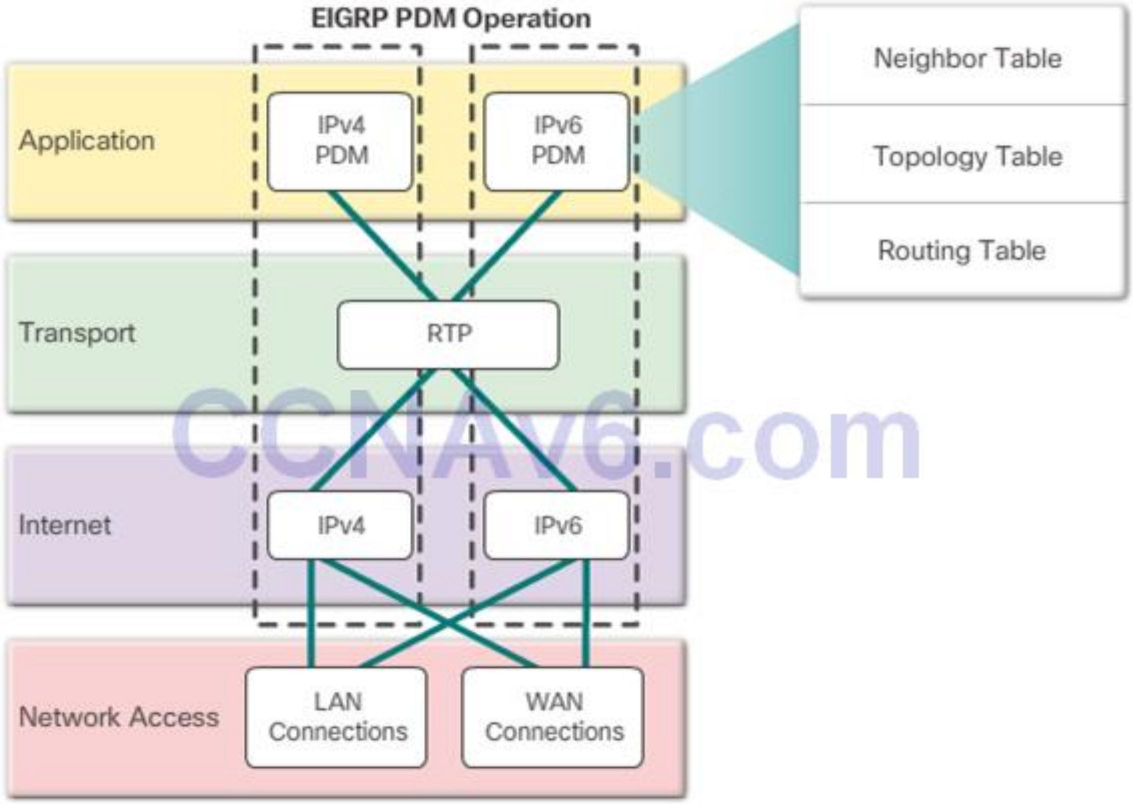
6.1 EIGRP Characteristics

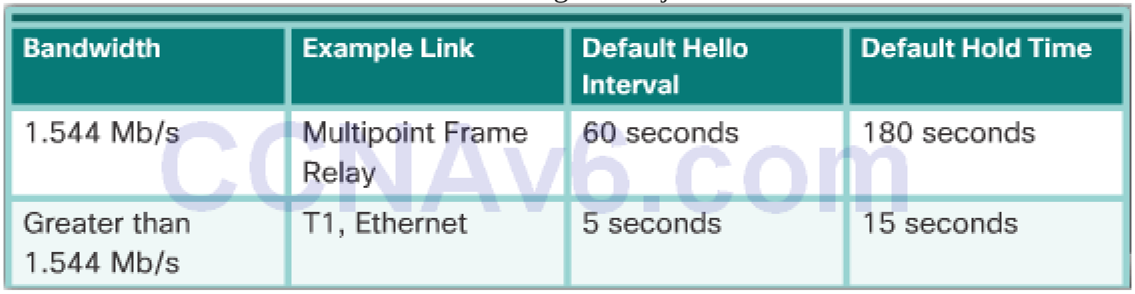
EIGRP Basic Features

- Features of EIGRP
- Uses the Diffusing Update Algorithm (DUAL) to calculate paths and back-up paths.
- Establishes Neighbor Adjacencies.
- Uses the Reliable Transport Protocol to provide delivery of EIGRP packets to neighbors.
- Partial and Bounded Updates. Sends updates only when there is a change and only to the routers that need the information.
- Supports Equal and Unequal Cost Load Balancing.
- Protocol Dependent Modules – responsible for network layer protocol-specific tasks
- Sends and receives EIGRP packets that are encapsulated in IPv4
- Parses EIGRP packets and informs DUAL of the new information and DUAL makes routing decisions. The results are stored in the IPv4 routing table.
- Reliable Transport Protocol
- Used for the delivery and reception of EIGRP packets
- Can send EIGRP packets as unicast or multicast.
- Reserved IPv4 multicast address 224.0.0.10.
- Reserved IPv6 multicast address FF02::A.
- Authentication
- Only accepts routing information from other routers with the same authentication information
- Does not encrypt the routing updates



EIGRP Packet Types

- EIGRP Hello Packets
- Are sent as multicasts and uses RTP for unreliable delivery
- Used to form and maintain EIGRP neighbor adjacencies

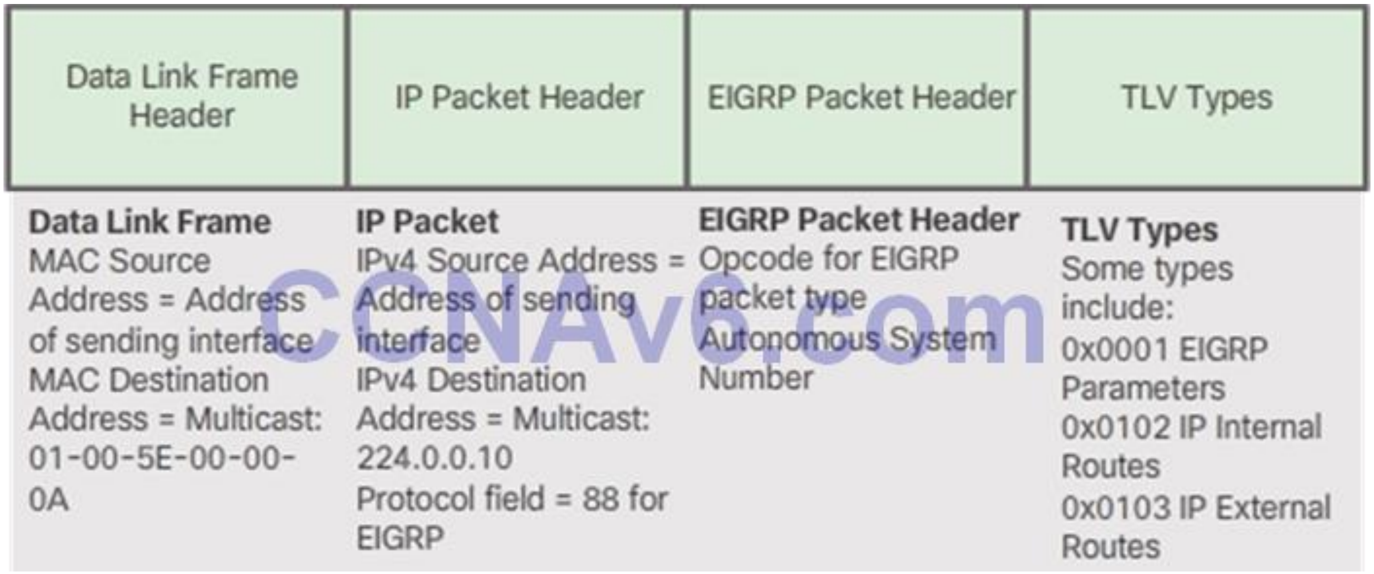


Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mb/s	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mb/s	T1, Ethernet	5 seconds	15 seconds

- EIGRP Update and Acknowledgment Packets
- Update packets propagate updated routing information when necessary to the routers that require the information using RTP
- Acknowledgment packets are send to acknowledge the update was received.
- EIGRP Query and Reply Packets
- Searches for networks
- Uses reliable delivery
- Queries are multicast or unicast. Replies are always unicast.

EIGRP Messages

- Encapsulating EIGRP Messages
- The EIGRP packet headers and TLV are encapsulated in an IP packet.
- EIGRP Packet Header and TLV
- EIGRP Packet Header
- EIGRP Packet Type: Update, Query, Reply, and Hello
- Autonomous System Number is the ID for the EIGRP routing process
- EIGRP Parameters TLV
- K values: K1 and K3 are set to 1. Other K values are set to 0
- Hold Time: Maximum time the router should wait for the next hello
- Internal TLV
- The IP internal message is used to advertise EIGRP routes within an autonomous system.
- Important metric fields: delay, bandwidth, prefix length, and destination
- EIGRP TLV: External Routes
- The IP external message is used when external routes are imported into the EIGRP routing process.



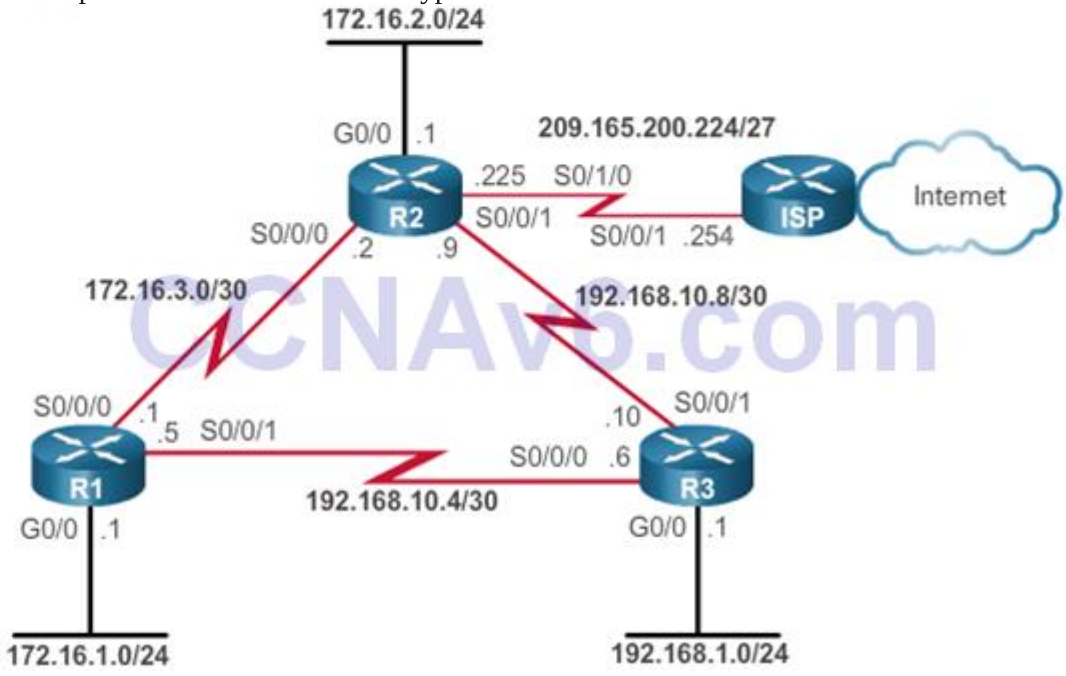
Data Link Frame Header	IP Packet Header	EIGRP Packet Header	TLV Types
Data Link Frame MAC Source Address = Address of sending interface MAC Destination Address = Multicast: 01-00-5E-00-00-0A	**IP Packet** IPv4 Source Address = Address of sending interface IPv4 Destination Address = Multicast: 224.0.0.10 Protocol field = 88 for EIGRP	**EIGRP Packet Header** Opcode for EIGRP packet type Autonomous System Number	**TLV Types** Some types include: 0x0001 EIGRP Parameters 0x0102 IP Internal Routes 0x0103 IP External Routes

6.2 Implement EIGRP for IPv4

Configure EIGRP with IPv4

- Autonomous System Numbers
- IANA globally assigned autonomous numbers
- Used by ISP and other large institutions
- Used in exterior routing protocol, such as BGP, to propagate routing information
- router eigrp autonomous-system command
- Autonomous system number is only significant to local EIGRP local domain
- Autonomous system number functions as a process ID
- All routers within the same domain must have the same autonomous system number
- The command is used to begin the EIGRP routing protocol
- EIGRP Router ID – uniquely identifies each router in the EIGRP routing domain
- Determined in 3 ways using the following order:
- The router router-id ipv4-address command
- The highest active IPv4 address of any of the loopback address
- The highest active IPv4 address of any of the physical interface
- The network ipv4-network-address router configuration mode command
- Enables any interface on the router that matches the network address in the network command to send and receive EIGRP updates
- By default, ipv4-network-address is the classful network address for each directly connected network
- The network command and Wildcard Mask
- network network-address [wildcard-mask]
- Wildcard mask is the inverse of a subnet mask
- To calculate the wildcard mask:
- 255.255.255.255
- – 255.255.255.252 Subnet mask
- ————————

- 0. 0. 0. 3 Wildcard mask
- Passive Interface – prevent the neighbor adjacencies
- Suppress unnecessary update traffic
- Increase security controls
- passive-interface interface-type interface-number



