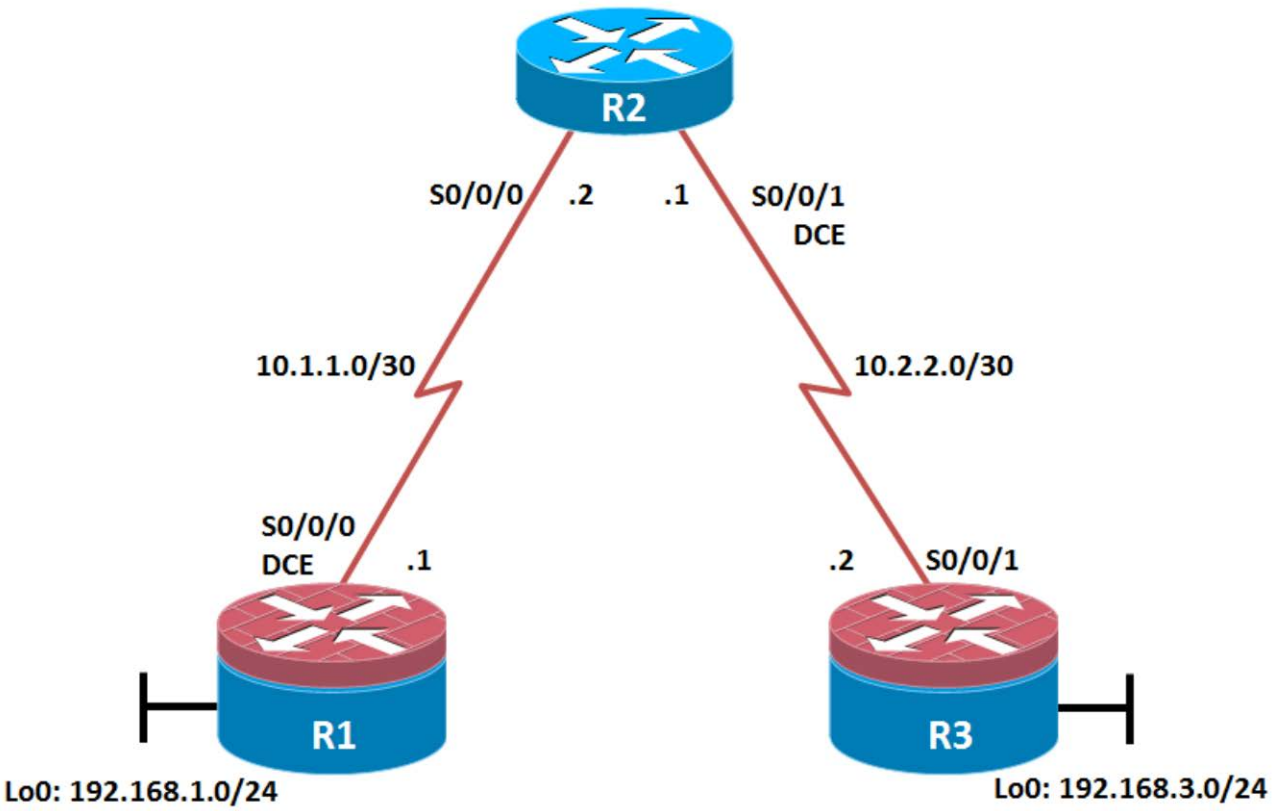
CCNPv7 ROUTE

Chapter 8 Lab 8-2, Routing Protocol Authentication

Topology



Objectives

- Secure EIGRP routing protocol using SHA authentication.
- Secure OSPF routing protocol using SHA authentication.

Background

The

In this lab, you build a multi-router network and secure the routing protocols used between R1, R2, and R3.

Note: This lab uses Cisco 1941 routers with Cisco IOS Release 15.2 with IP Base. 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 IOS Release 15.2 or comparable)
- Serial and Ethernet cables

Step 1: Configure loopbacks and assign addresses.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the R1, R2, and R3 routers.

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

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

R1

```
hostname R1

interface Loopback 0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
exit
!
interface Serial0/0/0
 description R1 --> R2
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 no shutdown
exit
!
end
```

R2

```
hostname R2
!
interface Serial0/0/0
 description R2 --> R1
 ip address 10.1.1.2 255.255.255.252
 no shutdown
exit

interface Serial0/0/1
 description R2 --> R3
```

```
 ip address 10.2.2.1 255.255.255.252
 clock rate 128000
 no shutdown
exit
!
end
```

R3

```
hostname R3
!
interface Loopback0
 description R3 LAN
 ip address 192.168.3.1 255.255.255.0
exit


interface Serial0/0/1
 description R3 --> R2
 ip address 10.2.2.2 255.255.255.252
 no shutdown
exit
!
end
```

Step 2: Configure named EIGRP routing.

