EIGRP

CCNA Routing and Switching

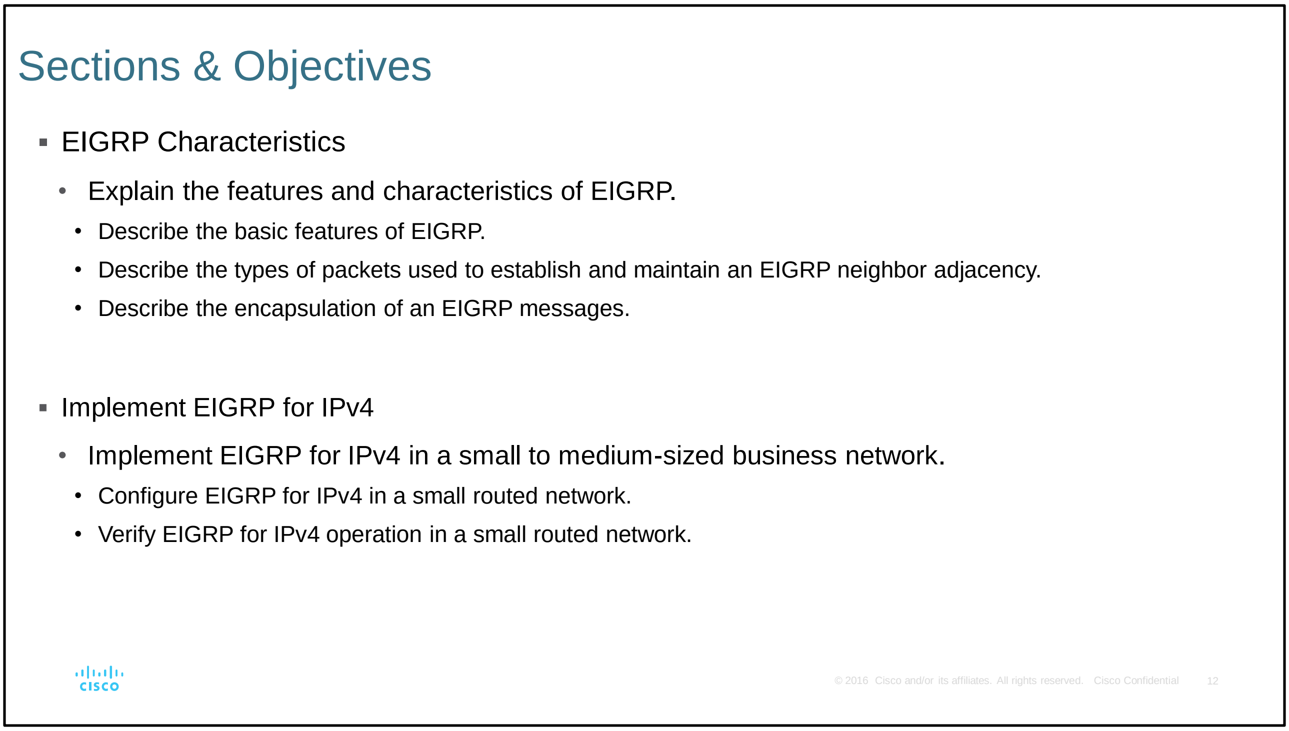
- Scaling Networks v6.0 - Chapter 6: EIGRP
- Scaling Networks v6.0 - Chapter 7: EIGRP Tuning and Troubleshooting

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol developed by Cisco Systems. As the name suggests, EIGRP is an enhancement of another Cisco routing protocol IGRP (Interior Gateway Routing Protocol). IGRP is an older classful, distance vector routing protocol, now obsolete since IOS 12.3.

EIGRP includes features found in link-state routing protocols. EIGRP is suited for many different topologies and media. In a well-designed network, EIGRP can scale to include multiple topologies and can provide extremely quick convergence times with minimal network traffic.

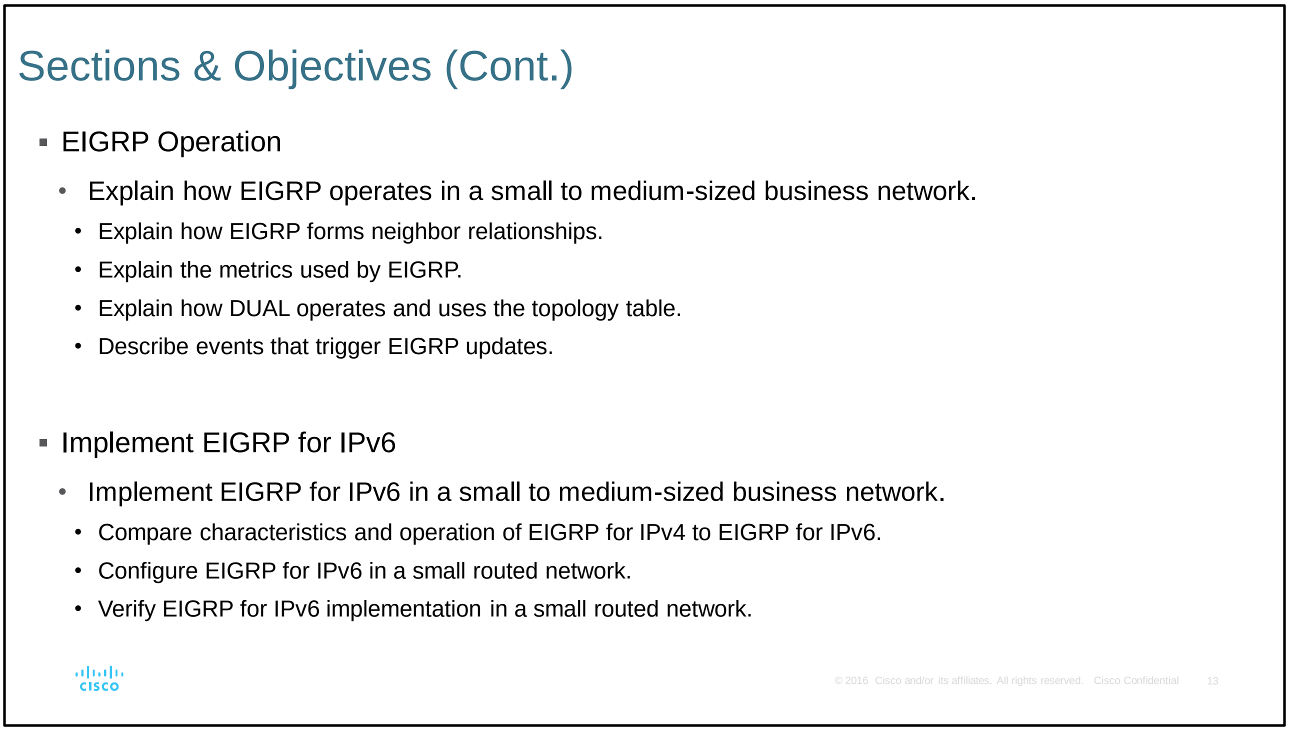
This chapter introduces EIGRP and provides basic configuration commands to enable it on a Cisco IOS router. It also explores the operation of the routing protocol and provides more detail on how EIGRP determines best path.



Sections & Objectives

- EIGRP Characteristics
  - Explain the features and characteristics of EIGRP.
    - Describe the basic features of EIGRP.
    - Describe the types of packets used to establish and maintain an EIGRP neighbor adjacency.
    - Describe the encapsulation of an EIGRP messages.

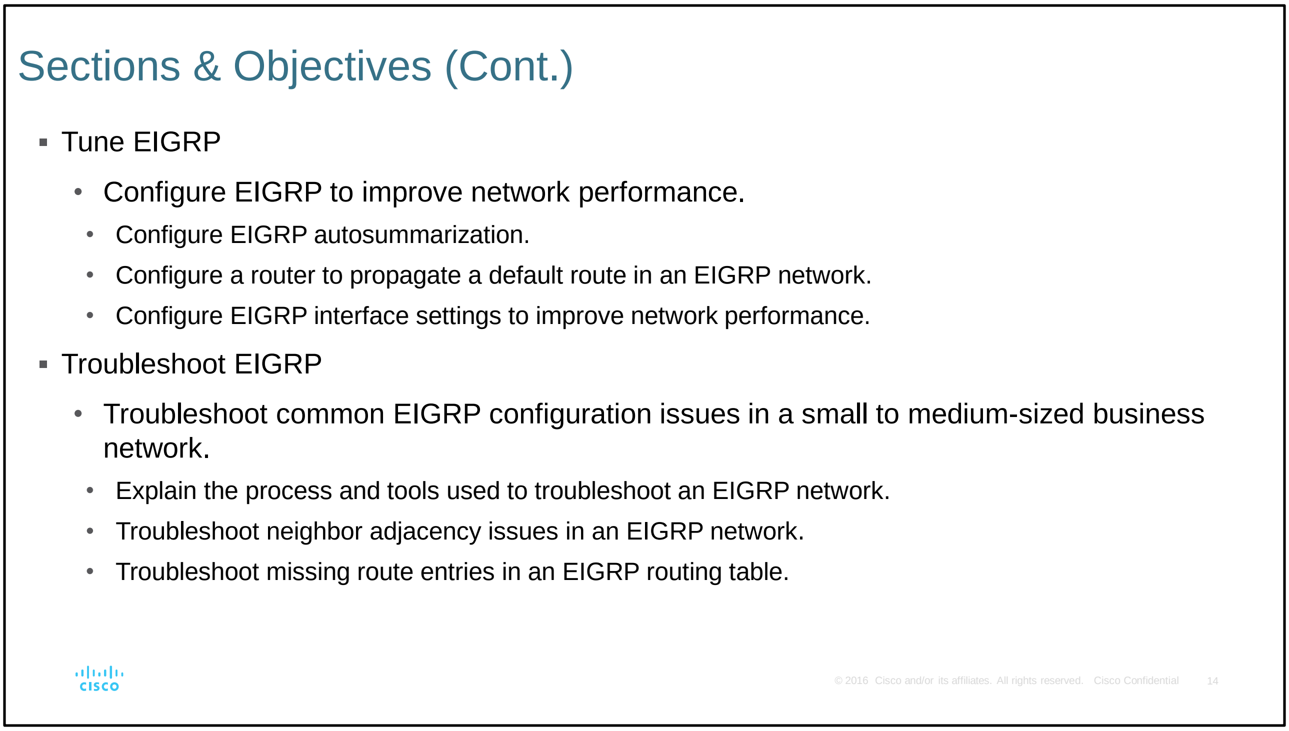
- Implement EIGRP for IPv4
  - Implement EIGRP for IPv4 in a small to medium-sized business network.
    - Configure EIGRP for IPv4 in a small routed network.
    - Verify EIGRP for IPv4 operation in a small routed network.



Sections & Objectives (Cont.)

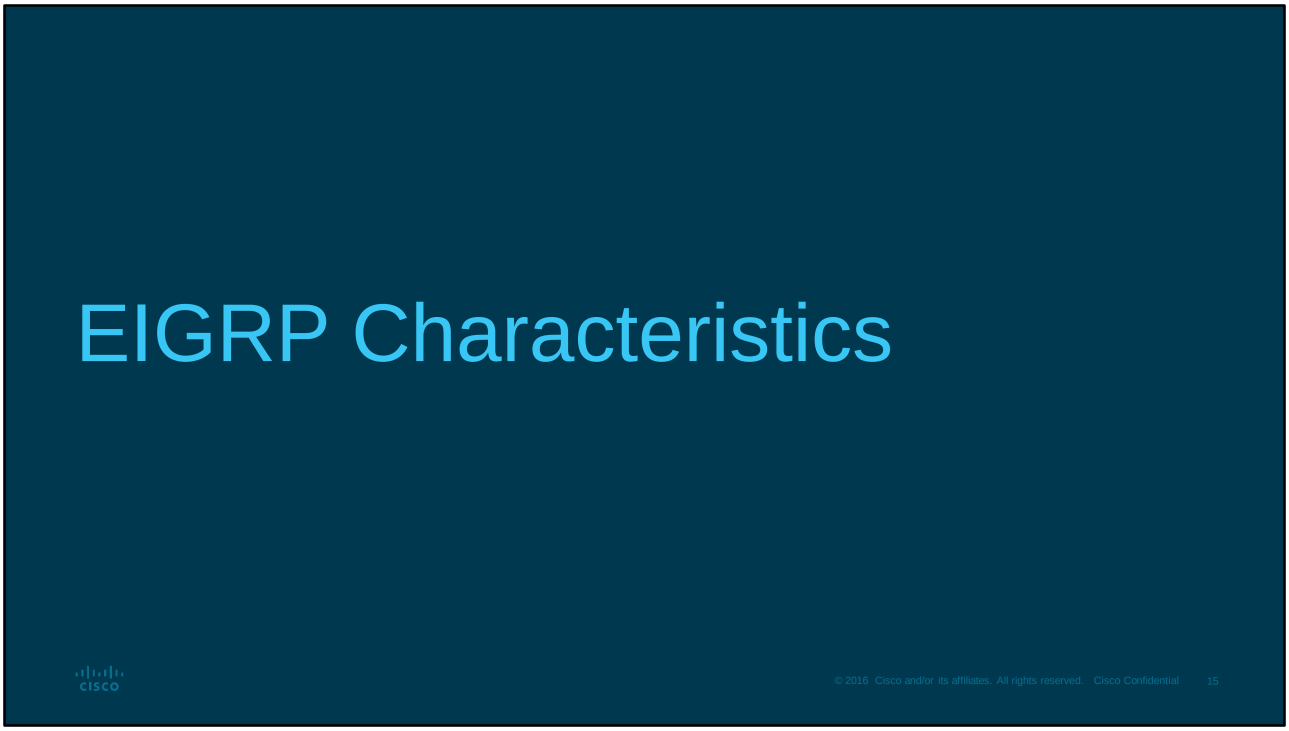
- EIGRP Operation
  - Explain how EIGRP operates in a small to medium-sized business network.
    - Explain how EIGRP forms neighbor relationships.
    - Explain the metrics used by EIGRP.
    - Explain how DUAL operates and uses the topology table.
    - Describe events that trigger EIGRP updates.

- Implement EIGRP for IPv6
  - Implement EIGRP for IPv6 in a small to medium-sized business network.
    - Compare characteristics and operation of EIGRP for IPv4 to EIGRP for IPv6.
    - Configure EIGRP for IPv6 in a small routed network.
    - Verify EIGRP for IPv6 implementation in a small routed network.

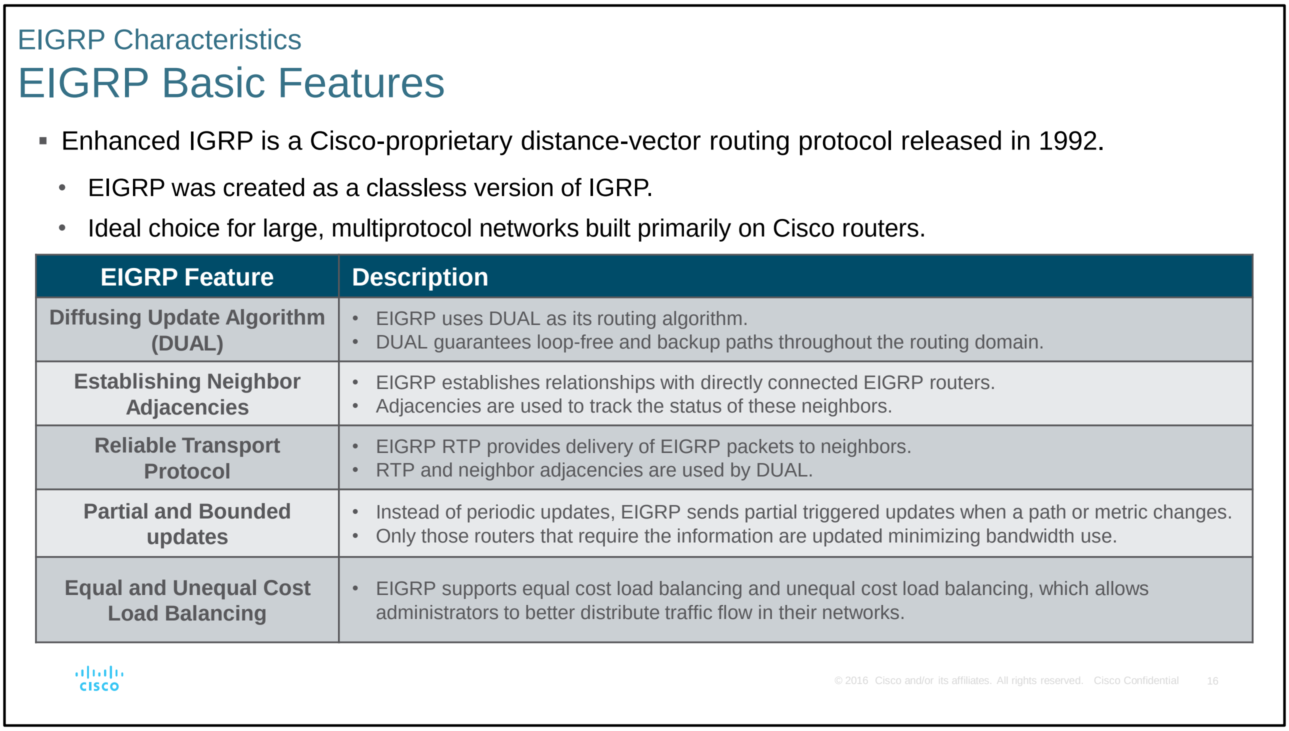


Sections & Objectives (Cont.)

