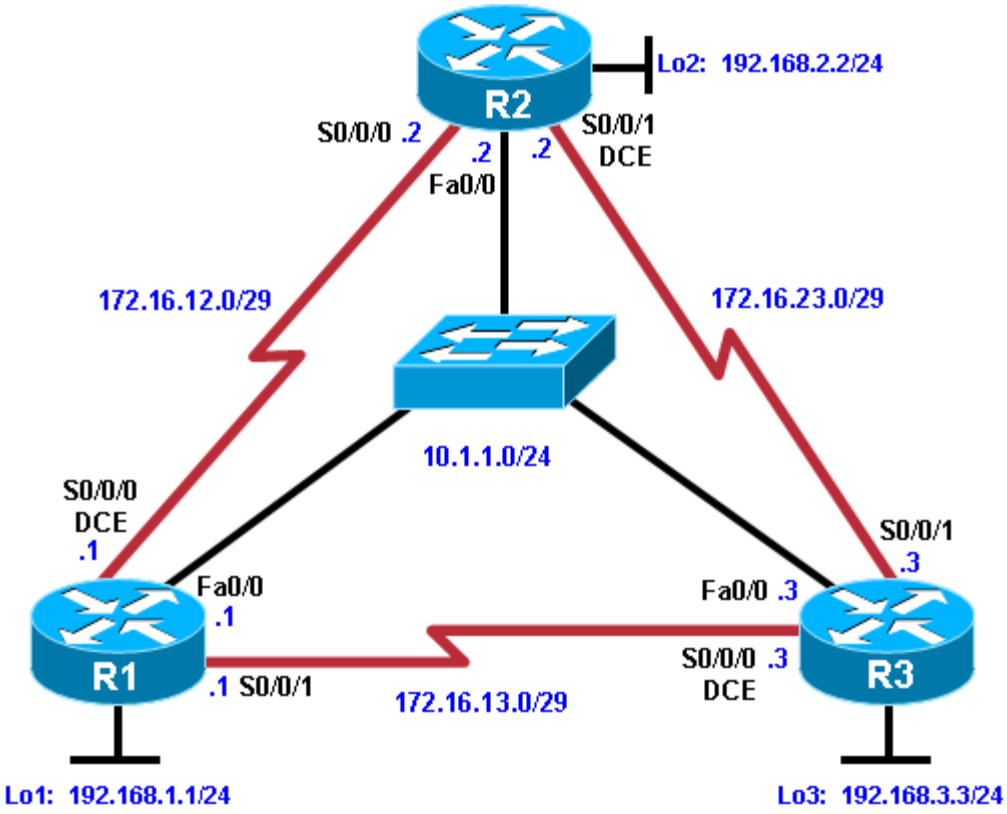
Chapter 2 Lab 2-5, EIGRP Authentication and Timers

Topology



Objectives

- Review a basic configuration of EIGRP.
- Configure and verify EIGRP authentication parameters.
- Configure EIGRP hello interval and hold time.
- Verify the hello interval and hold time.

Background

As a network engineer, you have weighed the benefits of routing protocols and deployed EIGRP in your corporation's network. Recently, a new Chief Information Officer replaced the previous CIO and outlined a new network policy detailing more robust security measures. The CIO has also drawn up specifications to allow more frequent checking between neighboring routers so that fewer packets are lost in transit during times of instability. In this lab, you implement the CIO's specifications on the network.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the advanced IP services image c1841-advipservicesk9-mz.124-24.T1.bin. The switch is a Cisco WS-C2960-24TT-L with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin. You can use other routers (such as a 2801 or 2811) and Cisco IOS Software versions if they have comparable capabilities and features. Depending on the router or switch

model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- 1 switch (Cisco 2960 with the Cisco IOS Release 12.2(46)SE C2960-LANBASEK9-M image or comparable)
- Serial and Ethernet cables

Step 1: Configure the hostname and interface addresses.

Using the addressing scheme in the diagram, apply IP addresses to the loopback, serial, and Fast Ethernet interfaces on R1, R2, and R3. Set the serial interface bandwidth on each router with the interface-level **bandwidth** *bandwidth* command. Specify the bandwidth as 64 kb/s on each serial interface. Specify the clock rate on the DCE end of each serial link using the **clock rate 64000** command.

Note: If you have WIC-2A/S serial interfaces, the maximum clock rate is 128 kb/s. If you have WIC-2T serial interfaces, the maximum clock rate is much higher (2.048 Mb/s or higher depending on hardware), which is more representative of a modern network WAN link. However, this lab uses 64 kb/s and 128 kb/s settings.

You can copy and paste the following configurations into your routers to begin.