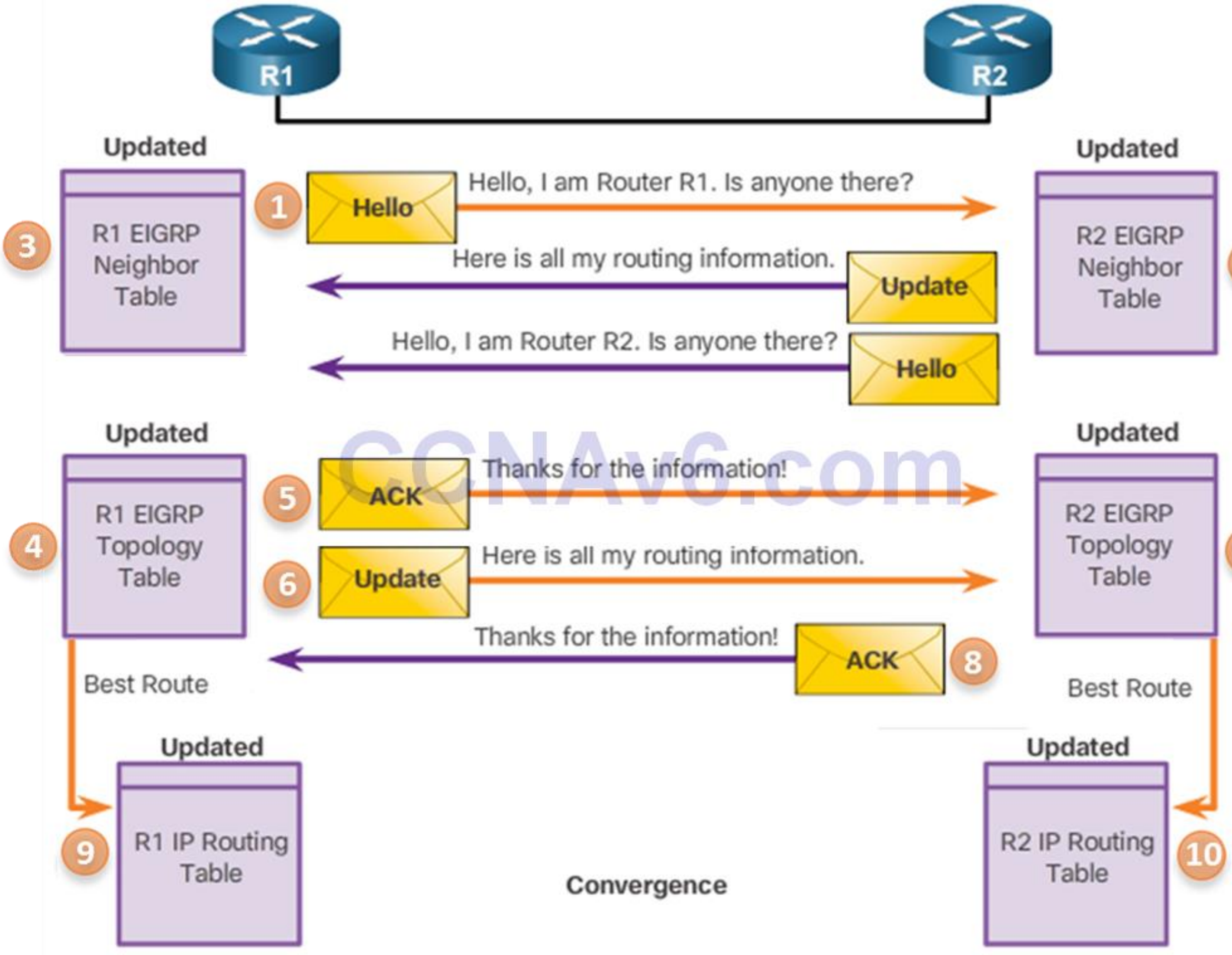
Verify EIGRP with IPv4

- The show commands are useful in verifying EIGRP operations and for debugging and troubleshooting purposes.
- show ip eigrp neighbors command
- View the neighbor table
- Verify neighbor adjacencies have been established
- show ip protocols Command
- Identify the parameters and other information about the current state of any active IPv4 routing protocol processes configured on the router
- What information can you get from this show command?
- show ip route
- Verify the routes are installed in the IPv4 routing table as expected
- Check for convergence

6.3 EIGRP Operation

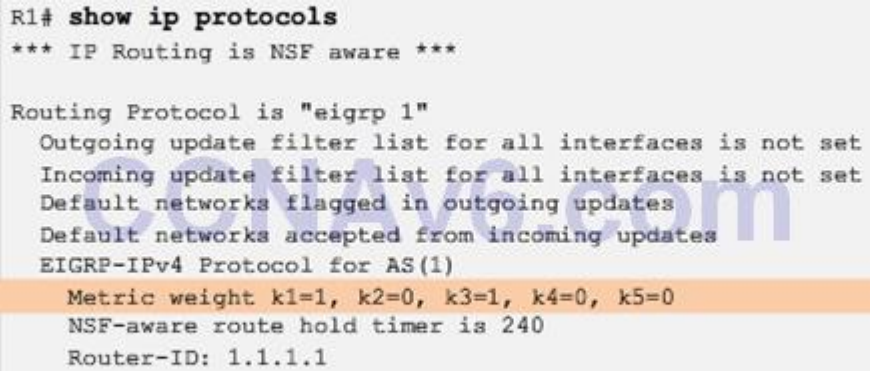
EIGRP Initial Route Discovery

- Can you describe the initial route discovery process?



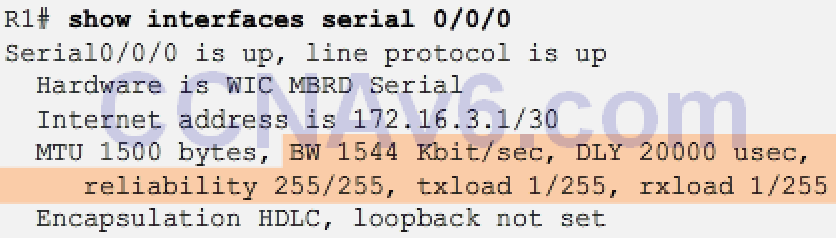
EIGRP Metrics

- Composite Metric
- EIGRP uses bandwidth and delay values in the composite metric to calculate the preferred path to a network.
- The k values and EIGRP AS number must match to form an adjacency.
- The show ip protocols command can be used to verify k values.
- Bandwidth Metric (BW)



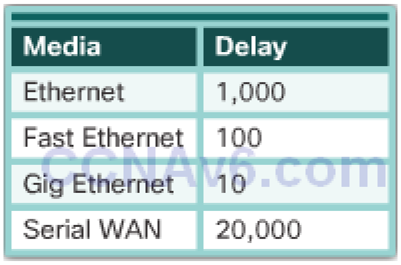
```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight k1=1, k2=0, k3=1, k4=0, k5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
```

- The bandwidth kilobits-bandwidth-value command is used to modify the bandwidth metric.
- Use the show interfaces command to verify the bandwidth changes
- Delay Metric (DLY)
- Delay is the measure of the time it takes for a packet to traverse a route.
- Use the show interfaces command to view the delay values.

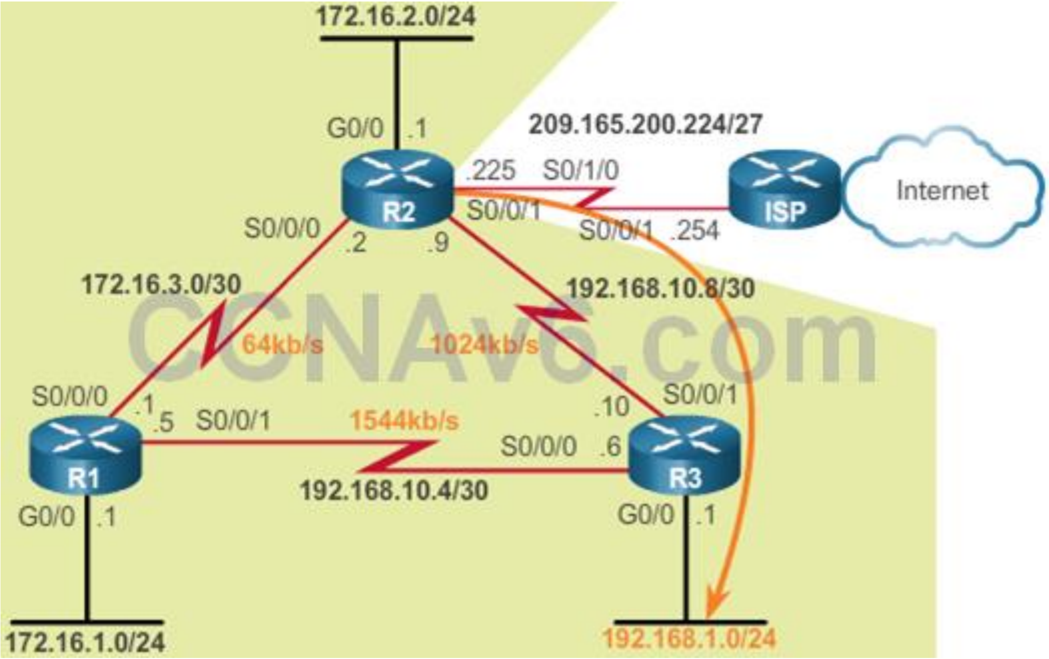


```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
```

- Complete Composite Metric Formula
- $(K1 * bandwidth + K2 * bandwidth\ 256 - load + K3 * delay) * K5\ reliability + K4 * 256$
- Using the default metric weight, the formula becomes
- Metric = $(K1 * bandwidth + K3 * delay) * 256$
- where K1 and K3 equal to 1, K2, K4, and K5 equal to 0 when not in use, and If K5 = 0, $K5\ reliability + K4$ becomes 1.
- Calculate the EIGRP metric between R2 and R3
- Metric = 256 $*(\ 10\ 7\ bandwidth$ + sum of delay 10)
- What is bandwidth of the slowest link?
- What is the sum of all delays?
- What command is used to verify the metric?

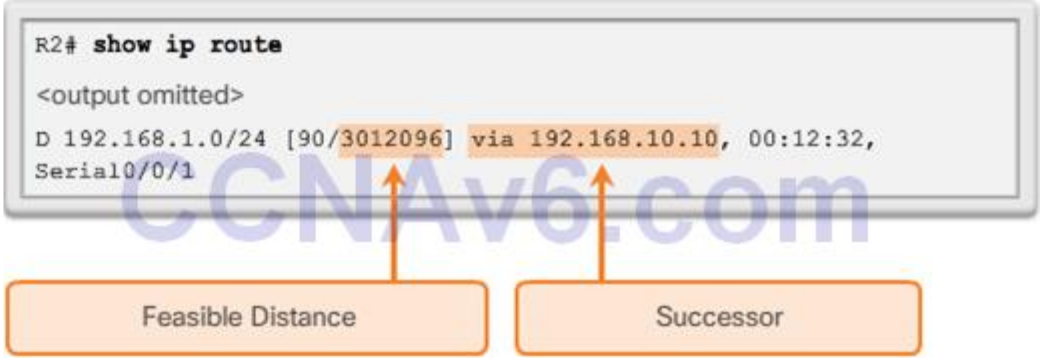


Media	Delay
Ethernet	1,000
Fast Ethernet	100
Gig Ethernet	10
Serial WAN	20,000



DUAL and the Topology Table

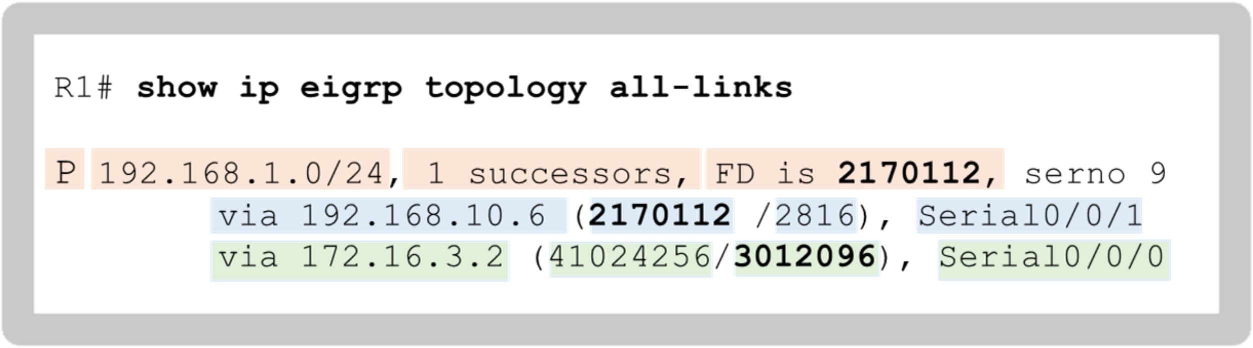
- Diffusing Update Algorithm (DUAL) provides
- Loop-free paths
- Loop-free backup paths that can be used immediately
- Fast convergence
- Successor and Feasible Distance
- A successor is a neighboring router that is used for packet forwarding and is the least-cost route to the destination network.
- Feasible Distance is the metric listed in the routing table entry
- Feasible Successors, Feasibility Condition, and Reported Distance
- The reported distance is an EIGRP neighbor's feasible distance to the destination network.
- The feasibility condition (FC) is met when a neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network.
- A feasible successor is a neighbor that has a loop-free backup path to the same network as the successor, and it satisfies the Feasibility Condition



```
R2# show ip route
<output omitted>
D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:12:32,
Serial0/0/1
```

