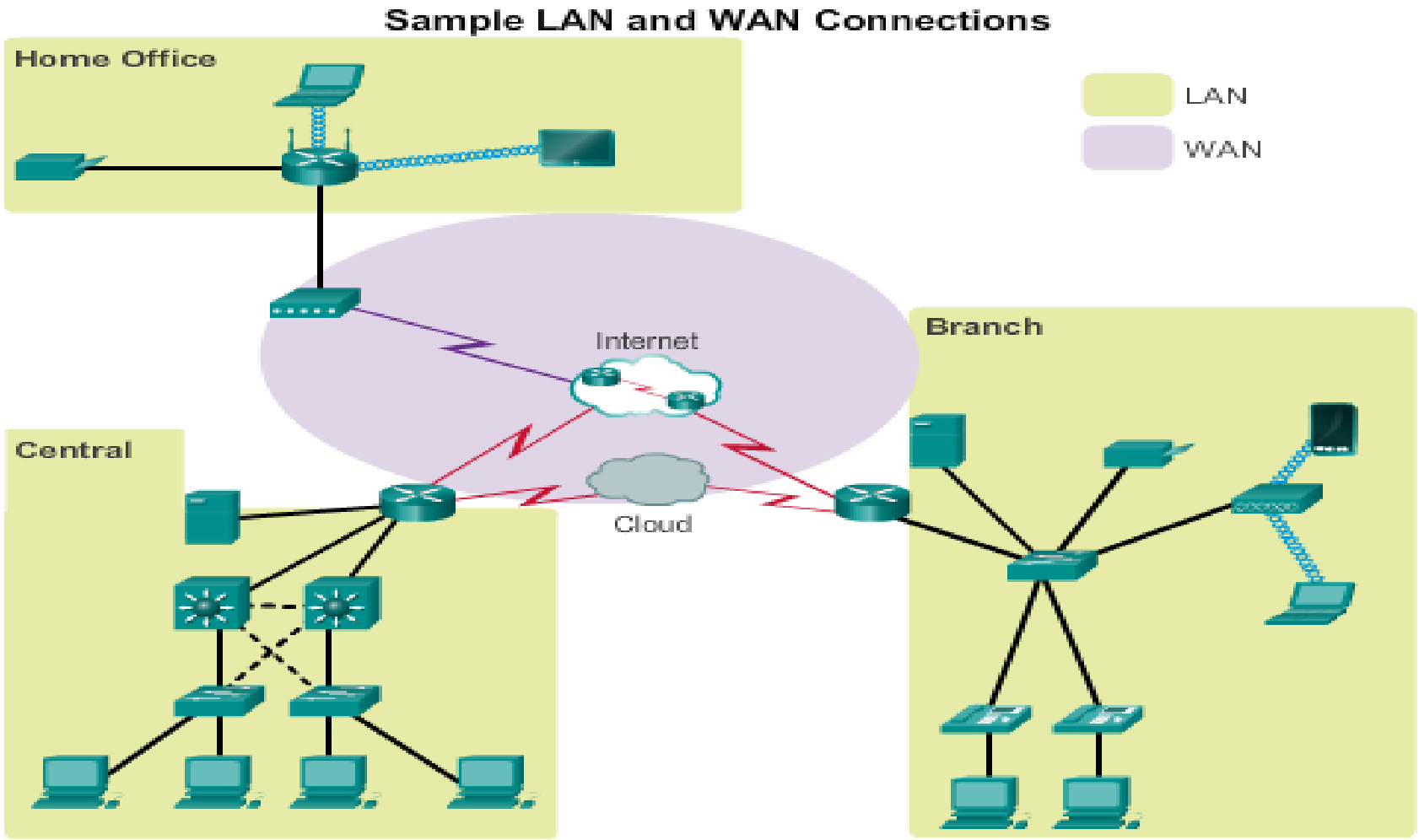
Packet Forwarding Methods

Cisco Express Forwarding



Connect to a Network

Network devices and end users typically connect to a network using a wired Ethernet or wireless connection.

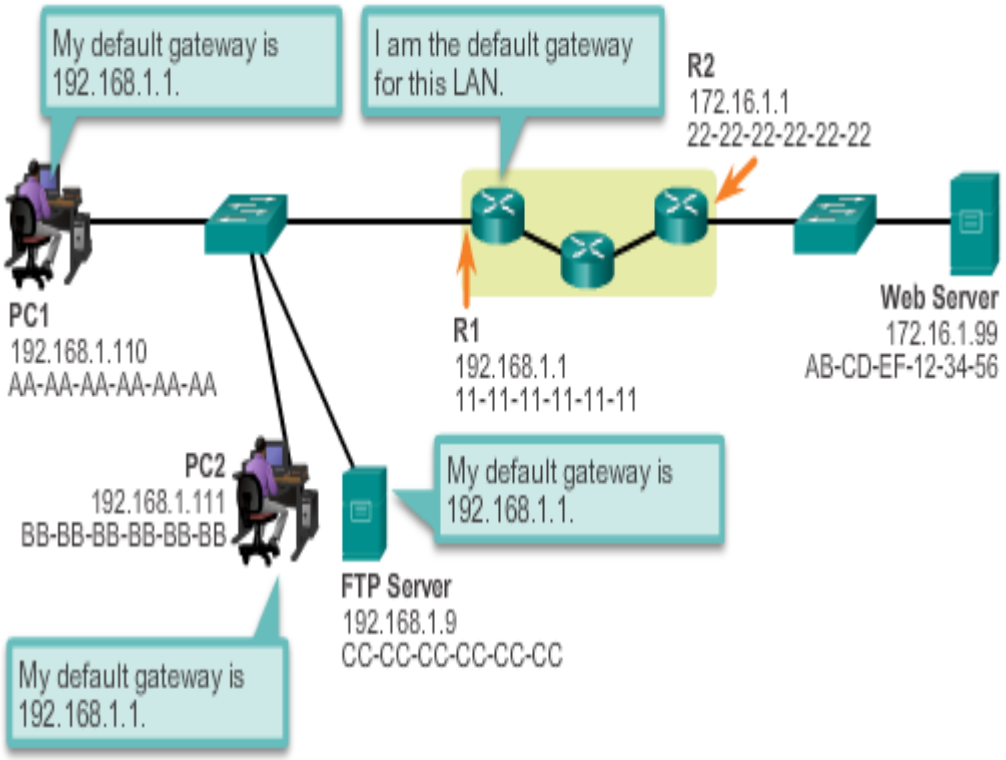


Default Gateways

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 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	

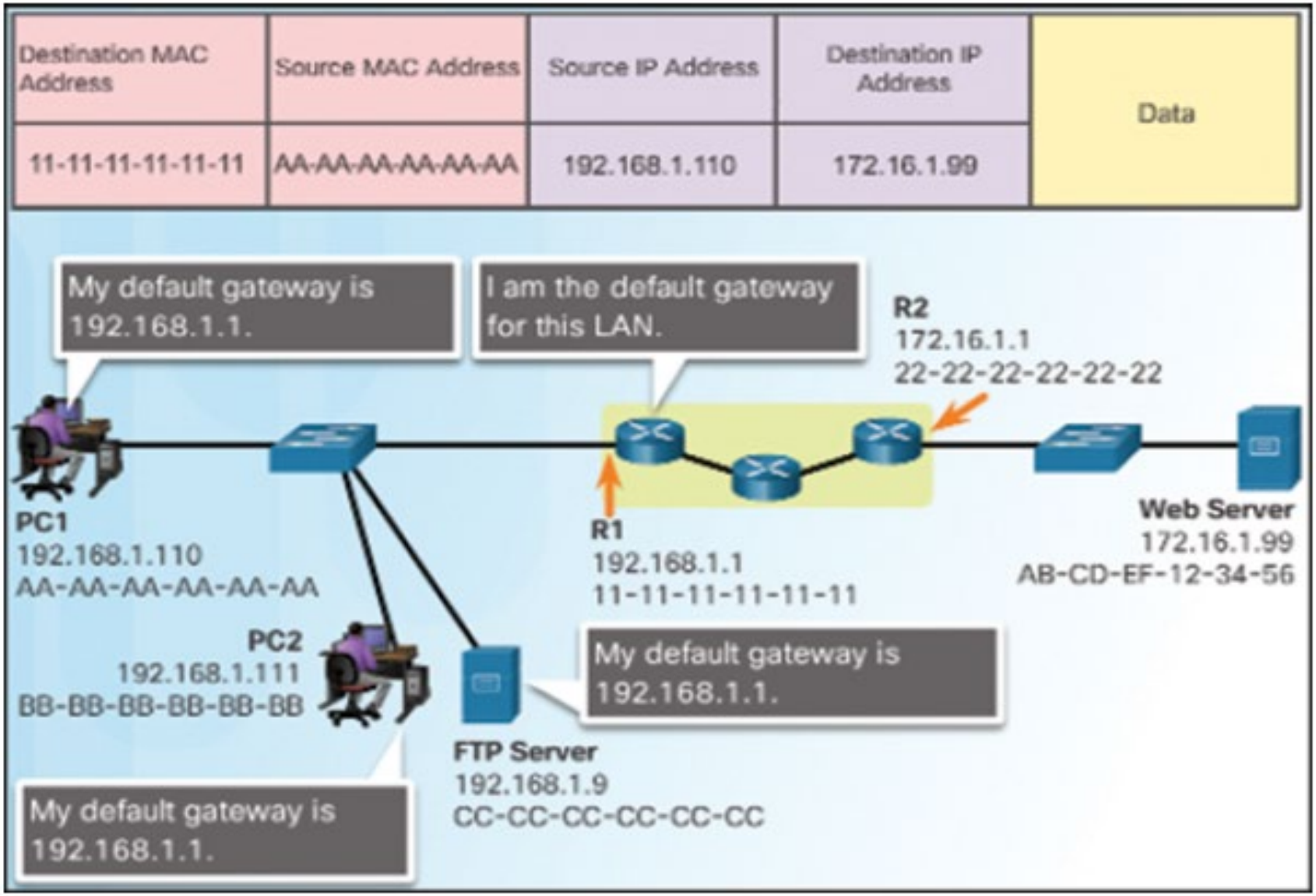


Default Gateways…

- When a host sends a packet to a device that is on the same IP network
  - the packet is simply forwarded out of the host interface to the destination device.
- When a host sends a packet to a device on a different IP network
  - the packet is forwarded to the default gateway because a host device cannot communicate directly with devices outside of the local network.
- Default gateway is usually the address of the interface on the router connected to the local network.

Note: A router is usually configured with its own default gateway known as **Gateway of Last Resort**.

Default Gateways…



Document Network Addressing

- When designing a new network or mapping an existing network, **document the network.**
- Network Documentation should include at least the following in a topology diagram and addressing table:
  - Device names
  - Interfaces used in the design
  - IP addresses and subnet masks
  - Default gateway addresses

- This information is captured by creating two useful network documents:

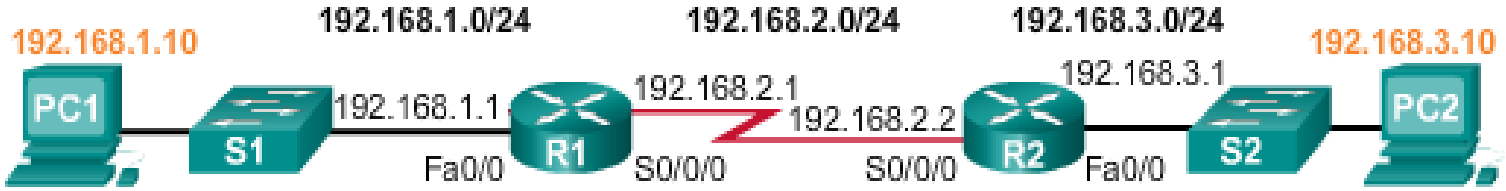
1. Topology diagram

- provides a visual reference that indicates the physical connectivity and logical Layer 3 addressing.
- Often created using diagramming software, such as Microsoft Visio.

Document Network Addressing…

2. An addressing table

- Is used to capture device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses,



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

Device LEDs

- Host computers connect to a wired network using a network interface and RJ-45 Ethernet cable.
- Most network interfaces have one or two LED link indicators next to the interface.

#	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

Configure Basic Router Settings

- Every network has unique settings that must be configured on a router.
- Cisco routers and Cisco switches are a lot alike.
- They support a similar modal operating system, similar command structures, and many of the same commands.
- In addition, both devices have similar initial configuration steps.
- Basics tasks that should be first configured on a Cisco Router and Cisco Switch:
  - **Name the device**
    - Distinguishes it from other routers.
  - **Secure management access**
    - Secures privileged EXEC, user EXEC, and Telnet access, and encrypts passwords to their highest level.
  - **Configure a banner**
    - Provides legal notification of unauthorized access.

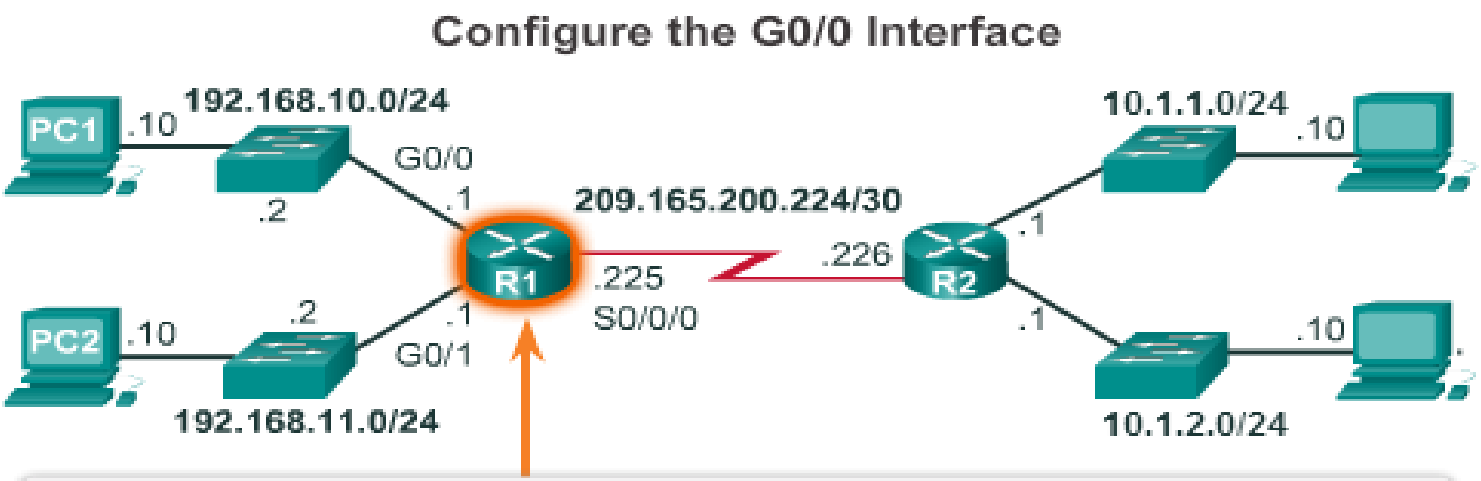
Configure Basic Router Settings…

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

Configure Router Interfaces

- To be available a router interface must be:
- **Configured with an address and subnet mask .**
- **Activated –** by default LAN and WAN interfaces are not activated. Must be activated using no shutdown command.
- Other parameters - serial cable end labeled DCE must be configured with the **clock rate** command.
- Optional description can be included.

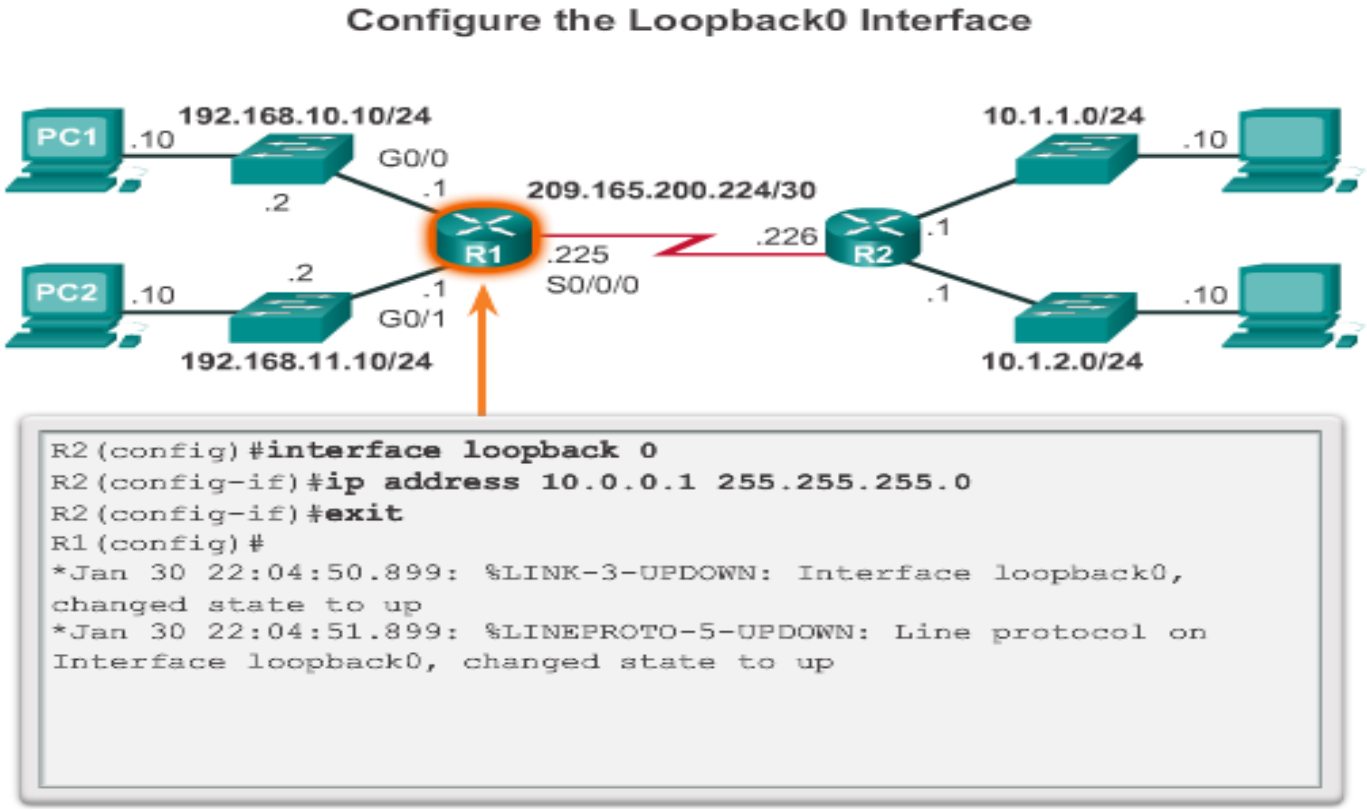
Configure Router Interfaces…




```
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 a Loopback Interface

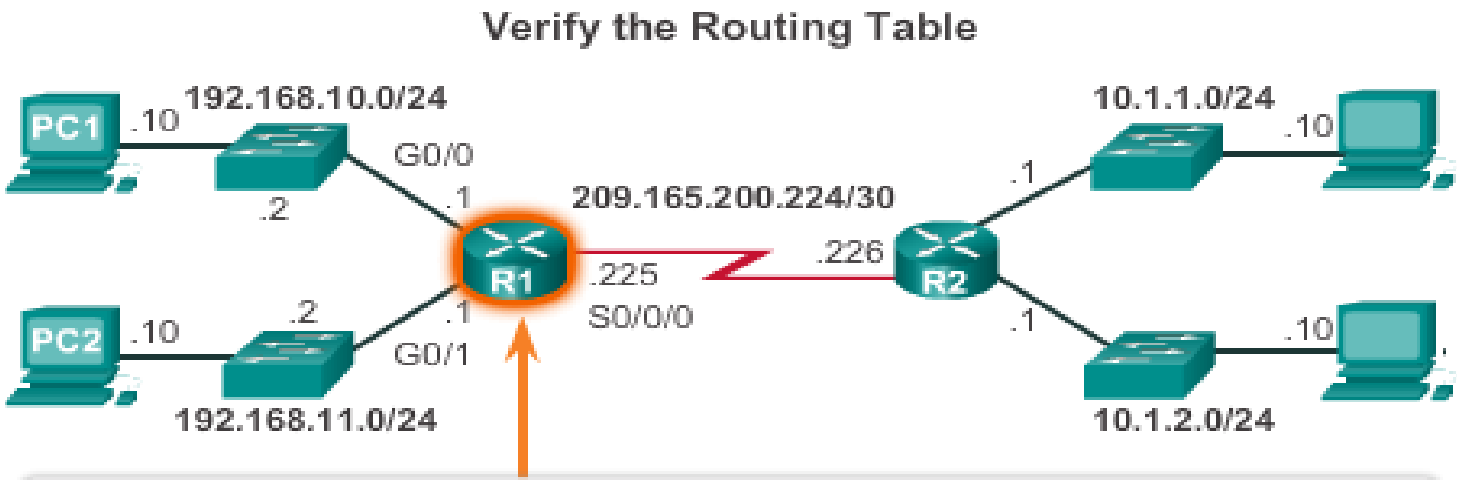
- Loopback interface is a logical interface internal to the router.
- It is not assigned to a physical port, it is considered a software interface that is automatically in an UP state.
- Useful for testing and important in the OSPF routing process.



Verify Interface Settings

- It is always important to know how to troubleshoot and verify whether a device is configured correctly.
- There are several **privileged EXEC mode *show*** commands that can be used to verify the operation and configuration of an interface.
  - **show ip interfaces brief**
    - *Displays a summary for all interfaces.*
  - **show ip route**
    - *Displays the contents of the IPv4 routing table stored in RAM.*
  - **show running-config interface**
    - *Displays the commands configured on the specified interface.*
  - **show** commands to gather more detailed interface information.
    - **show interfaces**
    - **show ip interfaces**

Verify Interface Settings…

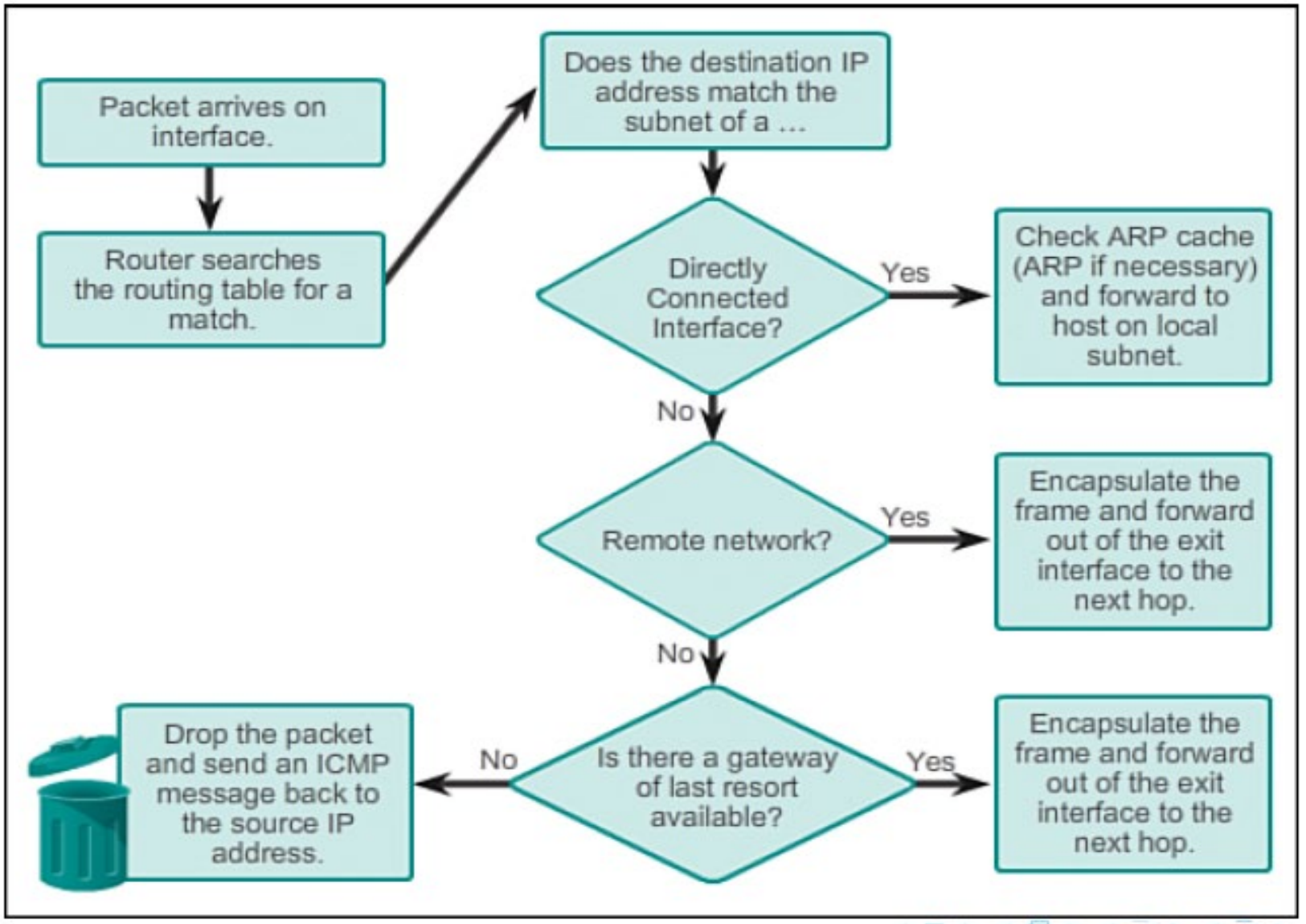



