Lab ID: 9.9K914A095.SQI2.1

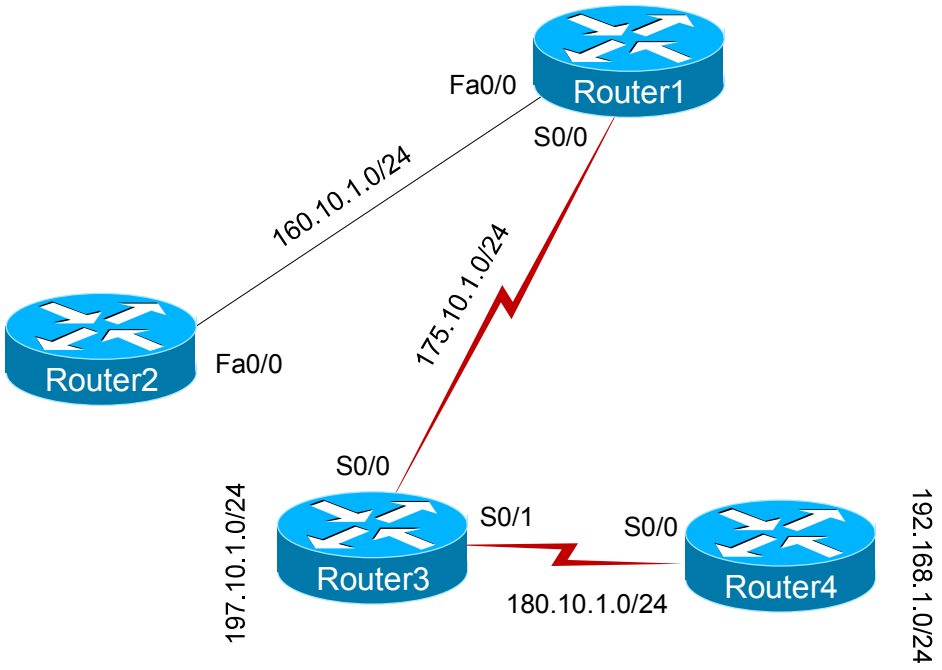
Sequential Lab: EIGRP

Objective

In this lab, you will configure the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol and Message Digest 5 (MD5) authentication.

Lab Topology

The topology diagram below represents the portion of the network you will configure in this lab.



Command Summary

Command	Description
auto-summary	restores the default behavior of automatic summarization of subnet routes into network-level routes
configure terminal	enters global configuration mode from privileged EXEC mode
debug eigrp neighbors	displays EIGRP neighbors discovered by EIGRP
enable	enters privileged EXEC mode
end	ends and exits configuration mode
exit	exits one level in the menu structure
interface *type number*	changes from global configuration mode to interface configuration mode
ip authentication key-chain eigrp *autonomous-system-number key-chain*	enables authentication of EIGRP packets

Command	Description
ip authentication mode eigrp *autonomous-system-number* **md5**	specifies the type of authentication used in EIGRP packets
key *key-id*	creates or modifies a key chain key
key chain *key-chain-name*	creates or modifies a key chain
key-string *key-string-text*	specifies the authentication string for the key
network *network-address*	activates EIGRP on the specified network
no debug all	turns off all diagnostic output
ping *ip-address*	sends an Internet Control Message Protocol (ICMP) echo request to the specified address
router eigrp *autonomous-system-number*	enters router configuration mode for EIGRP
show ip eigrp neighbors	displays information about EIGRP neighbors
show ip eigrp topology	displays EIGRP topology table
show ip eigrp traffic	displays EIGRP traffic information
show ip protocols	displays information about active routing protocols
show ip route	displays the IP routing table
show running-config	displays the active configuration file
shutdown; **no shutdown**	disables an interface; enables an interface

Lab Tasks

Passwords in this lab have been configured as **cisco**.

Task 1: Enable EIGRP, and Test Connectivity

1. Configure EIGRP on Router1, Router2, Router3, and Router4. Use autonomous system (AS) number **100**, and configure EIGRP to send and receive updates on all interfaces except the Frame Relay interfaces. While you are configuring EIGRP on the routers, you should see output to the console as EIGRP neighbor relationships form.

2. Display the dynamic routing protocols that are running on Router4. What is the maximum router hop count with EIGRP? _____

3. On Router1, display Router1's EIGRP neighbors.

4. On Router1, display the statistics for EIGRP packet types sent and received.

5. On Router1, display the EIGRP topology database. What does the EIGRP topology database contain? _____

6. On Router4, display the IP routing table. What is the administrative distance for EIGRP? _____

7. From Router4, ping Router1 (175.10.1.1) and Router2 (160.10.1.2). These pings should succeed if EIGRP is configured correctly on all routers.

