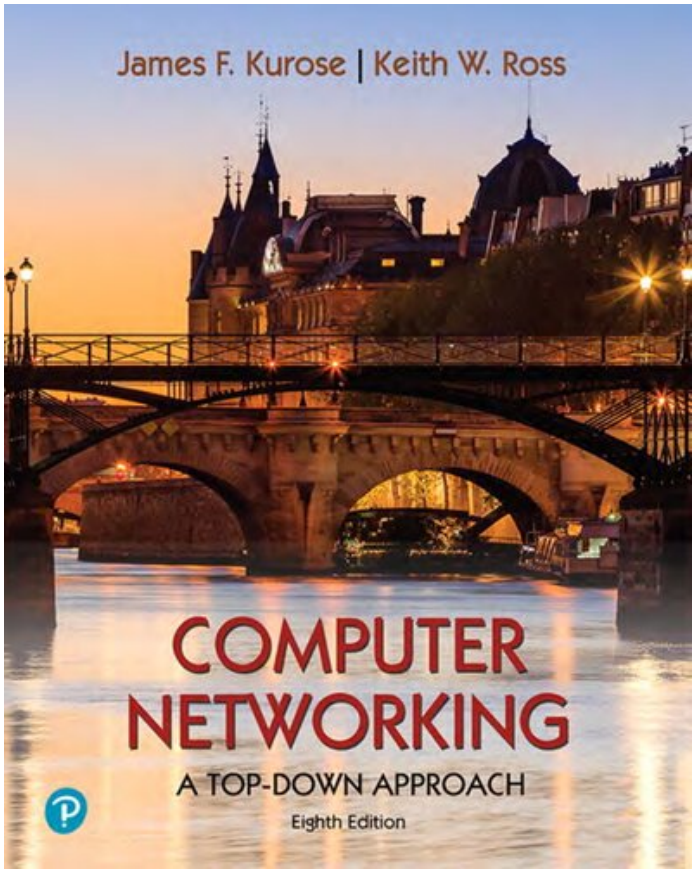
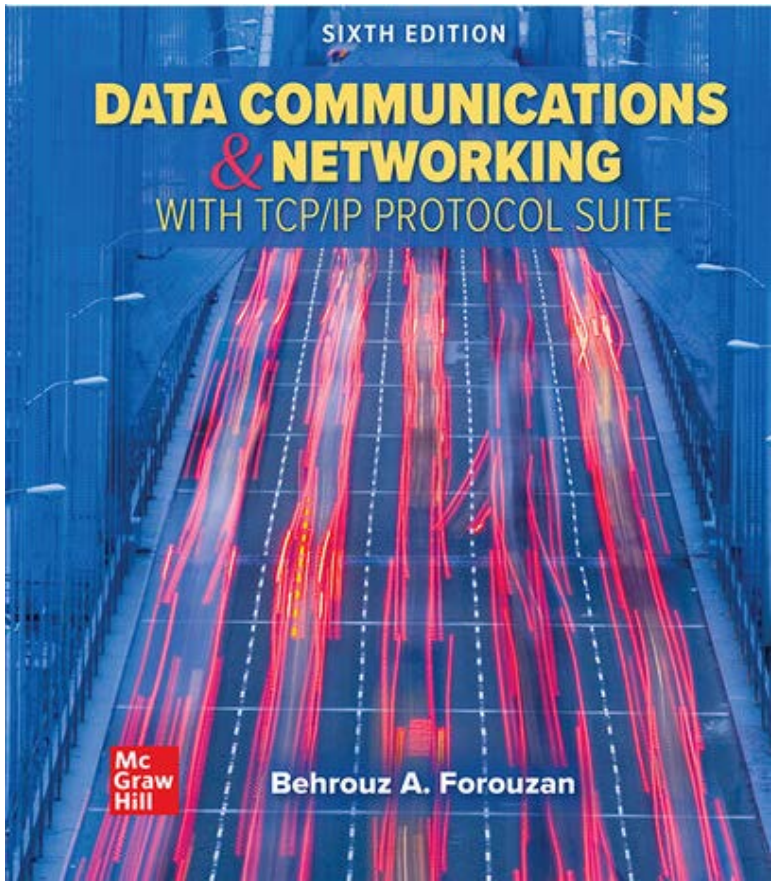
I3304
Network administration and security

Ahmad Fadlallah

Reference Textbooks





Outline

- Introduction
  - Introduction to the course
  - Recall Network Basics (I2208)
- Network Layer
  - Static Routing
  - Dynamic Routing Algorithm
  - Dynamic Routing Protocols
  - NAT (Network Address Translation)
- Transport Layer
  - Function of the transport layer
  - UDP Protocol
  - TCP Protocol
    - Connection management
    - Flow control
    - Congestion control
- Application Layer
  - HTTP protocol
  - FTP protocol
  - Mail protocols
  - DNS
- Introduction to Security
  - Security services
  - Cryptography
  - Digital Signature
  - Principle of network security protocols

References

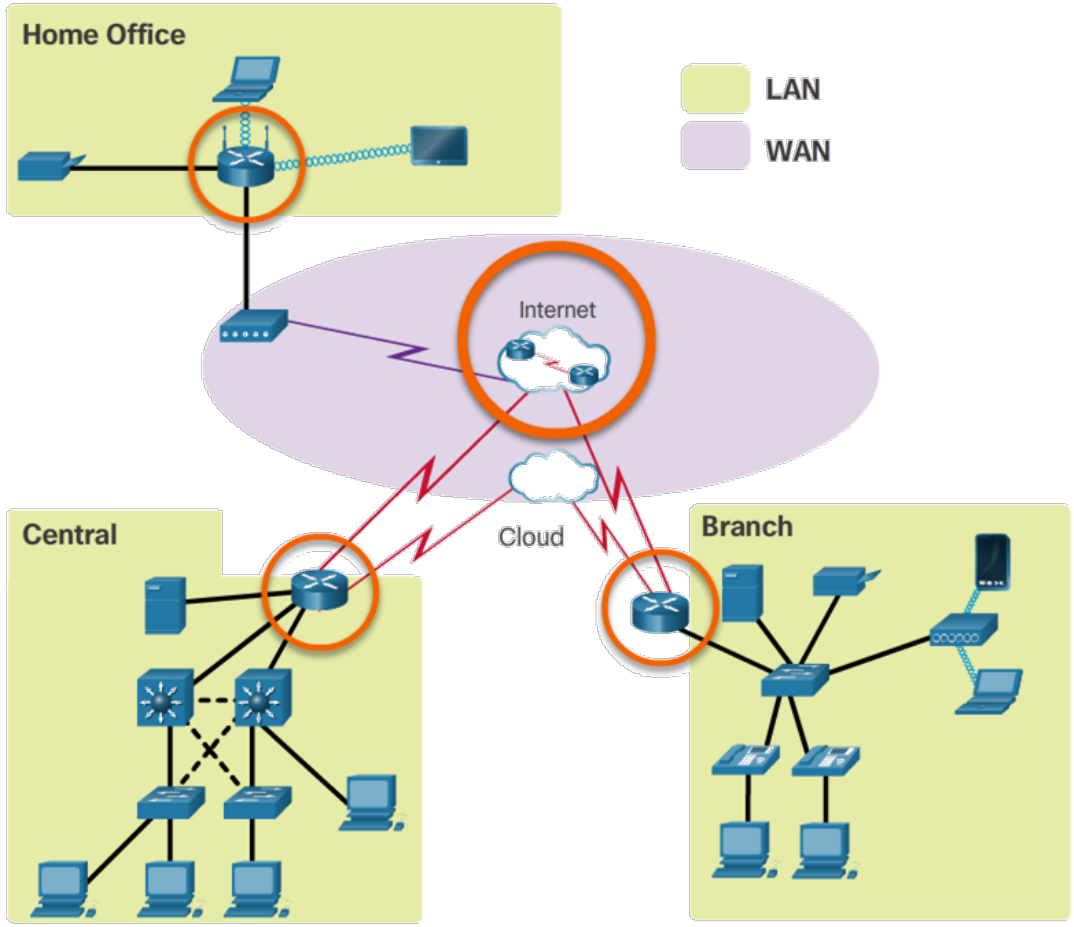
- The slides are based on the:
  - Cisco Networking Academy Program, Routing and Switching Essentials v6.0, Chapter 1: Routing Concepts
  - Jim Kurose, Keith Ross Slides for the Computer Networking: A Top-Down Approach, 8th edition, Pearson, 2020

Network Layer
Static Routing

Introduction

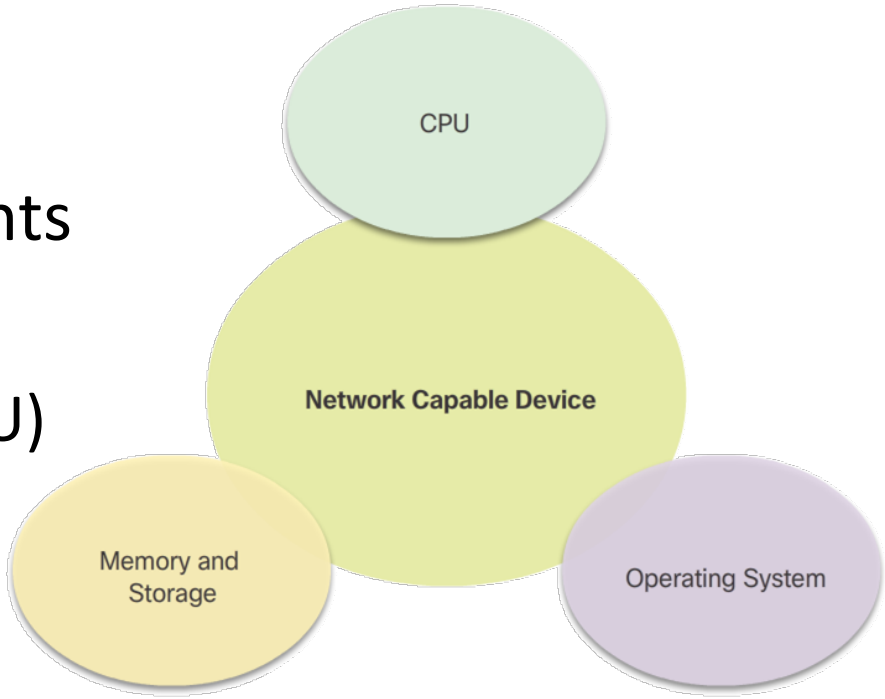
Router Functions/ Why Routing?

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



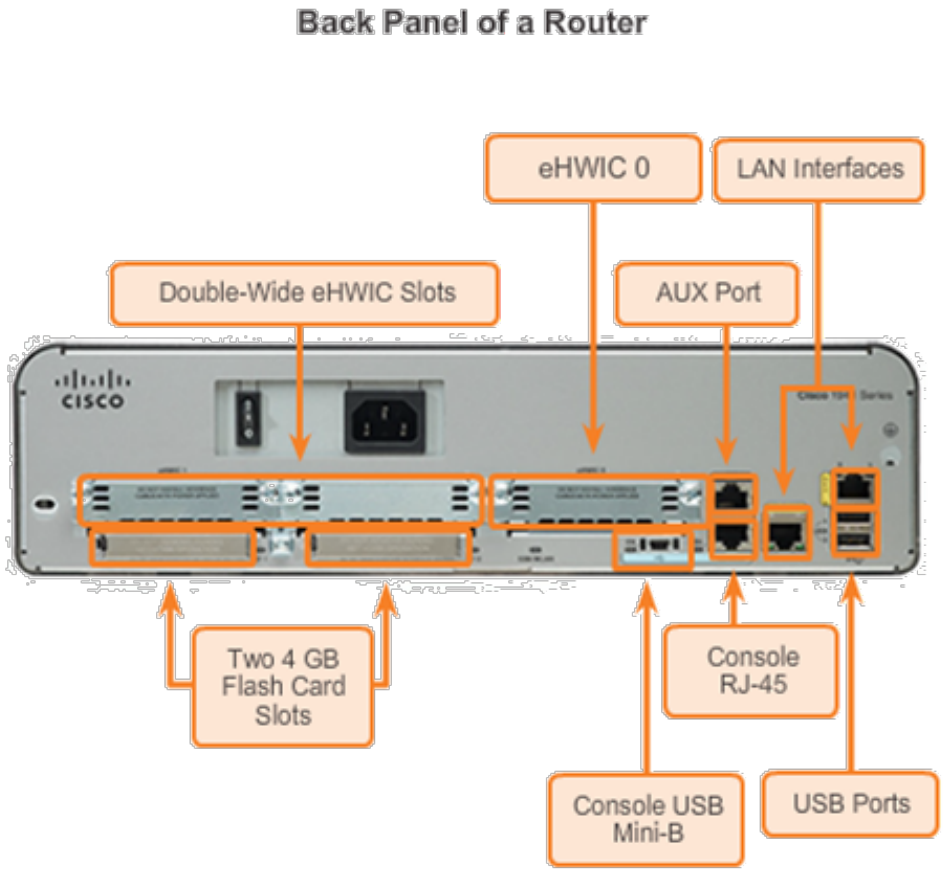
Router Functions/ Routers are Computers

- Routers are specialized computers containing the following required components to operate:
  - Central processing unit (CPU)
  - Operating system (OS) - Example: Cisco IOS
  - Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)



Router Functions/ Routers are Computers (cont.)

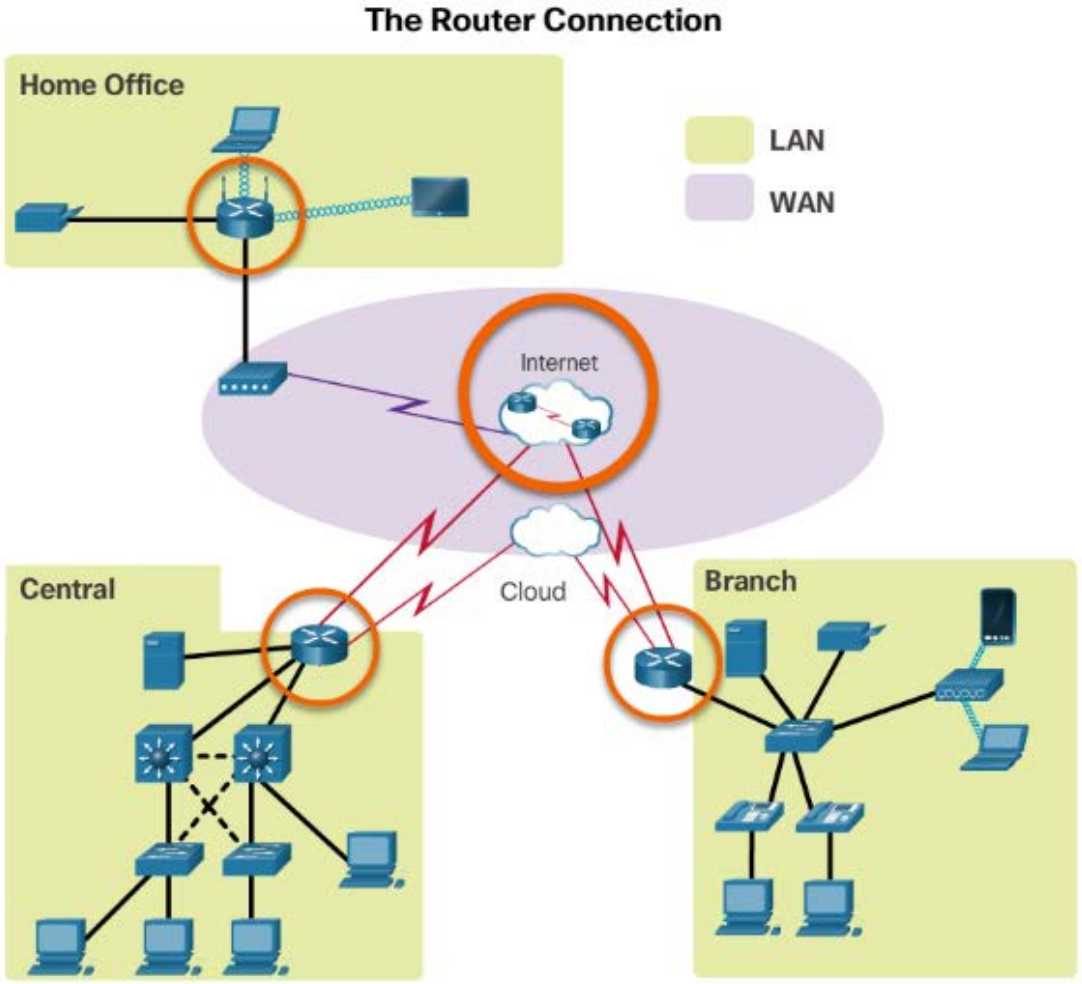
- Routers use specialized ports and network interface cards to **interconnect** to other networks.