```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mo

<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
```

Routing Decisions

- A primary function of a router is to **determine the best path** to use to send packets.
- To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet.
- Search results in one of three **path determinations**:
  - **Directly connected network**
  - **Remote network**
  - **No route determined**

Routing Decisions…

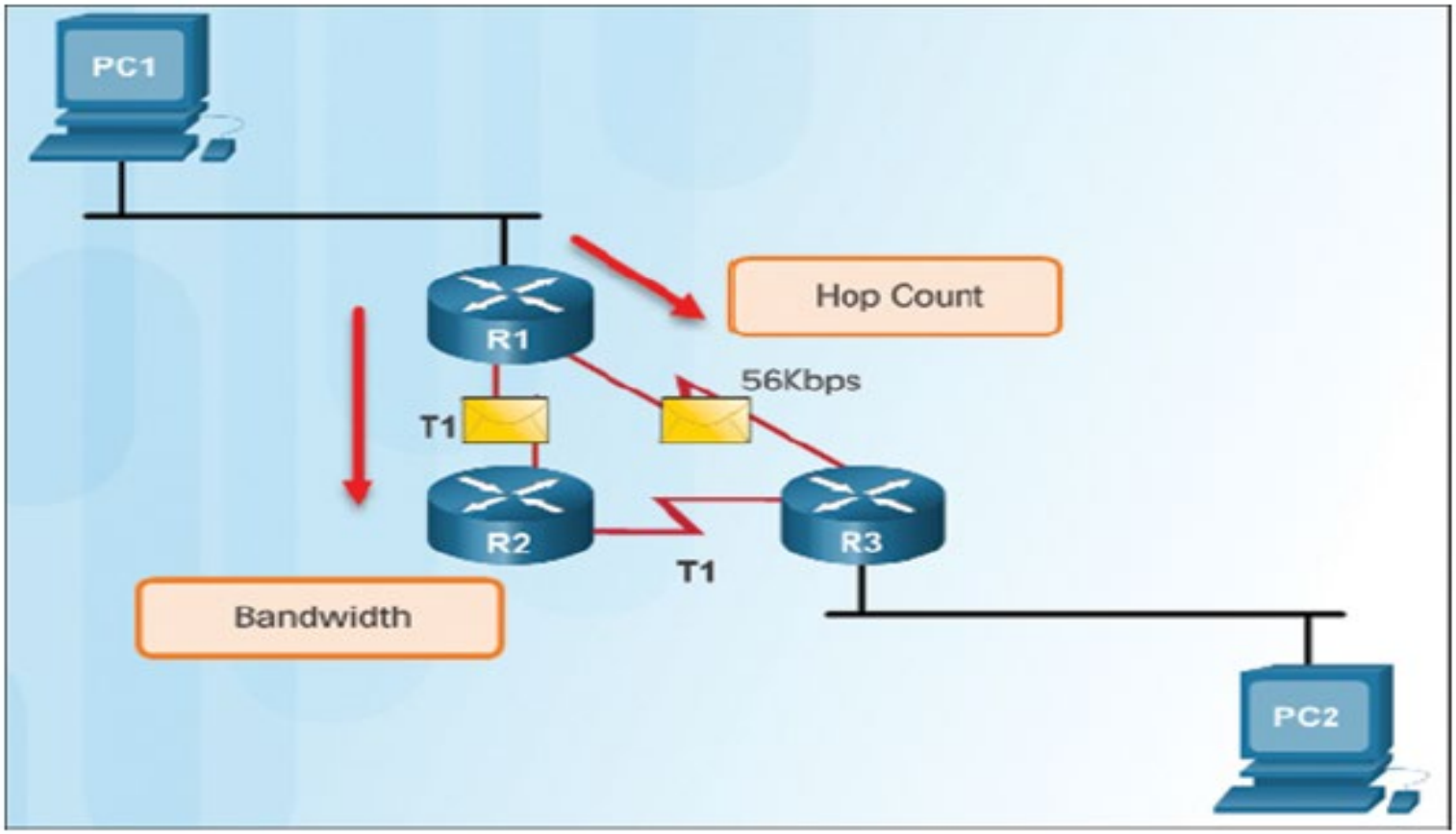


Best Path

- 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 for example:
  - **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

Best Path…

Path depending on the metric

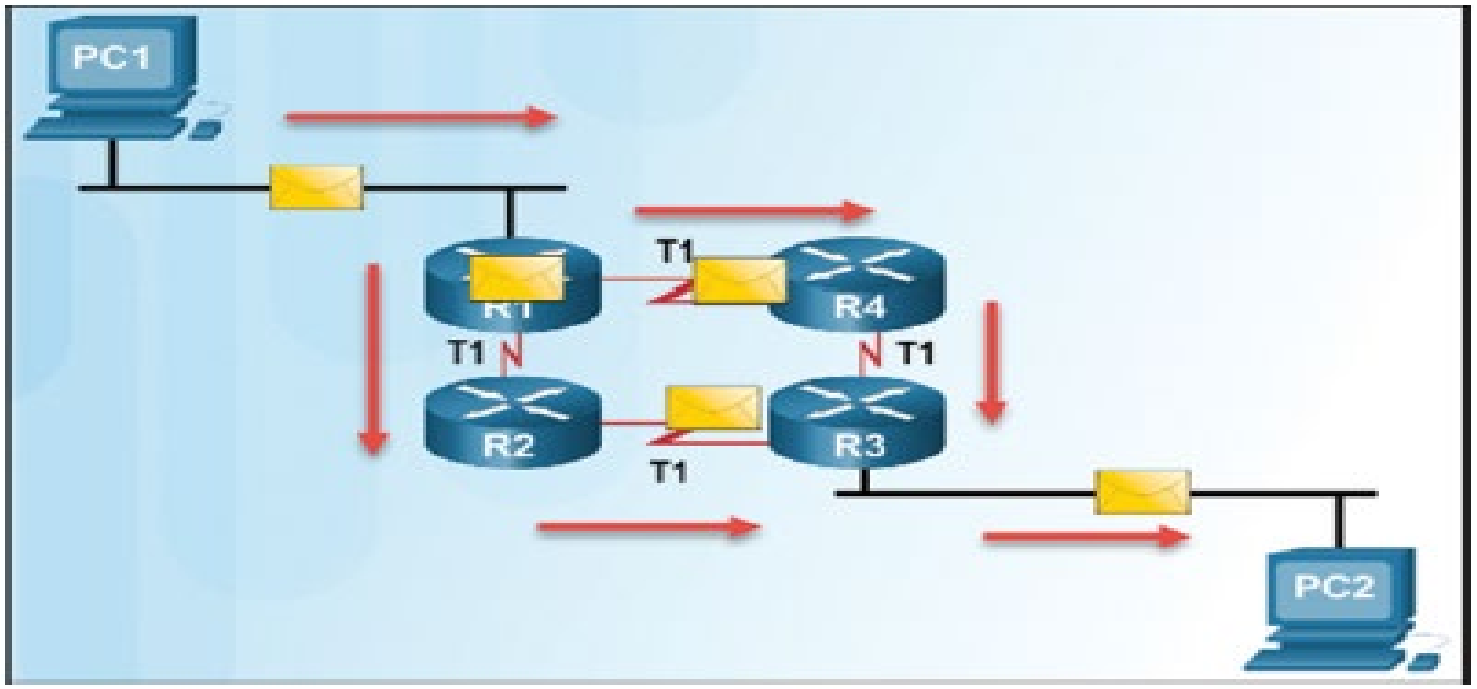


Paths with identical metrics???

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.
- This is called equal cost load balancing.
- Increase the effectiveness and performance of the network.

equal cost load balancing



Administrative Distance

- A router can be configured with multiple routing protocols (RIP, OSPF, EIGRP,…)
- The routing table may have more than one route source for the same destination network
- Each routing protocol may decide on a different path to reach the destination based on the metrics of that routing protocol
- How does the router know which route to use?
- Cisco IOS uses what is known as the AD to determine the route to install into the IP routing table

Administrative Distance

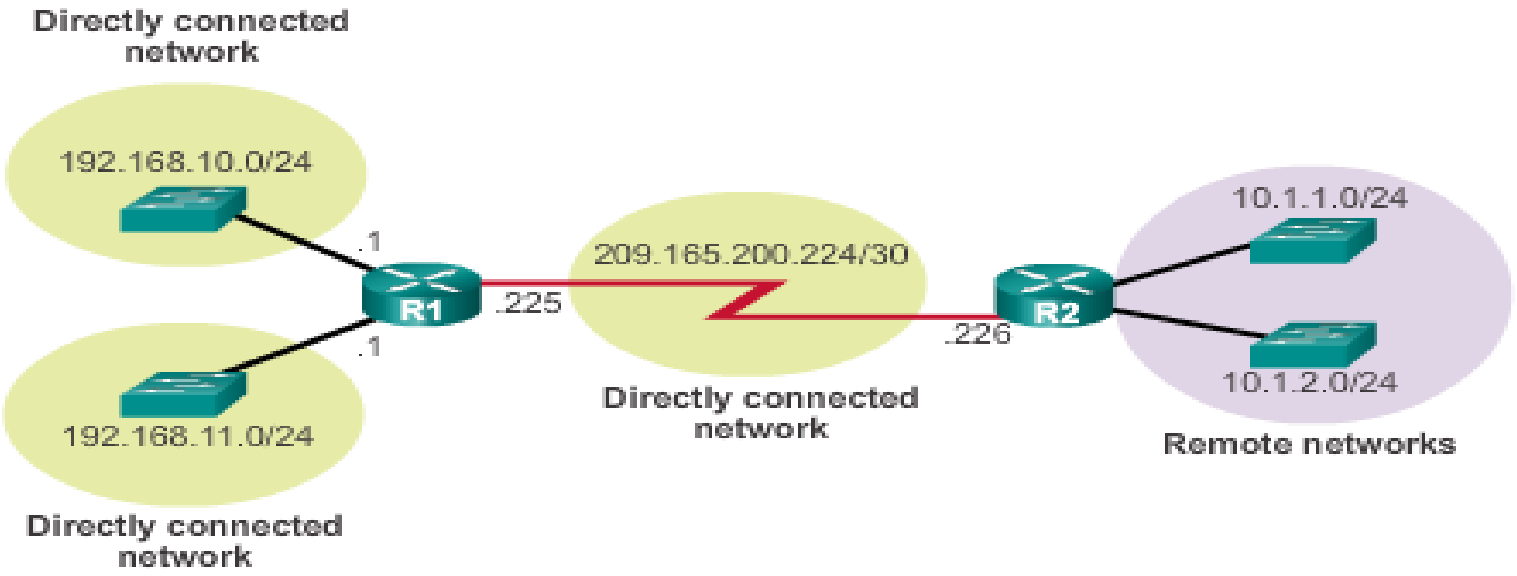
- Administrative Distance (AD) represents the "trustworthiness" of the route source
- The Lower the AD the more trustworthy the route.

Default Administrative Distances

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

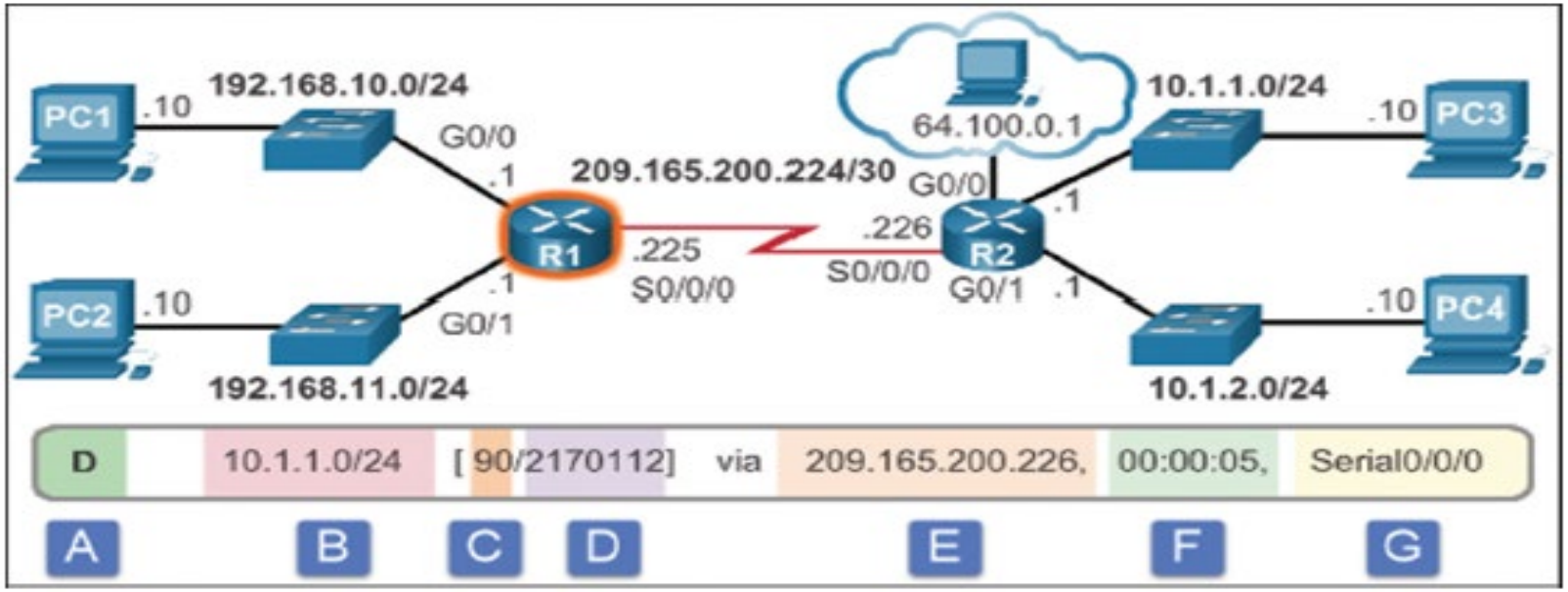
The Routing Table

- Is at the heart of making routing decisions
- Is a file stored in RAM that contains information about
  - Directly Connected Routes
  - Remote Routes
  - Network or Next hop Associations



Remote Network Routing Entry Identifiers

- The figure below displays an IPv4 routing table entry on R1 for the route to remote network 10.1.1.0



The entry identifies the following information:

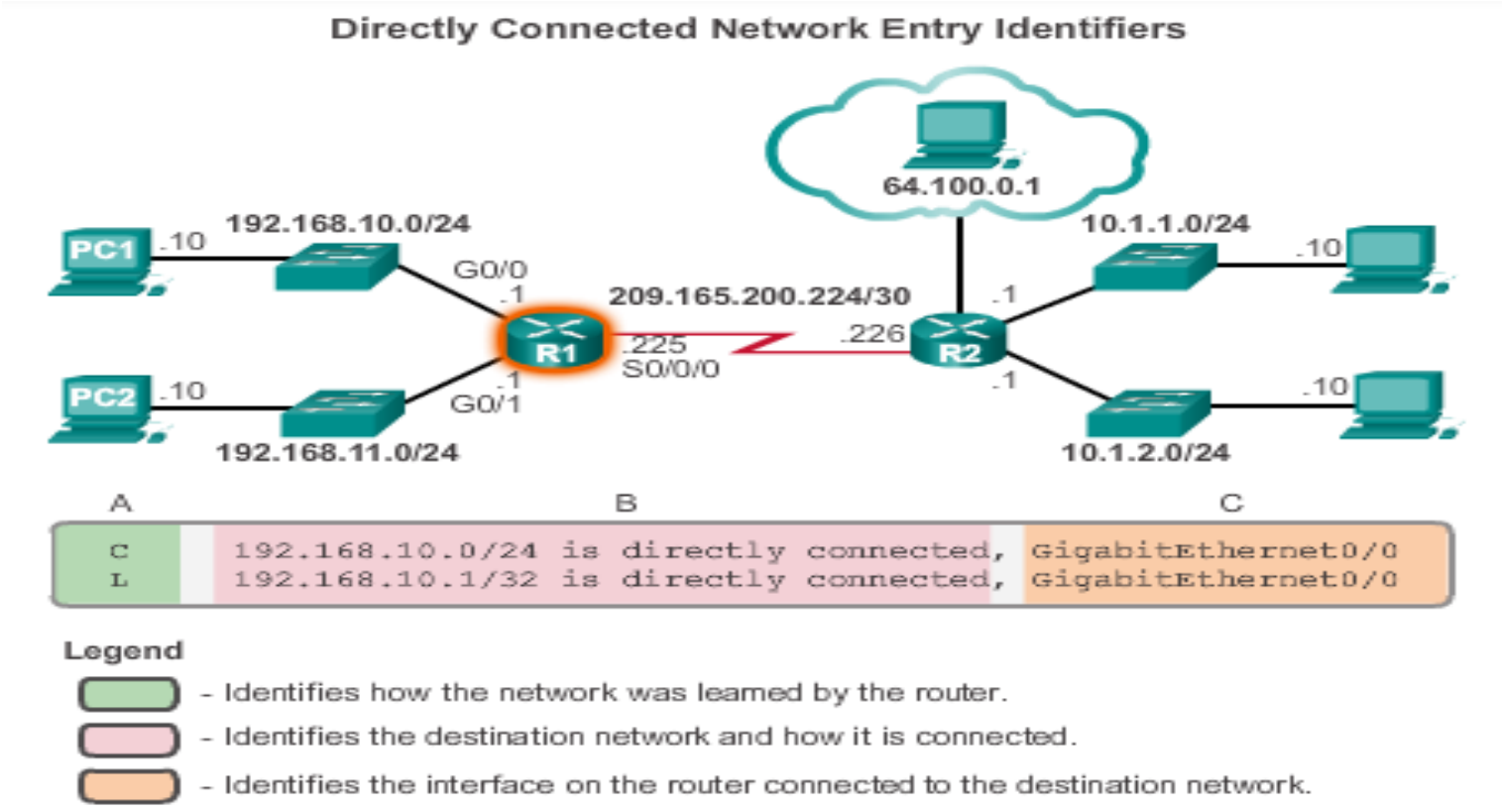
- **Route source (A)**
  - Identifies how the route was learned.
- **Destination network (B)**
  - Identifies the address of the remote network.

Remote Network Routing Entry Identifiers

- **Administrative distance** (**C**)
  - Identifies the trustworthiness of the route source.
  - Lower values indicate preferred route source.
- **Metric** (**D**)
  - Identifies the value assigned to reach the remote network.
  - Lower values indicate preferred routes.
- **Next-hop** (**E**)
  - Identifies the IPv4 address of the next router to forward the packet to.
- **Route timestamp** (**F**)
  - Identifies how much time has passed since the route was learned.
- **Outgoing interface** (**G**)
  - Identifies the exit interface to use to forward a packet toward the final destination.

Directly Connected Routes

- A newly deployed router, without any configured interfaces, has an empty routing table.
- An active, configured directly connected interface creates two routing table entries Link Local (L) and Directly Connected (C)



Directly Connected Routes…

- The routing table entry for directly connected interface is simpler than the entries for remote networks

Directly Connected Network Entry Identifiers

- **Route Source (A)**
  - Identifies how the network was learned by the router.
  - Directly connected interfaces have two route source codes.
    - 'C' identifies a directly connected network.
    - 'L' identifies the IPv4 address assigned to the router's interface.
- **Destination Network (B)**
  - Identifies the destination network and how it is connected.
- **Outgoing Interface (C)**
  - Identifies the exit interface to use when forwarding packets to the destination network.

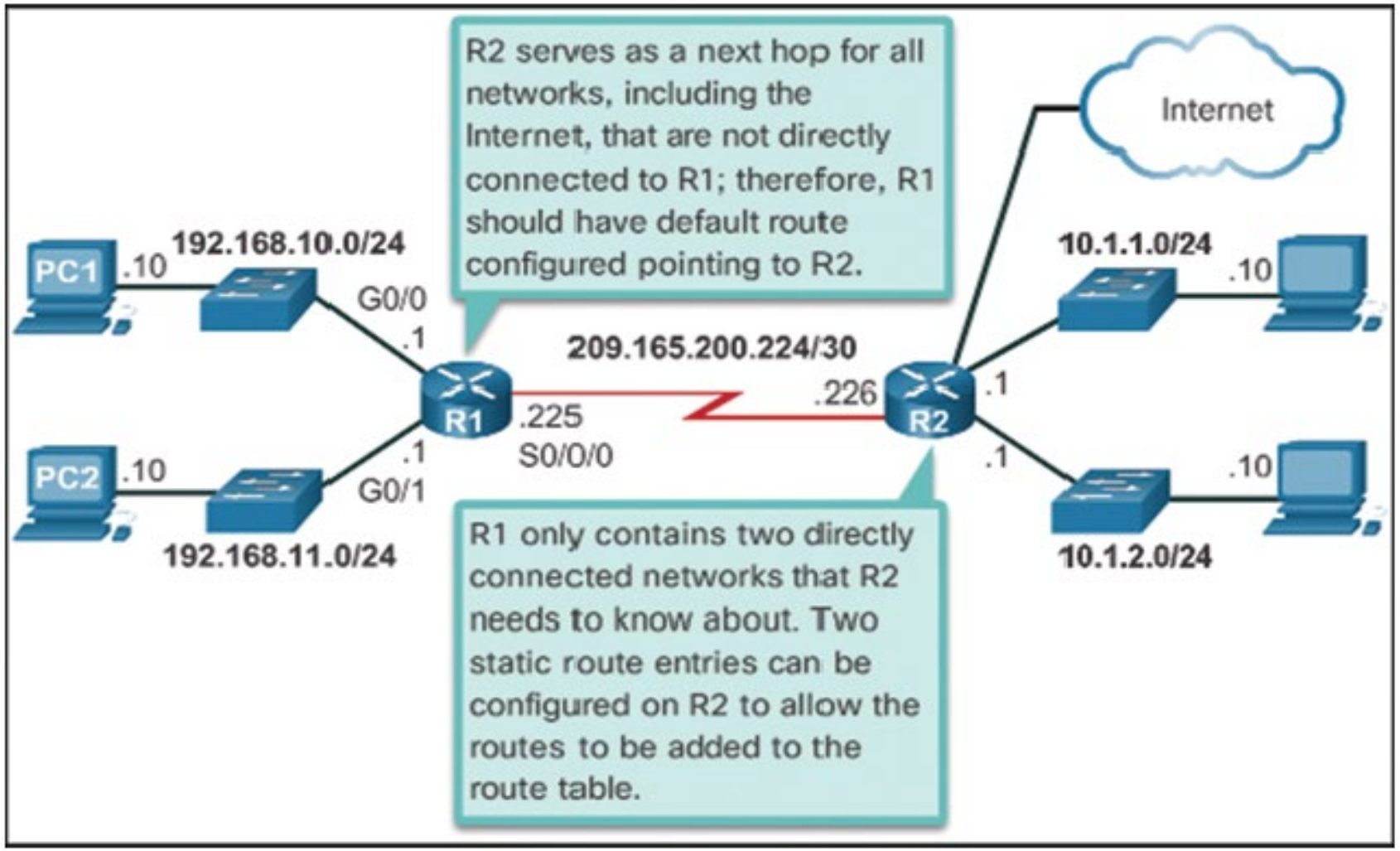
Statically Learned Routes

Static Routes

- After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented.
- Manually configured.
- Define an explicit path between two networking devices.
- Must be manually updated if the topology changes.
- Benefits include improved security and control of resources.
- Two common types of static routes in the routing table:
  - Static route to a specific network
    - **ip route** network-mask next-hop-ip | exit-intf
  - Default static route
    - used when the routing table does not contain a path for a destination network.
    - **ip route** 0.0.0.0 0.0.0.0 exit-intf | next-hop-ip

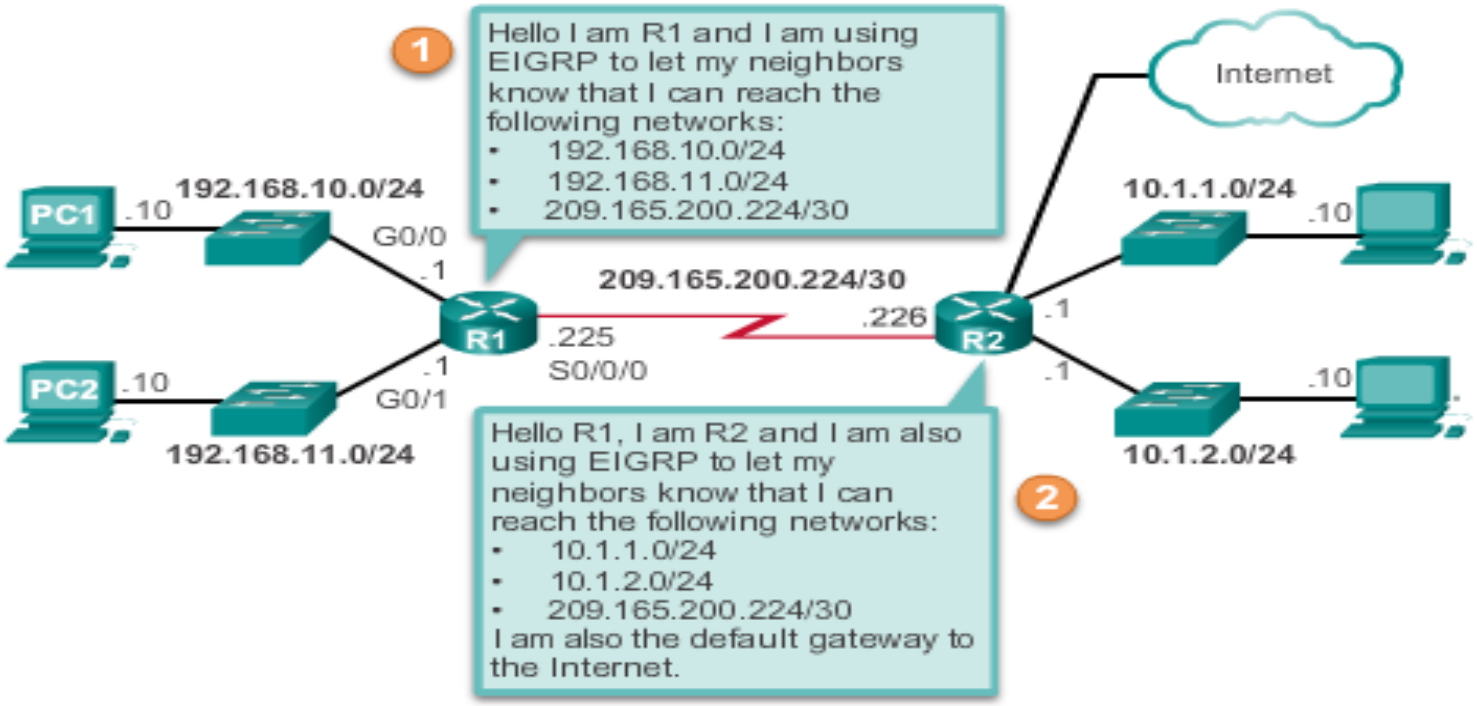
Statically Learned Routes

Static and Default Route



Dynamic Routing Protocols

- Used by routers to share information about the reachability and status of remote networks.
- Performs network discovery and maintaining routing tables.



Dynamic Routing Protocols

IPv4 Routing Protocols

- Cisco ISR 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

IPv6 Routing protocols

- Cisco ISR routers can support a variety of dynamic IPv6 routing protocols including:
  - RIPng (RIP next generation)
  - **OSPF v3**
  - EIGRP for IPv6
  - MP-BGP4 (Multicast Protocol-Border Gateway Protocol)

Why Use Static Routing?

Static routing provides some advantages over dynamic routing, including:

- Easy to implement in a small network.
- 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.
- No routing algorithm or update mechanisms are required.
  - Therefore, extra resources (CPU and memory) are not required.

Why Use Static Routing…

Static routing has the following disadvantages:

- Initial configuration and maintenance is time-consuming.
- Configuration is error-prone, especially in large networks.
- Administrator intervention is required to maintain changing route information.
- If a link fails, a static route cannot reroute traffic.
  - Therefore, manual intervention is required to re-route traffic.
- Does not scale well with growing networks; maintenance becomes cumbersome.
- Requires complete knowledge of the whole network for proper implementation.

When to Use Static Routes

Static routing has three primary uses:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from stub networks.
  - A stub network is a network accessed by a single route, and the router has no other neighbors.
- Accessing 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.

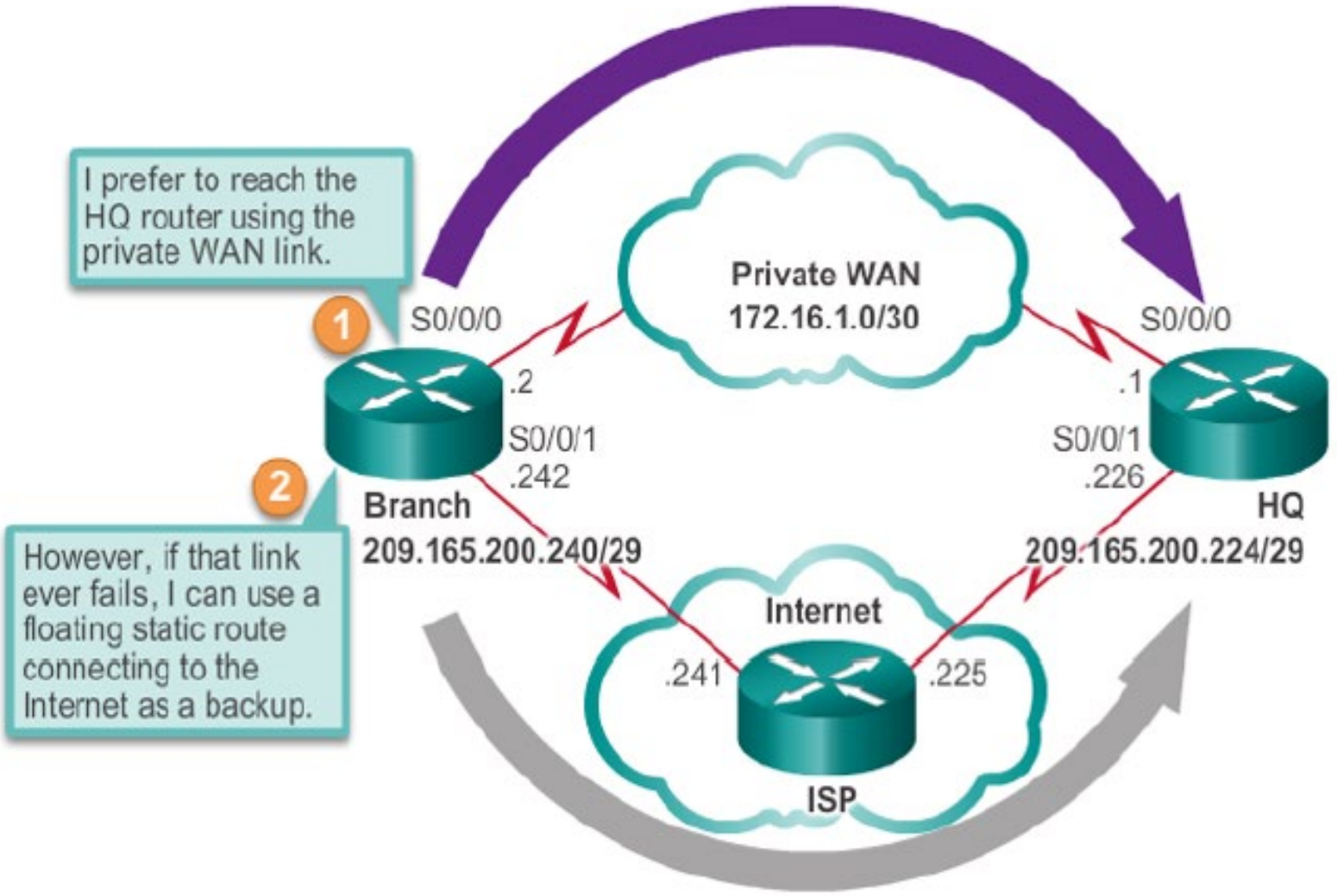
Static Route Applications

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

Standard Static Route

Configuring a Backup 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.

Floating Static Route

- Floating static routes are static routes that are used to provide a backup path to a primary static or dynamic route, in the event of a link failure.
- The floating static route is only used when the primary route is not available.
- In order to accomplish this, the floating static route is configured with higher administrative distance than the primary route.

Static Routes

IP route command syntax