EIGRP SHA authentication can only be configured when using the named EIGRP method. In this step, you will configure named EIGRP.

a. On R1, configure named EIGRP.

```
R1(config)# router eigrp ROUTE
R1(config-router)# address-family ipv4 autonomous-system 1
R1(config-router-af)# network 10.1.1.0 0.0.0.3
R1(config-router-af)# network 192.168.1.0 0.0.0.255
R1(config-router-af)#
```

b. On R2, configure named EIGRP.

```
R2(config)# router eigrp ROUTE
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# network 10.1.1.0 0.0.0.3
R2(config-router-af)# network 10.2.2.0 0.0.0.3
R2(config-router-af)#
Jan 10 10:10:59.823: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1
(Serial0/0/0) is up: new adjacency
R2(config-router-af)#
```

c. On R3, configure named EIGRP.

```
R3(config)# router eigrp ROUTE
R3(config-router)# address-family ipv4 autonomous-system 1
R3(config-router-af)# network 10.2.2.0 0.0.0.3
R3(config-router-af)# network 192.168.3.0 0.0.0.255
R3(config-router-af)#
Jan 10 10:10:58.795: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.2.2.1
(Serial0/0/1) is up: new adjacency
```

```
R3(config-router-af)#
```

d. Verify the routing table of R1.

```
R1# show ip route eigrp | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.2.2.0/30 [90/23796062] via 10.1.1.2, 00:05:56, Serial0/0/0
D     192.168.3.0/24 [90/23796702] via 10.1.1.2, 00:05:44, Serial0/0/0
R1#
```

e. From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {
192.168.1.1
10.1.1.1
10.1.1.2
10.2.2.1
10.2.2.2
192.168.3.1
} { ping $address }
```

```
R1(tcl)#foreach address {
+>(tcl)#192.168.1.1
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#192.168.3.1
+>(tcl)#} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1(tcl)#
```

Are the pings now successful?

_____

_____

Step 3: Secure the named EIGRP routing process.

a. On R1, create the key chain to be used for authentication.

```
R1(config)# key chain NAMED-R1-Chain
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)#
```

b. Next, enable authentication on the serial 0/0/0 interface of R1.

```
R1(config)# router eigrp ROUTE
R1(config-router)# address-family ipv4 autonomous-system 1
R1(config-router-af)# af-interface S0/0/0
R1(config-router-af-interface)# authentication key-chain NAMED-R1-Chain
R1(config-router-af-interface)# authentication mode hmac-sha-256 secret-2
R1(config-router-af-interface)#
Jan 10 10:19:35.035: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2
(Serial0/0/0) is down: authentication HMAC-SHA-256 configured
R1(config-router-af-interface)#
```

Notice how the adjacency with R2 has changed to down. This is because R1 no longer accepts the updates from R2 because they are not authenticated.

c. On R2, create the key chain to be used for authentication.

```
R2(config)# key chain NAMED-R2-Chain
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string secret-1
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)#
```

d. Next, enable authentication on the serial 0/0/0 and serial 0/0/1 interfaces of R2.

```
R2(config)# router eigrp ROUTE
R2(config-router)# address-family ipv4 autonomous-system 1
R2(config-router-af)# af-interface S0/0/0
R2(config-router-af-interface)# authentication key-chain NAMED-R2-Chain
R2(config-router-af-interface)# authentication mode hmac-sha-256 secret-2
R2(config-router-af-interface)# exit
R2(config-router-af)# af-interface S0/0/1
R2(config-router-af-interface)# authentication key-chain NAMED-R2-Chain
```

```
R2(config-router-af-interface)# authentication mode hmac-sha-256 secret-2
R2(config-router-af-interface)#
Jan 10 10:22:03.299: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.2.2.2
(Serial0/0/1) is down: authentication HMAC-SHA-256 configured
R2(config-router-af-interface)#
Jan 10 10:22:05.503: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1
(Serial0/0/0) is up: new adjacency
R2(config-router-af-interface)#
```

Notice how the first informational message is saying that the adjacency with R3 has changed to down. This is because R2 no longer accepts the updates from R3 because they are not authenticated.

However, the second information message is saying that the adjacency with R1 has been restored because they are now authenticating each other's routing updates.

e. On R3, create the key chain to be used for authentication.

```
R3(config)# key chain NAMED-R3-Chain
R3(config-keychain)# key 1
R3(config-keychain-key)# key-string secret-1
R3(config-keychain-key)# exit
R3(config-keychain)# exit
R3(config)#
```

f. Next, enable authentication on the serial 0/0/1 interface of R3.

```
R3(config)# router eigrp ROUTE
R3(config-router)# address-family ipv4 autonomous-system 1
R3(config-router-af)# af-interface S0/0/1
R3(config-router-af-interface)# authentication key-chain NAMED-R3-Chain
R3(config-router-af-interface)# authentication mode hmac-sha-256 secret-2
R3(config-router-af-interface)#
Jan 10 10:28:17.455: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.2.2.1
(Serial0/0/1) is up: new adjacency
R3#
```

f. Verify the routing table of R1.