- Tune EIGRP
  - Configure EIGRP to improve network performance.
  - Configure EIGRP autosummarization.
  - Configure a router to propagate a default route in an EIGRP network.
  - Configure EIGRP interface settings to improve network performance.
- Troubleshoot EIGRP
  - Troubleshoot common EIGRP configuration issues in a small to medium-sized business network.
  - Explain the process and tools used to troubleshoot an EIGRP network.
  - Troubleshoot neighbor adjacency issues in an EIGRP network.
  - Troubleshoot missing route entries in an EIGRP routing table.



EIGRP Characteristics



EIGRP Characteristics

EIGRP Basic Features

- Enhanced IGRP is a Cisco-proprietary distance-vector routing protocol released in 1992.
  - EIGRP was created as a classless version of IGRP.
  - Ideal choice for large, multiprotocol networks built primarily on Cisco routers.

EIGRP Feature	Description
Diffusing Update Algorithm (DUAL)	• EIGRP uses DUAL as its routing algorithm. • DUAL guarantees loop-free and backup paths throughout the routing domain.
Establishing Neighbor Adjacencies	• EIGRP establishes relationships with directly connected EIGRP routers. • Adjacencies are used to track the status of these neighbors.
Reliable Transport Protocol	• EIGRP RTP provides delivery of EIGRP packets to neighbors. • RTP and neighbor adjacencies are used by DUAL.
Partial and Bounded updates	• Instead of periodic updates, EIGRP sends partial triggered updates when a path or metric changes. • Only those routers that require the information are updated minimizing bandwidth use.
Equal and Unequal Cost Load Balancing	• EIGRP supports equal cost load balancing and unequal cost load balancing, which allows administrators to better distribute traffic flow in their networks.

Features of EIGRP

EIGRP was initially released in 1992 as a proprietary protocol available only on Cisco devices. However, in 2013, Cisco released a basic functionality of EIGRP as an open standard to the IETF, as an informational RFC. This means that other networking vendors can now implement EIGRP on their equipment to interoperate with both Cisco and non-Cisco routers running EIGRP. However, advanced features of EIGRP, such as EIGRP stub, needed for the Dynamic Multipoint Virtual Private Network (DMVPN) deployment, will not be released to the IETF. As an informational RFC, Cisco will continue to maintain control of EIGRP.

EIGRP includes features of both link-state and distance vector routing protocols. However, EIGRP is still based on the key distance vector routing protocol principle, in which information about the rest of the network is learned from directly connected neighbors.

EIGRP is an advanced distance vector routing protocol that includes features not found in other distance vector routing protocols like RIP and IGRP.

In Cisco IOS Release 15.0(1)M, Cisco introduced a new EIGRP configuration option called **named EIGRP**. Named EIGRP enables the configuration of EIGRP for both IPv4 and IPv6 under a single configuration mode. This helps eliminate configuration complexity that occurs when configuring EIGRP for both IPv4 and IPv6. Named EIGRP is beyond the scope of this course.

Features of EIGRP include:

Diffusing Update Algorithm - As the computational engine that drives EIGRP, the

Diffusing Update Algorithm (DUAL) resides at the center of the routing protocol. DUAL guarantees loop-free and backup paths throughout the routing domain. Using DUAL, EIGRP stores all available backup routes for destinations so that it can quickly adapt to alternate routes when necessary.

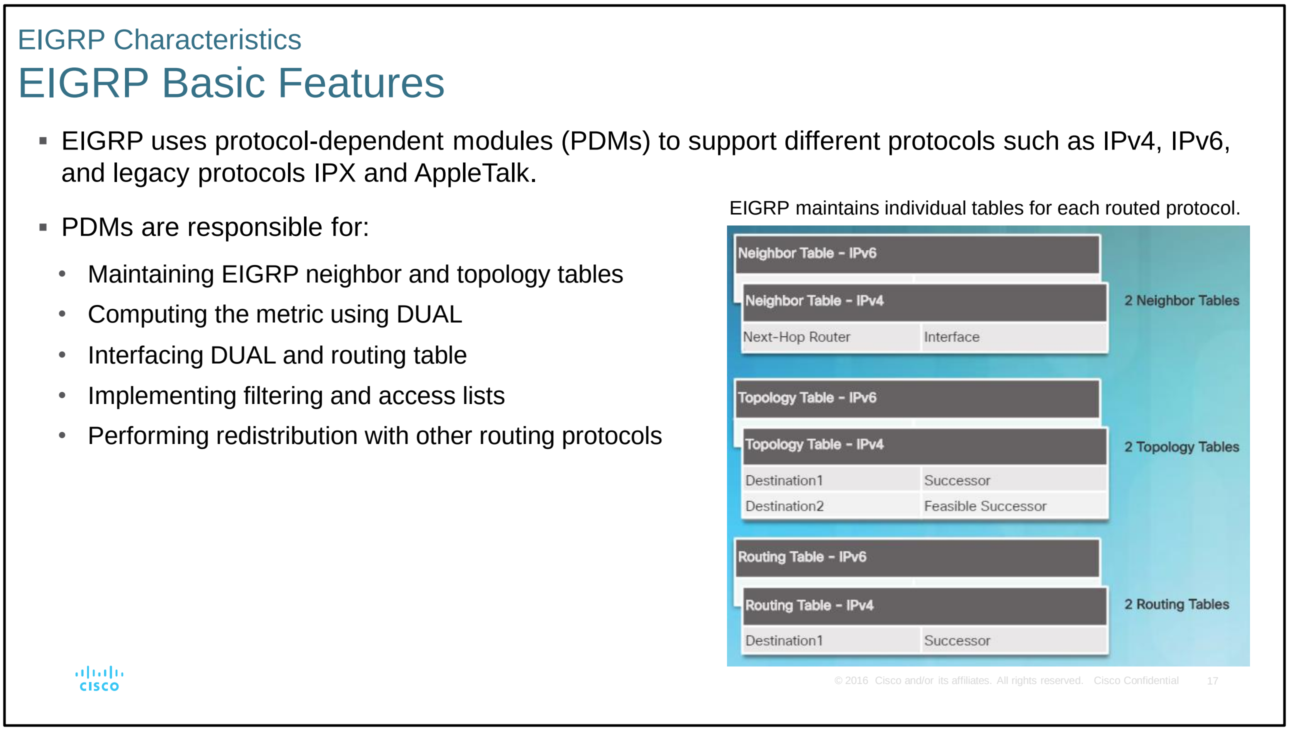
Establishing Neighbor Adjacencies - EIGRP establishes relationships with directly connected routers that are also enabled for EIGRP. Neighbor adjacencies are used to track the status of these neighbors.

Reliable Transport Protocol - The Reliable Transport Protocol (RTP) is unique to EIGRP and provides delivery of EIGRP packets to neighbors. RTP and the tracking of neighbor adjacencies set the stage for DUAL.

Partial and Bounded Updates - EIGRP uses the terms partial and bounded when referring to its updates. Unlike RIP, EIGRP does not send periodic updates and route entries do not age out. The term partial means that the update only includes information about the route changes, such as a new link or a link becoming unavailable. The term bounded refers to the propagation of partial updates that are sent only to those routers that the changes affect. This minimizes the bandwidth that is required to send EIGRP updates.

Equal and Unequal Cost Load Balancing - EIGRP supports equal cost load balancing and unequal cost load balancing, which allows administrators to better distribute traffic flow in their networks.

Note: The term “hybrid routing” protocol may be used in some older documentation to define EIGRP. However, this term is misleading because EIGRP is not a hybrid between distance vector and link-state routing protocols. EIGRP is solely a distance vector routing protocol; therefore, Cisco no longer uses this term to refer to it.



EIGRP Characteristics

EIGRP Basic Features

- EIGRP uses protocol-dependent modules (PDMs) to support different protocols such as IPv4, IPv6, and legacy protocols IPX and AppleTalk.
- PDMs are responsible for:
  - Maintaining EIGRP neighbor and topology tables
  - Computing the metric using DUAL
  - Interfacing DUAL and routing table
  - Implementing filtering and access lists
  - Performing redistribution with other routing protocols

EIGRP maintains individual tables for each routed protocol.

Neighbor Table - IPv6

Neighbor Table - IPv4	
Next-Hop Router	Interface

2 Neighbor Tables

Topology Table - IPv6

Topology Table - IPv4	
Destination1	Successor
Destination2	Feasible Successor

2 Topology Tables

Routing Table - IPv6

Routing Table - IPv4	
Destination1	Successor

2 Routing Tables

Protocol Dependent Modules

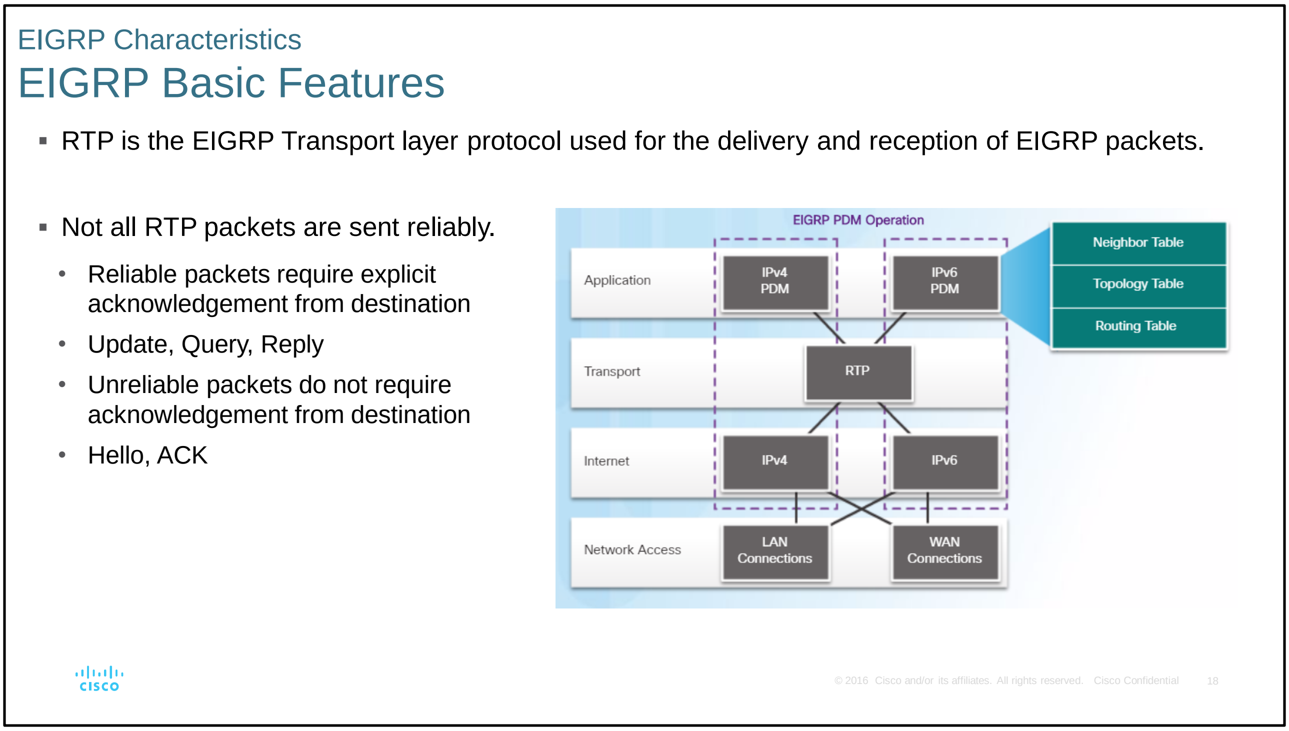
EIGRP has the capability for routing different protocols, including IPv4 and IPv6. EIGRP does so by using protocol-dependent modules (PDMs). PDMs were also used to support the now obsolete Novell IPX and Apple Computer's AppleTalk network layer protocols.

PDMs are responsible for network layer protocol-specific tasks. An example is the EIGRP module that is responsible for sending and receiving EIGRP packets that are encapsulated in IPv4. This module is also responsible for parsing EIGRP packets and informing DUAL of the new information that is received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IPv4 routing table.

PDMs are responsible for the specific routing tasks for each network layer protocol, including:

- Maintaining the neighbor and topology tables of EIGRP routers that belong to that protocol suite
- Building and translating protocol-specific packets for DUAL
- Interfacing DUAL to the protocol-specific routing table
- Computing the metric and passing this information to DUAL
- Implementing filtering and access lists
- Performing redistribution functions to and from other routing protocols
- Redistributing routes that are learned by other routing protocols

When a router discovers a new neighbor, it records the neighbor's address and interface as an entry in the neighbor table. One neighbor table exists for each protocol-dependent module, such as IPv4. EIGRP also maintains a topology table. The topology table contains all destinations that are advertised by neighboring routers. There is also a separate topology table for each PDM.



EIGRP Characteristics

EIGRP Basic Features

- RTP is the EIGRP Transport layer protocol used for the delivery and reception of EIGRP packets.

- Not all RTP packets are sent reliably.
  - Reliable packets require explicit acknowledgement from destination
  - Update, Query, Reply
  - Unreliable packets do not require acknowledgement from destination
  - Hello, ACK

Reliable Transport Protocol

EIGRP was designed as a network layer independent routing protocol. Because of this design, EIGRP cannot use the services of UDP or TCP. Instead, EIGRP uses the Reliable Transport Protocol (RTP) for the delivery and reception of EIGRP packets. This allows EIGRP to be flexible and can be used for protocols other than those from the TCP/IP protocol suite, such as the now obsolete IPX and AppleTalk protocols.

The figure conceptually shows how RTP operates.

Although “reliable” is part of its name, RTP includes both reliable delivery and unreliable delivery of EIGRP packets, similar to TCP and UDP, respectively. Reliable RTP requires an acknowledgment to be returned by the receiver to the sender. An unreliable RTP packet does not require an acknowledgment. For example, an EIGRP update packet is sent reliably over RTP and requires an acknowledgment. An EIGRP Hello packet is also sent over RTP, but unreliably. This means that EIGRP Hello packets do not require an acknowledgment.

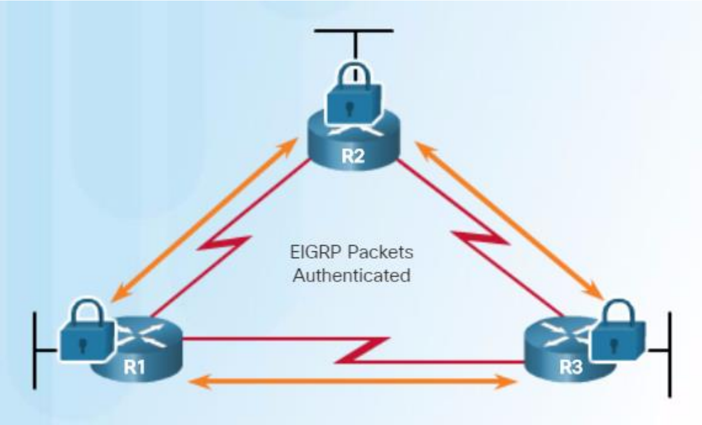
RTP can send EIGRP packets as unicast or multicast.

- Multicast EIGRP packets for IPv4 use the reserved IPv4 multicast address 224.0.0.10.
- Multicast EIGRP packets for IPv6 are sent to the reserved IPv6 multicast address FF02::A.

EIGRP Characteristics

EIGRP Basic Features

- EIGRP supports authentication and is recommended.
  - EIGRP authentication ensures that routers only accept routing information from other routers that have been configured with the same password or authentication information.
- **Note**:
  - Authentication does not encrypt the EIGRP routing updates.

