This chapter covers the following subjects:

- RIPv1
- RIPv2
- IGRP
- EIGRP

CHAPTER 12

RIP, IGRP, and EIGRP Characteristics and Design

This chapter reviews distance-vector routing protocols. It covers both versions of the Routing Information Protocol (RIP). It also discusses the Cisco Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP). The CCDA should understand the capabilities and constraints of each routing protocol.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you need to read the entire chapter. If you intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 8-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 12-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 12-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
RIPv1	1, 2, 5
RIPv2	1, 3, 7
IGRP	5
EIGRP	4, 6, 7, 8

CAUTION The goal of self assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or you are only partially sure of the answer, you should mark this question wrong for purposes of the self assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which protocol should you select if the network diameter is more than 17 hops?
   a. RIPv1
   b. RIPv2
   c. EIGRP
   d. Answers a and b
   e. Answers b and c
   f. Answers a, b, and c

2. How often does a RIPv1 router broadcast its routing table by default?
   a. Every 30 seconds.
   b. Every 60 seconds.
   c. Every 90 seconds.
   d. RIPv1 does not broadcast periodically.

3. RIPv2 improves RIPv1 with which of the following capabilities?
   a. Multicast updates, authentication, hop count
   b. Multicast updates, authentication, variable-length subnet mask (VLSM)
   c. Authentication, VLSM, hop count
   d. Multicast updates, hop count

4. Which protocol maintains neighbor adjacencies?
   a. RIPv2 and EIGRP
   b. IGRP and EIGRP
   c. RIPv2
   d. EIGRP

5. Which pair of routing protocols does not support VLSM or classless interdomain routing (CIDR)?
   a. EIGRP and IGRP
   b. RIPv1 and RIPv2
   c. RIPv1 and IGRP
   d. Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF)

6. Which parameters does the computation of the EIGRP composite metric use by default?
   a. Bandwidth and load
   b. Bandwidth and delay
   c. Bandwidth and reliability
   d. Bandwidth and maximum transmission unit (MTU)

7. Which protocols support VLSM?
   a. RIPv1 and RIPv2
   b. EIGRP and IGRP
   c. RIPv1 and IGRP
   d. RIPv2 and EIGRP

8. Which routing protocol implements the diffusing update algorithm (DUAL)?
   a. IS-IS
   b. IGRP
   c. EIGRP
   d. OSPF

The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to Chapter 'Do I Know This Already?' Quizzes and Q&A sections." The suggested choices for your next step are as follows:

- **6 or less overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **7–8 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

"Foundation Topics" covers the characteristics of the distance-vector routing protocols that the CCDA might choose from in a network design. *RIPv1* is a routing protocol developed in the late 1980s; it was the only interior gateway protocol (IGP) at that time. *RIPv2* provides enhancements to RIP, such as support for VLSMs.

The *IGRP* is an IGP developed by Cisco in the early 1990s that was not limited to the 15 router-hop constraint in RIP. EIGRP is a hybrid routing protocol that uses distance-vector metrics and link-state routing protocol characteristics.

RIPv1

RFC 1058 from June 1988 defines RIPv1. RIP is a distance-vector routing protocol that uses router hop count as the metric. RIP is a classful routing protocol that does not support VLSMs or CIDR.

There is no method for authenticating route updates. A RIP router sends a copy of its routing table to its neighbors every 30 seconds. RIP uses split horizon with poison reverse; therefore, route updates are sent out an interface with an infinite metric for routes learned (received) from the same interface.

The RIP standard was based on the popular **routed** program used in UNIX systems since the 1980s. The Cisco implementation of RIP adds support for load balancing. RIP will load-balance traffic if there are several paths with the same metric (equal-cost load balancing) to a destination. Also, RIP sends triggered updates when the metric of a route changes. Triggered updates can help the network converge faster rather than wait for the periodic update. RIP has an administrative distance of 120. Chapter 11, "Routing Protocol Selection Criteria," covers administrative distance.

RIP summarizes to IP network values at network boundaries. A network boundary occurs at a router that has one or more interfaces that do not participate in the specified IP network. The IP address assigned to the interface determines participation. IP class determines the network value. For example, an IP network that uses 24-bit subnetworks from 180.100.50.0/24 to 180.100.120.0/24 is summarized to 180.100.0.0/16 at a network boundary.

RIPv1 Forwarding Information Base

The RIPv1 protocol keeps the following information about each destination:

- **IP address**—IP address of the destination host or network
- **Gateway**—The first gateway along the path to the destination

- **Interface**—The physical network that must be used to reach the destination
- **Metric**—A number indicating the number of hops to the destination
- **Timer**—The amount of time since the entry was last updated

The database is updated with the route updates received from neighboring routers. As shown in Example 12-1, the **show ip rip database** command shows the RIP private database of a router.