Router Functions
Routers are Computers

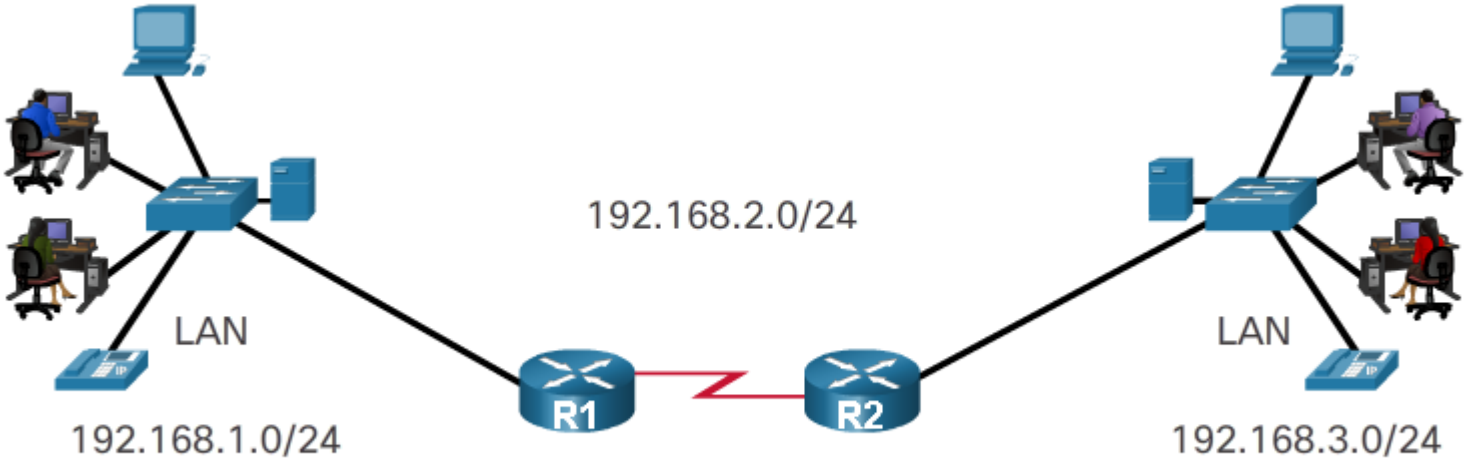
Memory	Description
Random Access Memory (RAM)	Volatile memory that provides temporary storage for various applications and processes including: • Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
Read-Only Memory (ROM)	Non-volatile memory that provides permanent storage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

Router Functions
Routers Interconnect Networks



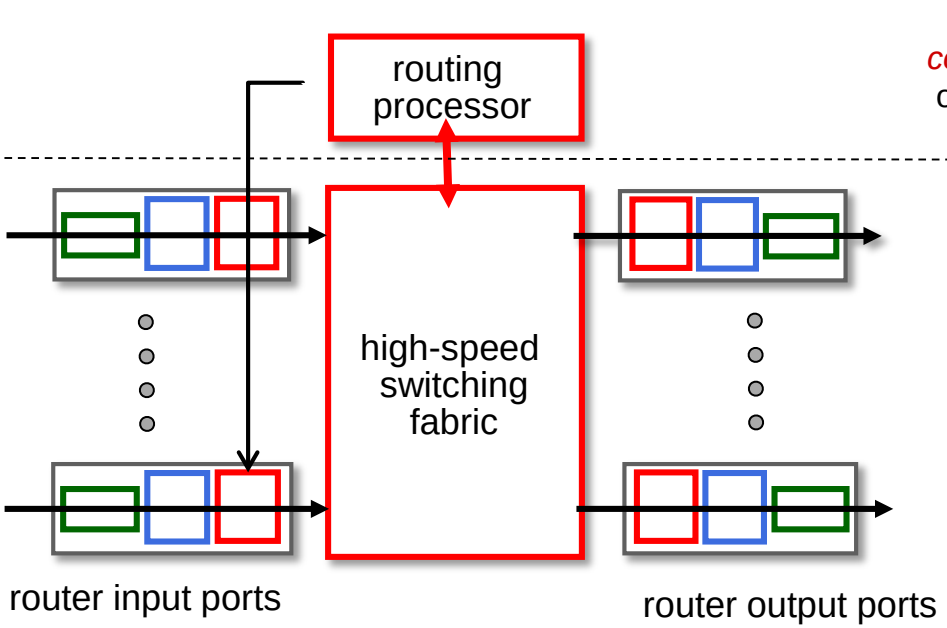
Router Functions
Routers Choose Best Paths

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

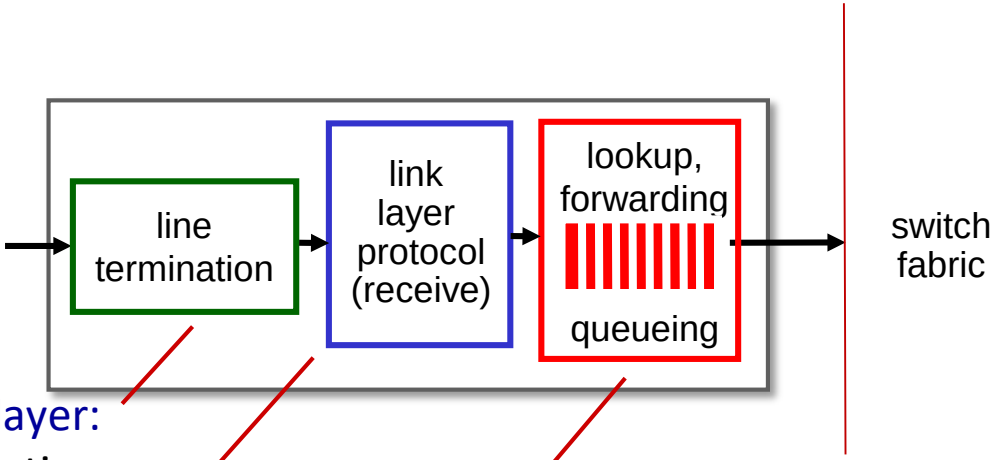


Router architecture overview

high-level view of generic router architecture:



Input port functions



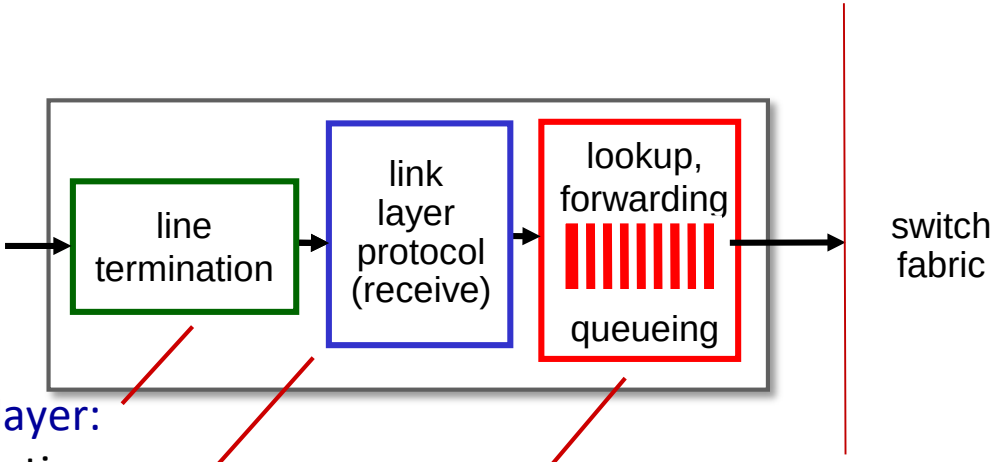
physical layer:
bit-level reception

link layer:
e.g., Ethernet

decentralized switching:

- using header field values, lookup output port using forwarding table in input port memory *("match plus action")*
- goal: complete input port processing at 'line speed'
- input port queuing: if datagrams arrive faster than forwarding rate into switch fabric

Input port functions



physical layer:
bit-level reception

link layer:
e.g., Ethernet

decentralized switching:

- using header field values, lookup output port using forwarding table in input port memory *("match plus action")*
- destination-based forwarding: forward based only on destination IP address (traditional)
- generalized forwarding: forward based on any set of header field values

Destination-based forwarding

forwarding table

Destination Address Range	Link Interface
11001000 00010111 00010000 00000000 through 11001000 00010111 00010000 00000100	0
11001000 00010111 00010000 00000101 through 11001000 00010111 00010000 00000111	3
11001000 00010111 00011000 11111111	
11001000 00010111 00011001 00000000 through 11001000 00010111 00011111 11111111	2
otherwise	3

Q: but what happens if ranges don't divide up so nicely?

Longest prefix matching

longest prefix match

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011** ********	2
otherwise	3

examples:

11001000 00010111 00010110 10100001 which interface?

11001000 00010111 00011000 10101010 which interface?

Longest prefix matching

longest prefix match

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010*** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011*** ********	2
otherwise	3

match!

examples:

11001000 00010111 00010110 10100001 which interface?

11001000 00010111 00011000 10101010 which interface?

Longest prefix matching

longest prefix match

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011** ********	2
otherwise	3

match!

examples:

11001000 00010110 10100001	which interface?
11001000 00010111 00011000 10101010	which interface?

Longest prefix matching

longest prefix match

when looking for forwarding table entry for given destination address, use *longest* address prefix that matches destination address.

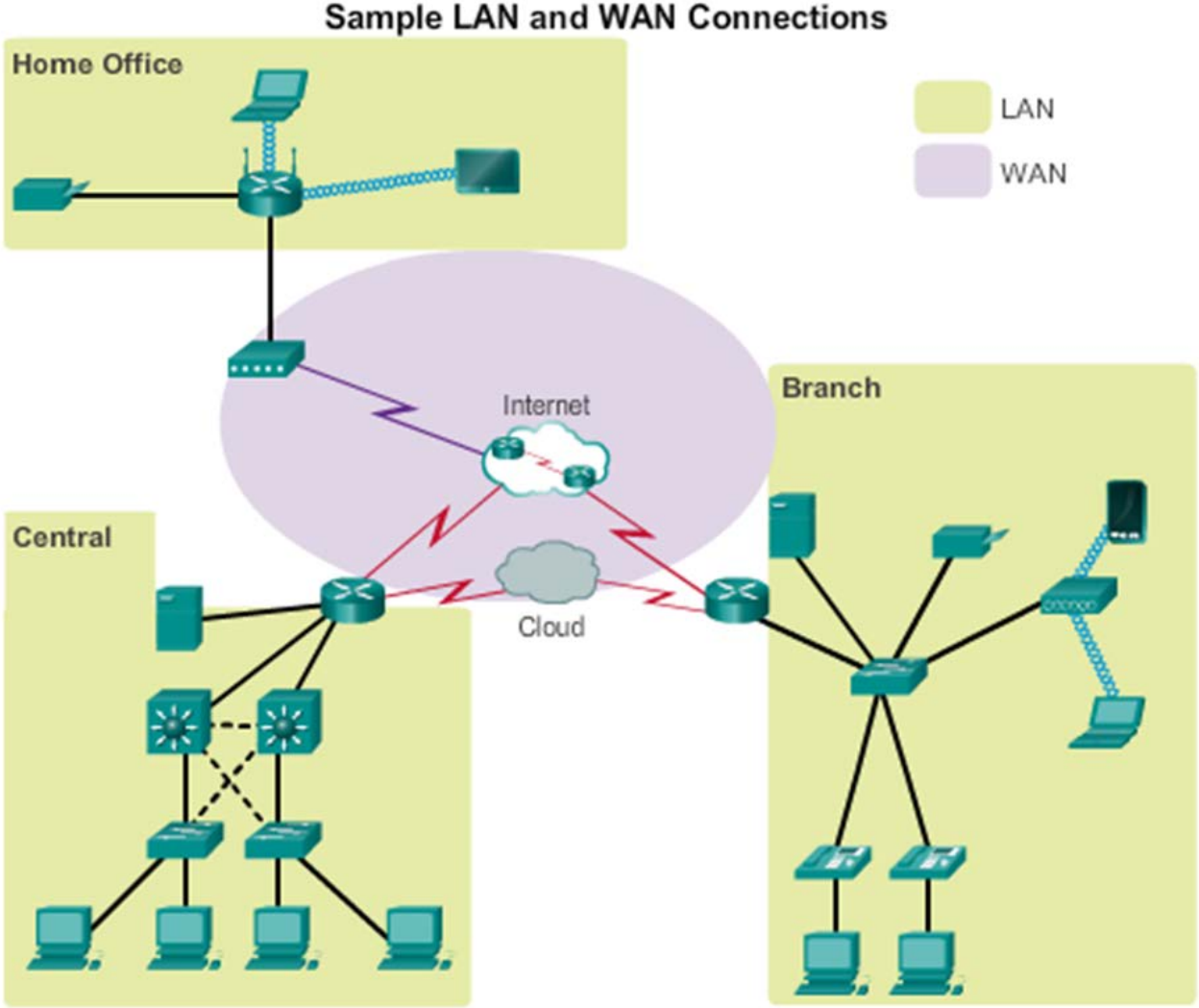
Destination Address Range	Link interface
11001000 00010111 00010** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011** ********	2
otherwise *	3

match!

examples:

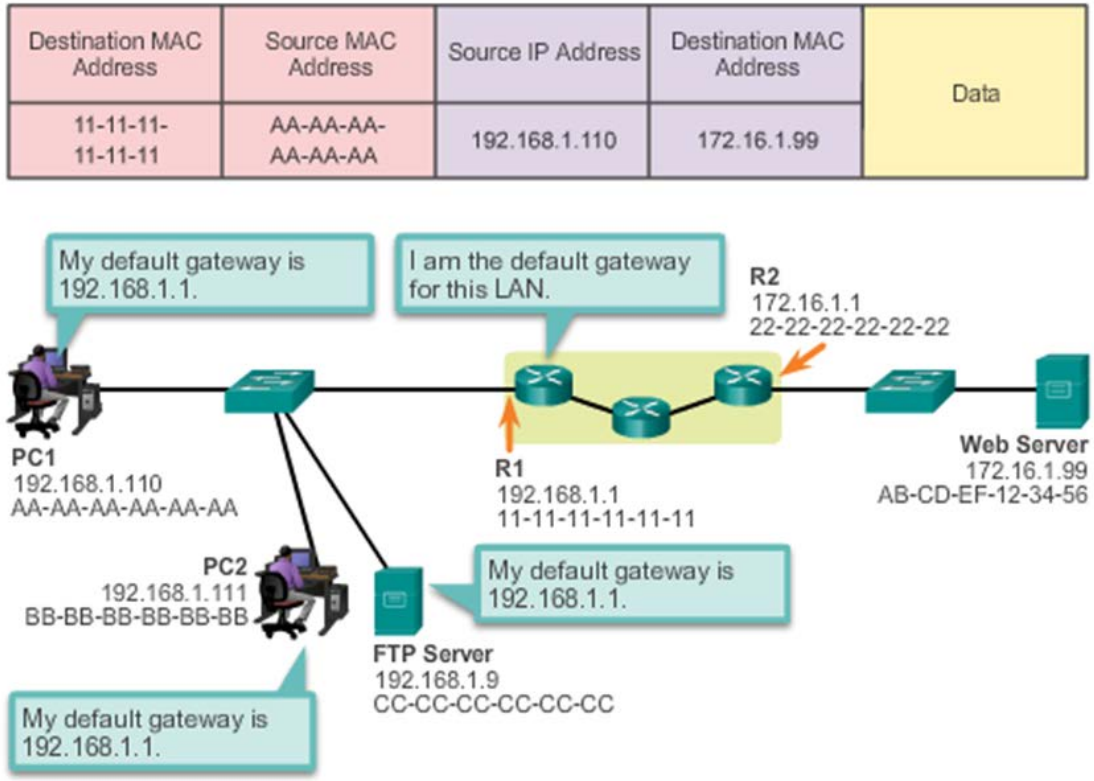
11001000 00010111 00010110 10100001	which interface?
11001000 00010111 00011000 10101010	which interface?

Connect Devices
Connect to a Network



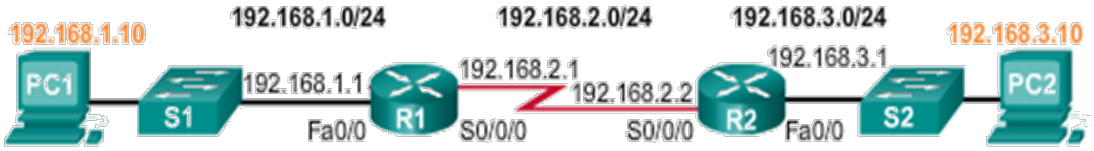
Connect Devices
Default Gateways

- To enable network access devices, must be configured with the following IP address information:
  - IP address - Identifies a unique host on a local network.
  - Subnet mask - Identifies the host's network subnet.
  - Default gateway - Identifies the router a packet is sent to when the destination is not on the same local network subnet.