Note: Depending on the router model, the interfaces might be numbered differently than those listed and might require you to alter the interface designation accordingly.

Router R1

```
hostname R1
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.12.1 255.255.255.248
 clock rate 64000
 bandwidth 64
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.13.1 255.255.255.248
 bandwidth 64
 no shutdown
!
end
```

Router R2

```
hostname R2
!
interface Loopback2
 ip address 192.168.2.2 255.255.255.0
!
interface FastEthernet0/0
```



```
 ip address 10.1.1.2 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.12.2 255.255.255.248
 bandwidth 64
 no shutdown
!
interface Serial0/0/1
ip address 172.16.23.2 255.255.255.248
 clock rate 64000
 bandwidth 64
 no shutdown
!
end
```

Router R3

```
hostname R3
!
interface Loopback3
 ip address 192.168.3.3 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 no shutdown
!
interface Serial0/0/0
ip address 172.16.13.3 255.255.255.248
 clock rate 64000
 bandwidth 64
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.23.3 255.255.255.248
 bandwidth 64
 no shutdown
!
end
```

Step 2: Configure basic EIGRP.

a. Configure EIGRP AS 1 as in the previous EIGRP labs. Run EIGRP on all connections in the lab, and leave auto-summarization on. Advertise networks 10.0.0.0/8, 172.16.0.0/16, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 from their respective routers.

b. Use the **show ip eigrp neighbors** command to check which routers have EIGRP adjacencies.

```
R1# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.2                Fa0/0             11 00:00:54    4   200  0  36
2   10.1.1.3                Fa0/0             11 00:00:54   13   200  0  39
1   172.16.12.2             Se0/0/0           14 00:14:18   27  2280  0  32
0   172.16.13.3             Se0/0/1           13 00:14:23   25  2280  0  37

R2# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
```



```
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Fa0/0             10 00:02:05 1020  5000  0  35
2   10.1.1.3                Fa0/0             14 00:02:05   11   200  0  39
1   172.16.12.1             Se0/0/0           14 00:15:25  106  2280  0  32
0   172.16.23.3             Se0/0/1           13 00:16:59    1  2280  0  38

R3# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Fa0/0             12 00:03:18  816  4896  0  34
2   10.1.1.2                Fa0/0             11 00:03:18  822  4932  0  35
1   172.16.13.1             Se0/0/0           14 00:16:47   22  2280  0  31
0   172.16.23.2             Se0/0/1           14 00:18:12    4  2280  0  33
```

Did you receive the output that you expected?

c. Run the following Tcl script on all routers to verify full connectivity.

```
R1# tclsh

foreach address {
10.1.1.1
172.16.12.1
172.16.13.1
192.168.1.1
10.1.1.2
172.16.12.2
172.16.23.2
192.168.2.2
10.1.1.3
172.16.13.3
172.16.23.3
192.168.3.3
} { ping $address }
```

You should get ICMP echo replies for every address pinged.

Step 3: Configure authentication keys.

Before you configure a link to authenticate the EIGRP adjacencies, you must configure the keys that are used for the authentication. EIGRP uses Cisco IOS generic router key chains as storage locations for keys. These key chains classify keys into groups, enabling keys to be easily changed periodically without bringing down adjacencies.

a. Use the **key chain** *name* command in global configuration mode to create a chain of keys with the label EIGRP-KEYS.

```
R1# conf t
R1(config)# key chain EIGRP-KEYS
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco

R2# conf t
R2(config)# key chain EIGRP-KEYS
```



```
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string cisco

R3# conf t
R3(config)# key chain EIGRP-KEYS
R3(config-keychain)# key 1
R3(config-keychain-key)# key-string cisco
```

b. Issue the **show key chain** command. You should have the same output on every router.

```
R1# show key chain
Key-chain EIGRP-KEYS:
    key 1 -- text "cisco"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

You can set a time span for sending a key to other routers and during which a key is accepted from other routers. Although lifetime values are not explored in the route labs, you should keep it in mind for production networks when you are rolling from one set of authentication strings to another. For now, you simply want to authenticate the EIGRP adjacencies for security reasons.

Step 4: Configure EIGRP link authentication.

When configuring EIGRP link authentication, you must first associate the key chain with a particular EIGRP process (or autonomous system) running on the interface using the **ip authentication key-chain** *eigrp as_number* **key** *key_chain_label* command. Then you activate the MD5 authentication for that EIGRP process using the **ip authentication mode eigrp** *as_number* **md5** command.

a. Apply the following commands on all active EIGRP interfaces.

