CCNA 2 v7.0 Curriculum: Module 14 – Routing Concepts

itexamanswers.net/ccna-2-v7-0-curriculum-module-14-routing-concepts.html

June 12, 2020

Contents

14.0 Introduction

14.0.1 Why should I take this module?

Welcome to Routing Concepts!

No matter how effectively you set up your network, something will always stop working correctly, or even stop working completely. This is a simple truth about networking. So, even though you already know quite a bit about routing, you still need to know how your routers actually work. This knowledge is critical if you want to be able to troubleshoot your network. This module goes into detail about the workings of a router. Jump in!

14.0.2 What will I learn to do in this module?

Module Title: Routing Concepts

Module Objective: Explain how routers use information in packets to make forwarding decisions.

Topic Title	Topic Objective
Path Determination	Explain how routers determine the best path.
Packet Forwarding	Explain how routers forward packets to the destination.
Basic Router Configuration Review	Configure basic settings on a router.
IP Routing Table	Describe the structure of a routing table.
Static and Dynamic Routing	Compare static and dynamic routing concepts.

14.1 Path Determination

14.1.1 Two Functions of Router

Before a router forwards a packet anywhere, it has to determine the best path for the packet to take. This topic explains how routers make this determination.

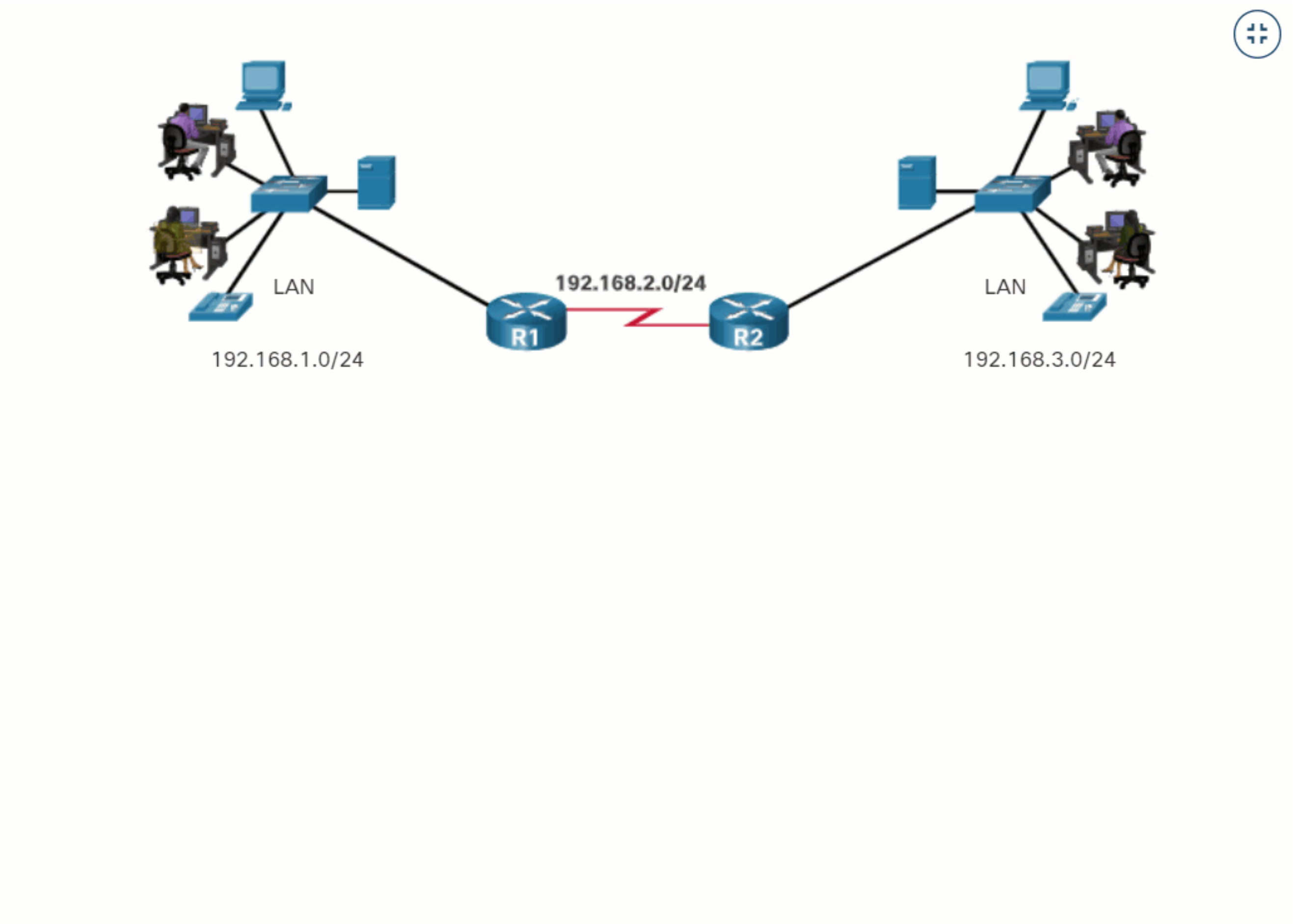
Ethernet switches are used to connect end devices and other intermediary devices, such as other Ethernet switches, to the same network. A router connects multiple networks, which means that it has multiple interfaces that each belong to a different IP network.

When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. This is known as routing. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network. Each network that a router connects to typically requires a separate interface, but this may not always be the case.

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.

14.1.2 Router Functions Example

The router uses its IP routing table to determine which path (route) to use to forward a packet. Click Play in the figure to follow a packet from the source PC to the destination PC. Watch how both R1 and R2 use their respective IP routing tables to first determine the best path, and then forward the packet.



14.1.3 Best Path Equals Longest Match

What is meant by the router must determine the best path in the routing table? The best path in the routing table is also known as the longest match. The longest match is a process the router uses to find a match between the destination IP address of the packet and a routing entry in the routing table.

The routing table contains route entries consisting of a prefix (network address) and prefix length. For there to be a match between the destination IP address of a packet and a route in the routing table, a minimum number of far-left bits must match between the IP address of the packet and the route in the routing table. The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match. Remember that an IP packet only contains the destination IP address and not the prefix length.

The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. The route with the greatest number of equivalent far-left bits, or the longest match, is always the preferred route.

Note: The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.

14.1.4 IPv4 Address Longest Match Example

In the table, an IPv4 packet has the destination IPv4 address 172.16.0.10. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and would be chosen to forward the packet. Remember, for any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.

Destination IPv4 Address		Address in Binary
172.16.0.10		**10101100.00010000.00000000.00**001010
Route Entry	**Prefix/Prefix Length**	**Address in Binary**
1	172.16.0.0/**12**	**10101100.0001**0000.00000000.00001010
2	172.16.0.0/**18**	**10101100.00010000.00**000000.00001010
3	172.16.0.0/**26**	**10101100.00010000.00000000.00**001010

14.1.5 IPv6 Address Longest Match Example

In the table, an IPv6 packet has the destination IPv6 address 2001:db8:c000::99. This example shows three route entries, but only two of them are a valid match, with one of those being the longest match. The first two route entries have prefix lengths that have the required number of matching bits as indicated by the prefix length. The first route entry with a prefix length of /40 matches the 40 far-left bits in the IPv6 address. The second route entry has a prefix length of /48 and with all 48 bits matching the destination IPv6 address, and is the longest match. The third route entry is not a match because its /64 prefix requires 64 matching bits. For the prefix 2001:db8:c000:5555::/64 to be a match, the first 64 bits must the destination IPv6 address of the packet. Only the first 48 bits match, so this route entry is not considered a match.

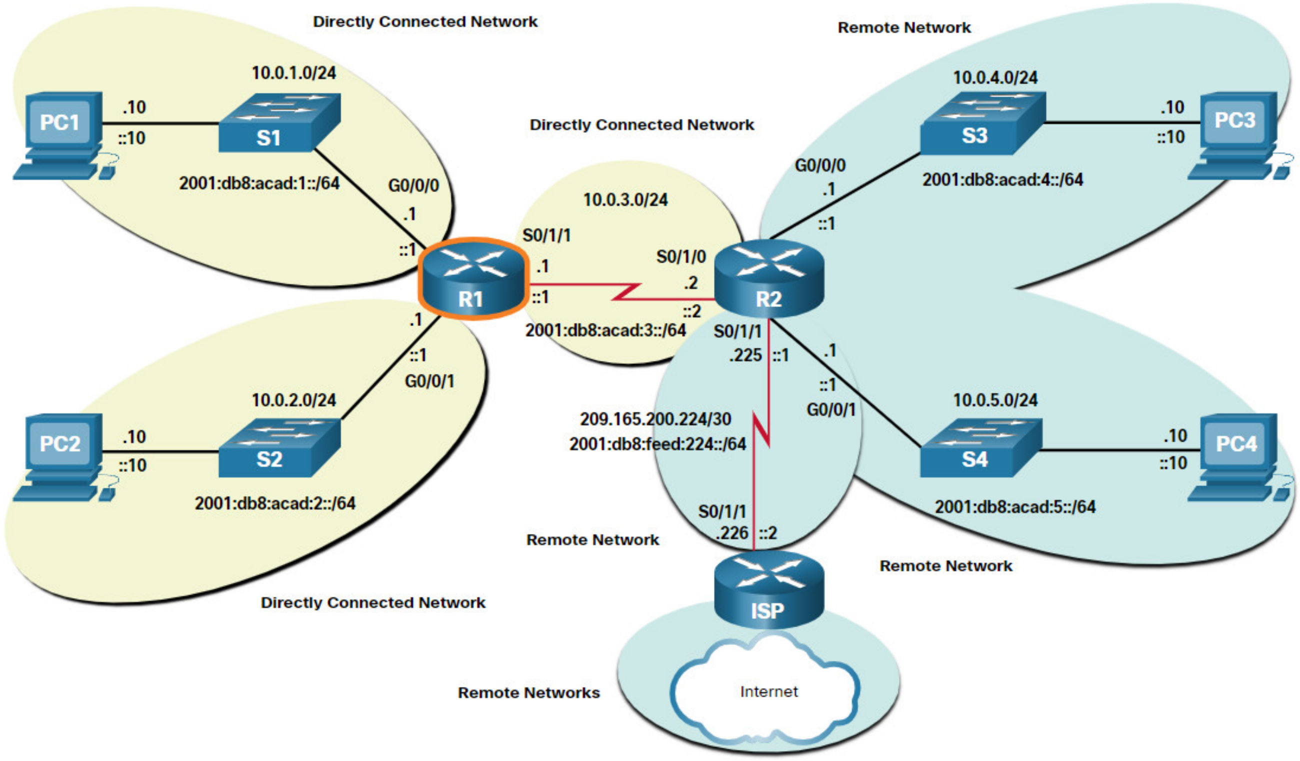
For the destination IPv6 packet with the address 2001:db8:c000::99, consider the following three route entries:

Route Entry	Prefix/Prefix Length	Does it match?
1	**2001:db8:c0**00::**/40**	Match of 40 bits
2	**2001:db8:c000**::**/48**	Match of 48 bits (longest match)
3	**2001:db8:c000**:5555::**/64**	Does not match 64 bits

14.1.6 Build the Routing Table

A routing table consists of prefixes and their prefix lengths. But how does the router learn about these networks? How does R1 in the figure populate its routing table?