Connect Devices
Document Network Addressing

- **Network documentation** should include at least the following in a topology diagram and addressing table:
  - Device names
  - Interfaces
  - IP addresses and subnet masks
  - Default gateways



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

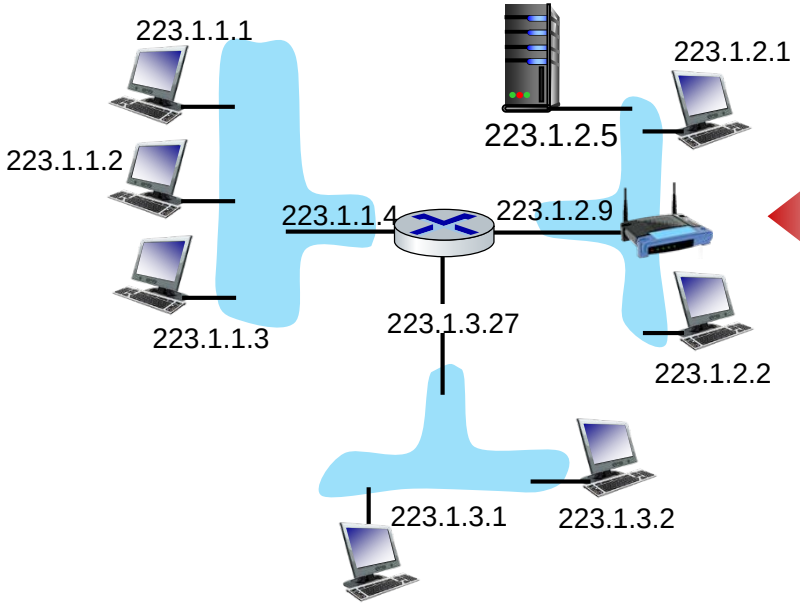
Connect Devices
Enable IP on a Host

- Statically Assigned IP address – The host is manually assigned an *IP address*, *subnet mask* and *default gateway*. A *DNS server* IP address can also be assigned.
  - ⊙ Used to identify specific network resources such as network servers and printers.
  - ⊙ Can be used in very small networks with few hosts.
- Dynamically Assigned IP Address – IP Address information is dynamically assigned by a server using Dynamic Host Configuration Protocol (DHCP).
  - ⊙ Most hosts acquire their IP address information through DHCP.

DHCP: Dynamic Host Configuration Protocol

- **Goal**: host dynamically obtains IP address from network server when it "joins" network
  - Can renew its lease on address in use
  - Allows reuse of addresses (only hold address while connected/on)
  - Support for mobile users who join/leave network
- **DHCP overview**:
  - Host broadcasts DHCP DISCOVER message [optional]
  - DHCP server responds with DHCP OFFER message [optional]
  - Host requests IP address: DHCP REQUEST message
  - DHCP server sends address: DHCP ACK message

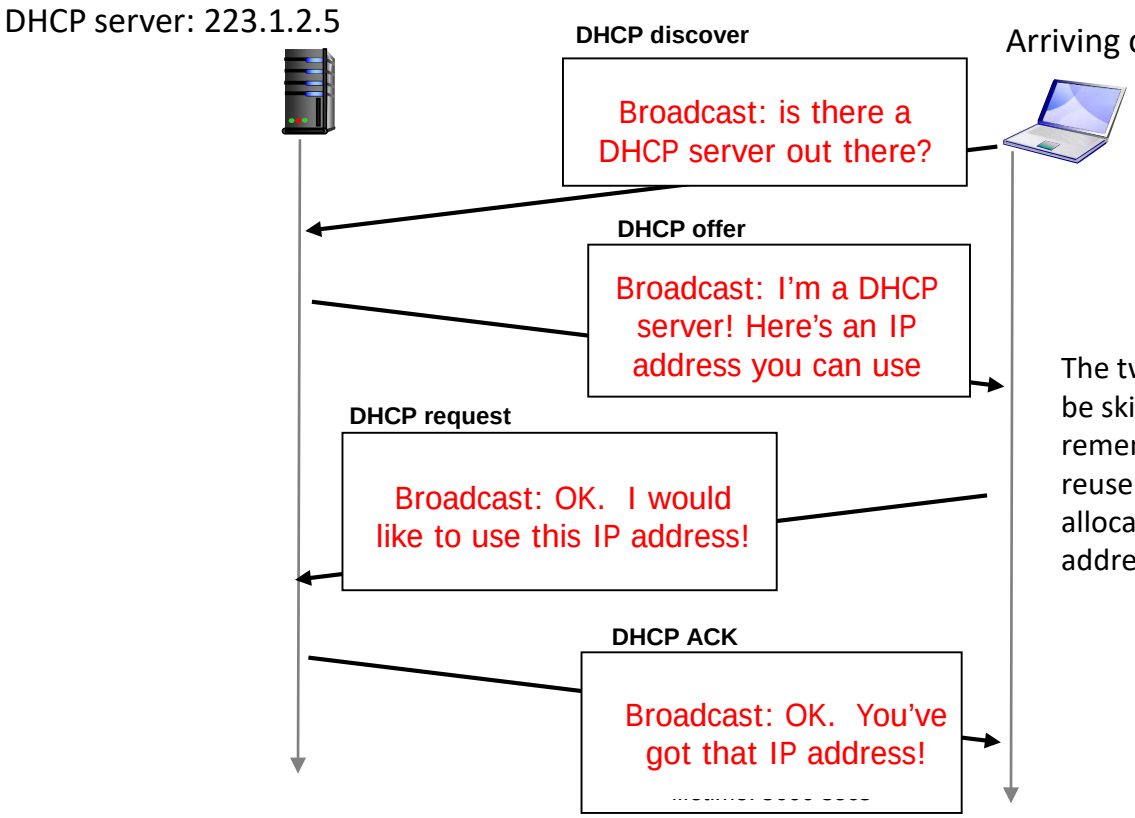
DHCP client-server scenario



Typically, DHCP server will be co-located in router, serving all subnets to which router is attached

arriving DHCP client needs address in this network

DHCP client-server scenario

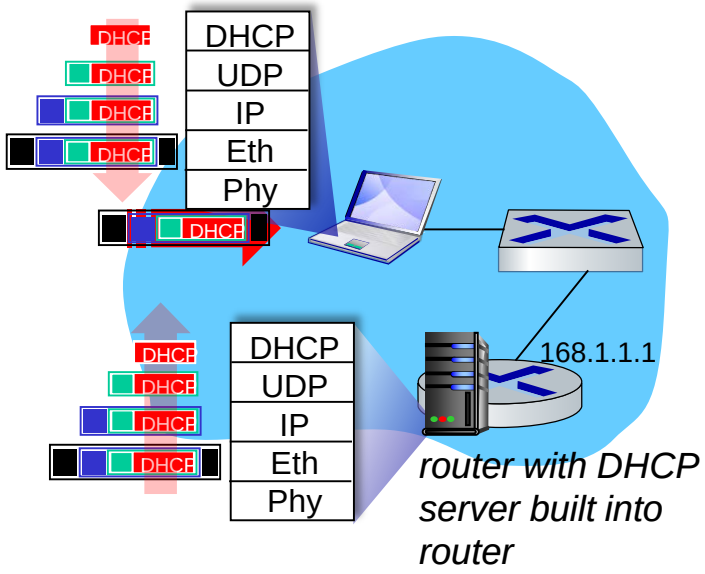


The two steps above can be skipped "if a client remembers and wishes to reuse a previously allocated network address" [RFC 2131]

DHCP: more than IP addresses

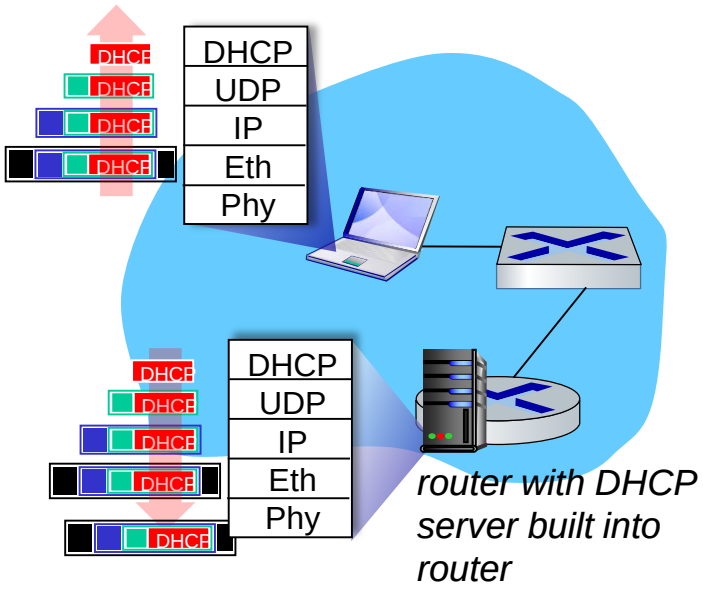
- DHCP can return more than just allocated IP address on subnet:
  - **Address of first-hop router for client**
  - **Name and IP address of DNS sever**
  - **Network mask**

DHCP: example



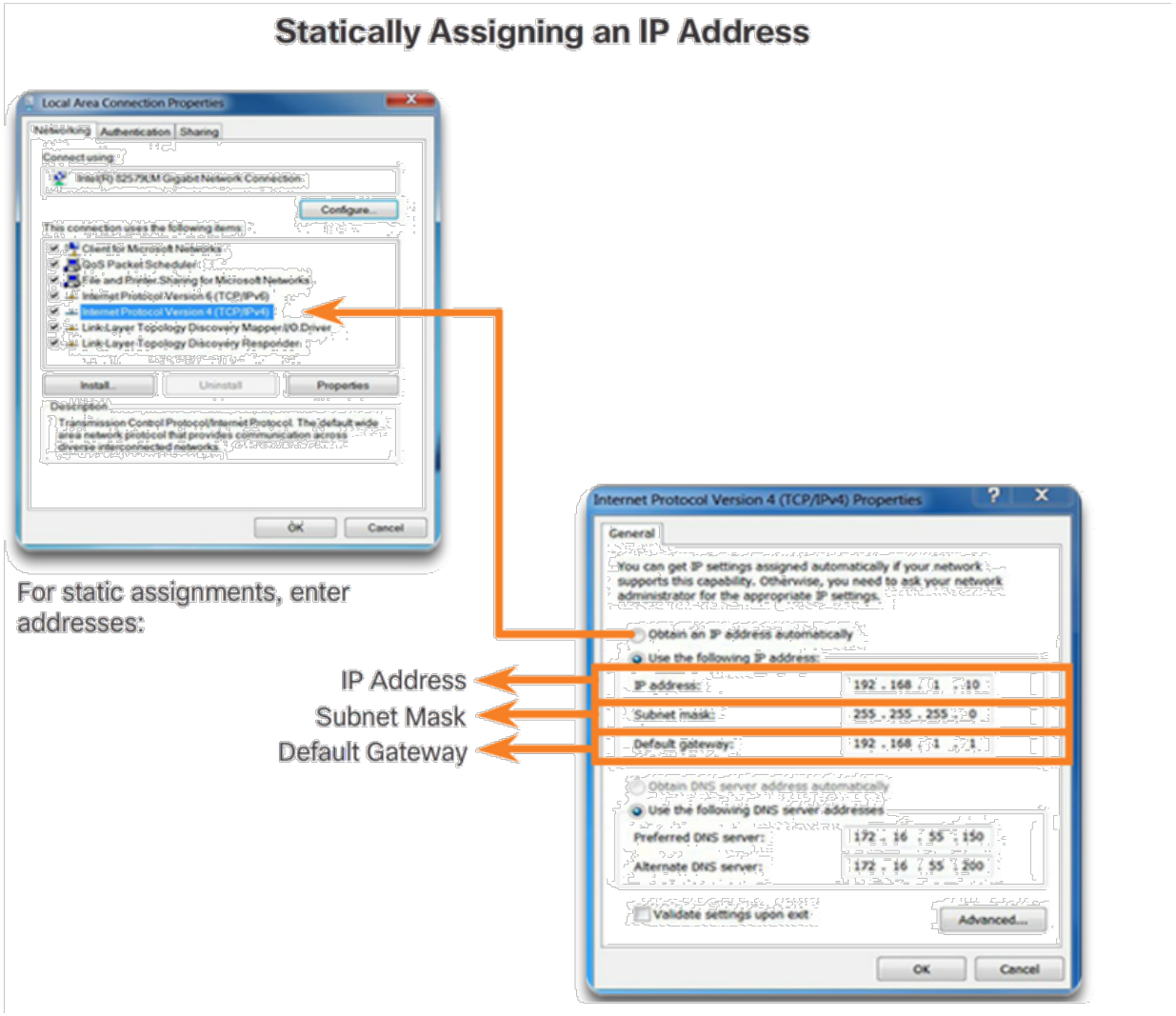
- Connecting laptop will use DHCP to get IP address, address of first-hop router, address of DNS server.
- **DHCP REQUEST** message encapsulated in UDP, encapsulated in IP, encapsulated in Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demux'ed to IP demux'ed, UDP demux'ed to DHCP

DHCP: example

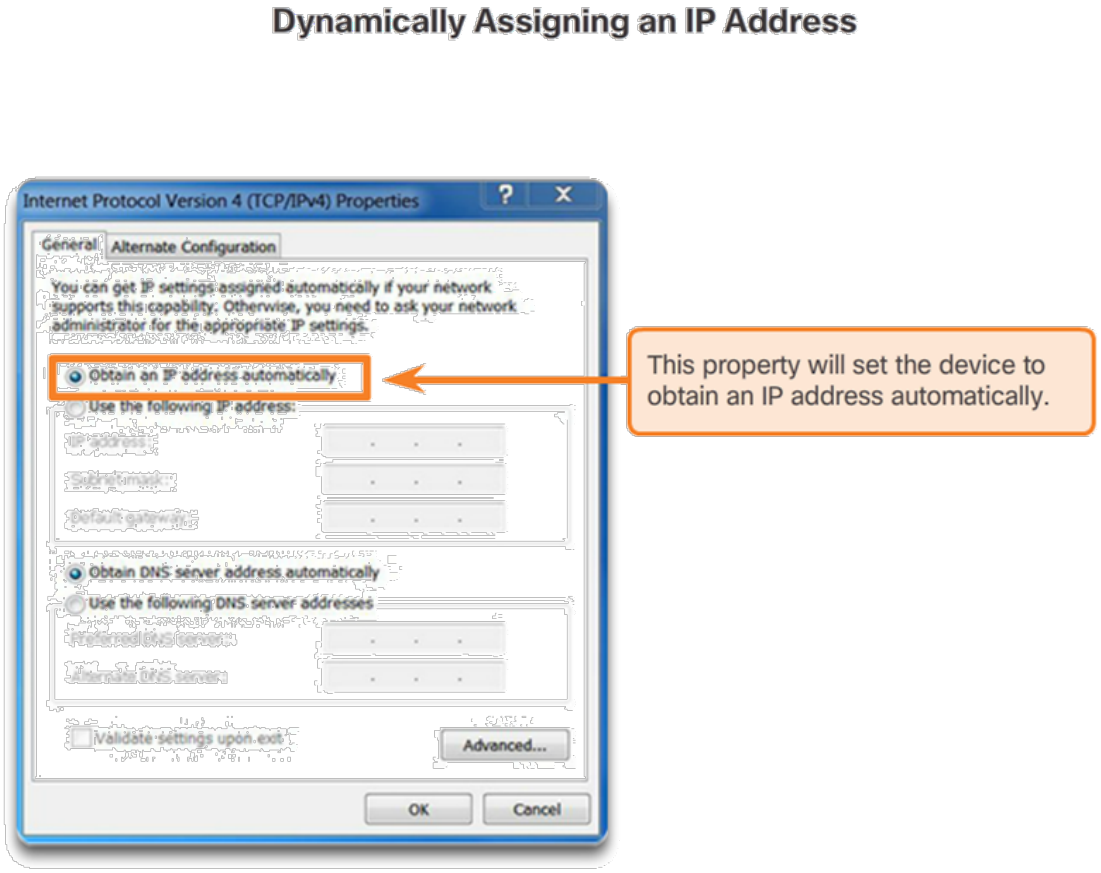


- DCP server formulates **DHCP ACK** containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- Encapsulated DHCP server reply forwarded to client, demuxing up to DHCP at client
- Client now knows its IP address, name and IP address of DNS server, IP address of its first-hop router