```
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.

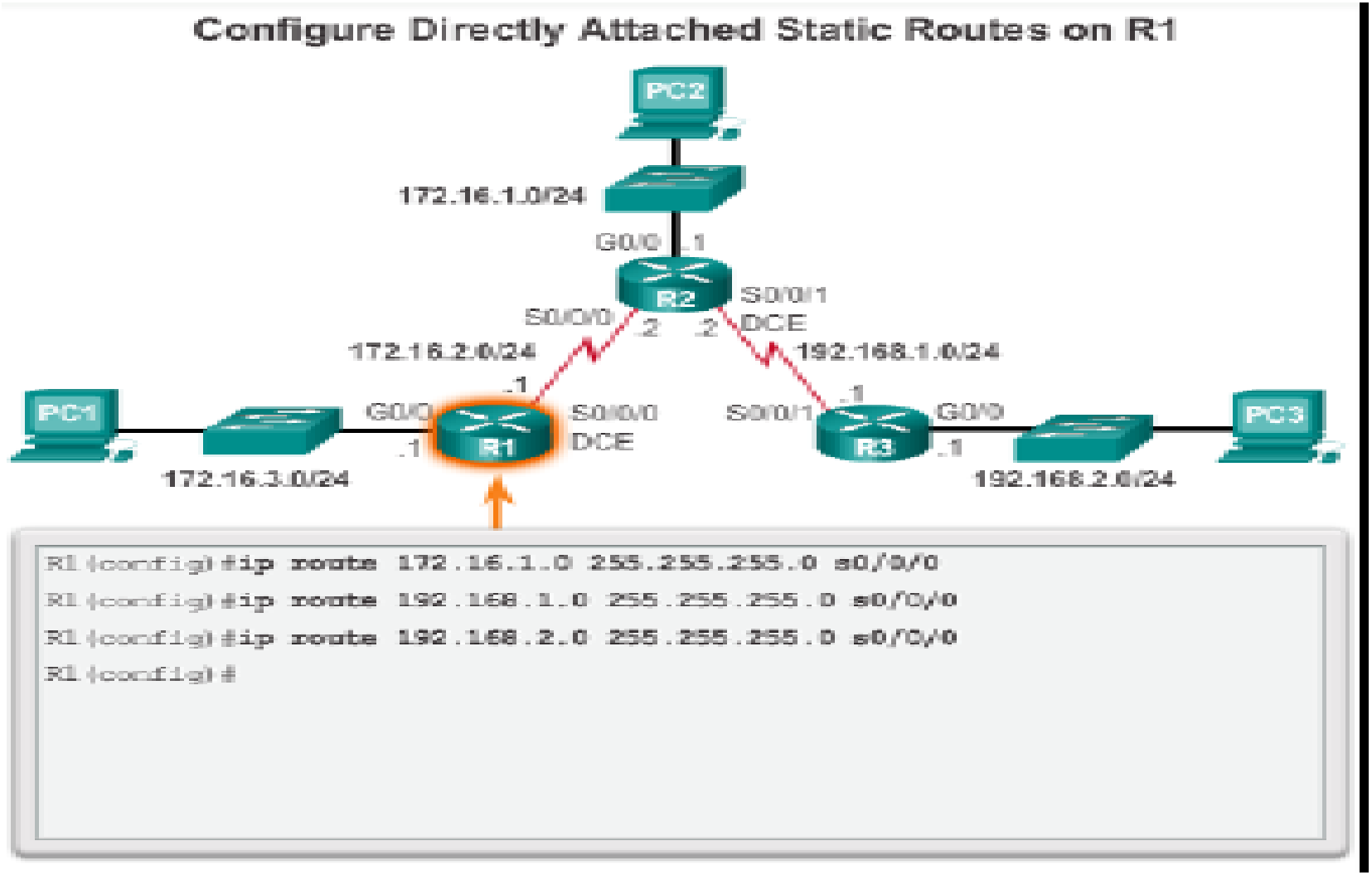
Configure IPv4 Static Routes

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 Default Routes

Configure a Next-HOP Static Route



Configure IPv4 Static Routes…

Configure Default Static Route

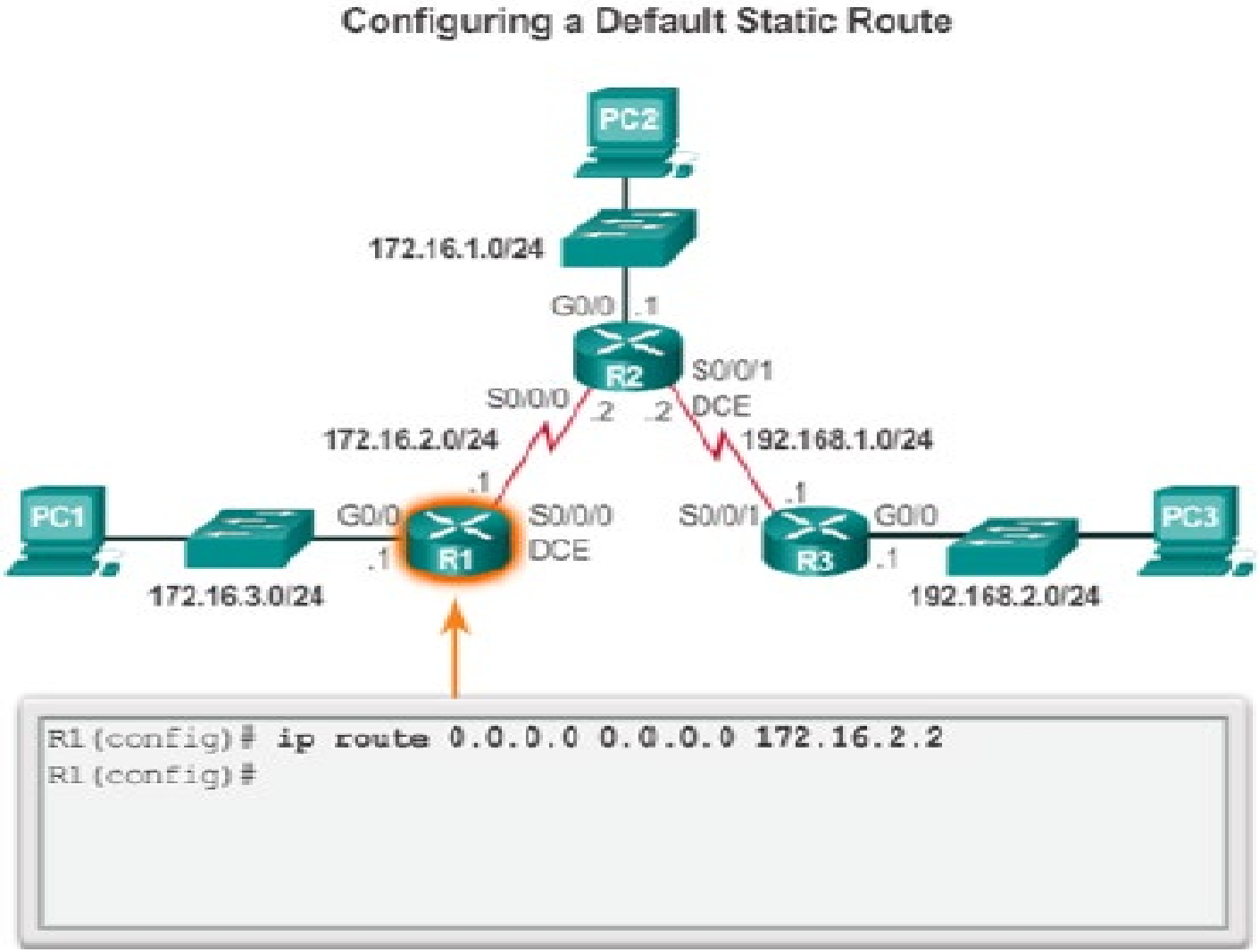
Default Static Route Syntax

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

Parameter	Description
0.0.0.0	Matches any network address.
0.0.0.0	Matches any subnet mask.
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…

Default Static Route



Configure IPv4 Static Routes…

Configure a Fully Specified Static Route

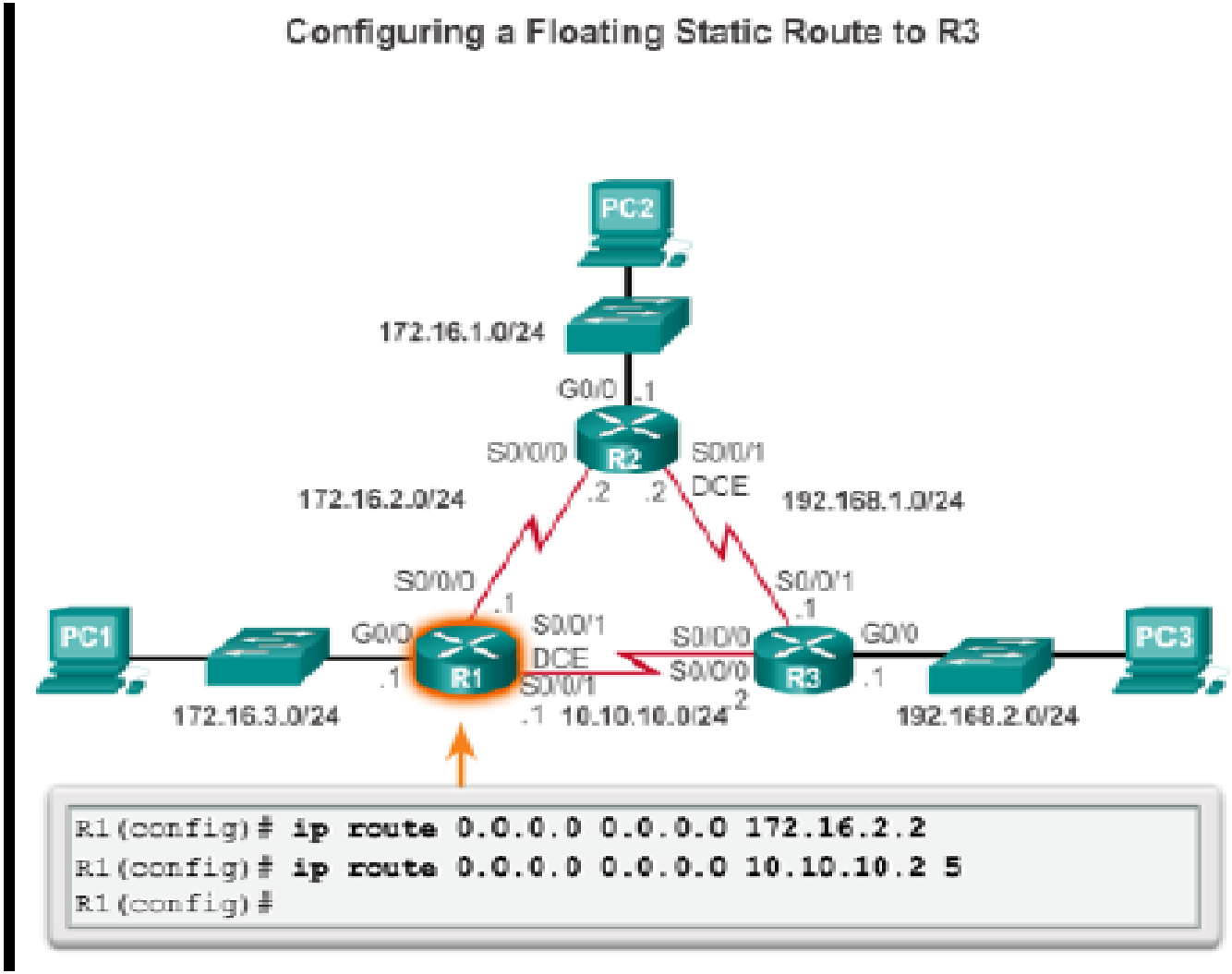
- In a fully specified static route, both the output interface and the next-hop IP address are specified.
- This is another type of static route that is used in older IOS's, prior to CEF.
- This form of static route is used when the output interface is a multi-access interface and it is necessary to explicitly identify the next hop.
- The next hop must be directly connected to the specified exit interface.

Configure Floating Static Routes

- Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static route or dynamic routes.
- The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol.
- In this way, the static route “floats” and is not used when the route with the better administrative distance is active.
- However, if the preferred route is lost, the floating static route can take over, and traffic can be sent through this alternate route.

Configure IPv4 Static Routes…

Configuring a floating static route



Configure Floating Static Routes…

Test the Floating Static Route

- Use a **show ip route** command to verify that the routing table is using the default static route.
- Use a **traceroute** command to follow the traffic flow out the primary route.
- Disconnect the primary link or shutdown the primary exit interface.
- 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.

Troubleshoot IPv4 Static and Default Route Configuration

Common IOS trouble-shooting commands include:

- *ping*
- *traceroute*
- *show ip route*
- *show ip interface brief*
- *show cdp neighbors detail*

Dynamic Routing Protocol

- **Routing Protocols**
  - Allow routers to dynamically share information about remote networks and automatically add this information to their own routing tables.
  - Used to facilitate the exchange of routing information between routers
  - Used to facilitate the exchange of routing information between routers
- 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 Protocol Operation

Main components of dynamic routing protocols include:

1. Data structures

- Routing protocols typically use tables or databases for its operations. This information is kept in RAM.

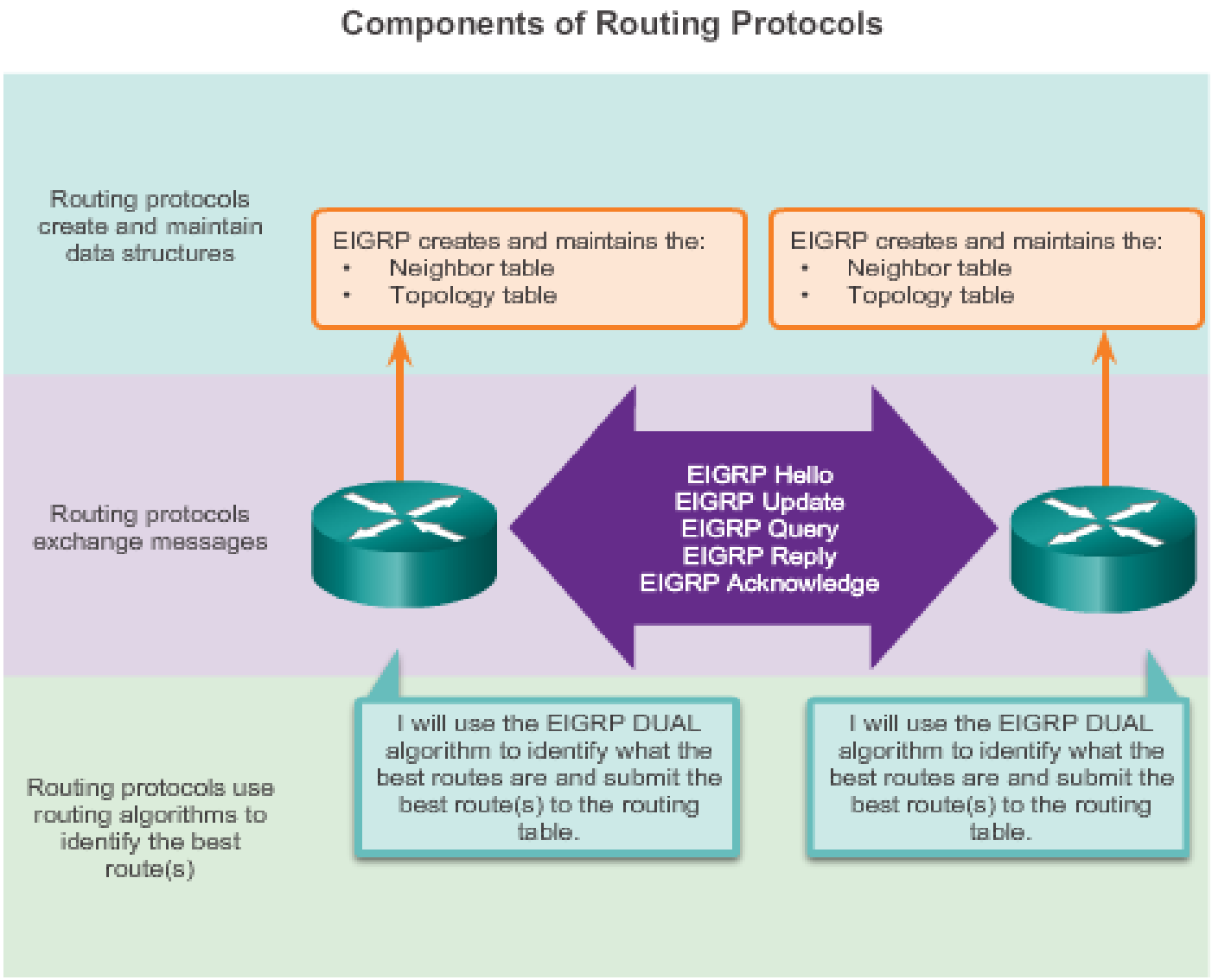
2. Routing protocol messages

- 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.

3. Algorithm

- Routing protocols use algorithms for facilitating routing information for best path determination.

Dynamic Routing Protocol Operation…



Dynamic Routing Advantages and Disadvantages

- **Advantages**
  - Automatically share information about remote networks
  - Determine the best path to each network and add this information to their routing tables
  - Compared to static routing, dynamic routing protocols require less administrative overhead
  - Help the network administrator manage the time-consuming process of configuring and maintaining static routes
  - Suitable in all topologies where multiple routers are required
- **Disadvantages**
  - Dedicate part of a routers resources for protocol operation, including CPU time and network link bandwidth
  - More administrator knowledge is required for configuration, verification, and troubleshooting
  - Times when static routing is more appropriate

Routing Protocol Operating Fundamentals

In general, the operations of a dynamic routing protocol can be described as follows:

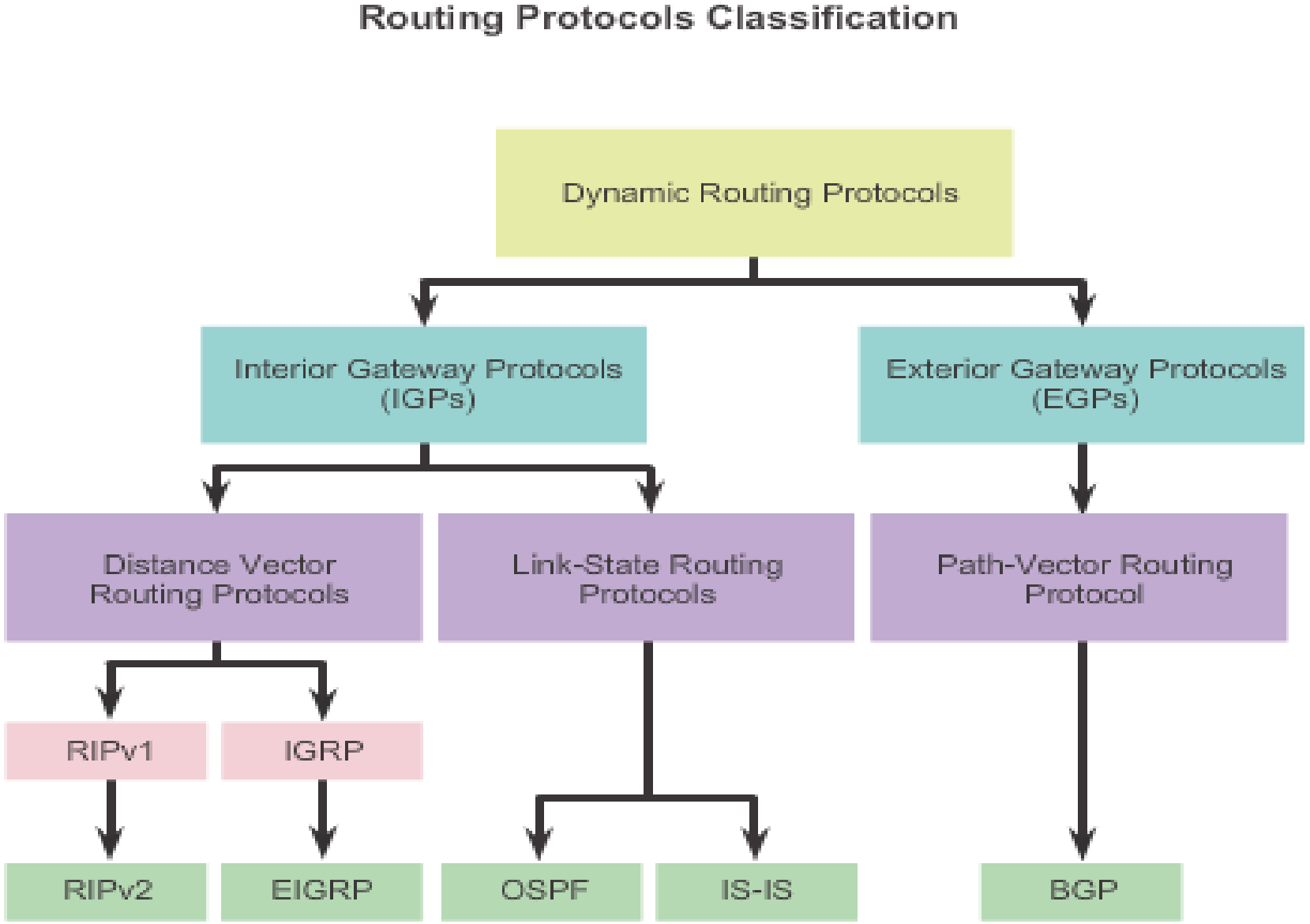
1. The router sends and receives routing messages on its interfaces.
2. The router shares routing messages and routing information with other routers that are using the same routing protocol.
3. Routers exchange routing information to learn about remote networks.
4. When a router detects a topology change the routing protocol can advertise this change to other routers.

