EIGRP Message Authentication Configuration Example

Document ID: 82110

This document was contributed by Cliff Stewart of PBM IT Solutions.

Contents

Introduction

This document illustrates how to add message authentication to your Enhanced Interior Gateway Routing Protocol (EIGRP) routers and protect the routing table from willful or accidental corruption.

The addition of authentication to your routers' EIGRP messages ensures that your routers only accept routing messages from other routers that know the same pre−shared key. Without this authentication configured, if someone introduces another router with different or conflicting route information on to the network, the routing tables on your routers could become corrupt and a denial of service attack could ensue. Thus, when you add authentication to the EIGRP messages sent between your routers, it prevents someone from purposely or accidentally adding another router to the network and causing a problem.

Caution: When EIGRP message authentication is added to the interface of a router, that router stops receiving routing messages from its peers until they are also configured for message authentication. This **does** interrupt routing communications on your network. See Messages When Only Dallas is Configured for more information.

Prerequisites

Requirements

- The time must be properly configured on all routers. Refer to Configuring NTP for more information.
- A working EIGRP configuration is recommended.

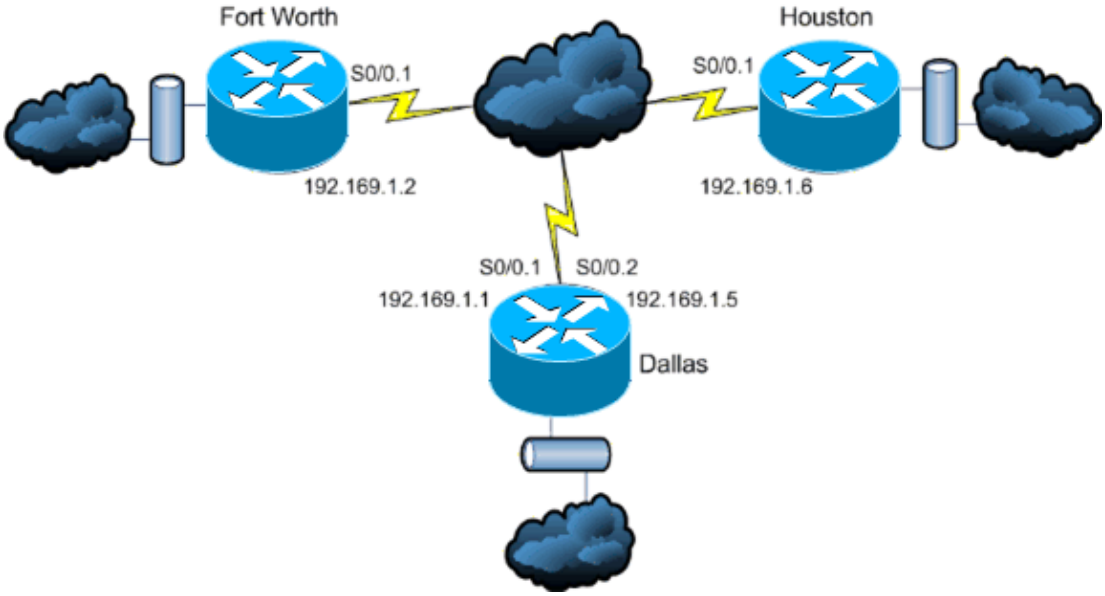
Components Used

The information in this document is based on Cisco IOS® Software Release 11.2 and later.

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.

Network Diagram

This document uses this network setup:



Conventions

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

Background Information

In this scenario a network administrator wants to configure authentication for EIGRP messages between the hub router in Dallas and the remote sites in Fort Worth and Houston. The EIGRP configuration (without authentication) is already complete on all three routers. This example output is from Dallas:

```
Dallas#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
1   192.169.1.6             Se0/0.2       11 15:59:57   44   264  0  2
0   192.169.1.2             Se0/0.1       12 16:00:40   38   228  0  3
Dallas#show cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Houston          Ser 0/0.2          146          R        2611      Ser 0/0.1
FortWorth        Ser 0/0.1          160          R        2612      Ser 0/0.1
```

Configure EIGRP Message Authentication

The configuration of EIGRP message authentication consists of two steps:

1. The creation of a keychain and key.
2. The configuration of EIGRP authentication to use that keychain and key.

This section illustrates the steps to configure EIGRP message authentication on the Dallas router and then the Fort Worth and Houston routers.

Create a Keychain on Dallas

Routing authentication relies on a key on a keychain to function. Before authentication can be enabled, a keychain and at least one key must be created.

1. Enter global configuration mode.

   ```
   Dallas#configure terminal
   ```
2. Create the key chain. **MYCHAIN** is used in this example.

   ```
   Dallas(config)#key chain MYCHAIN
   ```
3. Specify the key number. **1** is used in this example.