Connect Devices
Enable IP on a Host

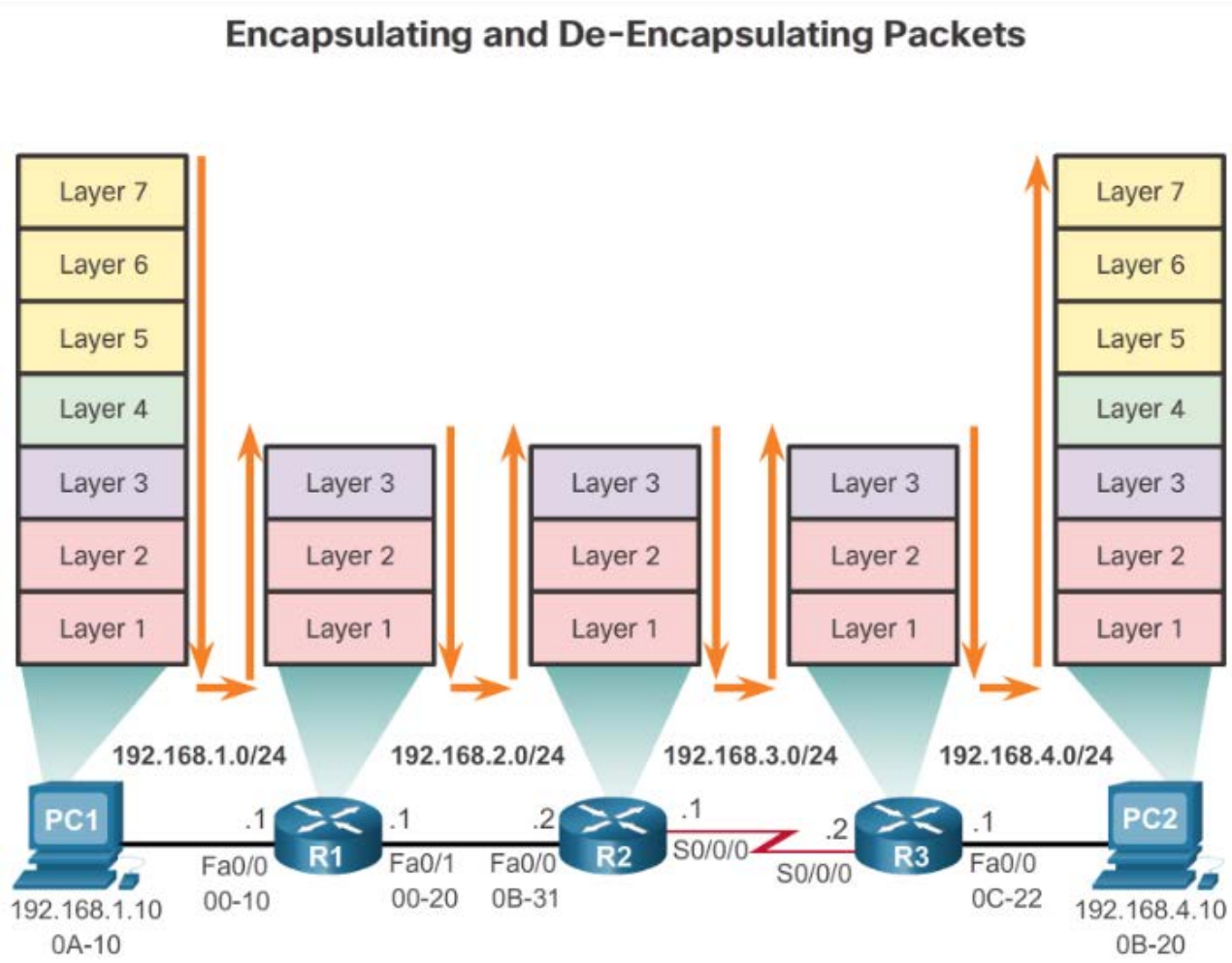


Connect Devices
Enable IP on a Host

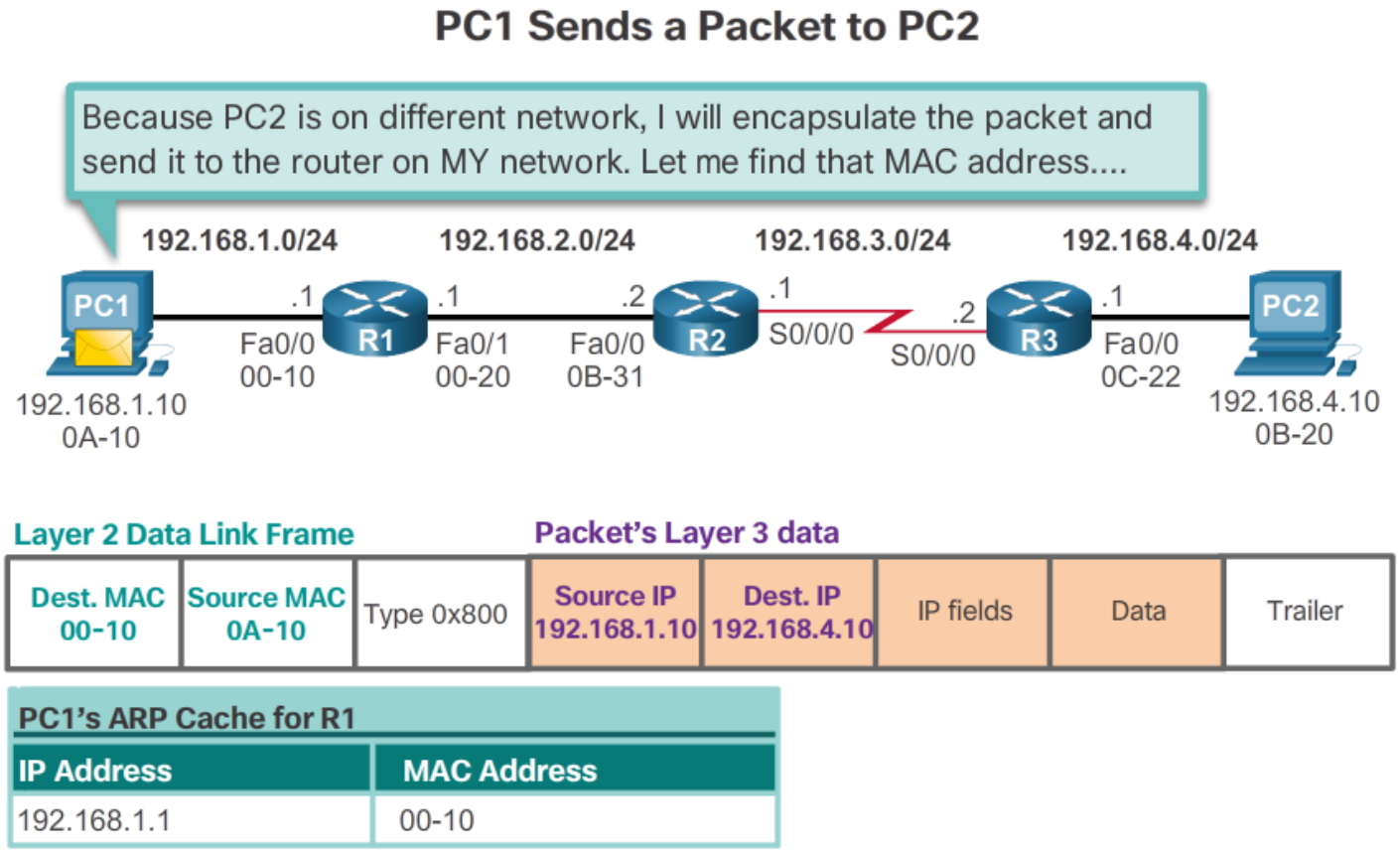


Routing Decisions

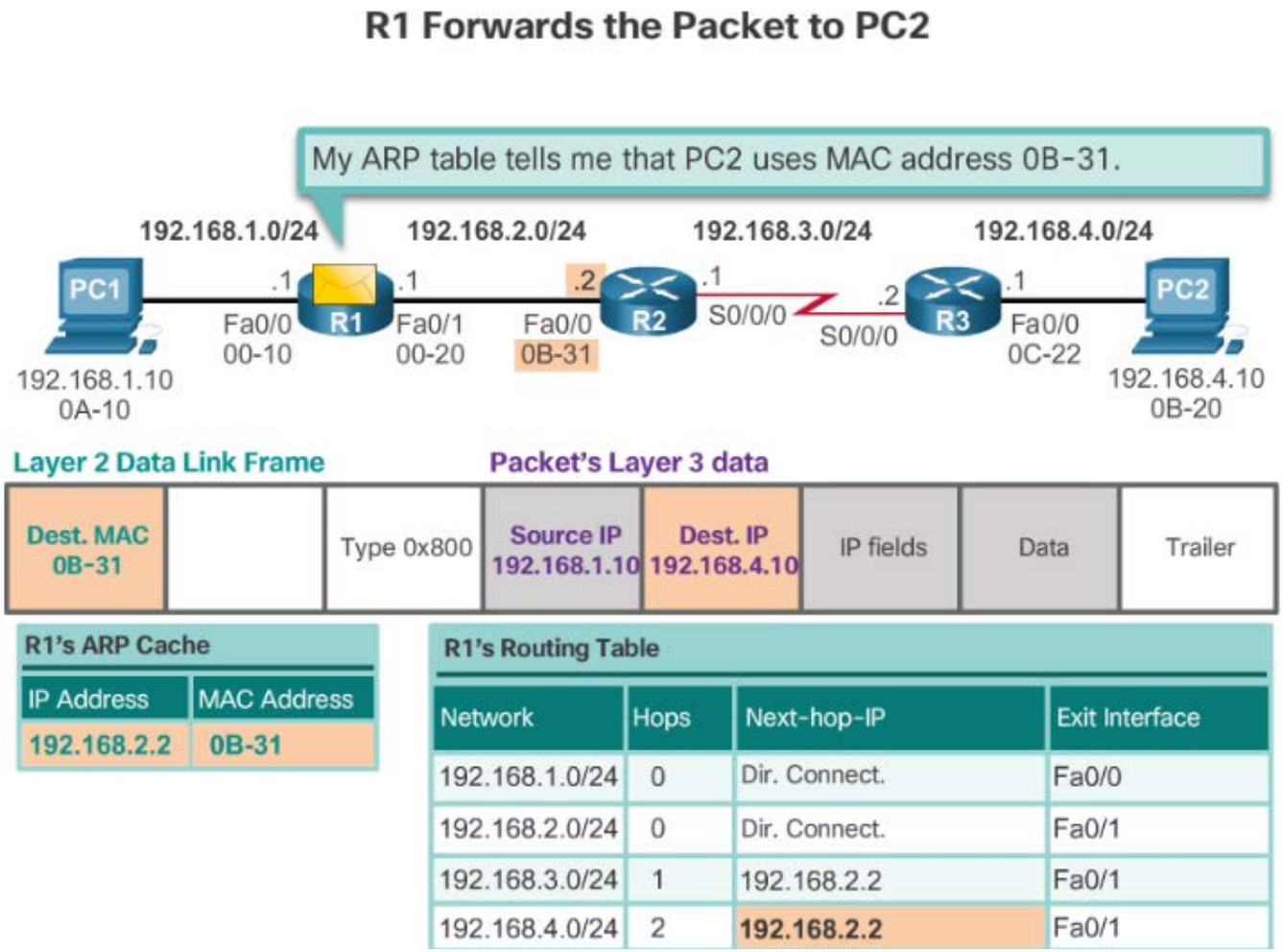
Switching Packets Between Networks
Router Switching Function



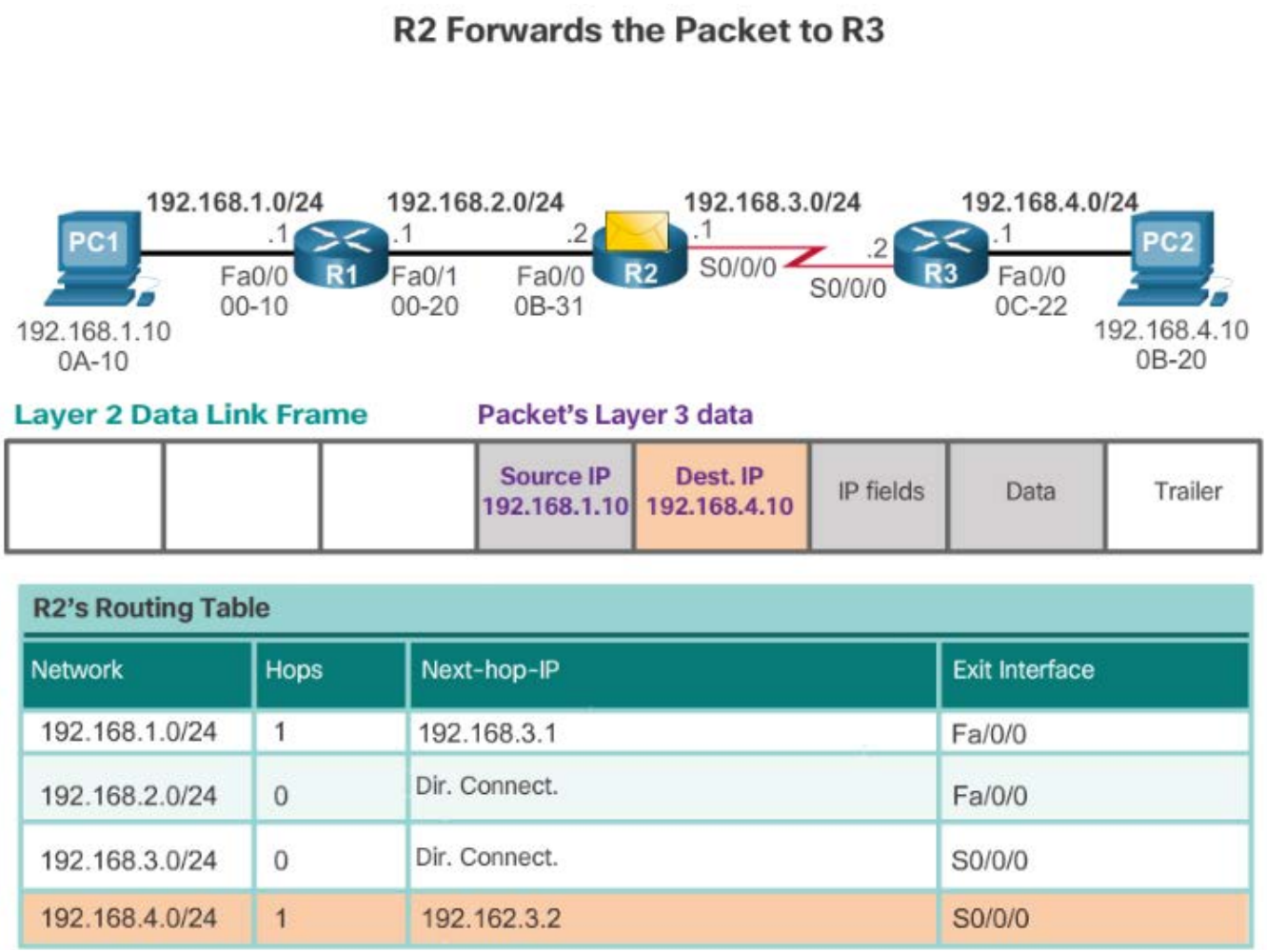
Switching Packets Between Networks Send a Packet



Switching Packets Between Networks Forward to Next Hop



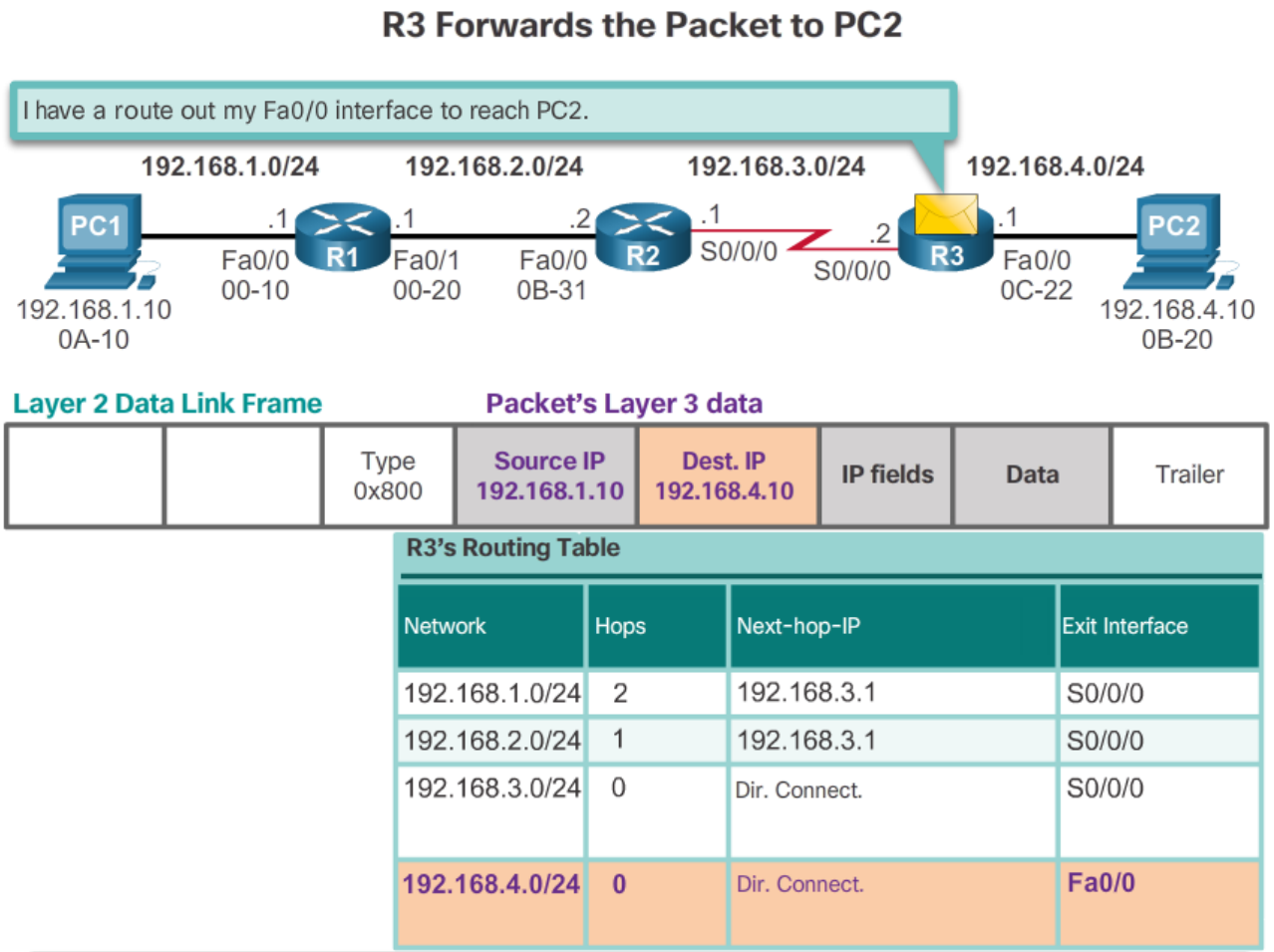
Switching Packets Between Networks Packet Routing