Networks from the Perspective of R1



The networks in the topology are highlighted and labelled from the perspective of R1. All the IPv4 and IPv6 networks highlighted in yellow are directly connected networks. All the IPv4 and IPv6 networks highlighted in blue are remote networks.

Click each button for more information about the different ways a router learns routes.

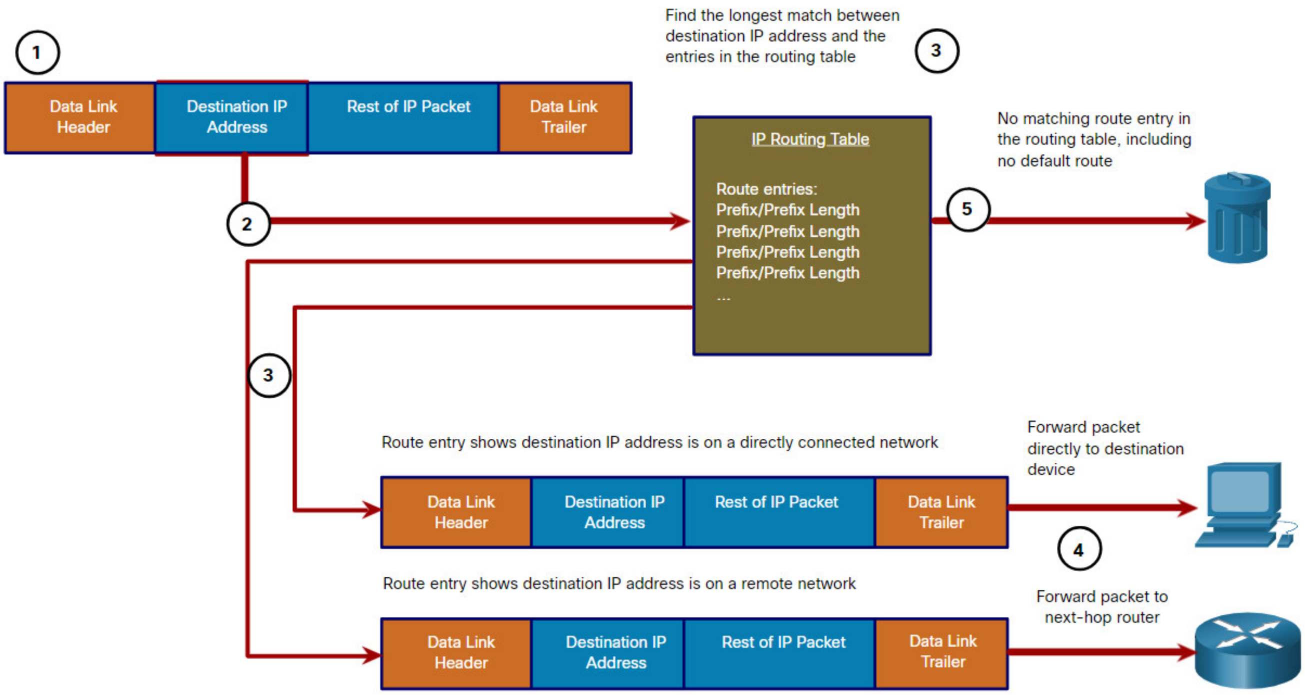
Directly Connected Networks
Directly connected networks are networks that are configured on the active interfaces of a router. A directly connected network is added to the routing table when an interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

14.2 Packet Forwarding

14.2.1 Packet Forwarding Decision Process

Now that the router has determined the best path for a packet based on the longest match, it must determine how to encapsulate the packet and forward it out the correct egress interface.

The figure demonstrates how a router first determines the best path, and then forwards the packet.


1
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer
Find the longest match between destination IP address and the entries in the routing table
3
2
IP Routing Table
Route entries:
Prefix/Prefix Length
Prefix/Prefix Length
Prefix/Prefix Length
Prefix/Prefix Length
...
No matching route entry in the routing table, including no default route
5
3
Route entry shows destination IP address is on a directly connected network
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer
Forward packet directly to destination device
4
Route entry shows destination IP address is on a remote network
Data Link Header
Destination IP Address
Rest of IP Packet
Data Link Trailer
Forward packet to next-hop router

The following steps describe the packet forwarding process shown in the figure:

1. The data link frame with an encapsulated IP packet arrives on the ingress interface.
2. The router examines the destination IP address in the packet header and consults its IP routing table.
3. The router finds the longest matching prefix in the routing table.
4. The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.
5. However, if there is no matching route entry the packet is dropped.

Click each button for a description of the three things a router can do with a packet after it has determined the best path.

Forwards the Packet to a Device on a Directly Connected Network

If the route entry indicates that the egress interface is a directly connected network, this means that the destination IP address of the packet belongs to a device on the directly connected network. Therefore, the packet can be forwarded directly to the destination device. The destination device is typically an end device on an Ethernet LAN, which means the packet must be encapsulated in an Ethernet frame.

To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet. The process varies based on whether the packet is an IPv4 or IPv6 packet:

- **IPv4 packet** - The router checks its ARP table for the destination IPv4 address and an associated Ethernet MAC address. If there is no match, the router sends an ARP Request. The destination device will return an ARP Reply with its MAC address. The router can now forward the IPv4 packet in an Ethernet frame with the proper destination MAC address.
- **IPv6 packet** - The router checks its neighbor cache for the destination IPv6 address and an associated Ethernet MAC address. If there is no match, the router sends an ICMPv6 Neighbor Solicitation (NS) message. The destination device will return an ICMPv6 Neighbor Advertisement (NA) message with its MAC address. The router can now forward the IPv6 packet in an Ethernet frame with the proper destination MAC address.

Forwards the Packet to a Next-Hop Router
If the route entry indicates that the destination IP address is on a remote network, this means the destination IP address of the packet belongs to a device on network that is not directly connected. Therefore, the packet must be forwarded to another router, specifically a next-hop router. The next-hop address is indicated in the route entry.

If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet as described previously. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address of the packet.

Note: This process will vary for other types of Layer 2 networks.

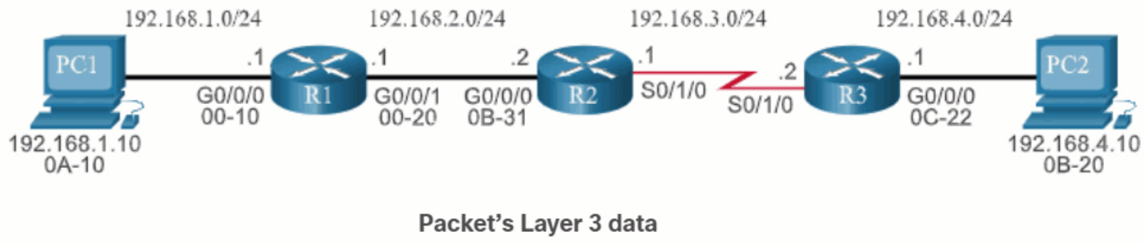
Drops the Packet - No Match in Routing Table
If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped.

14.2.2 End-to-End Packet Forwarding

The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. For example, the data link frame format for a serial link could be Point-to-Point (PPP) protocol, High-Level Data Link Control (HDLC) protocol, or some other Layer 2 protocol.

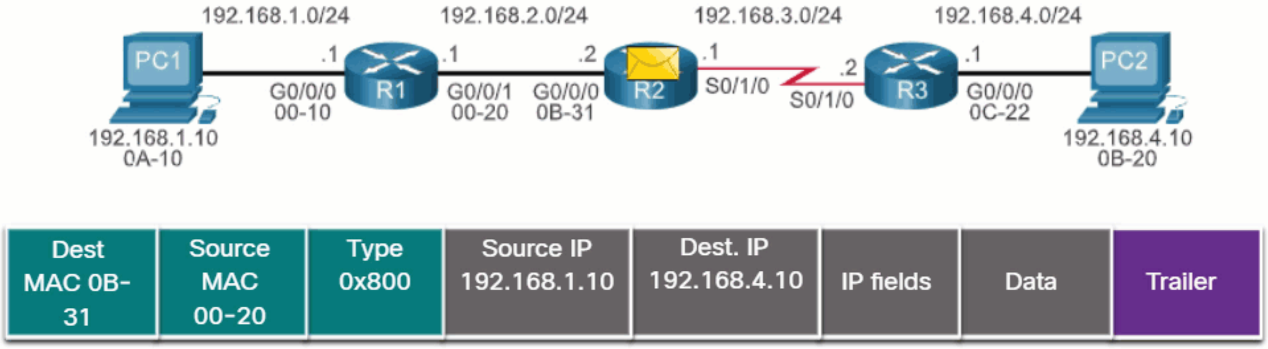
Click each button and play the animations of PC1 sending a packet to PC2. Notice how the contents and format of the data link frame change at each hop.

PC1 Sends Packet to PC2
In the first animation, PC1 sends a packet to PC2. Note that if an ARP entry does not exist in the ARP table for the default gateway of 192.168.1.1, PC1 sends an ARP request. Router R1 would then return an ARP reply.



R2 Forwards the Packet to R3

R2 now forwards the packet to R3. Because the exit interface is not an Ethernet network, R2 does not have to resolve the next-hop IPv4 address with a destination MAC address. When the interface is a point-to-point (P2P) serial connection, the router encapsulates the IPv4 packet into the proper data link frame format used by the exit interface (HDLC, PPP, etc.). Because there are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of a broadcast.