Routing Protocol Operating Fundamentals

Achieving Convergence

- Network converged when all routers have complete and accurate information about the entire network.
- Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables.
- A network is not completely operable until the network has converged.
- Convergence properties include the speed of propagation of routing information and the calculation of optimal paths.
- The speed of propagation refers to the amount of time it takes for routers within the network to forward routing information.
- Generally, older protocols, such as RIP, are slow to converge, whereas modern protocols, such as EIGRP and OSPF, converge more quickly.

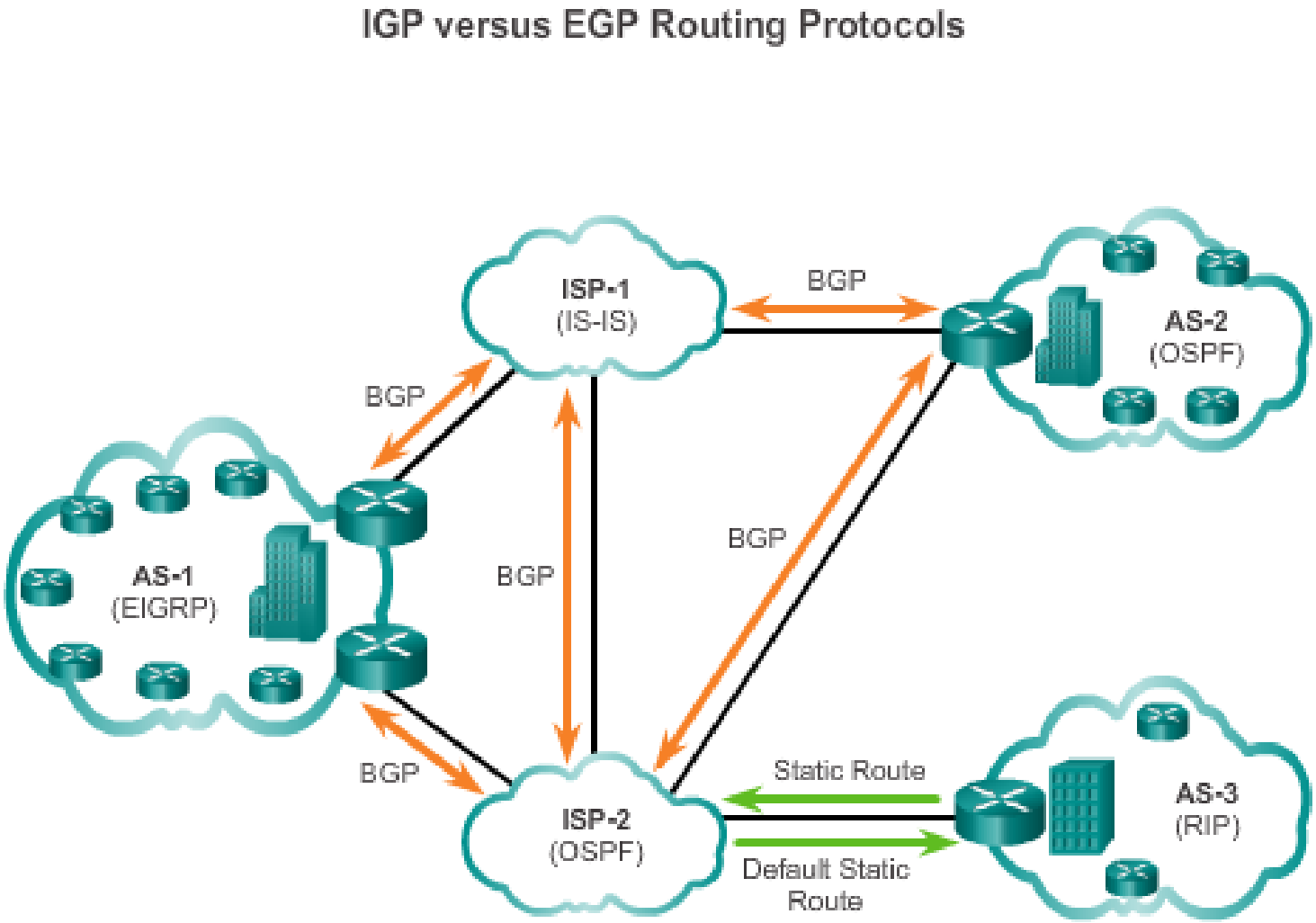
Types of Routing Protocols



Types of Routing Protocols….

- An **autonomous system** (AS) is a collection of routers under a common administration such as a company or an organization.
- An AS is also known as a routing domain.
- The Internet is based on the AS concept; therefore, two types of routing protocols are required:
  - **Interior Gateway Protocols (IGP)**
    - Used for routing within an AS
    - Include RIP, EIGRP, OSPF, and IS-IS
  - **Exterior Gateway Protocols (EGP)**
    - Used for routing between AS
    - Official routing protocol used by the Internet

Types of Routing Protocols…



Routing Protocol Characteristics

Routing protocols can be compared based on the following characteristics:

1. Speed of Convergence

- Defines how quickly the routers in the network topology share routing information and reach a state of consistent knowledge.
- The faster the convergence, the more preferable the protocol.
- Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.

2. Scalability

- Defines how large a network can become, based on the routing protocol that is deployed.
- The larger the network is, the more scalable the routing protocol needs to be.

Routing Protocol Characteristics…

3. Classful or Classless (Use of VLSM)

- Classful routing protocols do not include the subnet mask and cannot support VLSM.
- Classless routing protocols include the subnet mask in the updates.
- Classless routing protocols support VLSM and better route summarization.

4. Resource Usage

- Includes the requirements of a routing protocol such as memory space (RAM), CPU utilization, and link bandwidth utilization.
- Higher resource requirements necessitate more powerful hardware to support the routing protocol operation, in addition to the packet forwarding processes.

Routing Protocol Characteristics…

5. Implementation and Maintenance

- Describes the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed.

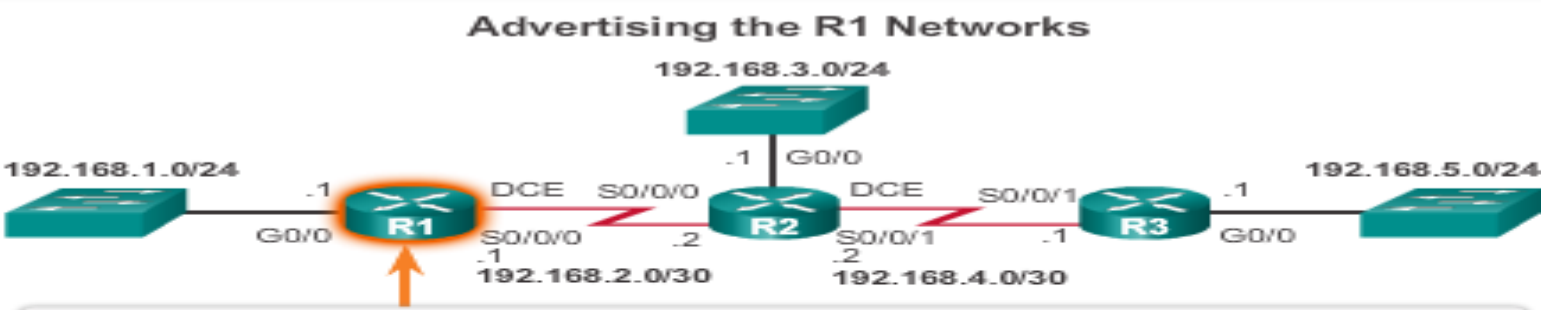
Routing Protocol Characteristics – Summary

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implemenation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Configuring the RIP Protocol

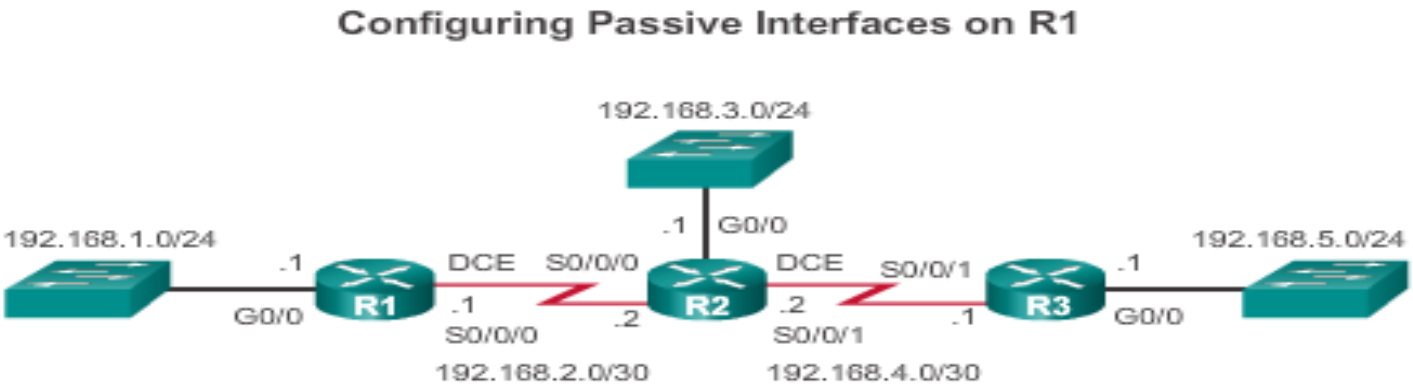
Router RIP Configuration Mode Advertising Networks

```
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)#
```

Configuring Passive Interfaces



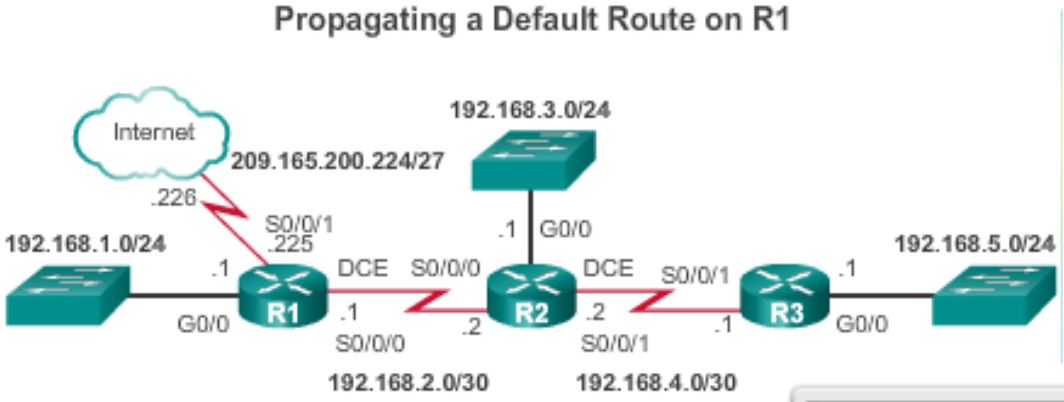
Sending out unneeded updates on a LAN impacts the network in three ways:

- **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#
```

Configuring the RIP Protocol

Propagating a Default Route




```
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,
```

Open Shortest Path First

Features of OSPF

Open Shortest Path First

Components of OSPF

OSPF Data Structures

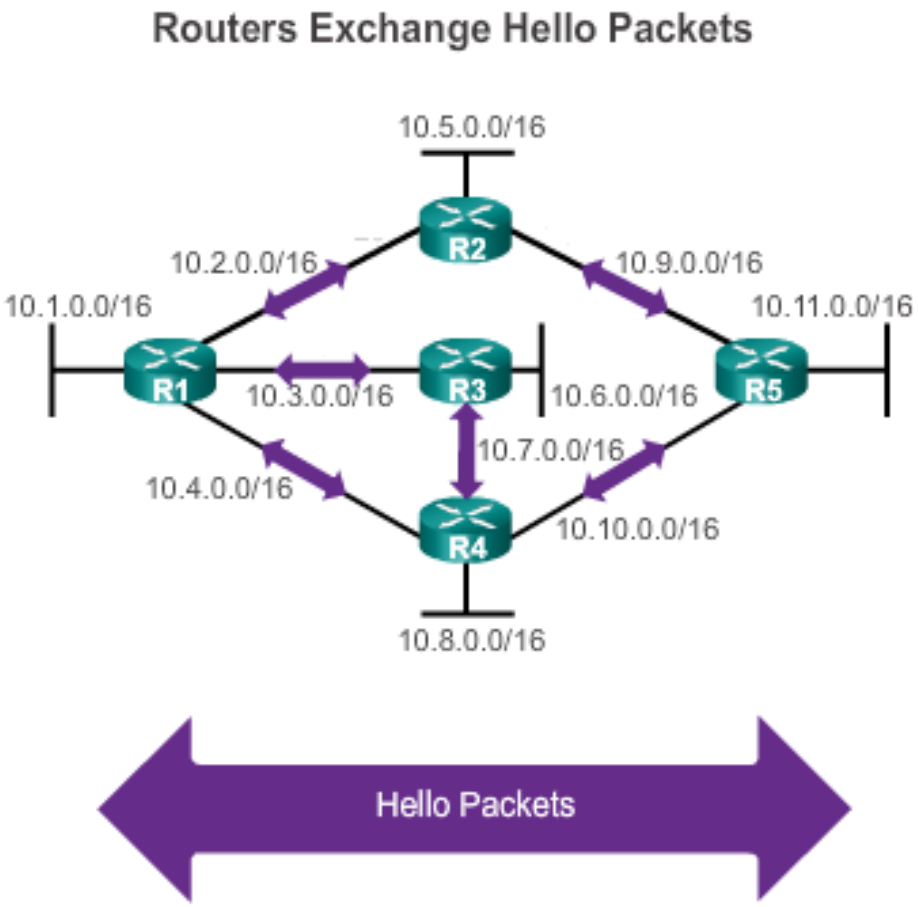
Database	Table	Description
Adjacency Database	Neighbor Table	• List of all neighbor routers to which a router has established bidirectional communication. • This table is unique for each router. • Can be viewed using the **`show ip ospf neighbor`** command.
Link-state Database (LSDB)	Topology Table	• 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

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

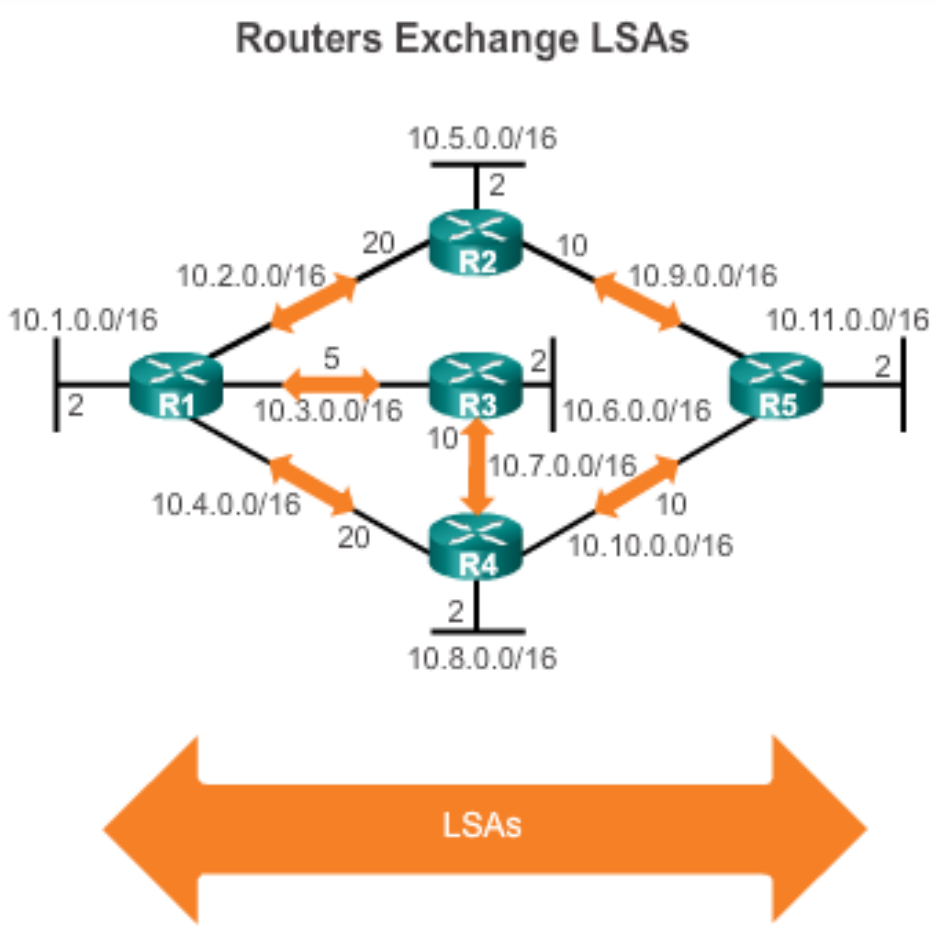
Link-State Operation



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

Open Shortest Path First

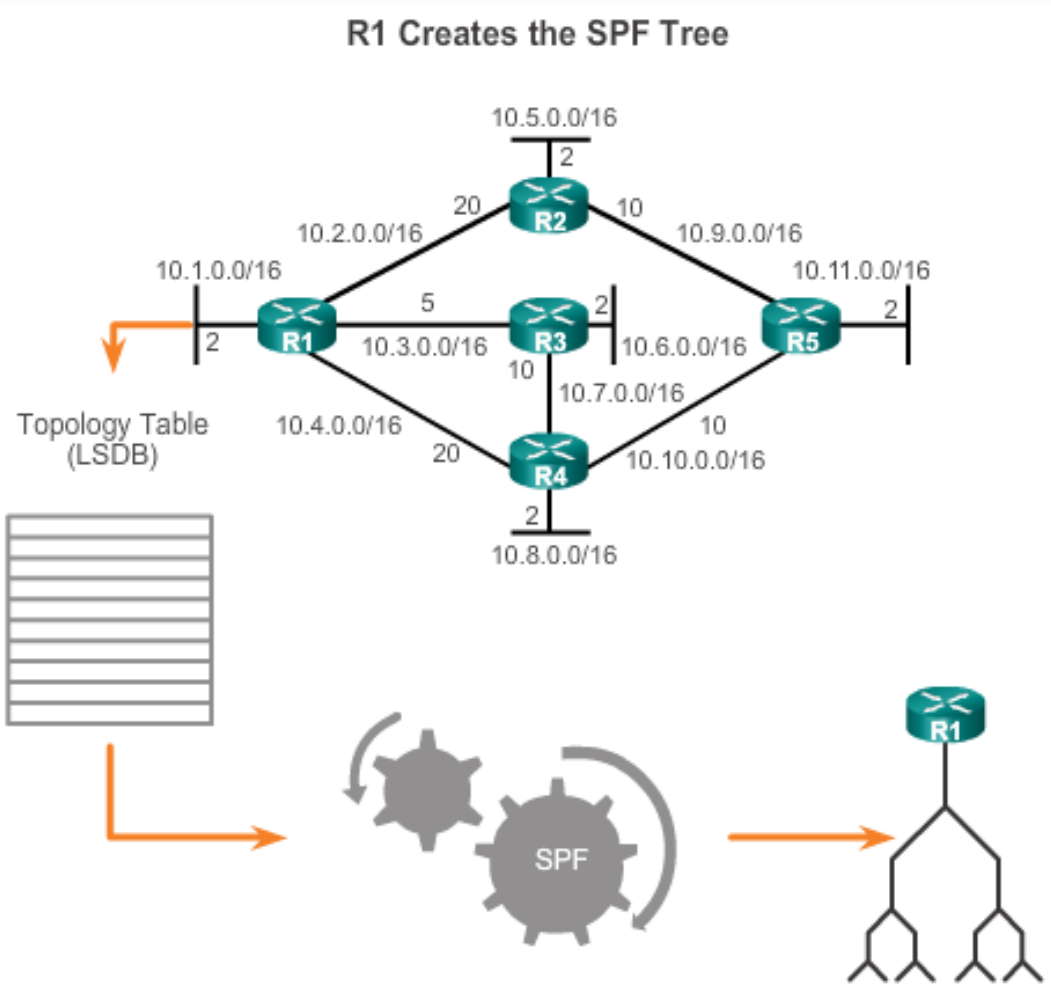
Link-State Operation



- 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

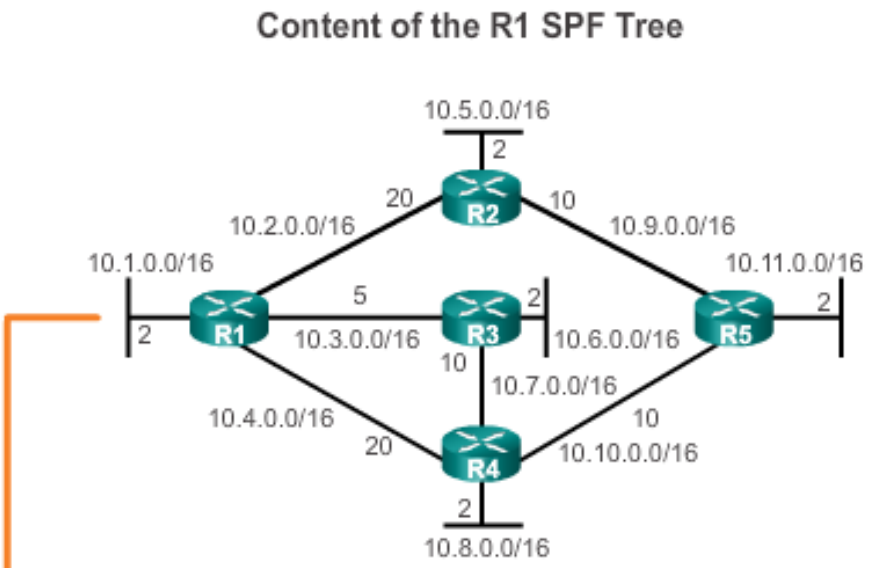
Link-State Operation



- 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

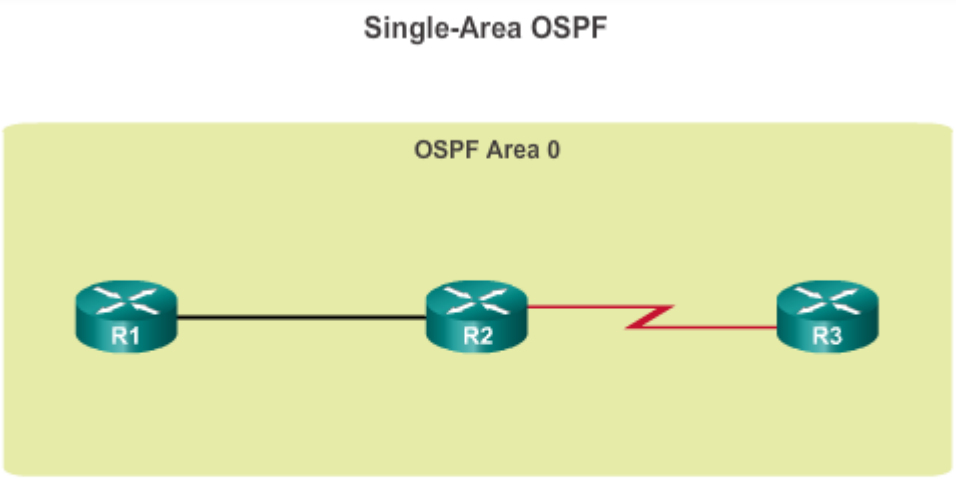


Destination	Shortest Path	Cost
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

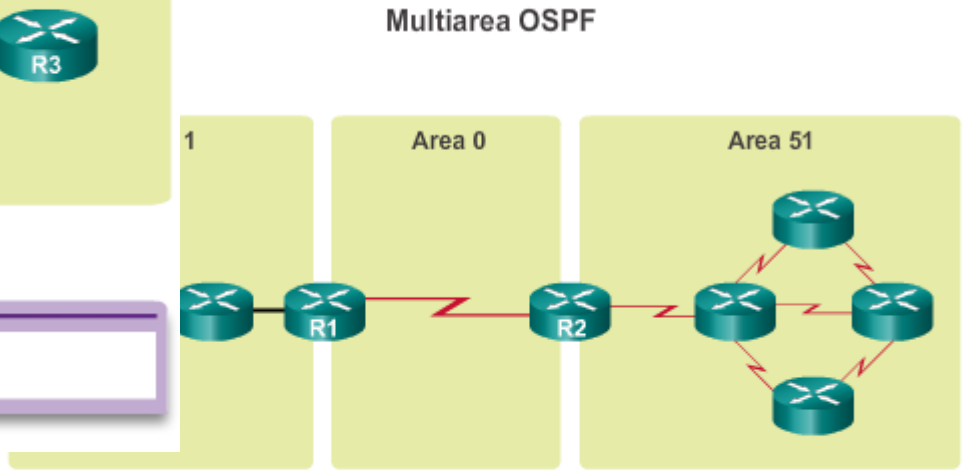
From the SPF tree, the best paths are inserted into the routing table.

Open Shortest Path First

Single-area and Multiarea OSPF



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

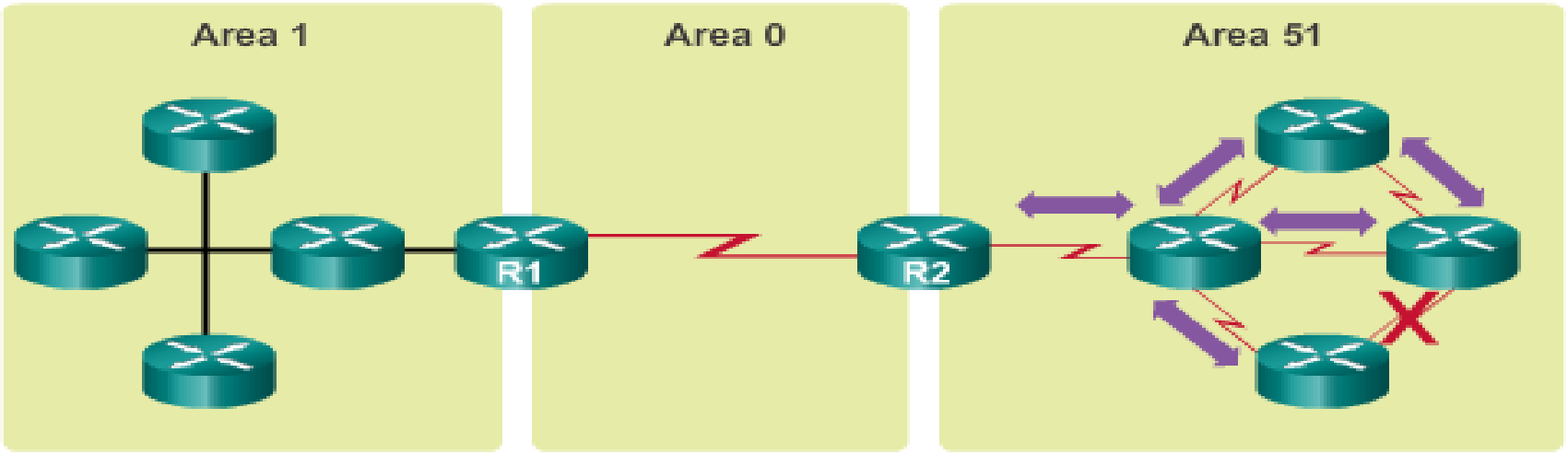


- Implemented using a two-layer area hierarchy as all areas must connect to the backbone area (area 0).
- Interconnecting routers are called Area Border Routers (ABR).
- Useful in larger network deployments to reduce processing and memory overhead.

Open Shortest Path First

Single-area and Multiarea OSPF

Link Change Impacts Local Area Only



- 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

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 multi access networks like Ethernet and Frame Relay

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 multi access and point-to-point networks)
- Every 30 seconds (default on non-broadcast multi access [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

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

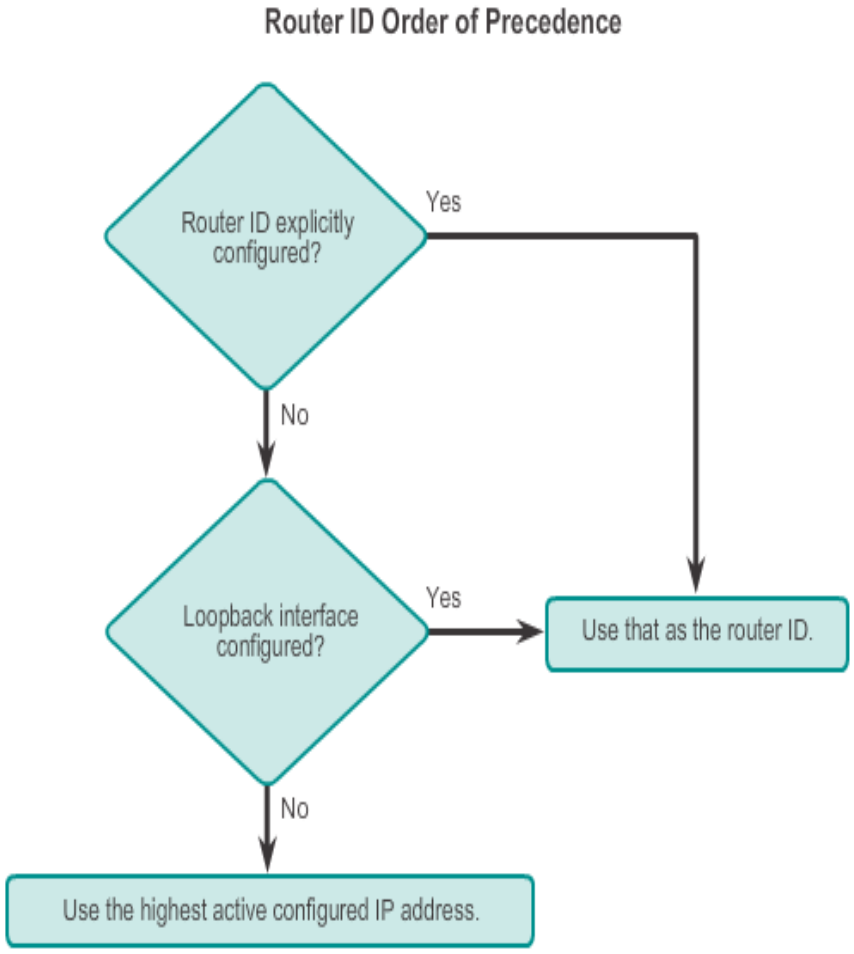
Router IDs