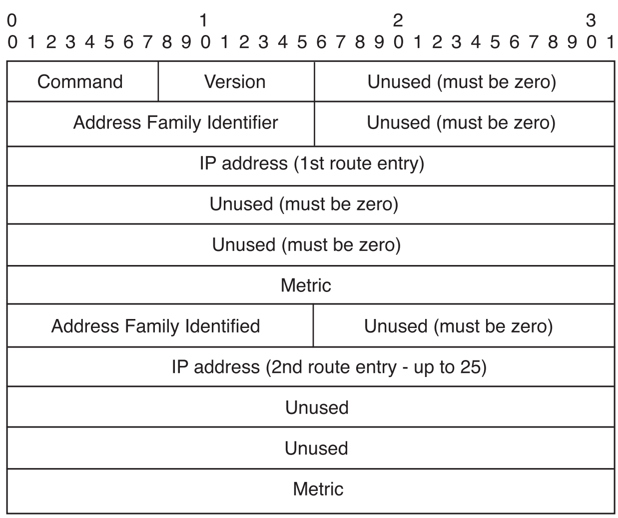
Example 12-1 **show ip rip database** *Command*

```
router9# show ip rip database
172.16.0.0/16    auto-summary
172.16.1.0/24    directly connected, Ethernet0
172.16.2.0/24
    [1] via 172.16.4.2, 00:00:06, Serial0
172.16.3.0/24
    [1] via 172.16.1.2, 00:00:02, Ethernet0
172.16.4.0/24    directly connected, Serial0
```

RIPv1 Message Format

As described in RFC 1058, the RIPv1 message format appears in Figure 12-1. The RIP messages are encapsulated using User Datagram Protocol (UDP). RIP uses the well-known UDP port 520.

Figure 12-1 *RIPv1 Message Format*



The following is a description of each field:

- **Command**—Describes the purpose of the packet. The RFC describes five commands, two of which are obsolete and one of which is reserved. The two used commands are
  - **request**—Requests all or part of the responding router's routing table.
  - **response**—Contains all or part of the sender's routing table. This message might be a response to a request, or it might be an update message generated by the sender.
- **Version**—Set to the value of 1 for RIPv1.
- **Address Family Identifier (AFI)**—Set to a value of 2 for IP.
- **IP address**—The destination route. It might be a network address, subnet, or host route. Special route 0.0.0.0 is used for the default route.
- **Metric**—A field that is 32 bits in length. It contains a value between 1 and 15 inclusive, specifying the current metric for the destination. The metric is set to 16 to indicate that a destination is not reachable.

Because RIP has a maximum hop count, it implements counting to infinity. For RIP, infinity is 16 hops. Notice in the RIP message that there are no subnet masks accompanying each route. Five 32-bit words are repeated for each route entry: AFI (16 bits); unused, which is 0 (16 bits); IP address; two more 32-bit unused fields; and the 32-bit metric. Five 32-bit words equals 20 bytes for each route entry. Up to 25 routes are allowed in each RIP message. The maximum datagram size is limited to 512 bytes, not including the IP header. Calculating 25 routes by 20 bytes each, plus the RIP header (4 bytes), plus an 8-byte UDP header, you get 512 bytes.

RIPv1 Timers

The Cisco implementation of RIP uses four timers:

- Update
- Invalid
- Flush
- Holddown

RIP sends its full routing table out all configured interfaces. The table is sent periodically as a broadcast (255.255.255.255) to all hosts.

Update Timer

The update timer specifies the frequency of the periodic broadcasts. By default, the update timer is set to 30 seconds. Each route has a timeout value associated with it. The timeout gets reset every time the router receives a routing update containing the route.

Invalid Timer

When the timeout value expires, the route is marked as unreachable because it is marked invalid. The router marks the route invalid by setting the metric to 16. The route is retained in the routing table. By default, the invalid timer is 180 seconds, or six updates periods (30 x 6 = 180).

Flush Timer

A route entry marked as invalid is retained in the routing table until the flush timer expires. By default, the flush timer is 240 seconds, which is 60 seconds longer than the invalid timer.

Holddown Timer

Cisco implements an additional timer for RIP, the holddown timer. The holddown timer stabilizes routes by setting an allowed time for which routing information regarding different paths is suppressed. After the metric for a route entry changes, the router accepts no updates for the route until the holddown timer expires. By default, the holddown timer is 180 seconds.

The output of the show ip protocol command, as shown in Example 12-2, shows the timers for RIP, unchanged from the defaults.

Example 12-2 *RIP Timers Verified with* **show ip protocol**

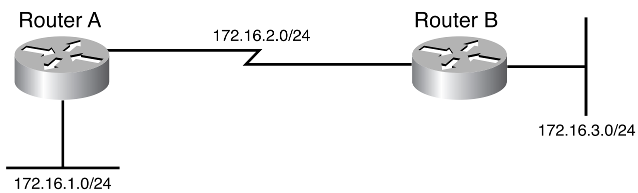
```
router9> show ip protocol
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 3 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    Ethernet0             1     1 2
    Serial0               1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    172.16.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.4.2           120      00:00:00
    172.16.1.2           120      00:00:07
  Distance: (default is 120)
```

RIPv1 Design

Things to remember in designing a network with RIPv1 include that it does not support VLSM and CIDR. The IP addressing scheme with RIPv1 requires the same subnet mask for the entire IP network, a flat IP network. RIPv1 is limited to 15 hops; therefore, the network diameter cannot exceed this limit. RIPv1 also broadcasts its routing table every 30 seconds. RIPv1 is usually limited to accessing networks where it can interoperate with servers running **routed** or with non-Cisco routers. RIP also appears at the edge of larger networks.

As shown in Figure 12-2, when you use RIPv1, all segments must have the same subnet mask.

Figure 12-2 *RIPv1 Design*



RIPv1 Summary

The characteristics of RIPv1 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classful protocol (no support for VLSM or CIDR).
- Metric is router hop count.
- Maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast every 30 seconds.
- 25 routes per RIP message.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks.