- The show ip eigrp topology command

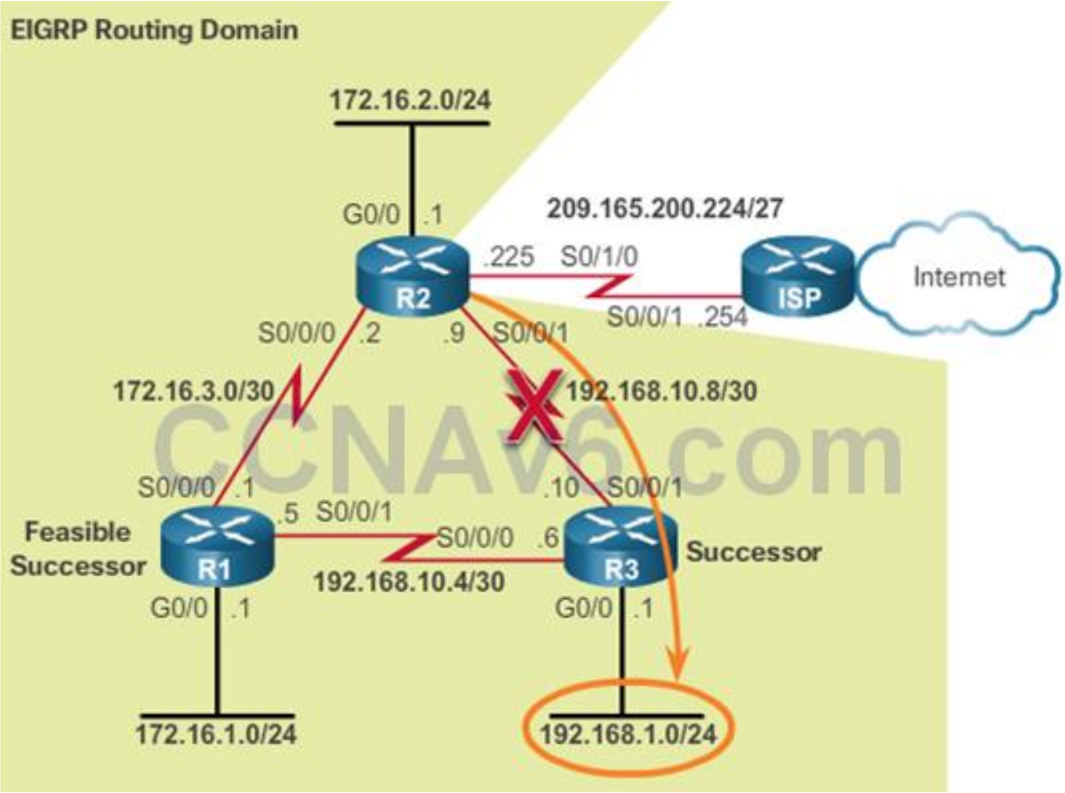
- Displays the Topology Table
- Topology Table
- Lists all successors and FSs to destination networks
- Only successors are installed in the routing tables
- Can you name all the highlighted parts in the topology table below?
- Which is the successor?
- Which is not a feasible successor?



```
R1# show ip eigrp topology all-links

P 192.168.1.0/24, 1 successors, FD is 2170112, serno 9
        via 192.168.10.6 (2170112 /2816), Serial0/0/1
        via 172.16.3.2 (41024256/3012096), Serial0/0/0
```

DUAL and Convergence

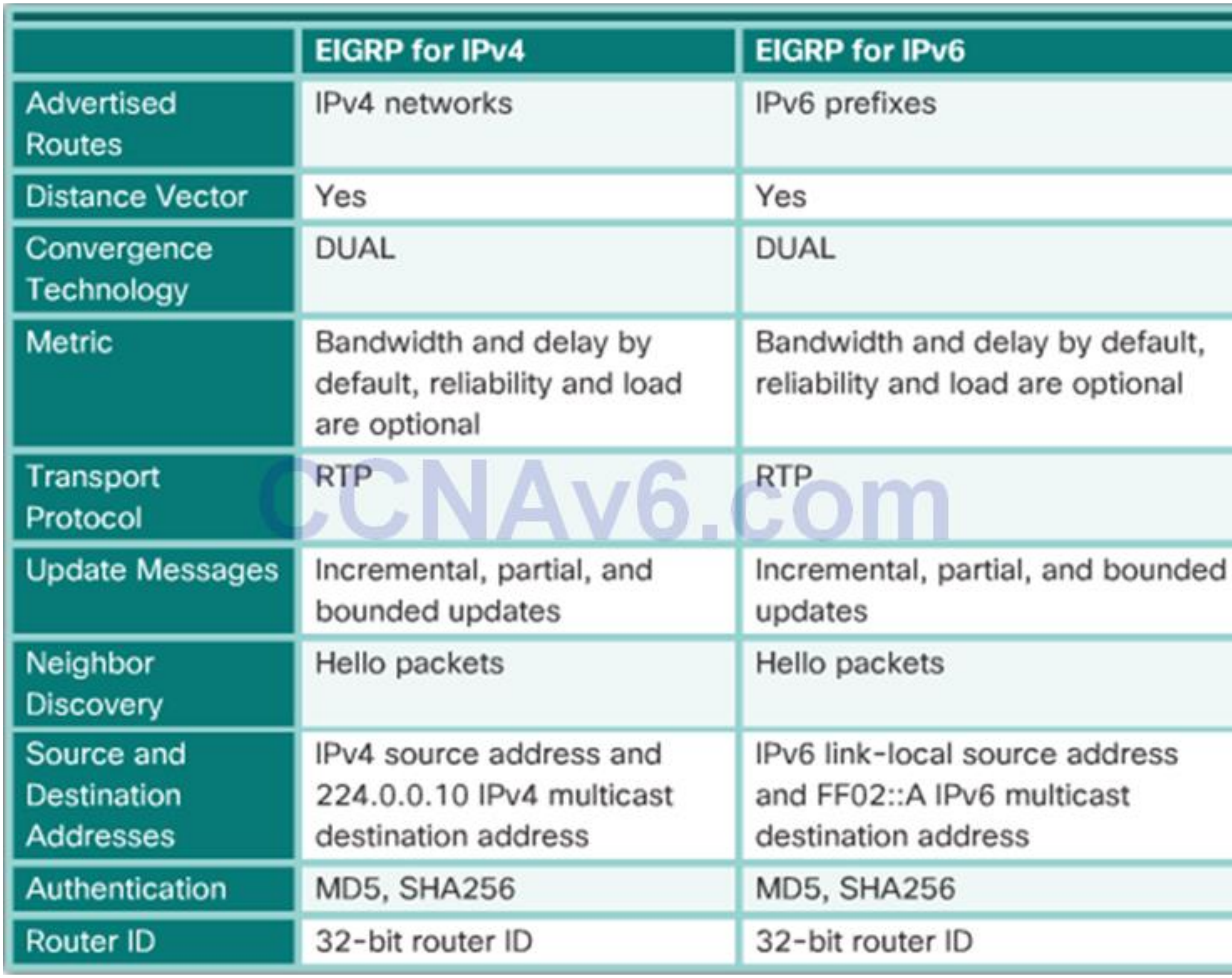
- DUAL Finite State Machine (FSM)
- Contains all of the logic used to calculate and compare routes in an EIGRP network
- DUAL: Feasible Successor
- When a path to the successor goes down with FS in the topology table:
- Router informs all EIGRP neighbors of the lost link.
- Router updates its own routing and topology table.
- DUAL: No Feasible Successor
- When a path to the successor goes down with no FS in the topology table:
- DUAL puts the route into an active state.
- DUAL sends EIGRP queries asking other routers for a path to the network.
- Other routers return EIGRP replies, letting the sender of the EIGRP query know that they have a path to the requested network. If there is no reply, the sender of the query does not have a route to this network.
- If the sender receives EIGRP replies with a path to the requested network, the preferred path is added as the new successor and also added to the routing table.



6.4 Implement EIGRP for IPv6

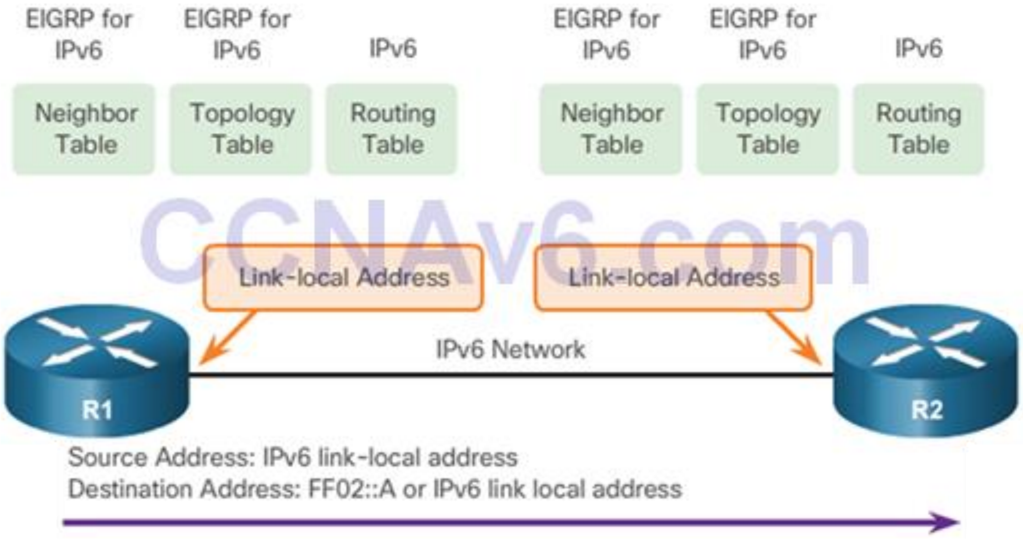
EIGRP for IPv6

- EIGRP for IPv6
- Similar functionality as EIGRP for IPv4
- Uses IPv6 for communicationwith EIGRP for IPv6 peers and advertising IPv6 routes
- Uses DUAL
- EIGRP for IPv6 is a separate process from EIGRP for IPv4



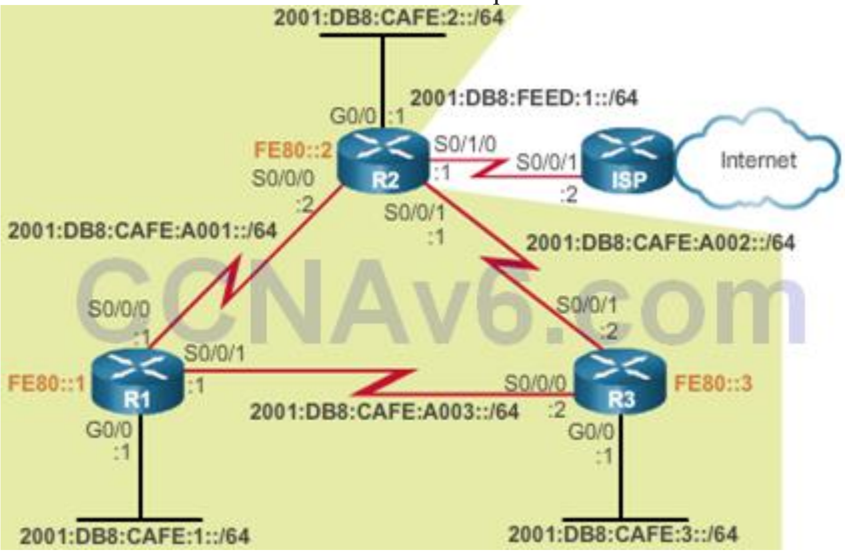
	EIGRP for IPv4	EIGRP for IPv6
Advertised Routes	IPv4 networks	IPv6 prefixes
Distance Vector	Yes	Yes
Convergence Technology	DUAL	DUAL
Metric	Bandwidth and delay by default, reliability and load are optional	Bandwidth and delay by default, reliability and load are optional
Transport Protocol	RTP	RTP
Update Messages	Incremental, partial, and bounded updates	Incremental, partial, and bounded updates
Neighbor Discovery	Hello packets	Hello packets
Source and Destination Addresses	IPv4 source address and 224.0.0.10 IPv4 multicast destination address	IPv6 link-local source address and FF02::A IPv6 multicast destination address
Authentication	MD5, SHA256	MD5, SHA256
Router ID	32-bit router ID	32-bit router ID

- IPv6 Link-local Address
- Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.
- IPv6 link-local addresses are in the FE80::/10 range.



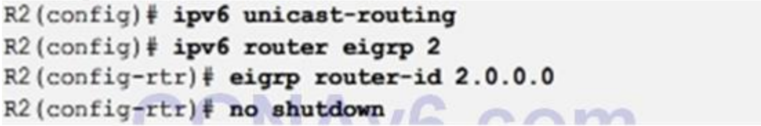
Configure EIGRP for IPv6

- Configuring IPv6 Link-local Addresses
- Link-local address can be automatically created or manually configured
- When created automatically, the router creates the link-local address using FE80::/10 prefix and the EUI-64 process. Use the ipv6 address link-local-address link-local command to manually configure the link-local address using the FE80::10 prefix
- Link-local addresses must be unique on the same local link.

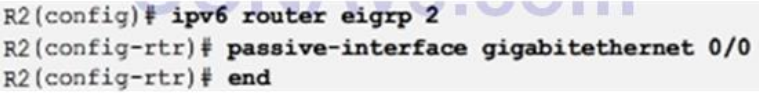


- Configuring the EIGRP for IPv6 Routing Process
- The ipv6 unicast-routing command enable IPv6 routing
- The ipv6 route eigrp autonomous-system command is used to enter the router configuration mode. The process needs to be activated with the no shutdown command.
- To configure the Router ID, use the eigrp router-id command.
- Both the no shutdown command and a router ID are required for the router to form neighbor adjacencies.