Task 2: Configure EIGRP MD5 Authentication

In this task, you will configure EIGRP MD5 authentication between Router3 and Router4.

1. On Router4, create a key chain that can be used for EIGRP authentication. Use a key chain of **ccna-chain**, a key of **1**, and a key string of **boson**.

2. Now that the key chain has been created, enable EIGRP authentication on Router4; use the new key chain. Note that the EIGRP neighbor relationship between Router3 and Router4 is lost.

3. On Router3, create a key chain that can be used for EIGRP authentication. Use a key chain of **ccna-chain**, a key of **1**, and a key string of **boson**.

4. Now that the key chain has been created, enable EIGRP authentication on Router3; use the new key chain. Note that the EIGRP neighbor relationship between Router3 and Router4 is restored.

5. From Router3, ping Router4's Serial 0/0 interface (180.10.1.2). The ping should be successful.

Task 3: Examine EIGRP Debugging Output

Reviewing debugging output can help you troubleshoot EIGRP issues.

1. On Router4, display EIGRP neighbors discovered by EIGRP.

2. On Router4, disable the Serial 0/0 interface. Review the EIGRP debugging output.

3. On Router4, enable the Serial 0/0 interface and review the EIGRP debugging output.

4. On Router4, disable EIGRP debugging.

5. What can you determine from the EIGRP neighbors debugging output? _____
   _____

Lab Solutions

Passwords in this lab have been configured as **cisco**.

Task 1: Enable EIGRP, and Test Connectivity

1. Issue the following commands to correctly configure EIGRP on Router1, Router2, Router3, and Router4; while you are configuring EIGRP on the routers, you should see output to the console as EIGRP neighbor relationships form:

```
Router1(config)#router eigrp 100
Router1(config-router)#auto-summary
Router1(config-router)#network 160.10.0.0
Router1(config-router)#network 175.10.0.0

Router2(config)#router eigrp 100
Router2(config-router)#auto-summary
Router2(config-router)#network 160.10.0.0

Router3(config)#router eigrp 100
Router3(config-router)#auto-summary
Router3(config-router)#network 175.10.0.0
Router3(config-router)#network 180.10.0.0
Router3(config-router)#network 197.10.1.0

Router4(config)#router eigrp 100
Router4(config-router)#auto-summary
Router4(config-router)#network 180.10.0.0
Router4(config-router)#network 192.168.1.0
```

2. The maximum router hop count with EIGRP is 100 hops. On Router4, issue the following command to display the dynamic routing protocols that are running on the router; sample output is shown below:

```
Router4#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  Routing for Networks:
  Automatic network summarization is in effect
    180.10.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last update
    180.10.1.1           90      00:00:35
  Distance: internal 90 external 170
```

3. On Router1, issue the following command to display Router1's EIGRP neighbors. Sample output is shown below:

```
Router1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address            Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                       (sec)         (ms)       Cnt Num
0   160.10.1.2         Fa0/0             13 00:01:52  382  2292  0  5
1   175.10.1.2         Se0/0             13 00:01:37  586  3516  0  6
```

4. On Router1, issue the following command to display the statistics for EIGRP packet types sent and received. Sample output is below:

```
Router1#show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 100
  Hellos sent/received: 119/121
  Updates sent/received: 10/12
  Queries sent/received: 14/4
  Replies sent/received: 11/11
  Acks sent/received: 2/13
  Input queue high water mark 2, 0 drops
  SIA-Queries sent/received: 0/0
  SIA Replies sent/received: 0/0:
  Hello Process ID: 107
  PDM Process ID: 105
```

5. On Router1, issue the following command to display the EIGRP topology database. The EIGRP topology database contains primary and backup routes to each destination learned from EIGRP neighbors. The best routes (those with the lowest composite metric) are termed successor routes and are inserted in the IP routing table on the router. Sample output is below:

```
Router1#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 160.10.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 160.10.2.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
P 175.10.1.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0
P 175.10.0.0/16, 1 successors, FD is 40512000
        via Summary (40512000/0), Null0
P 160.10.0.0/16, 1 successors, FD is 28160
        via Summary (28160/0), Null0
P 180.10.0.0/16, 1 successors, FD is 41024000
        via 175.10.1.2 (41024000/2169856), Serial0/0
P 197.10.1.0/24, 1 successors, FD is 40514560
        via 175.10.1.2 (40514560/28160), Serial0/0
P 192.168.1.0/24, 1 successors, FD is 41026560
        via 175.10.1.2 (41026560/2172416), Serial0/0
```