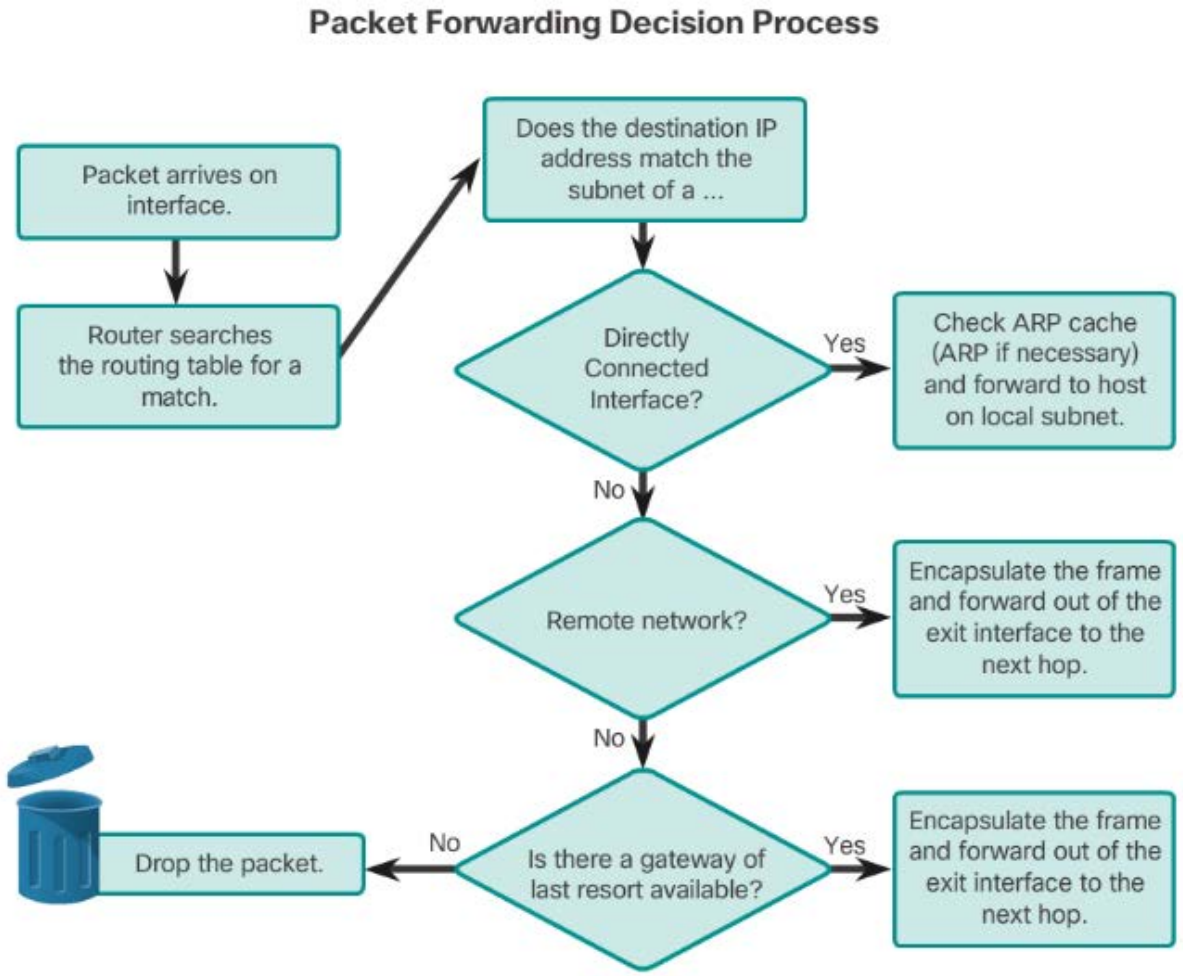
R2's Routing Table

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

Switching Packets Between Networks Reach the Destination



Path Determination
Routing Decisions

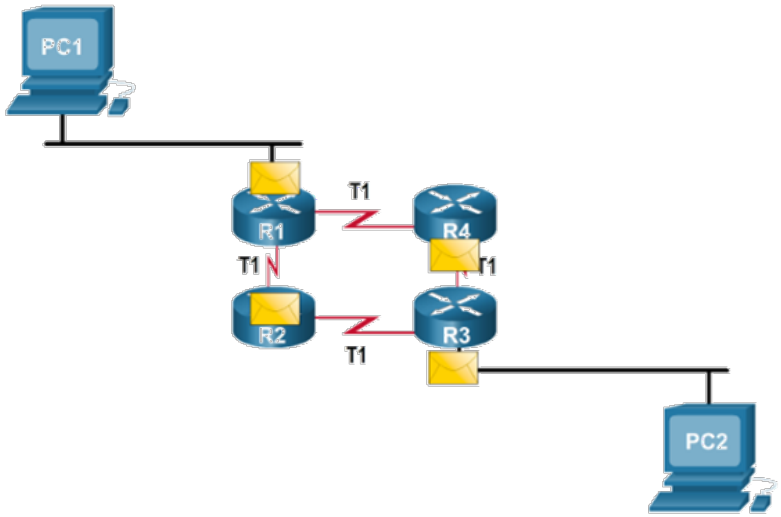


Path Determination
Best Path

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

Path Determination
Load Balancing

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



Path Determination
Administrative Distance

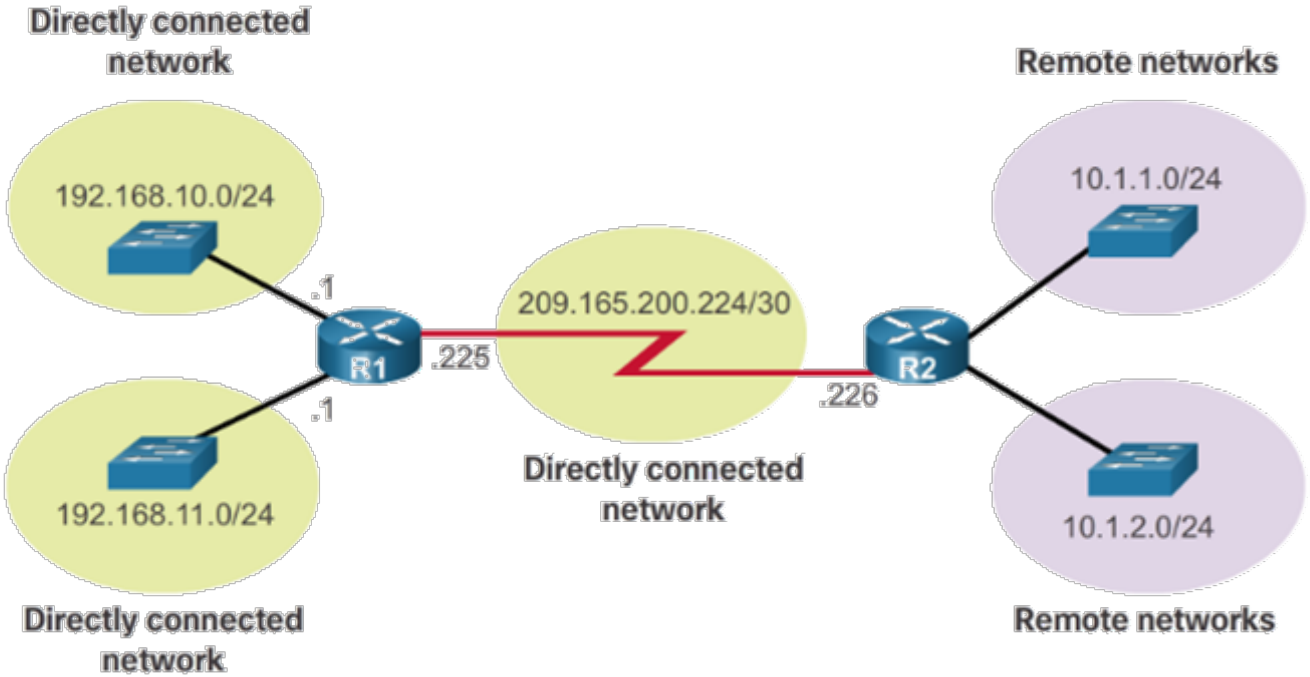
- When multiple paths to the same destination are available in its routing table, the router uses the route with the **lowest Administrative Distance (AD):**
  - A static route with an AD of 1 is more reliable than an EIGRP-discovered route with an AD of 90.
  - A directly connected route with an AD of 0 is more reliable than a static route with an AD of 1.

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

Router Operation

Analyze the Routing Table
The Routing Table

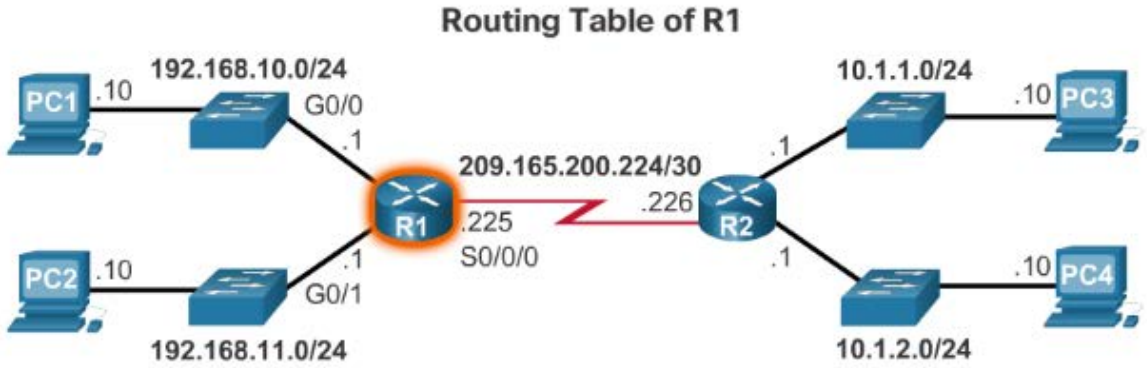
- A **routing table is a file stored in RAM** that contains information about:
  - Directly connected routes
  - Remote routes



Analyze the Routing Table
Routing Table Sources

- The `show ip route` command (on Cisco Routers) is used to display the contents of the routing table:
  - **Local route interfaces:** Added to the routing table when an interface is configured. (displayed in IOS 15 or newer for IPv4 routes and all IOS releases for IPv6 routes.)
  - **Directly connected interfaces:** Added to the routing table when an interface is configured and active.
  - **Static routes:** Added when a route is manually configured and the exit interface is active.
  - **Dynamic routing protocol:** Added when EIGRP or OSPF are implemented and networks are identified.

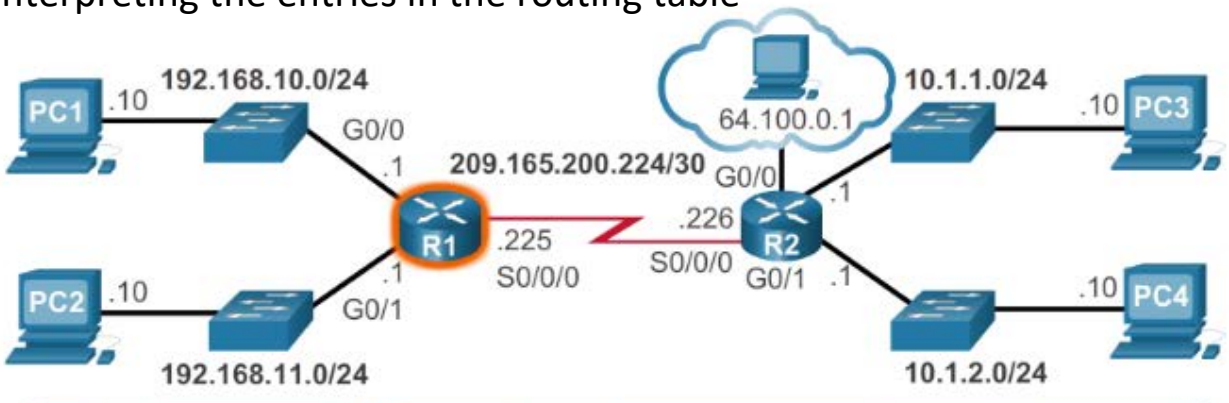
Analyze the Routing Table
Routing Table Sources (cont.)