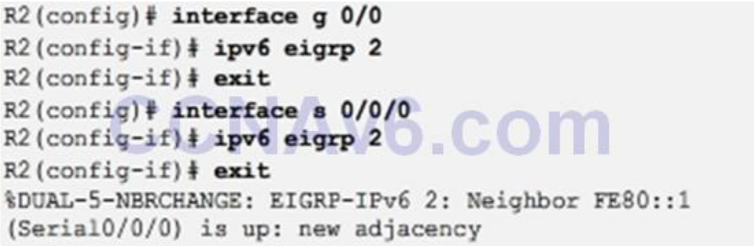
- The ipv6 eigrp interface Command
- EIGRP for IPv6 is configured directly on the interface.
- ipv6 eigrp autonomous-system
- Configure passive interface in the router configuration mode
- passive-interface interface



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



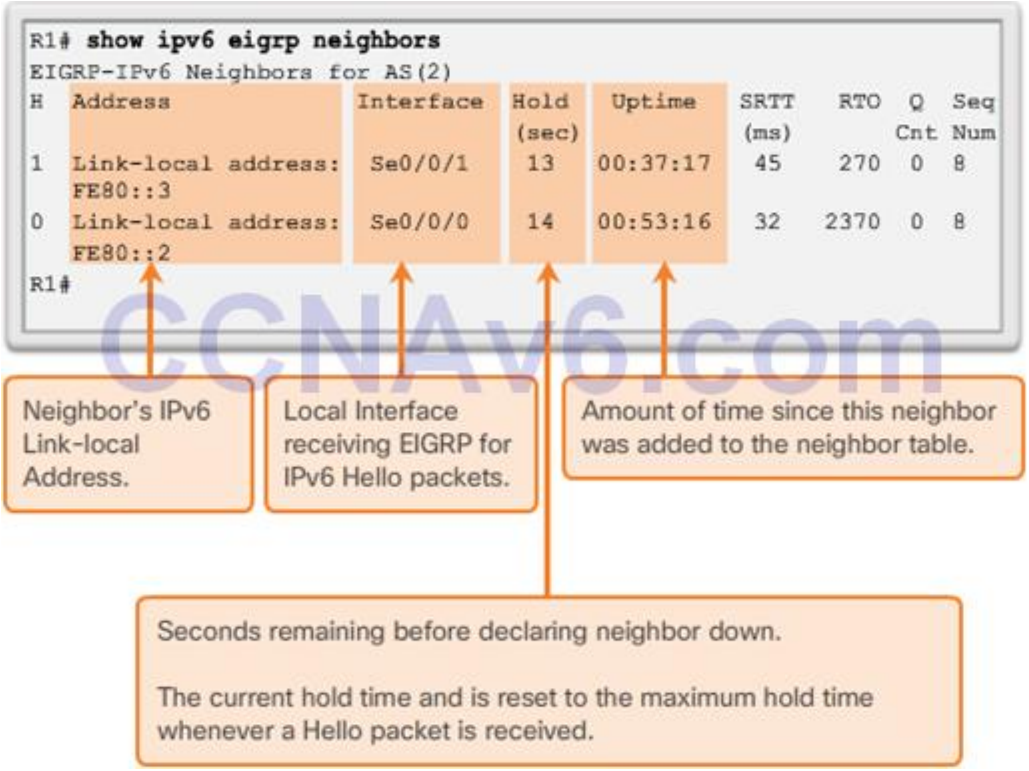
```
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# passive-interface gigabitethernet 0/0
R2(config-rtr)# end
```



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

Verify EIGRP for IPv6

- IPv6 Neighbor Table
- The show ipv6 eigrp neighbors command is used to display neighbor adjacencies
- The show ip protocols Command
- Displays the parameters and other information about the state of any active IPv6 routing protocol processes currently configured on the router.
- Displays different types of output specific to each IPv6 routing protocol.
- The EIGRP for IPv6 Routing Table
- The show ipv6 route command is used to view the IPv6 routing table



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

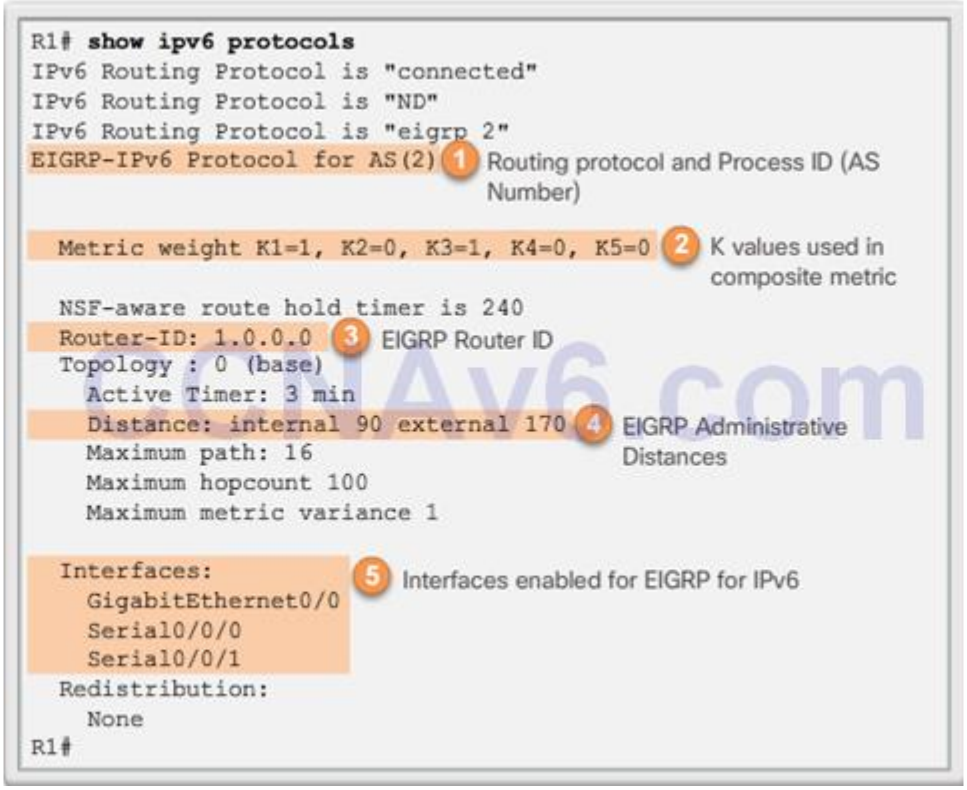
Neighbor's IPv6 Link-local Address.

Local Interface receiving EIGRP for IPv6 Hello packets.

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

Seconds remaining before declaring neighbor down.

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



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

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

  NSF-aware route hold timer is 240
  Router-ID: 1.0.0.0
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1