   Note: It is recommended that the key number be the same on all routers involved in the configuration.

   ```
   Dallas(config-keychain)#key 1
   ```
4. Specify the key-string for the key. **securetraffic** is used in this example.

   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```
5. End the configuration.

   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Configure Authentication on Dallas

Once you create a keychain and key, you must configure EIGRP to perform message authentication with the key. This configuration is completed on the interfaces that EIGRP is configured on.

Caution: When EIGRP message authentication is added to the Dallas interfaces, it stops receiving routing messages from its peers until they are also configured for message authentication. This **does** interrupt routing communications on your network. See Messages When Only Dallas is Configured for more information.

1. Enter global configuration mode.

   ```
   Dallas#configure terminal
   ```
2. From global configuration mode, specify the interface that you want to configure EIGRP message authentication on. In this example the first interface is **Serial 0/0.1**.

```
Dallas(config)#interface serial 0/0.1
```

3. Enable EIGRP message authentication. The **10** used here is the autonomous system number of the network. **md5** indicates that the md5 hash is to be used for authentication.

```
Dallas(config-subif)#ip authentication mode eigrp 10 md5
```

4. Specify the keychain that should be used for authentication. **10** is the autonomous system number. **MYCHAIN** is the keychain that was created in the Create a Keychain section.

```
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
```

5. Complete the same configuration on interface Serial 0/0.2.

```
Dallas#configure terminal
Dallas(config)#interface serial 0/0.2
Dallas(config-subif)#ip authentication mode eigrp 10 md5
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
Dallas#
```

Configure Fort Worth

This section shows the commands necessary to configure EIGRP message authentication on the Fort Worth router. For more detailed explanation of the commands shown here, see Create a Keychain on Dallas and Configure Authentication on Dallas.

```
FortWorth#configure terminal
FortWorth(config)#key chain MYCHAIN
FortWorth(config-keychain)#key 1
FortWort(config-keychain-key)#key-string securetraffic
FortWort(config-keychain-key)#end
FortWorth#
Fort Worth#configure terminal
FortWorth(config)#interface serial 0/0.1
FortWorth(config-subif)#ip authentication mode eigrp 10 md5
FortWorth(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
FortWorth(config-subif)#end
FortWorth#
```

Configure Houston

This section shows the commands necessary to configure EIGRP message authentication on the Houston router. For more detailed explanation of the commands shown here, see Create a Keychain on Dallas and Configure Authentication on Dallas.

```
Houston#configure terminal
Houston(config)#key chain MYCHAIN
Houston(config-keychain)#key 1
Houston(config-keychain-key)#key-string securetraffic
Houston(config-keychain-key)#end
Houston#
Houston#configure terminal
Houston(config)#interface serial 0/0.1
Houston(config-subif)#ip authentication mode eigrp 10 md5
Houston(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Houston(config-subif)#end
Houston#
```

Verify

Use this section to confirm that your configuration works properly.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Messages When Only Dallas is Configured

Once EIGRP message authentication is configured on the Dallas router, that router begins to reject messages from the Fort Worth and Houston routers because they do not yet have authentication configured. This can be verified by issuing a **debug eigrp packets** command on the Dallas router:

```
Dallas#debug eigrp packets
17:43:43: EIGRP: ignored packet from 192.169.1.2 (invalid authentication)
17:43:45: EIGRP: ignored packet from 192.169.1.6 (invalid authentication)

!--- Packets from Fort Worth and Houston are ignored because they are
!--- not yet configured for authentication.
```

Messages When All Routers are Configured

Once EIGRP message authentication is configured on all three routers, they begin to exchange EIGRP messages again. This can be verified by issuing a **debug eigrp packets** command once again. This time outputs from the Fort Worth and Houston routers are shown:

```
FortWorth#debug eigrp packets
00:47:04: EIGRP: received packet with MD5 authentication, key id = 1
00:47:04: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.1

!--- Packets from Dallas with MD5 authentication are received.


Houston#debug eigrp packets
 00:12:50.751: EIGRP: received packet with MD5 authentication, key id = 1
 00:12:50.751: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.5

!--- Packets from Dallas with MD5 authentication are received.
```

Troubleshoot

Unidirectional Link

You must configure EIGRP Hello and Hold−time timers on both ends. If you configure the timers only on one end, a unidirectional link occurs.

A router on a unidirectional link might be able to receive hello packets. However, the hello packets sent out are not received at the other end. This unidirectional link is usually indicated by *retry limit exceeded* messages on one end.

In order to view the *retry limit exceeded* messages, use the **debug eigrp packet** and **debug ip eigrp notifications** commands.

Related Information

- **Enhanced Interior Gateway Routing Protocol (EIGRP) Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 01, 2007 Document ID: 82110