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
```

Analyze the Routing Table
Remote Network Routing Entries

Interpreting the entries in the routing table



Legend

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

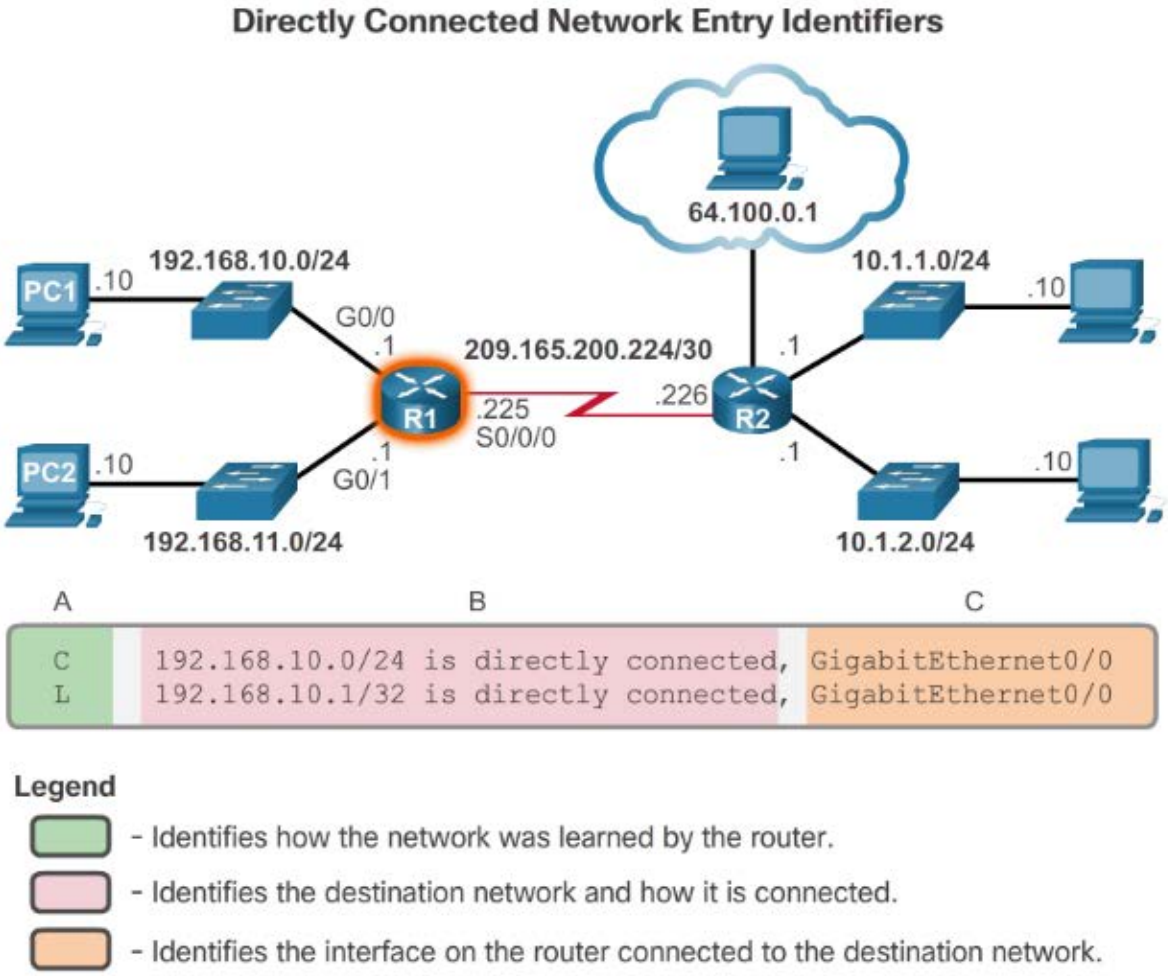
Directly Connected Routes
Directly Connected Interfaces

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

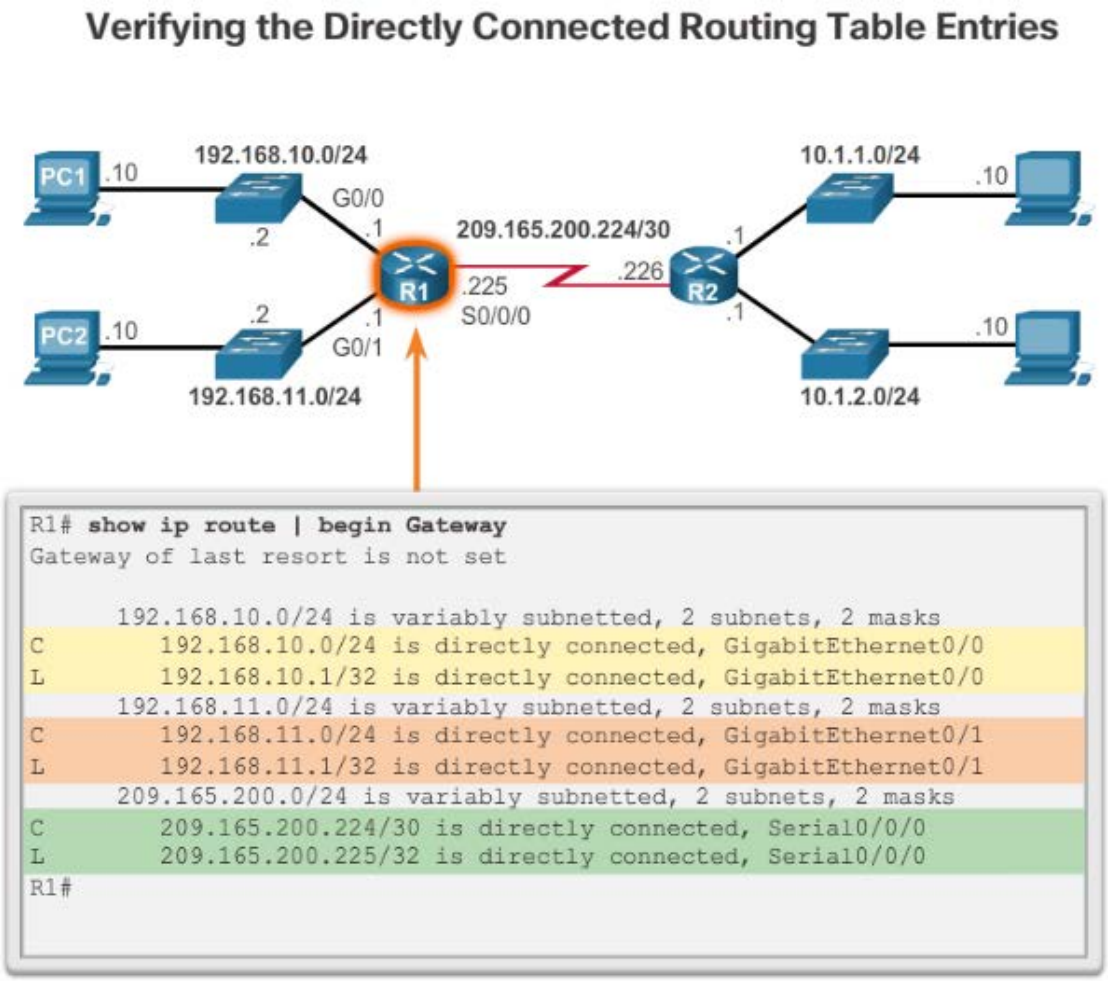
Empty Routing Table


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

Gateway of last resort is not set

R1#
```

Directly Connected Routes
Directly Connected Routing Table Entries

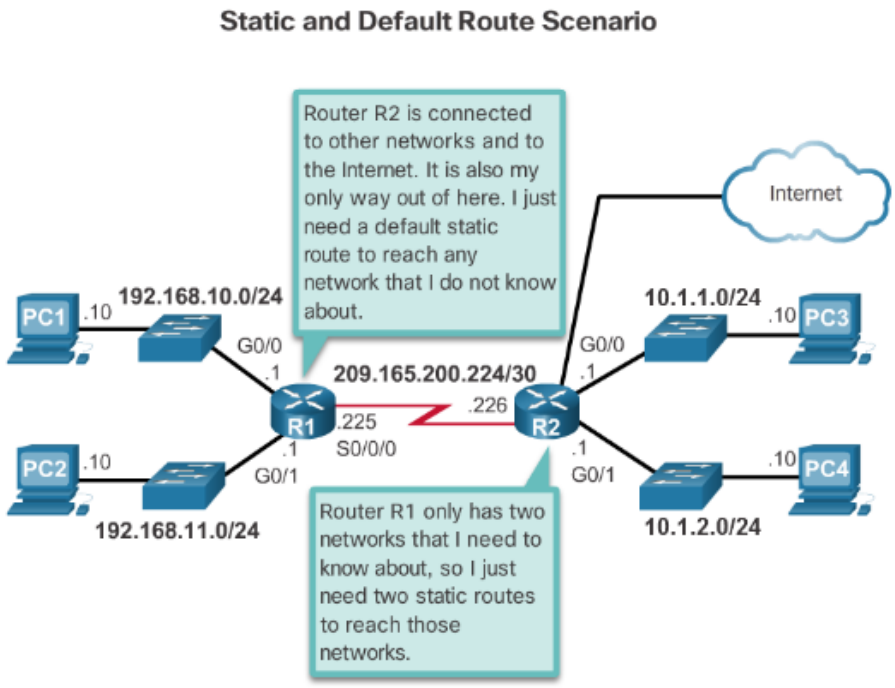


Directly Connected Routes
Directly Connected Example



Static Routing
Reach Remote Networks

- A router can learn about remote networks in one of two ways:
  - **Manually**: Remote networks are manually entered into the route table using static routes.
  - **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.



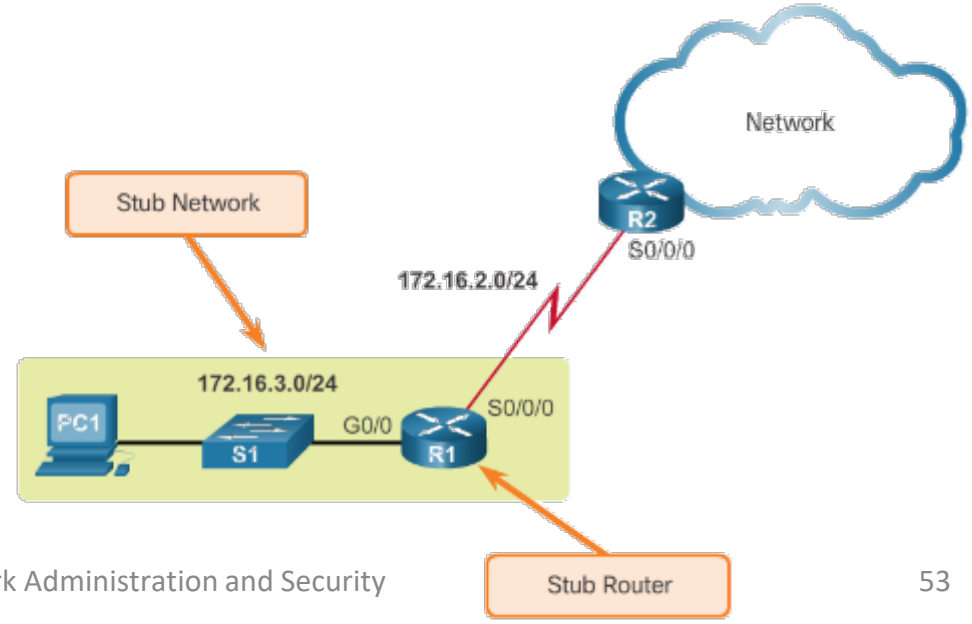
Static Routing
Why Use Static Routing?

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

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

Static Routing
When to Use Static Routes

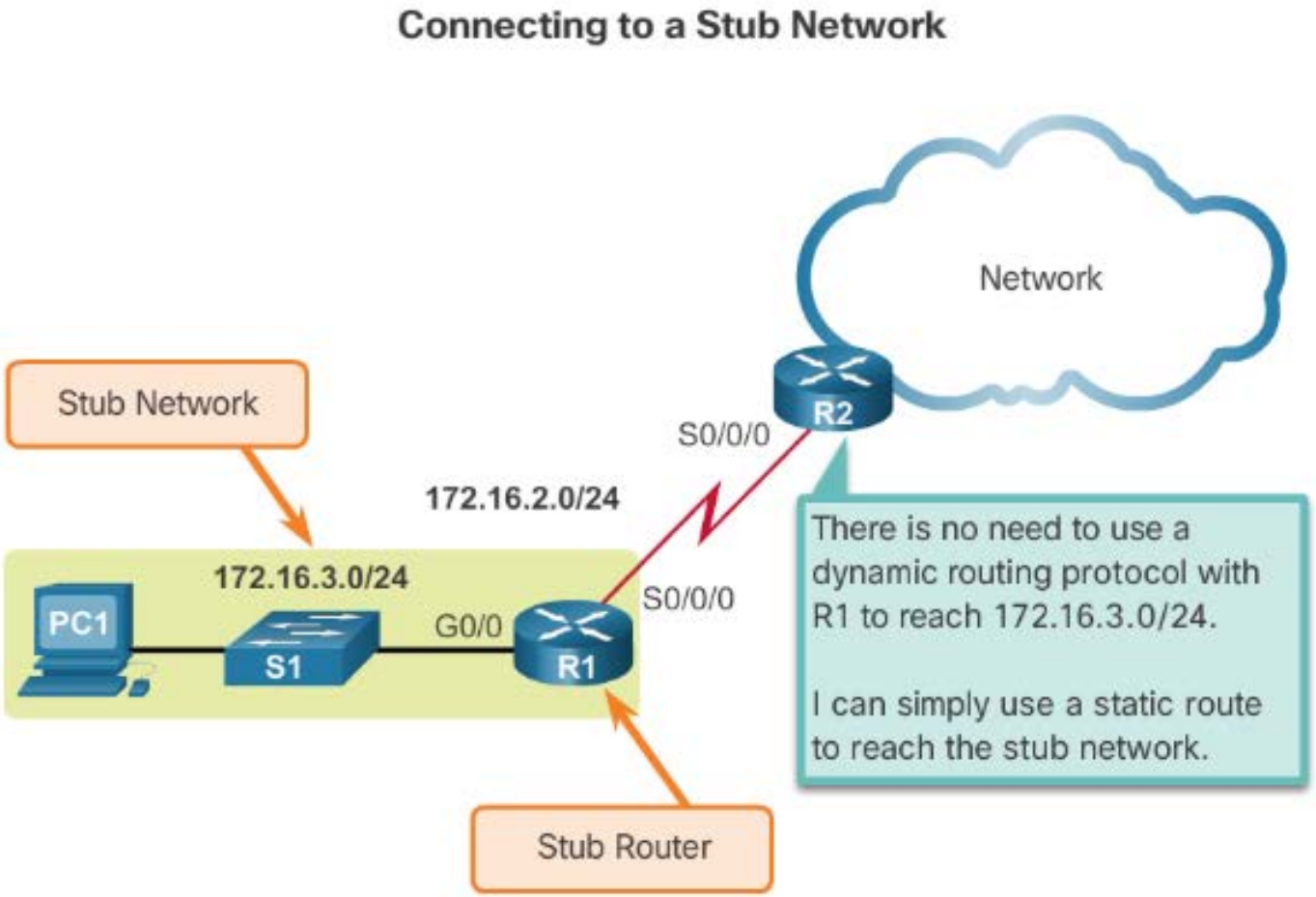
- Static routing has three primary uses:
  - Providing **ease of routing table maintenance in smaller networks**.
  - **Routing to and from stub networks**.
    - A stub network is a network accessed by a single route, and the router has no other neighbors.
  - **Using a single default route** to represent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



Types of Static Routes
Static Route Applications

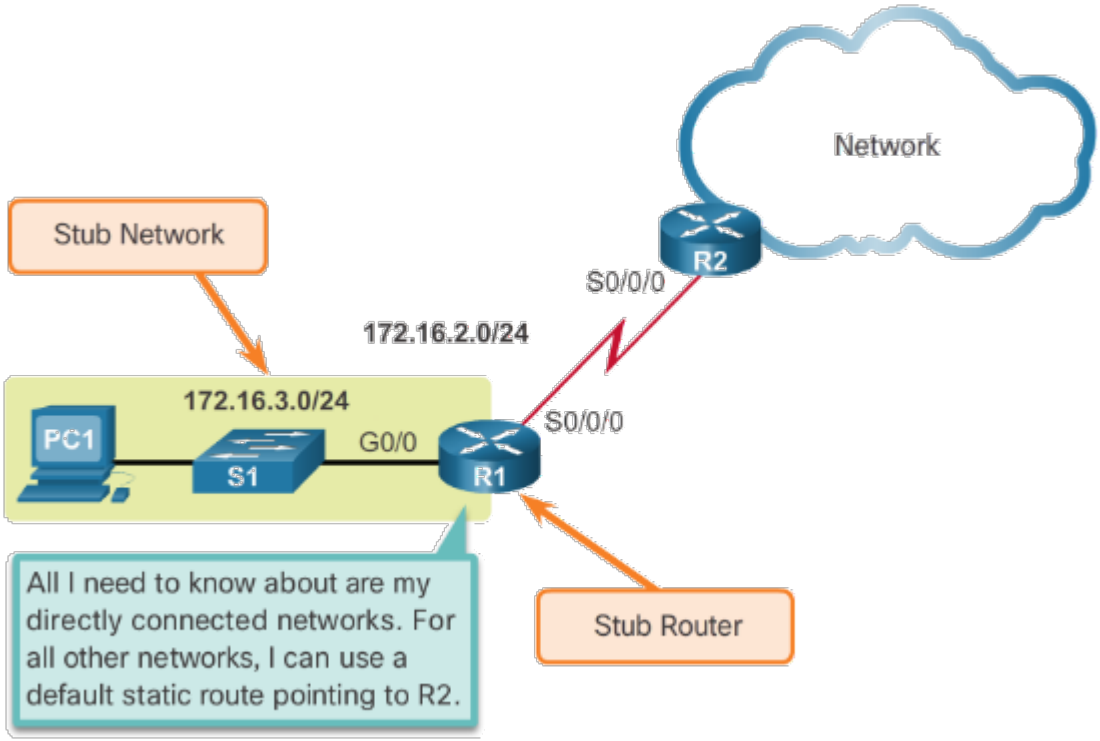
- Static Routes are often used to:
  - **Connect to a specific network.**
  - Provide a **Gateway of Last Resort** for a stub network.
  - **Reduce the number of routes** advertised by summarizing several contiguous networks as one static route.
  - **Create a backup route** in case a primary route link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

