

PIX/ASA 8.X: Configuring EIGRP on the Cisco Adaptive Security Appliance (ASA)

Document ID: 91264

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Adaptive Security Device Manager (ASDM) Configuration
- Configure EIGRP Authentication
- Cisco ASA CLI Configuration
- Cisco IOS Router (R1) CLI Configuration

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

The Cisco Adaptive Security Appliance (ASA) software Version 8.0 and later supports the Enhanced Interior Gateway Routing Protocol (EIGRP). This document explains how to configure the Cisco ASA to learn routes through EIGRP and perform authentication.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Cisco ASA must run Version 8.x or later.
- EIGRP is not supported in multi-context mode; it is supported only in single mode.

Components Used

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

- Cisco Adaptive Security Appliance Software Version 8.0(2)
- Cisco Adaptive Security Device Manager 6.0(2)
- 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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

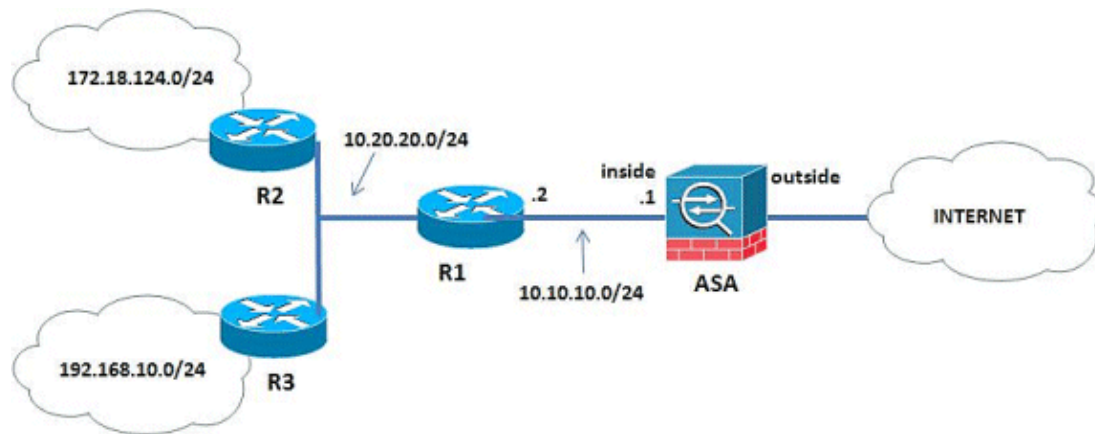
Configure

In this section, you are presented with the information to configure the features described in this document.

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

Network Diagram

This document uses this network setup:



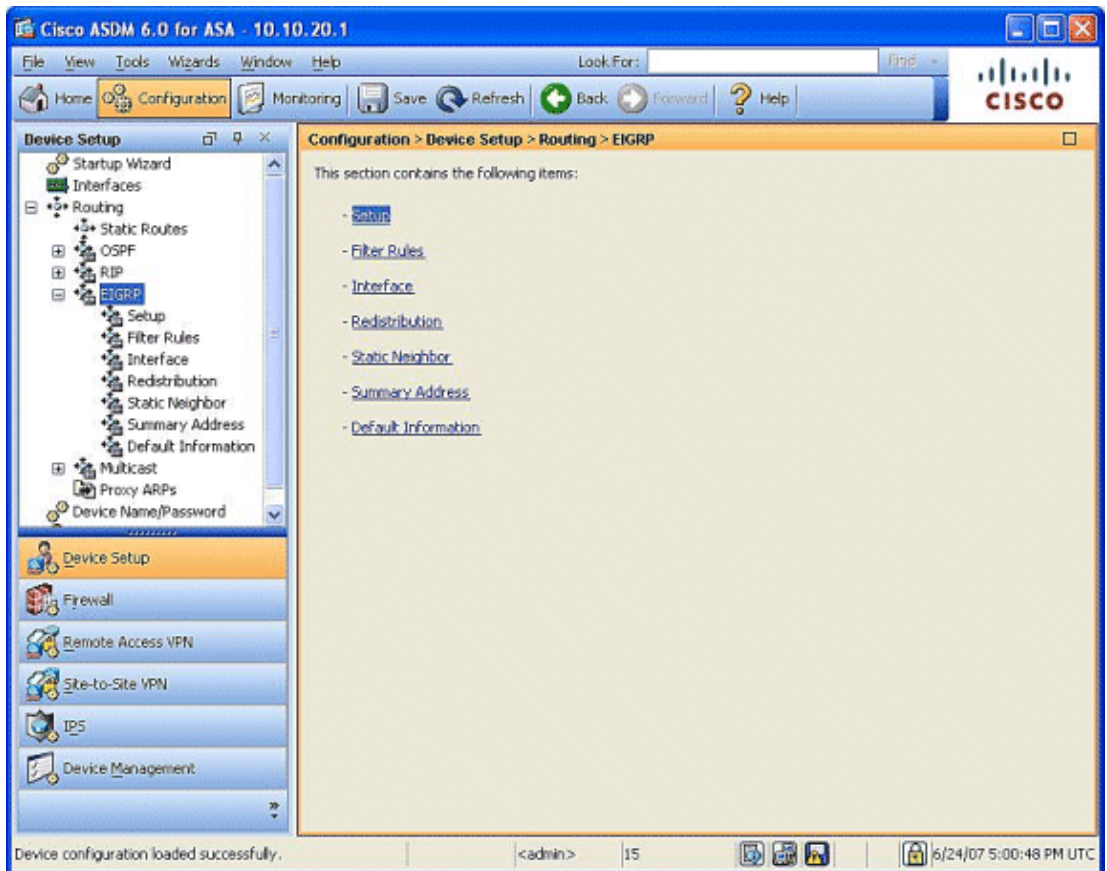
In the network topology that is illustrated, the Cisco ASA inside interface IP address is 10.10.10.1/24. The goal is to configure EIGRP on the Cisco ASA to learn routes to the internal networks (10.20.20.0/24, 172.18.124.0/24, and 192.168.10.0/24) dynamically through the adjacent router (R1). R1 learns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

Adaptive Security Device Manager (ASDM) Configuration

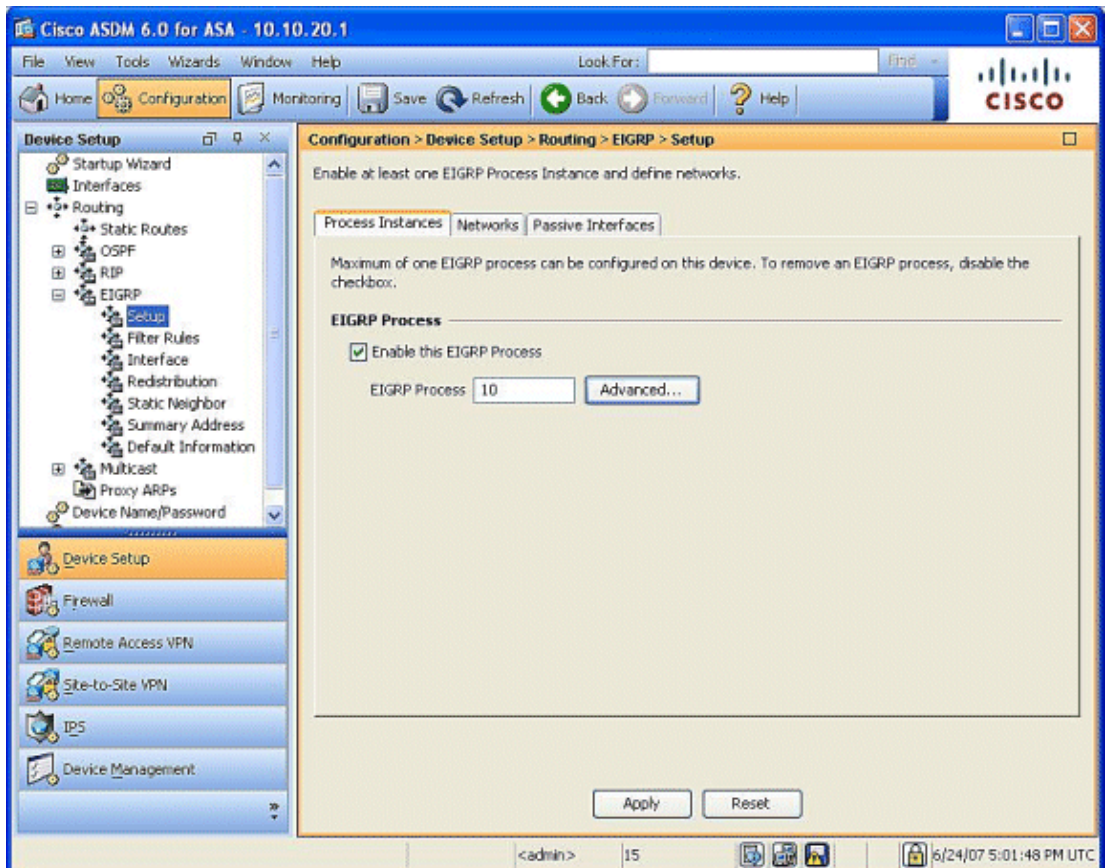
Adaptive Security Device Manager (ASDM) is a browser-based application used to configure and monitor the software on security appliances. ASDM is loaded from the security appliance, and then used to configure, monitor, and manage the device. You can also use the ASDM Launcher (Windows[®] only) to launch the ASDM application faster than the Java applet. This section describes the information you need to configure the features described in this document with ASDM.

