ASA 9.x EIGRP 設定例

目次

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）を用いて、ASA ソフトウェア バージョン 9.x 以降でサポートされている、Enhanced Interior Gateway Routing Protocol（EIGRP）を介したルート学習のための設定方法、および認証の実施方法について説明します。

前提条件

要件

この設定を行う前に、以下の条件を満たしていることを確認してください。

- Cisco ASA は、バージョン 9.x 以降を実行する必要があります。
- EIGRP は、マルチ コンテキスト モードでサポートされていないため、シングル コンテキスト モードである必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア バージョン 9.2.1
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.2.1
- バージョン 12.4 が稼働する Cisco IOS® ルータ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

ガイドラインと制限事項

- 1 つの EIGRP インスタンスは、シングル モードで、またマルチモードではコンテキストごとにサポートされています。
- マルチモードでは、2 つのスレッドがコンテキストごと、EIGRP インスタンスごとに作成され、表示プロセスで参照できます。
- 自動要約はデフォルトでは無効になっています。
- 個別インターフェイス モードでは、クラスタ ユニット間でネイバー関係は確立されません。
- デフォルト情報の in [<acl>] が、受信候補のデフォルト ルートの外部ビットをフィルタ処理するために使用されます。
- デフォルト情報の out [<acl>] が、送信候補のデフォルト ルートの外部ビットをフィルタ処理するために使用されます。

EIGRP およびフェイルオーバー

Cisco ASA コード バージョン 8.4.4.1 以降では、アクティブ装置からスタンバイ装置へのダイナミック ルートが同期されます。 また、ルートの削除もスタンバイ装置に同期されます。 ただし、ピア隣接関係の状態は同期されません。 アクティブ装置のみ、ネイバーの状態を維持し、ダイナミック ルーティングにアクティブに参加します。 「ASA FAQ： ダイナミック ルートが同期される場合、フェイルオーバー後に起きること』を参照してください。 参照してください。

設定

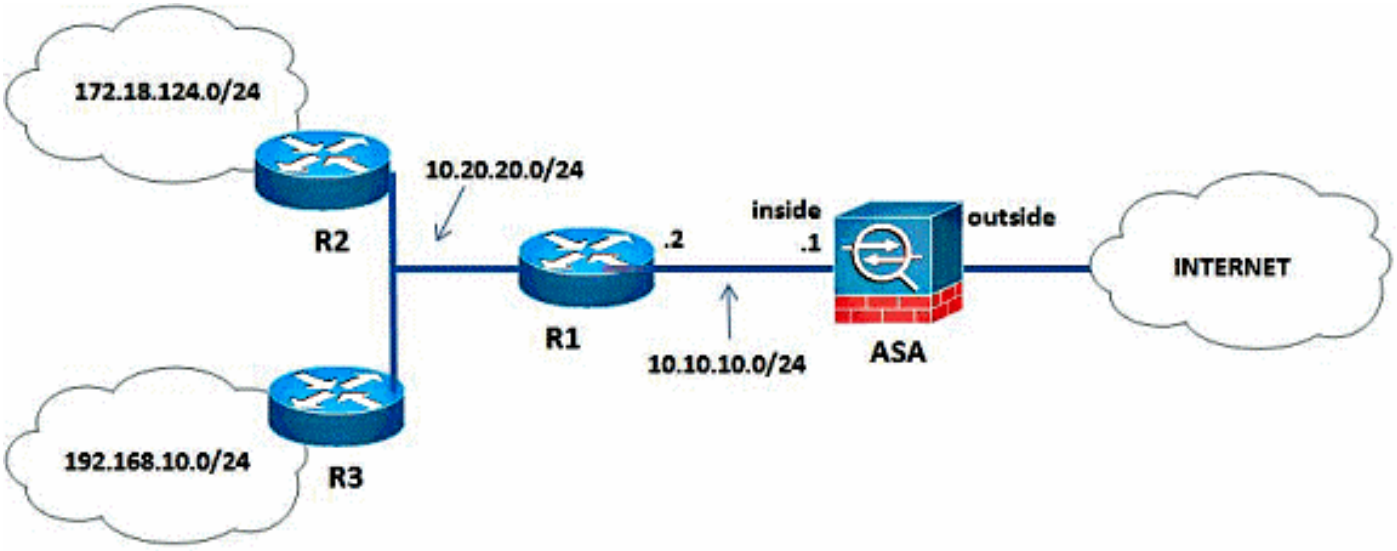
この項では、このドキュメントで網羅する機能の設定方法について説明します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup

Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



ここに示すネットワーク トポロジでは、Cisco ASA 内部インターフェイス IP アドレスは、10.10.10.1/24 です。 ここでは、EIGRP を Cisco ASA で設定し、隣接ルータ（R1）を直接介した内部ネットワーク（10.20.20.0/24、172.18.124.0/24、192.168.10.0/24）へのルートを学習することを目的とします。 R1 は、他の 2 つのルータ（R2 と R3）を介したリモート内部ネットワークへのルートを学習します。