Dest MAC 0B-31	Source MAC 00-20	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer

14.2.3 Packet Forwarding Mechanisms

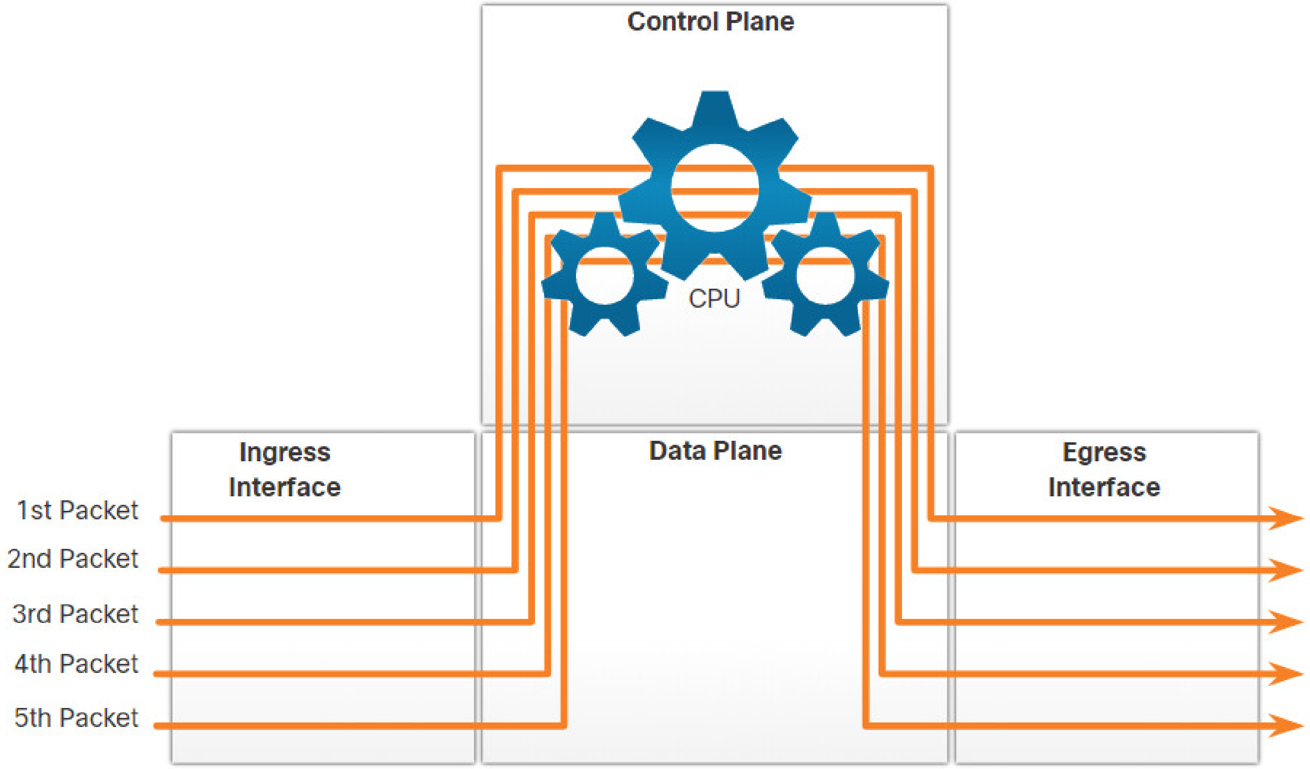
As mentioned previously, the primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. The more efficiently a router can perform this task, the faster packets can be forwarded by the router. Routers support the following three packet forwarding mechanisms:

- Process switching
- Fast switching
- Cisco Express Forwarding (CEF)

Assume that there is a traffic flow which consists of five packets. They are all going to the same destination. Click each button for more information about the packet forwarding mechanisms.

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 determines the exit interface and forwards the packet. It is important to understand that the router does this for every

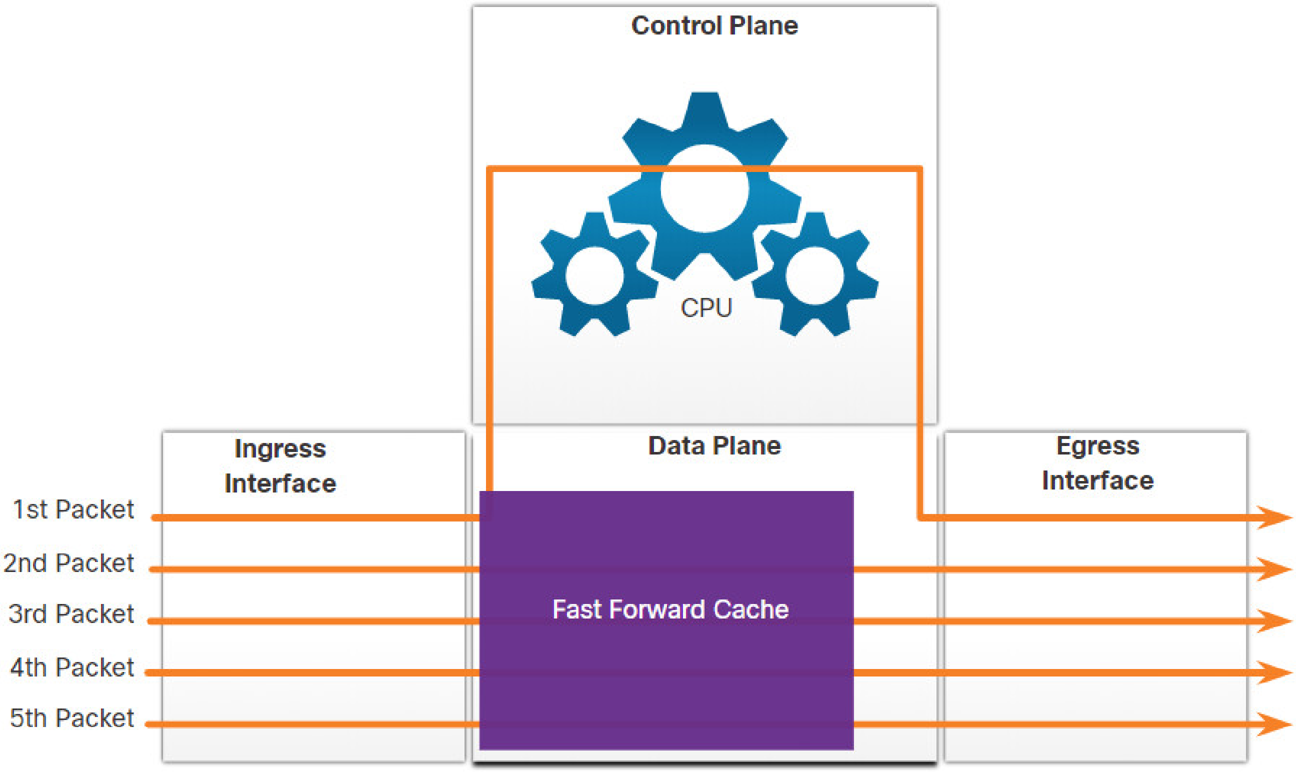
packet, even if the destination is the same for a stream of packets. This process-switching mechanism is very slow and is rarely implemented in modern networks. Contrast this with fast switching.



Fast Switching

Fast switching is another, older packet forwarding mechanism which was the successor to process switching. Fast switching 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 re-used without CPU intervention.

With fast switching, notice how only the first packet of a flow is process-switched and added to the fast-switching cache. The next four packets are quickly processed based on the information in the fast-switching cache.

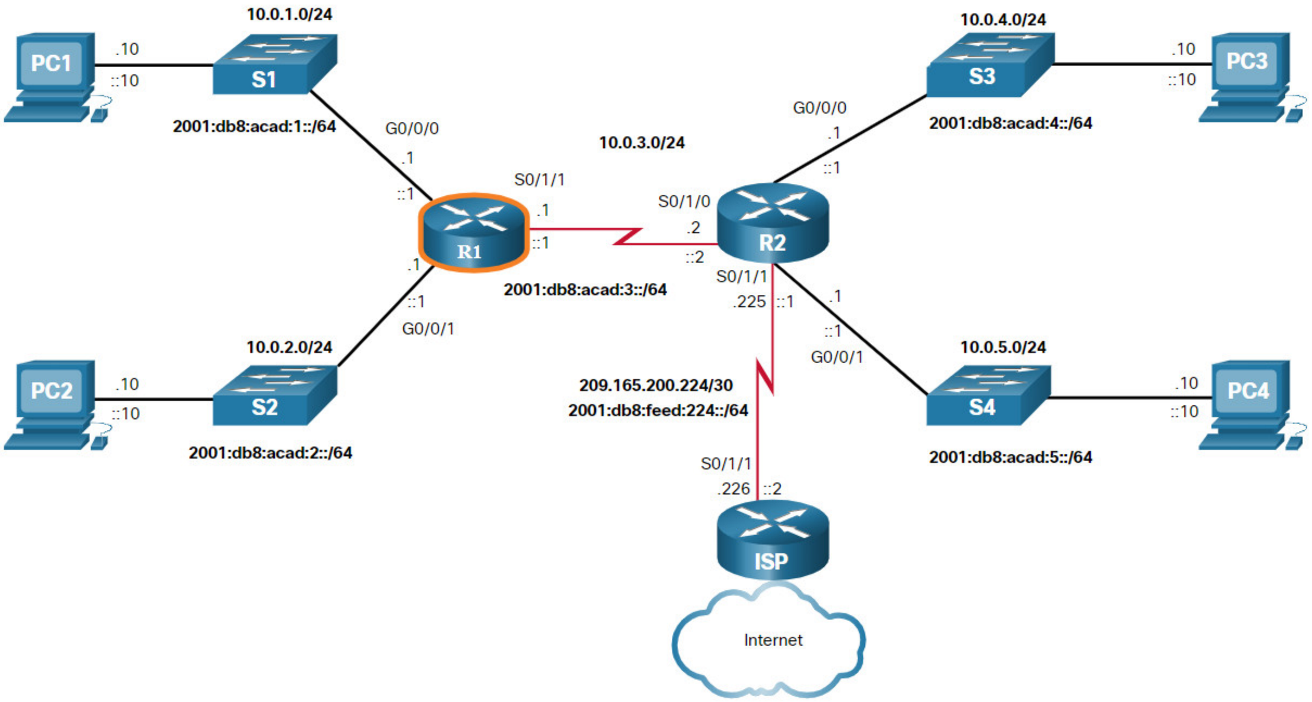


14.3 Basic Router Configuration Review

14.3.1 Topology

A router creates a routing table to help it determine where to forward packets. But before diving into the details of the IP routing table, this topic reviews basic router configuration and verification tasks. You will also complete a Packet Tracer activity to refresh your skills.

The topology in the figure will be used for configuration and verification examples. It will also be used in the next topic to discuss the IP routing table.



14.3.2 Configuration Commands

The following examples show the full configuration for R1.

