ASA 9.x EIGRP Configuration Example

Contents

Introduction

This document describes how to configure the Cisco Adaptive Security Appliance (ASA) in order to learn routes through the Enhanced Interior Gateway Routing Protocol (EIGRP), which is supported in ASA Software Version 9.x and later, and perform authentication.

Prerequisites

Requirements

Cisco requires that you meet these conditions before you attempt this configuration:

- Cisco ASA must run Version 9.x or later.

- EIGRP must be in single-context mode, because it is not supported in multi-context mode.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA Software Version 9.2.1
- Cisco Adaptive Security Device Manager (ASDM) Version 7.2.1
- Cisco IOS® Router that runs Version 12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Guidelines and Limitations

- One EIGRP instance is supported in single mode and per context in multimode.
- Two threads are created per context per EIGRP instance in multimode and can be viewed with the show process.
- Auto-summary is disabled by default.
- A Neighbor Relationship is not established between the cluster units in individual interface mode.
- Default-information in [<acl>] is used in order to filter the Exterior bit in incoming candidate default routes.
- Default-information out [<acl>] is used in order to filter the Exterior bit in outgoing candidate default routes.

EIGRP and Failover

Cisco ASA code Version 8.4.4.1 and later synchronizes dynamic routes from the ACTIVE unit to the STANDBY unit. In addition, deletion of routes is also synchronized to the STANDBY unit. However, the state of peer adjacencies is not synchronized; only the ACTIVE device maintains the neighbor state and actively participates in dynamic routing. Refer to ASA FAQ: What happens after failover if dynamic routes are synchronized? for more information.

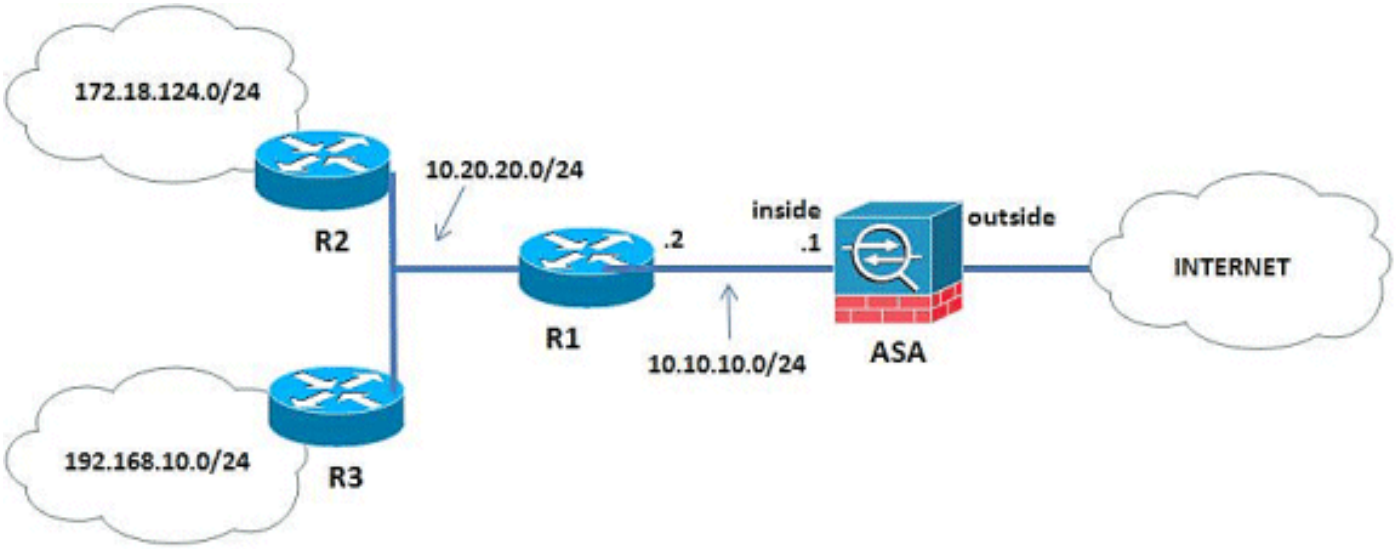
Configure

This section describes how to configure the features covered in this document.

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



In the network topology that is illustrated, the Cisco ASA inside interface IP address is 10.10.10.1/24. The goal is to configure EIGRP on the Cisco ASA in order to learn routes to the internal networks (10.20.20.0/24, 172.18.124.0/24, and 192.168.10.0/24) dynamically through the adjacent router (R1). R1 learns the routes to remote internal networks through the other two routers (R2 and R3).

