# EIGRP メッセージ認証の設定例

## 内容



## 概要

このドキュメントでは、Enhanced IGRP ( EIGRP ) ルータにメッセージ認証を追加する方法と、ルーティング テーブルを故意の破損や偶発的な破損から保護する方法を説明しています。

ルータの EIGRP メッセージに認証を追加することにより、ルータでは、同じ事前共有キーが認識されている他のルータからのルーティング メッセージのみが受け入れられるようになります。この認証を設定していないと、別のユーザが他のルート情報または矛盾するルート情報を使用して他のルータをネットワークに導入した場合に、ルータのルーティング テーブルが破損され、DoS 攻撃を受ける危険性があります。そのため、ルータ間を送信される EIGRP メッセージに認証を追加することにより、ネットワークに他のルータが意図的にまたは誤って追加され、問題が発生することを防ぐことができます。

**注意**：EIGRPメッセージ認証がルータのインターフェイスに追加されると、そのルータはメッセージ認証用にも設定されるまで、ピアからのルーティングメッセージの受信を停止します。これにより、ネットワーク上のルーティング通信が中断されます。詳細は、「Dallas のみ設定した場合のメッセージ」を参照してください。

## 前提条件

## 要件

- すべてのルータで時刻を正確に設定する必要があります。詳細については、「NTP の設定」を参照してください。
- 実稼働中の EIGRP の設定が推奨されます。

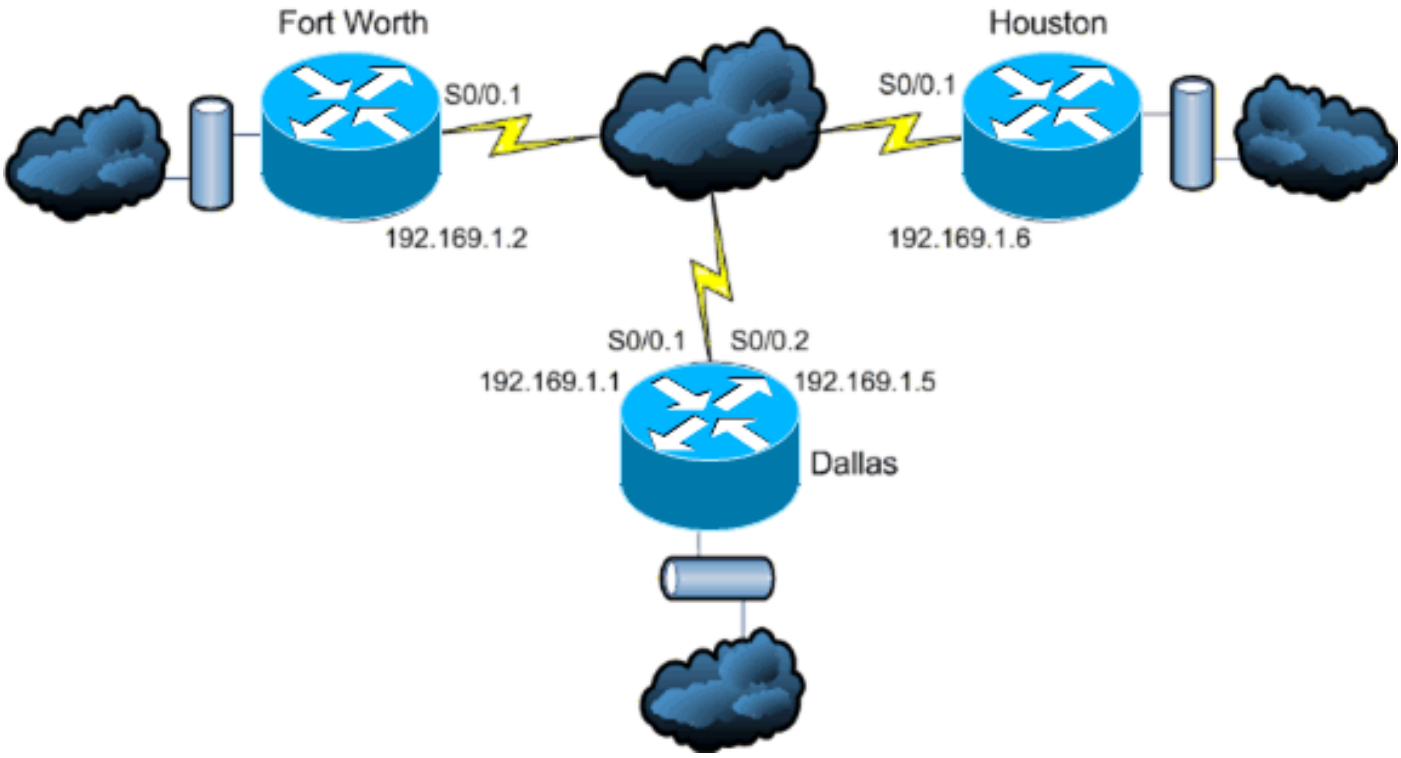
## 使用するコンポーネント

このドキュメントの情報は、Cisco IOS® ソフトウェア リリース 11.2 以降に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。