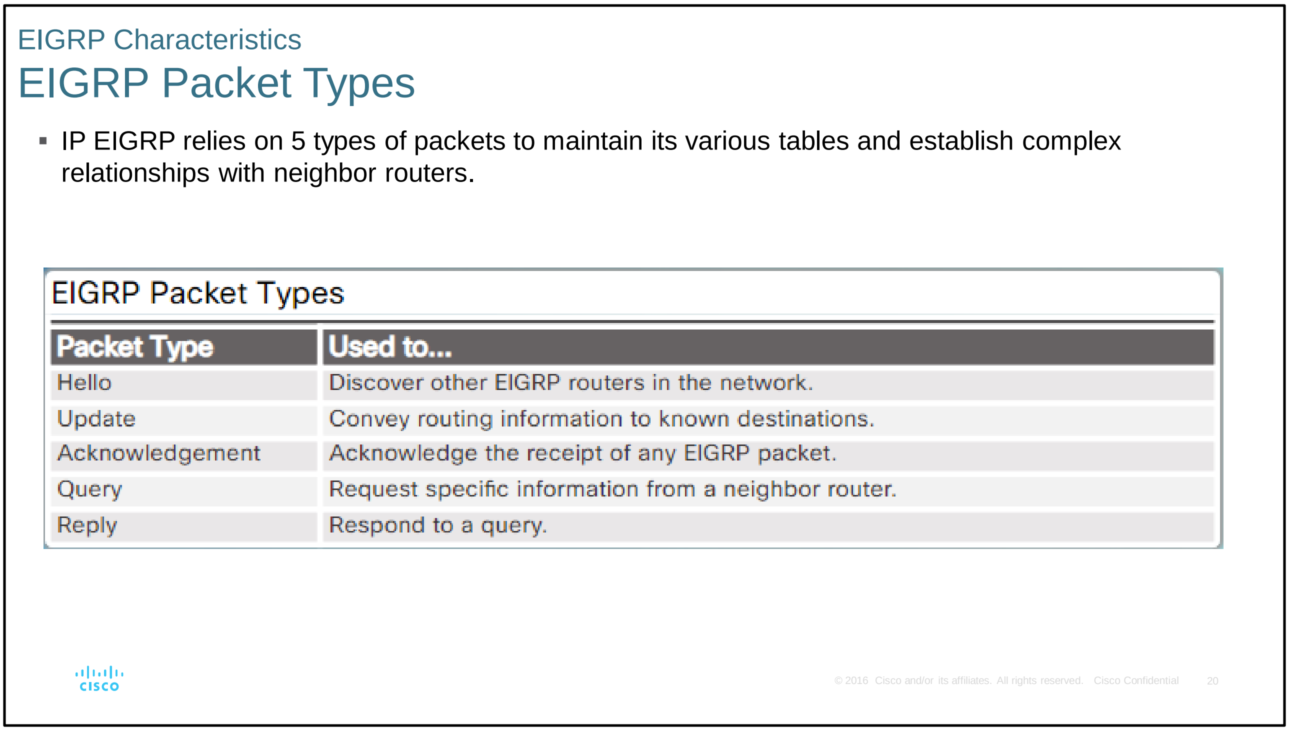


Authentication

Like other routing protocols, EIGRP can be configured for authentication. RIPv2, EIGRP, OSPF, IS-IS, and BGP can each be configured to authenticate their routing information.

It is a good practice to authenticate transmitted routing information. Doing so ensures that routers only accept routing information from other routers that have been configured with the same password or authentication information.

Note: Authentication does not encrypt the EIGRP routing updates.



EIGRP Characteristics

EIGRP Packet Types

- IP EIGRP relies on 5 types of packets to maintain its various tables and establish complex relationships with neighbor routers.

EIGRP Packet Types

Packet Type	Used to...
Hello	Discover other EIGRP routers in the network.
Update	Convey routing information to known destinations.
Acknowledgement	Acknowledge the receipt of any EIGRP packet.
Query	Request specific information from a neighbor router.
Reply	Respond to a query.

EIGRP Packet Types

EIGRP uses five different packet types, some in pairs. EIGRP packets are sent using either RTP reliable or unreliable delivery and can be sent as a unicast, multicast, or sometimes both. EIGRP packet types are also called EIGRP packet formats or EIGRP messages.

As shown in Figure, the five EIGRP packet types include:

Hello packets - Used for neighbor discovery and to maintain neighbor adjacencies.

- Sent with unreliable delivery
- Multicast (on most network types)

Update packets - Propagates routing information to EIGRP neighbors.

- Sent with reliable delivery
- Unicast or multicast

Acknowledgment packets - Used to acknowledge the receipt of an EIGRP message that was sent using reliable delivery.

- Sent with unreliable delivery
- Unicast

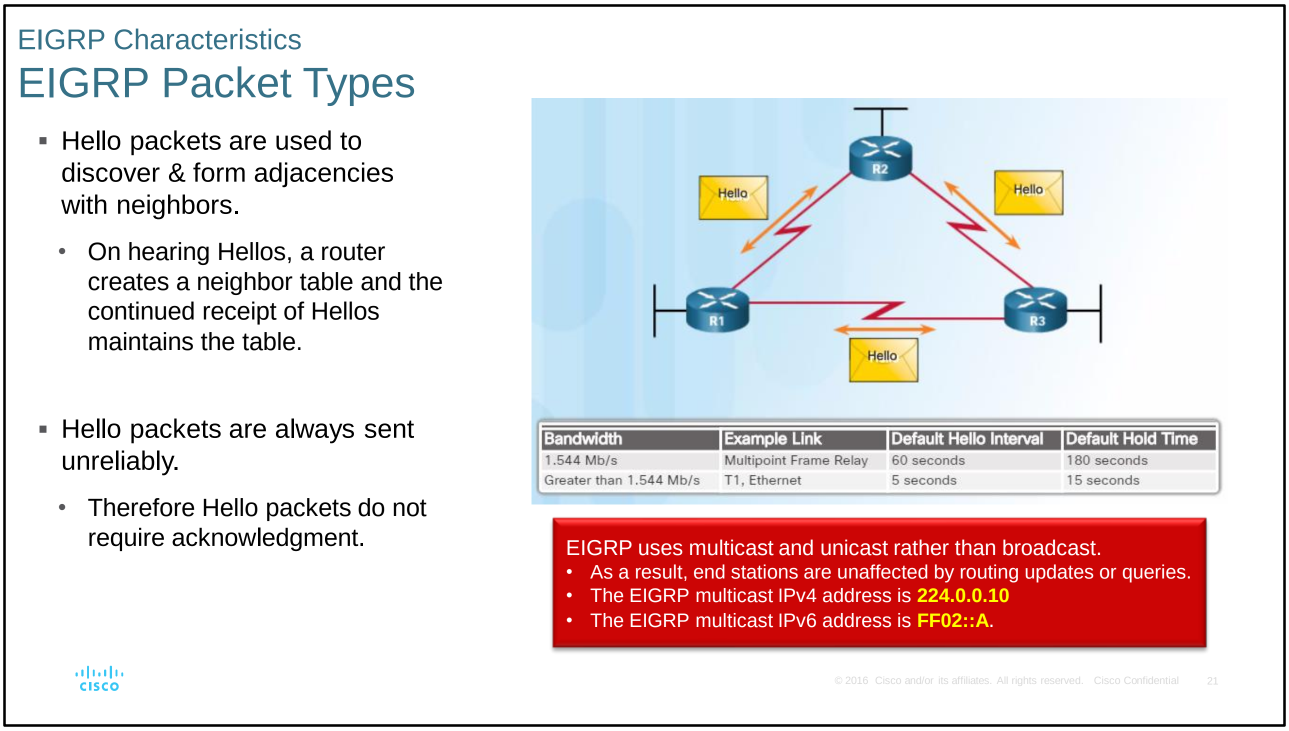
Query packets - Used to query routes from neighbors.

- Sent with reliable delivery
- Unicast or multicast

Reply packets - Sent in response to an EIGRP query.

- Sent with reliable delivery
- Unicast

EIGRP messages are typically encapsulated in IPv4 or IPv6 packets. EIGRP for IPv4 messages use IPv4 as the network layer protocol. The IPv4 protocol field uses 88 to indicate the data portion of the packet is an EIGRP for IPv4 message. EIGRP for IPv6 messages are encapsulated in IPv6 packets using the next header field of 88. Similar to the protocol field for IPv4, the IPv6 next header field indicates the type of data carried in the IPv6 packet.



EIGRP Characteristics

EIGRP Packet Types

- Hello packets are used to discover & form adjacencies with neighbors.
  - On hearing Hellos, a router creates a neighbor table and the continued receipt of Hellos maintains the table.
- Hello packets are always sent unreliably.
  - Therefore Hello packets do not require acknowledgment.

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 uses multicast and unicast rather than broadcast.

- As a result, end stations are unaffected by routing updates or queries.
- The EIGRP multicast IPv4 address is **224.0.0.10**
- The EIGRP multicast IPv6 address is **FF02::A**.

EIGRP Hello Packets

EIGRP uses small Hello packets to discover other EIGRP-enabled routers on directly connected links. Hello packets are used by routers to form EIGRP neighbor adjacencies, also known as neighbor relationships.

EIGRP Hello packets are sent as IPv4 or IPv6 multicasts, and use RTP unreliable delivery. This means that the receiver does not reply with an acknowledgment packet.

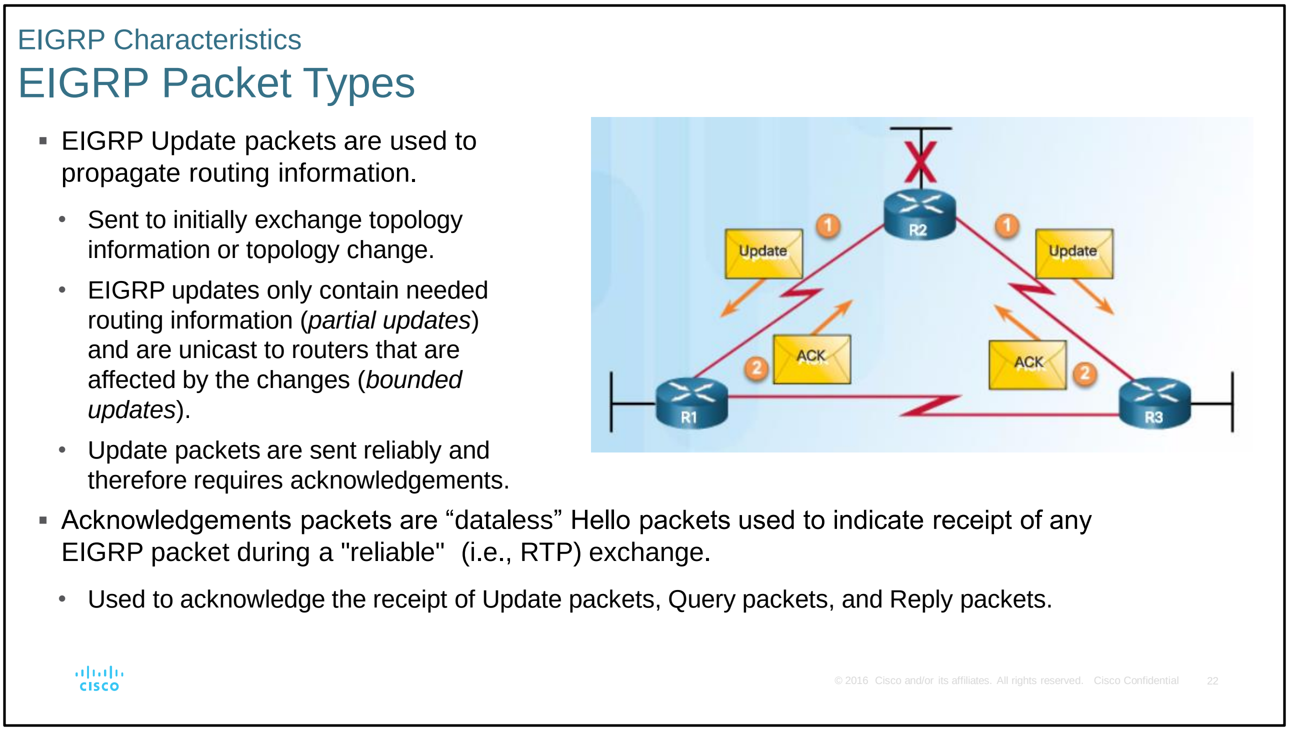
- The reserved EIGRP multicast address for IPv4 is 224.0.0.10.
- The reserved EIGRP multicast address for IPv6 is FF02::A.

EIGRP routers discover neighbors and establish adjacencies with neighbor routers using the Hello packet. On most modern networks, EIGRP Hello packets are sent as **multicast** packets **every five seconds**. However, on **multipoint, non-broadcast multiple access (NBMA) networks with access links of T1 (1.544 Mb/s) or slower**, Hello packets are sent as **unicast packets every 60 seconds**.

Note: NBMA networks using slower interfaces include legacy X.25, Frame Relay, and Asynchronous Transfer Mode (ATM).

EIGRP also uses Hello packets to maintain established adjacencies. An EIGRP router assumes that as long as it receives Hello packets from a neighbor, the neighbor and its routes remain viable.

EIGRP uses a Hold timer to determine the maximum time the router should wait to receive the next Hello before declaring that neighbor as unreachable. By default, **the hold time is three times the Hello interval**, or 15 seconds on most networks and 180 seconds on low-speed NBMA networks. If the hold time expires, EIGRP declares the route as down and DUAL searches for a new path by sending out queries.



EIGRP Characteristics

EIGRP Packet Types

- EIGRP Update packets are used to propagate routing information.
  - Sent to initially exchange topology information or topology change.
  - EIGRP updates only contain needed routing information (*partial updates*) and are unicast to routers that are affected by the changes (*bounded updates*).
  - Update packets are sent reliably and therefore requires acknowledgements.
- Acknowledgements packets are “dataless” Hello packets used to indicate receipt of any EIGRP packet during a "reliable" (i.e., RTP) exchange.
  - Used to acknowledge the receipt of Update packets, Query packets, and Reply packets.

EIGRP Update and Acknowledgment Packets

EIGRP Update Packets

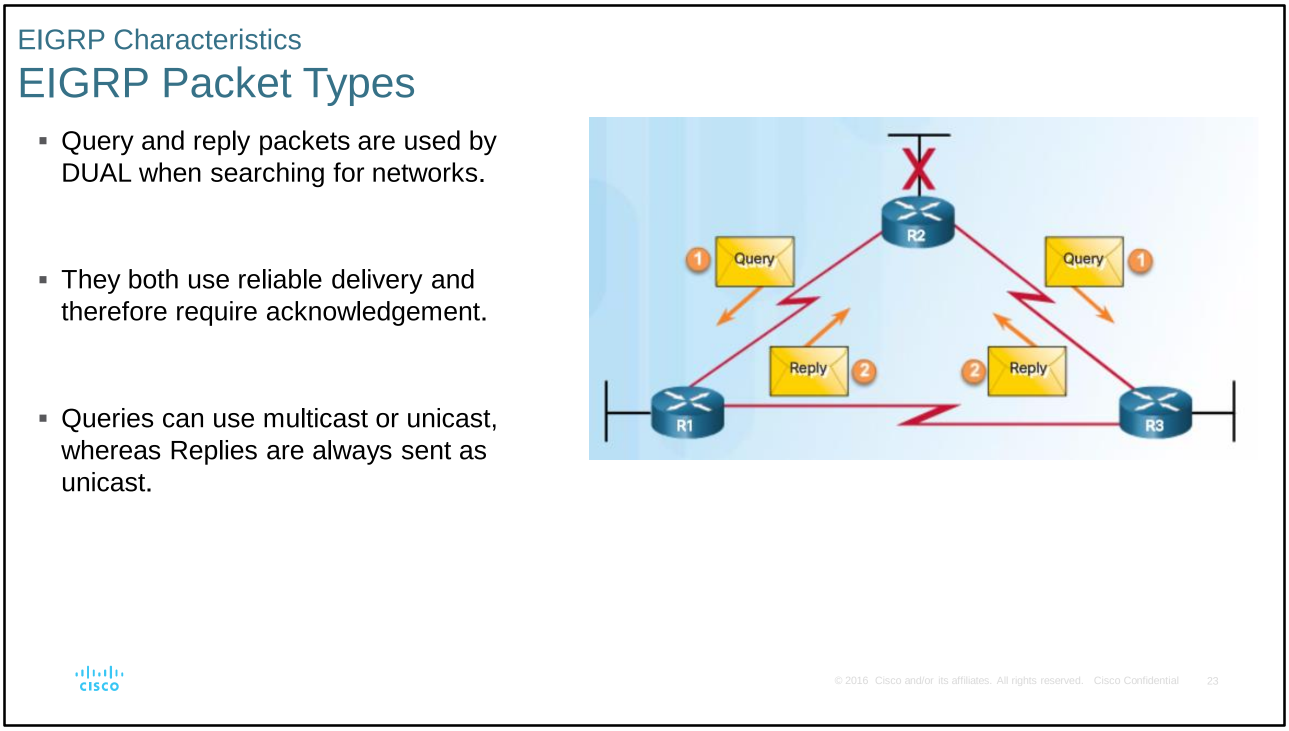
EIGRP sends Update packets to propagate routing information. Update packets are sent only when necessary. EIGRP updates contain only the routing information needed and are sent only to those routers that require it.
Unlike the older distance vector routing protocol RIP, EIGRP does not send periodic updates and route entries do not age out. Instead, EIGRP sends incremental updates only when the state of a destination changes. This may include when a new network becomes available, an existing network becomes unavailable, or a change occurs in the routing metric for an existing network.
EIGRP uses the terms *partial update* and *bounded update* when referring to its updates. A partial update means that the update only includes information about route changes. A bounded update refers to the sending of partial updates only to the routers that are affected by the changes. Bounded updates help EIGRP minimize the bandwidth that is required to send EIGRP updates.
EIGRP Update packets use reliable delivery, which means the sending router requires an acknowledgment. Update packets are sent as a multicast when required by multiple routers, or as a unicast when required by only a single router. In the figure, the updates are sent as unicasts because the links are point-to-point.