Complete these steps to configure EIGRP in the Cisco ASA.

1. Log in to the Cisco ASA with ASDM.
2. Navigate to the **Configuration > Device Setup > Routing > EIGRP** area of the ASDM interface, as shown in the screenshot.



3. Enable the EIGRP routing process on the **Setup > Process Instances** tab, as shown in the 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.

Edit EIGRP Process Advanced Properties

EIGRP: Router Id:

Summary

Auto-Summary

Default Metrics

Bandwidth: (1 - 4294967295) Delay: (1 - 4294967295)
Loading: (1 - 255) MTU: (1 - 65535)
Reliability: (0 - 255)

Stub

Stub Receive only (If selected, no other stub options may be selected.)
 Stub Connected Stub Redistributed
 Stub Static Stub Summary

Adjacency Changes

Enable this for the firewall to send a syslog message when a neighbor goes up/down.

Log neighbor changes

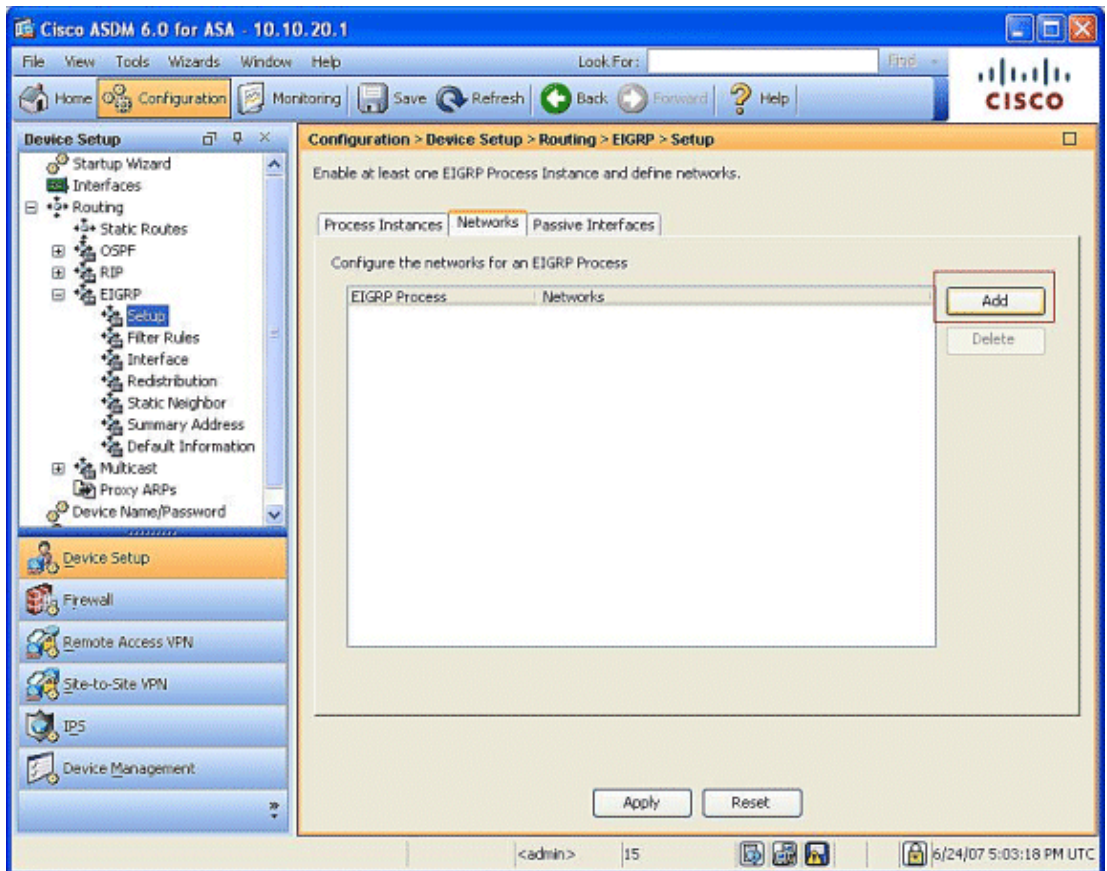
Enable this for the firewall to send a syslog message for warnings at interval in seconds.

Log neighbor warnings

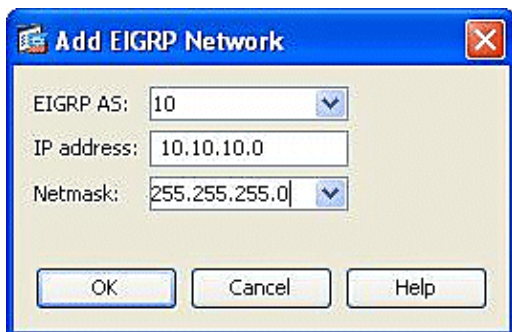
Administrative Distance

Internal distance: (1 - 255 default 90)
External distance: (1 - 255 default 170)

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 we 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 fall 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 RIP and 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 nonbroadcast 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.)