```
R1# conf t
R1(config)# interface serial 0/0/0
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# interface serial 0/0/1
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# interface fastethernet 0/0
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R1(config-if)# ip authentication mode eigrp 1 md5

R2# conf t
R2(config)# interface serial 0/0/0
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# interface serial 0/0/1
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# interface fastethernet 0/0
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R2(config-if)# ip authentication mode eigrp 1 md5

R3# conf t
R3(config)# interface serial 0/0/0
R3(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R3(config-if)# ip authentication mode eigrp 1 md5
R3(config-if)# interface serial 0/0/1
R3(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R3(config-if)# ip authentication mode eigrp 1 md5
```

```
R3(config-if)# interface fastethernet 0/0
R3(config-if)# ip authentication key-chain eigrp 1 EIGRP-KEYS
R3(config-if)# ip authentication mode eigrp 1 md5
```

Each EIGRP adjacency should flap (go down and come back up) when you implement MD5 authentication on one side of the link before the other side has been configured. In a production network, flapping causes some instability during a configuration, so make sure you implement MD5 outside of peak usage times.

b. Check the configuration with the **show ip eigrp interfaces detail** command.

```
R1# show ip eigrp interfaces detail
IP-EIGRP interfaces for process 1

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface Peers    Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0       2        0/0         3       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/14  Un/reliable ucasts: 26/21
  Mcast exceptions: 3  CR packets: 3  ACKs suppressed: 3
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use multicast
Se0/0/0     1        0/0         4       0/12          50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 10/28
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 5
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Se0/0/1     1        0/0         1       0/12          50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 10/22
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 8
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Lo1         0        0/0         0       0/1            0           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast

R2# show ip eigrp interfaces detail
IP-EIGRP interfaces for process 1

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface Peers    Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0       2        0/0         4       0/10          50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/7  Un/reliable ucasts: 34/15
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 7
```

```
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
Se0/0/0     1        0/0         1       0/12          50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 19/17
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 7
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
Se0/0/1     1        0/0         3       0/12          50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 11/9
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 4
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
Lo2         0        0/0         0       0/1            0           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast

R3# show ip eigrp interfaces detail
IP-EIGRP interfaces for process 1

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0           2        0/0         4       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/3  Un/reliable ucasts: 6/7
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 2  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use multicast
Se0/0/0         1        0/0       482      10/380       2732           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 3/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Se0/0/1         1        0/0       109      10/380        904           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 4/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Lo3             0        0/0         0       0/1           0           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
```

```
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast
```

At this point, the interfaces are authenticating each adjacency with the EIGRP-KEYS key chain. Make sure that you verify the number of neighbors out each interface in the above output. Notice that the number of peers is the number of adjacencies established out that interface.

When EIGRP has a key chain associated with an autonomous system on a given interface and EIGRP is authenticating its adjacencies, you have successfully completed the initial work.

c. Use the **debug eigrp packets** command to see the authenticated hellos.

```
R1# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY, SIAREPLY)
R1#
* Feb 9 19:10:51.090: EIGRP: Sending HELLO on Serial0/0/1
* Feb 9 19:10:51.090:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
* Feb 9 19:10:51.190: EIGRP: received packet with MD5 authentication, key id
= 1
* Feb 9 19:10:51.190: EIGRP: Received HELLO on Serial0/0/1 nbr 172.16.13.3
* Feb 9 19:10:51.190:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
peerQ un/rely 0/0
* Feb 9 19:10:51.854: EIGRP: received packet with MD5 authentication, key id
= 1
* Feb 9 19:10:51.854: EIGRP: Received HELLO on FastEthernet0/0 nbr 10.1.1.2
* Feb 9 19:10:51.854:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
peerQ un/rely 0/0
* Feb 9 19:10:53.046: EIGRP: received packet with MD5 authentication, key id
= 1

<output omitted>
```

d. Issue the **undebug all** command to stop the debugging output.

Step 5: Manipulate EIGRP timers.

The CIO also ordered you to change the hello and dead intervals on point-to-point serial interfaces so that dead neighbors are detected in roughly half the time that they are detected by default.

a. To view the default timers, use the **show ip eigrp interfaces detail** command.