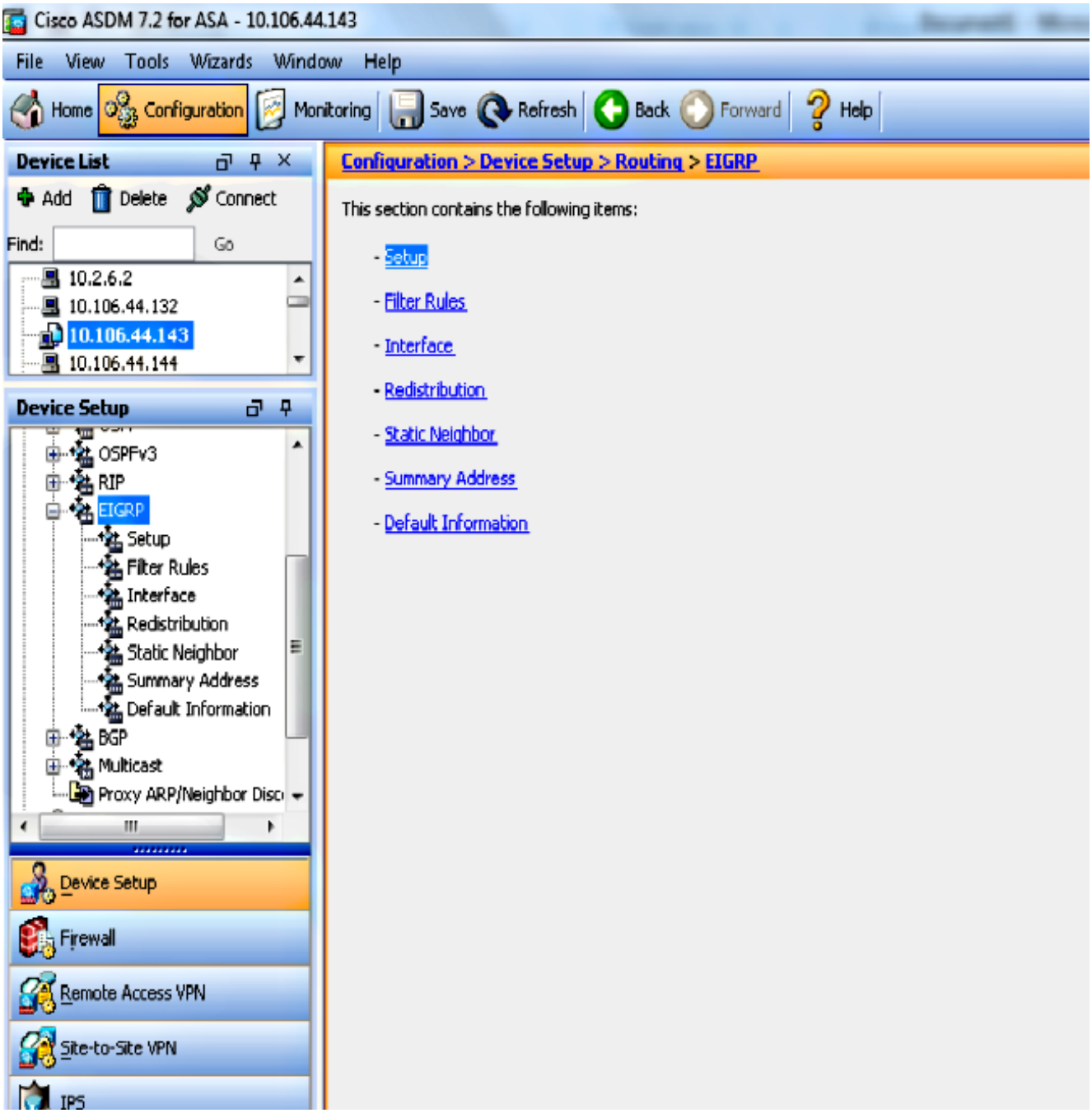
ASDM の設定

ASDM は、セキュリティ アプライアンスのソフトウェアの設定およびモニタのために使用されるブラウザベースのアプリケーションです。 ASDM は、セキュリティ アプライアンスからロードされ、デバイスの設定、モニタ、管理のために使用されます。 また、ASDM Launcher を使用して、Java アプレットより高速に ASDM アプリケーションを起動することもできます。 ここでは、この ASDM のドキュメントで説明する機能を設定するために必要な情報を説明します。

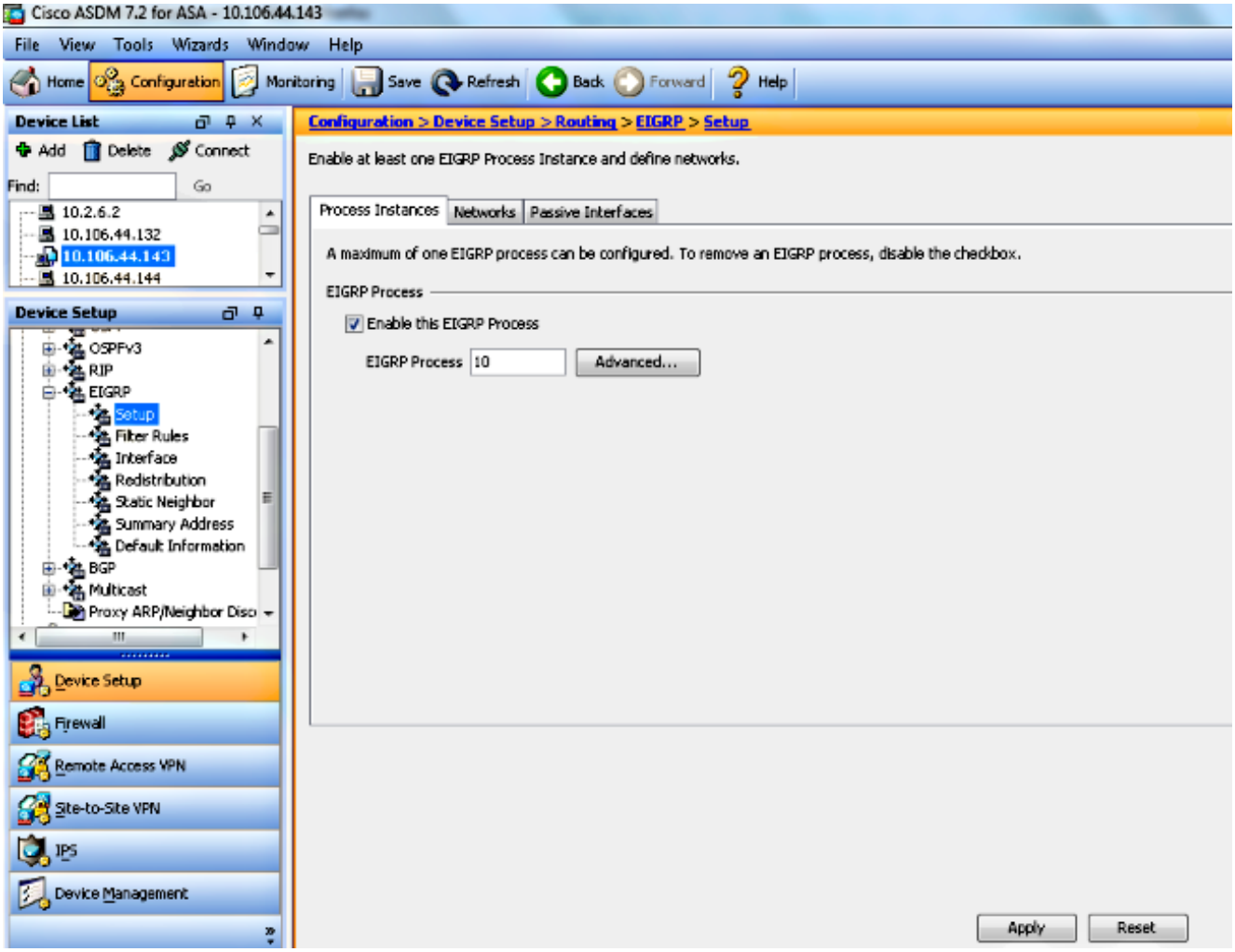
Cisco ASA で EIGRP を設定するには、次の手順を実行してください。