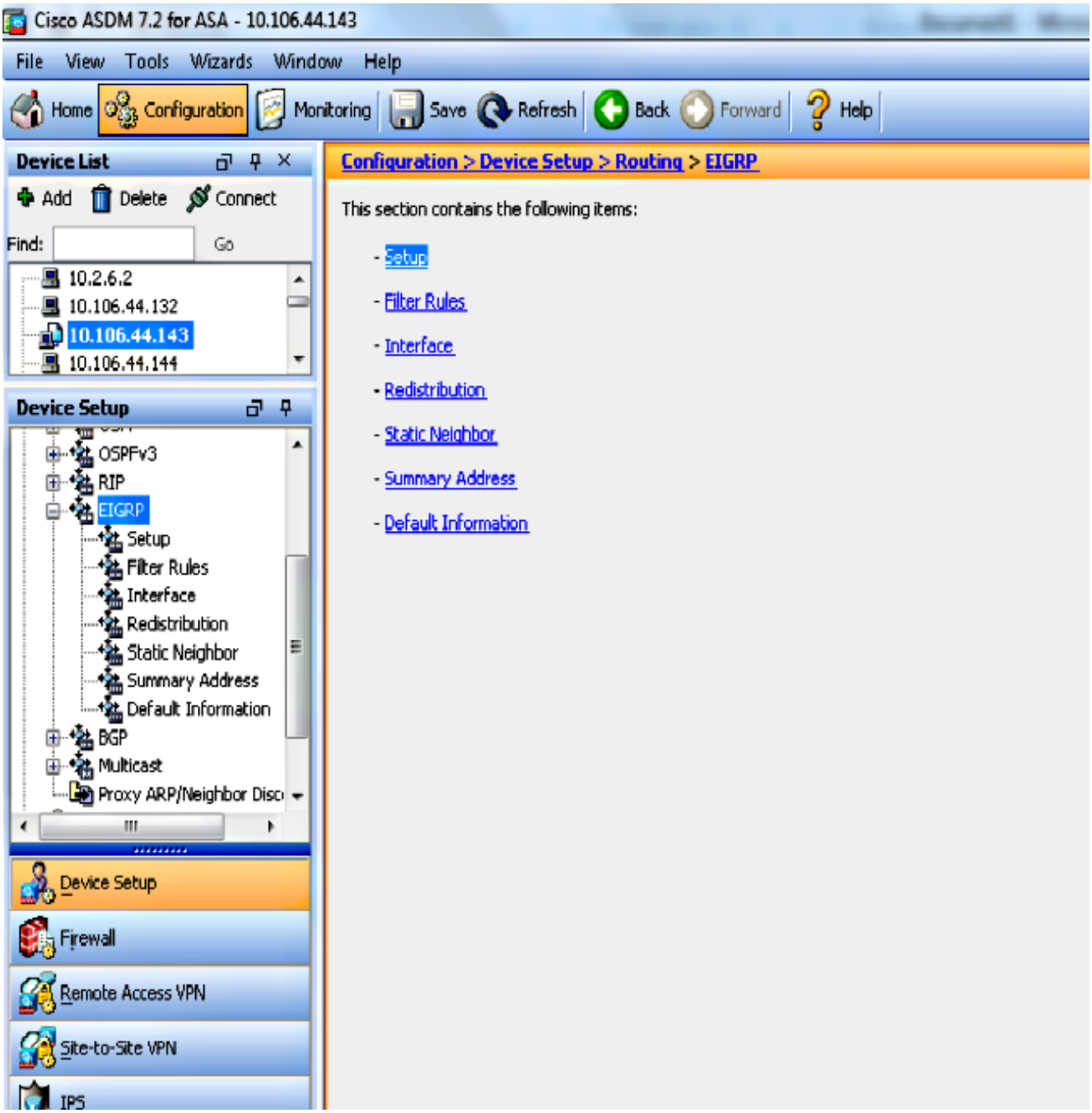
ASDM Configuration

ASDM is a browser-based application used in order to configure and monitor the software on security appliances. ASDM is loaded from the security appliance, and then used in order to configure, monitor, and manage the device. You can also use the ASDM Launcher in order to launch the ASDM application faster than the Java applet. This section describes the information you need in order to configure the features described in this document with ASDM.

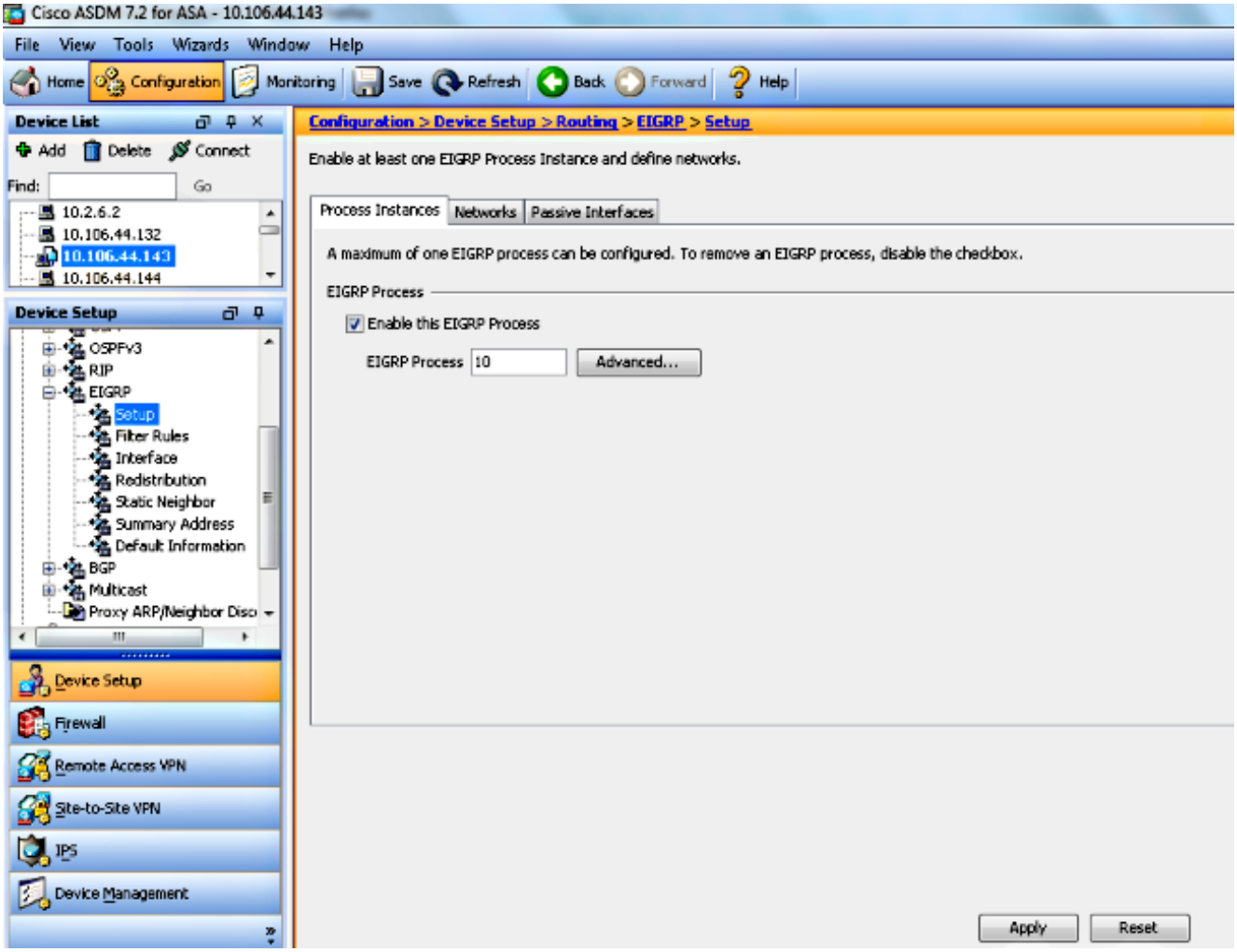
Complete these steps in order to configure EIGRP in the Cisco ASA.