EIGRP Acknowledgment Packets

EIGRP sends Acknowledgment (ACK) packets when reliable delivery is used. An EIGRP acknowledgment is an EIGRP Hello packet without any data. RTP uses reliable delivery for Update, Query, and Reply packets. EIGRP Acknowledgment packets are always sent as an unreliable unicast. Unreliable delivery makes sense; otherwise, there would be an endless loop of acknowledgments.

In the figure, R2 has lost connectivity to the LAN attached to its Gigabit Ethernet interface. R2 immediately sends an update to R1 and R3 noting the downed route. R1 and R3 respond with an acknowledgment to let R2 know that they have received the update.

Note: Some documentation refers to the Hello and acknowledgment as a single type of EIGRP packet.



EIGRP Characteristics

EIGRP Packet Types

- Query and reply packets are used by DUAL when searching for networks.
- They both use reliable delivery and therefore require acknowledgement.
- Queries can use multicast or unicast, whereas Replies are always sent as unicast.

R2
1
Query
Query
1
Reply
2
2
Reply
R1
R3

23

EIGRP Query and Reply Packets

EIGRP Query Packets

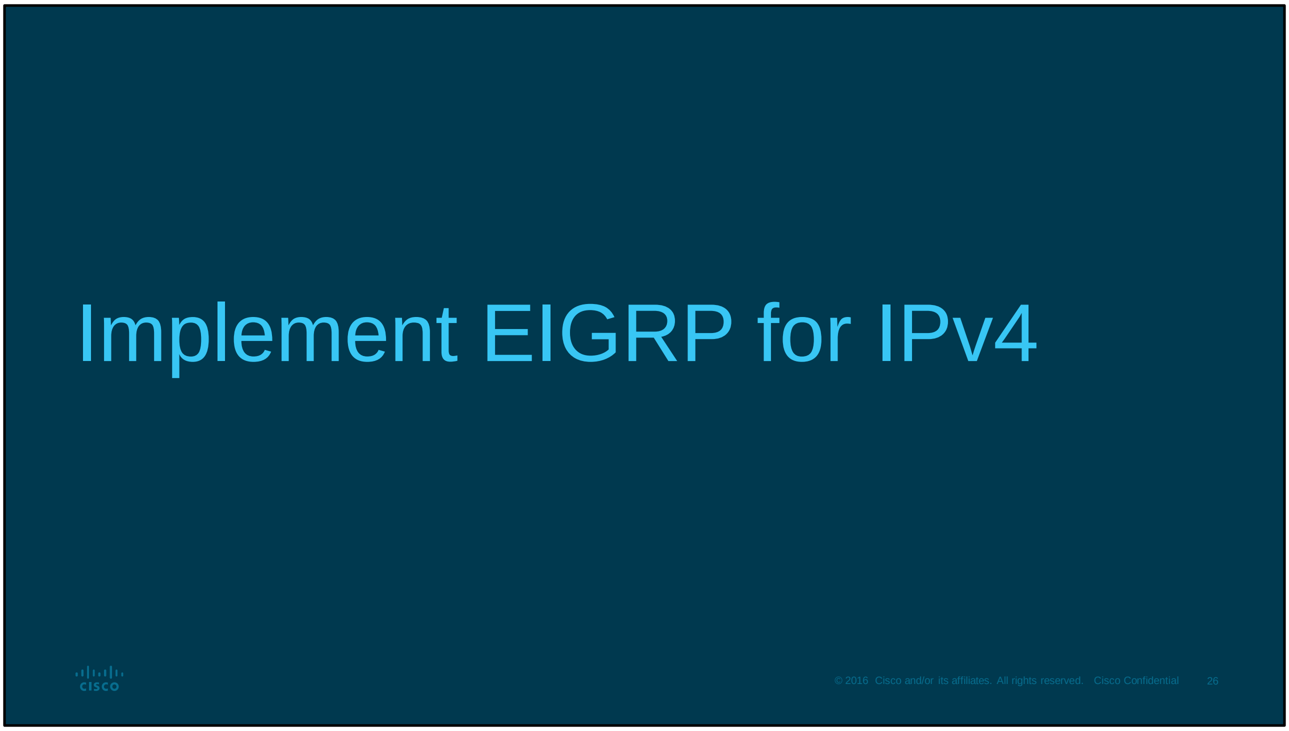
DUAL uses Query and Reply packets when searching for networks and other tasks. Queries and replies use reliable delivery. Queries can use multicast or unicast, whereas replies are always sent as unicast.

In the figure, R2 has lost connectivity to the LAN and it sends out queries to all EIGRP neighbors searching for any possible routes to the LAN. Because queries use reliable delivery, the receiving router must return an EIGRP acknowledgment. The acknowledgment informs the sender of the query that it has received the query message. To keep this example simple, acknowledgments were omitted in the graphic.

EIGRP Reply Packets

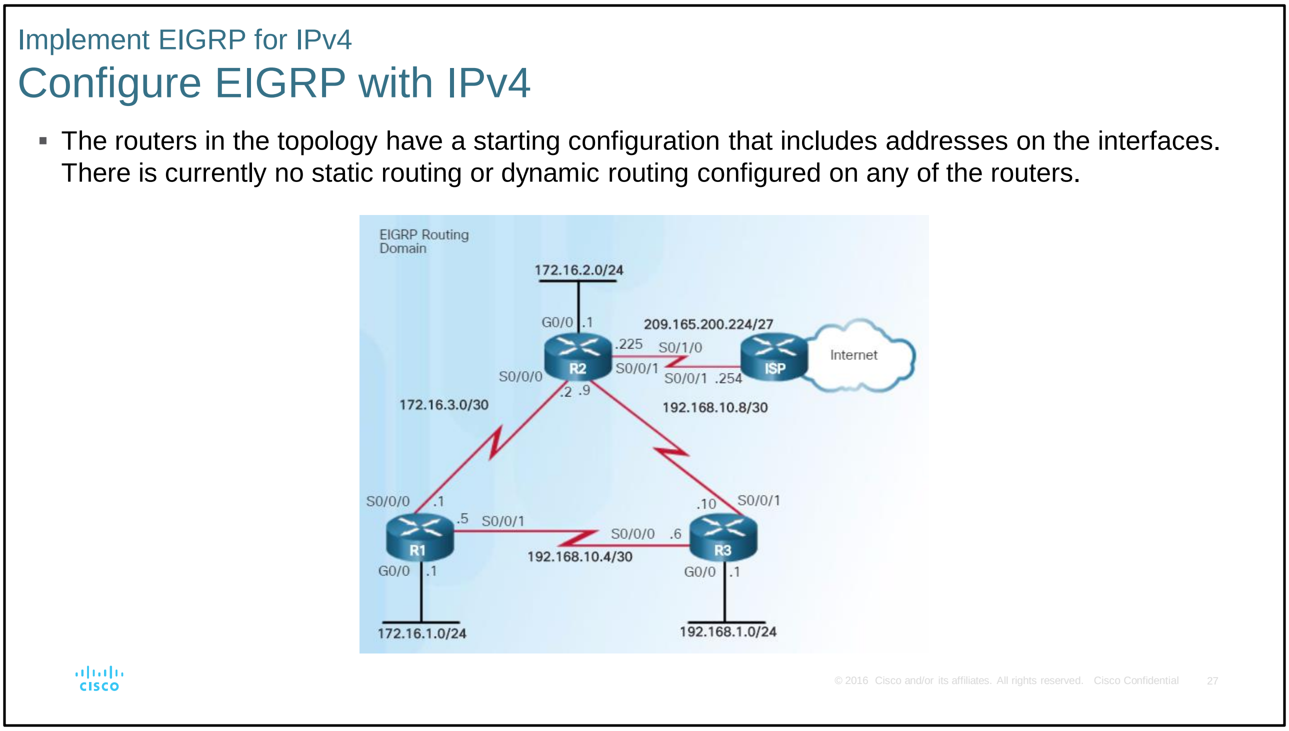
All neighbors must send a reply, regardless of whether or not they have a route to the downed network. Because replies also use reliable delivery, routers, such as R3, must send an acknowledgment.

It may not be obvious why R2 would send out a query for a network it knows is down. Actually, only R2’s interface that is attached to the network is down. Another router could be attached to the same LAN and have an alternate path to this same network. Therefore, R2 queries for such a router before completely removing the network from its topology table.



Implement EIGRP for IPv4

6 - EIGRP
6.2 – Implement EIGRP for IPv4



Implement EIGRP for IPv4

Configure EIGRP with IPv4

- The routers in the topology have a starting configuration that includes addresses on the interfaces. There is currently no static routing or dynamic routing configured on any of the routers.

EIGRP Network Topology

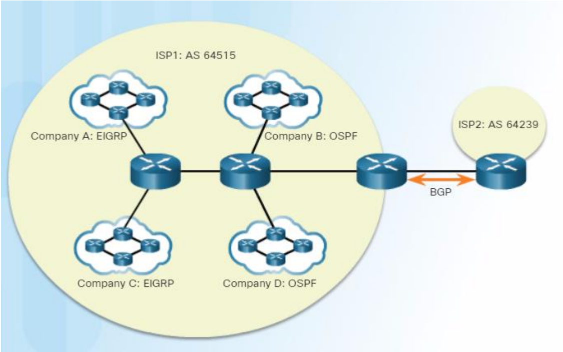
Figure displays the topology that is used in this chapter to configure EIGRP for IPv4. The routers in the topology have a starting configuration that includes addresses on the interfaces. There is currently no static routing or dynamic routing configured on any of the routers.

Only routers R1, R2, and R3 are part of the EIGRP routing domain. The ISP router is used as the routing domain’s gateway to the Internet.

Implement EIGRP for IPv4

Configure EIGRP with IPv4

- An Autonomous System (AS) is a collection of networks under the control of a single authority (reference RFC 1930).
  - AS numbers are needed to exchange routes between AS.
  - AS numbers are managed by IANA and assigned by RIRs to ISPs, Internet Backbone providers, and institutions connecting to other institutions using AS numbers.



- AS numbers are usually 16-bit numbers, ranging from 0 to 65535.
  - Since 2007, AS numbers can now be 32 bits, therefore increasing the number of AS numbers to over 4 billion.

Autonomous System Numbers

EIGRP uses the **router eigrp** *autonomous-system* command to enable the EIGRP process. The autonomous system number referred to in the EIGRP configuration is not associated with the Internet Assigned Numbers Authority (IANA) globally assigned autonomous system numbers used by external routing protocols.

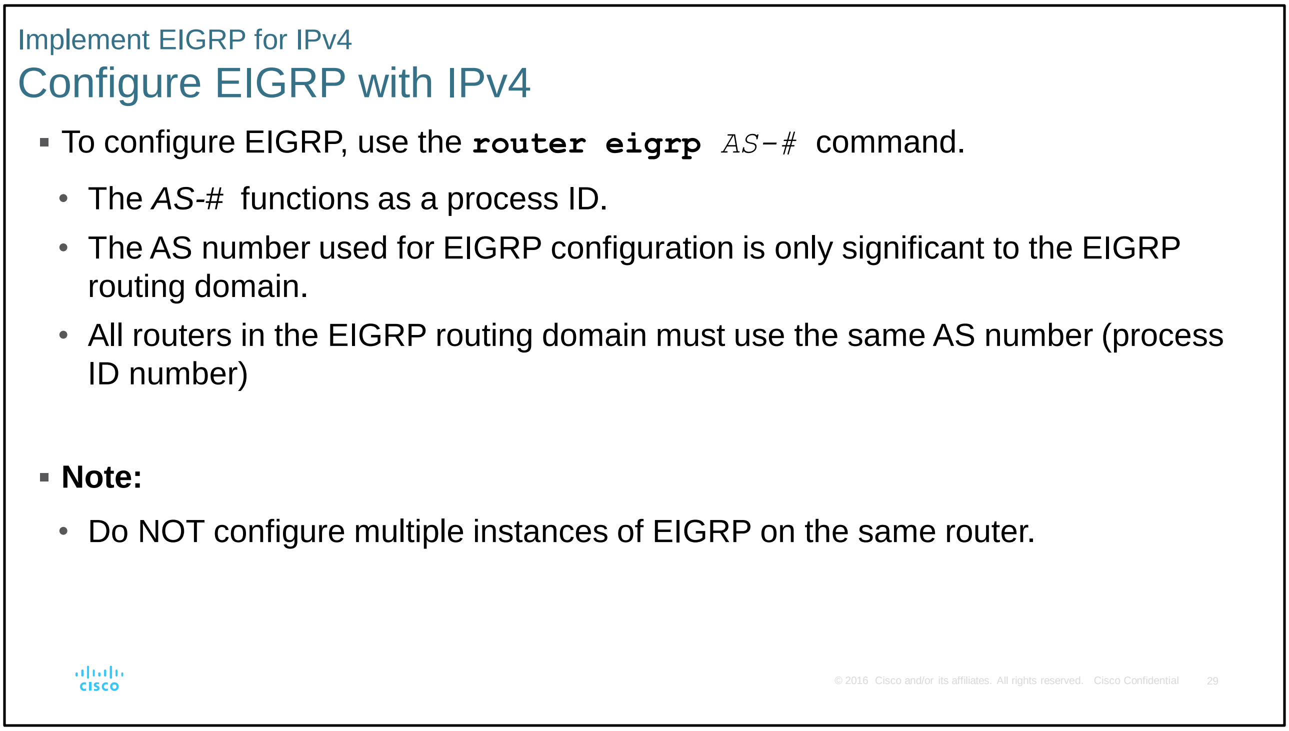
So what is the difference between the IANA globally assigned autonomous system number and the EIGRP autonomous system number?

An IANA globally assigned autonomous system is a collection of networks under the administrative control of a single entity that presents a common routing policy to the Internet. In the figure, companies A, B, C, and D are all under the administrative control of ISP1. ISP1 presents a common routing policy for all of these companies when advertising routes to ISP2.

The guidelines for the creation, selection, and registration of an autonomous system are described in RFC 1930. Global autonomous system numbers are assigned by IANA, the same authority that assigns IP address space. The local regional Internet registry (RIR) is responsible for assigning an autonomous system number to an entity from its block of assigned autonomous system numbers. Prior to 2007, assigned autonomous system numbers were 16-bit numbers ranging from 0 to 65,535. Today, 32-bit autonomous system numbers are assigned thereby increasing the number of available autonomous system numbers to over 4 billion.

Usually, only Internet Service Providers (ISPs), Internet backbone providers, and large institutions connecting to other entities require an autonomous system number.

These ISPs and large institutions use the exterior gateway routing protocol, Border Gateway Protocol (BGP), to propagate routing information. BGP is the only routing protocol that uses an actual autonomous system number in its configuration.
The vast majority of companies and institutions with IP networks do not need an autonomous system number, because they are controlled by a larger entity, such as an ISP. These companies use interior gateway protocols, such as RIP, EIGRP, OSPF, and IS-IS to route packets within their own networks. They are one of many independent and separate networks within the autonomous system of the ISP. The ISP is responsible for the routing of packets within its autonomous system and between other autonomous systems.
The autonomous system number used for EIGRP configuration is only significant to the EIGRP routing domain. It functions as a process ID to help routers keep track of multiple running instances of EIGRP. This is required because it is possible to have more than one instance of EIGRP running on a network. Each instance of EIGRP can be configured to support and exchange routing updates for different networks.