1. Cisco ASA の ASDM にログインします。

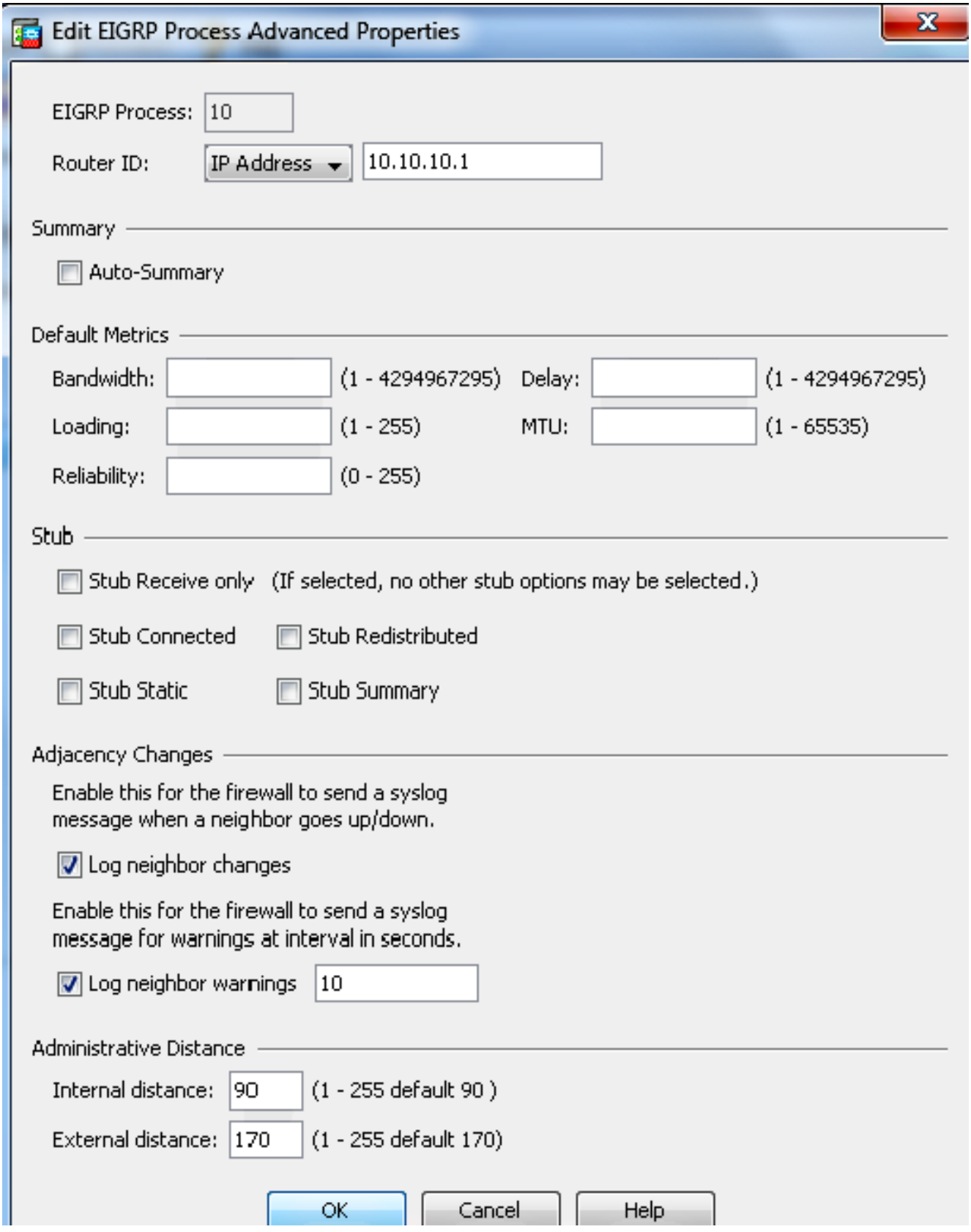
2. このスクリーンショットに示すように、ASDM インターフェイスの [Configuration] > [Device Setup] > [Routing] > [EIGRP] エリアに移動します。