```
R1#show ip route eigrp | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.2.2.0/30 [90/23796062] via 10.1.1.2, 00:08:18, Serial0/0/0
D     192.168.3.0/24 [90/23796702] via 10.1.1.2, 00:01:56, Serial0/0/0
R1#
```

g. From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {
```

```
192.168.1.1
10.1.1.1
10.1.1.2
10.2.2.1
10.2.2.2
192.168.3.1
} { ping $address }

R1(tcl)#foreach address {
+>(tcl)#192.168.1.1
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#192.168.3.1
+>(tcl)#} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1(tcl)#
```

Are the pings now successful?

_____

_____

h. Next we will configure OSPF routing protocol authentication. Therefore, remove EIGRP from R1, R2, and R3 using the **no router eigrp ROUTE** command on all three routers.

```
R1(config)# no router eigrp ROUTE
R1(config)
```

Step 4: Configure OSPF routing.

Since Cisco IOS Software Release 15.4(1)T, OSPFv2 supports SHA hashing authentication using key chains. Cisco refers to this as OSPFv2 Cryptographic Authentication feature. The feature prevents unauthorized or invalid routing updates in a network by authenticating OSPFv2 protocol packets using HMAC-SHA algorithms.

a. On R1, configure OSPF.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#
```

b. On R2, configure OSPF.

```
R2(config)# router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#
```

c. On R3, configure OSPF.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.3.0 0.0.0.255 area 0
R1(config-router)# network 10.2.2.0 0.0.0.3 area 0
R1(config-router)#
```

d. From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {
192.168.1.1
10.1.1.1
10.1.1.2
10.2.2.1
10.2.2.2
192.168.3.1
} { ping $address }
```

```
R1(tcl)#foreach address {
+>(tcl)#192.168.1.1
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#192.168.3.1
+>(tcl)#} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1(tcl)#
```

Are the pings now successful?

_____

_____

Step 5: Secure the OSPF routing protocol.

OSPF will use the OSPFv2 Cryptographic Authentication.

a. On R1, create the key chain to be used for OSPF authentication.

```
R1(config)# key chain SHA-CHAIN
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)#
```

b. Next, enable authentication on the serial 0/0/0 interface of R1.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA-CHAIN
R1(config-if)#
Jan 10 11:08:34.075: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
```

Notice how the adjacency with R2 has changed to down. This is because R1 no longer accepts the updates from R2 because they are not authenticated.

c. On R2, create the key chain to be used for authentication.

```
R2(config)# key chain SHA-CHAIN
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string secret-1
R2(config-keychain-key)# cryptographic-algorithm hmac-sha-256
```

```
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)#
```

d. Next, enable authentication on the serial 0/0/0 and serial 0/0/1 interfaces of R2.

```
R2(config)# interface s0/0/0
R2(config-if)# ip ospf authentication key-chain SHA-CHAIN
R2(config-if)# exit
R2(config)#
R2(config)# interface s0/0/1
R2(config-if)# ip ospf authentication key-chain SHA-CHAIN
R2(config-if)#
Jan 10 11:08:42.523: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#
Jan 10 11:09:14.487: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Notice how the first informational message is saying that the adjacency with R1 has been restored because they are now authenticating each other's routing updates.

However, the second information message is saying that the adjacency with R3 has changed to down. This is because R2 no longer accepts the updates from R3 because they are not authenticated.

e. On R3, create the key chain to be used for authentication.

```
R3(config-router)# key chain SHA-CHAIN
R3(config-keychain)# key 1
R3(config-keychain-key)# key-string secret-1
R3(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R3(config-keychain-key)# exit
R3(config-keychain)# exit
R3(config)#
```

f. Next, enable authentication on the serial 0/0/1 interface of R3.

```
R3(config)#interface s0/0/1
R3(config-if)#ip ospf authentication key-chain SHA-CHAIN
R3(config-if)#
Jan 10 11:09:20.223: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1
from LOADING to FULL, Loading Done
R3#
```

e. Verify the routing table of R1.

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

```
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:05:23, Serial0/0/0
      192.168.3.0/32 is subnetted, 1 subnets
O        192.168.3.1 [110/129] via 10.1.1.2, 00:04:23, Serial0/0/0
R1#
```

f. Verify the routing table of R1.

```
R1# show ip ospf interface s0/0/0 | section Crypto
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain SHA-CHAIN
R1#
```

g. From the R1 router, run the following Tcl script to verify connectivity.

```
foreach address {
192.168.1.1
10.1.1.1
10.1.1.2
10.2.2.1
10.2.2.2
192.168.3.1
} { ping $address }
```

```
R1(tcl)#foreach address {
+>(tcl)#192.168.1.1
+>(tcl)#10.1.1.1
+>(tcl)#10.1.1.2
+>(tcl)#10.2.2.1
+>(tcl)#10.2.2.2
+>(tcl)#192.168.3.1
+>(tcl)#} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1(tcl)#
```

Are the pings now successful?

_____

_____