Implement EIGRP for IPv4

Configure EIGRP with IPv4

- To configure EIGRP, use the **`router eigrp`** *`AS-#`* command.
  - The *AS-#* functions as a process ID.
  - The AS number used for EIGRP configuration is only significant to the EIGRP routing domain.
  - All routers in the EIGRP routing domain must use the same AS number (process ID number)
- **Note:**
  - Do NOT configure multiple instances of EIGRP on the same router.

29

The router eigrp Command

The Cisco IOS includes the processes to enable and configure several different types of dynamic routing protocols. The **router** global configuration mode command is used to begin the configuration of any dynamic routing protocol. The topology shown in Figure 1 is used to demonstrate this command.

When followed by a question mark (**?**), the **router** global configuration mode command lists of all the available routing protocols supported by this specific IOS release running on the router.

The following global configuration mode command is used to enter the router configuration mode for EIGRP and begin the configuration of the EIGRP process:

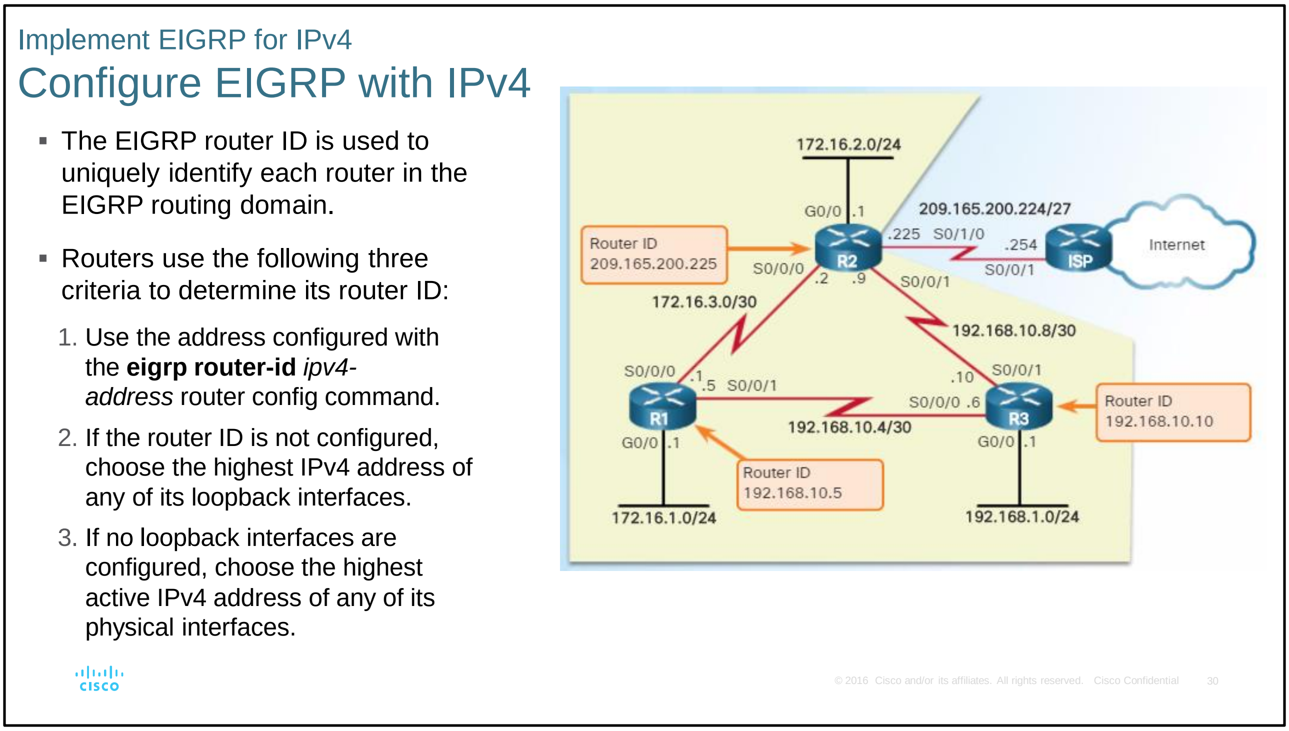
Router(config)# **router eigrp** *autonomous-system*

The *autonomous-system* argument can be assigned to any 16-bit value between the number 1 and 65,535. All routers within the EIGRP routing domain must use the same autonomous system number.

Note: EIGRP and OSPF can support multiple instances of the routing protocol. However, this multiple routing protocol implementation is not usually needed or recommended.

The **router eigrp** *autonomous-system* command does not start the EIGRP process itself. The router does not start sending updates. Rather, this command only provides access to configure the EIGRP settings.

To completely remove the EIGRP routing process from a device, use the **no router eigrp** *autonomous-system* global configuration mode command, which stops the EIGRP process and removes all existing EIGRP router configurations.



Implement EIGRP for IPv4

Configure EIGRP with IPv4

- The EIGRP router ID is used to uniquely identify each router in the EIGRP routing domain.
- Routers use the following three criteria to determine its router ID:

1. Use the address configured with the **eigrp router-id** *ipv4-address* router config command.
2. If the router ID is not configured, choose the highest IPv4 address of any of its loopback interfaces.
3. If no loopback interfaces are configured, choose the highest active IPv4 address of any of its physical interfaces.

EIGRP Router ID

The EIGRP router ID is used to uniquely identify each router in the EIGRP routing domain.

The router ID is used in both EIGRP and OSPF routing protocols. However, the role of the router ID is more significant in OSPF. In EIGRP IPv4 implementations, the use of the router ID is not that apparent. EIGRP for IPv4 uses the 32-bit router ID to identify the originating router for redistribution of external routes. The need for a router ID becomes more evident in the discussion of EIGRP for IPv6. While the router ID is necessary for redistribution, the details of EIGRP redistribution are beyond the scope of this curriculum. For purposes of this curriculum, it is only necessary to understand what the router ID is and how it is determined.

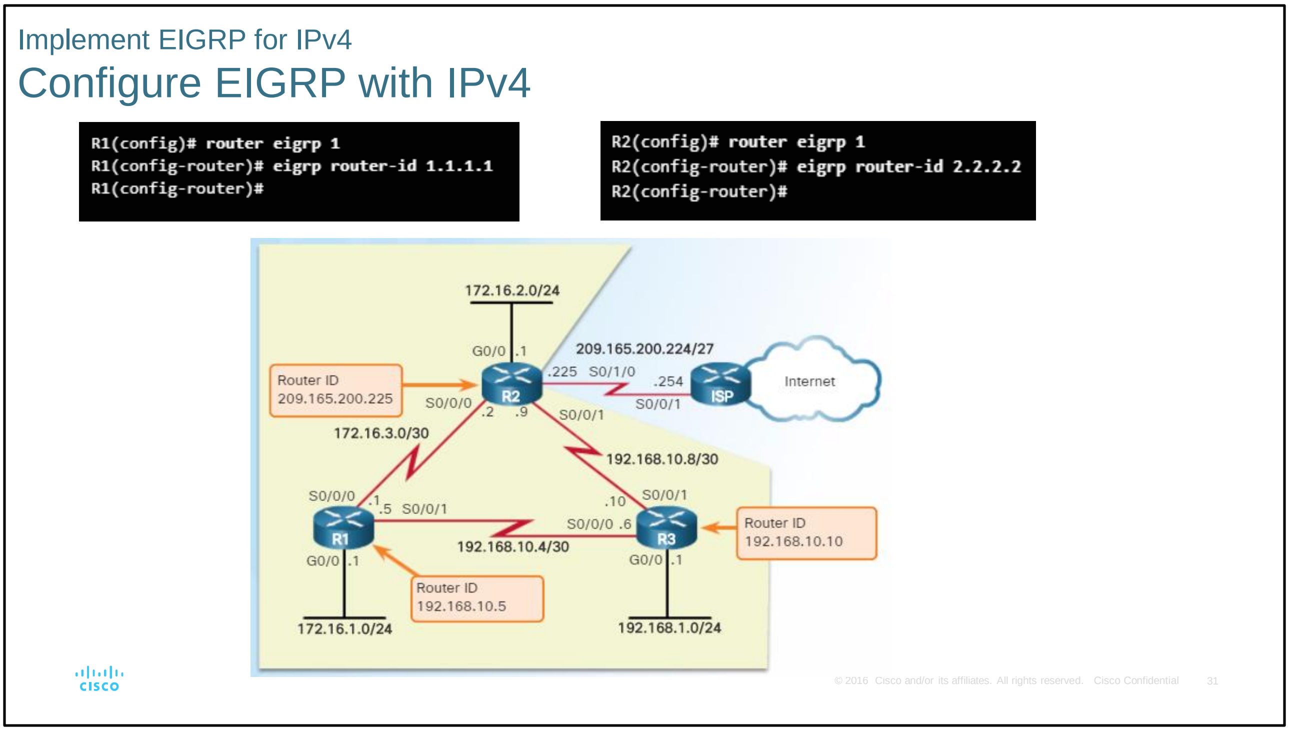
To determine its router ID, a Cisco IOS router will use the following three criteria in order:

1. Use the address configured with the **eigrp router-id** *ipv4-address* router configuration mode command.
2. If the router ID is not configured, choose the highest IPv4 address of any of its loopback interfaces.
3. If no loopback interfaces are configured, choose the highest active IPv4 address of any of its physical interfaces.

If the network administrator does not explicitly configure a router ID using the **eigrp**

router-id command, EIGRP generates its own router ID using either a loopback or physical IPv4 address. A loopback address is a virtual interface and is automatically in the up state when configured. The interface does not need to be enabled for EIGRP, meaning that it does not need to be included in one of the EIGRP **network** commands. However, the interface must be in the up/up state.
Using the criteria described above, the figure shows the default EIGRP router IDs that are determined by the routers' highest active IPv4 address.

Note: The **eigrp router-id** command is used to configure the router ID for EIGRP. Some versions of IOS will accept the command **router-id**, without first specifying **eigrp**. The running-config, however, will display **eigrp router-id** regardless of which command is used.



Implement EIGRP for IPv4

Configure EIGRP with IPv4

```
R1(config)# router eigrp 1
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)#
```

```
R2(config)# router eigrp 1
R2(config-router)# eigrp router-id 2.2.2.2
R2(config-router)#
```

31

Configuring the EIGRP Router ID

The **eigrp router-id** *ipv4-address* router configuration command is the preferred method used to configure the EIGRP router ID. This method takes precedence over any configured loopback or physical interface IPv4 addresses.

Note: The IPv4 address used to indicate the router ID is actually any 32-bit number displayed in dotted-decimal notation.

The *ipv4-address* router ID can be configured with any IPv4 address except 0.0.0.0 and 255.255.255.255. The router ID should be a unique 32-bit number in the EIGRP routing domain; otherwise, routing inconsistencies can occur.

Figure shows the configuration of the EIGRP router ID for routers R1 and R2.

If a router ID is not explicitly configured, then the router would use its highest IPv4 address configured on a loopback interface. The advantage of using a loopback interface is that unlike physical interfaces, loopbacks cannot fail. There are no actual cables or adjacent devices on which the loopback interface depends for being in the up state. Therefore, using a loopback address for the router ID can provide a more consistent router ID than using an interface address.

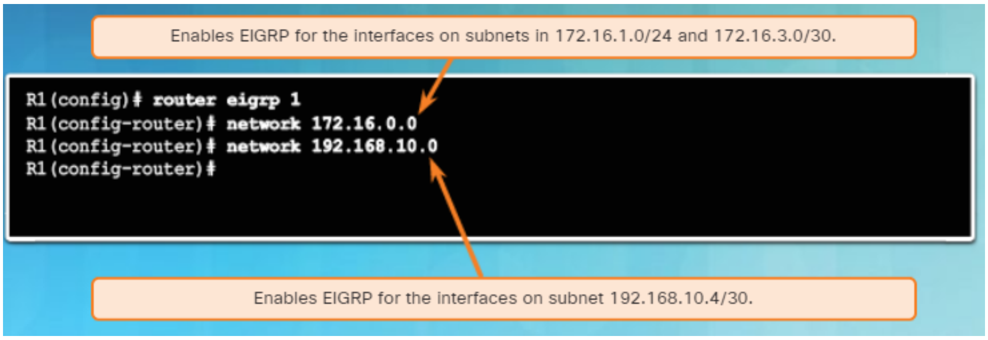
If the **eigrp router-id** command is not used and loopback interfaces are configured, EIGRP chooses the highest IPv4 address of any of its loopback interfaces. The following commands are used to enable and configure a loopback interface:

- Router(config)# **interface loopback** *number*
- Router(config-if)# **ip address** *ipv4-address subnet-mask*

Implement EIGRP for IPv4

Configure EIGRP with IPv4

- Use the **network** *network-number* [*wildcard-mask*] router config command to enable and advertise a network in EIGRP.
  - It enables the interfaces configured for that network address to begin transmitting & receiving EIGRP updates
  - Includes network or subnet in EIGRP updates



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

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

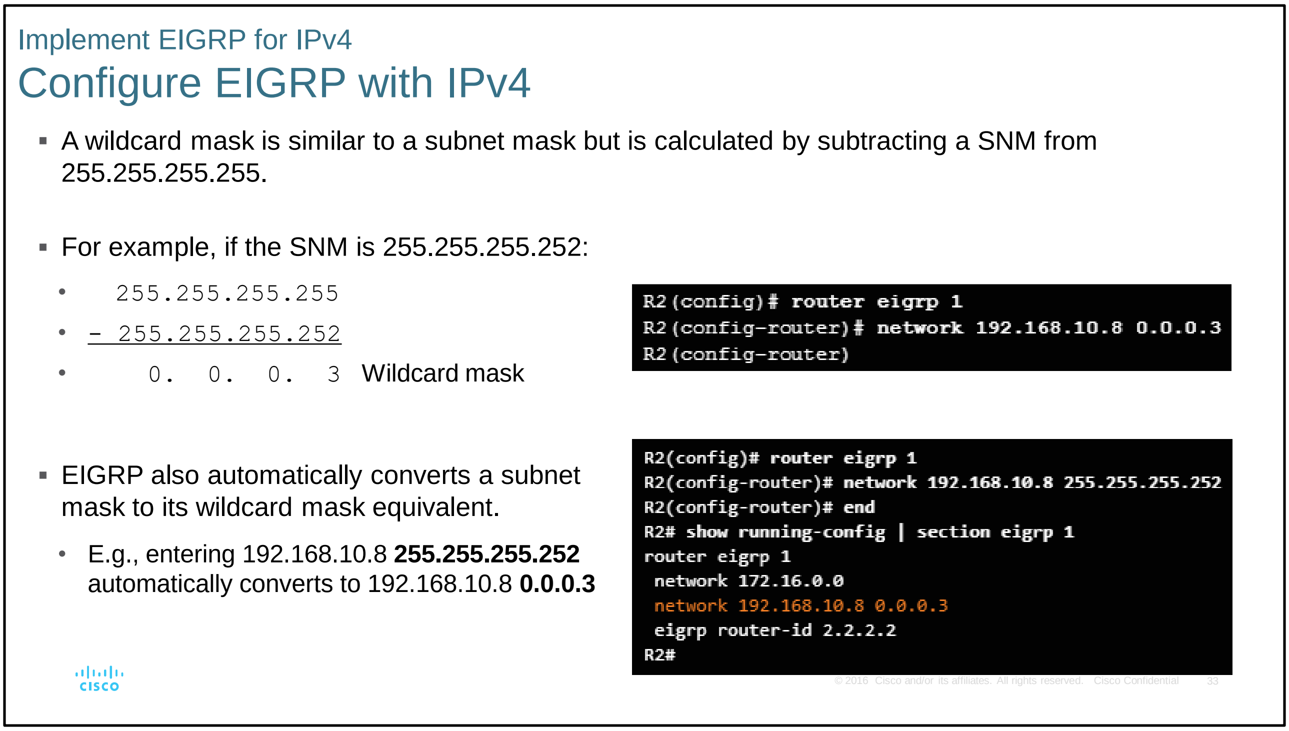
Enables EIGRP for the interfaces on subnet 192.168.10.4/30.

The network Command

EIGRP router configuration mode allows for the configuration of the EIGRP routing protocol. To enable EIGRP routing on an interface, use the **network** *ipv4-network-address* router configuration mode command. The *ipv4-network-address* is the classful network address for each directly connected network.