```
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#
```

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

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 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 bandwidth

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            E
 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#
```

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 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 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#
```

EIGRP (Enhanced Interior gateway routing protocol)

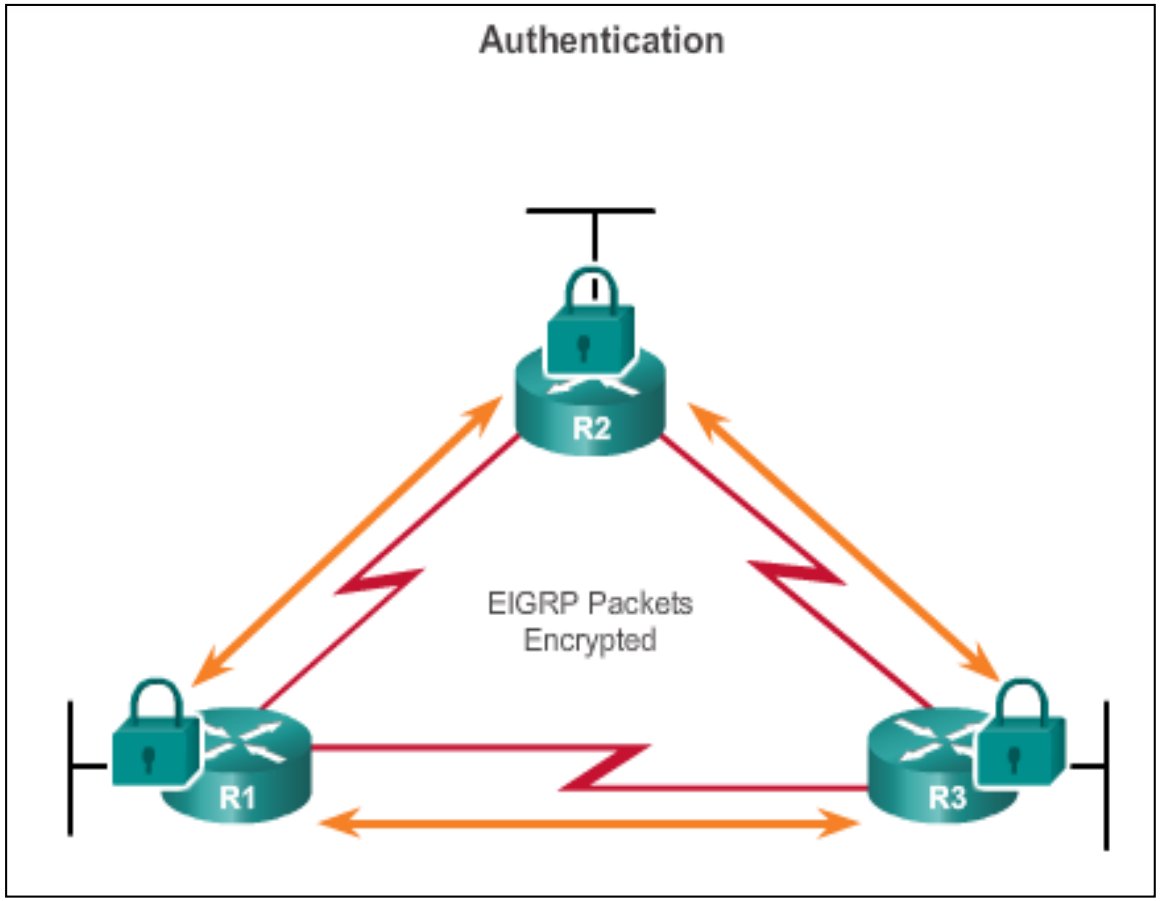
Features of EIGRP

- Released in 1992 as a Cisco proprietary protocol.
- 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.

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

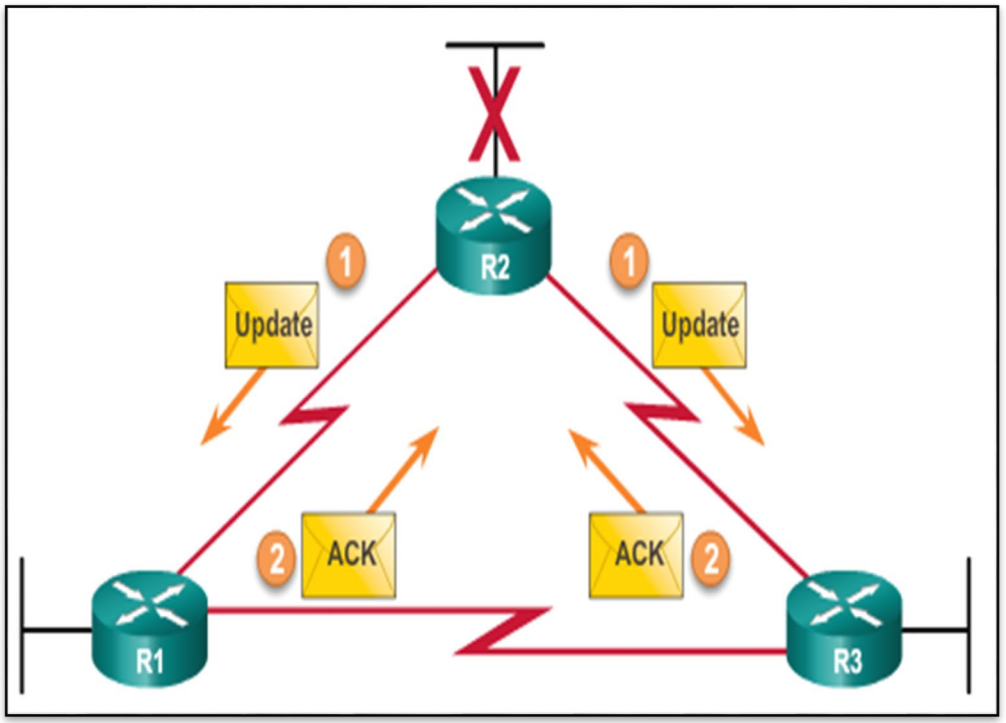
EIGRP Hello Packets

- 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

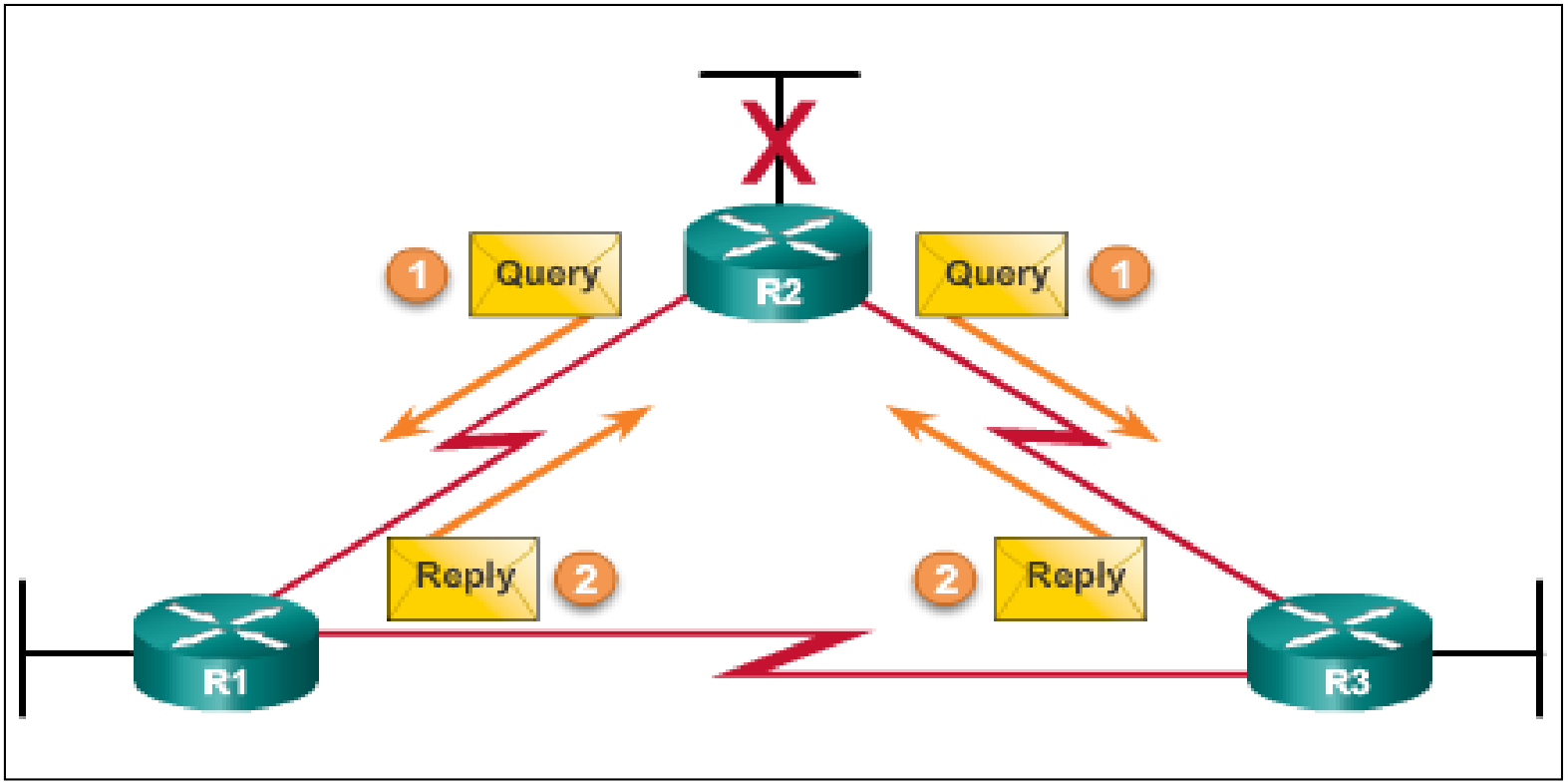
- Update packets are sent to propagate routing information, only when necessary.
- Sends **Partial** updates – only contains information about route changes.
- Sends **Bounded** updates- sent only to routers affected by the change.
- Updates use reliable delivery, therefore, require an **acknowledgement**.



Types of EIGRP Packets

EIGRP Query and Reply Packets

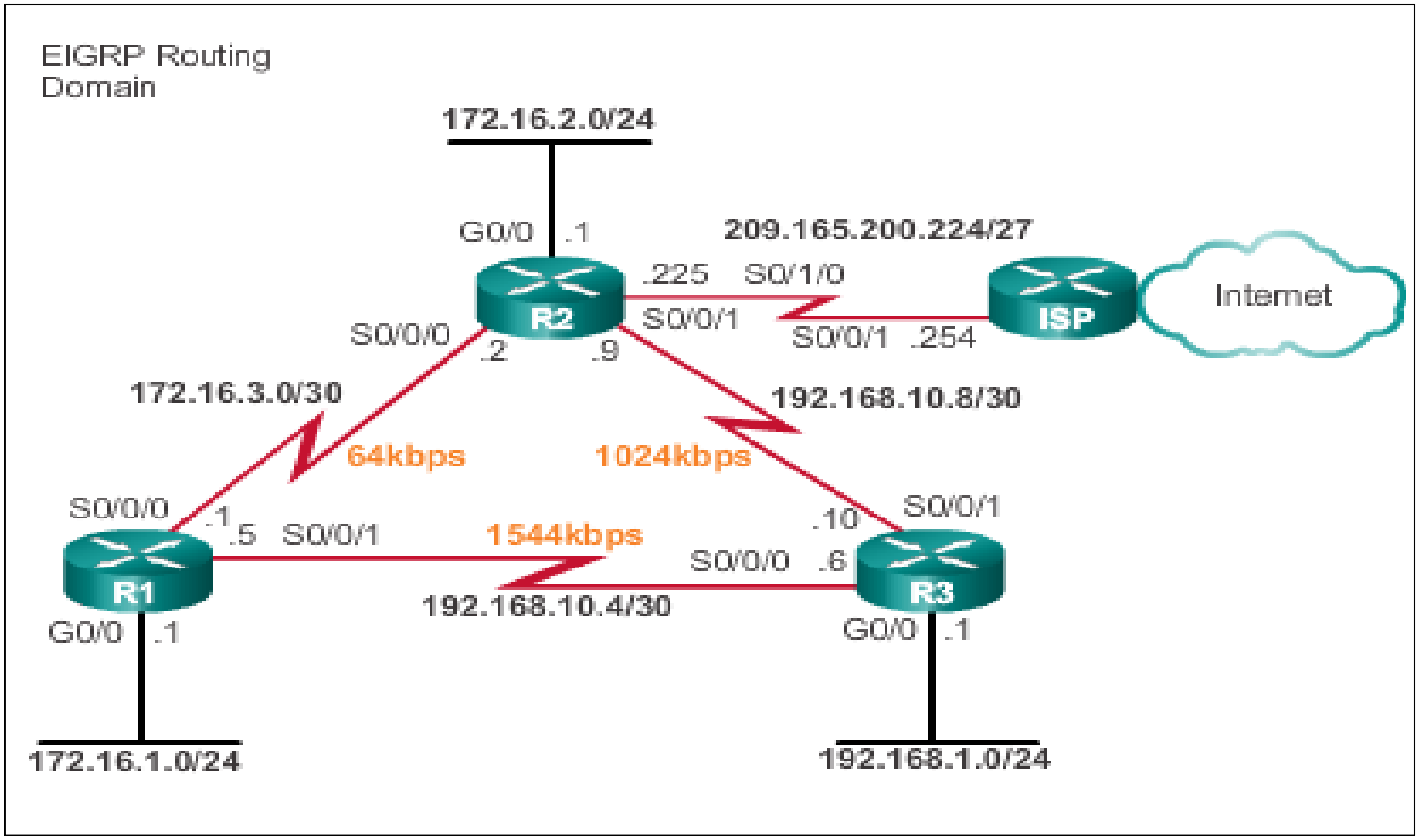
- Used when searching for networks.
- Queries use reliable delivery, which can be multicast or unicast.
- Replies use reliable delivery.



Configuring EIGRP with IPv4

EIGRP Network Topology

The topology that configures 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

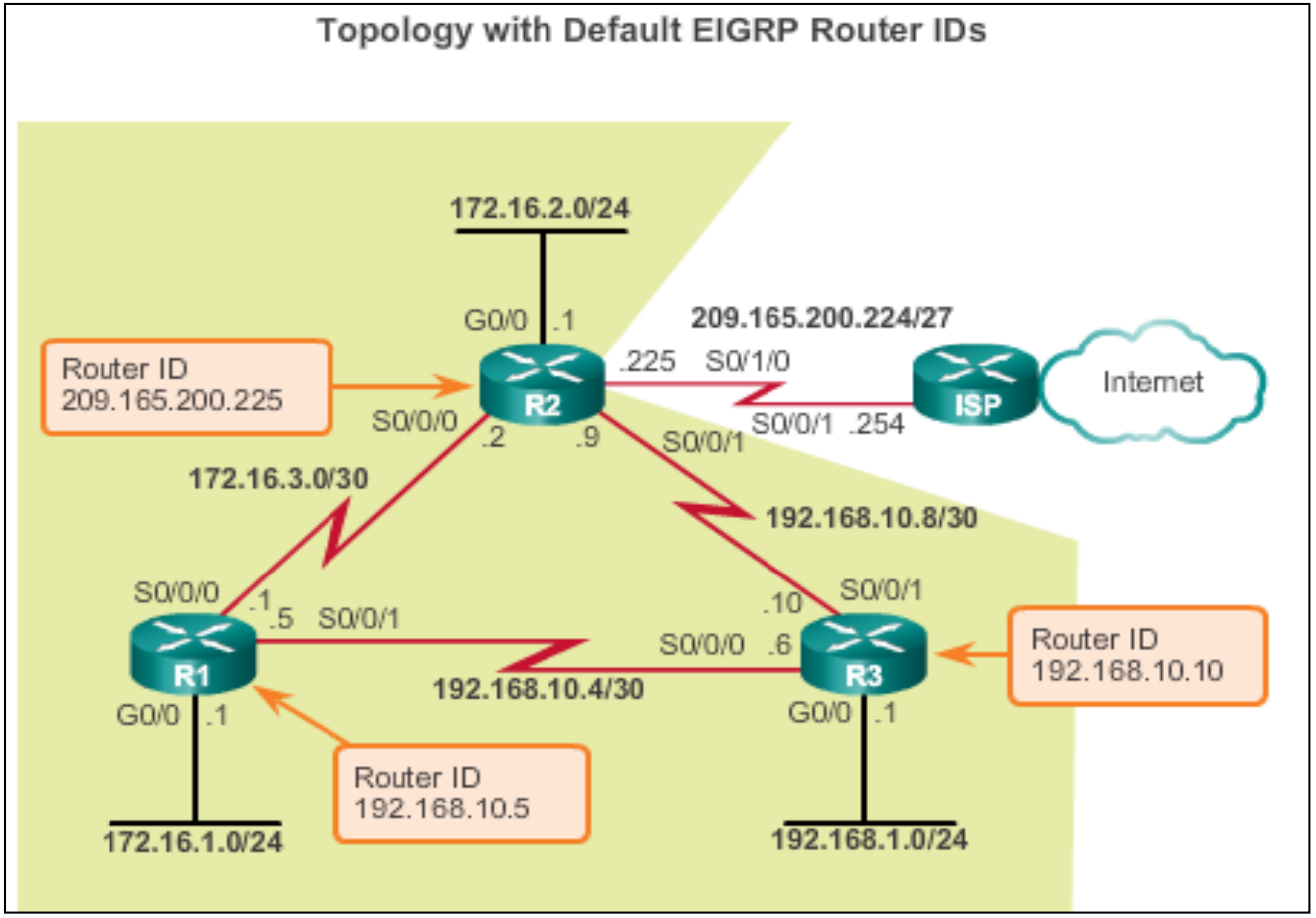
```
Router(config)# router eigrp autonomous-system
```

```
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

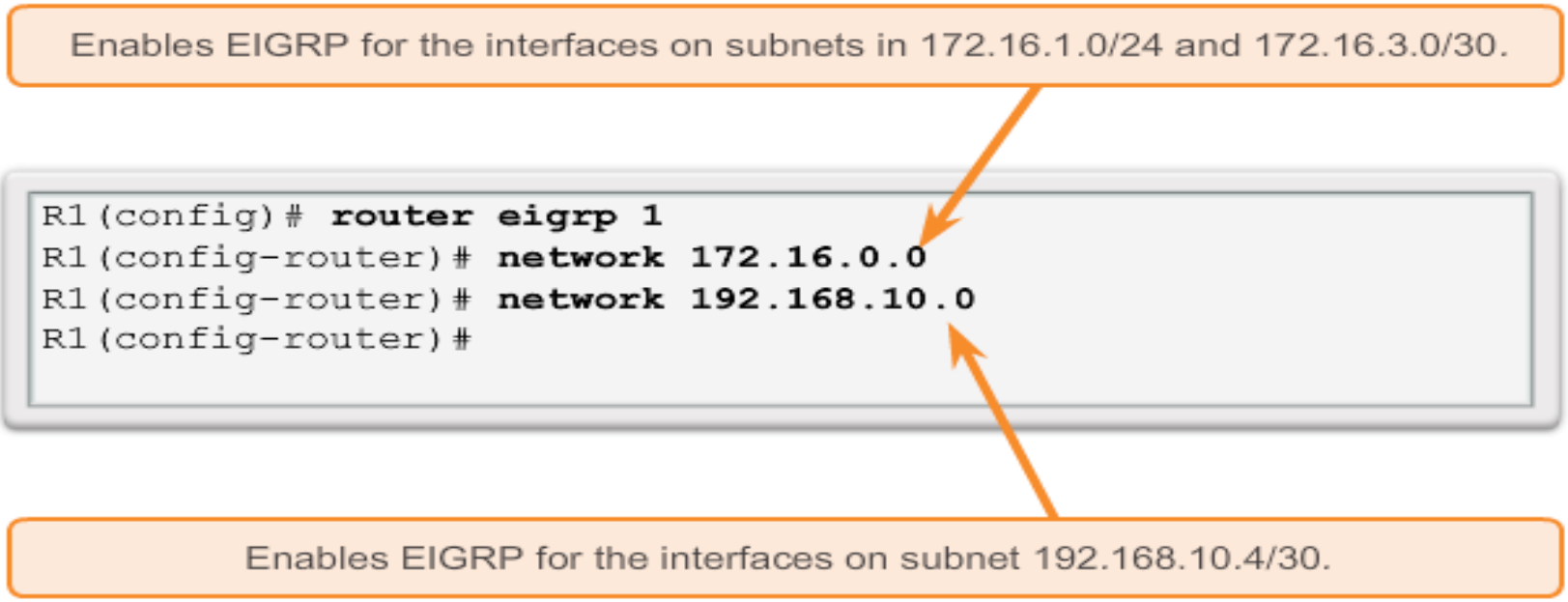
- Configuring the EIGRP router ID

  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*

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.