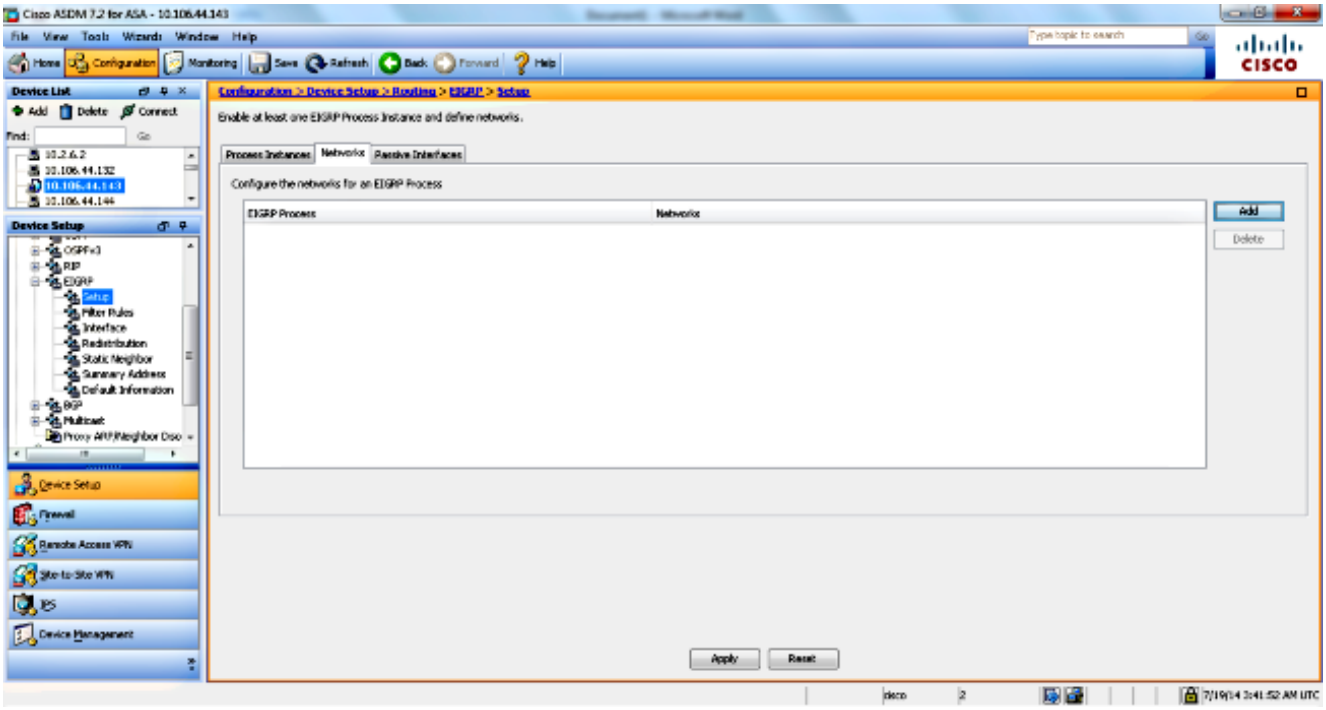
3. このスクリーンショットに示すように、[Setup] > [Process Instances] タブで EIGRP ルーティング プロセスをイネーブルにします。 この例では、EIGRP プロセスは**10** です。



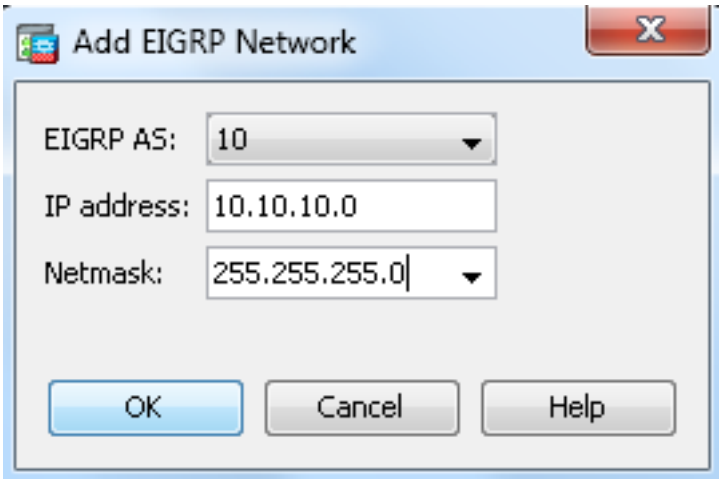
4. オプションで、高度な EIGRP ルーティング プロセスのパラメータを設定できます。 [Setup] > [Process Instances] タブで [Advanced] をクリックします。 EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定し、自動ルート集約をディセーブルにし、再配布されるルートのデフォルト メトリックを定義できます。また、内外 EIGRP ルートのアドミニストレーティブ ディスタンスを変更し、スタティック ルータ ID を設定し、隣接関係の変更のロギングをイネーブルまたはディセーブルにすることもできます。 この例では、EIGRP の [Router ID] は、内部インターフェイス (10.10.10.1) の IP アドレスで静的に設定されます。 また、**自動要約**も無効になります。 それ以外のオプションはデフォルト値に設定されます。



5. 上記の手順が完了したら、[Setup] > [Networks] タブで、EIGRP ルーティングに参加するネットワークとインターフェイスを定義します。 このスクリーンショットに示すように、[Add] をクリックします。



6. 次の画面が表示されます。 この例では、EIGRP が内部インターフェイスのみでイネーブルにされているため、追加するネットワークだけが内部ネットワーク（10.10.10.0/24）です。



IP アドレスが定義済みネットワークの範囲内にあるインターフェイスだけが、EIGRP ルーティング プロセスに参加します。 EIGRP ルーティングに参加させないインターフェイスがアドバタイズ先のネットワークに接続されている場合は、そのインターフェイスが接続されているネットワーク エントリを [Setup] > [Networks] タブで設定し、次にそのインターフェイスをパッシブ インターフェイスとして設定して、インターフェイスが EIGRP 更新を送受信できないようにします。

注: パッシブに設定されたインターフェイスは、EIGRP 更新を送受信しません。

7. オプションで、[Filter Rules] ペインでルート フィルタを定義できます。 ルート フィルタにより、EIGRP 更新で送受信することを許可されているルートをより細かく制御できます。

8. オプションで、ルート再配布を設定できます。 Cisco ASA は、Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）によって検出されたルートを EIGRP ルーティング プロセスに再配布できます。 スタティック ルートおよび接続されてい

るルートも、EIGRP ルーティング プロセスに再配布できます。 スタティックまたは接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。 [Redistribution] ペインでルート再配布を定義します。

9. EIGRP Hello パケットはマルチキャスト パケットとして送信されます。 EIGRP ネイバーが非ブロードキャスト ネットワークを越えた場所にある場合、そのネイバーを手動で定義する必要があります。 手動で EIGRP ネイバーを定義すると、Hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。 スタティック EIGRP ネイバーを定義するには、[Static Neighbor] ペインに移動します。

10. デフォルトでは、デフォルト ルートが送信され、受け入れられます。 デフォルトのルート情報の送受信を制限またはディセーブルにするには、[Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Default Information] ペインを開きます。 [Default Information] ペインには、EIGRP 更新でのデフォルト ルート情報の送受信を制御するルールのテーブルが表示されます。

    注: EIGRP ルーティング プロセスごとに、「*in*」ルールと「*out*」ルールを 1 つずつ設定できます。（現在は 1 つのプロセスだけがサポートされています）。