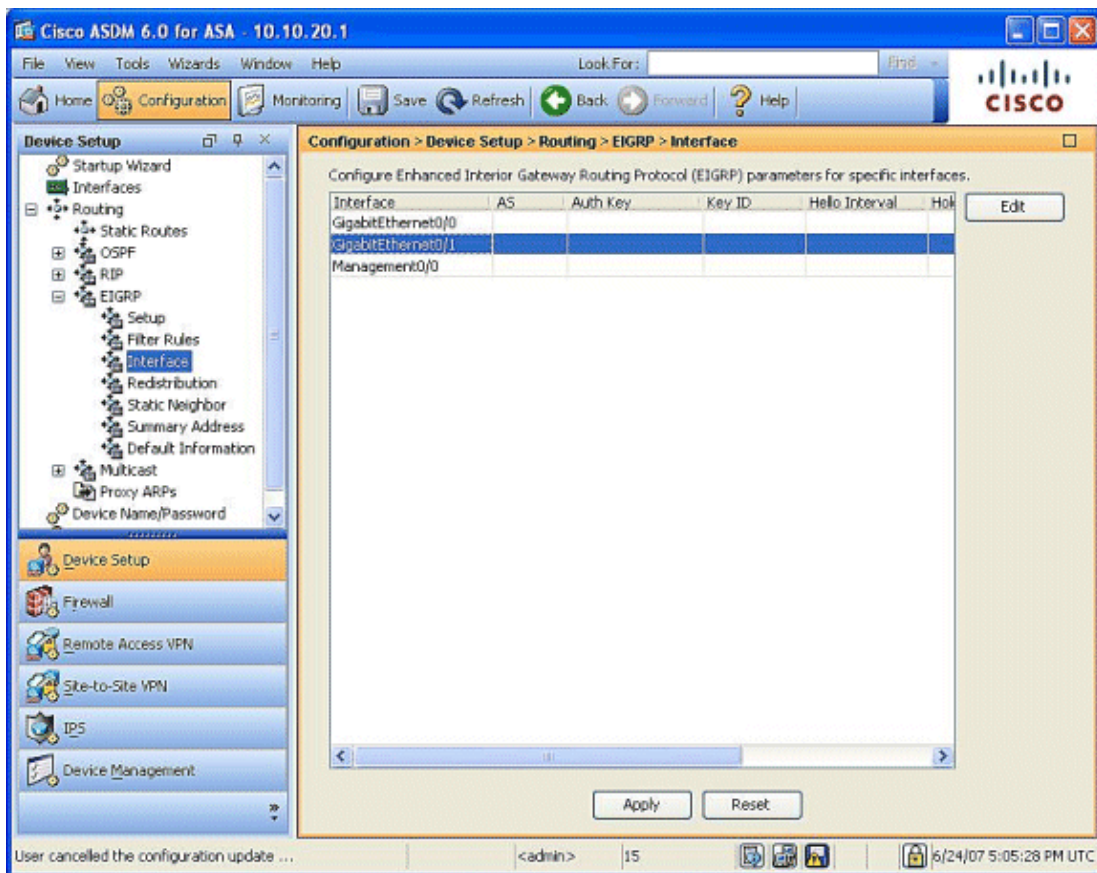
Configure EIGRP Authentication

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 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 purposeful or accidental addition of another router to the network and any problem.

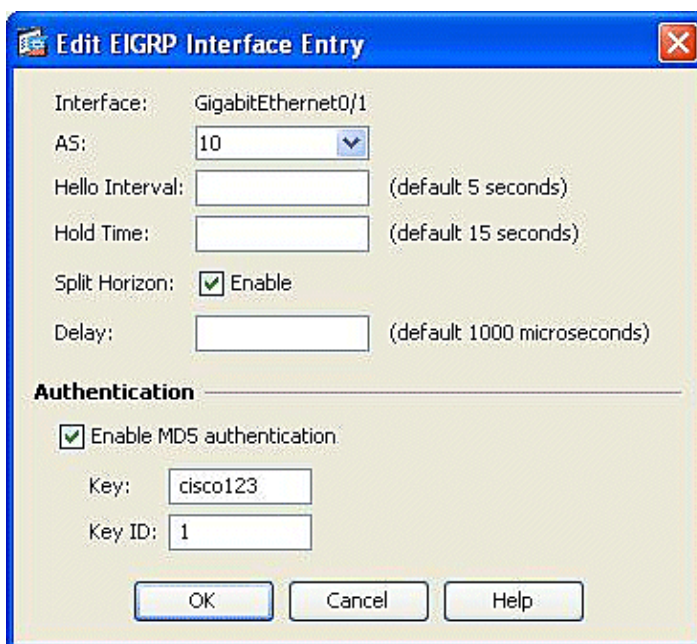
EIGRP route authentication is configured on a per-interface basis. All EIGRP neighbors on interfaces configured for EIGRP message authentication must be configured with the same authentication mode and key for adjacencies to be established.

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

1. On 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 authentication parameters here. In this case, the preshared key is **cisco123**, and the key ID is **1**.



Cisco ASA CLI Configuration

This is the Cisco ASA CLI configuration:

Cisco ASA CLI Configuration

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 100.10.10.1 255.255.255.0
!