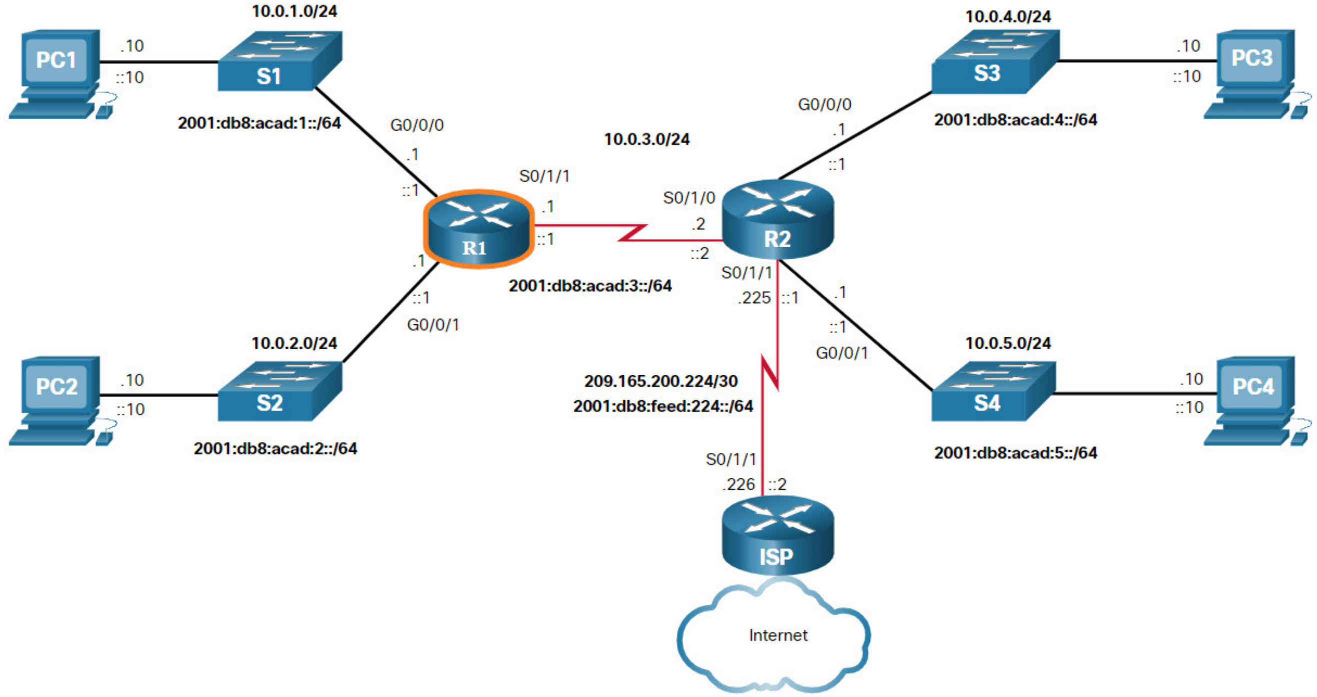
```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
************************************************
WARNING: Unauthorized access is prohibited!
************************************************
#
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

14.3.3 Verification Commands

Common verification commands include the following:

- **show ip interface brief**
- **show running-config interface** *interface-type number*
- **show interfaces**
- **show ip interface**
- **show ip route**
- **ping**

In each case, replace **ip** with **ipv6** for the IPv6 version of the command. The figure shows the topology again for easy reference.



Click each button for the command output for R1.

- show ip interface brief
- show ipv6 interface brief
- show running-config interface
- show interfaces
- show ip interface
- show ipv6 interface
- show ip route
- show ipv6 route
- ping

show ip interface brief

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   10.0.1.1        YES manual up                    up
GigabitEthernet0/0/1   10.0.2.1        YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            10.0.3.1        YES manual up                    up
GigabitEthernet0       unassigned      YES unset  down                  down
R1#
```

show running-config interface

```
R1# show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 10.0.1.1 255.255.255.0
 negotiation auto
 ipv6 address FE80::1:A link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

show ipv6 route

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/1, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

14.3.4 Filter Command Output

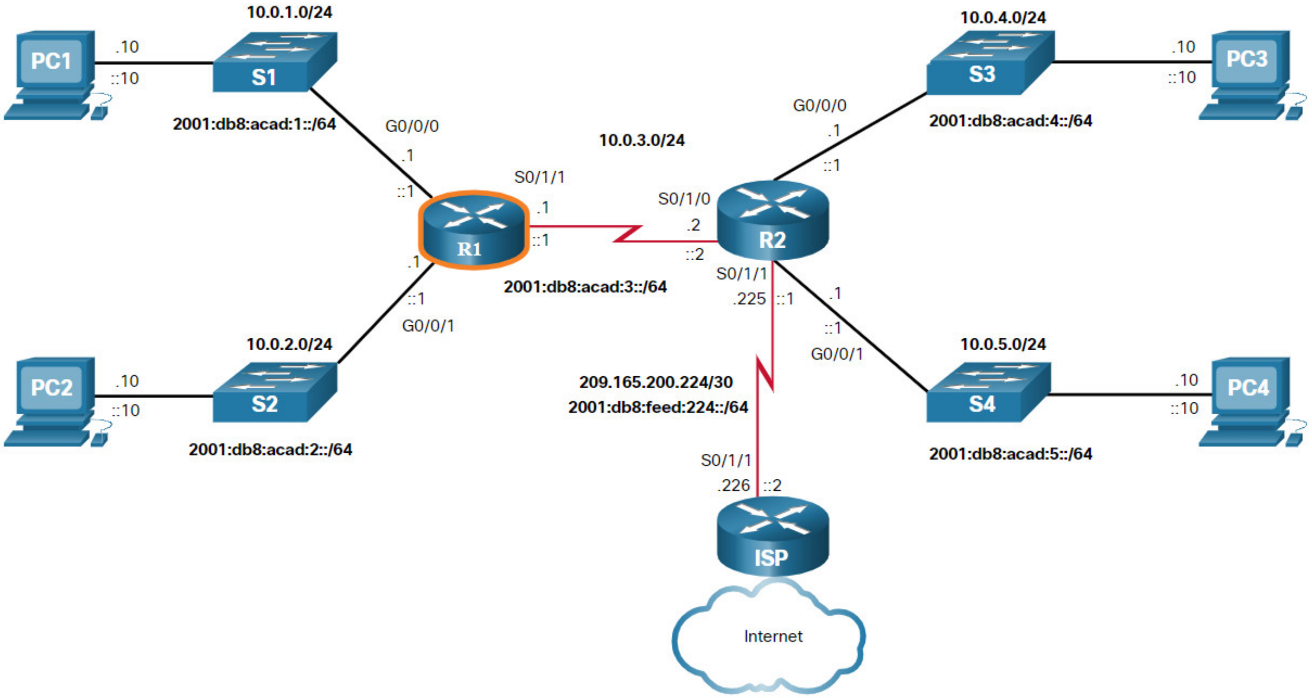
Another useful feature that improves user experience in the command-line interface (CLI) is filtering **show** output. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the **show** command and then enter a filtering parameter and a filtering expression.

The filtering parameters that can be configured after the pipe include:

- **section** – This displays the entire section that starts with the filtering expression.
- **include** – This includes all output lines that match the filtering expression.
- **exclude** – This excludes all output lines that match the filtering expression.
- **begin** – This displays all the output lines from a certain point, starting with the line that matches the filtering expression.

Note: Output filters can be used in combination with any **show** command.

The figure again shows the topology for your convenience



These examples demonstrate some of the more common uses of filtering parameters.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 121A0C0411044C
 login
 transport input telnet ssh
R1#
R1# show ipv6 interface brief | include up
GigabitEthernet0/0/0   [up/up]
GigabitEthernet0/0/1   [up/up]
Serial0/1/1            [up/up]
R1#
R1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/1            209.165.200.225 YES manual up                    up
R1#
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/1
L        209.165.200.225/32 is directly connected, Serial0/1/1
R1#
```

14.3.5 Packet Tracer – Basic Router Configuration Review

Routers R1 and R2 each have two LANs. R1 is already configured. Your task is to configure the appropriate addressing for R2 and verify connectivity between the LANs.

14.3.5 Packet Tracer – Basic Router Configuration Review

14.4 IP Routing Table

14.4.1 Route Sources

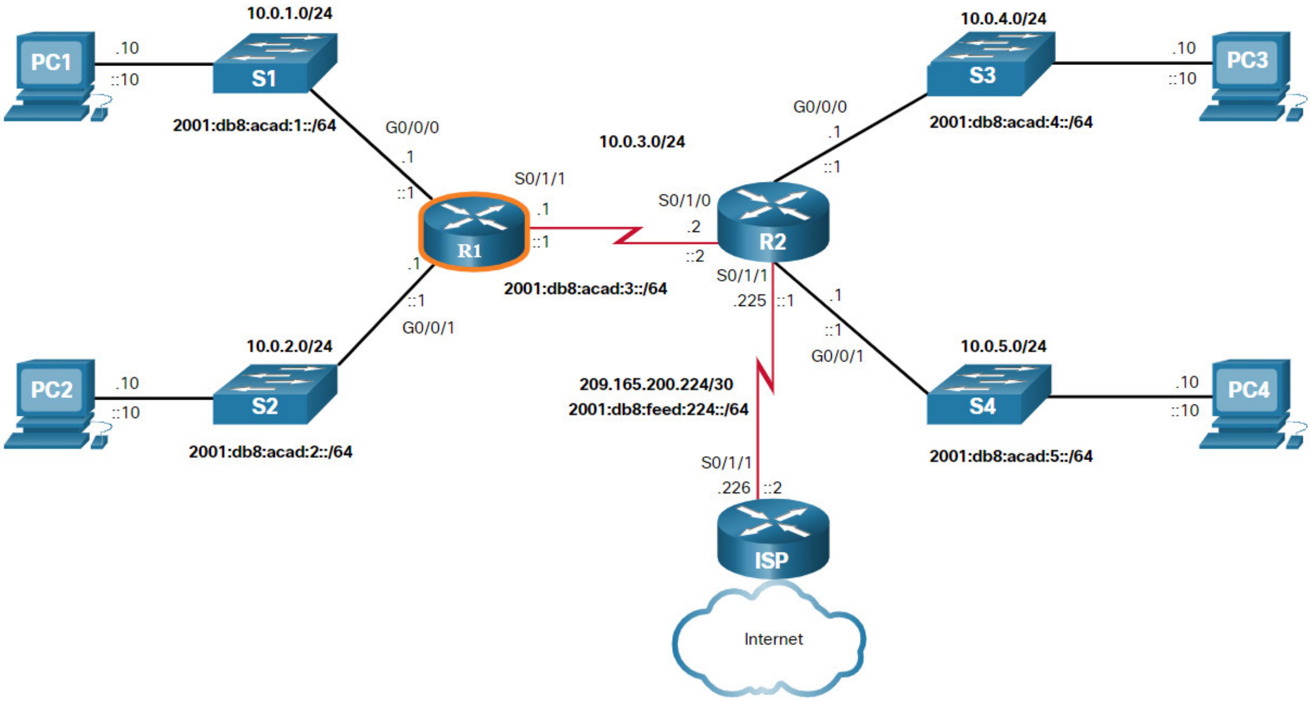
How does a router know where it can send packets? It creates a routing table that is based on the network in which it is located.

A routing table contains a list of routes to known networks (prefixes and prefix lengths). The source of this information is derived from the following:

- Directly connected networks
- Static routes

- Dynamic routing protocols

In the figure, R1 and R2 are using the dynamic routing protocol OSPF to share routing information. In addition, R2 is configured with a default static route to ISP.