  Interfaces:
    GigabitEthernet0/0
    Serial0/0/0
    Serial0/0/1
  Redistribution:
    None
R1#
```

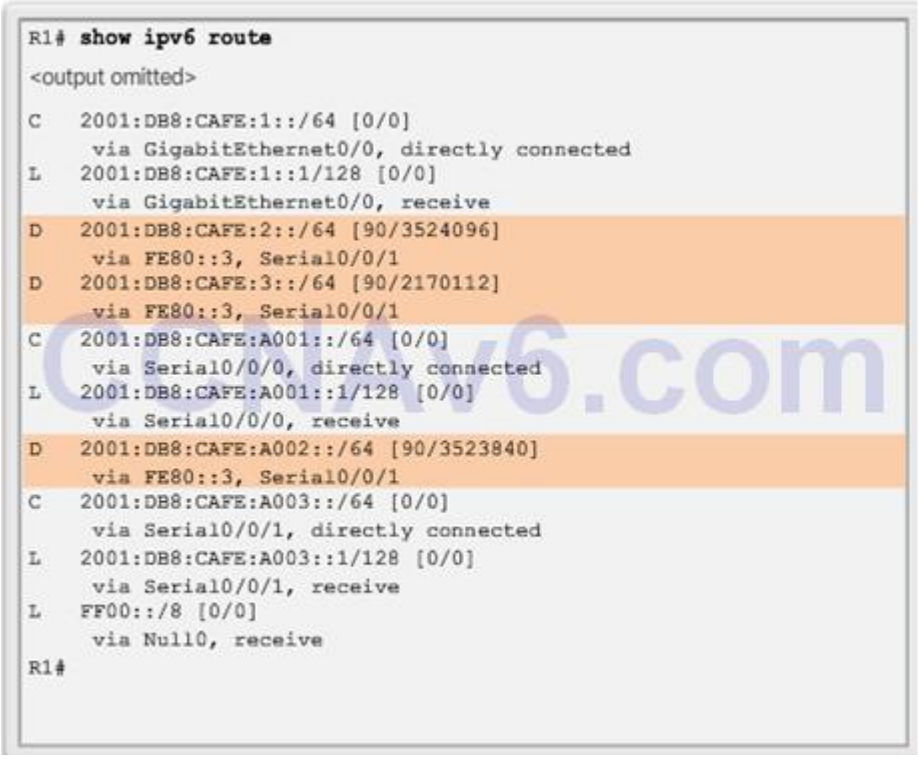
1 Routing protocol and Process ID (AS Number)

2 K values used in composite metric

3 EIGRP Router ID

4 EIGRP Administrative Distances

5 Interfaces enabled for EIGRP for IPv6



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

6.5 Chapter Summary

EIGRP (Enhanced Interior Gateway Routing Protocol) is a classless, distance vector routing protocol.

EIGRP uses the source code of “D” for DUAL in the routing table. EIGRP has a default administrative distance of 90 for internal routes and 170 for routes imported from an external source, such as default routes. These features include: Diffusing Update Algorithm (DUAL), establishing neighbor adjacencies, Reliable Transport Protocol (RTP), partial and bounded updates, and equal and unequal cost load balancing.

EIGRP uses PDMs (Protocol Dependent Modules) giving it the capability to support different Layer 3 protocols including IPv4 and IPv6. EIGRP uses reliable delivery for EIGRP updates, queries and replies; and uses unreliable delivery for EIGRP Hellos and acknowledgments. Reliable RTP means an EIGRP acknowledgment must be returned.

Before any EIGRP updates are sent, a router must first discover its neighbors using EIGRP Hello packets. The Hello and hold-down values do not need to match for two routers to become neighbors. The show ip eigrp neighbors command is used to view the neighbor table and verify that EIGRP has established an adjacency with its neighbors.

EIGRP sends partial or bounded updates, which include only route changes. Updates are sent only to those routers that are affected by the change. EIGRP composite metric uses bandwidth, delay, reliability, and load to determine the best path. By default only bandwidth and delay are used.

At the center of EIGRP is DUAL (Diffusing Update Algorithm). The DUAL Finite State Machine is used to determine best path and potential backup paths to every destination network. The successor is a neighboring router that is used to forward the packet using the least-cost route to the destination network. Feasible distance (FD) is the lowest calculated metric to reach the destination network through the successor. A feasible successor (FS) is a neighbor who has a loop-free backup path to the same network as the successor, and also meets the feasibility condition. The feasibility condition (FC) is met when a neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network. The reported distance is simply an EIGRP neighbor's feasible distance to the destination network.

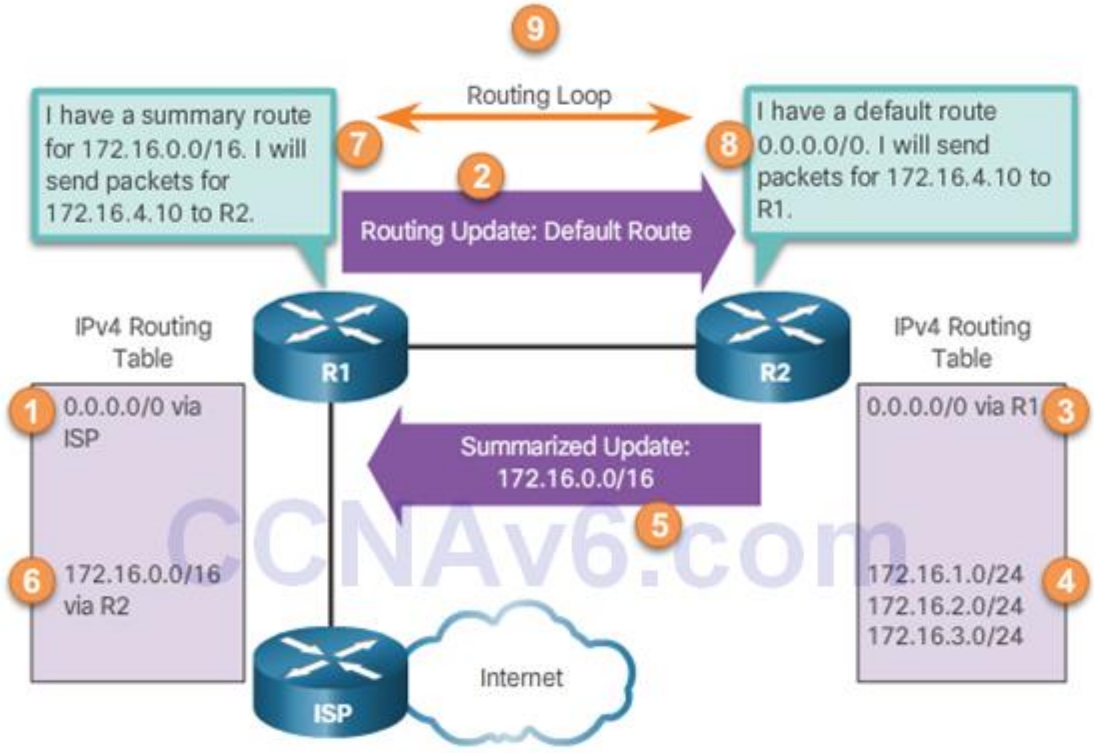
EIGRP is configured with the router eigrp autonomous-system command. The autonomous-system value is actually a process-id and must be the same on all routers in the EIGRP routing domain. The network command is similar to that used with RIP. The network is the classful network address of the directly connected interfaces on the router. A wildcard mask is an optional parameter that can be used to include only specific interfaces.

EIGRP for IPv6 shares many similarities with EIGRP for IPv4. However, unlike the IPv4 network command, IPv6 is enabled on the interface using the ipv6 eigrp autonomous-system interface configuration command.

7.1 Tune EIGRP

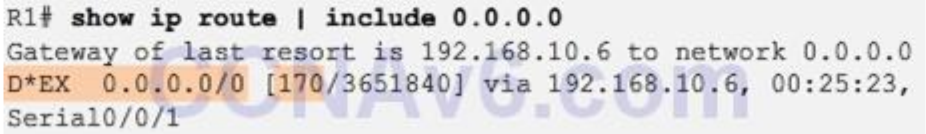
Automatic Summarization

- EIGRP Automatic Summarization
- Summarization limits the number of routing advertisements and the size of the routing table
- EIGRP performs automatic summarization at classful boundaries.
- Configuring EIGRP Automatic Summarization
- R1(config)# router eigrp as-number
- R1(config-router)# auto-summary
- Verifying Auto-Summary
- show ip protocols
- show ip eigrp topology all-links
- show ip route
- Null0 summary route exists when:
- Automatic summarization is enabled.
- There is at least one subnet that was learned via EIGRP.
- There are two or more network EIGRP router configuration mode commands.
- Automatic summarization could cause routing loops


9
Routing Loop
I have a summary route for 172.16.0.0/16. I will send packets for 172.16.4.10 to R2.
7
2
Routing Update: Default Route
8
I have a default route 0.0.0.0/0. I will send packets for 172.16.4.10 to R1.
IPv4 Routing Table
R1
R2
IPv4 Routing Table
1
0.0.0.0/0 via ISP
Summarized Update: 172.16.0.0/16
0.0.0.0/0 via R1
3
5
6
172.16.0.0/16 via R2
172.16.1.0/24
172.16.2.0/24
172.16.3.0/24
4
ISP
Internet

Default Route Propagation

- Propagating a Default Static Route
- The default static route (0.0.0.0 / 0) is usually configured on the router that has a connection to a network outside the EIGRP routing domain; for example, to an ISP.
- One way to propagate the default static route
- The redistribute static command
- Verifying the Propagated Default Route



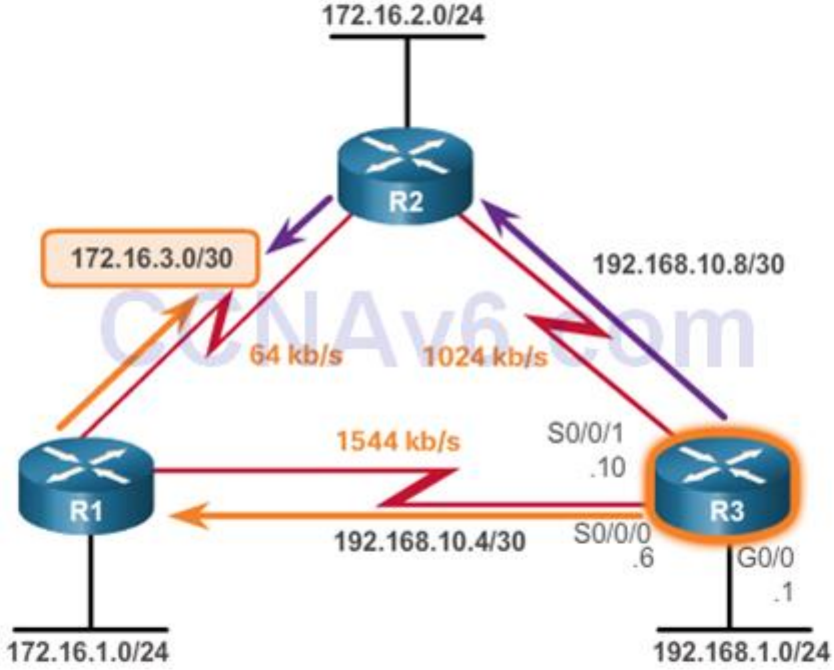
```
R1# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:25:23,
Serial0/0/1
```

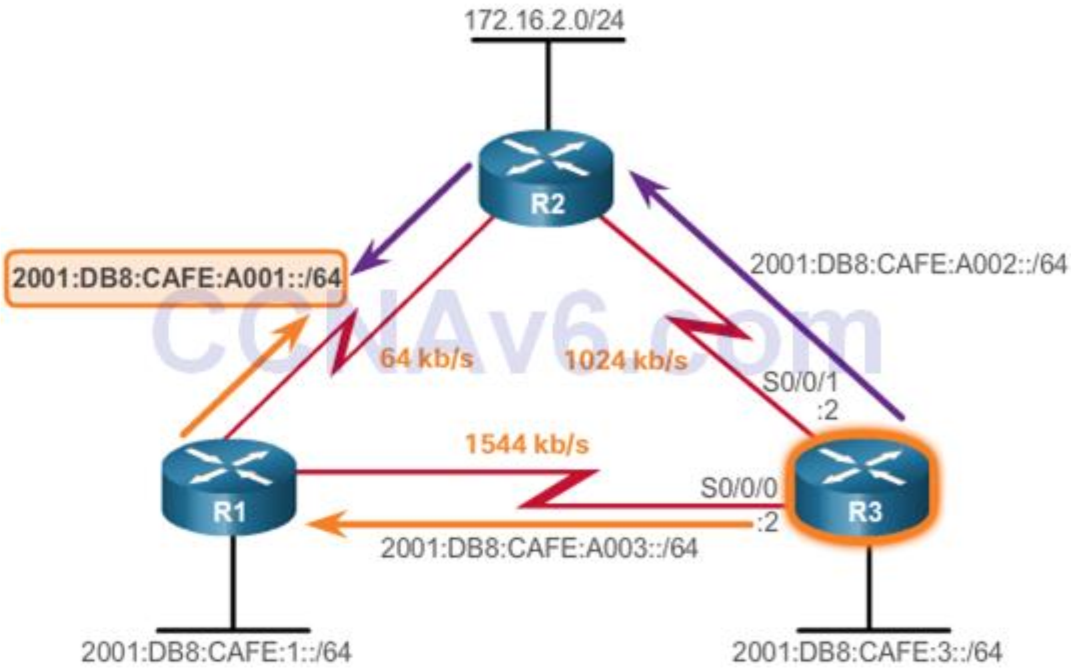
- D – This route was learned from an EIGRP routing update.
- * – The route is a candidate for a default route.
- EX – The route is an external EIGRP route, in this case a static route outside of the EIGRP routing domain.
- 170 – This is the administrative distance of an external EIGRP route.
- EIGRP for IPv6: Default Route
- To configure a IPv6 static default route: ipv6 route ::/0 exit-interface
- To propapate a IPv6 static default route: redistribute static
- To verify the propagation of IPv6 static default route: show ipv6 route

Fine-tuning EIGRP Interfaces

- EIGRP Bandwidth Utilization

- By default, EIGRP uses only up to 50 percent of an interface's bandwidth for EIGRP information. This prevents the EIGRP process from over-utilizing a link and not allowing enough bandwidth for the routing of normal traffic.
- Commands to configure the bandwidth percentage used by EIGRP on an interface:
- IPv4: ip bandwidth-percent eigrp as-number percent
- IPv6: ipv6 bandwidth-percent eigrp as-number percent
- Hello and Hold Timers – Do not have to match with other EIGRP routers
- Hello packets are used to establish and monitor the connection status of neighbors
- Commands to configure the hello intervals per interface:
- ip hello-interval eigrp as-number seconds
- ipv6 hello-interval eigrp as-number seconds
- Hold time tells the router the maximum time that the router should wait to receive the next Hello before declaring that neighbor as unreachable.
- Commands to configure the hold time intervals per interface:
- ip hold-time eigrp as-number seconds
- ipv6 hold-time eigrp as-number seconds
- What are the default hello intervals and hold times for EIGRP?
- Load Balancing
- Equal-cost load balancing
- The ability of a router to distribute outbound traffic using all interfaces that have the same metric from the destination address
- IPv4 and IPv6: The maximum-paths value determines the maximum number of routes
- Unequal-cost load balancing
- The ability to balance traffic across multiple routes that have different metrics
- IPv4 and IPv6: The variance command is used to install multiple loop-free routes with unequal cost in a local routing table

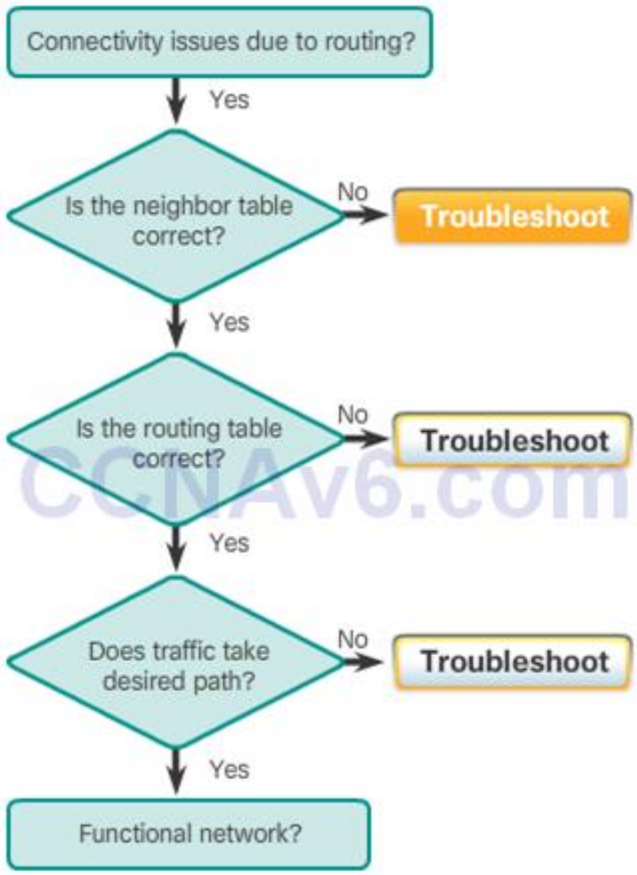




7.2 Troubleshoot EIGRP

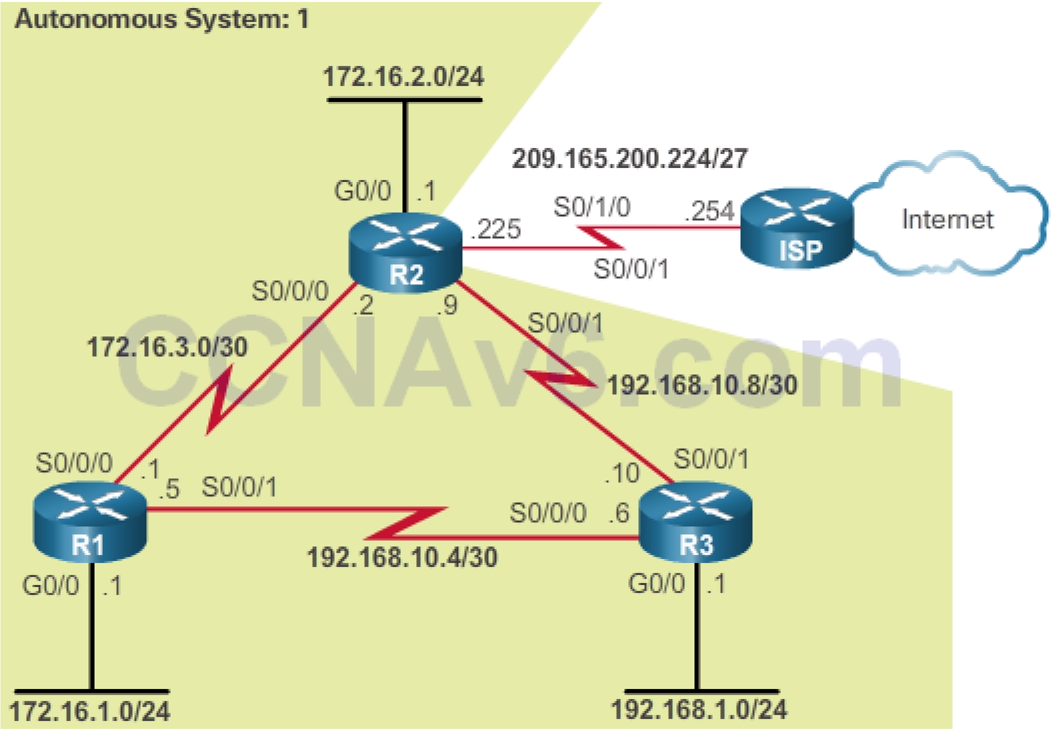
Components of Troubleshooting EIGRP

- Basic EIGRP Troubleshooting Commands
- Verify the neighbor adjacency
- show ip eigrp neighbors
- show ipv6 eigrp neighbors
- Verify the learned route to remote networks
- show ip route eigrp
- show ipv6 route eigrp
- Verify the various EIGRP settings
- show ip protocols
- show ipv6 protocols


Connectivity issues due to routing?
Yes
Is the neighbor table correct?
No
Troubleshoot
Yes
Is the routing table correct?
No
Troubleshoot
Yes
Does traffic take desired path?
No
Troubleshoot
Yes
Functional network?

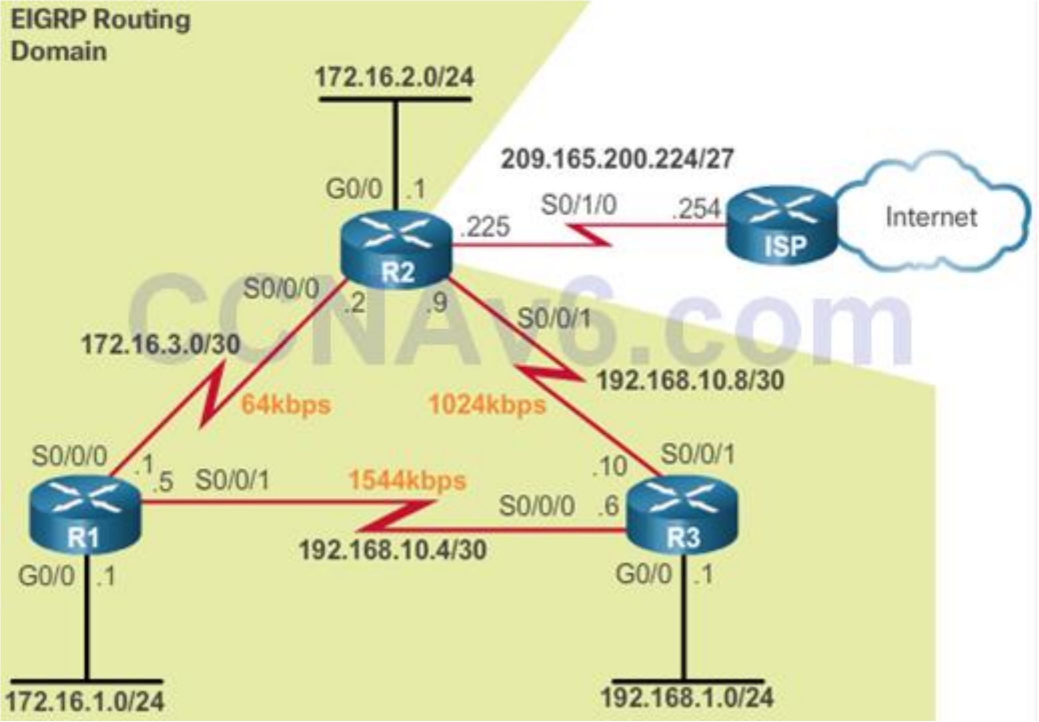
Troubleshoot EIGRP Neighbor Issues

- Layer 3 Connectivity
- Verify the connection
- show ip interface brief or show ipv6 interface brief
- ping ip address
- EIGRP Parameters
- Verify that the routers are in the same EIGRP domain with the same AS number
- show ip protocols or show ipv6 protocols
- Configure AS number
- IPv4: router eigrp as-number
- IPv6: ipv6 router eigrp as-number
- EIGRP Interfaces
- Verify that the router interfaces
- are participating in the EIGRP network
- show ip eigrp interfaces or show ipv6 eigrp interfaces
- show ip protocols or show ipv6 protocols
- show running-config | section eigrp



Troubleshoot EIGRP Routing Table Issues

- Passive Interface
- Prevent routers from becoming neighbors
- show ip eigrp neighbors or show ipv6 eigrp neighbors
- The show ip protocols or show ipv6 protocols command is used to verify whether the interface has been configured as passive
- Passive interface is configured if neighbor adjacency is not desirable
- Where would you configure passive interfaces in the graphics?
- Missing Network Statement
- Verify the advertised networks
- show ip protocols or show ipv6 protocols
- show ip route or show ipv6 route
- Configure network statements
- IPv4: network ip-address [mask]
- IPv6: ipv6 eigrp autonomous-system command in interface configuration mode
- Autosummarization
- IPv4: Could cause inconsistent routing
- Disable autosummarization: no auto-summary
- IPv6: All summarization can only be accomplished using EIGRP manual summary routes.



7.3 Chapter Summary

EIGRP is one of the routing protocols commonly used in large enterprise networks. Modifying EIGRP features and troubleshooting problems is one of the most essential skills for a network engineer involved in the implementation and maintenance of large routed enterprise networks that use EIGRP.

Summarization decreases the number of entries in routing updates and lowers the number of entries in local routing tables. It also reduces bandwidth utilization for routing updates and results in faster routing table lookups. EIGRP for IPv4 automatic summarization is disabled by default beginning with Cisco IOS Release 15.0(1)M and 12.2(33). Prior to this, automatic summarization was enabled by default. To enable automatic summarization for EIGRP use the auto-summary command in router configuration mode. Use the show ip protocols command to verify the status of automatic summarization. Examine the routing table to verify that automatic summarization is working.

EIGRP automatically includes summary routes to Null0 to prevent routing loops that are included in the summary but do not actually exist in the routing table. The Null0 interface is a virtual IOS interface that is a route to nowhere, commonly known as “the bit bucket”. Packets that match a route with a Null0 exit interface are discarded.

One method of propagating a default route within the EIGRP routing domain is to use the redistribute static command. This command tells EIGRP to include this static route in its EIGRP updates to other routers. The show ip protocols command verifies that static routes within the EIGRP routing domain are being redistributed.

Use the ip bandwidth-percent eigrp as-number percent interface configuration mode command to configure the percentage of bandwidth that can be used by EIGRP on an interface.

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

Hello intervals and hold times are configurable on a per-interface basis in EIGRP and do not have to match with other EIGRP routers to establish or maintain adjacencies.

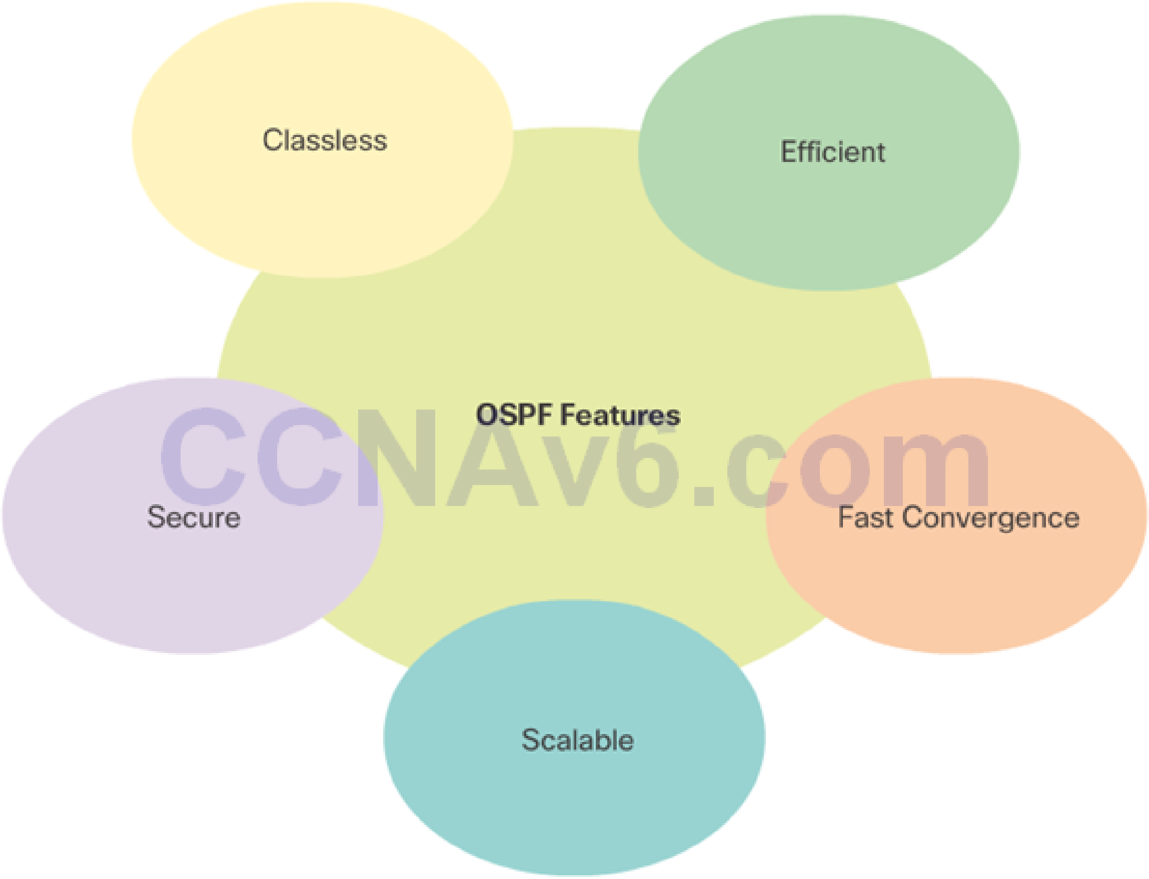
For IP in EIGRP, Cisco IOS software applies load balancing using up to four equal-cost paths by default. With the maximum-paths router configuration mode command, up to 32 equal-cost routes can be kept in the routing table.

The show ip route command verifies that the router learned EIGRP routes. The show ip protocols command is used to verify that EIGRP displays the currently configured values.