1. Log in to the Cisco ASA with the ASDM.

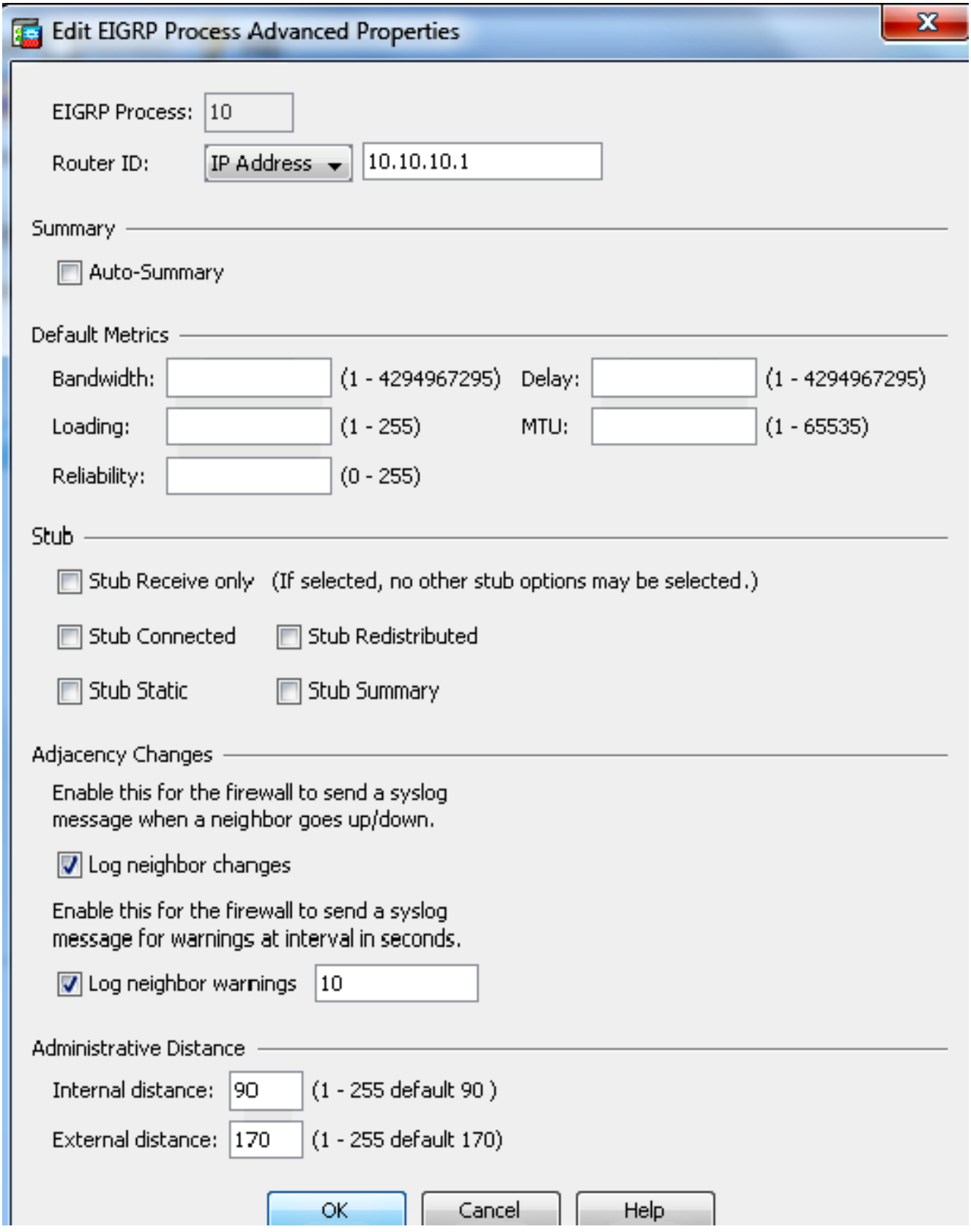
2. Navigate to the **Configuration > Device Setup > Routing > EIGRP** area of the ASDM interface, as shown in this screenshot.