Types of Static Routes
Standard Static Route

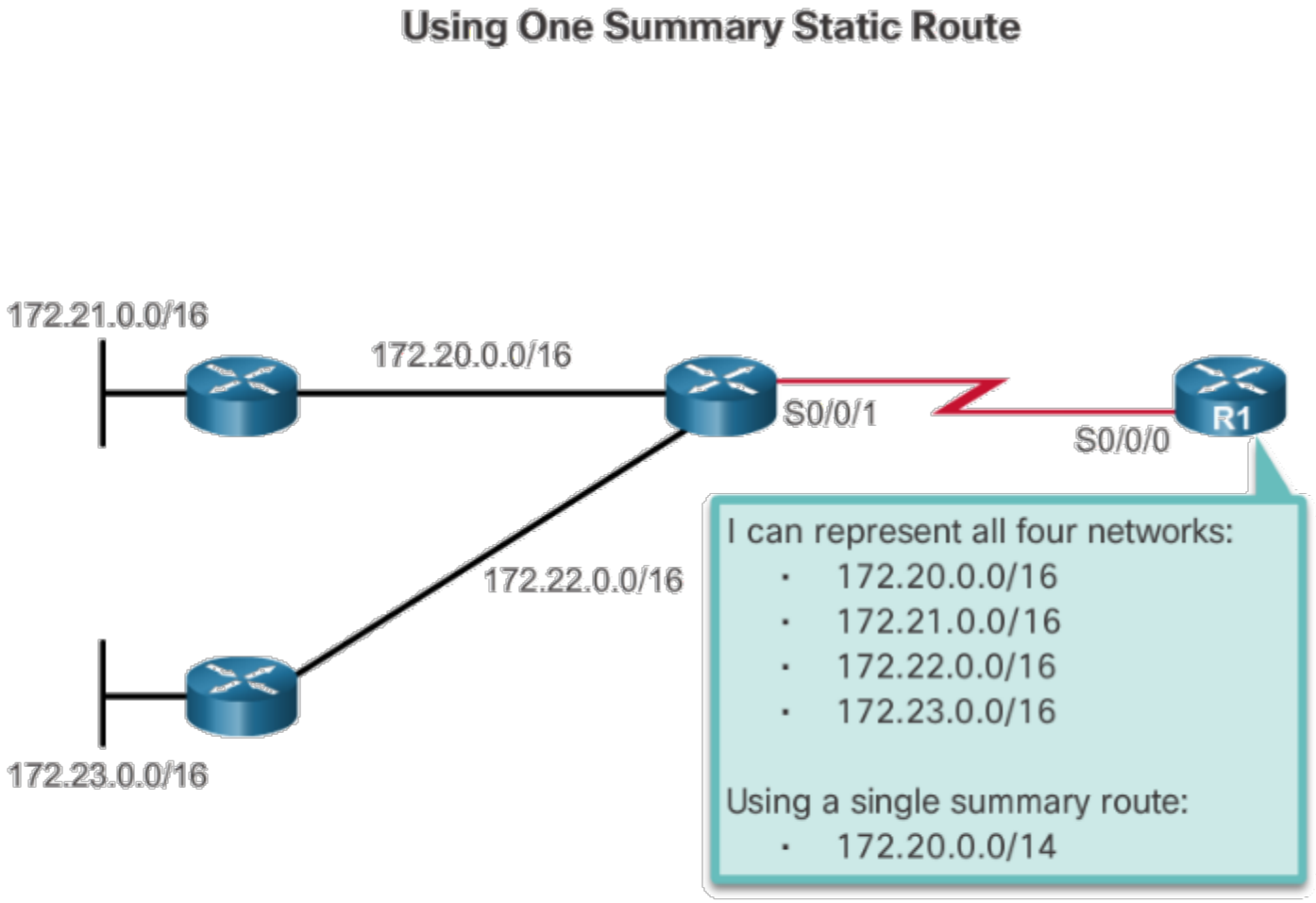


Types of Static Routes
Default Static Route

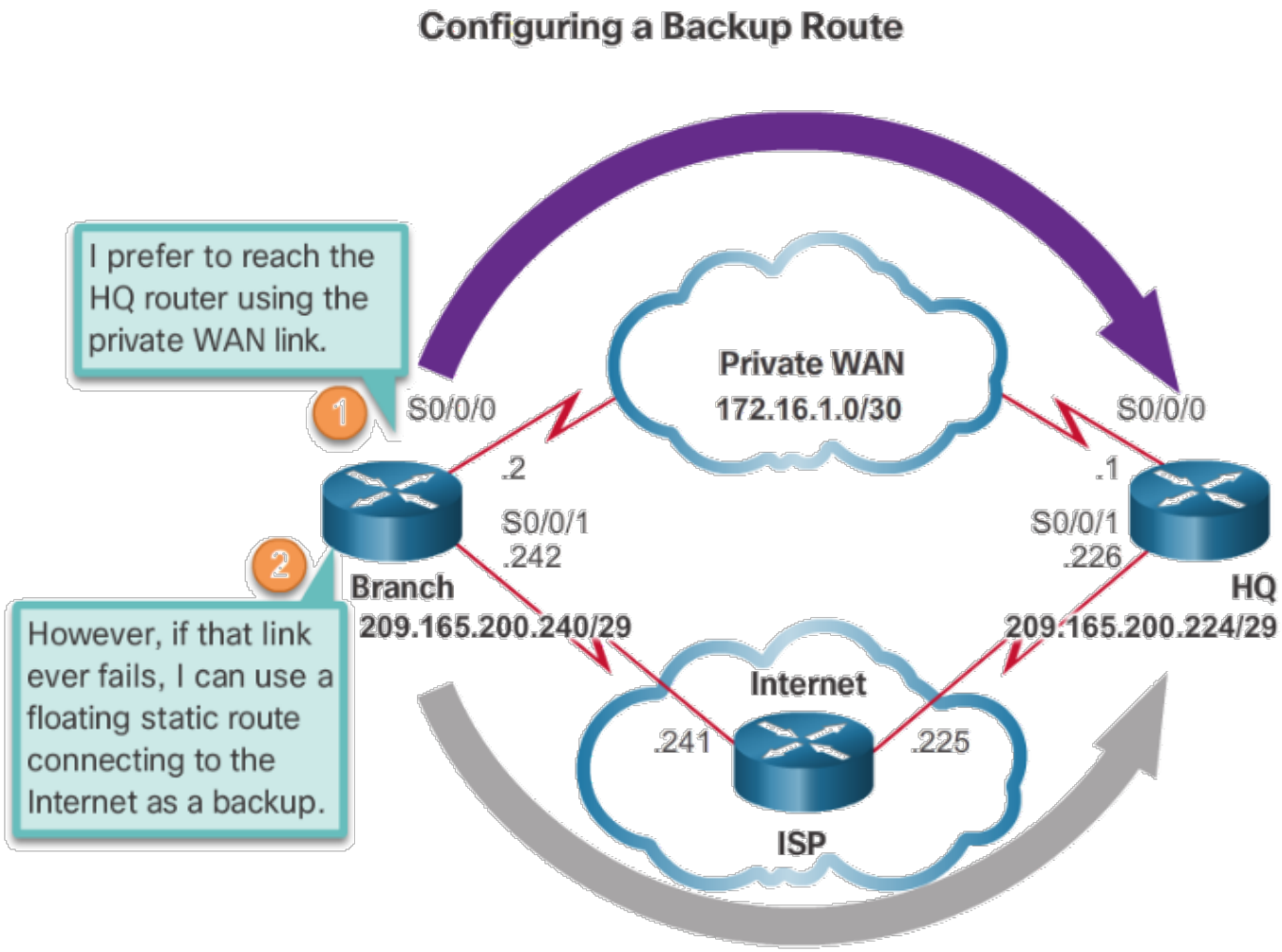
- A default static route is a route that matches all packets.
- A default route identifies the gateway IP address to which the router sends all IP packets that it does not have a learned or static route.
- A default static route is simply a static route with 0.0.0.0/0 as the destination IPv4 address.



Types of Static Routes
Summary Static Route

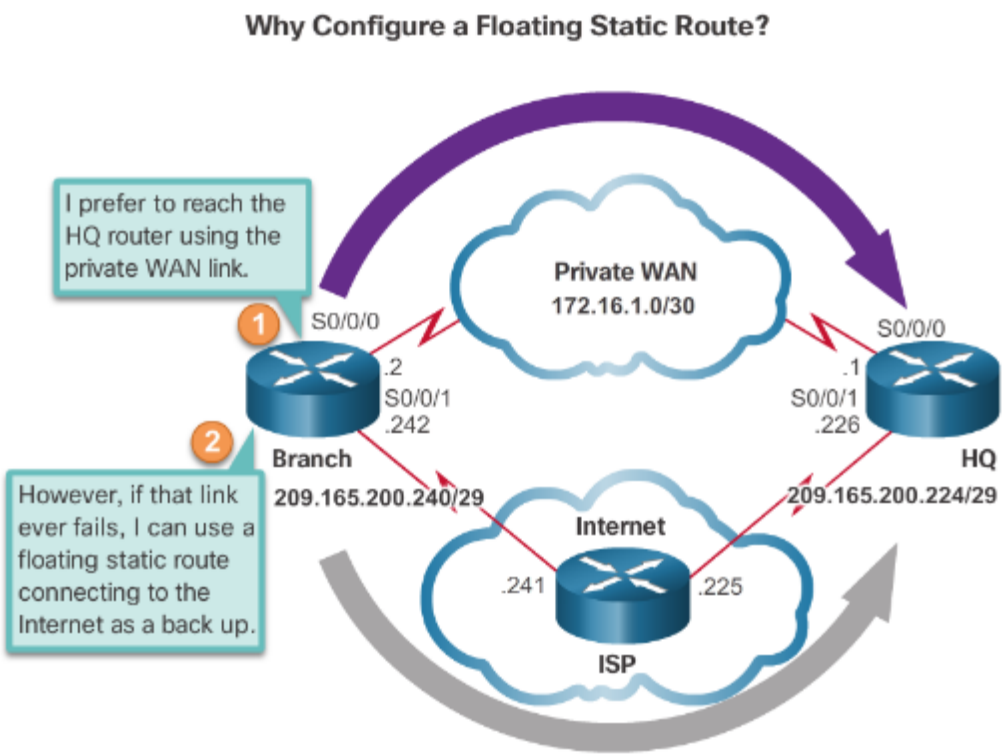


Types of Static Routes
Floating Static Route



Types of Static Routes
Floating Static Route

- Floating static routes have an administrative distance greater than the administrative distance of another static route or dynamic routes.
- The static route “floats” and is not used when the route with the better administrative distance is active.
- If the preferred route is lost the floating static route can take over.



Configure Static and Default Routes

Configure IPv4 Static Routes

ip route Command

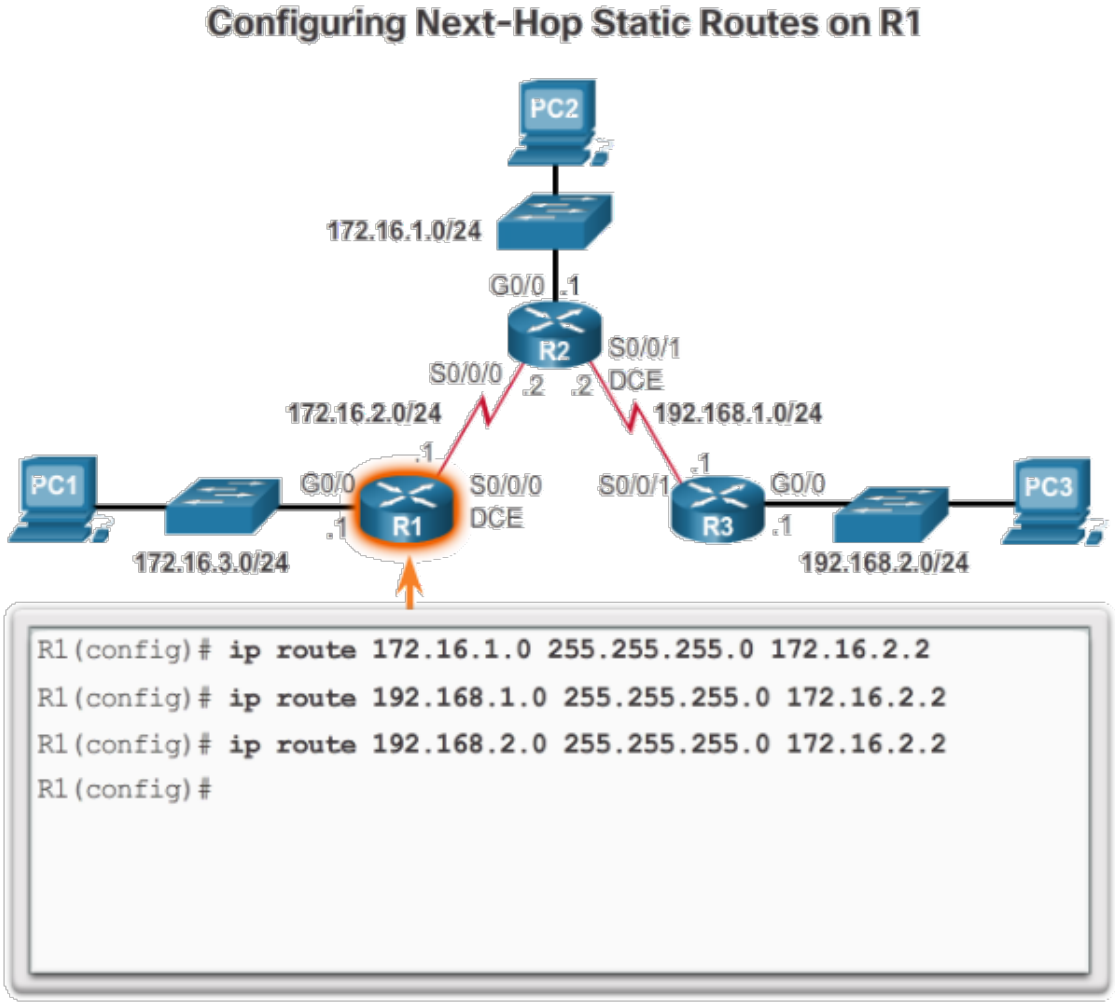
```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

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

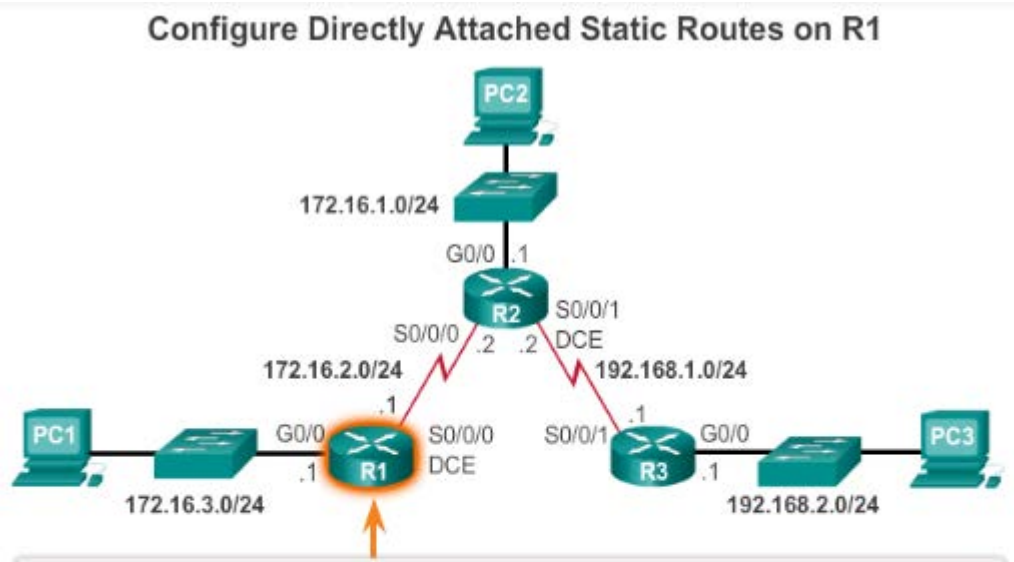
Configure IPv4 Static Routes
Next-Hop Options

- The **next hop can be identified by an IP address, exit interface, or both**.
- How the destination is specified creates one of the three following route types:
  - **Next-hop route -** Only the next-hop IP address is specified.
  - **Directly connected static route** - Only the router exit interface is specified.
  - **Fully specified static route** - The next-hop IP address and exit interface are specified.

Configure IPv4 Static Routes
Configure a Next-Hop Static Route

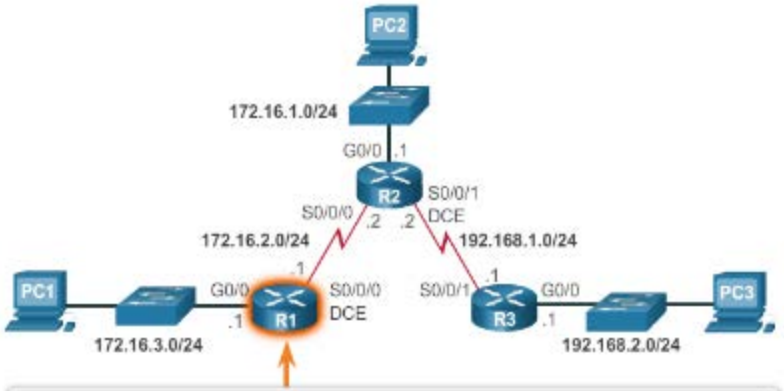


Configure IPv4 Static Routes
Configure Directly Connected Static Route




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

Configure IPv4 Static Routes
Verify a Static Route




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

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

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

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

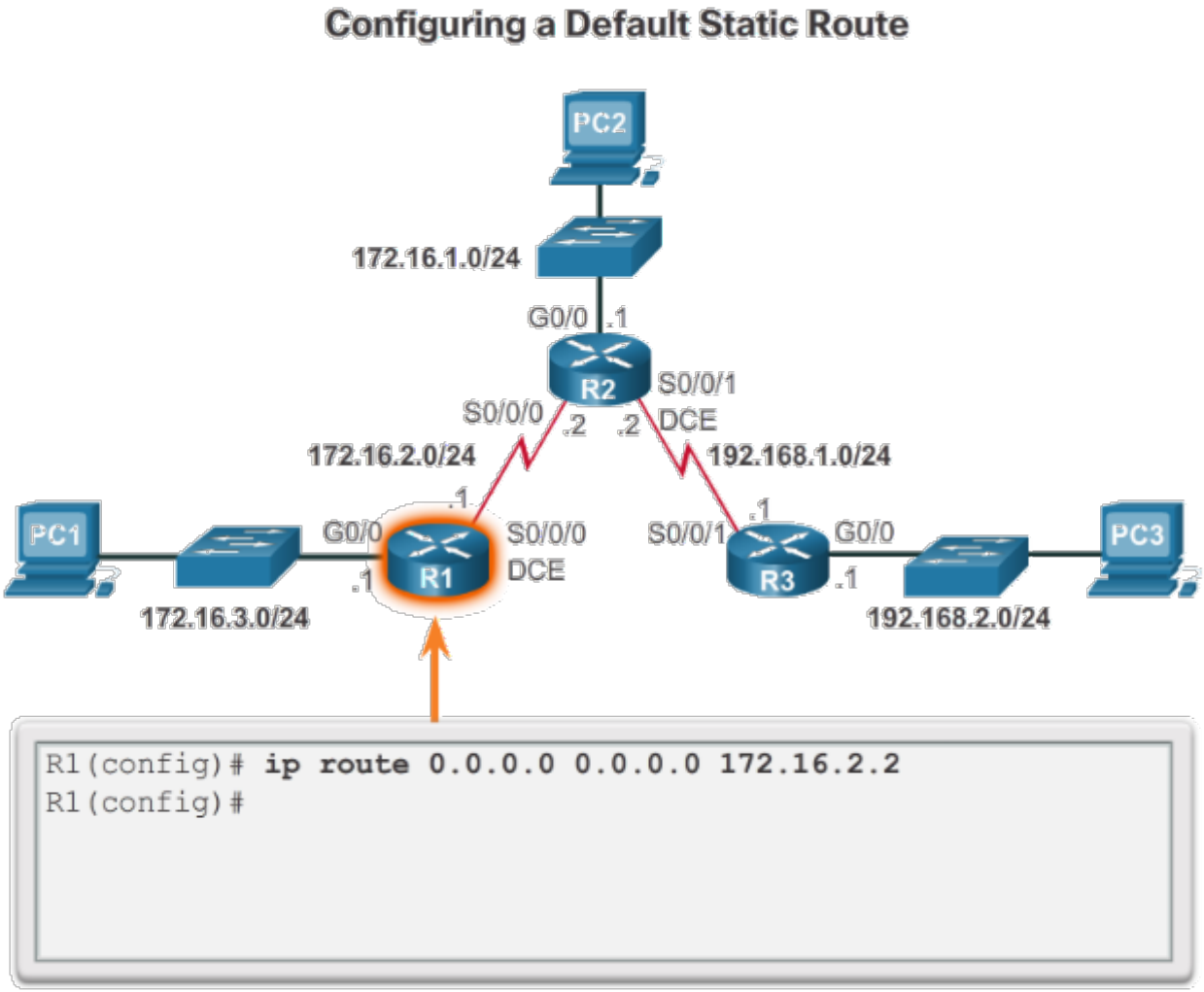
Configure IPv4 Static Routes
Default Static Route

Default Static Route Syntax

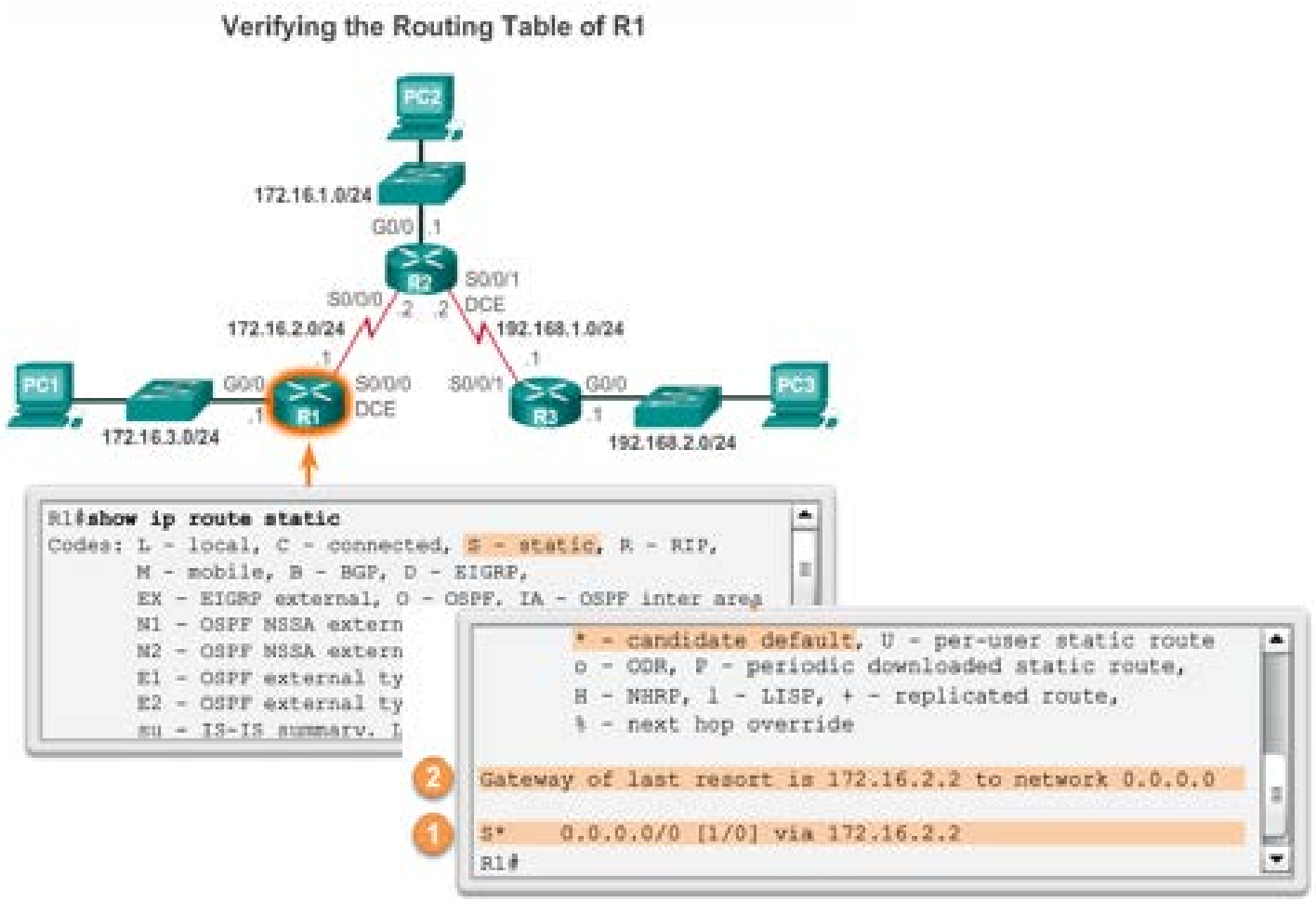
```
Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