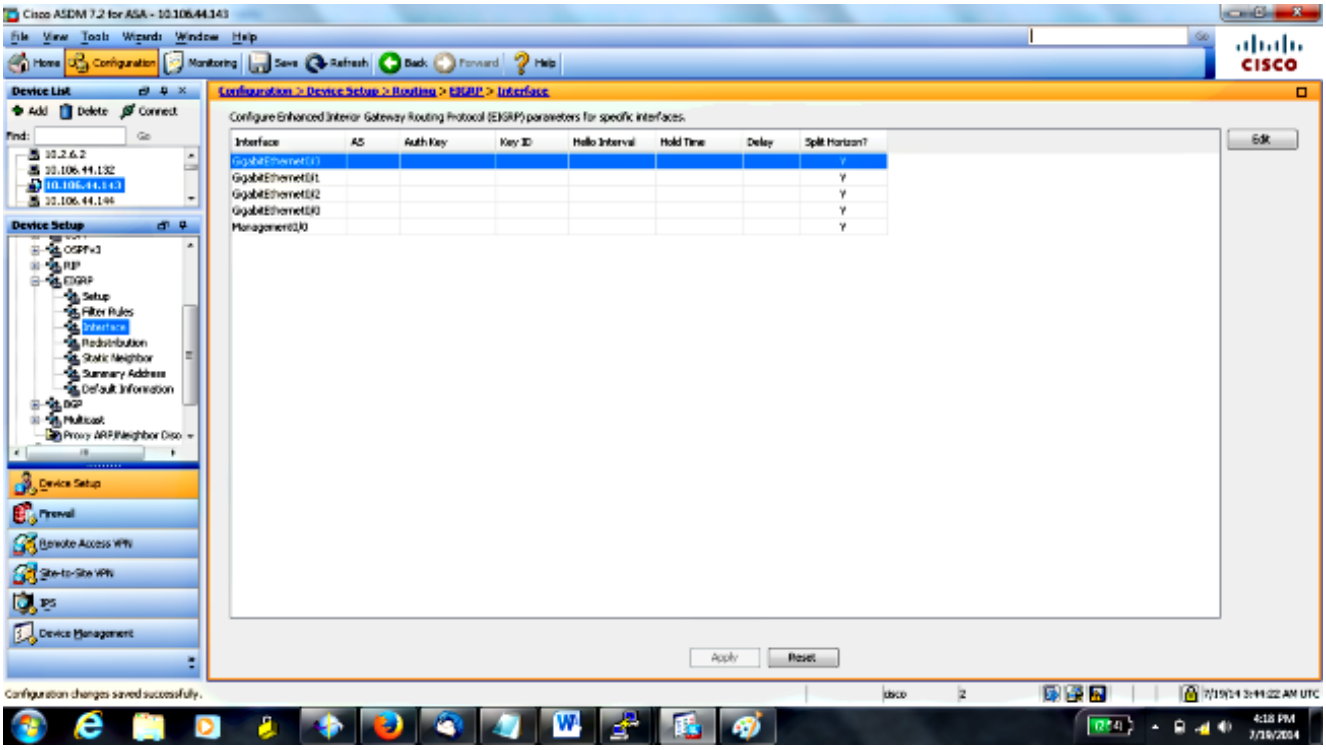
EIGRP 認証の設定

Cisco ASA は、EIGRP ルーティング プロトコルからのルーティング アップデートの MD5 認証をサポートします。 MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。 認証を EIGRP メッセージに追加すると、ルータおよび Cisco ASA は、同じ事前共有キーが設定された他のルーティング デバイスからのルーティング メッセージのみを受信します。 この認証を設定しない場合、ネットワークへの異なるまたは逆方向のルート情報を持つ別のルーティング デバイスが別のユーザにより導入されると、ルータまたは Cisco ASA のルーティング テーブルが破損し、DoS 攻撃を受ける危険性があります。 ルーティング デバイス（ASA を含む）間で送信される EIGRP メッセージに認証を追加すると、承認されていない EIGRP ルータのルーティング トポロジへの追加を回避できます。

EIGRP ルート認証は、インターフェイスごとに設定します。 EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

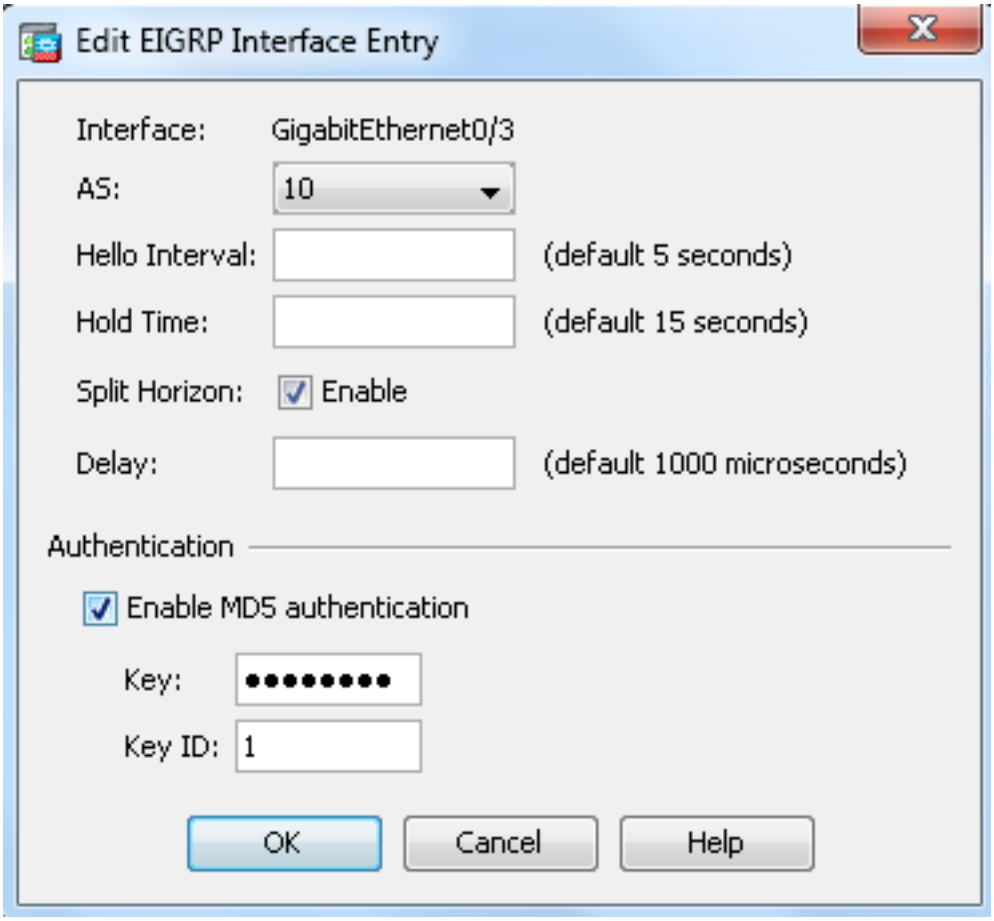
Cisco ASA で EIGRP MD5 認証をイネーブルにするには、次の手順を実行します。