RIPv2

RIPv2 was first described in RFC 1388 and RFC 1723 (1994); the current RFC is 2453, written in November 1998. Although current environments use advanced routing protocols such as OSPF and EIGRP, there still are networks using RIP. The need to use VLSMs and other requirements prompted the definition of RIPv2.

RIPv2 improves upon RIPv1 with the ability to use VLSM, with support for route authentication, and with multicasting of route updates. RIPv2 supports CIDR. It still sends updates every 30 seconds and retains the 15-hop limit; it also uses triggered updates. RIPv2 still uses UDP port 520; the RIP process is responsible for checking the version number. It retains the loop-prevention strategies of poison reverse and counting to infinity. On Cisco routers, RIPv2 has the same administrative distance as RIPv1, which is 120. Finally, RIPv2 uses the IP address 224.0.0.9 when multicasting route updates to other RIP routers. As in RIPv1, RIPv2 will, by default, summarize IP networks at network boundaries. You can disable autosummarization if required.

You can use RIPv2 in small networks where VLSM is required. It also works at the edge of larger networks.

Authentication

Authentication can prevent communication with any RIP routers that are not intended to be part of the network, such as UNIX stations running **routed**. Only RIP updates with the authentication password are accepted. RFC 1723 defines simple plain-text authentication for RIPv2.

MD5 Authentication

In addition to plain-text passwords, the Cisco implementation provides the ability to use Message Digest 5 (MD5) authentication, which is defined in RFC 1321. Its algorithm takes as input a message of arbitrary length and produces as output a 128-bit fingerprint or message digest of the input, making it much more secure than plain-text passwords.

RIPv2 Forwarding Information Base

RIPv2 maintains a routing table database as in Version 1. The difference is that it also keeps the subnet mask information. The following list repeats the table information of RIPv1:

- **IP address**—IP address of the destination host or network, with subnet mask
- **Gateway**—The first gateway along the path to the destination
- **Interface**—The physical network that must be used to reach the destination
- **Metric**—A number indicating the number of hops to the destination
- **Timer**—The amount of time since the route entry was last updated

RIPv2 Message Format

The RIPv2 message format takes advantage of the unused fields in the RIPv1 message format by adding subnet masks and other information. Figure 12-3 shows the RIPv2 message format.

Figure 12-3 *RIPv2 Message Format*

0 1 2 3 (bit positions 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1)

Command	Version	Unused (must be zero)
Address Family Identifier		Route Tag
IP address (1st route entry)		
Subnet Mask		
Next Hop		
Metric		
Address Family Identified		Route Tag
IP address (2nd route entry - up to 25)		
Subnet Mask		
Next Hop		
Metric		

The following is a description of each field:

- **Command**—Indicates whether the packet is a request or a response message. The request message asks that a router send all or a part of its routing table. Response messages contain route entries. The router sends the response periodically or as a reply to a request.
- **Version**—Specifies the RIP version used. It is set to 2 for RIPv2 and set to 1 for RIPv1.
- **AFI**—Specifies the address family used. RIP is designed to carry routing information for several different protocols. Each entry has an AFI to indicate the type of address specified. The AFI for IP is 2. The AFI is set to 0xFFF for the first entry to indicate that the remainder of the entry contains authentication information.
- **Route tag**—Provides a method for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols). You can add this optional attribute during the redistribution of routing protocols.
- **IP address**—Specifies the IP address (network) of the destination.
- **Subnet mask**—Contains the subnet mask for the destination. If this field is 0, no subnet mask has been specified for the entry.

- **Next hop**—Indicates the IP address of the next hop where packets are sent to reach the destination.
- **Metric**—Indicates how many router hops to reach the destination. The metric is between 1 and 15 for a valid route or 16 for an unreachable or infinite route.

Again, as in Version 1, the router permits up to 25 occurrences of the last five 32-bit words (20 bytes) for up to 25 routes per RIP message. If the AFI specifies an authenticated message, the router can specify only 24 routing-table entries. The updates are sent to the multicast address of 224.0.0.9.

RIPv2 Timers

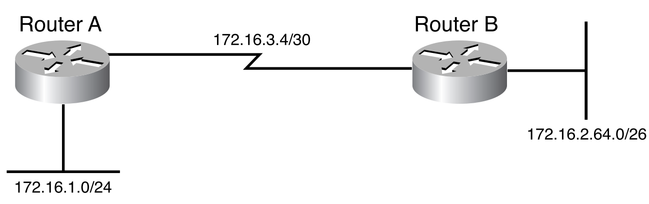
RIPv2 timers are the same as in Version 1. They send periodic updates every 30 seconds. The default invalid timer is 180 seconds, the holddown timer is 180 seconds, and the flush timer is 240 seconds. You can write this list as 30/180/180/240 representing the U/I/H/F timers.

RIPv2 Design

Things to remember in designing a network with RIPv2 include that it supports VLSM within networks and CIDR for network summarization across adjacent networks. RIPv2 allows for the summarization of routes in a hierarchical network. RIPv2 is still limited to 16 hops; therefore, the network diameter cannot exceed this limit. RIPv2 multicasts its routing table every 30 seconds to the multicast IP address 224.0.0.9. RIPv2 is usually limited to accessing networks where it can interoperate with servers running **routed** or with non-Cisco routers. RIPv2 also appears at the edge of larger internetworks. RIPv2 further provides for route authentication.

As shown in Figure 12-4, when you use RIPv2, all segments can have different subnet masks.