- R1 Routing Table
- R2 Routing Table

R1 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
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 10.0.3.2 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L        10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C        10.0.3.0/24 is directly connected, Serial0/1/1
L        10.0.3.1/32 is directly connected, Serial0/1/1
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1#
```

In the routing tables for R1 and R2, notice that the sources for each route are identified by a code. The code identifies how the route was learned. For instance, common codes include the following:

- **L** – Identifies the address assigned to a router interface. This allows the router to efficiently determine when it receives a packet for the interface instead of being forwarded.
- **C** – Identifies a directly connected network.
- **S** – Identifies a static route created to reach a specific network.
- **O** – Identifies a dynamically learned network from another router using the OSPF routing protocol.
- ***** – This route is a candidate for a default route.

14.4.2 Routing Table Principles

There are three routing table principles as described in the table. These are issues that are addressed by the proper configuration of dynamic routing protocols or static routes on all the routers between the source and destination devices.

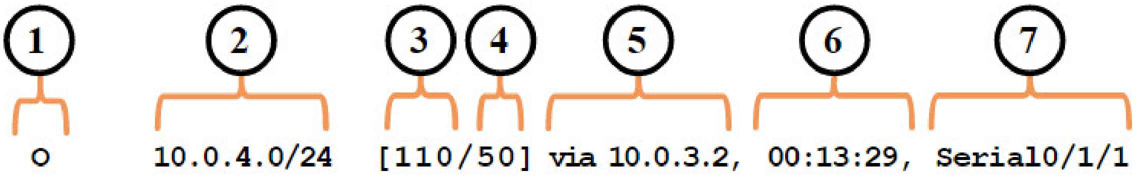
Routing Table Principle	Example

Routing Table Principle	Example
Every router makes its decision alone, based on the information it has in its own routing table.	• R1 can only forward packets using its own routing table. • R1 does not know what routes are in the routing tables of other routers (e.g., R2).
The information in a routing table of one router does not necessarily match the routing table of another router.	Just because R1 has route in its routing table to a network in the internet via R2, that does not mean that R2 knows about that same network.
Routing information about a path does not provide return routing information.	R1 receives a packet with the destination IP address of PC1 and the source IP address of PC3. Just because R1 knows to forward the packet out its G0/0/0 interface, doesn't necessarily mean that it knows how to forward packets originating from PC1 back to the remote network of PC3.

14.4.3 Routing Table Entries

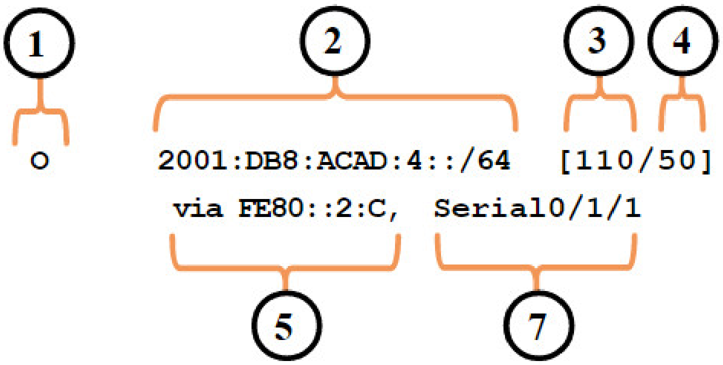
As a network administrator, it is imperative to know how to interpret the content of IPv4 and IPv6 routing tables. The figure displays IPv4 and IPv6 routing table entries on R1 for the route to remote network 10.0.4.0/24 and 2001:db8:acad:4::/64. Both these routes were learned dynamically from the OSPF routing protocol.

IPv4 Routing Table



```
O     10.0.4.0/24  [110/50] via 10.0.3.2,  00:13:29,  Serial0/1/1
```

IPv6 Routing Table



```
O     2001:DB8:ACAD:4::/64  [110/50]
       via FE80::2:C,  Serial0/1/1
```

In the figure, the numbers identify the following information:

1. **Route source** – This identifies how the route was learned.
2. **Destination network (prefix and prefix length)** – This identifies the address of the remote network.
3. **Administrative distance** – This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
4. **Metric** – This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
5. **Next-hop** – This identifies the IP address of the next router to which the packet would be forwarded.
6. **Route timestamp** – This identifies how much time has passed since the route was learned.
7. **Exit interface** – This identifies the egress interface to use for outgoing packets to reach their final destination.

Note: The prefix length of the destination network specifies the minimum number of far-left bits that must match between the IP address of the packet and the destination network (prefix) for this route to be used.

14.4.4 Directly Connected Networks

Before a router can learn about any remote networks, it must have at least one active interface configured with an IP address and subnet mask (prefix length). This is known as a directly connected network or a directly connected route. Routers add a directly connected route to its routing table when an interface is configured with an IP address and is activated.

A directly connected network is denoted by a status code of **C** in the routing table. The route contains a network prefix and prefix length.

The routing table also contains a local route for each of its directly connected networks, indicated by the status code of **L**. This is the IP address that is assigned to the interface on that directly connected network. For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match. The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

Directly connected networks and local routes are shown in the following output.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(Output omitted)
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
R1#
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
R1#
```

14.4.5 Static Routes

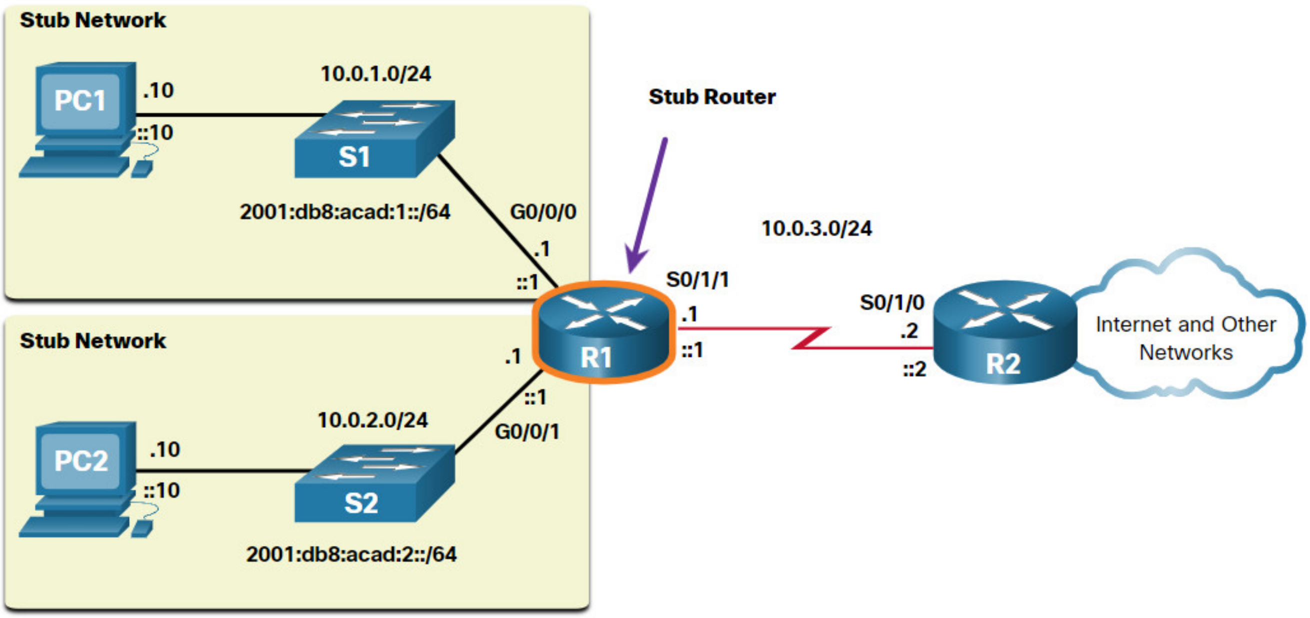
After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks.

Static routes are manually configured. They define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include improved security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols, and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routing has three primary uses:

- It provides ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- It uses 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.
- It routes to and from stub networks. A stub network is a network accessed by a single route, and the router has only one neighbor.

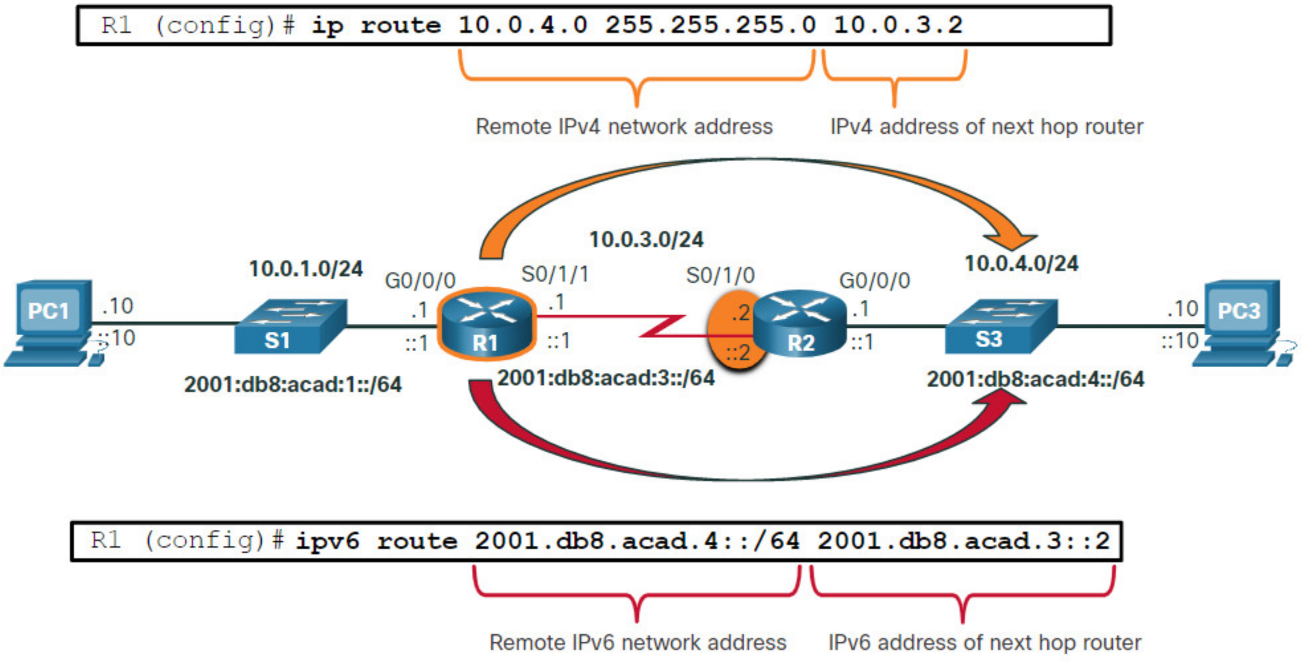
The figure shows an example of stub networks. Notice that any network attached to R1 would only have one way to reach other destinations, whether to networks attached to R2, or to destinations beyond R2. This means that networks 10.0.1.0/24 and 10.0.2.0/24 are stub networks and R1 is a stub router.



In this example, a static route can be configured on R2 to reach the R1 networks. Additionally, because R1 has only one way to send out non-local traffic, a default static route can be configured on R1 to point to R2 as the next hop for all other networks.