The **network** command has the same function as in all IGP routing protocols. The **network** command in EIGRP:

- Enables any interface on this router that matches the network address in the **network** router configuration mode command to send and receive EIGRP updates.
- The network of the interfaces is included in EIGRP routing updates.



Implement EIGRP for IPv4

Configure EIGRP with IPv4

- A wildcard mask is similar to a subnet mask but is calculated by subtracting a SNM from 255.255.255.255.
- For example, if the SNM is 255.255.255.252:

```
•   255.255.255.255
• - 255.255.255.252
•     0.  0.  0.  3   Wildcard mask
```

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.10.8 0.0.0.3
R2(config-router)
```

- EIGRP also automatically converts a subnet mask to its wildcard mask equivalent.
  - E.g., entering 192.168.10.8 **255.255.255.252** automatically converts to 192.168.10.8 **0.0.0.3**

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.10.8 255.255.255.252
R2(config-router)# end
R2# show running-config | section eigrp 1
router eigrp 1
 network 172.16.0.0
 network 192.168.10.8 0.0.0.3
 eigrp router-id 2.2.2.2
R2#
```

The network Command and Wildcard Mask

By default, when using the **network** command and an IPv4 network address, such as 172.16.0.0, all interfaces on the router that belong to that classful network address are enabled for EIGRP. However, there may be times when the network administrator does not want to include all interfaces within a network when enabling EIGRP. For example, in Figure, assume that an administrator wants to enable EIGRP on R2, but only for the subnet 192.168.10.8 255.255.255.252, on the S0/0/1 interface.

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

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

A wildcard mask is similar to the inverse of a subnet mask. In a subnet mask, binary 1s are significant while binary 0s are not. In a wildcard mask, binary 0s are significant, while binary 1s are not. For example, the inverse of subnet mask 255.255.255.252 is 0.0.0.3.

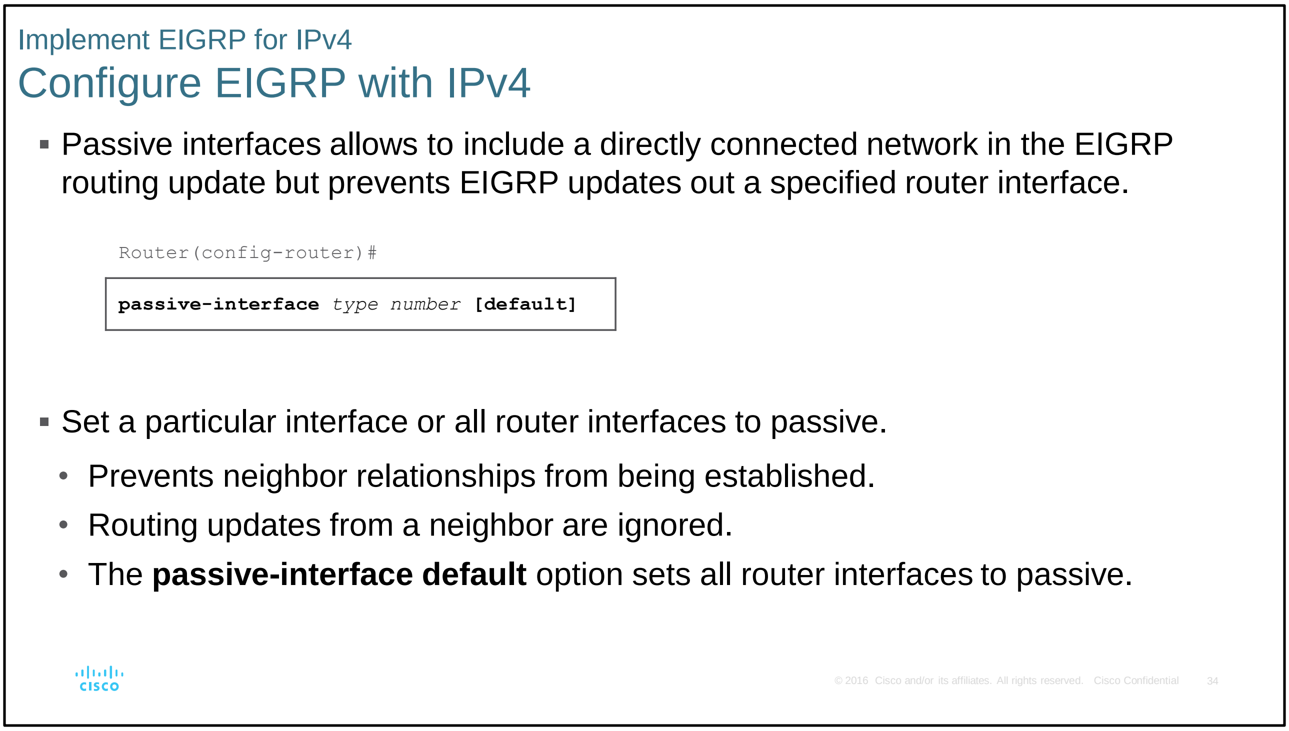
Calculating a wildcard mask may seem daunting at first but it’s actually pretty easy to do. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255 as follows:

```
  255.255.255.255
- 255.255.255.252
  ---------------
```

0. 0. 0. 3 Wildcard mask

Figure continues the EIGRP network configuration of R2. The **network 192.168.10.8 0.0.0.3** command specifically enables EIGRP on the S0/0/1 interface, a member of the 192.168.10.8 255.255.255.252 subnet.

Configuring a wildcard mask is the official command syntax of the EIGRP **network** command. However, the Cisco IOS versions also accepts a subnet mask to be used instead. For example, Figure 3 configures the same S0/0/1 interface on R2, but this time using a subnet mask in the **network** command. Notice in the output of the **show running-config** command, the IOS converted the subnet mask command to its wildcard mask.



Implement EIGRP for IPv4

Configure EIGRP with IPv4

- Passive interfaces allows to include a directly connected network in the EIGRP routing update but prevents EIGRP updates out a specified router interface.

```
Router(config-router)#
passive-interface type number [default]
```

- Set a particular interface or all router interfaces to passive.
  - Prevents neighbor relationships from being established.
  - Routing updates from a neighbor are ignored.
  - The **passive-interface default** option sets all router interfaces to passive.

Passive Interface

As soon as a new interface is enabled within the EIGRP network, EIGRP attempts to form a neighbor adjacency with any neighboring routers to send and receive EIGRP updates.

At times it may be necessary, or advantageous, to include a directly connected network in the EIGRP routing update, but not allow any neighbor adjacencies off of that interface to form.

The **passive-interface** command can be used to prevent the neighbor adjacencies.

There are two primary reasons for enabling the **passive-interface** command:

- To suppress unnecessary update traffic, such as when an interface is a LAN interface, with no other routers connected
- To increase security controls, such as preventing unknown rogue routing devices from receiving EIGRP updates

The **passive-interface** router configuration mode command disables the transmission and receipt of EIGRP Hello packets on these interfaces.

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

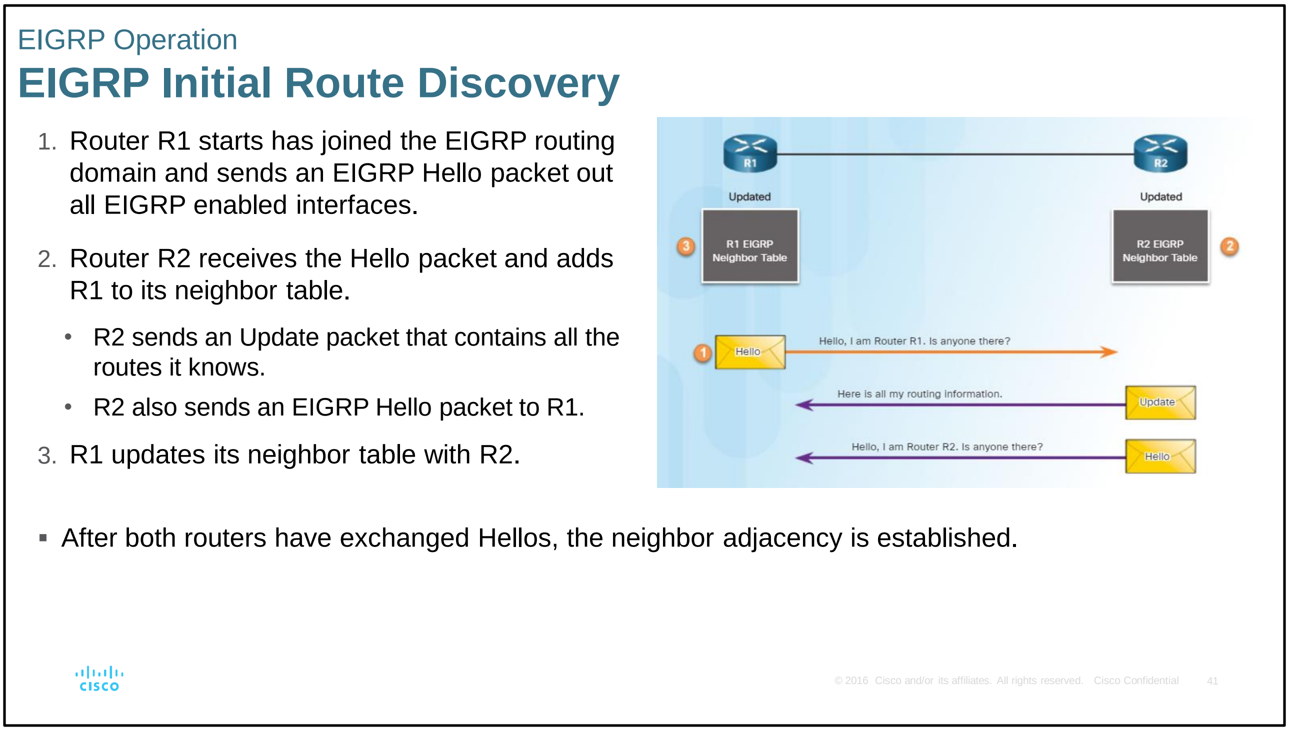
Figure shows the **passive-interface** command configured to suppress Hello packets on the LANs for R3.

Without a neighbor adjacency, EIGRP cannot exchange routes with a neighbor. Therefore, the **passive-interface** command prevents the exchange of routes on the interface. Although EIGRP does not send or receive routing updates on an interface configured with the **passive-interface** command, it still includes the address of the interface in routing updates sent out of other non-passive interfaces.

Note: To configure all interfaces as passive, use the **passive-interface default** command. To disable an interface as passive, use the **no passive-interface** *interface-type interface-number* command.
An example of using the passive interface to increase security controls is when a network must connect to a third-party organization, for which the local administrator has no control, such as when connecting to an ISP network. In this case, the local network administrator would need to advertise the interface link through their own network, but would not want the third-party organization to receive or send routing updates to the local routing device, as this is a security risk.

EIGRP Operation

6 - EIGRP
6.3 – EIGRP Operation



EIGRP Operation

EIGRP Initial Route Discovery

1. Router R1 starts has joined the EIGRP routing domain and sends an EIGRP Hello packet out all EIGRP enabled interfaces.
2. Router R2 receives the Hello packet and adds R1 to its neighbor table.
   - R2 sends an Update packet that contains all the routes it knows.
   - R2 also sends an EIGRP Hello packet to R1.
3. R1 updates its neighbor table with R2.

- After both routers have exchanged Hellos, the neighbor adjacency is established.

R1
R2
Updated
Updated
3
R1 EIGRP Neighbor Table
R2 EIGRP Neighbor Table
2
1
Hello
Hello, I am Router R1. Is anyone there?
Here is all my routing information.
Update
Hello, I am Router R2. Is anyone there?
Hello
cisco

EIGRP Neighbor Adjacency

The goal of any dynamic routing protocol is to learn about remote networks from other routers and to reach convergence in the routing domain. Before any EIGRP update packets can be exchanged between routers, EIGRP must first discover its neighbors. EIGRP neighbors are other routers running EIGRP on directly connected networks.

EIGRP uses Hello packets to establish and maintain neighbor adjacencies. For two EIGRP routers to become neighbors, several parameters between the two routers must match. For example, two EIGRP routers must use the same EIGRP metric parameters and both must be configured using the same autonomous system number.

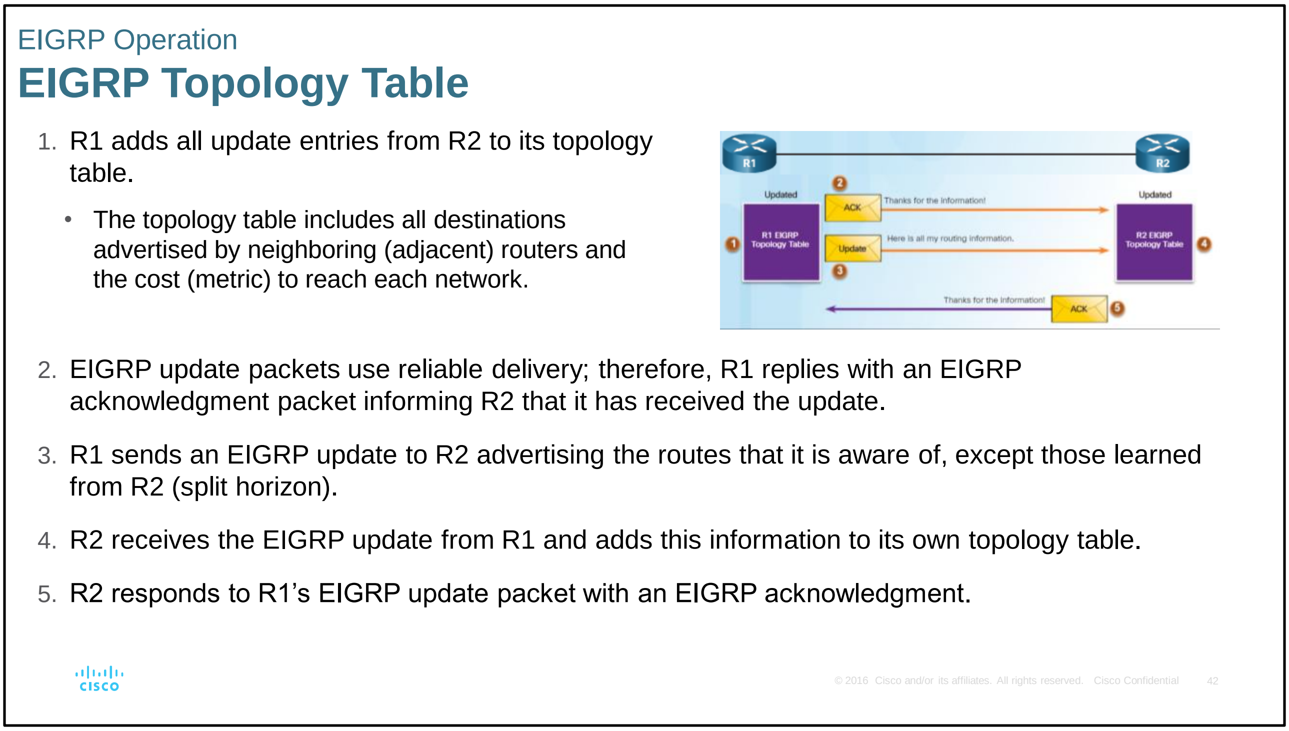
Each EIGRP router maintains a neighbor table, which contains a list of routers on shared links that have an EIGRP adjacency with this router. The neighbor table is used to track the status of these EIGRP neighbors.

The figure shows two EIGRP routers exchanging initial EIGRP Hello packets. When an EIGRP enabled router receives a Hello packet on an interface, it adds that router to its neighbor table.

1. A new router (R1) comes up on the link and sends an EIGRP Hello packet through all of its EIGRP-configured interfaces.

2. Router R2 receives the Hello packet on an EIGRP-enabled interface. R2 replies with an EIGRP update packet that contains all the routes it has in its routing table, except those learned through that interface (split horizon). However, the neighbor adjacency

is not established until R2 also sends an EIGRP Hello packet to R1.
3. After both routers have exchanged Hellos, the neighbor adjacency is established. R1 and R2 update their EIGRP neighbor tables adding the adjacent router as a neighbor.



EIGRP Operation

EIGRP Topology Table

1. R1 adds all update entries from R2 to its topology table.
   - The topology table includes all destinations advertised by neighboring (adjacent) routers and the cost (metric) to reach each network.