6. The administrative distance for EIGRP is 90. On Router4, issue the following command to display the IP routing table on Router4; sample output is shown below:

```
Router4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E – EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set

     180.10.0.0/16 is variably subnetted, 2 subnets
C       180.10.1.0/24 is directly connected, Serial0/0
D       180.10.0.0/16 is a summary, 00:06:07, Null0
C    192.168.1.0 is directly connected, FastEthernet0/1
D    197.10.1.0 [90/2172416] via 180.10.1.1, 00:06:07, Serial0/0
D    160.10.0.0 [90/2684416] via 180.10.1.1, 00:06:07, Serial0/0
D    175.10.0.0 [90/2681856] via 180.10.1.1, 00:06:07, Serial0/0
```

7. Pings from Router4 to Router1 (175.10.1.1) and Router2 (160.10.1.2) should succeed if EIGRP is configured correctly on all routers.

Task 2: Configure EIGRP MD5 Authentication

1. On Router4, issue the following commands to create a key chain that can be used for EIGRP authentication:

```
Router4(config)#key chain ccna-chain
Router4(config-keychain)#key 1
Router4(config-keychain-key)#key-string boson
Router4(config-keychain-key)#exit
```

2. Now that the key chain has been created, issue the following commands on Router4 to enable EIGRP authentication using the new key chain. Note that the EIGRP neighbor relationship between Router3 and Router4 is lost.

```
Router4(config)#interface serial 0/0
Router4(config-if)#ip authentication mode eigrp 100 md5
Router4(config-if)#ip authentication key-chain eigrp 100 ccna-chain

*Mar 30 13:08:58.359: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 180.10.1.1
(Serial0/0) is down: authentication mode changed
```

3. On Router3, issue the following commands to create a key chain that can be used for EIGRP authentication:

```
Router3(config)#key chain ccna-chain
Router3(config-keychain)#key 1
Router3(config-keychain-key)#key-string boson
```

4. Now that the key chain has been created, issue the following commands on Router3 to enable EIGRP authentication using the new key chain. Note that the EIGRP neighbor relationship between Router3 and Router4 is restored.

```
Router3(config)#interface serial 0/1
Router3(config-if)#ip authentication mode eigrp 100 md5
Router3(config-if)#ip authentication key-chain eigrp 100 ccna-chain

*Mar 30 13:16:04.177: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 180.10.1.2
(Serial0/1) is up: new adjacency
```

5. A ping from Router3 to Router4's Serial 0/0 interface (180.10.1.2) should be successful.

Task 3: Examine EIGRP Debugging Output

1. On Router4, issue the following command to display EIGRP neighbors discovered by EIGRP:

```
Router4#debug eigrp neighbors
EIGRP Neighbors debugging is on
```

2. On Router4, issue the following commands to disable the Serial 0/0 interface. Review the EIGRP debugging output:

```
Router4(config)#interface serial 0/0
Router4(config-if)#shutdown
*Mar 30 12:46:00.582: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 180.10.1.1
(Serial0/0) is down: interface down

*Mar 30 12:46:00.782: EIGRP: Neighbor 180.10.1.1 went down on Serial0/0

%LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
```

3. On Router4, issue the following command to enable the Serial 0/0 interface. Review the EIGRP debugging output:

```
Router4(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up

*Mar 30 12:47:34.523: EIGRP: New peer 180.10.1.1

*Mar 30 12:47:34.679: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 180.10.1.1
(Serial0/0) is up: new adjacency
```

4. On Router4, issue the following commands to disable EIGRP debugging:

```
Router4#no debug all
All possible debugging has been turned off
```

5. You can determine from the EIGRP neighbors debugging output that a neighbor relationship was lost when the Serial 0/0 interface was disabled and a new relationship formed when it was subsequently enabled.

Sample Configuration Script

Router1

```
Router1#show running-config
Building configuration...
Current configuration : 1113 bytes
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
enable secret 5 $sdf$6978yhg$jnb76sd
enable password boson
!
ip subnet-zero
!
ip cef
no ip domain-lookup
ip host Router2 160.10.1.2
!
interface Loopback0
 ip address 160.10.2.1 255.255.255.0
 no ip directed broadcast
!
interface Serial0/0
 description Serial Link to Router3
 ip address 175.10.1.1 255.255.255.0
 no ip directed-broadcast
 clock rate 64000
 bandwidth 64
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
```

Router1 (continued)

```
!
interface FastEthernet0/0
 ip address 160.10.1.1 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
router eigrp 100
 network 160.10.0.0
 network 175.10.0.0
 auto-summary
!
ip classless
no ip http server
!
cdp holdtime 20
cdp timer 50
!
banner motd ^C
Unauthorized Access Prohibited^C
line con 0
 login
 password cisco
line aux 0
line vty 0 4
!
no scheduler allocate
end
```