Figure 12-4 *RIPv2 Design*



RIPv2 Summary

The characteristics of RIPv2 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classless protocol (support for CIDR).

- Supports VLSMs.
- Metric is router hop count.
- Maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates sent every 30 seconds to multicast address 224.0.0.9.
- 25 routes per RIP message (24 if you use authentication).
- Supports authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Subnet mask included in route entry.
- Administrative distance for RIPv2 is 120.
- Used in small, flat networks or at the edge of larger networks.

IGRP

Cisco Systems developed the IGRP to overcome the limitations of RIPv1. IGRP is a distance-vector routing protocol that considers a composite metric which, by default, uses bandwidth and delay as parameters instead of hop count. IGRP is not limited to the 15-hop limit of RIP. IGRP has a maximum hop limit of 100, by default, and can be configured to support a network diameter of 255.

With IGRP, routers usually select paths with a larger minimum-link bandwidth over paths with a smaller hop count. Links do not have a hop count. They are exactly one hop.

IGRP is a classful protocol and cannot implement VLSM or CIDR. IGRP summarizes at network boundaries. As in RIP, IGRP implements split horizon with poison reverse, triggered updates, and holddown timers for stability and loop prevention. Another benefit of IGRP is that it can load-balance over unequal-cost links. As a routing protocol developed by Cisco, IGRP is available only on Cisco routers.

By default, IGRP will load-balance traffic if there are several paths with equal cost to the destination. IGRP will do unequal-cost load balancing if configured with the **variance** command.

IGRP Timers

IGRP sends its routing table to its neighbors every 90 seconds. IGRP's default update period of 90 seconds is a benefit compared to RIP, which can consume excessive bandwidth when sending updates every 30 seconds. IGRP uses an invalid timer to mark a route as invalid after 270 seconds (three times the update timer). As with RIP, IGRP uses a flush timer to remove a route from the routing table; the default flush timer is set to 630 seconds (seven times the update period and more than 10 minutes).

If a network goes down or the metric for the network increases, the route is placed in holddown. The router accepts no new changes for the route until the holddown timer expires. This setup prevents routing loops in the network. The default holddown timer is 280 seconds (three times the update timer plus 10 seconds). Table 12-2 summarizes the default settings for IGRP timers.

Table 12-2 *IGRP Timers*

IGRP Timer	Default Time
Update	90 seconds
Invalid	270 seconds
Holddown	280 seconds
Flush	630 seconds

IGRP Metrics

IGRP uses a composite metric based on bandwidth, delay, load, and reliability. Chapter 11 discussed these metrics. By default, IGRP uses bandwidth and delay to calculate the composite metric, as follows:

$$IGRP_{metric} = \{k1 \text{ x } BW + [(k2 \text{ x } BW)/(256 - load)] + k3 \text{ x } delay\} \text{ x } \{k5/(reliability + k4)\}$$

In this formula, BW uses the lowest interface bandwidth in the path, and delay is the sum of all outbound interface delays in the path. The router dynamically measures reliability and load. The values of reliability and load used in the metric computation range from 1 to 255. Cisco IOS routers display a 100 percent reliability as 255/255. They also display load as a fraction of 255. They display an interface with no load as 1/255. By default, k1 and k3 are set to 1, and k2, k4, and k5 are set to 0. With the default values, the metric becomes

$$IGRP_{metric} = \{1 \text{ x } BW + [(0 \text{ x } BW)/(256 - load)] + 1 \text{ x } delay\} \text{ x } \{0/(reliability + 0)\}$$
$$IGRP_{metric} = BW + delay$$

The BW is 10,000,000 divided by the smallest of all the bandwidths (in kbps) from outgoing interfaces to the destination. To find delay, add all the delays (in microseconds) from the outgoing interfaces to the destination and divide this number by 10. (The delay is in 10s of microseconds.)

Example 12-3 shows the output interfaces of two routers. For a source host to reach network 172.16.2.0, a path takes the serial link and then the Ethernet interface. The bandwidths are 10,000 and 1544; the slowest bandwidth is 1544. The sum of delays is 20000 + 1000 = 21000.