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

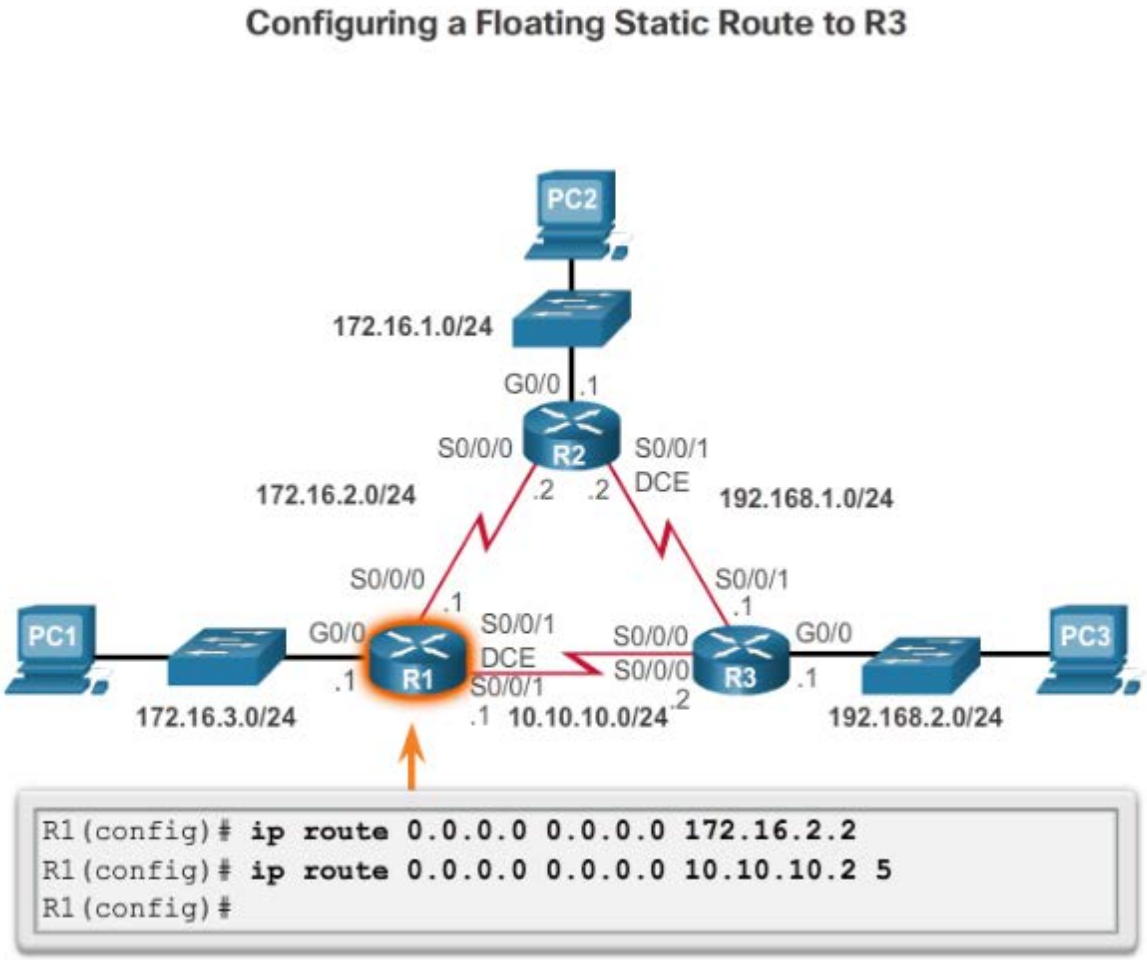
Configure IPv4 Static Routes
Configure a Default Static Route



Configure IPv4 Static Routes
Verify a Default Static Route



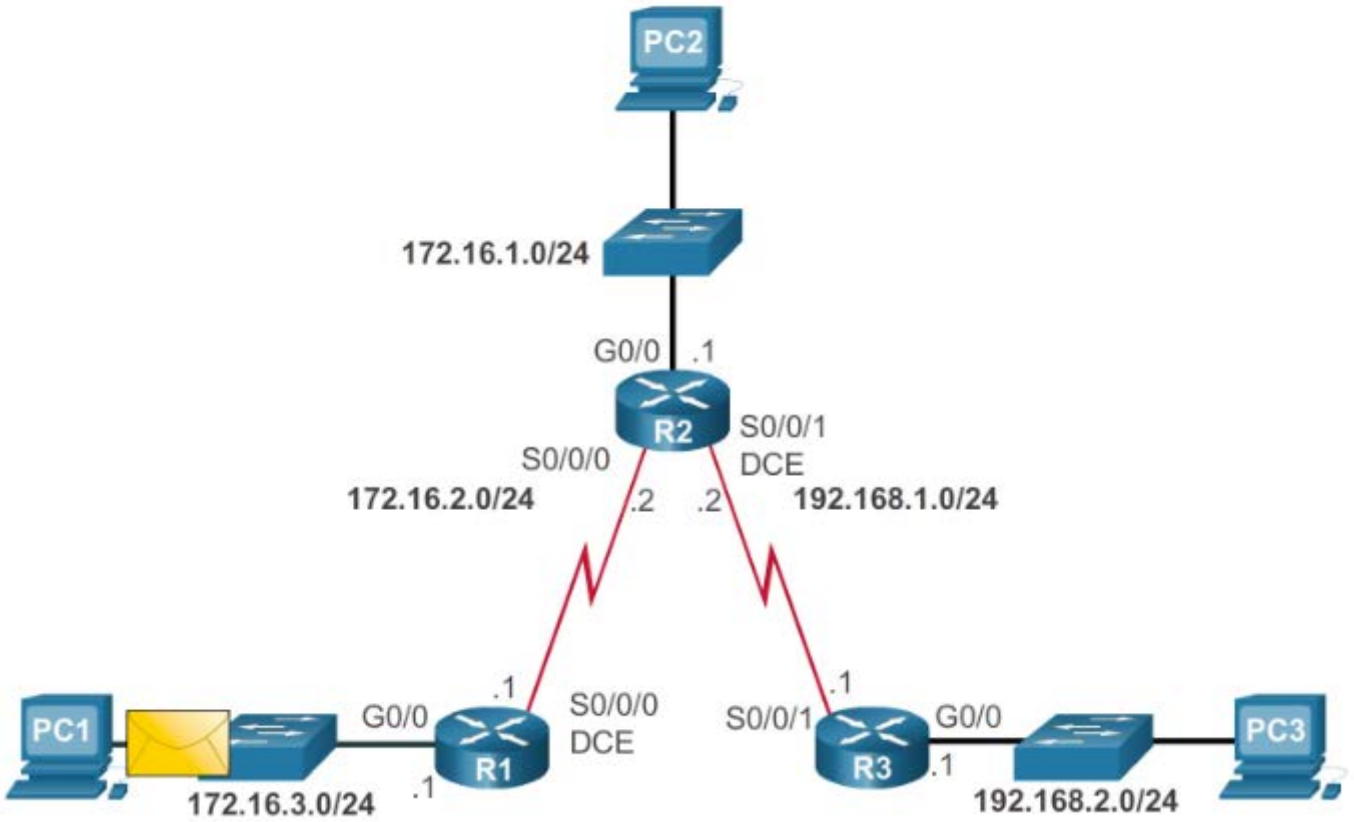
Configure an IPv4 Floating Static Route



Test the IPv4 Floating Static Route

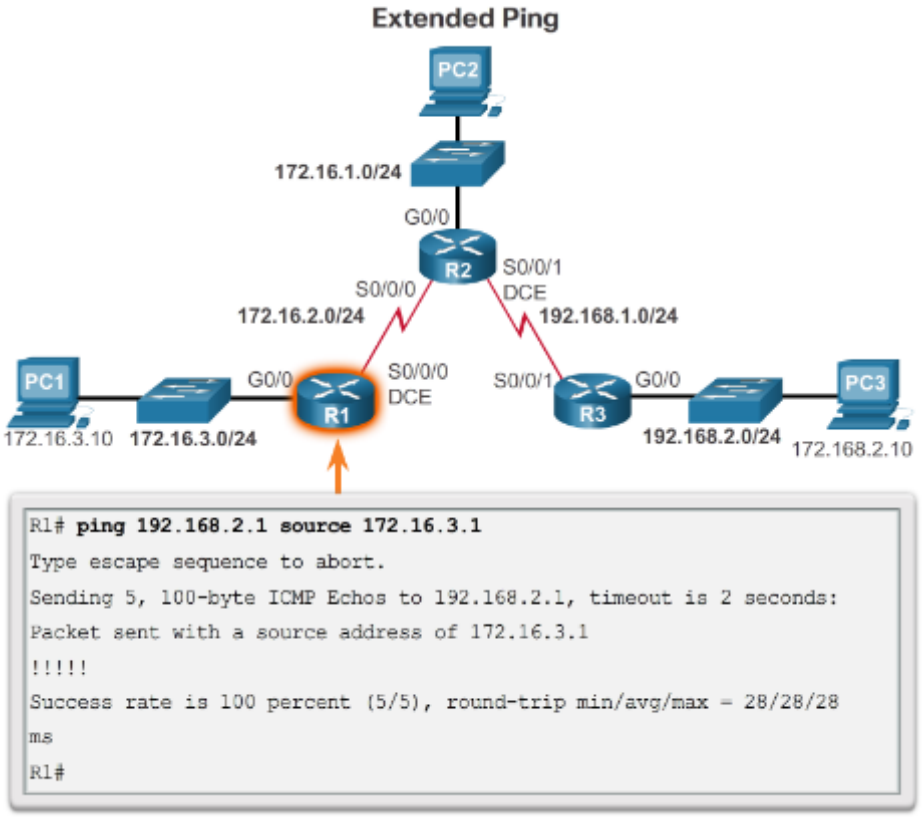
- To test a floating static route:
  - Use the show ip route command to verify that the routing table is using the default static route.
  - Use the traceroute command to follow the traffic flow out the primary route.
  - Disconnect the link or shutdown the primary interface(s). In the curriculum example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

Packet Processing with Static Routes
Static Routes and Packet Forwarding



Troubleshoot a Missing Route

- IOS troubleshooting commands include:
  - ping
  - Extended ping enables you to specify the source IP address for the ping packets.
  - traceroute
  - show ip route
  - show ip interface brief
  - show cdp neighbors detail



Packet Processing with Static Routes Solve a Connectivity Problem

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

Thanks !