14.4.6 Static Routes in the IP Routing Table

For demonstrating static routing, the topology in the figure is simplified to show only one LAN attached to each router. The figure shows IPv4 and IPv6 static routes configured on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2. The configuration commands are for demonstration only and are discussed in another module.



```
R1 (config)# ip route 10.0.4.0 255.255.255.0 10.0.3.2
```

```
R1 (config)#ipv6 route 2001.db8.acad.4::/64 2001.db8.acad.3::2
```

The output shows the IPv4 and IPv6 static routing entries on R1 that can reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2. Notice that both routing entries use the status code of **S** indicating that the route was learned by a static route. Both entries also include the IP address of the next hop router, via *ip-address*. The **static** parameter at the end of the command displays only static routes.

```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(output omitted)

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
S        10.0.4.0/24 [1/0] via 10.0.3.2
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(output omitted)

S   2001:DB8:ACAD:4::/64 [1/0]
     via 2001:DB8:ACAD:3::2
```

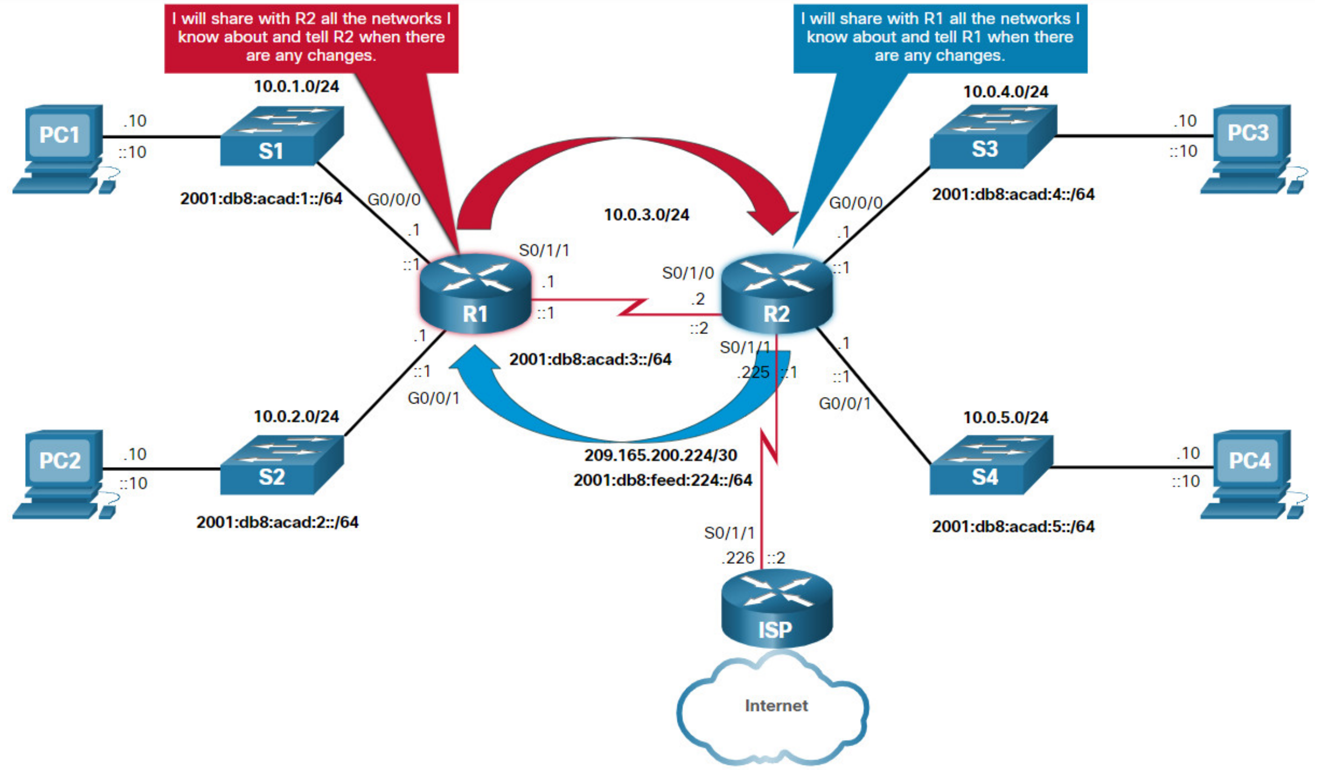
14.4.7 Dynamic Routing Protocols

Dynamic routing protocols are used by routers to automatically share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.

Important advantages of dynamic routing protocols are the ability to select a best path, and the ability to automatically discover a new best path when there is a change in the topology.

Network discovery is the ability of a routing protocol to share information about the networks that it knows about with other routers that are also using the same routing protocol. Instead of depending on manually configured static routes to remote networks on every router, a dynamic routing protocol allows the routers to automatically learn about these networks from other routers. These networks, and the best path to each, are added to the routing table of the router, and identified as a network learned by a specific dynamic routing protocol.

The figure shows routers R1 and R2 using a common routing protocol to share network information.



14.4.8 Dynamic Routes in the IP Routing Table

A previous example used static routes to the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks. These static routes are no longer configured and OSPF is now being used to dynamically learn all the networks connected to R1 and R2. The following examples show the IPv4 and IPv6 OSPF routing entries on R1 that can reach these networks on R2. Notice that both routing entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol. Both entries also include the IP address of the next-hop router, via *ip-address*.

Note: IPv6 routing protocols use the link-local address of the next-hop router.

Note: OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

```
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
(output omitted for brevity)
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O   2001:DB8:ACAD:4::/64 [110/50]
     via FE80::2:C, Serial0/1/1
O   2001:DB8:ACAD:5::/64 [110/50]
     via FE80::2:C, Serial0/1/1
```

14.4.9 Default Route

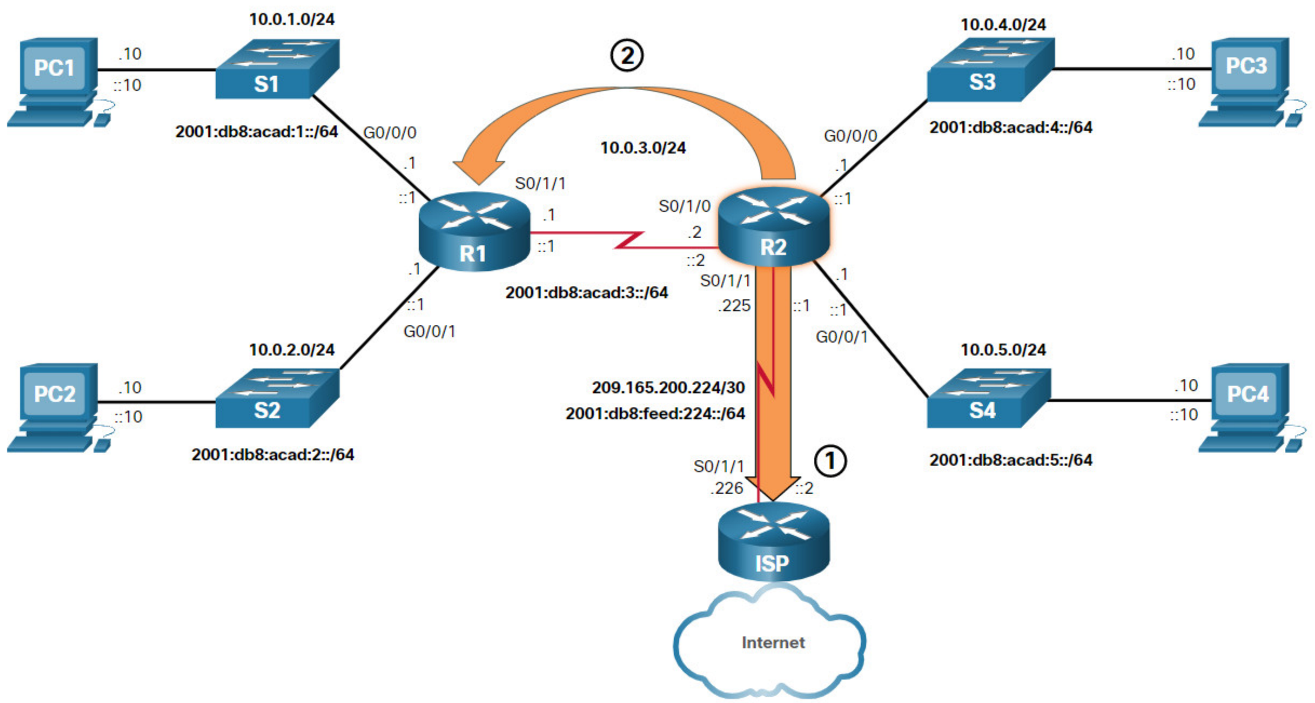
A default route is similar to a default gateway on a host. The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address.

A default route can be either a static route or learned automatically from a dynamic routing protocol. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or no bits need to match between the destination IP address and the default route.

Most enterprise routers have a default route in their routing table. This is to reduce the number of routes in a routing table.

A router, such as a home or small office router that only has one LAN, may reach all its remote networks through a default route. This is useful when the router has only directly connected networks and one exit point to a service provider router.

In the figure, routers R1 and R2 are using OSPF to share routing information about their own networks (10.0.x.x/24 and 2001:db8:acad:x::/64 networks). R2 has a static default route to the ISP router. R2 will forward any packets with a destination IP address that does not specifically match one of the networks in its routing table to the ISP router. This would include all packets destined for the internet.



1. R2 has a static default route to the ISP router.
2. The default route is advertised by R2 to R1 using the dynamic routing protocol OSPF.

R2 has shared its default route with R1 using OSPF. R1 will now have a default route in its routing table that it learned dynamically from OSPF. R1 will also forward any packets with a destination IP address that does not specifically match one of the networks in its routing table to R2.

The following examples show the IPv4 and IPv6 routing table entries for the static default routes configured on R2.

```
R2# show ip route
(Output omitted)
S*    0.0.0.0/0 [1/0] via 209.165.200.226
R2#
R2# show ipv6 route
(Output omitted)
S   ::/0 [1/0]
     via 2001:DB8:FEED:224::2
R2#
```

14.4.10 Structure of an IPv4 Routing Table

IPv4 was standardized in the early 1980s using the now obsolete classful addressing architecture. The IPv4 routing table is organized using this same classful structure. In the **show ip route** output, notice that some route entries are left justified while others are indented. This is based on how the routing process searches the IPv4 routing table for the longest match. This was all because of classful addressing. Although the lookup process no longer uses classes, the structure of the IPv4 routing table still retains in this format.

```
Router# show ip route
(Output omitted)
     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
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
Router#
```

Note: The IPv4 routing table in the example is not from any router in the topology used in this module.

Although the details of the structure are beyond the scope of this module, it is helpful to recognize the structure of the table. An indented entry is known as a child route. A route entry is indented if it is the subnet of a classful address (class A, B or C network). Directly connected networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32. The child route will include the route source and all the forwarding information such as the next-hop address. The classful network address of this subnet will be shown above the route entry, less indented, and without a source code. That route is known as a parent route.

Note: This is just a brief introduction to the structure of an IPv4 routing table and does not cover details or specifics of this architecture.

The next example shows the IPv4 routing table of R1 in the topology. Notice that all of the networks in the topology are subnets, which are child routes, of the class A network and parent route10.0.0.0/8.

```
R1# show ip route
(output omitted for brevity)
O*E2  0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L        10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C        10.0.3.0/24 is directly connected, Serial0/1/1
L        10.0.3.1/32 is directly connected, Serial0/1/1
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1#
```

14.4.11 Structure of an IPv6 Routing Table

The concept of classful addressing was never part of IPv6, so the structure of an IPv6 routing table is very straight forward. Every IPv6 route entry is formatted and aligned the same way.