Example 12-3 show interface

```
RouterA> show interface serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 172.16.4.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255

RouterB> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0010.7b80.bad5 (bia 0010.7b80.bad5)
  Internet address is 172.16.2.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

The IGRP metric is calculated as follows:

$$IGRP_{metric} = (10{,}000{,}000/1544) + (20000 + 1000)/10$$
$$IGRP_{metric} = 6476 + 2100 = 8576$$

You can change the default metrics using the **metric weight** *tos k1 k2 k3 k4 k5* subcommand under **router igrp**. Cisco once intended to implement the tos field as a specialized service in IGRP; it was not implemented so the value of tos is always 0. The *k* arguments are the k values used to build the composite metric. For example, if you want to use all metrics, the command is as follows:

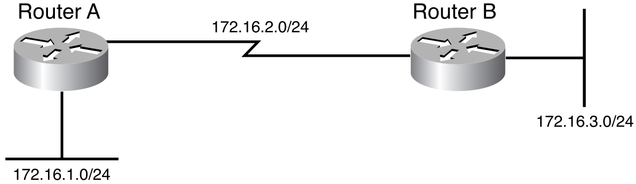
```
router igrp n
 metric weight 0 1 1 1 1 1
```

IGRP Design

Something to remember when designing a network with IGRP is that it does not support VLSMs. The IP addressing scheme with IGRP requires the same subnet mask for the entire IP network, a flat IP network. IGRP does not support CIDR and network summarization within the major network boundary. IGRP is not limited to a maximum of 15 hops as RIP is; therefore, the network diameter can be larger than that of networks using RIP. IGRP also broadcasts its routing table every 90 seconds, which produces less network overhead than RIP. IGRP is limited to Cisco-only networks. EIGRP is recommended over IGRP.

As shown in Figure 12-5, when you use IGRP, all segments must have the same subnet mask.

Figure 12-5 *IGRP Design*



IGRP Summary

The characteristics of IGRP follow:

- Distance-vector protocol.
- Uses IP protocol 9.
- Classful protocol (no support for CIDR).
- No support for VLSMs.
- Composite metric using bandwidth and delay by default.
- You can include load and reliability in the metric.
- Route updates sent every 90 seconds.
- 104 routes per IGRP message.
- Hop count limited to 100 by default, configurable to up to 255.
- No support for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- By default, equal-cost load balancing. Unequal-cost load-balancing with the **variance** command.
- Administrative distance is 100.
- Previously used in large networks; now replaced by EIGRP.

EIGRP

Cisco Systems released EIGRP in the early 1990s as an evolution of IGRP toward a more scalable routing protocol for large internetworks. EIGRP is a classless protocol that permits the use of VLSMs and that supports CIDR for the scalable allocation of IP addresses. EIGRP does not send routing updates periodically, as does IGRP. EIGRP allows for authentication with simple passwords or with MD5. EIGRP autosummarizes networks at network borders and can load-balance over unequal–cost paths. Packets using EIGRP use IP protocol 88. Only Cisco routers can use EIGRP.

EIGRP is an advanced distance-vector protocol that implements some characteristics similar to those of link-state protocols. Some Cisco documentation refers to EIGRP as a hybrid protocol. EIGRP advertises its routing table to its neighbors as distance-vector protocols do, but it uses hellos and forms neighbor relationships as link-state protocols do. EIGRP sends partial updates when a metric or the topology changes on the network. It does not send full routing-table updates in periodic fashion as do distance-vector protocols. EIGRP uses DUAL to determine loop-free paths to destinations. This section discusses DUAL.

By default, EIGRP load-balances traffic if there are several paths with equal cost to the destination. EIGRP performs unequal-cost load balancing if you configure it with the **variance** <*n*> command. EIGRP includes routes that are equal to or less that *n* times the minimum metric route to a destination. As in RIP and IGRP, EIGRP also summarizes IP networks at network boundaries.

EIGRP internal routes have an administrative distance of 90. EIGRP summary routes have an administrative distance of 5, and EIGRP external routes (from redistribution) have an administrative distance of 170.

EIGRP Components

EIGRP has four components that characterize it:

- Protocol-dependent modules
- Neighbor discovery and recovery
- Reliable Transport Protocol (RTP)
- DUAL

Know the role of the EIGRP components, which are described in the following sections.

Protocol-Dependent Modules

EIGRP uses different modules that independently support IP, Internetwork Packet Exchange (IPX), and AppleTalk routed protocols. These modules are the logical interface between DUAL and routing protocols such as IPX RIP, AppleTalk Routing Table Maintenance Protocol (RTMP), and IGRP. The EIGRP module sends and receives packets but passes received information to DUAL, which makes routing decisions.

EIGRP automatically redistributes with IGRP if you configure both protocols with the same autonomous system number. When configured to support IPX, EIGRP communicates with the IPX RIP and forwards the route information to DUAL to select the best paths. AppleTalk EIGRP automatically redistributes routes with AppleTalk RTMP to support AppleTalk networks. AppleTalk is not a CCDA objective and is not covered in this book.

Neighbor Discovery and Recovery

EIGRP discovers and maintains information about its neighbors. It multicasts hello packets (224.0.0.10) every 5 seconds for most networks. The router builds a table with EIGRP neighbor information. The holdtime to maintain a neighbor is three times the hello time: 15 seconds. If the router does not receive a hello in 15 seconds, it removes the neighbor from the table. EIGRP multicasts hellos every 60 seconds on multipoint WAN interfaces (X.25, Frame Relay, ATM) with speeds less than 1544 Mbps, inclusive. The neighbor holdtime is 180 seconds on these types of interfaces. To summarize, hello/holdtime timers are 5/15 seconds for high-speed links and 60/180 seconds for low-speed links.

Example 12-4 shows an EIGRP neighbor database. The table lists the neighbor's IP address, the interface to reach it, the neighbor holdtime timer, and the uptime.

Example 12-4 *EIGRP Neighbor Database*

```
Router# show ip eigrp neighbor
IP-EIGRP neighbors for process 100
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
1   172.17.1.1              Se0           11 00:11:27   16   200  0  2
0   172.17.2.1              Et0           12 00:16:11   22   200  0  3
```

RTP

EIGRP uses RTP to manage EIGRP packets. RTP ensures the reliable delivery of route updates and also uses sequence numbers to ensure ordered delivery. It sends update packets using multicast address 224.0.0.10. It acknowledges updates using unicast hello packets with no data.

DUAL

EIGRP implements DUAL to select paths and guarantee freedom from routing loops. J.J. Garcia Luna-Aceves developed DUAL, which is mathematically proven to result in a loop-free topology, providing no need for periodic updates or route-holddown mechanisms that make convergence slower.

DUAL selects a best path and a second best path to reach a destination. The best path selected by DUAL is the *successor*, and the second best path (if available) is the *feasible successor*. The feasible distance is the lowest calculated metric of a path to reach the destination. The topology table in Example 12-5 shows the feasible distance. The example also shows two paths (Ethernet 0 and Ethernet 1) to reach 172.16.4.0/30. Because the paths have different metrics, DUAL chooses only one successor.

Example 12-5 *Feasible Distance as Shown in the EIGRP Topology Table*