```
R1# show ip eigrp interfaces detail
IP-EIGRP interfaces for process 1

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0           2        0/0         4       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/3  Un/reliable ucasts: 6/7
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 2  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use multicast
Se0/0/0         1        0/0       482      10/380       2732           0
  Hello interval is 5 sec
```

```
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 3/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Se0/0/1         1        0/0       109      10/380        904           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 4/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast

<output omitted>
```

The default hello interval for point-to-point serial links is 5 seconds, regardless of the bandwidth, and 5 seconds for LAN interfaces. The default hold time is three times the length of the hello interval.

The hello interval determines how often *outgoing* EIGRP hellos are sent, while the hold time defines how long other neighbors tolerate the loss of the hello packets You are more concerned with the hold time than the hello interval, because the hold time detects a dead neighbor. However, you also want the neighbors to send the same number of hellos as under normal circumstances before declaring a neighbor dead.

The requirements from the CIO specify that the hold time should be roughly half of the default, which is 15 seconds, so a new hold time of 7 or 8 seconds would be appropriate. A shorter hold time allows a dead neighbor to be detected more quickly. A hello interval of 2 seconds results in detecting new neighbors more rapidly.

b. Change both the hello interval and the hold time for AS 1 for serial 0/0/0 on R1 and R2 using the **ip hello-interval eigrp 1 2** and **ip hold-time eigrp 1 8** commands. If necessary, use the **?** to investigate what each parameter does.

```
R1# conf t
R1(config)# interface serial 0/0/0
R1(config-if)# ip hello-interval eigrp 1 2
R1(config-if)# ip hold-time eigrp 1 8

R2# conf t
R2(config)# interface serial 0/0/0
R2(config-if)# ip hello-interval eigrp 1 2
R2(config-if)# ip hold-time eigrp 1 8
```

c. Verify that the hello interval has been successfully changed on routers R1 and R2 using the **show ip eigrp 1 interfaces detail serial 0/0/0** command.

```
R1# show ip eigrp 1 interfaces detail serial 0/0/0
IP-EIGRP interfaces for process 1

                      Xmit Queue   Mean   Pacing Time   Multicast
Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0/0         1        0/0       482      10/380       2732           0
  Hello interval is 2 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 3/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
```



```
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast

R2# show ip eigrp 1 interfaces detail serial 0/0/0
IP-EIGRP interfaces for process 1
                      Xmit Queue   Mean   Pacing Time   Multicast
Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0/0            1        0/0       190      10/380       1300           0
  Hello interval is 2 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 4/5
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
```

d. Verify that the hold time has been successfully changed with the **show ip eigrp neighbors** command.

```
R1# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.2                Fa0/0             11 01:32:00    7   200  0  19
2   10.1.1.3                Fa0/0             12 01:32:03    1   200  0  18
1   172.16.12.2             Se0/0/0            7 01:32:27  482  2892  0  17
0   172.16.13.3             Se0/0/1           11 01:32:28  109  2280  0  19

R2# show ip eigrp neighbors
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Fa0/0             14 01:30:33  816  4896  0  19
2   10.1.1.3                Fa0/0             12 01:30:33  819  4914  0  21
1   172.16.12.1             Se0/0/0            7 01:30:58  190  2280  0  21
0   172.16.23.3             Se0/0/1           13 01:30:59   80  2280  0  20
```

e. Configure the same hello interval and hold time on each active serial interface in the topology.

```
R1# conf t
R1(config)# interface serial 0/0/1
R1(config-if)# ip hello-interval eigrp 1 2
R1(config-if)# ip hold-time eigrp 1 8

R2# conf t
R2(config)# interface serial 0/0/1
R2(config-if)# ip hello-interval eigrp 1 2
R2(config-if)# ip hold-time eigrp 1 8

R3# conf t
R3(config)# interface serial 0/0/0
R3(config-if)# ip hello-interval eigrp 1 2
R3(config-if)# ip hold-time eigrp 1 8
R3(config-if)# interface serial 0/0/1
R3(config-if)# ip hello-interval eigrp 1 2
R3(config-if)# ip hold-time eigrp 1 8
```

f. Make sure that all of the EIGRP neighbor relationships remain up during the configuration process. Use the **show ip eigrp neighbors** command to verify the hold time, and the **show ip eigrp interfaces detail** command to verify the hello interval.


```
R1# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.2                Fa0/0             14 01:35:15    7   200  0  19
2   10.1.1.3                Fa0/0             12 01:35:18    1   200  0  18
1   172.16.12.2             Se0/0/0            7 01:35:43  482  2892  0  17
0   172.16.13.3             Se0/0/1            6 01:35:43  109  2280  0  19

R1# show ip eigrp interfaces detail
IP-EIGRP interfaces for process 1

                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0           2        0/0         4       0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/3  Un/reliable ucasts: 6/7
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 2  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use multicast
Se0/0/0         1        0/0       482      10/380       2732           0
  Hello interval is 2 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 3/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast
Se0/0/1         1        0/0       109      10/380        904           0
  Hello interval is 2 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 4/7
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 2
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-KEYS"
  Use unicast

<output omitted>
```

g. Run the Tcl script again to make sure you still have full connectivity after making the changes to the EIGRP default configuration. You should receive all ICMP echo replies back successfully.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
2800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than list all combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. For example, for an ISDN BRI interface, the string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				