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

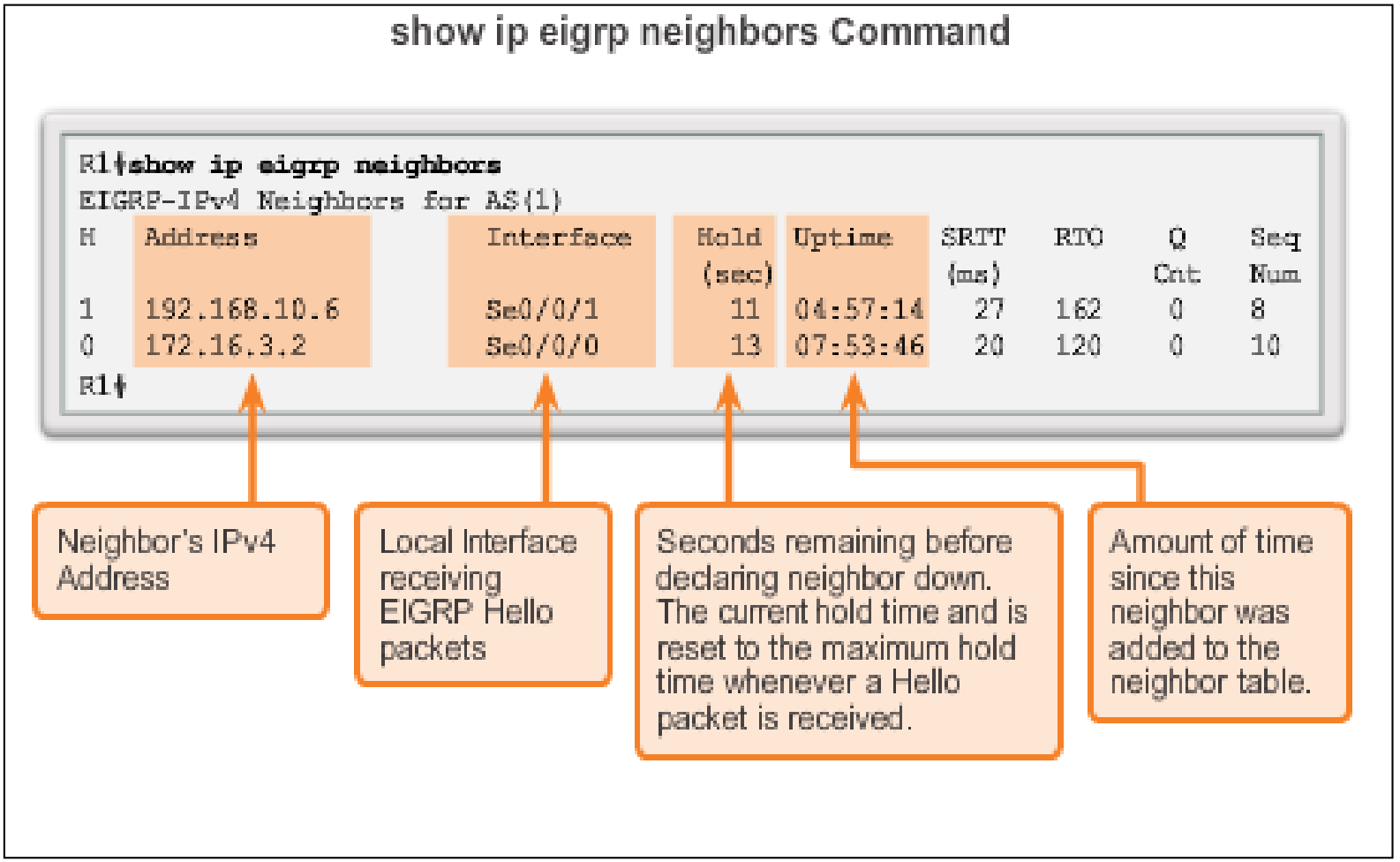
  0. 0. 0. 3 wildcard mask

- **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**

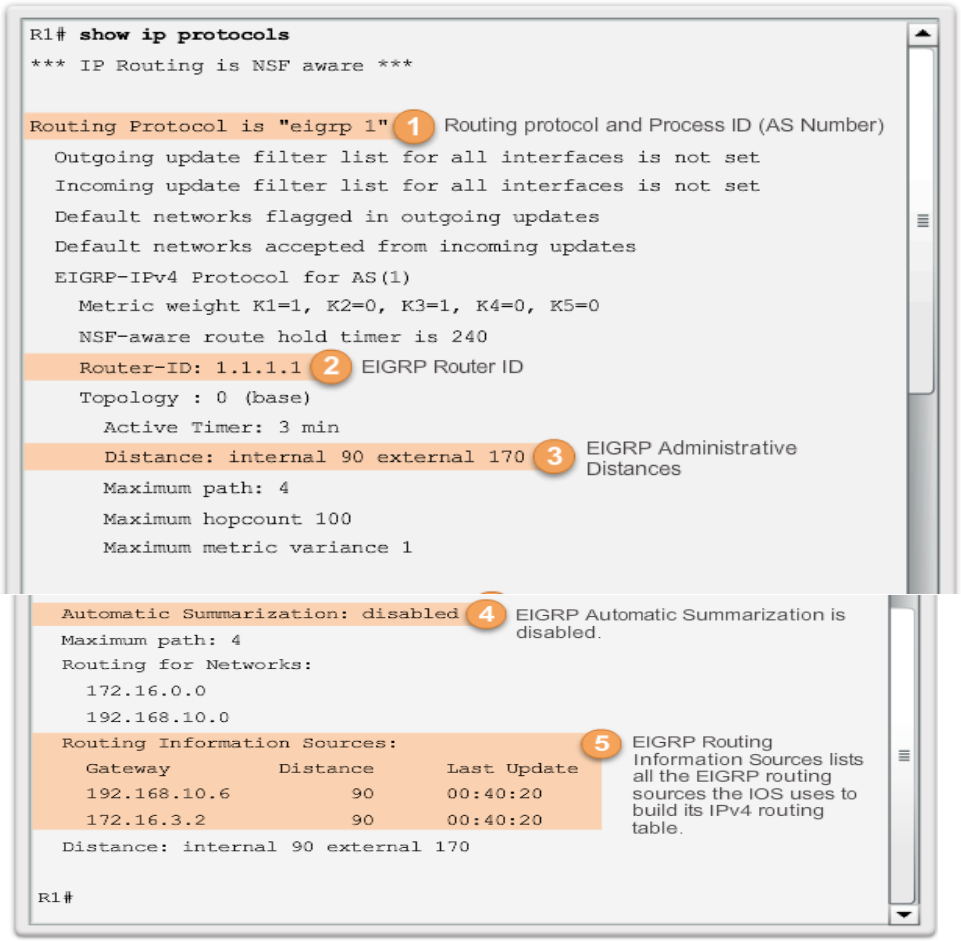
Verifying EIGRP: Examining Neighbors



Configuring EIGRP with IPv4

Verifying EIGRP: show ip protocols Command

show ip protocols Command



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#
```

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>
```

Metrics

Delay Metric

Interface Delay Values

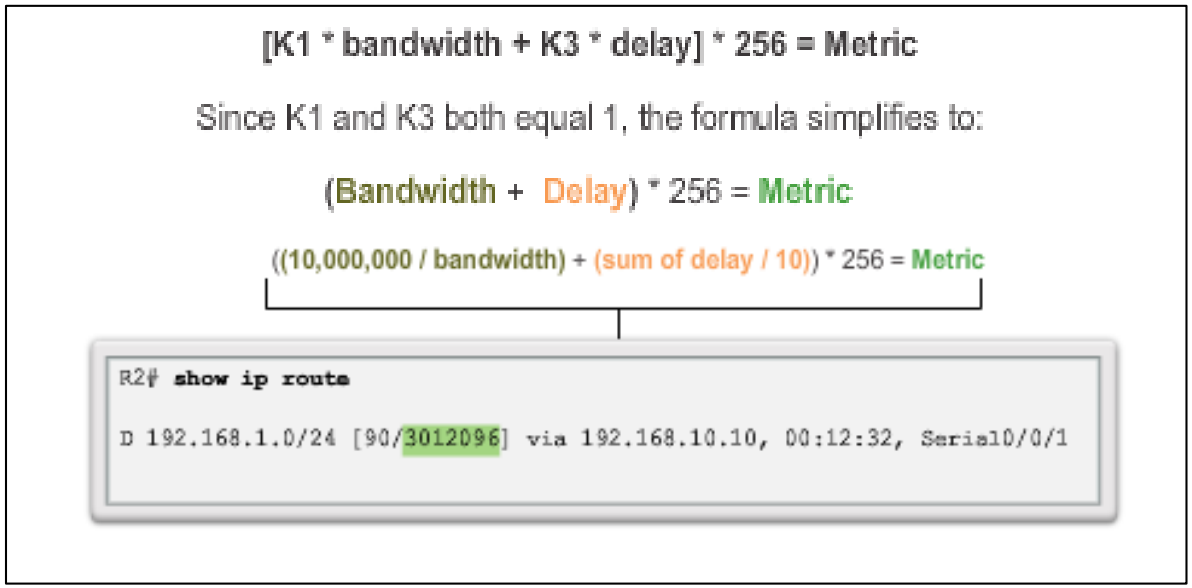
Media	Delay
Ethernet	1,000
Fast Ethernet	100
Gigabit Ethernet	10
16M Token Ring	630
FDDI	100
T1 (Serial Default)	20,000
DS0 (64 Kbps)	20,000
1024 Kbps	20,000
56 Kbps	20,000

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.

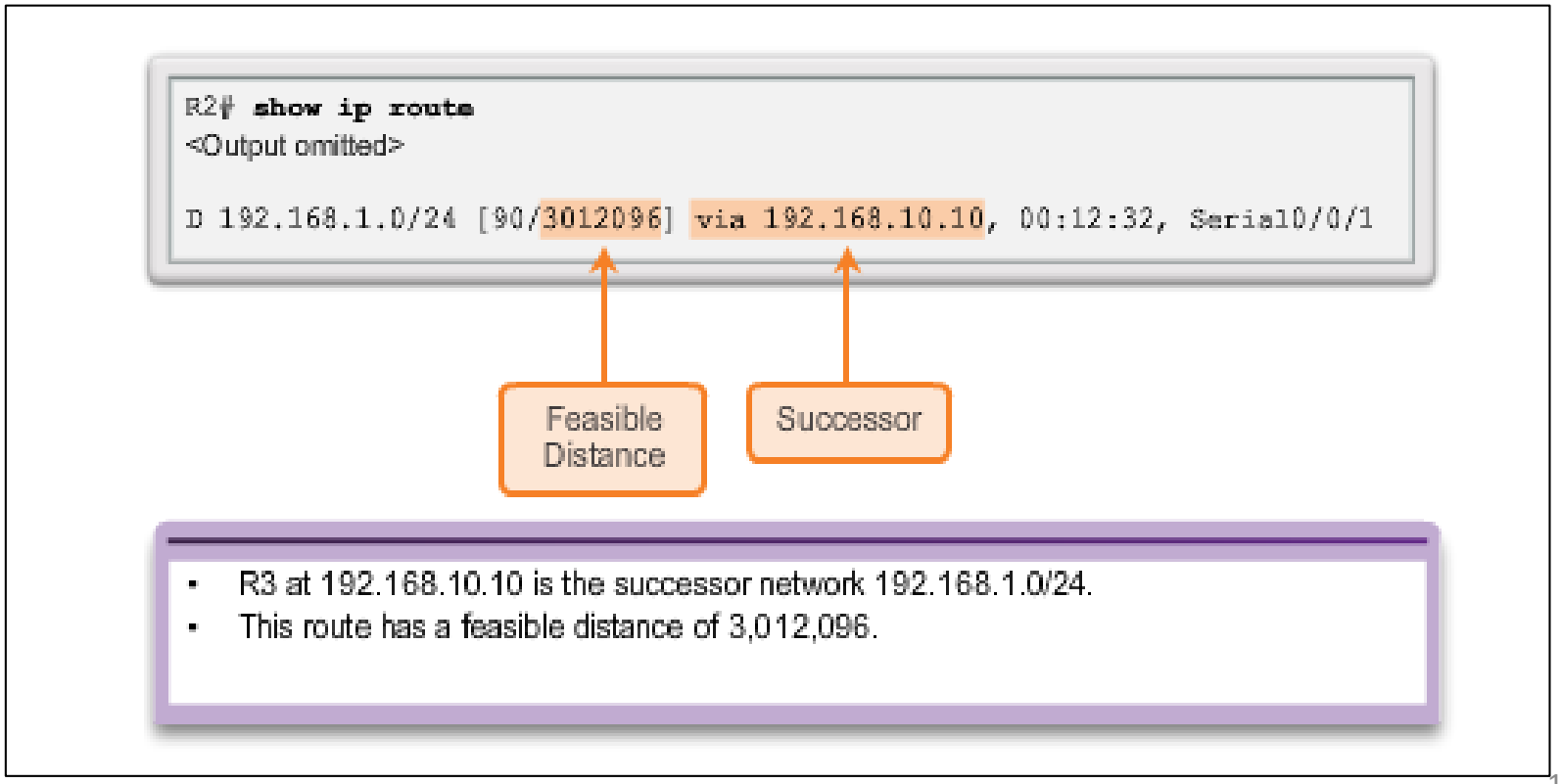


DUAL Concepts

- **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.

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
```

Feasible distance

Successor's (R3) Reported Distance

Next hop address of the successor

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
```

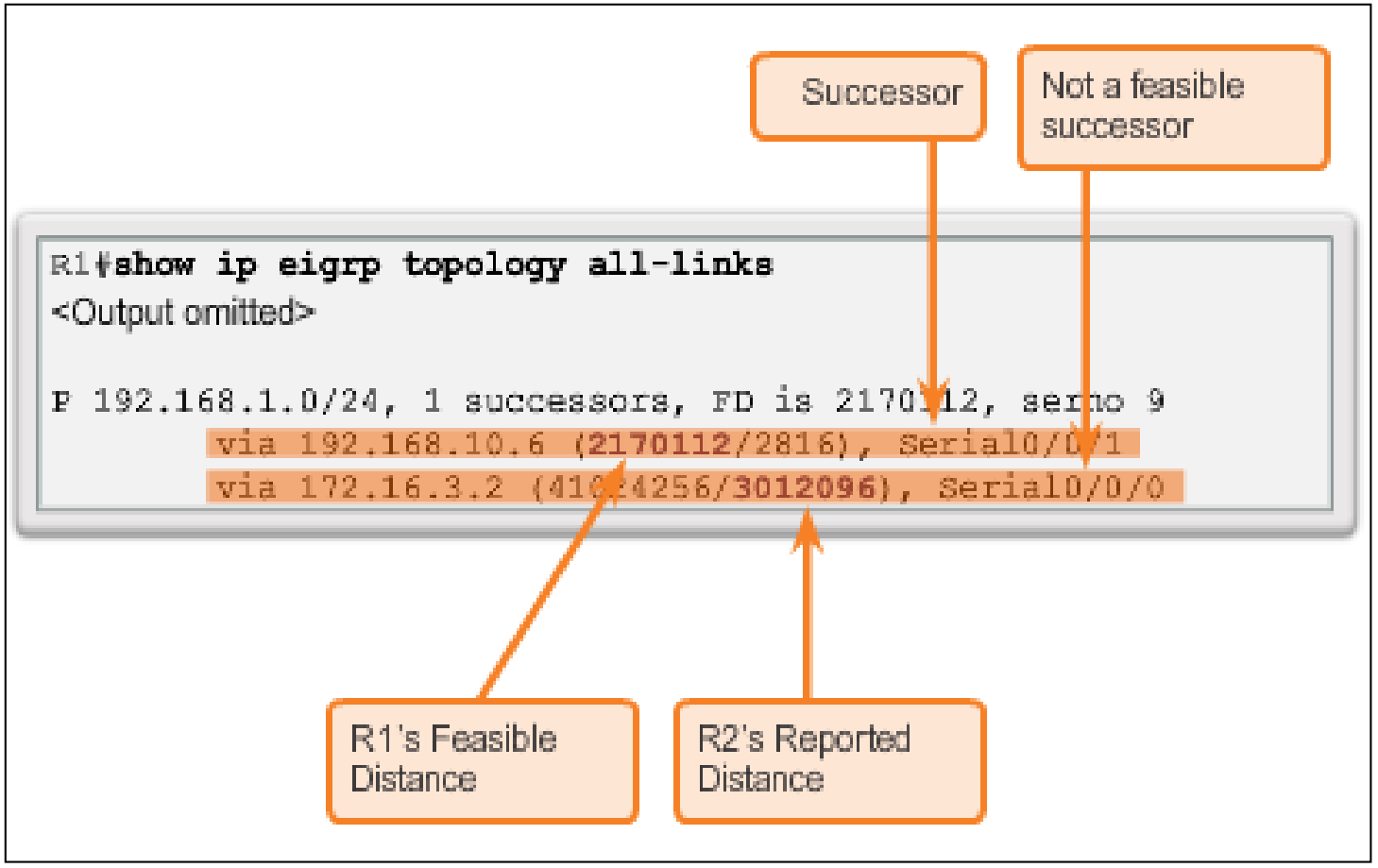
Feasible distance if the feasible successor (R1) was the successor

Outbound interface to reach this network

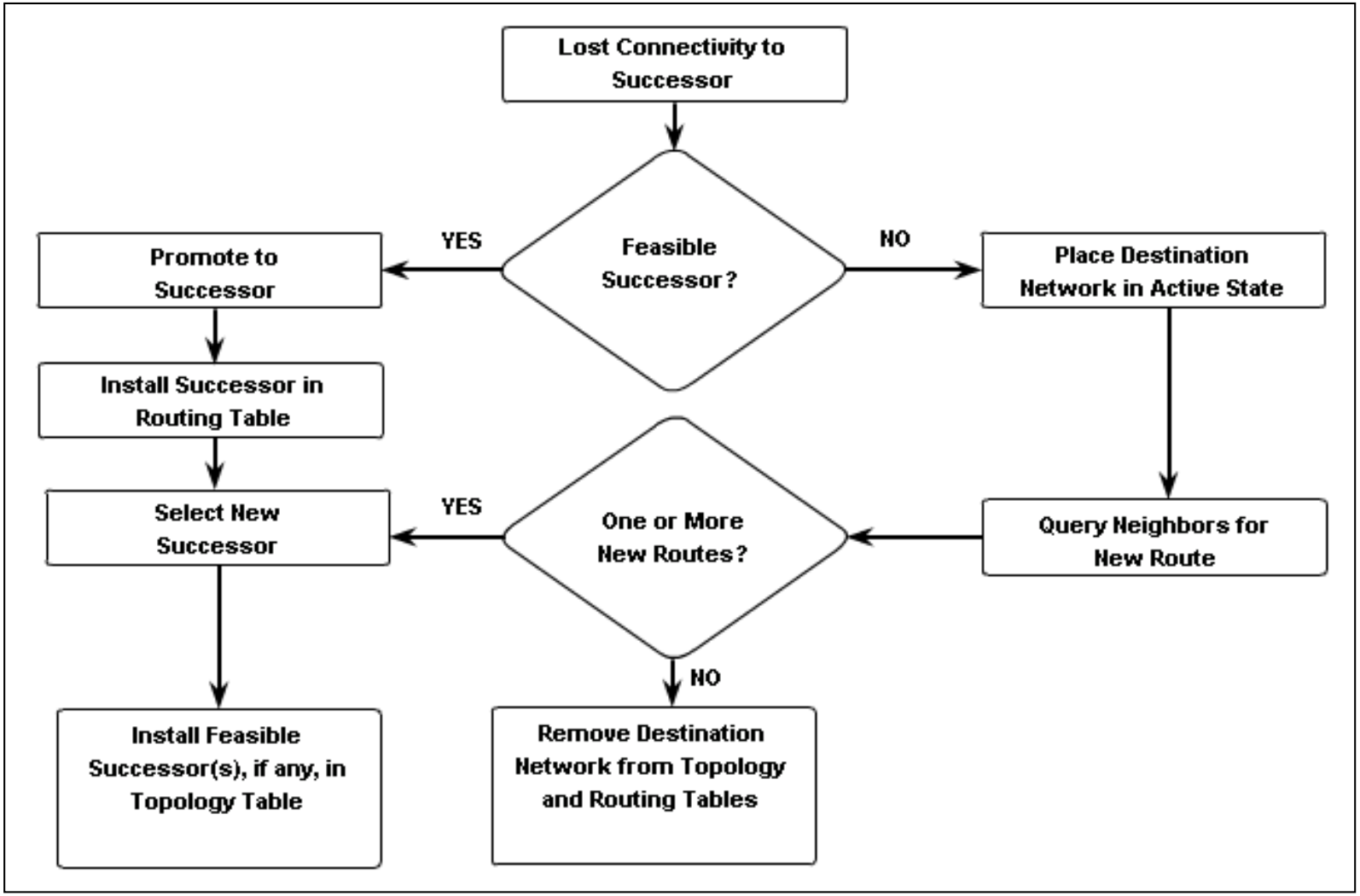
Next hop address of the feasible successor (R1)

Feasible Successor's (R1) Reported Distance

DUAL and the Topology Table
Topology Table: No Feasible Successor



DUAL and Convergence
DUAL Finite State Machine (FSM)