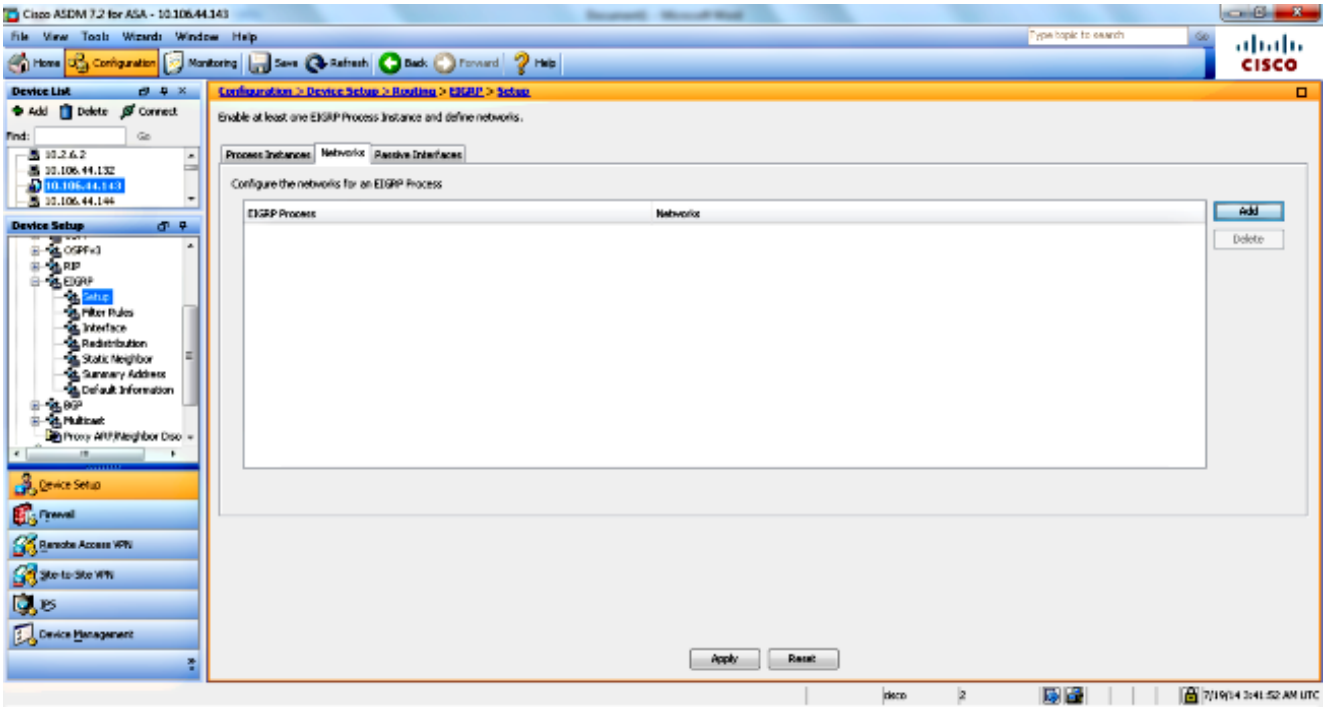
3. Enable the EIGRP routing process on the **Setup > Process Instances** tab, as shown in this screenshot. In this example, the EIGRP process is **10**.



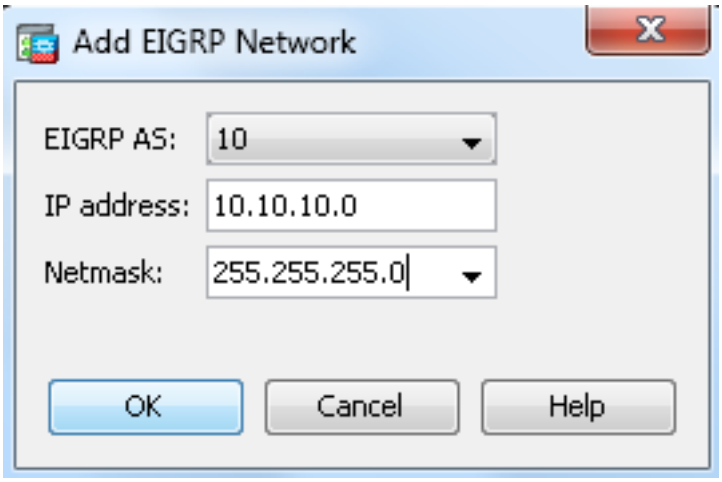
4. You can configure optional advanced EIGRP routing process parameters. Click **Advanced** on the **Setup > Process Instances** tab. You can configure the EIGRP routing process as a stub routing process, disable automatic route summarization, define the default metrics for redistributed routes, change the administrative distances for internal and external EIGRP routes, configure a static router ID, and enable or disable the logging of adjacency changes. In this example, the EIGRP Router ID is statically configured with the IP address of the inside interface (10.10.10.1). Additionally, **Auto-Summary** is also disabled. All other options are configured with their default values.



5. After you complete the previous steps, define the networks and interfaces that participate in EIGRP routing on the **Setup > Networks** tab. Click **Add** as shown in this screenshot.



6. This screen appears. In this example, the only network that you add is the inside network (10.10.10.0/24) since EIGRP is enabled only on the inside interface.



   Only interfaces with an IP address that falls within the defined networks participate in the EIGRP routing process. If you have an interface that you do not want to participate in EIGRP routing but that is attached to a network that you want advertised, configure a network entry on the **Setup > Networks** tab that covers the network to which the interface is attached, and then configure that interface as a passive interface so that the interface cannot send or receive EIGRP updates.

   Note: Interfaces configured as passive do not send or receive EIGRP updates.

7. You can optionally define route filters on the Filter Rules pane. Route filtering provides more control over the routes that are allowed to be sent or received in EIGRP updates.

8. You can optionally configure route redistribution. The Cisco ASA can redistribute routes discovered by Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) into the EIGRP routing process. You can also redistribute static and connected routes into the

EIGRP routing process. You do not need to redistribute static or connected routes if they fall within the range of a network configured on the **Setup > Networks** tab. Define route redistribution on the Redistribution pane.

9. EIGRP Hello packets are sent as multicast packets. If an EIGRP neighbor is located across a non-broadcast network, you must manually define that neighbor. When you manually define an EIGRP neighbor, Hello packets are sent to that neighbor as unicast messages. In order to define static EIGRP neighbors, go to the **Static Neighbor** pane.

10. By default, default routes are sent and accepted. In order to restrict or disable the sending and receiving of default route information, open the **Configuration > Device Setup > Routing > EIGRP > Default Information** pane. The Default Information pane displays a table of rules to control the sending and receiving of default route information in EIGRP updates.

    Note: You can have one "*in"* and one "*out*" rule for each EIGRP routing process. (Only one process is currently supported.)