R1
R2
Updated
Updated
2
ACK
Thanks for the information!
R1 EIGRP Topology Table
1
Update
Here is all my routing information.
R2 EIGRP Topology Table
4
3
Thanks for the information!
ACK
5

2. EIGRP update packets use reliable delivery; therefore, R1 replies with an EIGRP acknowledgment packet informing R2 that it has received the update.
3. R1 sends an EIGRP update to R2 advertising the routes that it is aware of, except those learned from R2 (split horizon).
4. R2 receives the EIGRP update from R1 and adds this information to its own topology table.
5. R2 responds to R1's EIGRP update packet with an EIGRP acknowledgment.

EIGRP Topology Table

EIGRP updates contain networks that are reachable from the router sending the update. As EIGRP updates are exchanged between neighbors, the receiving router adds these entries to its EIGRP topology table.

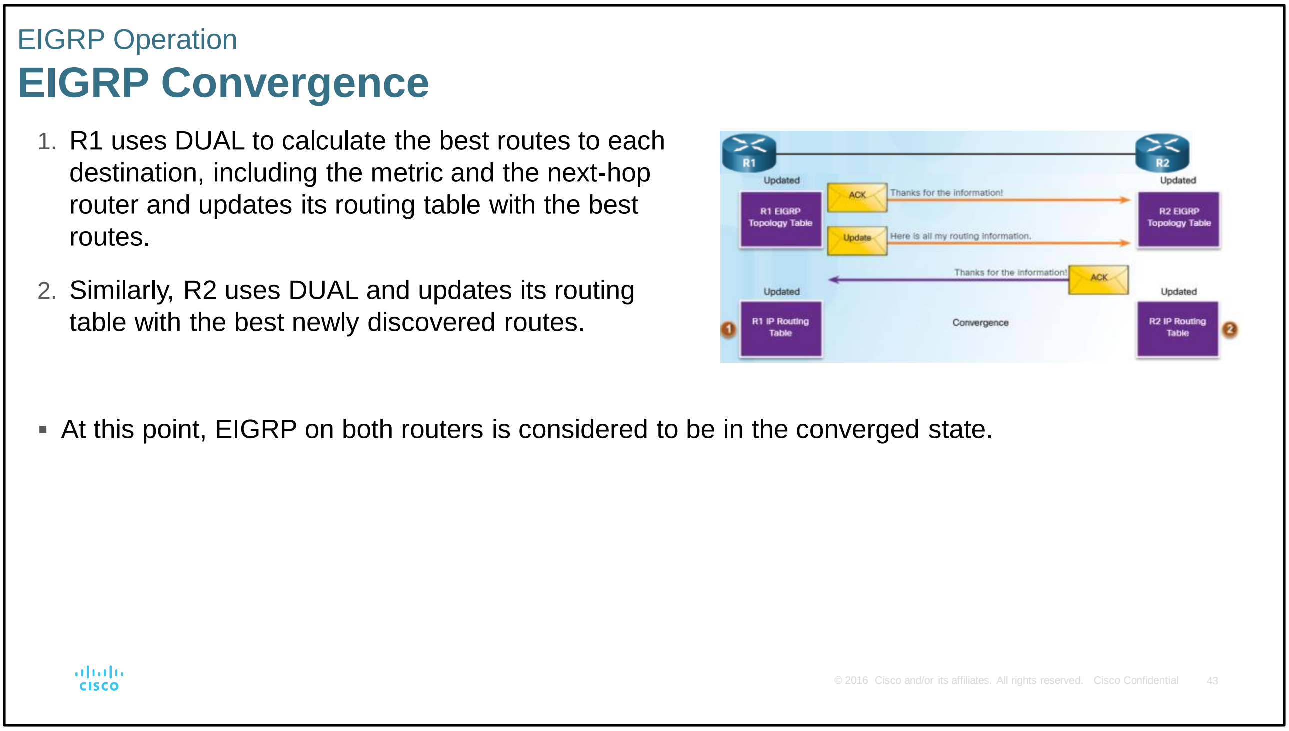
Each EIGRP router maintains a topology table for each routed protocol configured, such as IPv4 and IPv6. The topology table includes route entries for every destination that the router learns from its directly connected EIGRP neighbors.

The figure shows the continuation of the initial route discovery process from the previous page. It now shows the update of the topology table.

When a router receives an EIGRP routing update, it adds the routing information to its EIGRP topology table and replies with an EIGRP acknowledgment.

1. R1 receives the EIGRP update from neighbor R2 that includes information about the routes that the neighbor is advertising, including the metric to each destination. R1 adds all update entries to its topology table. The topology table includes all destinations advertised by neighboring (adjacent) routers and the cost (metric) to reach each network.
2. EIGRP update packets use reliable delivery; therefore, R1 replies with an EIGRP acknowledgment packet informing R2 that it has received the update.
3. R1 sends an EIGRP update to R2 advertising the routes that it is aware of, except those learned from R2 (split horizon).
4. R2 receives the EIGRP update from neighbor R1 and adds this information to its own topology table.

5. R2 responds to R1’s EIGRP update packet with an EIGRP acknowledgment.



EIGRP Operation

EIGRP Convergence

1. R1 uses DUAL to calculate the best routes to each destination, including the metric and the next-hop router and updates its routing table with the best routes.
2. Similarly, R2 uses DUAL and updates its routing table with the best newly discovered routes.

- At this point, EIGRP on both routers is considered to be in the converged state.

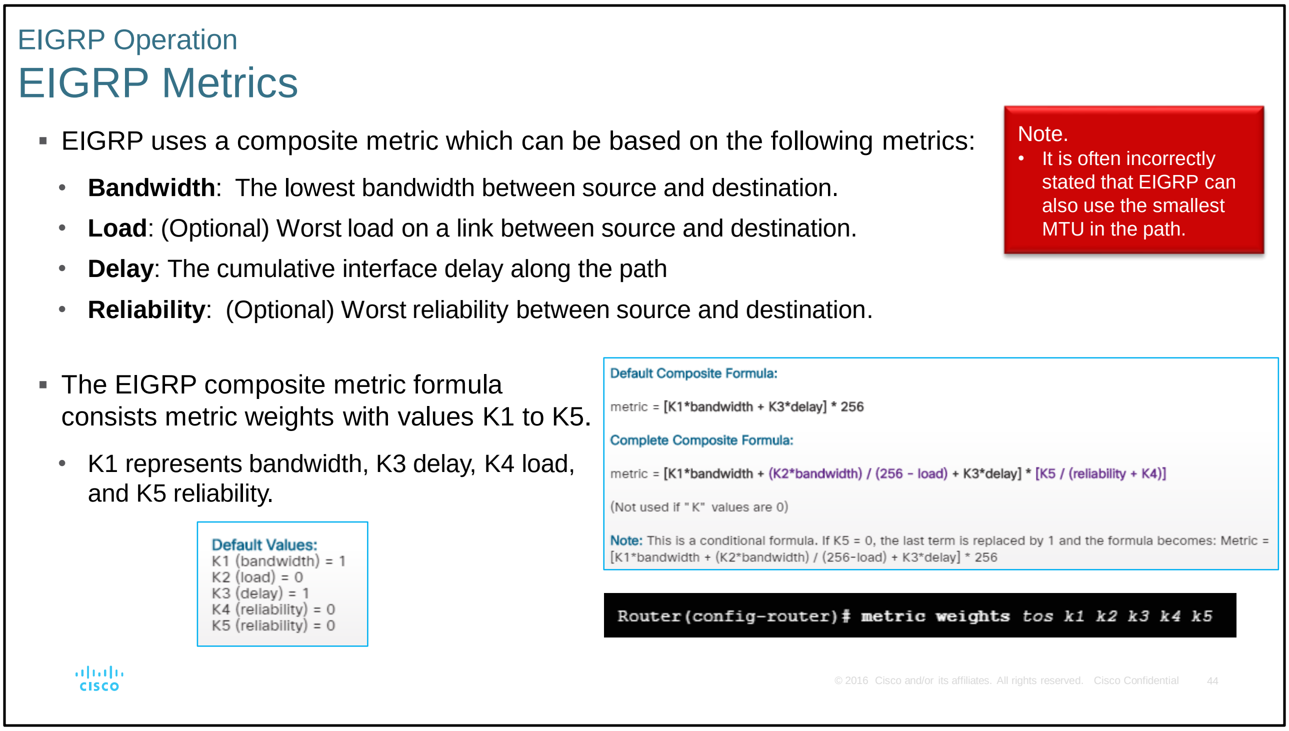
EIGRP Convergence

The figure illustrates the final steps of the initial route discovery process.

1. After receiving the EIGRP update packets from R2, using the information in the topology table, R1 updates its IP routing table with the best path to each destination, including the metric and the next-hop router.

2. Similar to R1, R2 updates its IP routing table with the best path routes to each network.

At this point, EIGRP on both routers is considered to be in the converged state.



EIGRP Operation

EIGRP Metrics

- EIGRP uses a composite metric which can be based on the following metrics:
  - **Bandwidth**: The lowest bandwidth between source and destination.
  - **Load**: (Optional) Worst load on a link between source and destination.
  - **Delay**: The cumulative interface delay along the path
  - **Reliability**: (Optional) Worst reliability between source and destination.

Note.
- It is often incorrectly stated that EIGRP can also use the smallest MTU in the path.

- The EIGRP composite metric formula consists metric weights with values K1 to K5.
  - K1 represents bandwidth, K3 delay, K4 load, and K5 reliability.

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

Default Composite Formula:

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

Complete Composite Formula:

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

(Not used if " K" values are 0)

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

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

44

EIGRP Composite Metric

By default, EIGRP uses the following values in its composite metric to calculate the preferred path to a network:

Bandwidth - The slowest bandwidth among all of the outgoing interfaces, along the path from source to destination.

Delay - The cumulative (sum) of all interface delay along the path (in tens of microseconds).

The following values can be used, but are not recommended, because they typically result in frequent recalculation of the topology table:

Reliability - Represents the worst reliability between the source and destination, which is based on keepalives.

Load - Represents the worst load on a link between the source and destination, which is computed based on the packet rate and the configured bandwidth of the interface.

Note: Although the MTU is included in the routing table updates, it is not a routing metric used by EIGRP.

The Composite Metric

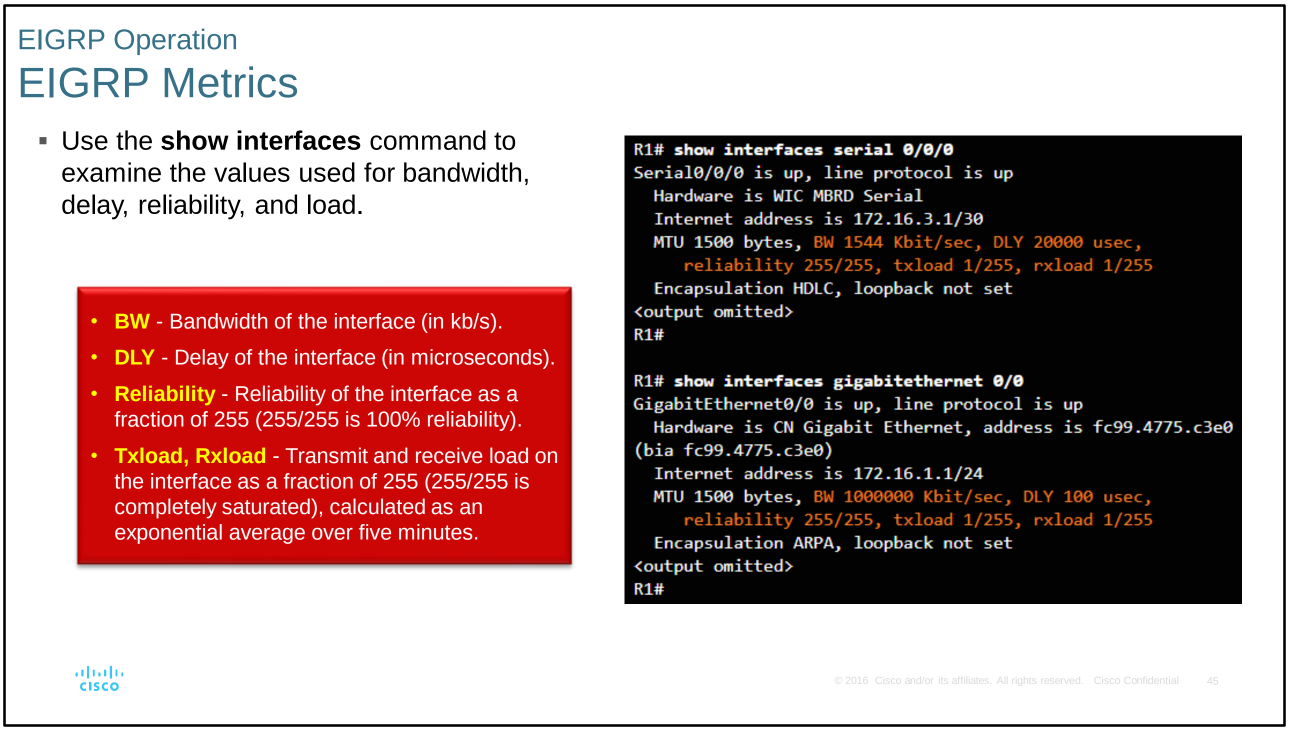
Figure shows the composite metric formula used by EIGRP. The formula consists of values K1 to K5, known as EIGRP metric weights. K1 and K3 represent bandwidth and delay, respectively. K2 represents load, and K4 and K5 represent reliability. By default, K1 and K3 are set to 1, and K2, K4, and K5 are set to 0. The result is that only the

bandwidth and delay values are used in the computation of the default composite metric. EIGRP for IPv4 and EIGRP for IPv6 use the same formula for the composite metric.
The metric calculation method (*k* values) and the EIGRP autonomous system number must match between EIGRP neighbors. If they do not match, the routers do not form an adjacency.
The default *k* values can be changed with the **metric weights** router configuration mode command:

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

Note: Modifying the **metric weights** value is generally not recommended and beyond the scope of this course. However, its relevance is important in establishing neighbor adjacencies. If one router has modified the metric weights and another router has not, an adjacency does not form.

Verifying the *k* Values
The **show ip protocols** command is used to verify the *k* values.



EIGRP Operation

EIGRP Metrics

- Use the **show interfaces** command to examine the values used for bandwidth, delay, reliability, and load.

- **BW** - Bandwidth of the interface (in kb/s).
- **DLY** - Delay of the interface (in microseconds).
- **Reliability** - Reliability of the interface as a fraction of 255 (255/255 is 100% reliability).
- **Txload, Rxload** - Transmit and receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes.

```
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
<output omitted>
R1#

R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<output omitted>
R1#
```

Examining Interface Metric Values

The **show interfaces** command displays interface information, including the parameters used to compute the EIGRP metric. The figure shows the **show interfaces** command for the Serial 0/0/0 interface on R1.

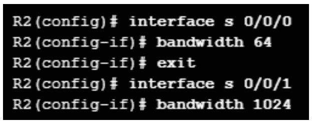
- **BW** - Bandwidth of the interface (in kilobits per second).
- **DLY** - Delay of the interface (in microseconds).
- **Reliability** - Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over five minutes. By default, EIGRP does not include its value in computing its metric.
- **Txload, Rxload** - Transmit and receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over five minutes. By default, EIGRP does not include its value in computing its metric.

Note: Throughout this course, bandwidth is referenced as kb/s. However, router output displays bandwidth using the Kbit/sec abbreviation. Router output also displays delay as usec. In this course, delay is referenced as microseconds.

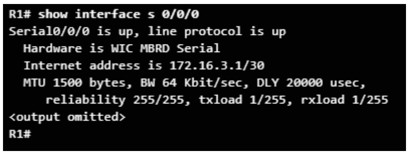
EIGRP Operation

EIGRP Metrics

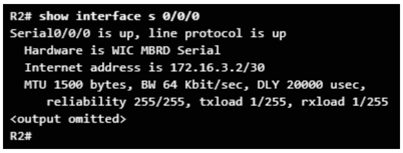
- Use the following interface configuration mode command to modify the bandwidth metric:
  - Router(config-if)# **bandwidth** *kilobits-bandwidth-value*
- Use the **show interfaces** command to verify the new bandwidth parameters.