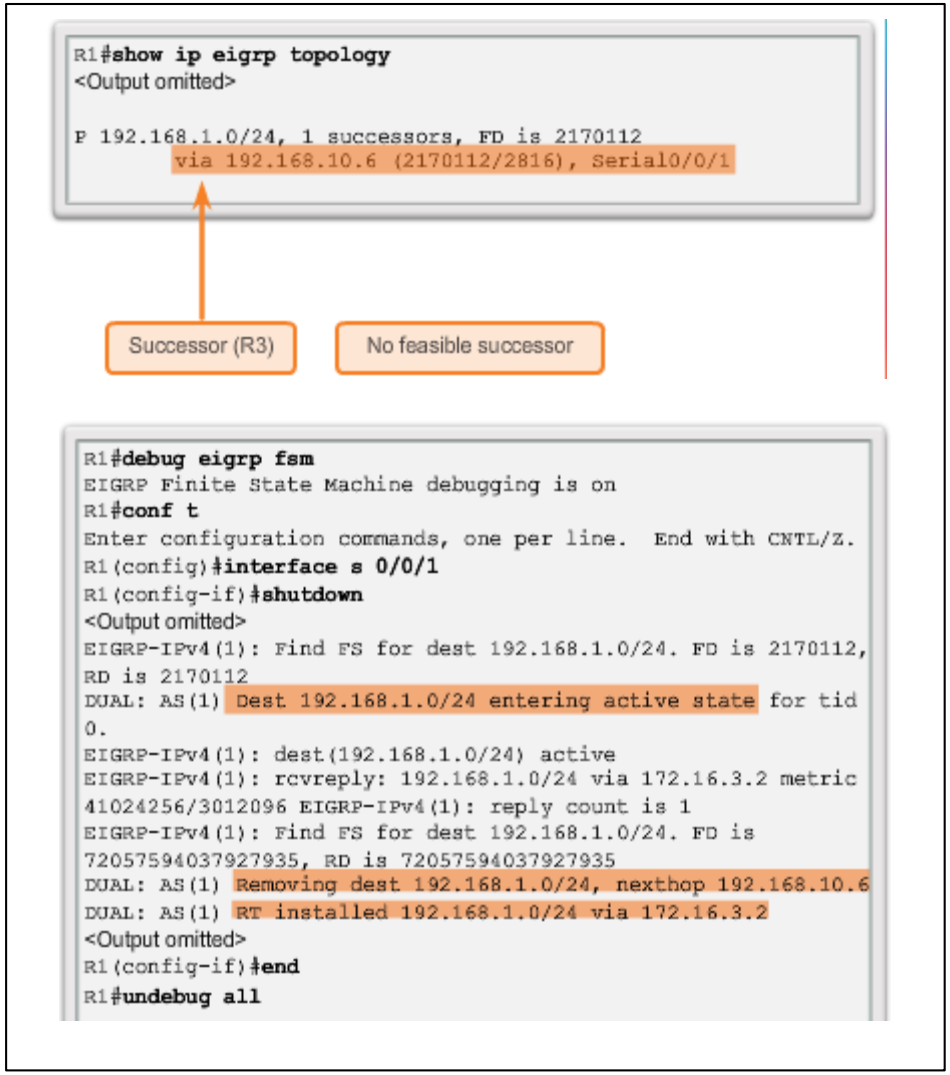
DUAL: Feasible Successor

```
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: No Feasible Successor



DHCP

- Dynamic Host Configuration Protocol (DHCP) is a network protocol that provides automatic IP addressing and other information to clients:IP address
  - Subnet mask (IPv4) or prefix length (IPv6)
  - Default gateway address
  - DNS server address
- Available for both IPv4and IPv6
- This chapter explores the functionality, configuration, and troubleshooting of both DHCPv4 and DHCPv6

Introducing DHCPv4

- DHCPv4 uses three different address allocation methods

  Manual Allocation - The administrator assigns a pre-allocated IPv4 address to the client, and DHCPv4 communicates only the IPv4 address to the device.

  Automatic Allocation - DHCPv4 automatically assigns a static IPv4 address permanently to a device, selecting it from a pool of available addresses. No lease.

  Dynamic Allocation - DHCPv4 dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address. Most commonly used.

Configuring a DHCPv4 Server

- A Cisco router running Cisco IOS software can be configured to act as a DHCPv4 server. To set up DHCP

  1.Exclude addresses from the pool.

  2. Set up DHCP pool name

  3. Configuring Specific Tasks –

  - define range of addresses and subnet mask.
  - Use default-router command for default gateway.
  - Optional items that can be included in pool – dns server, domain-name

- To disable dhcp **- no service dhcp**

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

DHCPv4 Operation

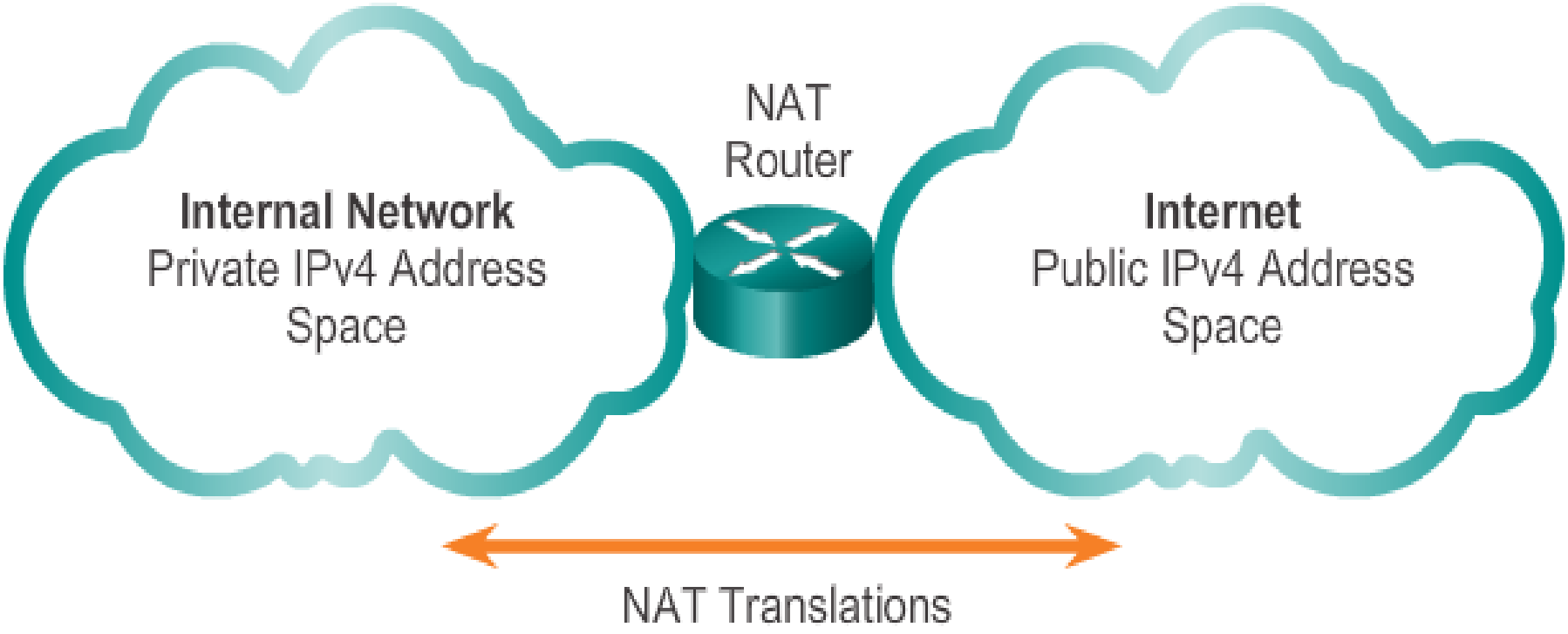
Verifying a DHCPv4 Server

- Commands to verify DHCP
  - ✓ **show running-config | section dhcp**
  - ✓ **show ip dhcp binding**
  - ✓ **show ip dhcp server statistics**
- On the PC –**issue the ipconfig /all command**

Network Address Translation for IPv4
IPv4 Private Address Space

- The IPv4 address space is not big enough to uniquely address all the devices that need to be connected to the Internet
- Network private addresses are described in RFC 1918 and are to designed to be used within an organization or site only
- Private addresses are not routed by Internet routers while public addresses are
- Private addresses can alleviate IPv4 scarcity but since they aren't routed by Internet devices, they need to be translated first.
- NAT is process used to perform such translation

IPv4 Private Address Space



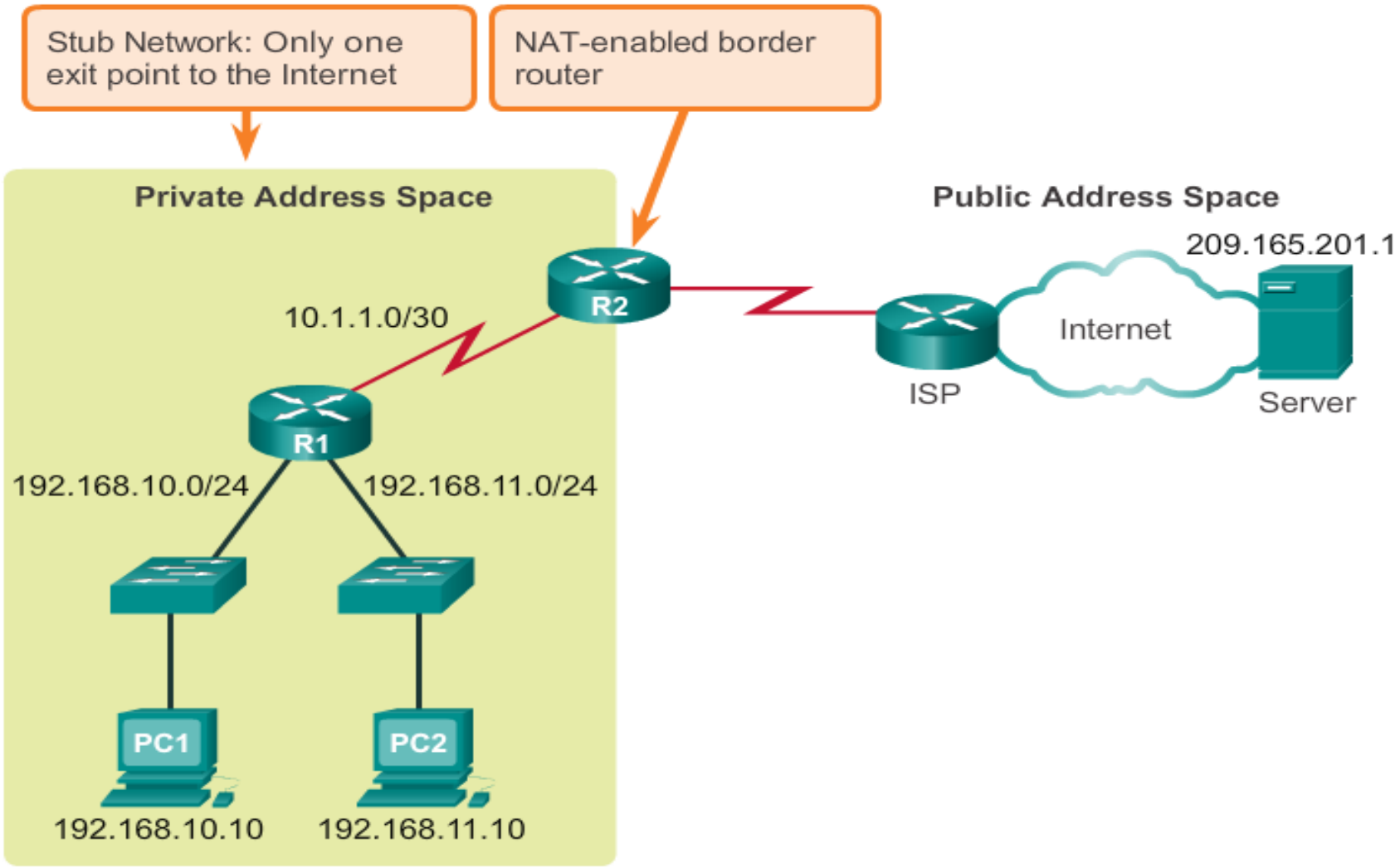
Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

What is NAT?

- NAT is a process used to translate network addresses
- NAT's primary use is to conserve public IPv4 addresses usually implemented at border network devices such as firewalls or routers
- This allows the networks to use private addresses internally, only translating to public addresses when needed
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent/received to/from other organizations or the Internet, the border router translates the addresses to a public and globally unique address

What is NAT?


Stub Network: Only one exit point to the Internet
NAT-enabled border router
Private Address Space
Public Address Space
209.165.201.1
R2
10.1.1.0/30
Internet
ISP
Server
R1
192.168.10.0/24
192.168.11.0/24
PC1
PC2
192.168.10.10
192.168.11.10

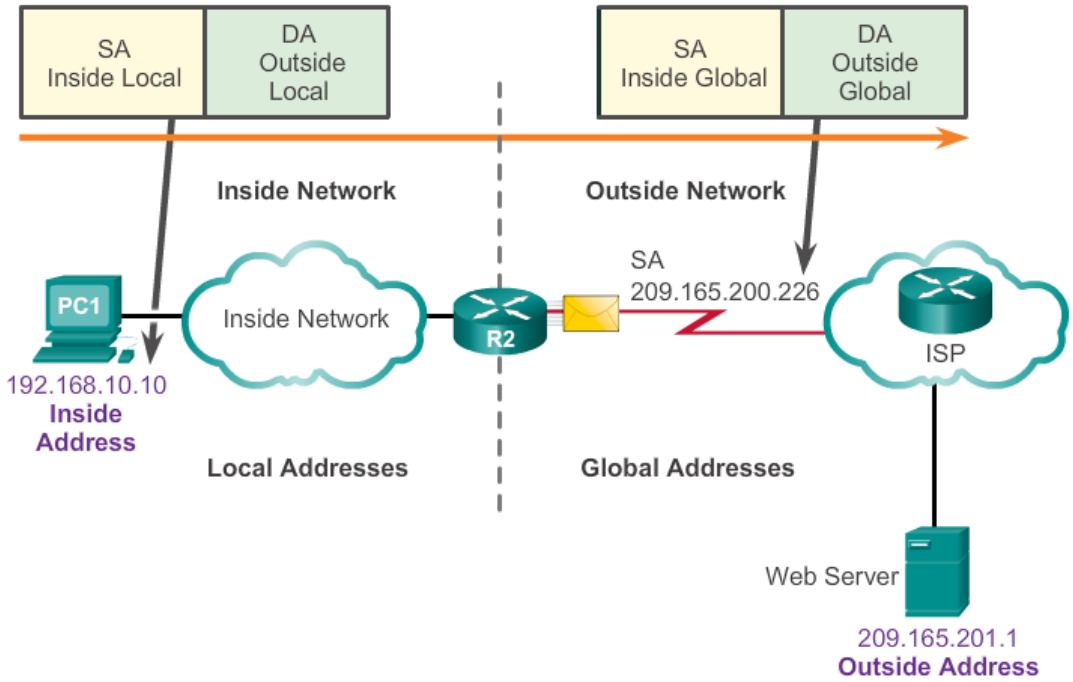
NAT Characteristics

NAT Terminology

- In NAT terminology, inside network is the set of devices using private addresses. Outside networks are all other networks

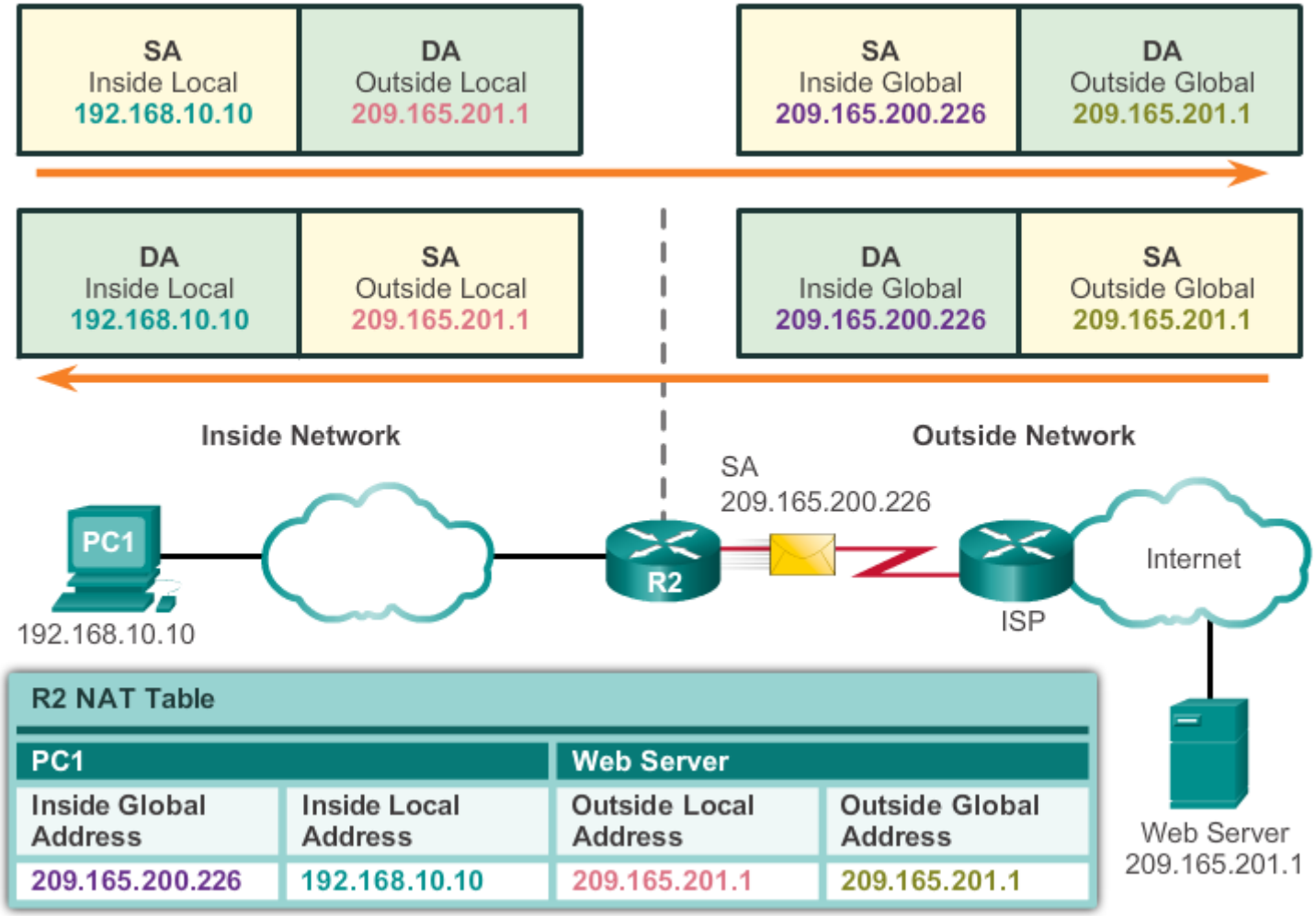
NAT includes 4 types of addresses:

- Inside local address
- Inside global address
- Outside local address
- Outside global address



NAT Characteristics

How NAT Works



R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Types Of NAT

Static NAT

- Static NAT uses a one-to-one mapping of local and global addresses
- These mappings are configured by the network administrator and remain constant
- Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network
- A network administrator can SSH to a server in the inside network by point his SSH client to the proper inside global address

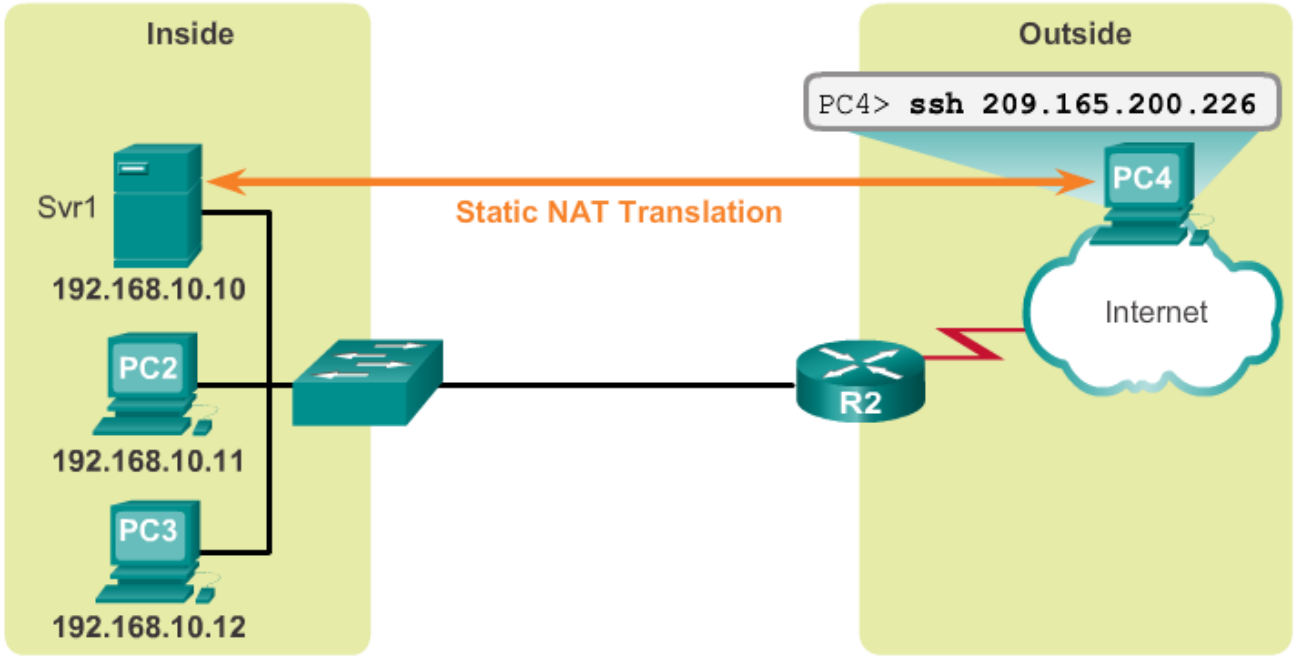
Types Of NAT

Static NAT

Static NAT

Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



Dynamic NAT

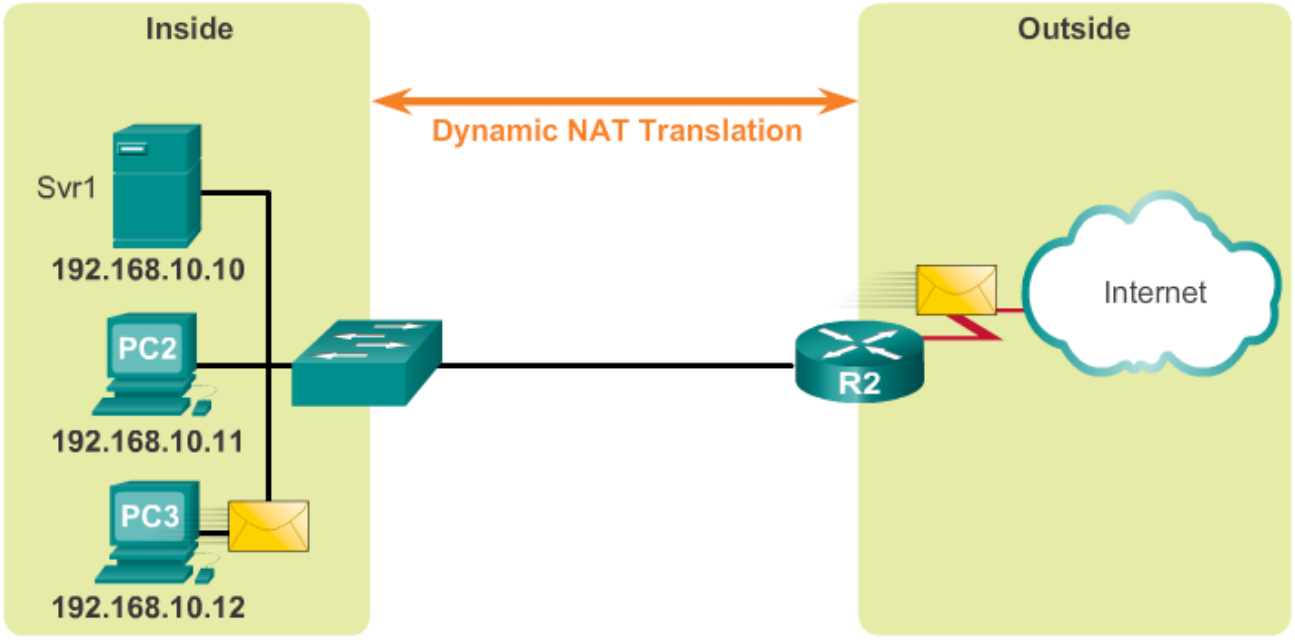
- Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis
- When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool
- Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions

Types Of NAT

Dynamic NAT

Dynamic NAT

IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230



Types Of NAT

Port Address Translation NAT (PAT)

- PAT maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
- PAT uses the pair source port and source IP address to keep track of what traffic belongs to what internal client
- PAT is also known as NAT overload
- By also using the port number, PAT is able to forward the response packets to the correct internal device
- The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session

Types Of NAT

Comparing NAT and PAT

- NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses
- PAT modifies both the address and the port number
- NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address given by the host on the public network
- With PAT, there is generally only one or a very few publicly exposed IPv4 addresses
- PAT is also able to translate protocols that don't use port numbers such as ICMP. Each one of these protocols are supported differently by PAT

Benefits Of NAT

Benefits of NAT

- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes
- Provides network security

Disadvantages of NAT

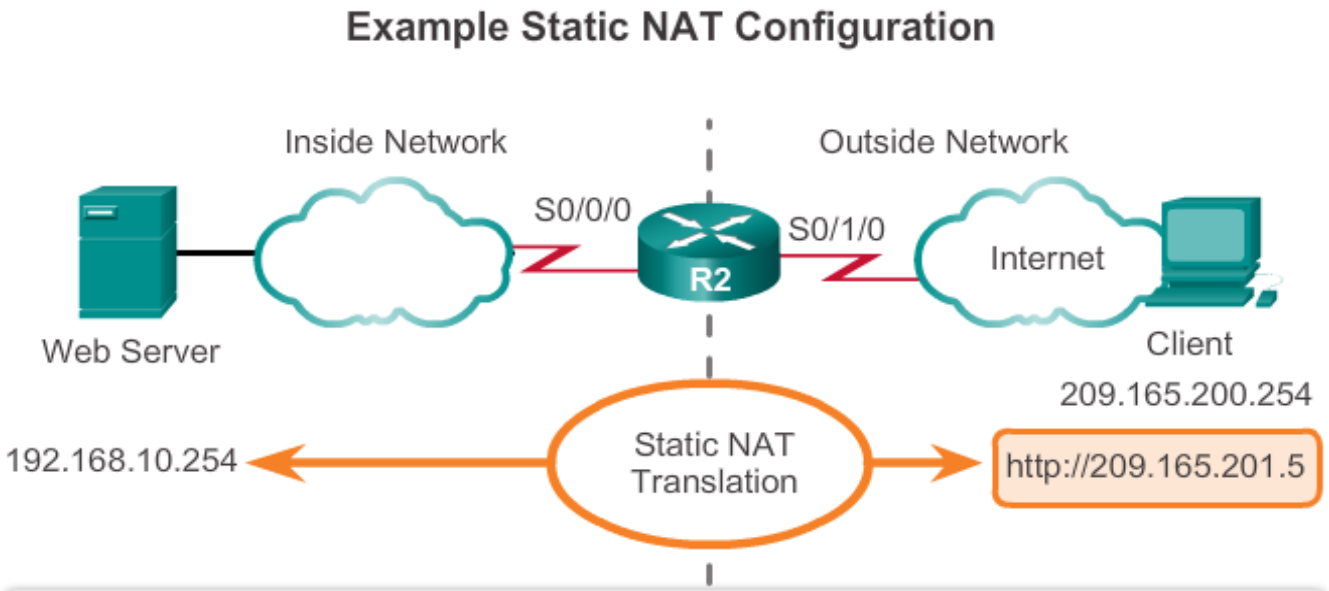
Disadvantages of NAT

- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted

Configuring Static NAT

- There are two basic tasks when configuring static NAT translations:
  - Create the mapping between the inside local and outside local addresses
  - Define which interface belong to the inside network and which belong to the outside network

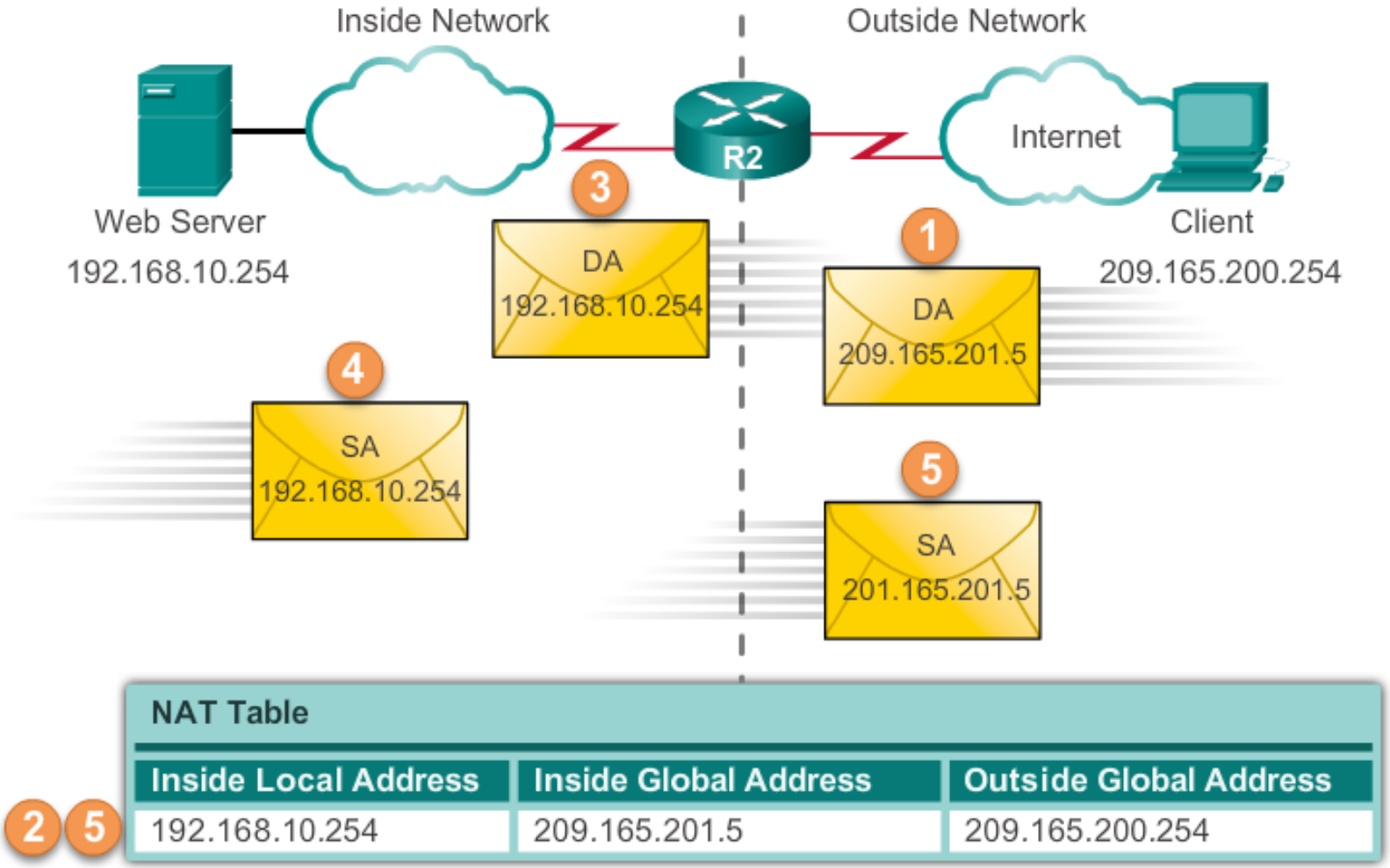
Configuring Static NAT