1. ここに示すように、ASDM で [Configuration] > [Device Setup] > [Routing] > [EIGRP] > [Interface] に移動します。



2. この場合、EIGRP は、内部インターフェイス (GigabitEthernet 0/1) でイネーブルにされます。 [GigabitEthernet 0/1] インターフェイスを選択し、[Edit] をクリックします。

3. [Authentication] で、[Enable MD5 authentication] を選択します。 認証パラメータの詳細をここに追加します。 この場合、事前共有キーは [cisco123] で、キー ID は [1] です。



EIGRP ルート フィルタリング

EIGRP では、送受信したルーティング アップデートを制御できます。 この例では、R1 の背後にある、ネットワーク プレフィックスが 192.168.10.0/24 の ASA のルーティング アップデートをブロックします。 ルート フィルタリングには、[STANDARD ACL] のみ使用できます。

```
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
```

確認

```
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
```

設定

Cisco ASA CLI 設定

これは Cisco ASA CLI の設定です。

```
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
```

Cisco IOS ルータ (R1) CLI 設定

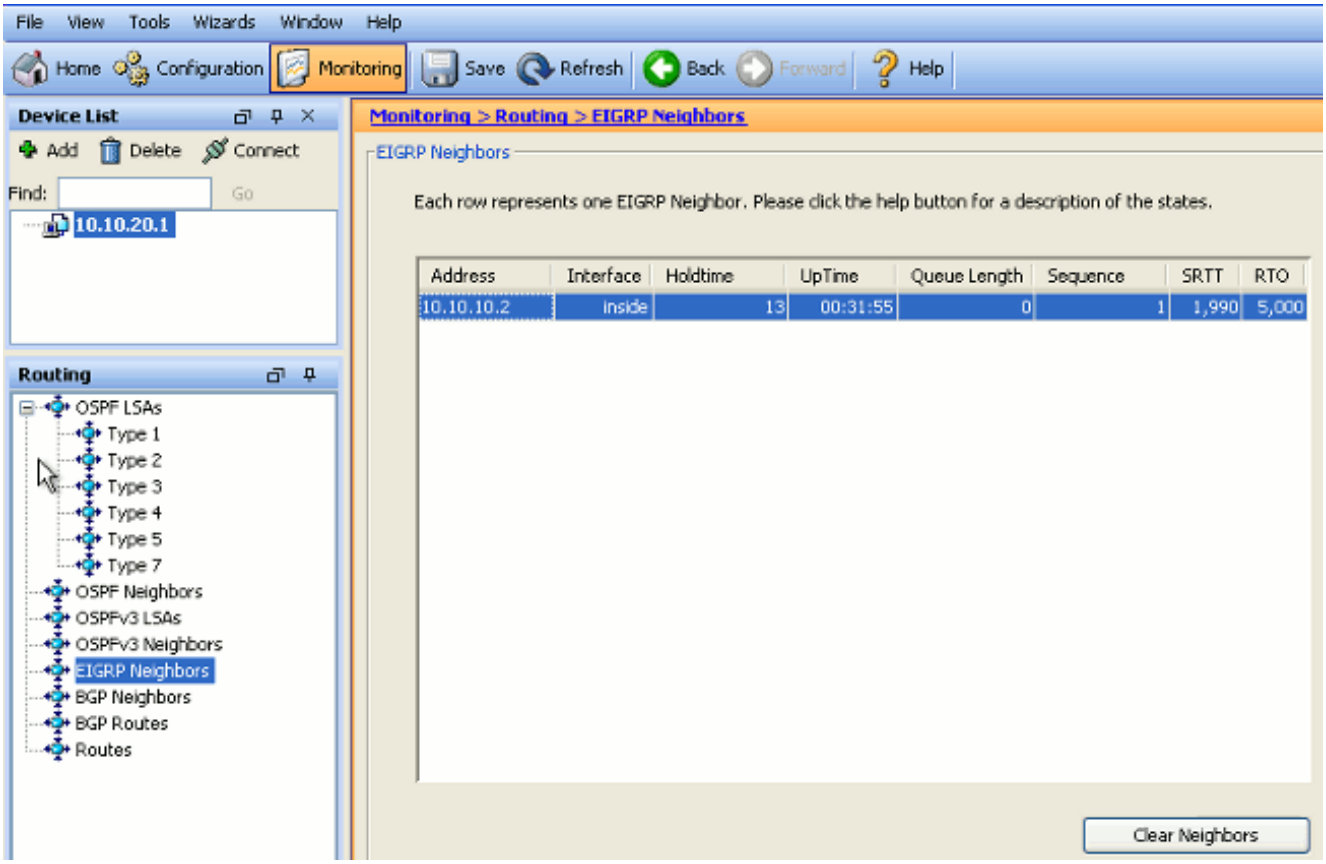
これは R1 (内部ルータ) CLI の設定です。

```
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
```