!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 0.0.0.0 100.10.10.2 1
```

Cisco IOS Router (R1) CLI Configuration

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

Cisco IOS Router (R1) CLI Configuration

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

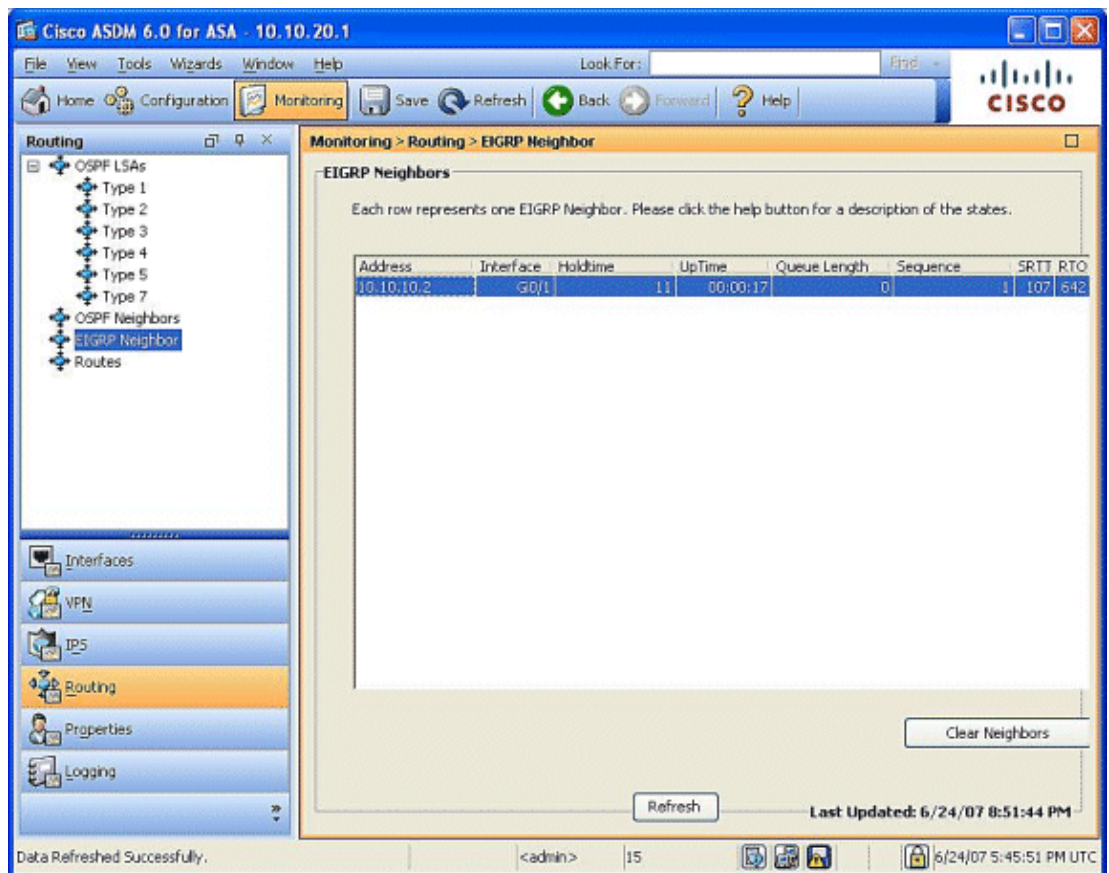
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
```

```
!  
!  
  
! 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
```