```
Router8# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(172.16.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.4.0/30, 1 successors, FD is 2195456
         via 172.16.1.1 (2195456/2169856), Ethernet0
         via 172.16.5.1 (2376193/2348271), Ethernet1
P 172.16.1.0/24, 1 successors, FD is 281600
         via Connected, Ethernet0
```

The route entries in Example 12-5 are marked **P** as in the “passive” state. A destination is in passive state when the router is not performing any recomputations for the entry. If the successor goes down and the route entry has feasible successors, the router does not need to perform any recomputations and does not go into active state.

DUAL places the route entry for a destination into active state if the successor goes down and there are no feasible successors. EIGRP routers send query packets to neighboring routers to find a feasible successor to the destination. A neighboring router can send a reply packet that indicates it has a feasible successor or a query packet. The query packet indicates that the neighboring router does not have a feasible successor and will participate in the recomputation. A route does not return to passive state until it has received a reply packet from each neighboring router. If the router does not receive all the replies before the “active-time” timer expires, DUAL declares the route as stuck-in-active (SIA). The default active timer is 3 minutes.

EIGRP Timers

EIGRP sets updates only when necessary and sends them only to neighboring routers. There is no periodic update timer.

EIGRP uses hello packets to learn of neighboring routers. On high-speed networks, the default hello packet interval is 5 seconds. On multipoint networks with link speeds of T1 and slower, hello packets are unicast every 60 seconds.

The holdtime to maintain a neighbor adjacency is three times the hello time: 15 seconds. If a router does not receive a hello within the holdtime, it removes the neighbor from the table. Hellos are multicast every 60 seconds on multipoint WAN interfaces (X.25, Frame Relay, ATM) with speeds less than 1544 Mbps, inclusive. The neighbor holdtime is 180 seconds on these types of interfaces. To summarize, hello/holdtime timers are 5/15 seconds for high-speed links and 60/180 seconds for multipoint WAN links less than 1544 Mbps, inclusive.

NOTE EIGRP does not send updates using a broadcast address; instead, it sends them to the multicast address 224.0.0.10 (all EIGRP routers).

EIGRP Metrics

EIGRP uses the same composite metric as IGRP, but the BW term is multiplied by 256 for finer granularity. The composite metric is based on bandwidth, delay, load, and reliability. MTU is not an attribute for calculating the composite metric.

EIGRP calculates the composite metric with the following formula:

$$EIGRP_{metric} = \{k1 \text{ x } BW + [(k2 \text{ x } BW)/(256 - load)] + k3 \text{ x } delay\} \text{ x } \{k5/(reliability + k4)\}$$

In this formula, BW is the lowest interface bandwidth in the path, and delay is the sum of all outbound interface delays in the path. The router dynamically measures reliability and load. It expresses a 100 percent reliability as 255/255. It expresses load as a fraction of 255. An interface with no load is represented as 1/255.

Bandwidth is the inverse minimum bandwidth (in kbps) of the path in bits per second scaled by a factor of 256 x 10^7. The formula for bandwidth is

$$(256 \text{ x } 10^7)/BW_{min}$$

The delay is the sum of the outgoing interface delays (in microseconds) to the destination. A delay of all 1s (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable. The formula for delay is

$$[\text{sum of delays}] \text{ x } 256$$

Reliability is a value between 1 and 255. Cisco IOS routers display reliability as a fraction of 255. That is, 255/255 is 100 percent reliability or a perfectly stable link; a value of 229/255 represents a 90 percent reliable link.

Load is a value between 1 and 255. A load of 255/255 indicates a completely saturated link. A load of 127/255 represents a 50 percent saturated link.

By default, k1=k3=1 and k2=k4=k5=0. The default composite metric, adjusted for scaling factors, for EIGRP is

$$EIGRP_{metric} = 256 \times \{ [10^7/BW_{min}] + [sum\_of\_delays] \}$$

BW_{min} is in kbps, and the sum_of_delays is in 10s of microseconds. The bandwidth and delay for an Ethernet interface are 10 Mbps and 1 ms, respectively.

The calculated EIGRP BW metric is

$256 \times 10^7/BW = 256 \times 10^7/10{,}000$

$= 256 \times 10{,}000$

= 256,000

The calculated EIGRP delay metric is

256 x sum of delay = 256 x 1 ms

= 256 x 100 x 10 microseconds

= 25,600 (in tens of microseconds)

Table 12-3 shows some default values for bandwidth and delay.

Table 12-3 *Default EIGRP Values for Bandwidth and Delay*

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 Mbps)
Ethernet	25,600 (1 ms)	256,000 (10 Mbps)
T-1 (1.544 Mbps)	512,000 (20,000 ms)	1,657,856
64 kbps	512,000	40,000,000
56 kbps	512,000	45,714,176

As with IGRP, you use the **metric weights** subcommand to change EIGRP metric computation. You can change the k values in the EIGRP composite metric formula to select which EIGRP metrics to use. The command to change the k values is the **metric weights** *tos k1 k2 k3 k4 k5* subcommand under **router eigrp** *n*. The tos value is always 0. You set the other arguments to 1 or 0 to alter the composite metric. For example, if you want the EIGRP composite metric to use all the parameters, the command is as follows:

```
router eigrp n
 metric weights 0 1 1 1 1 1
```

EIGRP Packet Types

EIGRP uses five packet types:

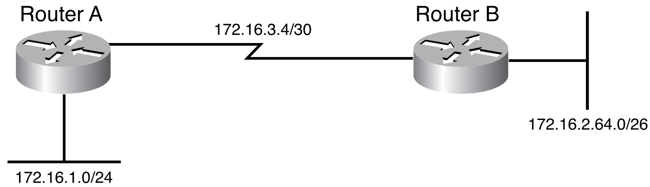
- **Hello**—EIGRP uses hello packets in the discovery of neighbors. They are multicast to 224.0.0.10. By default, EIGRP sends hello packets every 5 seconds (60 seconds on WAN links with 1544 Mbps speeds or less).
- **Acknowledgment**—An acknowledgment packet acknowledges the reception of an update packet. It is a hello packet with no data. EIGRP sends acknowledgment packets to the unicast address of the sender of the update packet.
- **Update**—Update packets contain routing information for destinations. EIGRP unicasts update packets to newly discovered neighbors; otherwise, it multicasts update packets to 224.0.0.10 when a link or metric changes. Update packets are acknowledged to ensure reliable transmission.
- **Query**—EIGRP sends query packets to find feasible successors to a destination. Query packets are always multicast.
- **Reply**—EIGRP sends reply packets to respond to query packets. Reply packets provide a feasible successor to the sender of the query. Reply packets are unicast to the sender of the query packet.

EIGRP Design

When designing a network with EIGRP, remember that it supports VLSMs, CIDR, and network summarization. EIGRP allows for the summarization of routes in a hierarchical network. EIGRP is not limited to 16 hops as RIP is; therefore, the network diameter can exceed this limit. EIGRP does not broadcasts its routing table periodically so there is no large network overhead. You can use EIGRP for large networks; it is a potential routing protocol for the core of a large network. EIGRP further provides for route authentication.

As shown in Figure 12-6, when you use EIGRP, all segments can have different subnet masks.

Figure 12-6 *EIGRP Design*



EIGRP Summary

The characteristics of EIGRP follow:

- Hybrid routing protocol (distance vector that has link-state protocol characteristics).
- Uses IP protocol 88.
- Classless protocol (supports VLSMs).
- Default composite metric uses bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends partial route updates only when there are changes.
- Support for authentication.
- Uses DUAL for loop prevention.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.
- Potential routing protocol for the core of a network; used in large networks.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCDA exam, a well-prepared CCDA candidate should at a minimum know all the details in each "Foundation Summary" before going to take the exam.

This chapter covered the following topics that you will need to master for the CCDA exam:

- **RIPv1**—The first version of RIP
- **RIPv2**—The enhancements in Version 2 of RIP to support network designs
- **IGRP**—The Cisco proprietary routing protocol IGRP
- **EIGRP**—The enhanced version of IGRP and its uses in network design

Some reviews listings and/or tables that appear in this summary were copied directly from within the chapter to emphasize their significance for exam preparation.

Table 12-5 compares the routing protocols covered in this chapter.

Table 12-4 *Routing Protocols Comparison*

	Routing Protocol			
	RIPv1	**RIPv2**	**IGRP**	**EIGRP**
Distance Vector	Yes	Yes	Yes	Hybrid
VLSMs	No	Yes	No	Yes
Authentication	No	Yes	No	Yes
Update Timer (sec)	30	30	90	n/a
Invalid Timer (sec)	180	180	270	n/a
Flush Timer (sec)	240	240	630	n/a
Holddown Timer (sec)	180	180	280	n/a
Protocol/port	UDP 520	UDP 520	IP 9	IP 88
Admin Distance	120	120	100	90

RIPv1 Summary

The characteristics of RIPv1 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classful protocol (no support for VLSMs or CIDR).
- Metric is router hop count.
- Maximum hop count is 15; unreachable routes have a metric of 16.
- Periodic route updates broadcast (255.255.255.255) every 30 seconds.
- 25 routes per RIP message.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- No support for authentication.
- Administrative distance for RIP is 120.
- Used in small, flat networks or at the edge of larger networks.

RIPv2 Summary

The characteristics of RIPv2 follow:

- Distance-vector protocol.
- Uses UDP port 520.
- Classless protocol (support for CIDR).
- Supports VLSMs.
- Metric is router hop count.
- Maximum hop count is 15; infinite (unreachable) routes have a metric of 16.
- Periodic route updates sent every 30 seconds to multicast address 224.0.0.9.
- 25 routes per RIP message (24 if authentication is used).
- Supports authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Subnet mask included in route entry.
- Administrative distance for RIPv2 is 120.
- Used in small, flat networks or at the edge of larger networks.

IGRP Summary

The characteristics of IGRP follow:

- Distance-vector protocol.
- Uses IP protocol 9.
- Classful protocol (no support for CIDR).
- No support for VLSMs.
- Composite metric of bandwidth and delay.
- You can factor load and reliability into the metric.