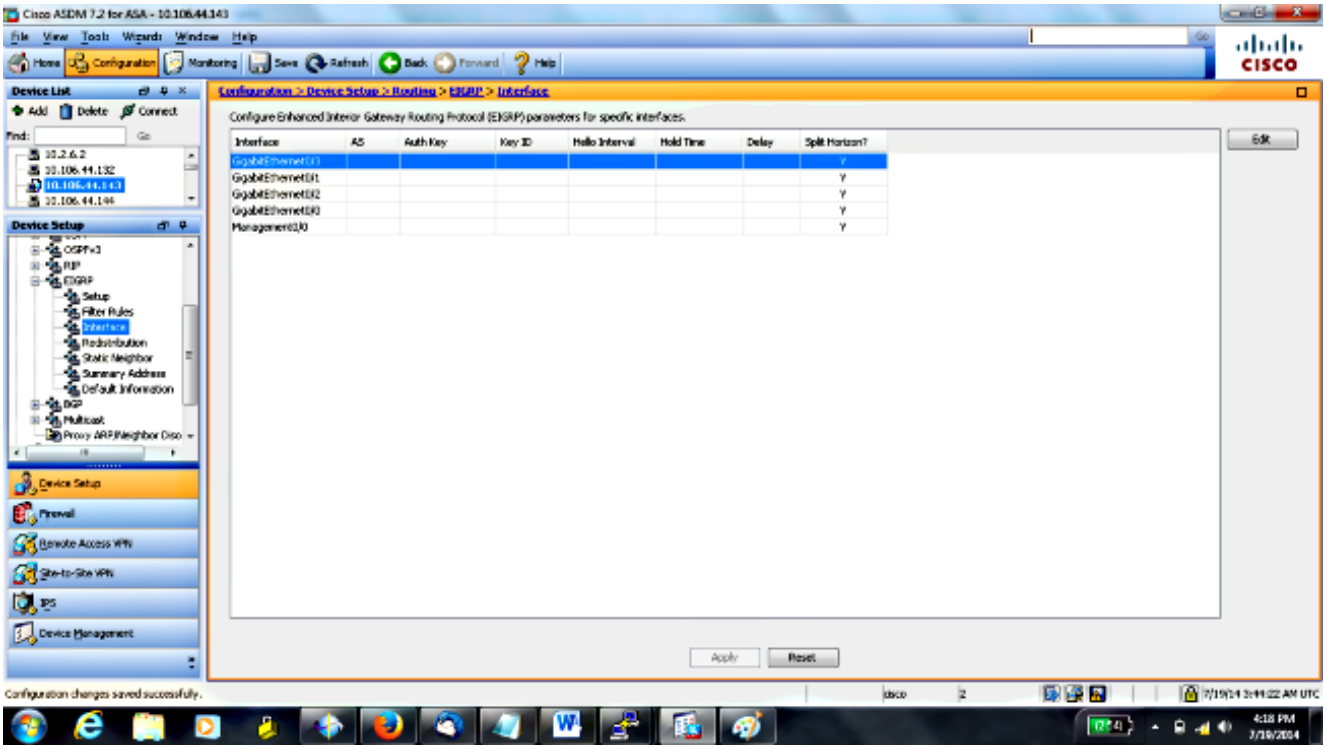
Configure EIGRP Authentication

The Cisco ASA supports MD5 authentication of routing updates from the EIGRP routing protocol. The MD5-keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources. The addition of authentication to your EIGRP messages ensures that your routers and the Cisco ASA only accept routing messages from other routing devices that are configured with the same pre-shared key. Without this authentication configured, if someone introduces another routing device with different or contrary route information on to the network, the routing tables on your routers or the Cisco ASA can become corrupt and a denial of service attack can ensue. When you add authentication to the EIGRP messages sent between your routing devices (which includes the ASA), it prevents the unauthorized additions of EIGRP routers into your routing topology.

EIGRP route authentication is configured on a per-interface basis. All EIGRP neighbors on interfaces configured for EIGRP message authentication must be configured with the same authentication mode and key for adjacencies to be established.

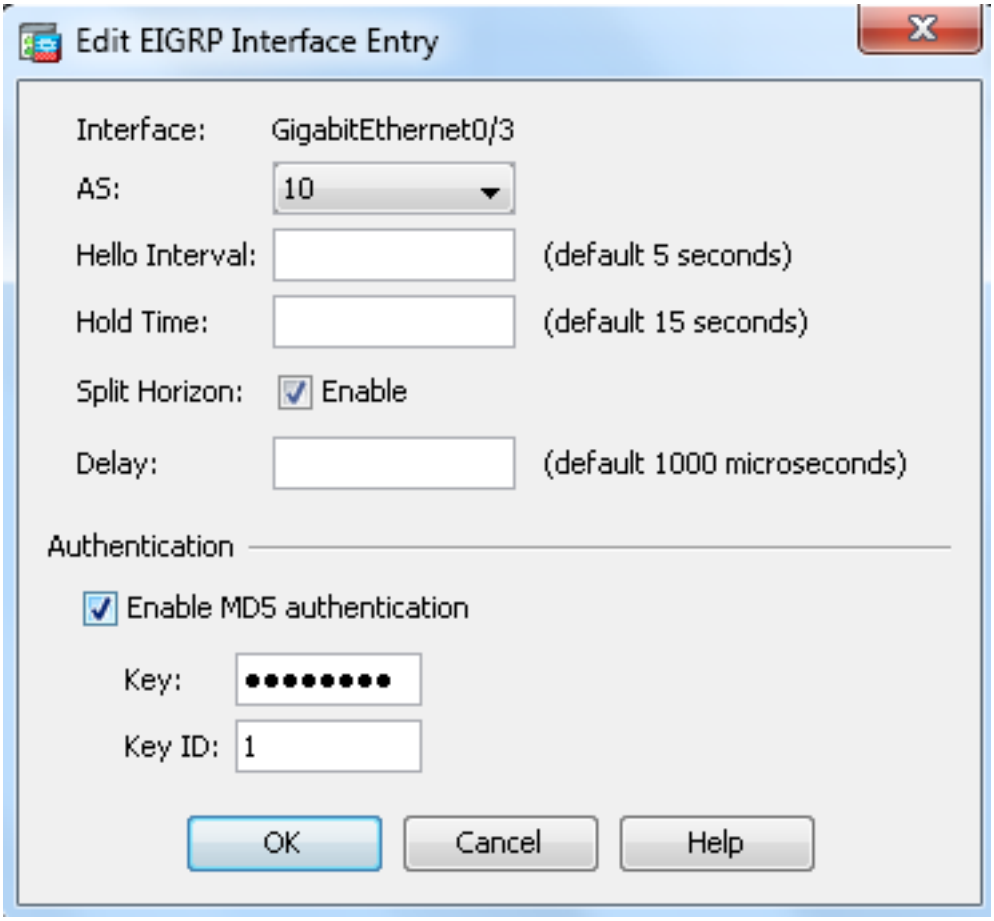
Complete these steps in order to enable EIGRP MD5 authentication on the Cisco ASA.