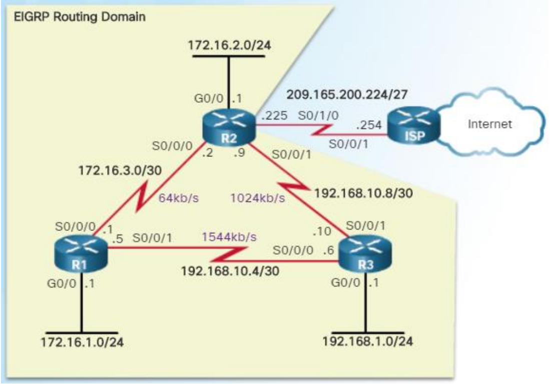
```
R2(config)# interface s 0/0/0
R2(config-if)# bandwidth 64
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# bandwidth 1024
```

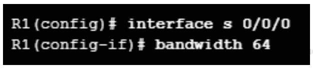


```
R1# show interface s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R1#
```

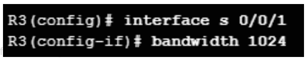


```
R2# show interface s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.2/30
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R2#
```





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



```
R3(config)# interface s 0/0/1
R3(config-if)# bandwidth 1024
```

Bandwidth Metric

The bandwidth metric is a static value used by some routing protocols, such as EIGRP and OSPF, to calculate their routing metric. The bandwidth is displayed in kilobits per second (kb/s).

On older routers, the serial link bandwidth metric defaults to 1544 kb/s. This is the bandwidth of a T1 connection. On newer routers, such as the Cisco 4321, serial link bandwidth defaults to the clock rate used on the link. The serial links in topology have been configured with the bandwidths that will be used in this section.

Note: The bandwidths used in this topology were chosen to help explain the calculation of the routing protocol metrics and the process of best path selection. These bandwidth values do not reflect the more common types of connections found in today's networks.

Always verify bandwidth with the **show interfaces** command. The default value of the bandwidth may or may not reflect the actual physical bandwidth of the interface. If actual bandwidth of the link differs from the default bandwidth value, the bandwidth value should be modified.

Configuring the Bandwidth Parameter

Because both EIGRP and OSPF use bandwidth in default metric calculations, a correct value for bandwidth is very important to the accuracy of routing information.

Use the following interface configuration mode command to modify the bandwidth metric:

Router(config-if)# **bandwidth** *kilobits-bandwidth-value*

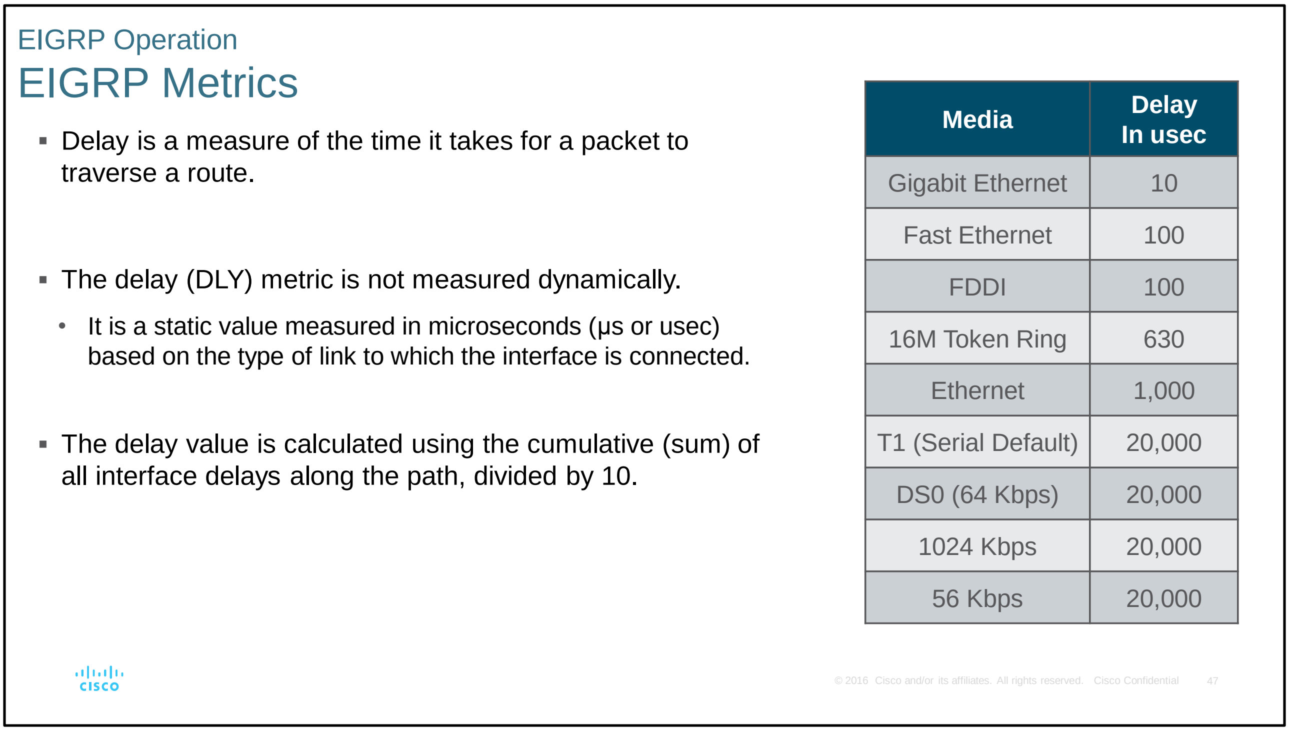
Use the **no bandwidth** command to restore the default value.

In Figure, the link between R1 and R2 has a bandwidth of 64 kb/s, and the link between R2 and R3 has a bandwidth of 1,024 kb/s. The figure shows the configurations used on all three routers to modify the bandwidth on the appropriate serial interfaces. Modify the bandwidth metric on both sides of the link to ensure proper routing in both directions.

Verifying the Bandwidth Parameter

Use the **show interfaces** command to verify the new bandwidth parameters, as shown in Figure.

Modifying the bandwidth value does not change the actual bandwidth of the link. The **bandwidth** command only modifies the bandwidth metric used by routing protocols, such as EIGRP and OSPF.



EIGRP Operation

EIGRP Metrics

- Delay is a measure of the time it takes for a packet to traverse a route.
- The delay (DLY) metric is not measured dynamically.
  - It is a static value measured in microseconds (μs or usec) based on the type of link to which the interface is connected.
- The delay value is calculated using the cumulative (sum) of all interface delays along the path, divided by 10.

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

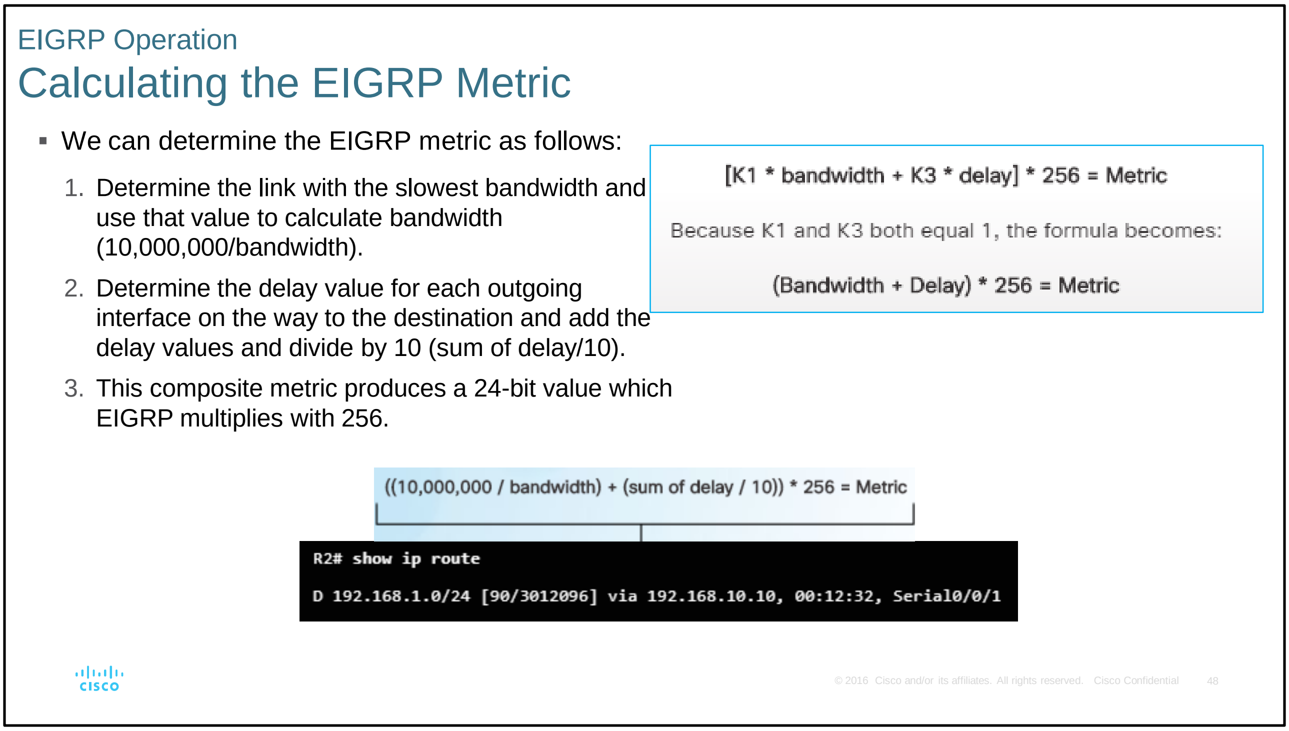
Delay Metric

Delay is the measure of the time it takes for a packet to traverse a route. The delay (DLY) metric is a static value based on the type of link to which the interface is connected and is expressed in microseconds. Delay is not measured dynamically. In other words, the router does not actually track how long packets take to reach the destination. The delay value, much like the bandwidth value, is a default value that can be changed by the network administrator.

When used to determine the EIGRP metric, delay is the cumulative (sum) of all interface delays along the path (measured in tens of microseconds).

The table in Figure shows the default delay values for various interfaces. Notice that the default value is 20,000 microseconds for serial interfaces and 10 microseconds for GigabitEthernet interfaces.

Use the **show interfaces** command to verify the delay value on an interface, as shown in Figure 2. Although an interface with various bandwidths can have the same delay value, by default, Cisco recommends not modifying the delay parameter, unless the network administrator has a specific reason to do so.



EIGRP Operation

Calculating the EIGRP Metric

- We can determine the EIGRP metric as follows:
  1. Determine the link with the slowest bandwidth and use that value to calculate bandwidth (10,000,000/bandwidth).
  2. Determine the delay value for each outgoing interface on the way to the destination and add the delay values and divide by 10 (sum of delay/10).
  3. This composite metric produces a 24-bit value which EIGRP multiplies with 256.

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

Because K1 and K3 both equal 1, the formula becomes:

(Bandwidth + Delay) * 256 = Metric

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

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

How to Calculate the EIGRP Metric

Although EIGRP automatically calculates the routing table metric used to choose the best path, it is important that the network administrator understands how these metrics were determined.

The figure shows the composite metric used by EIGRP. Using the default values for K1 and K3, the calculation can be simplified to the slowest bandwidth (or minimum bandwidth), plus the sum of all of the delays.

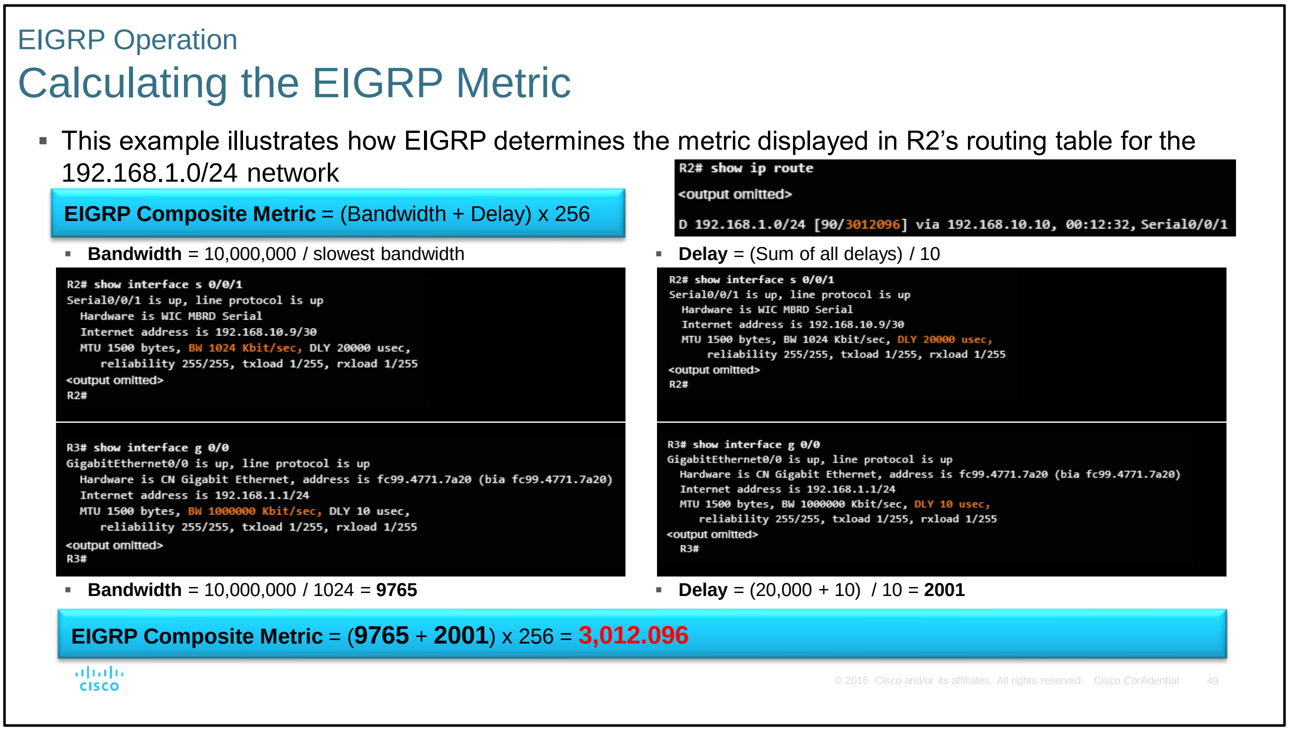
In other words, by examining the bandwidth and delay values for all of the outgoing interfaces of the route, we can determine the EIGRP metric as follows:

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

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

Step 3. This composite metric produces a 24-bit value; however, EIGRP uses a 32-bit value. Multiplying the 24-bit value with 256 extends the composite metric into 32 bits. Therefore, add the computed values for bandwidth and delay, and multiply the sum by 256 to obtain the EIGRP metric.

The routing table output for R2 shows that the route to 192.168.1.0/24 has an EIGRP metric of 3,012,096.



EIGRP Operation

Calculating the EIGRP Metric

- This example illustrates how EIGRP determines the metric displayed in R2's routing table for the 192.168.1.0/24 network

```
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
```

EIGRP Composite Metric = (Bandwidth + Delay) x 256

- **Bandwidth** = 10,000,000 / slowest bandwidth

```
R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R2#
```

```
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20 (bia fc99.4771.7a20)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R3#
```

- **Bandwidth** = 10,000,000 / 1024 = **9765**

- **Delay** = (Sum of all delays) / 10

```
R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R2#
```

```
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20 (bia fc99.4771.7a20)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
  R3#
```

- **Delay** = (20,000 + 10) / 10 = **2001**

EIGRP Composite Metric = (**9765** + **2001**) x 256 = **3,012.096**

CISCO

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 49

Calculating the EIGRP Metric

This example illustrates how EIGRP determines the metric displayed in R2's routing table for the 192.168.1.0/24 network, in the three router topology.

Bandwidth

EIGRP uses the slowest bandwidth in its metric calculation. The slowest bandwidth can be determined by examining each interface between R2 and the destination network 192.168.1.0. The Serial 0/0/1 interface on R2 has a bandwidth of 1,024 kb/s. The GigabitEthernet 0/0 interface on R3 has a bandwidth of 1,000,000 kb/s. Therefore, the slowest bandwidth is 1,024 kb/s and is used in the calculation of the metric.

EIGRP divides a reference bandwidth value of 10,000,000 by the interface bandwidth value in kb/s. This results in higher bandwidth values receiving a lower metric and lower bandwidth values receiving a higher metric. 10,000,000 is divided by 1,024. If the result is not a whole number, then the value is rounded down. In this case, 10,000,000 divided by 1,024 equals 9,765.625. The .625 is dropped to yield 9,765 for the bandwidth portion of the composite metric, as shown in Figure.

Delay

The same outgoing interfaces are used to determine the delay value.

EIGRP uses the sum of all delays to the destination. The Serial 0/0/1 interface on R2 has a delay of 20,000 microseconds. The Gigabit 0/0 interface on R3 has a delay of 10 microseconds. The sum of these delays is divided by 10. In the example, (20,000+10)/10 results in a value of 2,001 for the delay portion of the composite metric.

Calculate Metric

Use the calculated values for bandwidth and delay in the metric formula. This results in a metric of 3,012,096. This value matches the value shown in the routing table for R2.