- Route updates broadcast every 90 seconds.
- 104 routes per IGRP message.
- No support for authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 100.
- Previously used in large networks; now replaced by EIGRP.

EIGRP Summary

The characteristics of EIGRP follow:

- Hybrid routing protocol (distance vector that has link-state protocol characteristics).
- Uses IP protocol 88.
- Classless protocol (supports VLSMs).
- Default composite metric of bandwidth and delay.
- You can factor load and reliability into the metric.
- Sends route updates to multicast address 224.0.0.10.
- Sends partial route updates only when there are changes.
- Support for authentication.
- Uses DUAL for loop prevention.

- By default, equal-cost load balancing. Unequal-cost load balancing with the **variance** command.
- Administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.
- Potential routing protocol for the core of a network; used in large networks.

Q&A

As mentioned in the introduction, you have two choices for review questions. Some of the questions that follow give you a bigger challenge than the exam itself by using a short-answer question format. By reviewing now with more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. The answers to these questions appear in Appendix A.

For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. True or false? RIPv2 broadcasts (255.255.255.255) its routing table every 30 seconds.
2. True or false? By default, EIGRP uses bandwidth, delay, reliability, and load to calculate the composite metric.
3. True or false? EIGRP routers maintain neighbor adjacencies.
4. True or false? EIGRP and RIPv2 support VLSMs and CIDR.
5. True or false? RIPv2 does not have the 15-hop limit of RIPv1.
6. RIP uses _________ port _________.
7. IGRP uses IP protocol number _________.
8. EIGRP uses IP protocol number _________.
9. Between RIP, IGRP, and EIGRP, which protocol would you recommend for use in a large network?
10. Between RIPv2, IGRP, and EIGRP, which protocol would you use in a small network that has both Cisco and non-Cisco routers?
11. Which protocol broadcasts its routing table every 90 seconds by default?
12. Match the protocol with the characteristic:

i. RIPv1	**a.** No VLSM or CIDR support; default update period of 90 seconds.
ii. RIPv2	**b.** VLSM and CIDR support; limited to 15 hops
iii. IGRP	**c.** No VLSM or CIDR support; default update period of 30 seconds
iv. EIGRP	**d.** Uses triggered updates

13. Why is EIGRP sometimes considered a hybrid protocol?

14. True or False? IGRP is limited to 16 router hops.

15. Which routing protocol can you use to exchange route updates with UNIX workstations running the **routed** process?

16. Match the RIP routing table field with its description:

i. IP address	a. The number of hops to the destination
ii. Gateway	b. Next router along the path to the destination
iii. Interface	c. Destination network or host, with subnet mask
iv. Metric	d. Used to access the physical network that must be used to reach the destination
v. Timer	e. Time since the route entry was last updated

17. Match the EIGRP component with its description:

i. RTP	a. An interface between DUAL and IPX RIP, IGRP, and AppleTalk
ii. DUAL	b. Used to deliver EIGRP messages reliably
iii. Protocol-dependent modules	c. Builds an adjacency table
iv. Neighbor discovery	d. Guarantees a loop-free network

18. With Cisco routers, which protocols use only equal-cost load balancing?

19. With Cisco routers, which protocols allow unequal-cost load balancing?

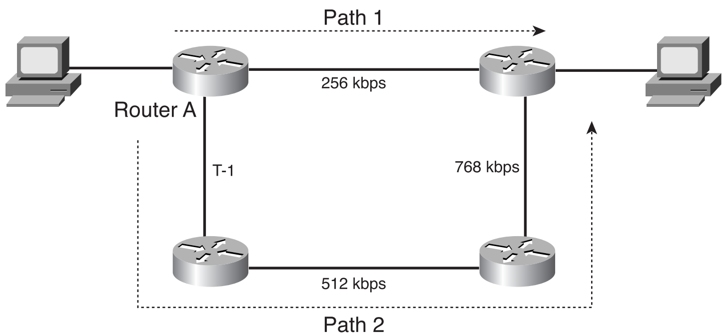
20. Complete Table 12-6 with the VLSM, authentication, and administrative-distance capabilities of each routing protocol.

Table 12-5 *Distance Capabilities*

Routing Protocol	VLSM	Authentication	Admin Distance
RIPv1			
RIPv2			
IGRP			
EIGRP			

Use the Figure 12-7 to answer the following questions.

Figure 12-7 *Path Selection*



21. By default, if RIPv2 is enabled on all routers, what path is taken?

- **a.** Path 1
- **b.** Path 2
- **c.** Unequal load balance with Path 1 and Path 2
- **d.** Equal load balance with Path 1 and Path 2

22. By default, if IGRP is enabled on all routers, what path is taken?

- **a.** Path 1
- **b.** Path 2
- **c.** Unequal load balance with Path 1 and Path 2
- **d.** Equal load balance with Path 1 and Path 2

23. By default, if EIGRP is enabled on all routers, what path is taken?

- **a.** Path 1
- **b.** Path 2
- **c.** Unequal load balance with Path 1 and Path 2
- **d.** Equal load balance with Path 1 and Path 2

24. EIGRP is configured on the routers. If configured with the variance command, what path is taken?

- **a.** Path 1
- **b.** Path 2
- **c.** Unequal load balance with Path 1 and Path 2
- **d.** Equal load balance with Path 1 and Path 2

25. By default, if RIPv1 is enabled on all routers, what path is taken?

- **a.** Path 1
- **b.** Path 2
- **c.** Unequal load balance with Path 1 and Path 2
- **d.** Equal load balance with Path 1 and Path 2