1. On the ASDM, navigate to **Configuration > Device Setup > Routing > EIGRP > Interface** as shown.



2. In this case, EIGRP is enabled on the inside interface (GigabitEthernet 0/1). Choose the **GigabitEthernet 0/1** interface and click **Edit**.

3. Under Authentication, choose **Enable MD5 authentication**. Add more information about the authentication parameters here. In this case, the preshared key is **cisco123**, and the key ID is **1**.



EIGRP Route Filtering

With EIGRP, you can control routing updates that are sent and received. In this example, you will block routing updates on the ASA for the network prefix 192.168.10.0/24, which is behind R1. For route-filtering, you can only use **STANDARD ACL**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

Verify

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Configurations

Cisco ASA CLI Configuration

This is the Cisco ASA CLI configuration.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
nameif management
security-level 99
ip address 10.10.20.1 255.255.255.0 management-only
!
!
```

```
!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Cisco IOS Router (R1) CLI Configuration

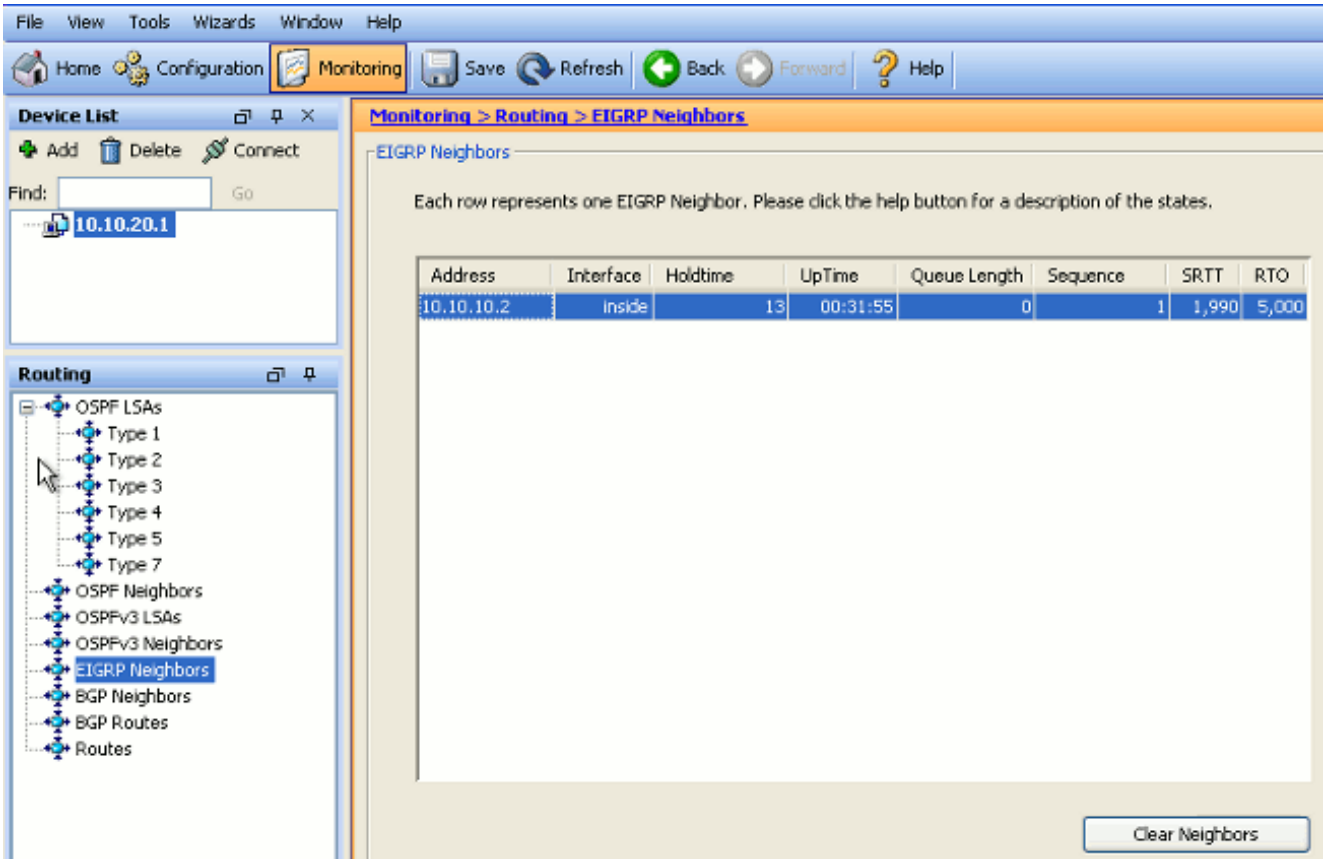
This is the CLI configuration of R1 (internal router).