## 表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

# 背景説明

このシナリオでは、ネットワーク管理者は、Dallas に設置されているハブ ルータと Fort Worth および Houston のリモート サイトの間でやりとりされる EIGRP メッセージの認証を設定したいと考えています。これら 3 つのルータでは、EIGRP 設定（認証なし）はすでに完了しています。

次の出力例は、Dallas に設置されているルータのものです。

```
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
```

# EIGRP メッセージ認証の設定

EIGRP メッセージ認証の設定は、次の 2 つのステップから構成されています。

1. キーチェーンとキーを作成する。
2. 作成したキーチェーンとキーを使用するように EIGRP 認証を設定する。

このセクションでは、EIGRP メッセージ認証を、Dallas に設置されているルータで設定してから、Fort Worth と Houston に設置されているルータで設定する手順を示しています。

## Dallas でのキーチェーンの作成

ルーティング認証が機能するためには、キーチェーン上のキーが必要です。認証を有効にする前に、キーチェーンと少なくとも 1 つのキーを作成する必要があります。

1. グローバル コンフィギュレーション モードに入ります。
   ```
   Dallas#configure terminal
   ```
2. キーチェーンを作成します。**この例では、「MYCHAIN」を使用しています。**
   ```
   Dallas(config)#key chain MYCHAIN
   ```
3. キー番号を指定します。**この例では、「1」を使用しています。注：キー**番号は、設定に関係するすべてのルータで同じにすることを推奨します。
   ```
   Dallas(config-keychain)#key 1
   ```
4. キーのキー ストリングを指定します。**この例では、「securetraffic」を使用しています。**
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```
5. 設定が完了しました。
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

## Dallas での認証の設定

キーチェーンとキーを作成したら、そのキーを使用してメッセージ認証を行うように EIGRP を設定する必要があります。EIGRP が設定されているインターフェイスではこの設定が完了しています。

**注意**：EIGRPメッセージ認証がDallasインターフェイスに追加されると、メッセージ認証用にも設定されるまで、ピアからのルーティングメッセージの受信が停止されます。これにより、ネットワーク上のルーティング通信が中断されます。詳細は、「Dallas のみ設定した場合のメッセージ」を参照してください。

1. グローバル コンフィギュレーション モードに入ります。
```
Dallas#configure terminal
```

2. グローバル コンフィギュレーション モードで、EIGRP メッセージ認証を設定するインターフェイスを指定します。この例では、最初のインターフェイスは「Serial 0/0.1」です。
```
Dallas(config)#interface serial 0/0.1
```

3. EIGRP メッセージ認証をイネーブルにします。ここで使用されている「10」は、ネットワークの自律システム番号です。md5 は、MD5 ハッシングを認証に使用することを示しています。
```
Dallas(config-subif)#ip authentication mode eigrp 10 md5
```

4. 認証に使用するキーチェーンを指定します。「10」は自律システム番号です。「MYCHAIN」は、[Create a Keychain] セクションで作成したキーチェーンです。
```
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
```

5. インターフェイス Serial 0/0.2 で同じ設定を行います。
```
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#
```

## Fort Worth の設定

このセクションでは、Fort Worth に設置されているルータで EIGRP メッセージ認証を設定するために必要なコマンドを説明しています。ここで示すコマンドの詳しい説明は、「Dallas でのキーチェーンの作成」と「Dallas での認証の設定」を参照してください。

```
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#
```

## Houston の設定

このセクションでは、Houston に設置されているルータで EIGRP メッセージ認証を設定するために必要なコマンドを説明しています。ここで示すコマンドの詳しい説明は、「Dallas でのキーチェーンの作成」と「Dallas での認証の設定」を参照してください。

```
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#
```

# 確認

ここでは、設定が正常に機能しているかどうかを確認します。

**注：**debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

## Dallas のみ設定した場合のメッセージ

Dallas に設置されているルータで EIGRP メッセージ認証が設定されると、そのルータでは Fort Worth と Houston に設置されているルータからのメッセージが拒否されるようになります。これは、これらのルータではまだ認証が設定されていないためです。このことは、Dallas に設置されているルータで **debug eigrp packets コマンドを発行すると確認できます。**

```
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.
```

## すべてのルータを設定した場合のメッセージ

3 つのルータすべてで EIGRP メッセージ認証が設定されると、再び EIGRP メッセージがやりとりされるようになります。このことは、再び **debug eigrp packets コマンドを発行すると確認できます。**この場合、Fort Worth と Houston に設置されているルータからの出力は、次のようになります。

```
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.
```

# トラブルシュート

## 単方向リンク

両端で、EIGRP Hello および保留時間タイマーを設定する必要があります。一方でのみタイマーを設定すると、単方向リンクが発生します。

単方向リンク上のルータは、Hello パケットを受信できる場合があります。ただし、送り出された Hello パケットはもう一方の端では受信されません。通常、この単方向リンクは、*retry limit exceeded メッセージが一方の側に表示されることでわかります。*

*retry limit exceeded メッセージを表示するには、*debug eigrp packet および debug ip eigrp notifications コマンドを使用します。

## 関連情報

- Enhanced IGRP ( EIGRP ) テクノロジーに関するサポート
- テクニカル サポートとドキュメント – Cisco Systems