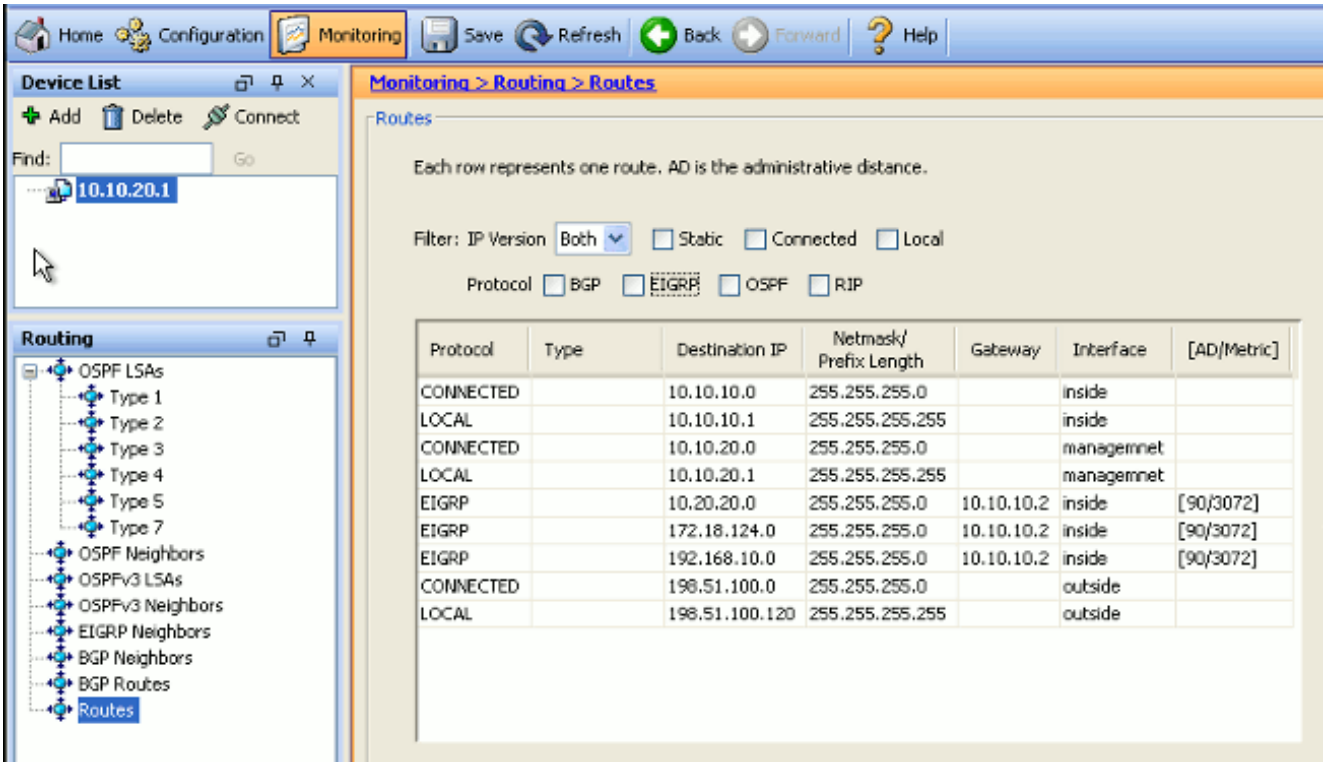
確認

設定を検証するには、次の手順を実行します。

1. ASDM で、[Monitoring] > [Routing] > [EIGRP Neighbor] に移動し、各 EIGRP ネイバーを確認できます。 このスクリーンショットは、アクティブ ネイバーとしての内部ルータ (R1) を示しています。 ネイバーが常駐するインターフェイス、待機時間、ネイバー関係が稼働している時間 (UpTime) も確認できます。



2. また、[Monitoring] > [Routing] > [Routes] に移動して、ルーティング テーブルを確認できます。 この画面では、192.168.10.0/24、172.18.124.0/24、10.20.20.0/24 ネットワークが R1（10.10.10.2）を通して学習されたことを示しています。



CLI から、**show route** コマンドを使用して、同じ出力を取得できます。

```
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
```

ASA バージョン 9.2.1 以降では、**show route eigrp コマンド**を使用して、EIGRP ルートのみを表示できます。

```
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. また、**show eigrp topology** コマンドを使用して、学習したネットワークおよび EIGRP トポロジに関する情報を取得することもできます。

```
    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. **show eigrp neighbors** コマンドは、アクティブ ネイバーおよび対応情報の検証にも役に立ちます。 この例では、手順 1 で ASDM から取得した情報と同じ情報を示します。

```
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
```

パケット フロー

パケット フローを以下に示します。

1. ASA はリンク上でアップすると、EIGRP が設定されたすべてのインターフェイスを介して mCast Hello パケットを送信します。

2. R1 は Hello パケットを受信し、mCast Hello パケットを送信します。

13 5.572557	10.10.10.1	224.0.0.10	EIGRP	86 0x3b1a (15130)	Hello
14 5.573335	10.10.10.2	224.0.0.10	EIGRP	86 0x2321 (8993)	Hello
15 5.575212	10.10.10.1	10.10.10.2	EIGRP	54 0x0589 (1417)	Update
16 5.581712	10.10.10.2	10.10.10.1	EIGRP	54 0x19d9 (6617)	Update
17 5.585145	10.10.10.1	10.10.10.2	EIGRP	54 0x755e (30046)	Hello (Ack)
18 5.585373	10.10.10.1	10.10.10.2	EIGRP	96 0x1c93 (7315)	Update
19 5.591919	10.10.10.2	10.10.10.1	EIGRP	54 0x6695 (26261)	Hello (Ack)
20 5.591950	10.10.10.2	10.10.10.1	EIGRP	180 0x7925 (31013)	Update
21 5.595200	10.10.10.1	10.10.10.2	EIGRP	96 0x62e8 (25320)	Update
22 5.601913	10.10.10.2	10.10.10.1	EIGRP	54 0x08a7 (2215)	Hello (Ack)
23 5.601944	10.10.10.2	10.10.10.1	EIGRP	96 0x31c5 (12741)	Update