8.1 OSPF Characteristics

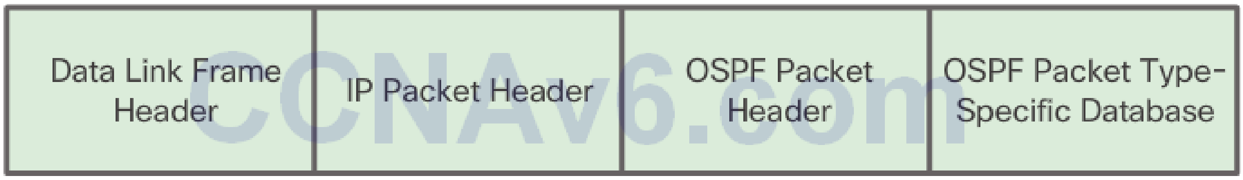
Open Shortest Path First

- OSPF
- Version 2 (OSPFv2) is available for IPv4 while OSPF version 3 (OSPFv3) is available for IPv6.
- 3 Main Components
- Data Structures, Routing Protocol Messages, and Algorithm
- Achieving Convergence:
- Establish Neighbor Adjacencies
- Exchange Link-State Advertisements
- Build the Topology Table
- Execute the SPF Algorithm
- OSPF can be implemented in one of two ways:
- Single-Area OSPF
- Multi-area OSPF



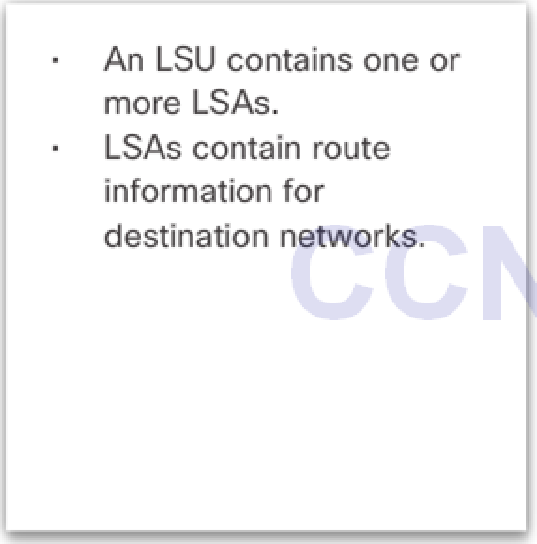
OSPF Messages

- OSPFv2 messages contain:

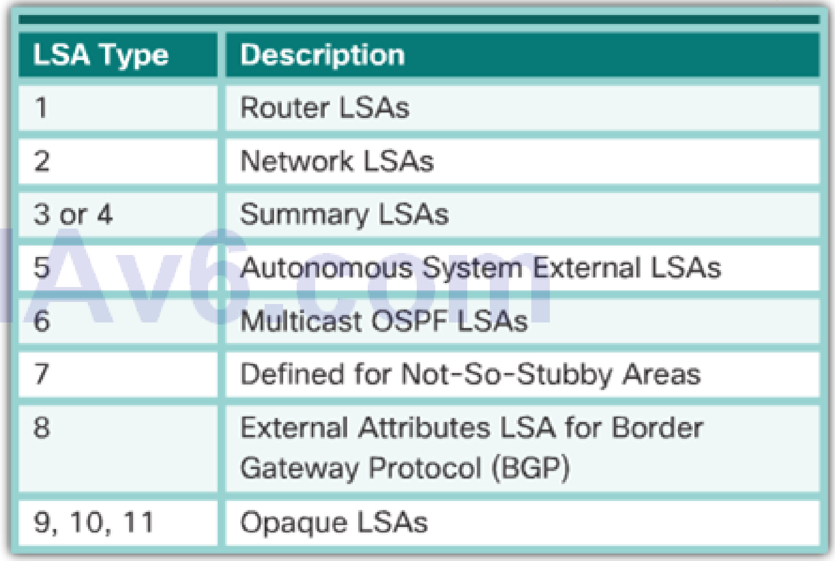


Data Link Frame Header	IP Packet Header	OSPF Packet Header	OSPF Packet Type-Specific Database

- LSP Types:
- Type 1: Hello packet
- Type 2: Database Description (DBD) packet
- Type 3: Link-State Request (LSR) packet
- Type 4: Link-State Update (LSU) packet
- Type 5: Link-State Acknowledgment (LSAck) packet
- Hello Packets are used to:
- Discover OSPF neighbors and establish neighbor adjacencies.
- Advertise parameters on which two routers must agree to become neighbors.
- Elect the Designated Router (DR) and Backup Designated Router (BDR) on multi-access networks like Ethernet and Frame Relay.
- OSPF Hello packets are transmitted to multicast address 224.0.0.5 in IPv4 and FF02::5 in IPv6



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



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

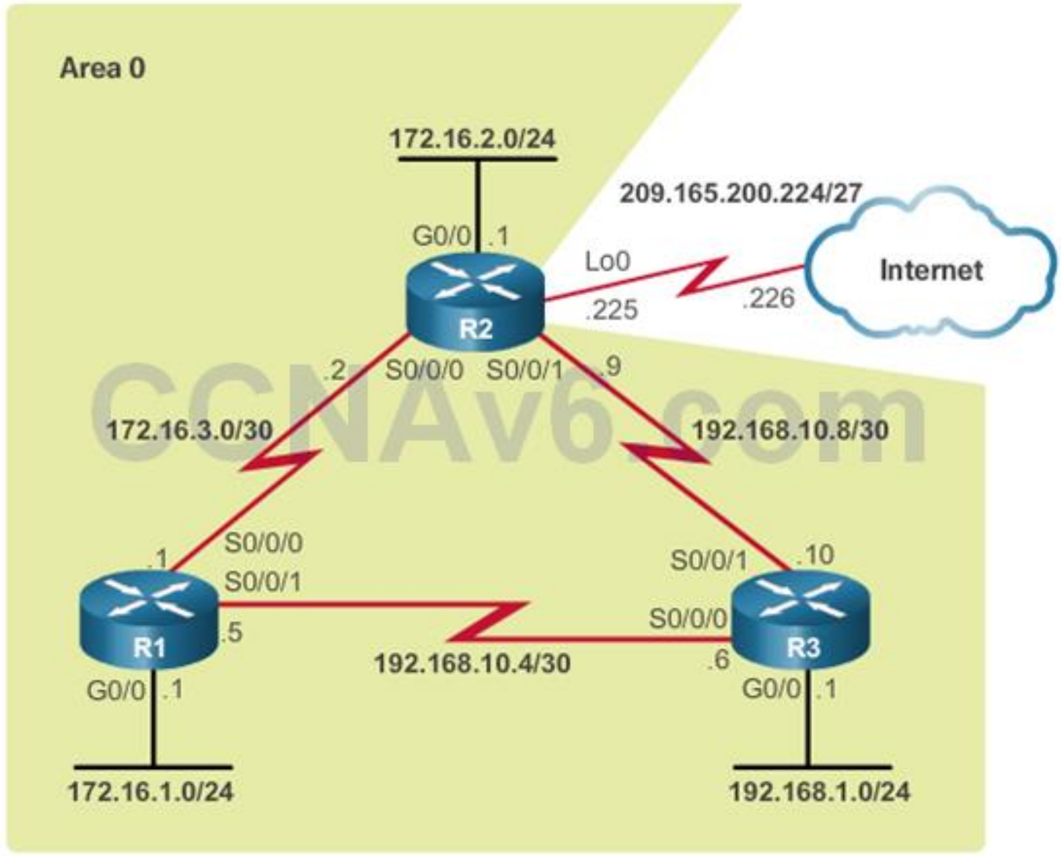
OSPF Operation

- OSPF progresses through several states while attempting to reach convergence
- Down state, Init state, Two-Way state, ExStart state, Exchange state, Loading state, and Full state
- Establishing Adjacencies
- When a neighboring OSPF-enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router.
- OSPF DR and BDR
- On multiaccess networks, OSPF elects a DR to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails.
- After the Two-Way state, routers transition to database synchronization states.

8.2 Single-Area OSPFv2

OSPF Router ID

- Enabling OSPFv2
- OSPFv2 is enabled using the router ospf process-id global configuration mode command.
- The process-id value represents a number between 1 and 65,535 and is selected by the network administrator.
- The process-id value is locally significant, which means that it does not have to be the same value on the other OSPF routers to establish adjacencies with those neighbors.

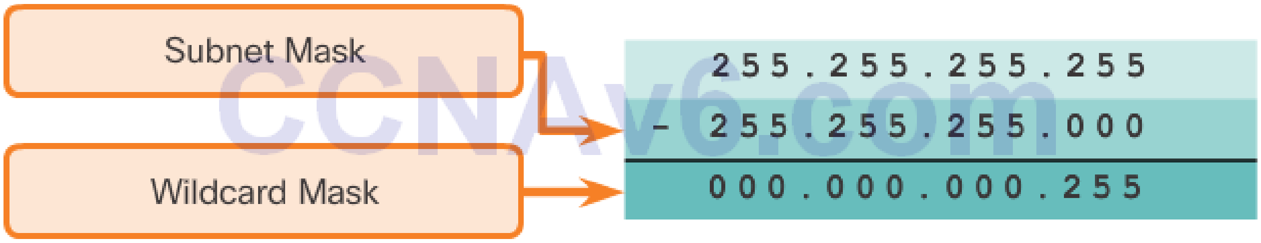


- Router ID
- The router ID is used by the OSPF-enabled router to uniquely identify the router and participate in the election of the DR
- Router ID based on one of three criteria
- Explicitly configured using the OSPF router-id rid command
- Router chooses the highest IPv4 address of any of configured loopback interfaces
- If no loopback interfaces are configured, then the router chooses the highest active IPv4 address of any of its physical interfaces
- Clearing the OSPF process is the preferred method to reset the router ID.
- Note: The router ID looks like an IPv4 address, but it is not routable and, therefore, is not included in the routing table, unless the OSPF routing process chooses an interface (physical or loopback) that is appropriately defined by a network command.

Configure Single-Area OSPFv2

- Enabling OSPF
- Any interfaces on a router that match the network address in the network command are enabled to send and receive OSPF packets.
- Wildcard Mask
- In a wildcard mask, binary 0 is equal to a match and binary 1 is not a match.

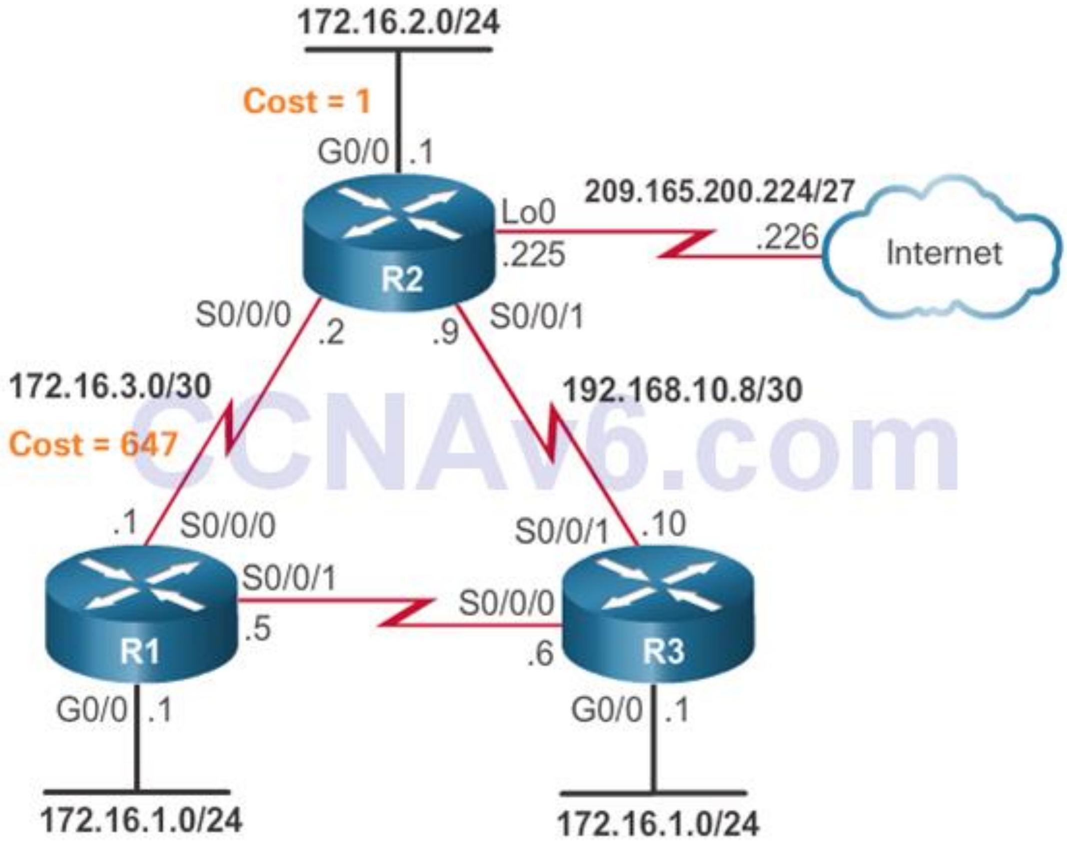
Calculating a Wildcard Mask for /24



- The network Command
- OSPFv2 can be enabled using the network intf-ip-address 0.0.0.0 area area-id router configuration mode command.
- The advantage of specifying the interface is that the wildcard mask calculation is not necessary.
- Unneeded OSPFv2 messages affect the network:
- Inefficient use of bandwidth, inefficient use of resources, and increased security risk
- Configure passive interfaces
- Use the passive-interface router configuration mode command to prevent the transmission of routing messages through a router interface, but still allow that network to be advertised to other routers.
- A neighbor adjacency cannot be formed over a passive interface.

OSPF Cost

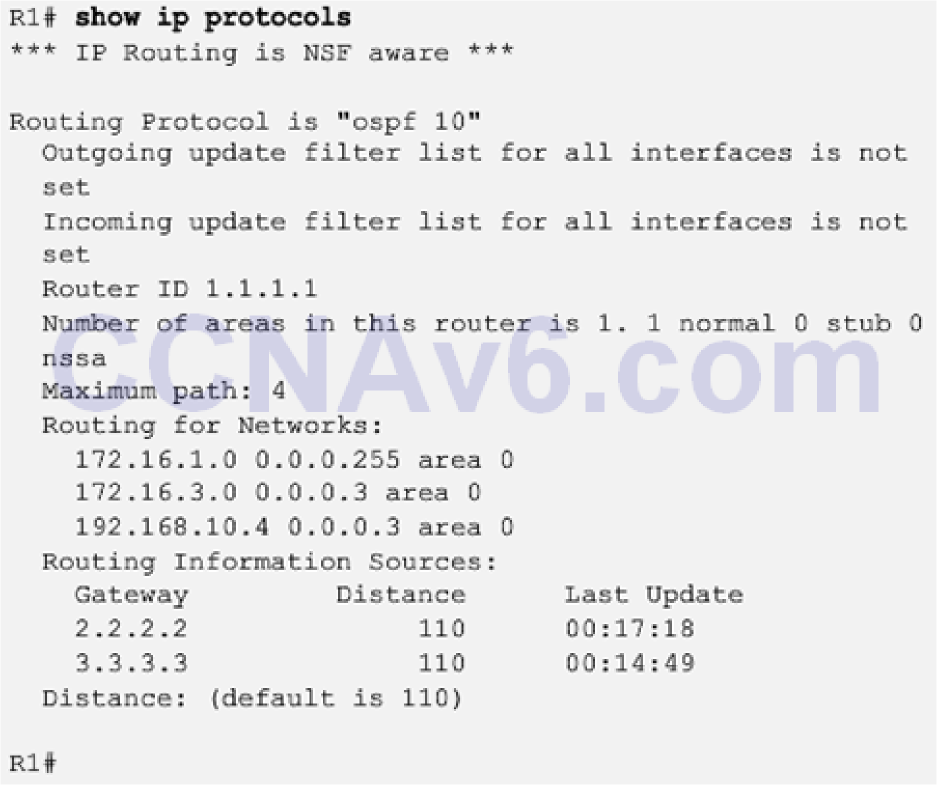
- OSPF Metric = Cost
- The cost of an interface is inversely proportional to the bandwidth of the interface.
- Cost = reference bandwidth / interface bandwidth
- The cost of an OSPF route is the accumulated value from one router to the destination network.
- To adjust the reference bandwidth, use the auto-cost reference-bandwidth Mb/s router configuration command.



- Default Interface Bandwidths
- As with reference bandwidth, interface bandwidth values do not actually affect the speed or capacity of the link.
- Use the show interfaces command to view the interface bandwidth setting.
- Adjust Interface Bandwidth
- To adjust the interface bandwidth use the bandwidth kilobits interface configuration command.
- Use the no bandwidth command to restore the default value.
- Set OSPF Cost Manually
- The cost can be manually configured on an interface using the ip ospf cost value interface configuration command.

Verify OSPF

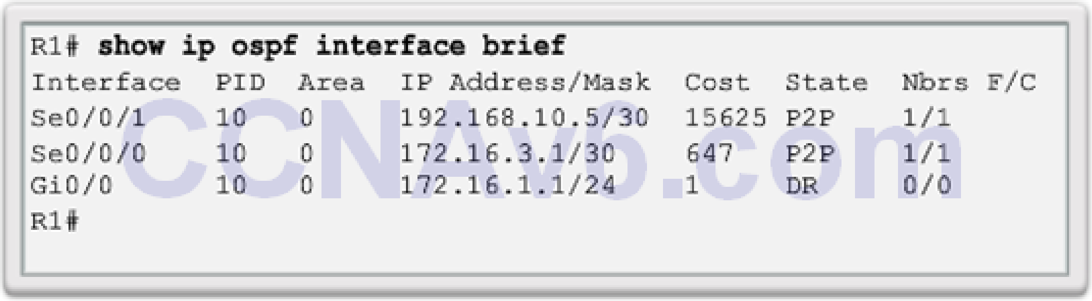
- Verify OSPF Neighbors
- Use the show ip ospf neighbor command to verify that the router has formed an adjacency with its neighboring routers.
- Verify OSPF Protocol Settings
- The show ip protocols command is a quick way to verify vital OSPF configuration information.
- Verify OSPF Process Information
- The show ip ospf command can also be used to examine the OSPFv2 process ID and router ID



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

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

R1#
```