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

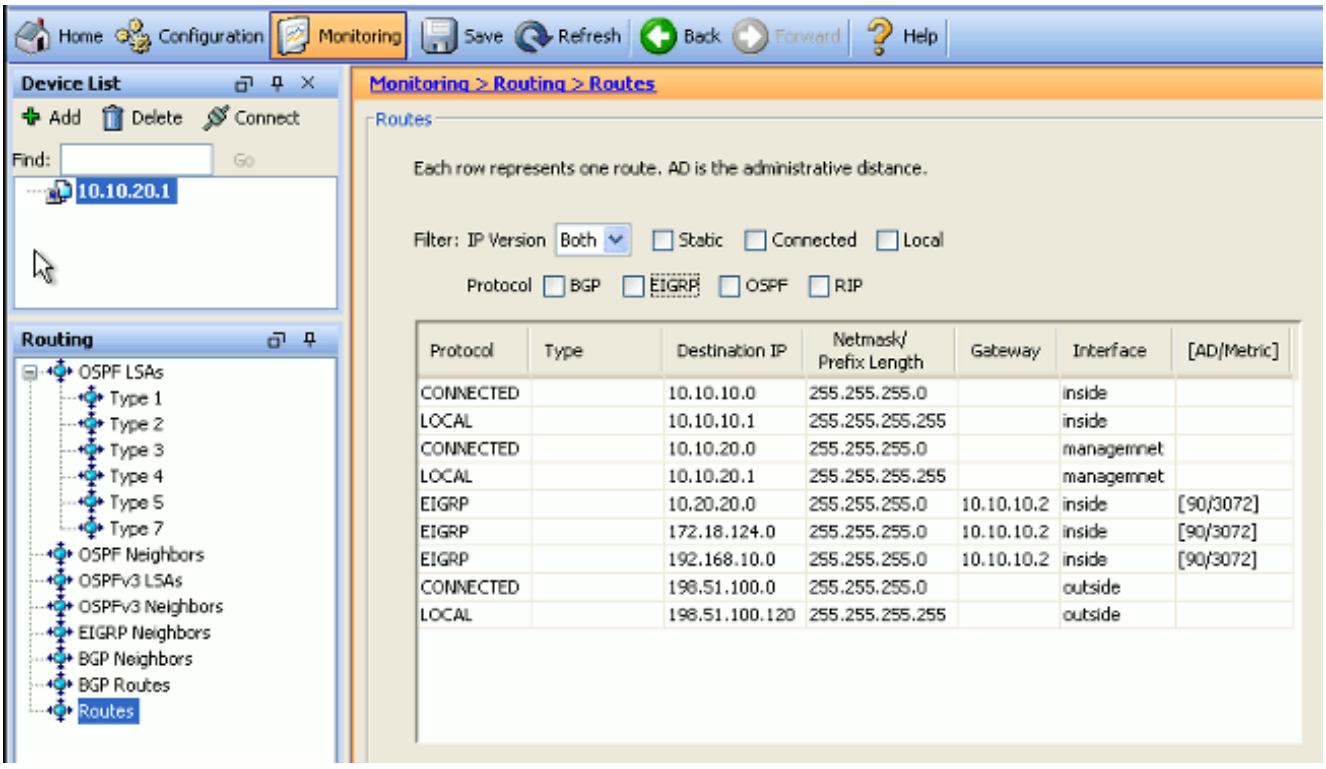
Verify

Complete these steps in order to verify your configuration.

1. On the ASDM, you can navigate to **Monitoring > Routing > EIGRP Neighbor** in order to see each of the EIGRP neighbors. This screenshot shows the inside router (R1) as an active neighbor. You can also see the interface where this neighbor resides, the holdtime, and how long the neighbor relationship has been up (UpTime).



2. Additionally, you can verify the routing table if you navigate to **Monitoring > Routing > Routes**. In this screenshot, you can see that the **192.168.10.0/24, 172.18.124.0/24**, and **10.20.20.0/24** networks are learned through R1 (**10.10.10.2**).



From the CLI, you can use the **show route** command in order to get the same output.

```
ciscoasa# show 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

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
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, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

With ASA Version 9.2.1 and later, you can use **show route eigrp** command in order to display only EIGRP routes.

```
ciscoasa(config)# show route eigrp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. You can also use the **show eigrp topology** command in order to obtain information about the learned networks and the EIGRP topology.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. The **show eigrp neighbors** command is also useful in order to verify the active neighbors and correspondent information. This example shows the same information you obtained from the ASDM in Step 1.