3. ASA は、Hello パケットを受信し、初期化プロセスであることを示す最初のビット セットと共に、アップデート パケットを送信します。

4. R1 は、アップデート パケットを受信し、初期化プロセスであることを示す最初のビット セットと共に、アップデート パケットを送信します。

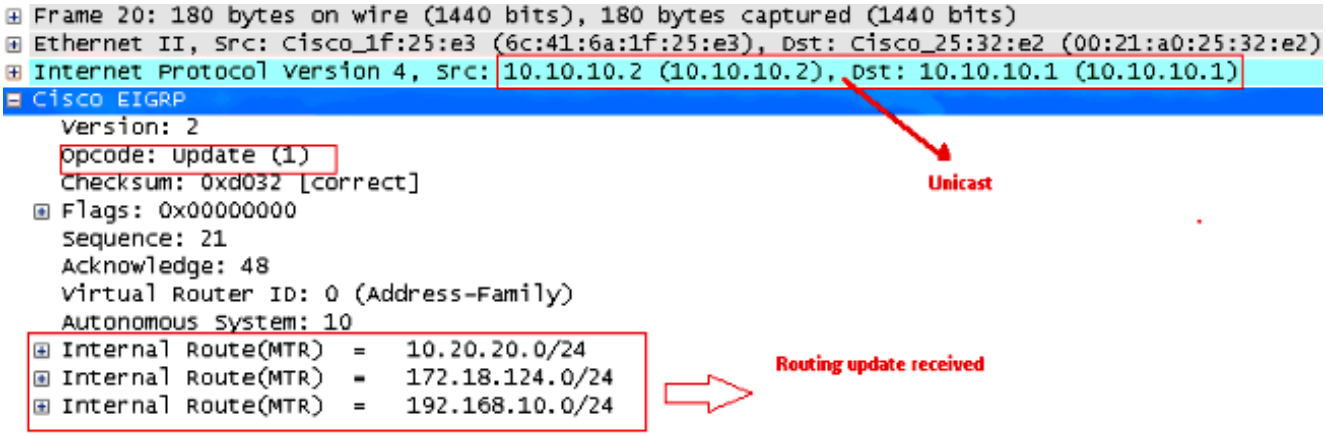
```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xfdc4 [correct]
  ⊟ Flags: 0x00000001, Init
      .... .... .... .... .... .... .... ...1 = Init: Set
      .... .... .... .... .... .... .... ..0. = Conditional Receive: Not set
      .... .... .... .... .... .... .... .0.. = Restart: Not set
      .... .... .... .... .... .... .... 0... = End Of Table: Not set
    Sequence: 47
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
```

5. ASA および R1 が Hello を交換し、隣接関係が確立された後、ASA および R1 は、更新情報を受信したことを示す ACK パケットで応答します。

6. ASA はアップデート パケットで R1 にルーティング情報を送信します。

7. R1 は、トポロジ テーブルにアップデート パケットの情報を挿入します。 トポロジ テーブルには、ネイバーによってアドバタイズされたすべての接続先が含まれます。 これは構造化されていて、接続先に送信できるすべてのネイバーと、それに関連するメトリックスと共に、各接続先がリストされます。

8. 次に、R1 は ASA にアップデート パケットを送信します。



9. アップデート パケットを受信すると、ASA は R1 に ACK パケットを送信します。 ASA および R1 が互いにアップデート パケットの受信に成功すると、トポロジ テーブル内のサクセサ（ベスト）、およびフィージブル サクセサ（バックアップ）ルートの選択が可能になり、サクセサのルートをルーティング テーブルに提供します。

トラブルシューティング

この項には、EIGRP 問題のトラブルシュートに役立つ、**debug および show コマンド**に関する情報が含まれています。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

> **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。 Diffusing Update Algorithm（DUAL）有限状態マシンのデバッグ情報を表示するには、特権 EXEC モードで**debug eigrp fsm** コマンドを使用します。 このコマンドを使用すると、EIGRP フィージブル サクセサ アクティビティをモニタし、ルート更新がルーティング プロセスによりインストールされているかどうか、および削除されているかどうかを確認できます。

これは、R1 に正常にピアリングされた場合の、**debug コマンド**の出力です。 システムにインストールされているルートごとに表示できます。

```
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
```

また、**debug eigrp neighbor** コマンドも使用できます。 これは、Cisco ASA が R1 に新しいネイバー関係を作成したときの、**debug コマンド**の出力です。

```
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 ()
```

Cisco ASA とピア間の EIGRP メッセージ交換情報の詳細については、デバッグ EIGRP パケットも使用できます。 この例では、認証キーはルータ（R1）で変更され、問題は認証の不一致であるとデバッグ出力に示されています。

```
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 ネイバーシップのダウンと Syslog ASA-5-336010

ASA は、EIGRP 配布リストに変更がある場合、EIGRP ネイバーシップをドロップします。 この Syslog メッセージが表示されます。

```
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)
```

この設定では、ACL に**新しい ACL エントリが追加**されるたびに、**Eigrp-network-list** EIGRP ネイバーシップがリセットされます。

```
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)
```

ネイバー関係は、隣接関係のデバイスで動作していることを確認できます。

```
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
```

ここに、**access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0** を追加できます。

```
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
```

これらのログは、**debug eigrp fsm** で確認できます。

```
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
```

これは、8.4 および 8.6 ~ 9.1 のすべての新しい ASA バージョンにおいて想定される動作です。同様のことが、12.4 ~ 15.1 のコード トレインが動作するルータでも確認されました。 ただし、ASA バージョン 8.2 以前の ASA ソフトウェア バージョンでは、ACL に加えられた変更により EIGRP の隣接関係はリセットされないため、この動作は見られません。

EIGRP は、最初にネイバーが起動されたときに、ネイバーにすべてのトポロジ テーブルを送信し、その後変更のみを送信するため、EIGRP のイベント起動と共に配布リストを設定する仕組みでは、ネイバー関係を全リセットせずに、変更を適用するのは困難です。 現在の配布リストで指示される変更を適用するには、ルータは、どのルートが変更されたか (送信/承認されたかどうか) を知るため、ネイバーから送受信されたすべてのルートをトラックする必要があります。 単にネイバー間の隣接関係を切断し、再確立する方がより簡単です。

隣接関係が切断され、再確立されると、特定のネイバー間のすべての学習ルートは削除され、新しい配布リストと共に、ネイバー間のすべての同期が再度実行されます。

Cisco IOS ルータのトラブルシューティングに使用する EIGRP 手法のほとんどは Cisco ASA に適用できます。 EIGRP をトラブルシューティングするには、「主要なトラブルシューティングのフローチャート」を使用してください。 **Main**とマーキングされたボックスで開始します。