



ルーティングの概要

この章では、Cisco ASA 内でのルーティング動作の基本概念と、サポートされているルーティングプロトコルについて説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも1つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、インターネットワーク経由でのパケットの転送という2つの基本的なアクティビティが含まれます。

- [パス判別 \(1 ページ\)](#)
- [サポートされるルート タイプ \(2 ページ\)](#)
- [ASA 内でのルーティングの仕組み \(4 ページ\)](#)
- [ルーティングにサポートされているインターネット プロトコル \(7 ページ\)](#)
- [Routing Table \(8 ページ\)](#)
- [管理トラフィック用ルーティングテーブル \(15 ページ\)](#)
- [プロキシ ARP 要求のディセーブル化 \(16 ページ\)](#)
- [ルーティング テーブルの表示 \(17 ページ\)](#)
- [参照先 \(17 ページ\)](#)

パス判別

ルーティングプロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティングアルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティングアルゴリズムは、ルート情報が格納されるルーティングテーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティングアルゴリズムにより、さまざまな情報がルーティングテーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティングテーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決めます。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティングテーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの1つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。



(注) 非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。ASAでは、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブルマップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとし

て機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティングシステムでは、一部のルータが実質的なルーティングバックボーンを形成します。バックボーン以外のルータからのパケットはバックボーンルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーンルータから、1つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織に類似しているため、そのトラフィック パターンもサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステートアルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ASA 内でのルーティングの仕組み

ASA は NAT の設定に応じて、ルーティングの判断のために、ルーティング テーブルまたは NAT (xlate) テーブルを使用します。

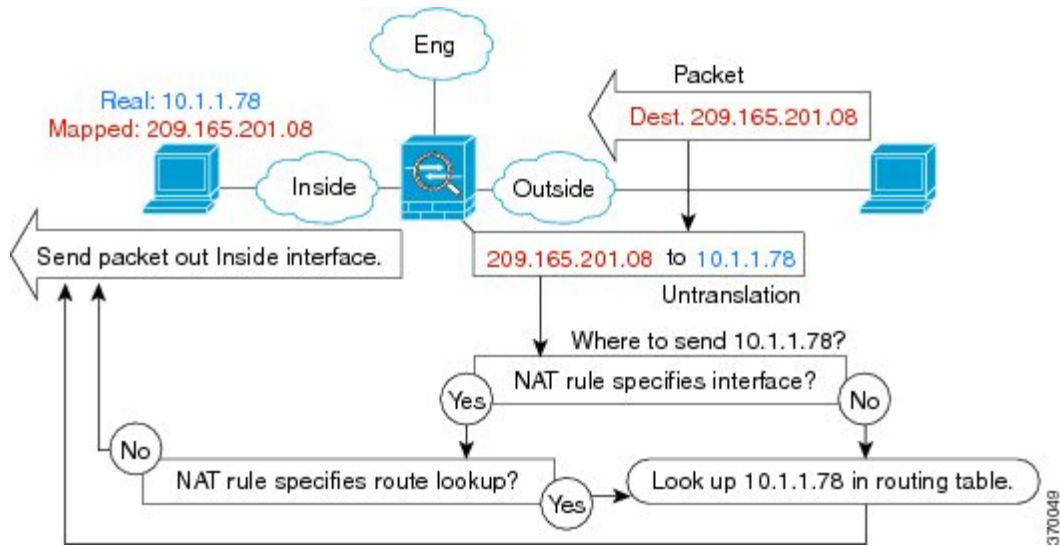
出力インターフェイスの決定

NAT を使用していて、ASA がマッピング アドレスのトラフィックを受信する場合、ASA は NAT ルールに従って宛先アドレスを変換解除し、実際のアドレスにパケットを送信します。ASA は、次の方法でパケットの出力インターフェイスを決定します。

- トランスペアレント モードまたはルーテッドモードのブリッジ グループ インターフェイス：ASA は NAT ルールを使用して実際のアドレスの出力インターフェイスを決定します。NAT ルールの一部として送信元、宛先のブリッジ グループ メンバー インターフェイスを指定する必要があります。
- ルーテッドモードの通常インターフェイス：ASA は、次のいずれかの方法で出力インターフェイスを決定します。
 - NAT ルールでインターフェイスを設定する：ASA は NAT ルールを使用して出力インターフェイスを決定します。(8.3(1) ~ 8.4(1)) 唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルートルックアップが使用されます。(8.4(2)以降) アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションを使用することです。ただし、代わりにオプションとして常にルートルックアップを使用することもできます。一部のシナリオでは、ルートルックアップの上書きが必要になる場合があります。
 - NAT ルールでインターフェイスを設定しない：ASA はルートルックアップを使用して出力インターフェイスを決定します。