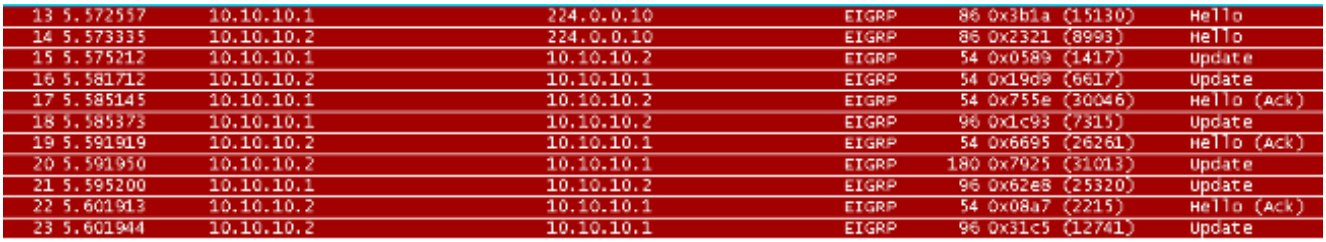
```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

Packet Flow

Here is the packet flow.

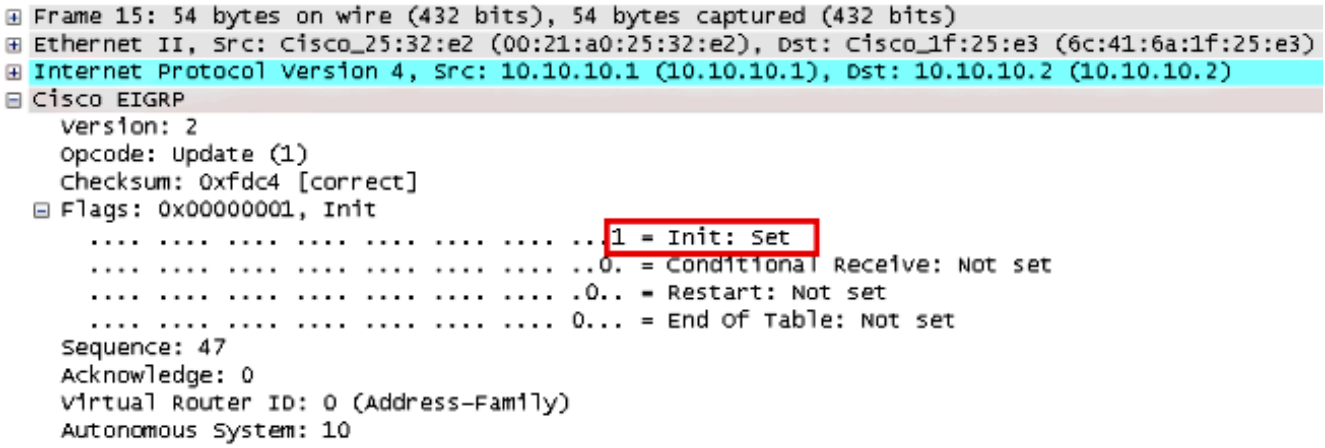
1. The ASA comes up on the link and sends a mCast Hello packet through all of its EIGRP-configured interfaces.

2. R1 receives a Hello packet and sends a mCast Hello packet.



3. The ASA receives Hello packet and sends an Update packet with an initial bit set, which indicates that this is the initialization process.

4. R1 receives an Update packet and sends an Update packet with an initial bit set, which indicates that this is the initialization process.

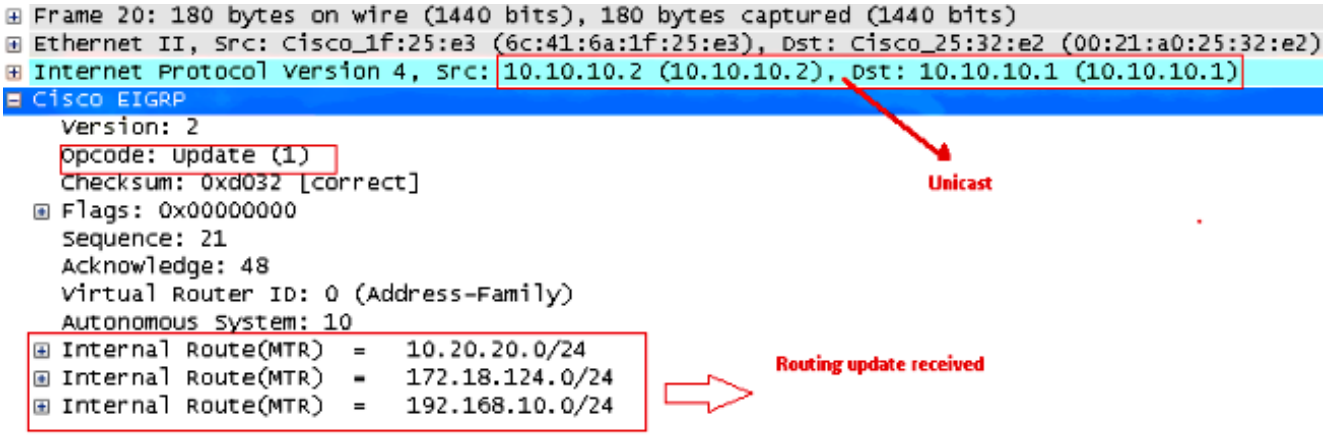


5. After both the ASA and R1 have exchanged hellos and the neighbor adjacency is established, both the ASA and R1 reply with an ACK packet, which indicates that the update information was received.

6. ASA sends its routing information to R1 in an Update packet.

7. R1 inserts the Update packet information in its topology table. The topology table includes all destinations advertised by neighbors. It is organized so that each destination is listed, along with all of the neighbors that can travel to the destination and their associated metrics.

8. R1 then sends an Update packet to the ASA.



9. Once it receives the Update packet, the ASA sends an ACK packet to R1. After the ASA and R1 successfully receive the Update packets from each other, they are ready to chose the successor (best) and feasible successor (backup) routes in the topology table, and offer the successor routes to the routing table.

Troubleshoot

This section includes information about **debug** and **show** commands that can be useful in order to troubleshoot EIGRP problems.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands. In order to display debug information the Diffusing Update Algorithm (DUAL) finite state machine, use the **debug eigrp fsm** command in privileged EXEC mode. This command lets you observe EIGRP feasible successor activity and determine whether route updates are installed and deleted by the routing process.

This is the output of the **debug** command within the successful peering with R1. You can see each of the different routes that is successfully installed on the system.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
```

```
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

You can also use the **debug eigrp neighbor** command. This is the output of this **debug** command when the Cisco ASA successfully created a new neighbor relation with R1.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

You can also use the debug EIGRP packets for detailed EIGRP message exchange information between the Cisco ASA and its peers. In this example, the authentication key was changed on the router (R1), and the debug output shows you that the problem is an authentication mismatch.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

EIGRP Neighborship Goes Down with Syslogs ASA-5-336010

ASA drops EIGRP neighborship when any changes in the EIGRP distribution list are made. This Syslog message is seen.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

With this configuration, whenever a **new acl entry is added** in the ACL, the **Eigrp-network-list** EIGRP neighborship is reset.

```
router eigrp 10
distribute-list Eigrp-network-list in
```

```
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

You can observe that the neighbor relationship is up with the adjacent device.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

Now you can add **access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0**.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

These logs can be seen in **debug eigrp fsm**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

This is expected behavior in all new ASA Versions from 8.4 and 8.6 to 9.1. The same has been observed in routers that run the 12.4 to 15.1 code trains. However, this behavior is not observed in ASA Version 8.2 and earlier ASA software versions because changes made to an ACL do not reset the EIGRP adjacencies.

Since EIGRP sends the full topology table to a neighbor when the neighbor first comes up, and then it sends only the changes, configuring a distribute list with the event-driven nature of EIGRP would make it difficult for the changes to apply without a full reset of the neighbor relationship. The routers would need to keep track of every route sent to and received from a neighbor in order to know which route has changed (that is, would or would not be sent/accepted) in order to apply the changes as dictated by the current distribute list. It is much easier to simply tear down and reestablish the adjacency between neighbors.

When an adjacency is torn down and reestablished, all learned routes between particular neighbors are simply forgotten and the entire synchronization between the neighbors is performed anew - with the new distribute list in place.

Most of the EIGRP techniques that you use in order to troubleshoot Cisco IOS routers can be applied on the Cisco ASA. In order to troubleshoot EIGRP, use the Main Troubleshooting Flowchart; start at the box marked **Main**.