- Verify OSPF Interface Settings
- The quickest way to verify OSPFv2 interface settings is to use the show ip ospf interface command.
- To get a summary of OSPFv2-enabled interfaces, use the show ip ospf interface brief command.

Verifying R1's OSPF Interfaces



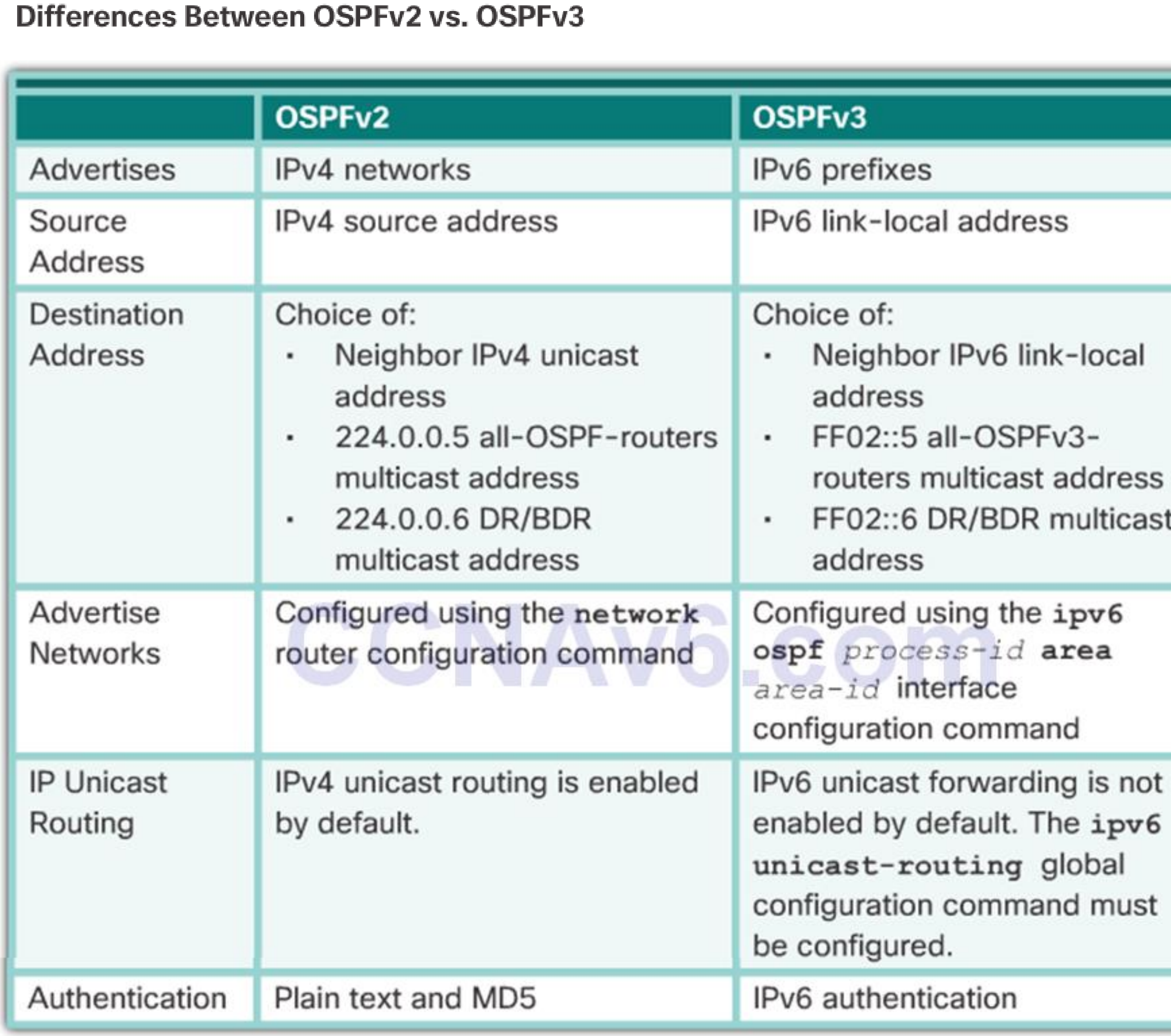
```
R1# show ip ospf interface brief
Interface  PID  Area  IP Address/Mask   Cost  State  Nbrs F/C
Se0/0/1    10   0     192.168.10.5/30   15625 P2P    1/1
Se0/0/0    10   0     172.16.3.1/30     647   P2P    1/1
Gi0/0      10   0     172.16.1.1/24     1     DR     0/0
R1#
```

8.3 Single-Area OSPFv3

OSPFv2 vs. OSPFv3

- OSPFv3
- Similar to its IPv4 counterpart, OSPFv3 exchanges routing information to populate the IPv6 routing table with remote prefixes

- Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.



Differences Between OSPFv2 vs. OSPFv3

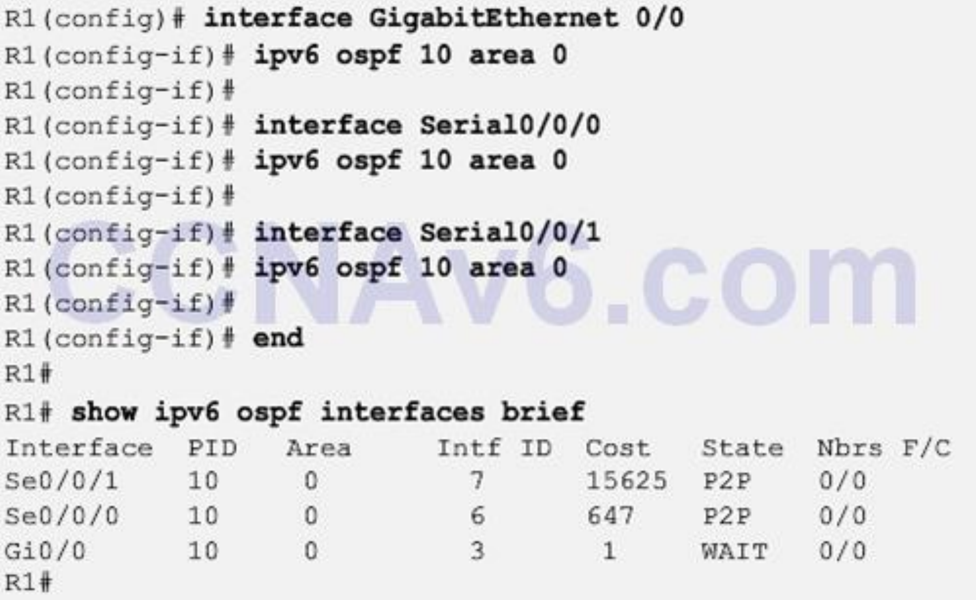
	OSPFv2	OSPFv3
Advertises	IPv4 networks	IPv6 prefixes
Source Address	IPv4 source address	IPv6 link-local address
Destination Address	Choice of: • Neighbor IPv4 unicast address • 224.0.0.5 all-OSPF-routers multicast address • 224.0.0.6 DR/BDR multicast address	Choice of: • Neighbor IPv6 link-local address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

- Link-Local Addresses
- Link-local addresses are automatically created when an IPv6 global unicast address is assigned to the interface.
- Assigning Link-Local Addresses
- Link-local addresses can be configured manually using the same interface command used to create IPv6 global unicast addresses, but appending the link-local keyword to the ipv6 address command.
- Configuring the OSPFv3 Router ID

- OSPFv3 requires a 32-bit router ID to be assigned before OSPF can be enabled on an interface.
- The router-id rid command is used to assign a router ID in OSPFv3.
- Clearing the OSPF process is the preferred method to reset the router ID.

Configuring OSPFv3

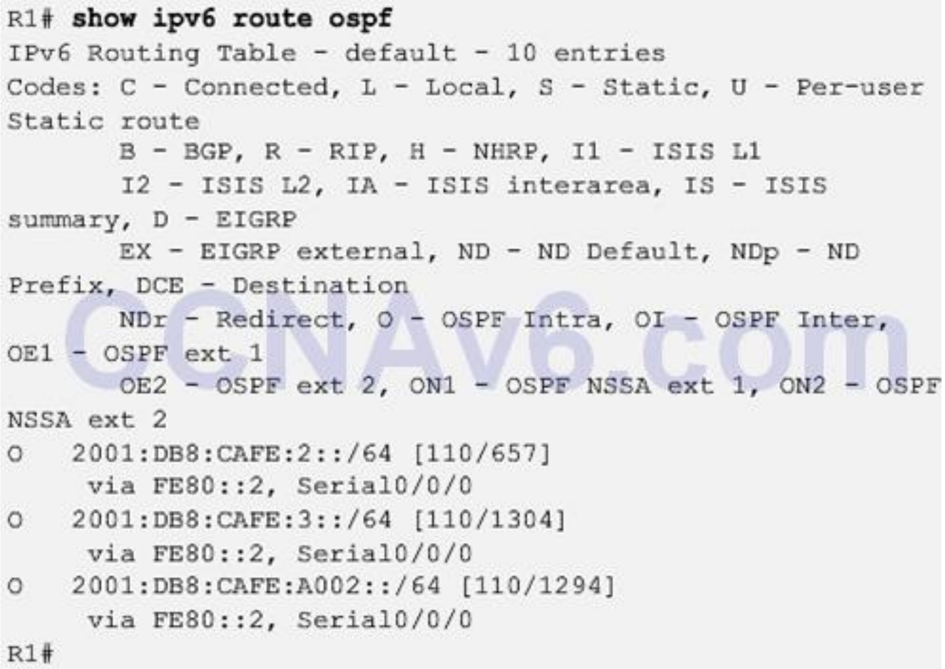
- Enabling OSPFv3 on Interfaces
- To enable OSPFv3 on an interface, use the ipv6 ospf process-id area area-id interface configuration mode command.



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

Verify OSPFv3

- Verify OSPFv3 Neighbors
- Use the show ipv6 ospf neighbor command to verify that the router has formed an adjacency with its neighboring routers.
- Verify OSPFv3 Protocol Settings
- The show ipv6 protocols command is a quick way to verify vital OSPFv3 configuration information, including the OSPFv3 process ID, the router ID, and the interfaces enabled for OSPFv3.
- Verify OSPFv3 Interfaces
- The quickest way to verify OSPFv3 interface settings is to use the show ipv6 ospf interface command.
- To retrieve and view a summary of OSPFv3-enabled interfaces on R1, use the show ipv6 ospf interface brief command
- Verify the IPv6 Routing Table
- The show ipv6 route ospf command provides specifics about OSPFv3 routes in the routing table.



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

8.4 Chapter Summary

The current version of OSPF for IPv4 is OSPFv2 introduced in RFC 1247 and updated in RFC 2328 by John Moy. In 1999, OSPFv3 for IPv6 was published in RFC 2740.

OSPF is a link-state routing protocol with a default administrative distance of 110, and is denoted in the routing table with a route source code of O.

OSPFv2 is enabled with the router ospf process-id global configuration mode command. The process-id value is locally significant, which means that it does not need to match other OSPFv2 routers to establish adjacencies with those neighbors.

The network command used with OSPFv2 has the same function as when used with other IGP routing protocols, but with slightly different syntax. The wildcard-mask value is the inverse of the subnet mask, and the area-id value should be set to 0.

By default, OSPF Hello packets are sent every 10 seconds on multi-access and point-to-point segments and every 30 seconds on NBMA segments (Frame Relay, X.25, ATM), and are used by OSPF to establish neighbor adjacencies. The Dead interval is four times the Hello interval, by default.

For routers to become adjacent, their Hello interval, Dead interval, network types, and subnet masks must match. Use the show ip ospf neighbors command to verify OSPFv2 adjacencies.

OSPF elects a DR to act as collection and distribution point for LSAs sent and received in the multi-access network. A BDR is elected to assume the role of the DR should the DR fail.

All other routers are known as DROTHERs. All routers send their LSAs to the DR, which then floods the LSA to all other routers in the multi-access network.

The show ip protocols command is used to verify important OSPFv2 configuration information, including the OSPF process ID, the router ID, and the networks the router is advertising.

OSPFv3 is enabled on an interface and not under router configuration mode. OSPFv3 needs link-local addresses to be configured. IPv6 Unicast routing must be enabled for OSPFv3. A 32-bit router-ID is required before an interface can be enabled for OSPFv3. Similar verification commands used for OSPFv2 are used for OSPFv3.