```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Configuring Static NAT

Analyzing Static NAT



Verifying Static NAT

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

Configuring Static NAT
Verifying Static NAT

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

Dynamic NAT Operation

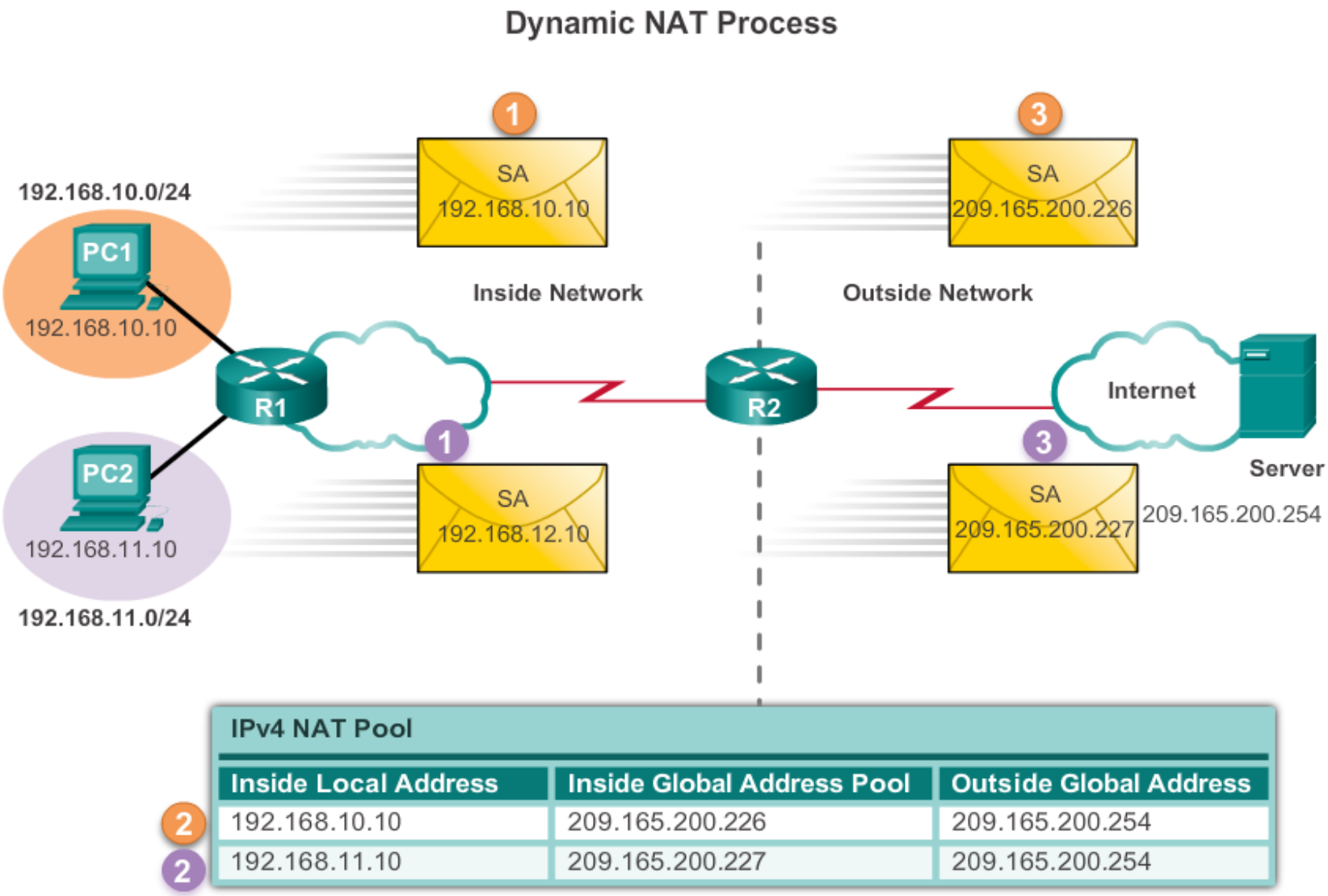
- The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come first-served basis
- With dynamic NAT, a single inside address is translated to a single outside address
- The pool must be large enough to accommodate all inside devices
- A device won't be able to communicate to any external networks if no addresses are available in the pool

Configuring Dynamic NAT

Dynamic NAT Configuration Steps

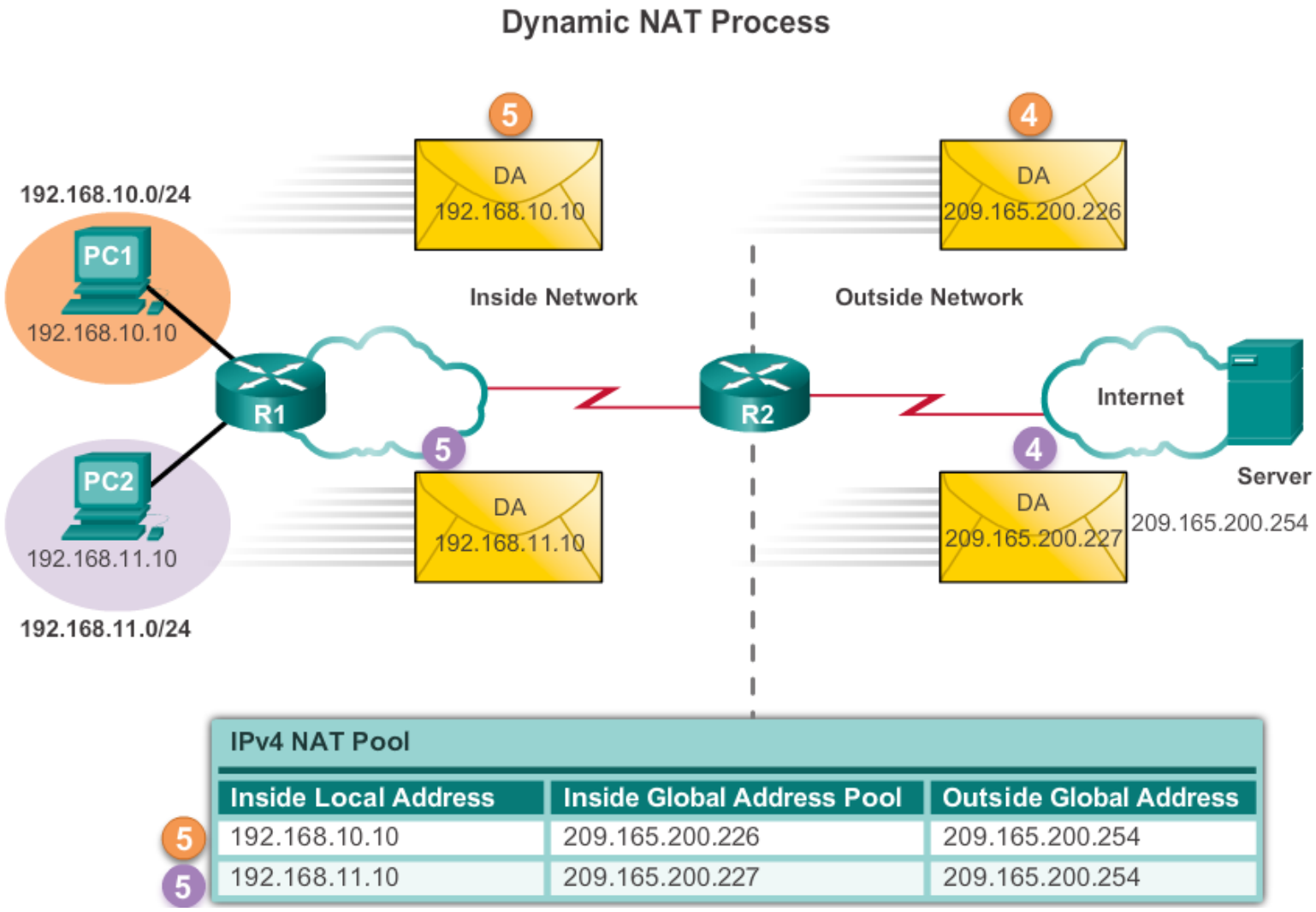
Dynamic NAT Configuration Steps	
Step 1	Define a pool of global addresses to be used for translation. **ip nat pool** *name start-ip end-ip* { **netmask***netmask* | **prefix-length** *prefix-length* }
Step 2	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source [source-wildcard]*
Step 3	Establish dynamic source translation, specifying the access list and pool defined in prior steps. **ip nat inside source list** *access-list-number* **pool** *name*
Step 4	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 5	Identify the outside interface. **interface** *type number* **ip nat outside**

Analyzing Dynamic NAT



Configuring Dynamic NAT

Analyzing Dynamic NAT



Configuring Dynamic NAT

Verifying Dynamic NAT

Verifying Dynamic NAT with show ip nat translations

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---    ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

Configuring Dynamic NAT

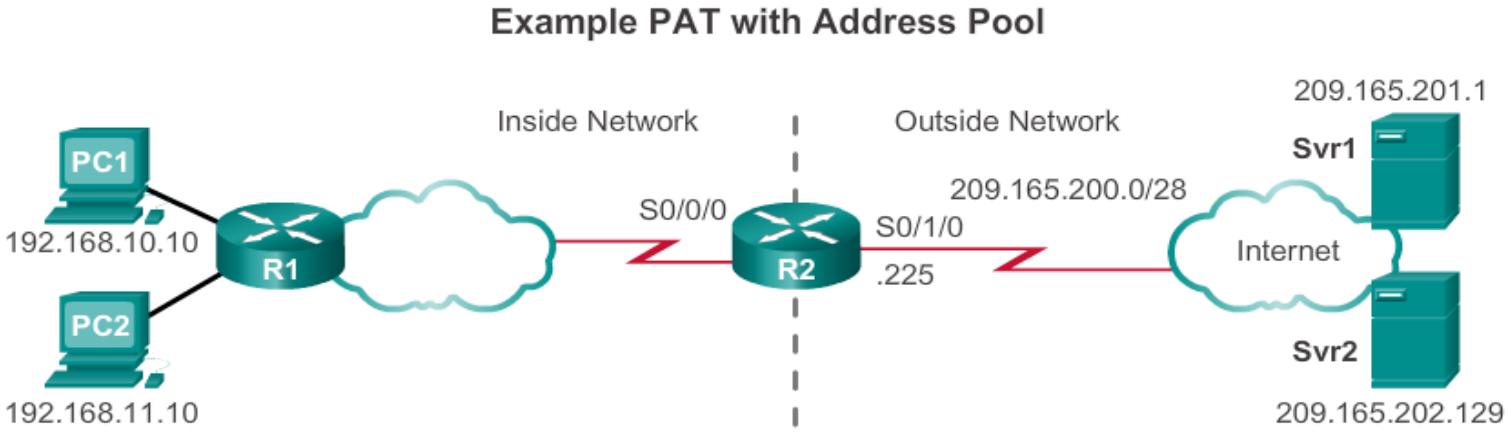
Verifying Dynamic NAT

Verifying Dynamic NAT with show ip nat statistics

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Configuring Port Address Translation (PAT)

Configuring PAT: Address Pool



Define a pool of public IPv4 addresses under the pool name NAT-POOL2.
R2(config)# **ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224**
Define which addresses are eligible to be translated.
R2(config)# **access-list 1 permit 192.168.0.0 0.0.255.255**
Bind NAT-POOL2 with ACL 1.
R2(config)# **ip nat inside source list 1 pool NAT-POOL2 overload**

Identify interface serial 0/0/0 as an inside NAT interface.
R2(config)# **interface Serial0/0/0**
R2(config-if)# **ip nat inside**

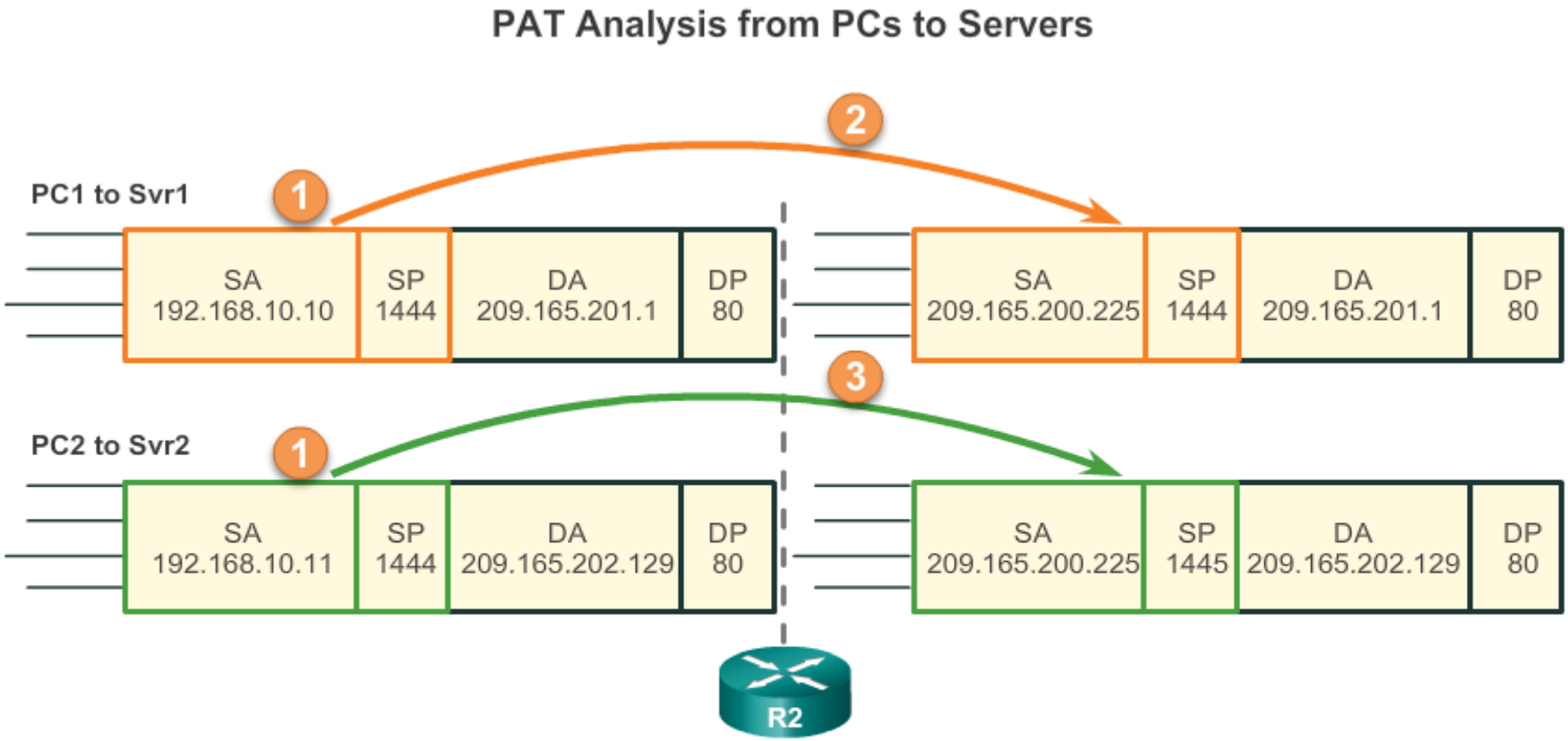
Identify interface serial 0/1/0 as the outside NAT interface.
R2(config)# **interface Serial0/1/0**
R2(config-if)# **ip nat outside**

Configuring Port Address Translation (PAT)

Configuring PAT: Single Address

Step 1	Define a standard access list permitting the addresses that should be translated. **access-list** *access-list-number* **permit** *source*[*source-wildcard*]
Step 2	Establish dynamic source translation, specifying the ACL, exit interface and overload options. **ip nat inside source list***access-list-number***interface** *type number* **overload**
Step 3	Identify the inside interface. **interface** *type number* **ip nat inside**
Step 4	Identify the outside interface. **interface** *type number* **ip nat outside**

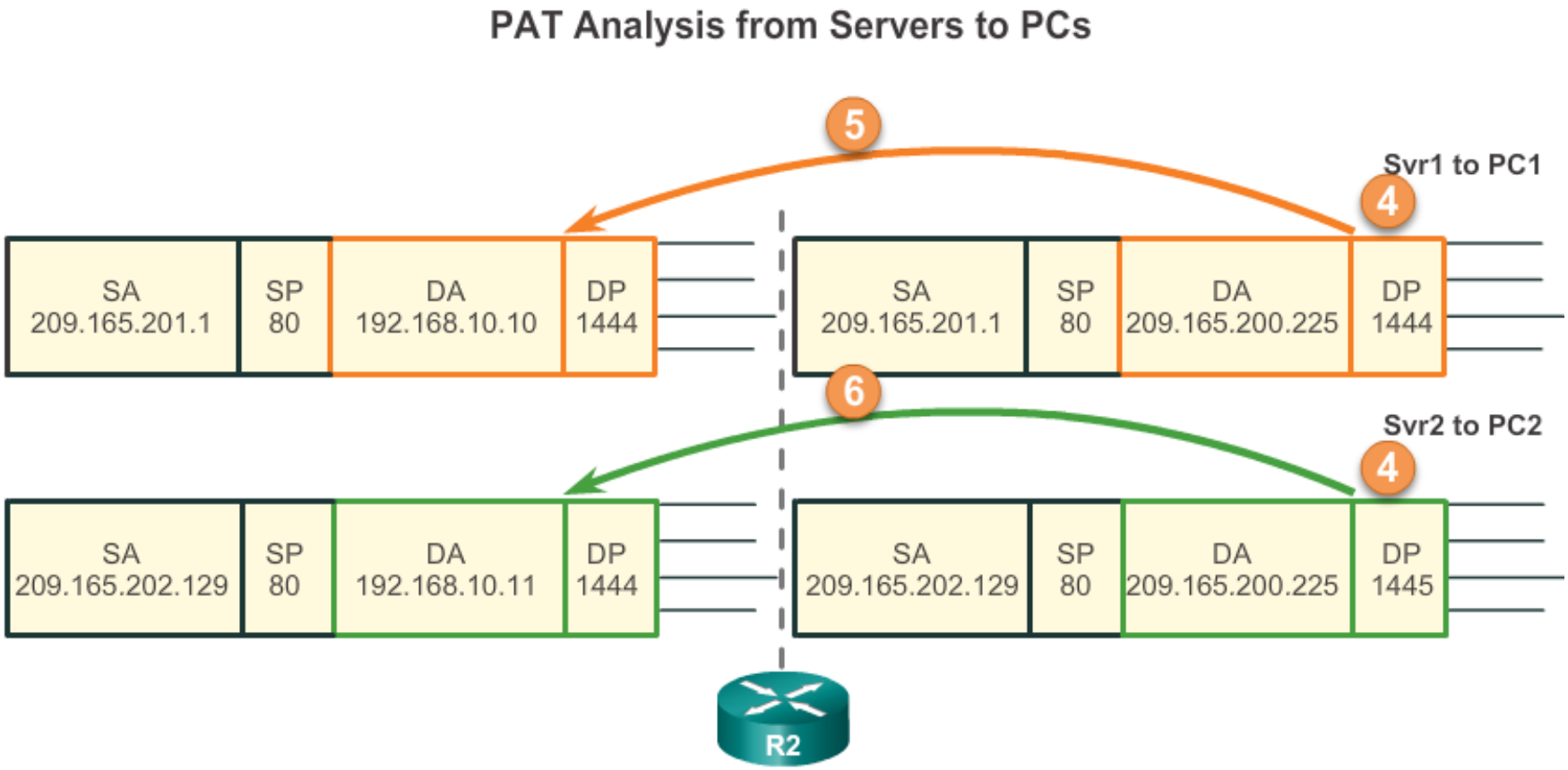
Analyzing PAT



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Analyzing PAT



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

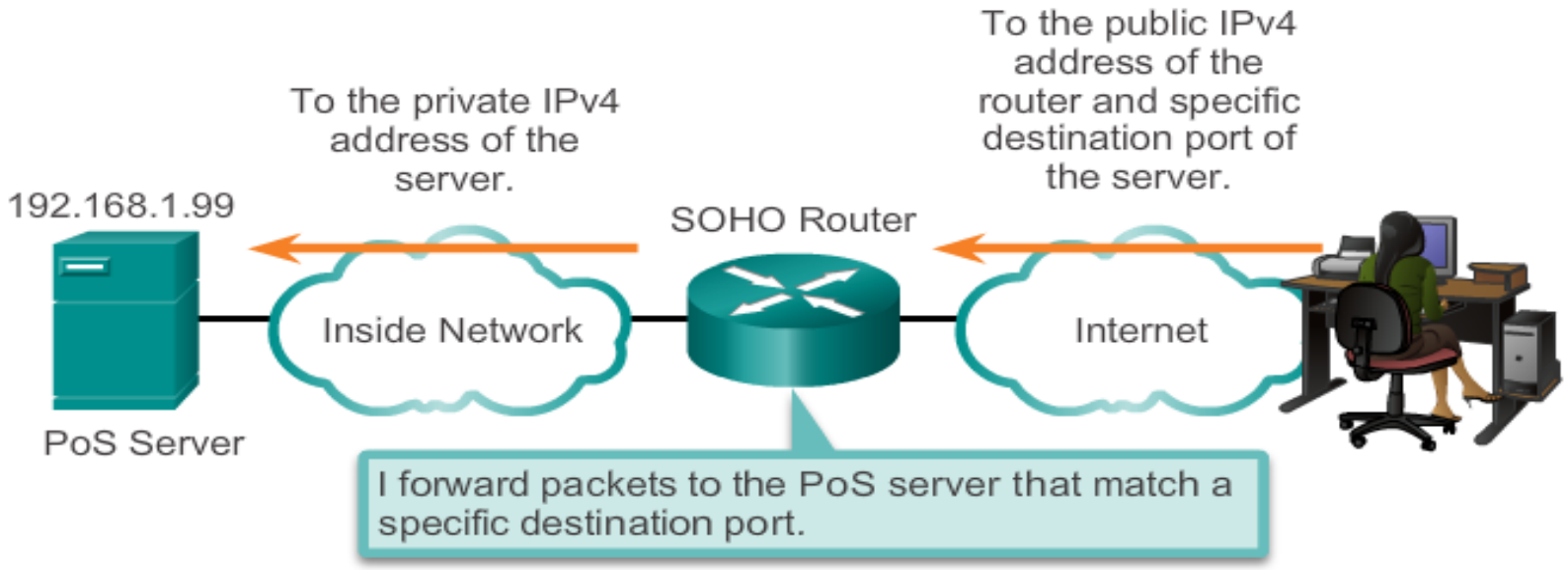
Configuring Port Address Translation (PAT)
Verifying PAT

Verifying PAT Translations

```
R2# show ip nat translations
Pro Inside global          Inside local        Outside local       Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839 209.165.201.1:80    209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558 209.165.202.129:80  209.165.202.129:80
R2#
```

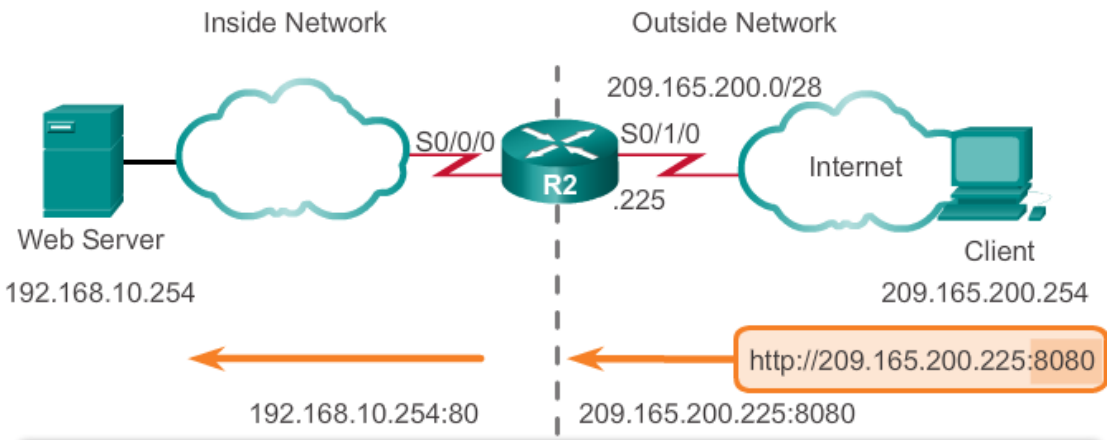
Port Forwarding

- Port forwarding is the act of forwarding a network port from one network node to another
- A packet sent to the public IP address and port of a router can be forwarded to a private IP address and port in inside network
- This is helpful in situations where servers have private addresses, not reachable from the outside networks



Configuring Port Forwarding with IOS

- In IOS, Port forwarding is essentially a static NAT translation with a specified TCP or UDP port number



Establishes static translation between an inside local address and local port and an inside global address and global port.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```