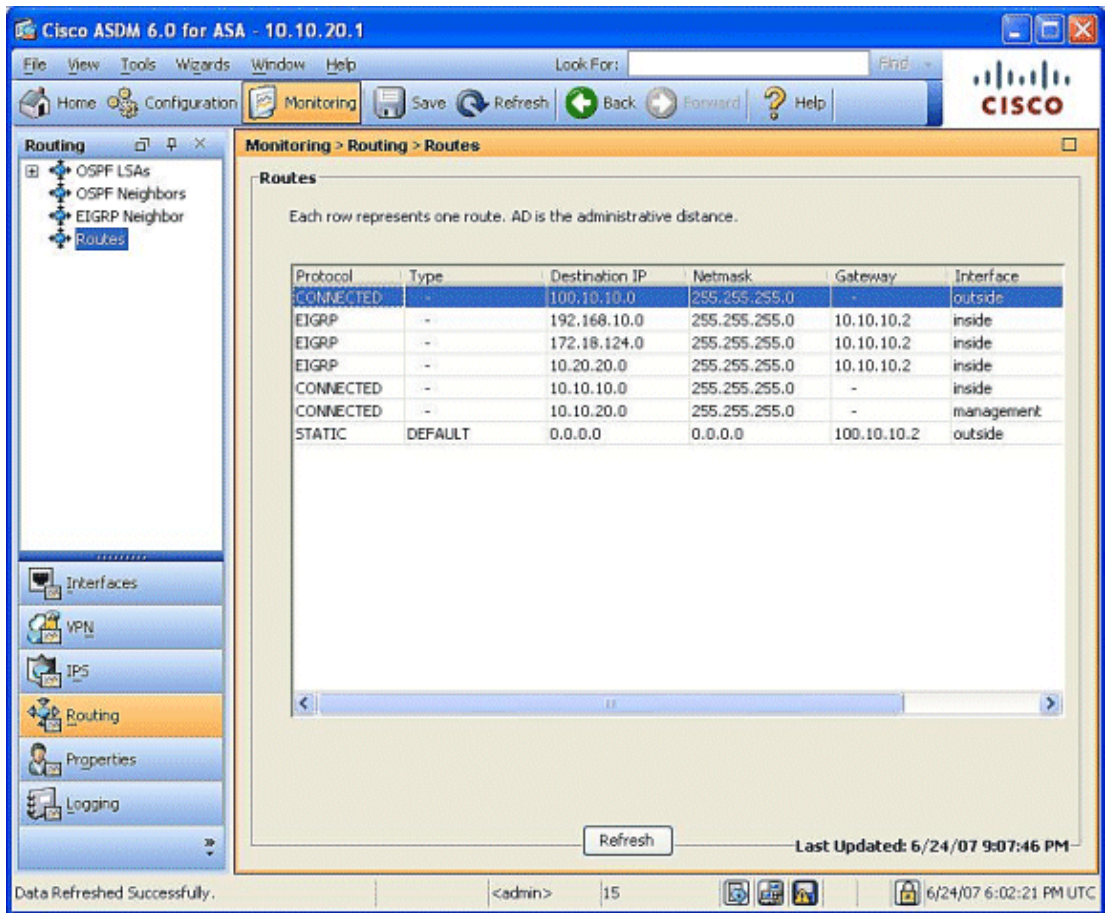
Verify

Complete these steps to verify your configuration.

1. On ASDM you can navigate to **Monitoring > Routing > EIGRP Neighbor** 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**).



3. From the CLI, you can use the **show route** command 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    100.10.10.0 255.255.255.0 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 100.10.10.2, outside
ciscoasa#
```

4. You can also use the **show eigrp topology** command to obtain information about the learned networks and 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
ciscoasa#

```

5. The **show eigrp neighbors** command is also useful to verify the active neighbors and correspondent information. This example shows the same information you obtained from ASDM on 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

```

Troubleshoot

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

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT 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 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.

```

ciscoasa# 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 4294967295 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 topoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967295 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 topoid 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 4294967295 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 topoid 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 GigabitEthernet0/1
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)

```

Most of the EIGRP techniques that you use to troubleshoot Cisco IOS routers can be applied on the Cisco ASA. In order to troubleshoot EIGRP, use the flowchart at this link; start at the box marked **Main**. Dependent upon the symptoms, the flowchart can refer to one of the three flowcharts later in this document or to other relevant documents on Cisco.com. There are some problems that possibly are not resolvable here. In these cases, links are provided to Cisco Technical Support. In order to open a service request, you must have a valid service contract.

Related Information

- **Technical Support & Documentation – Cisco Systems**

Contacts & Feedback | Help | Site Map

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Apr 02, 2007

Document ID: 91264