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
     via FE80::2:C, Serial0/0/1
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/1, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/1, receive
O   2001:DB8:ACAD:4::/64 [110/50]
     via FE80::2:C, Serial0/1/1
O   2001:DB8:ACAD:5::/64 [110/50]
     via FE80::2:C, Serial0/1/1
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

14.4.12 Administrative Distance

A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, it is possible that the routing table learns about the same network address from more than one routing source.

Except for very specific circumstances, only one dynamic routing protocol should be implemented on a router. However, it is possible to configure both OSPF and EIGRP on a router, and both routing protocols may learn of the same destination network. Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.

This raises a few questions, such as the following:

- How does the router know which source to use?
- Which route should it install in the routing table? The route learned from OSPF, or the route learned from EIGRP?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the “trustworthiness” of the route. The lower the AD, the more trustworthy the route source. Because EIGRP has an AD of 90 and OSPF has an AD of 110, the EIGRP route entry would be installed in the routing table.

Note: The AD does not necessarily represent which dynamic routing protocol is best.

A more common example is a router learning the same network address from a static route and a dynamic routing protocol, such as OSPF. A static route has an AD of 1, whereas an OSPF-discovered route has an AD of 110. Given two separate route sources to the same destination, the router chooses to install the route with the lowest AD. When a router has the choice of a static route and an OSPF route, the static route takes precedence.

Note: Directly connected networks have the lowest AD of 0. Only a directly connected network can have an AD of 0.

The table lists various routing protocols and their associated ADs.

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120

Route Source	Administrative Distance
External EIGRP	170
Internal BGP	200

14.5 Static and Dynamic Routing

14.5.1 Static or Dynamic?

The previous topic discussed the ways that a router creates its routing table. So, you now know that routing, like IP addressing, can be either static or dynamic. Should you use static or dynamic routing? The answer is both! Static and dynamic routing are not mutually exclusive. Rather, most networks use a combination of dynamic routing protocols and static routes.

Static Routes

Static routes are commonly used in the following scenarios:

- As a default route forwarding packets to a service provider
- For routes outside the routing domain and not learned by the dynamic routing protocol
- When the network administrator wants to explicitly define the path for a specific network
- For routing between stub networks

Static routes are useful for smaller networks with only one path to an outside network. They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.

Dynamic Routing Protocols

Dynamic routing protocols help the network administrator manage the time-consuming and exacting process of configuring and maintaining static routes. Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers. Dynamic routing protocols are scalable and automatically determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

- In networks consisting of more than just a few routers
- When a change in the network topology requires the network to automatically determine another path

- For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

The table shows a comparison of some the differences between dynamic and static routing.

Feature	**Dynamic Routing**	**Static Routing**
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed
Path Predictability	Route depends on topology and routing protocol used	Explicitly defined by the administrator

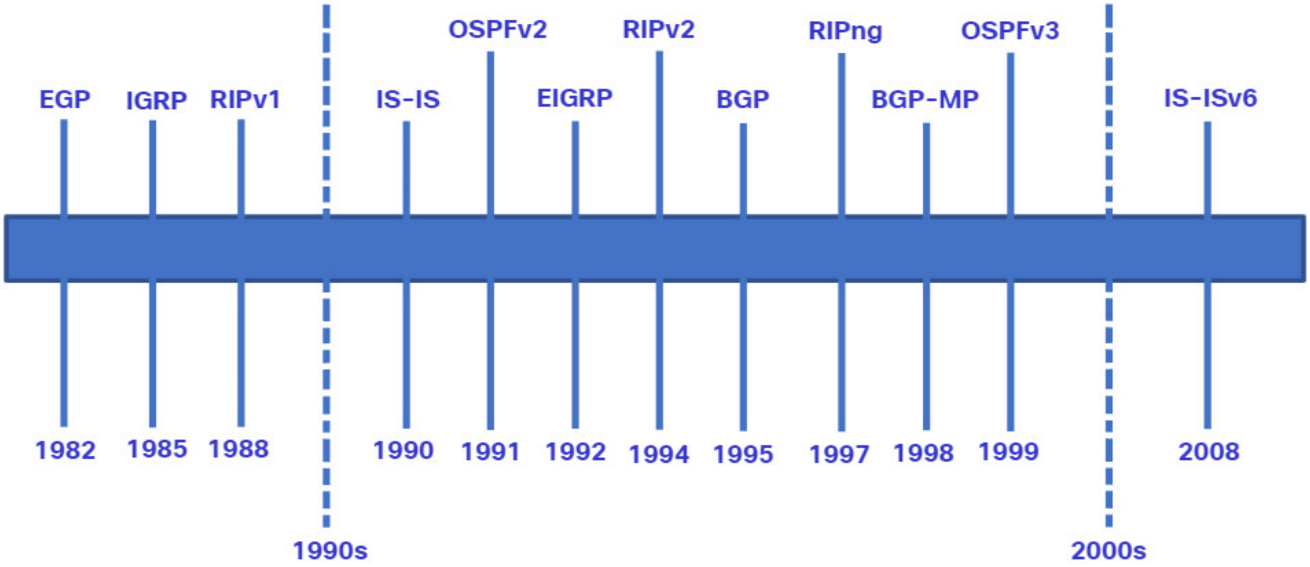
14.5.2 Dynamic Routing Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969.

As networks evolved and became more complex, new routing protocols emerged. The RIP protocol was updated to RIPv2 to accommodate growth in the network environment. However, RIPv2 still does not scale to the larger network implementations of today. To address the needs of larger networks, two advanced routing protocols were developed: OSPF and Intermediate System-to-Intermediate System (IS-IS). Cisco developed the Interior Gateway Routing Protocol (IGRP), which was later replaced by Enhanced IGRP (EIGRP), which also scales well in larger network implementations.

Additionally, there was the need to connect the different routing domains of different organizations and provide routing between them. The Border Gateway Protocol (BGP), the successor of Exterior Gateway Protocol (EGP) is used between Internet Service Providers (ISPs). BGP is also used between ISPs and some private organizations to exchange routing information.

The figure displays the timeline of when the various protocols were introduced.



To support IPv6 communication, newer versions of the IP routing protocols have been developed, as shown in the IPv6 row in the table.

The table classifies the current routing protocols. Interior Gateway Protocols (IGPs) are routing protocols used to exchange routing information within a routing domain administered by a single organization. There is only one EGP and it is BGP. BGP is used to exchange routing information between different organizations, known as autonomous systems (AS). BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.

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

14.5.3 Dynamic Routing Protocol Concepts

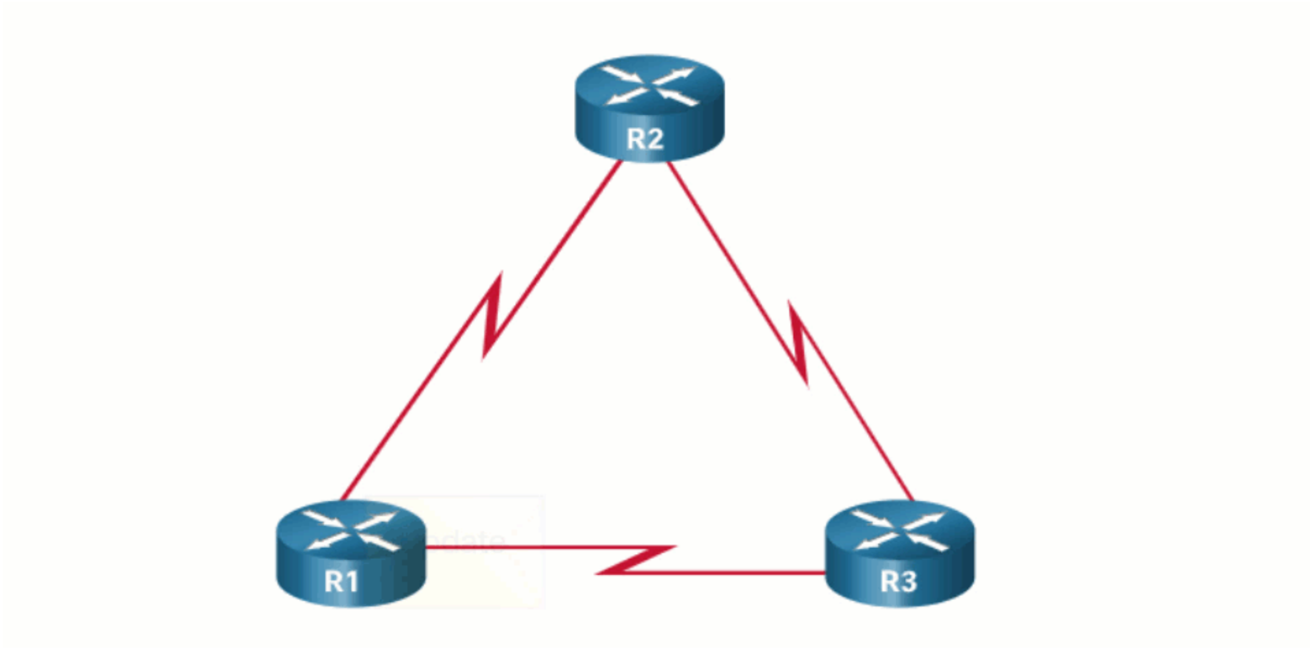
A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the choice of best paths. The purpose of dynamic routing protocols includes the following:

- 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

The main components of dynamic routing protocols include the following:

- **Data structures –** Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages –** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm –** An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for the best path determination.

Routing protocols allow routers to dynamically share information about remote networks and automatically offer this information to their own routing tables. Click Play to see an animation of this process.



Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table if there is not another routing source with a lower AD. A primary benefit of dynamic routing protocols is that routers exchange routing information when there is a topology change. This exchange allows routers to automatically learn about new networks and to find alternate paths when there is a link failure to a current network.

14.5.4 Best Path

Before a path to a remote network is offered to the routing table, the dynamic routing protocol must determine the best path to that network. Determining the best path may involve the evaluation of multiple paths to the same destination network and selecting the optimum or shortest path to reach that network. Whenever multiple paths to the same network exist, each path uses a different exit interface on the router to reach that network.

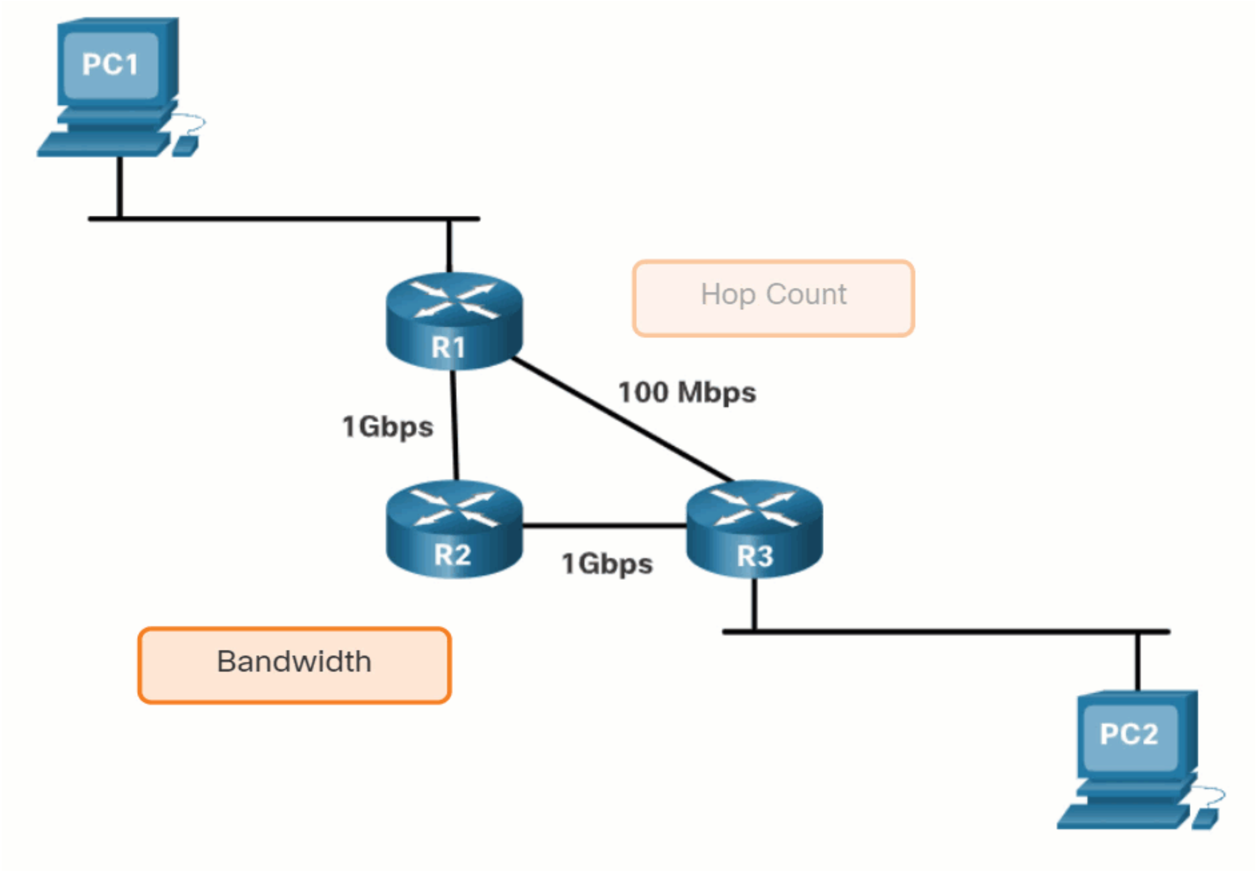
The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The routing algorithm generates a value, or a metric, for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path. Some routing protocols can base route selection on multiple metrics, combining them into a single metric.

The following table lists common dynamic protocols and their metrics.

Routing Protocol	Metric
Routing Information Protocol (RIP)	• The metric is “hop count”. • Each router along a path adds a hop to the hop count. • A maximum of 15 hops allowed.
Open Shortest Path First (OSPF)	• The metric is “cost” which is the based on the cumulative bandwidth from source to destination. • Faster links are assigned lower costs compared to slower (higher cost) links.
Enhanced Interior Gateway Routing Protocol (EIGRP)	• It calculates a metric based on the slowest bandwidth and delay values. • It could also include load and reliability into the metric calculation.

The animation in the figure highlights how the path may be different depending on the metric being used. If the best path fails, the dynamic routing protocol will automatically select a new best path if one exists.



14.5.5 Load Balancing

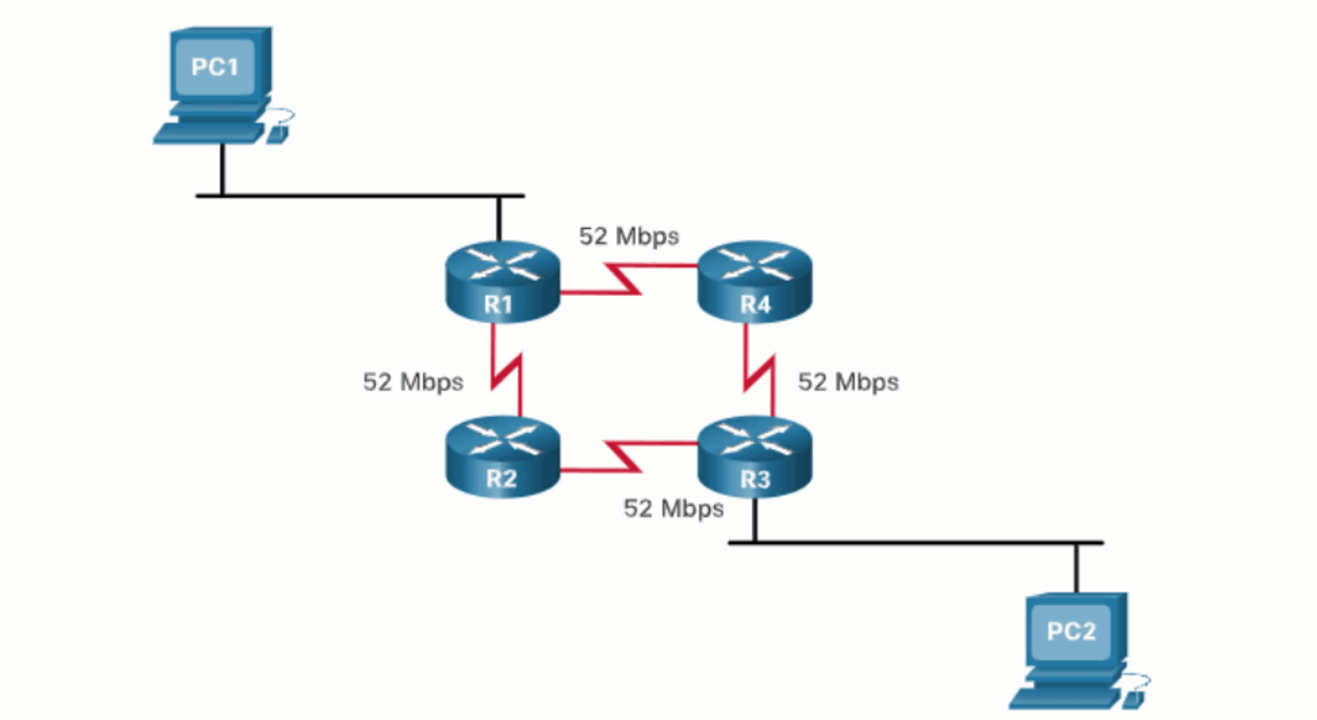
What happens if a routing table has two or more paths with identical metrics to the same destination network?

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. The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.

If configured correctly, load balancing can increase the effectiveness and performance of the network.

Equal cost load balancing is implemented automatically by dynamic routing protocols. It is enabled with static routes when there are multiple static routes to the same destination network using different next-hop routers.

Note: Only EIGRP supports unequal cost load balancing.



14.6 Module Practice and Quiz

14.6.1 What did I learn in this module?

Path Determination

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination. The best path in the routing table is also known as the longest match. The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. Directly connected networks are networks that are configured on the active interfaces of a router. A directly connected network is added to the routing table when an interface is configured with an IP address and subnet mask (prefix length) and is active (up and up). Routers learn about remote networks in two ways: static routes are added to the routing table when a route is manually configured, and with dynamic routing protocols. Using dynamic routing protocols such as EIGRP and OSPF, routes are added to the routing table when routing protocols dynamically learn about the remote network.

Packet Forwarding

After a router determines the correct path, it can forward the packet on a directly connected network, it can forward the packet to a next-hop router, or it can drop the packet. The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. Routers support three packet forwarding mechanisms: process switching, fast switching, and CEF. The following steps describe the packet forwarding process:

1. The data link frame with an encapsulated IP packet arrives on the ingress interface.
2. The router examines the destination IP address in the packet header and consults its IP routing table.
3. The router finds the longest matching prefix in the routing table.
4. The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.
5. However, if there is no matching route entry the packet is dropped.

Basic Router Configuration Review

There are several configuration and verification commands for routers, including **show ip route**, **show ip interface**, **show ip interface brief** and **show running-config**. To reduce the amount of command output, use a filter. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the **show** command and then enter a filtering parameter and a filtering expression. The filtering parameters that can be configured after the pipe include the following:

- **section** – Shows entire section that starts with the filtering expression
- **include** – Includes all output lines that match the filtering expression
- **exclude** – Excludes all output lines that match the filtering expression
- **begin** – Shows all the output lines from a certain point, starting with the line that matches the filtering expression

IP Routing Table

A routing table contains a list of routes known networks (prefixes and prefix lengths). The source of this information is derived from directly connected networks, static routes, and dynamic routing protocols. Common routing table codes include:

- **L** – Identifies the address assigned to a router interface. This allows the router to efficiently determine when it receives a packet for the interface instead of being forwarded.
- **C** – Identifies a directly connected network.
- **S** – Identifies a static route created to reach a specific network.
- **O** – Identifies a dynamically learned network from another router using the OSPF routing protocol.
- * – This route is a candidate for a default route.

Every router makes its decision alone, based on the information it has in its own routing table. The information in a routing table of one router does not necessarily match the routing table of another router. Routing information about a path does not provide return routing information. Routing table entries include the route source, destination network, AD, metric, next-hop, route timestamp, and exit interface. To learn about remote networks, a router must have at least one active interface configured with an IP address and subnet mask (prefix length), called a directly connected network. Static routes are manually configured and define an explicit path between two networking devices. Dynamic routing protocols can discover a network, maintain routing tables, select a best path, and automatically discover a new best path if the topology changes. The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. A default route can be either a static route or learned automatically from a dynamic routing protocol. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. IPv4 routing tables still have a structure based on classful addressing represented by levels of indentation. IPv6 routing tables do not use the IPv4 routing table structure. Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.

Static and Dynamic Routing

Static routes are commonly used:

- As a default route forwarding packets to a service provider.
- For routes outside the routing domain and not learned by the dynamic routing protocol.
- When the network administrator wants to explicitly define the path for a specific network.
- For routing between stub networks.

Dynamic routing protocol are commonly used:

- In networks consisting of more than just a few routers
- When a change in the network topology requires the network to automatically determine another path
- For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

Current routing protocols include IGPs and EGPs. IGPs exchange routing information within a routing domain administered by a single organization. The only EGP is BGP. BGP exchanges routing information between different organizations. BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path. The main components of dynamic routing protocols are data structures, routing protocol messages, and algorithms. The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric. 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.

14.6.2 Module Quiz – Routing Concepts

Download Slide Powerpoint (PPT)

PPT

CCNA 2 v7.0 Curriculum: Module 14 - Routing Concepts.pptx

1 file(s) 1.53 MB

Download

Tags:ccna 2 v7 modules