次の図に、ルーテッドモードでの出力インターフェイスの選択方法を示します。ほとんどの場合、ルートルックアップは NAT ルールのインターフェイスと同じです。ただし、一部のコンフィギュレーションでは、2 つの方法が異なる場合があります。

図 1: NATによるルーテッド モードでの出力インターフェイスの選択



ネクスト ホップの選択プロセス

前述のいずれかの方法を使用して出力インターフェイスを選択した後、さらにルート ルックアップが実行され、これまでに選択した出力インターフェイスに属する適切なネクストホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティングテーブルにない場合は、パケットがドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されます（別の出力インターフェイスに属する、指定の宛先ネットワークへの別のルートがあるかどうかにかかわらず）。選択した出力インターフェイスに属するルートが見つかり、パケットは対応するネクスト ホップに転送されます。

ASAでのロードシェアリングは、1つの出力インターフェイスを使用して複数のネクストホップが使用できる場合に限り可能です。ロードシェアリングでは、複数の出力インターフェイスの共有はできません。

ダイナミック ルーティングが ASA で使用されており、XLATE の作成後にルート テーブルが変更された場合も（ルート フラップなど）、宛先変換トラフィックは、XLATE がタイムアウトするまでは、ルート テーブルではなく古い XLATE を使用して転送されます。トラフィックが、正しくないインターフェイスに転送されたり、ドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されたりすることもあります（ルーティングプロセスによって古いルートが古いインターフェイスから削除されて別のインターフェイスに接続された場合）。

ASA 自体でルート フラップが発生していないにもかかわらず、その周りで一部のルーティングプロセスがフラッピングし、発信元変換された、同じフローに属するパケットを、別のインターフェイスを使用して ASA 経由で送信する場合は、同様の問題が発生することがあります。宛先変換された返送パケットは、間違った出力インターフェイスを使用して戻されることがあります。

セキュリティトラフィック構成によっては、この問題が高い確率で発生します。具体的には、ほぼすべてのトラフィックが、フローの最初のパケットの方向に応じて、発信元変換されるか宛先変換されるような構成です。ルートフラップの後にこの問題が発生した場合は、**clear xlate** コマンドを使用して手動で解決するか、XLATE のタイムアウトによって自動的に解決できます。XLATE のタイムアウトは、必要に応じて小さくできます。この問題がほとんど発生しないようにするには、ASA やその周りでルートフラップが発生しないようにします。つまり、同じフローに属する宛先変換されたパケットが必ず同じ方法で ASA を通して転送されることを確認します。

ECMP ルーティング

ASA は、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大 8 の等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロード バランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

ゾーンがある場合は、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミックルーティングプロトコルは、自動的に等コストルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス間でトラフィックをロード バランスします。

ルートが紛失した場合、デバイスはフローをシームレスに別のルートに移動させます。

ルーティングにサポートされているインターネット プロトコル

ASA は、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First (OSPF)

OSPF は、インターネット プロトコル (IP) ネットワーク向けに、インターネット技術特別調査委員会 (IETF) の Interior Gateway Protocol (IGP) 作業部会によって開発されたルーティングプロトコルです。OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- ルーティング情報プロトコル (RIP)

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol (IGP) です。つまり、1 つの自律システム内部でルーティングを実行します。

- Border Gateway Protocol (BGP)

BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービスプロバイダー (ISP) 間で使用されるプロトコルです。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP ルートを交換します。自律システム (AS) 間で BGP を使用する場合、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP (IBGP) と呼ばれます。

- Intermediate System to Intermediate System (IS-IS)

IS-IS はリンクステート内部ゲートウェイ プロトコル (IGP) です。リンクステート プロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。

Routing Table

ここでは、ルーティング テーブルについて説明します。

ルーティング テーブルへの入力方法

ASAのルーティング テーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。ASAは、ルーティング テーブルに含まれるスタティック ルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2つのルートのネットワークプレフィックス長（ネットワークマスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティング テーブルに入力されます。入力された後は、パケット転送ロジックが2つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASAが、1つのルーティング プロトコル（RIP など）から同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティング テーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティング テーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロード バランシングが行われます。

- ASA が、ある宛先へのルーティング プロトコルが複数あることを検知すると、ルートのアドミニストレーティブ ディスタンスが比較され、アドミニストレーティブ ディスタンスが最も小さいルートがルーティング テーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブ ディスタンスが同じ場合、

デフォルトのアドミニストレーティブ ディスタンスが小さい方のルートがルーティング テーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブ ディスタンスは、2つの異なるルーティングプロトコルから同じ宛先への異なるルートが複数存在する場合に、ASA が最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常に最適パスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、ASA がサポートするルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス値を示します。

表 1: サポートされるルーティングプロトコルのデフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
内部 BGP	200
不明 (Unknown)	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASA が OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティング プロセスの方が優先度が高いため、ASA は OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASA は、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPFを通して取得したルートのアドミニストレーティブディスタンスを変更するために **distance-ospf** コマンドを使用する場合、その変更は、コマンドが入力された ASA のルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブディスタンスは、ルーティングプロセスに影響を与えません。EIGRP、OSPF、RIP および BGP ルーティングプロセスは、そのルーティングプロセスによって検出されたルートまたはそのルーティングプロセスに再配布されたルートのみをアドバタイズします。たとえば、RIP ルーティングプロセスは、ASA のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

バックアップルート

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティングテーブルメンテナンスプロセスが、登録されたバックアップルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミックルーティングプロトコルによって検出されたルートに障害が発生したときにルーティングテーブルにインストールされるフローティングスタティックルートを作成できます。フローティングスタティックルートとは、単に、ASA で動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミックルーティングプロセスで検出された対応するルートに障害が発生すると、このスタティックルートがルーティングテーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティングテーブル内のエントリと一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティングテーブル内の複数のエントリと一致する場合、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 のゲートウェイ 10.1.1.2
- 192.168.32.0/19 のゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティングテーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



(注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

ダイナミック ルーティングと フェールオーバー

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

ダイナミック ルーティングおよびクラスタリング

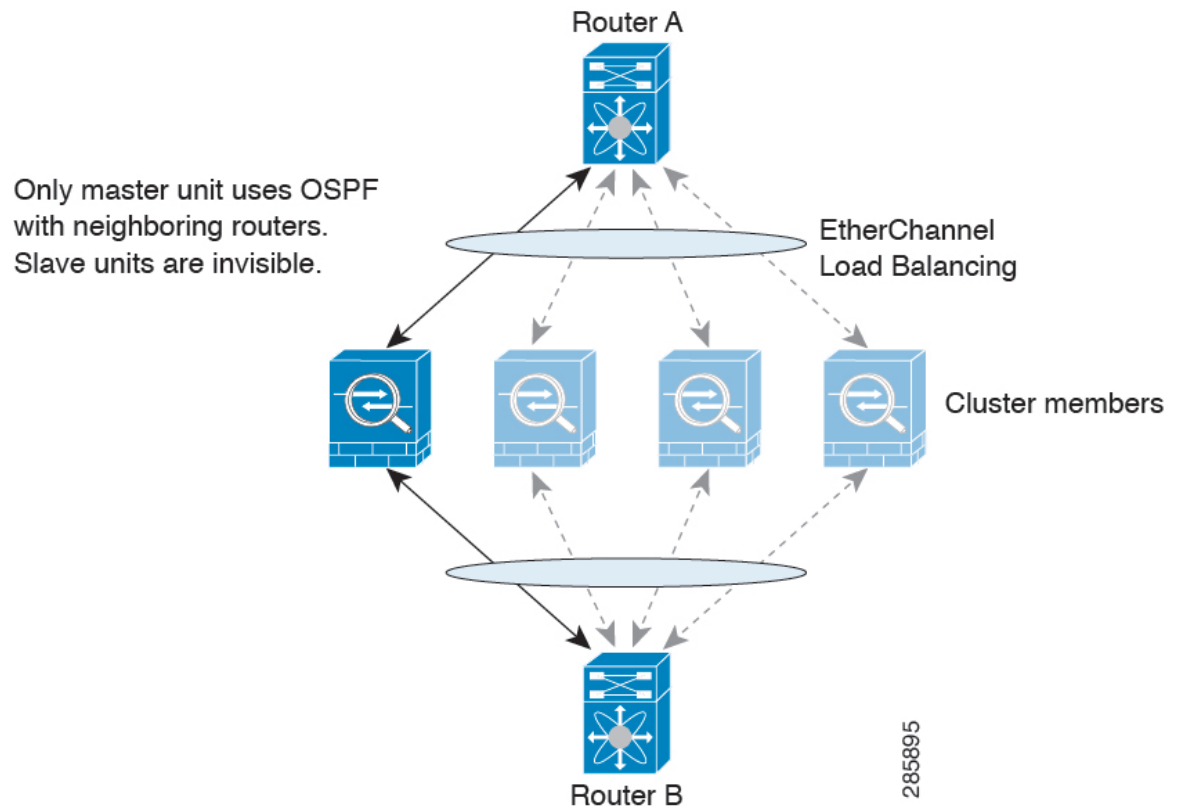
ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング



(注) IS-IS は、スパンド EtherChannel モードではサポートされていません。

スパンド EtherChannel モード：ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスターユニットを介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 2: スパンド *EtherChannel* モードでのダイナミック ルーティング


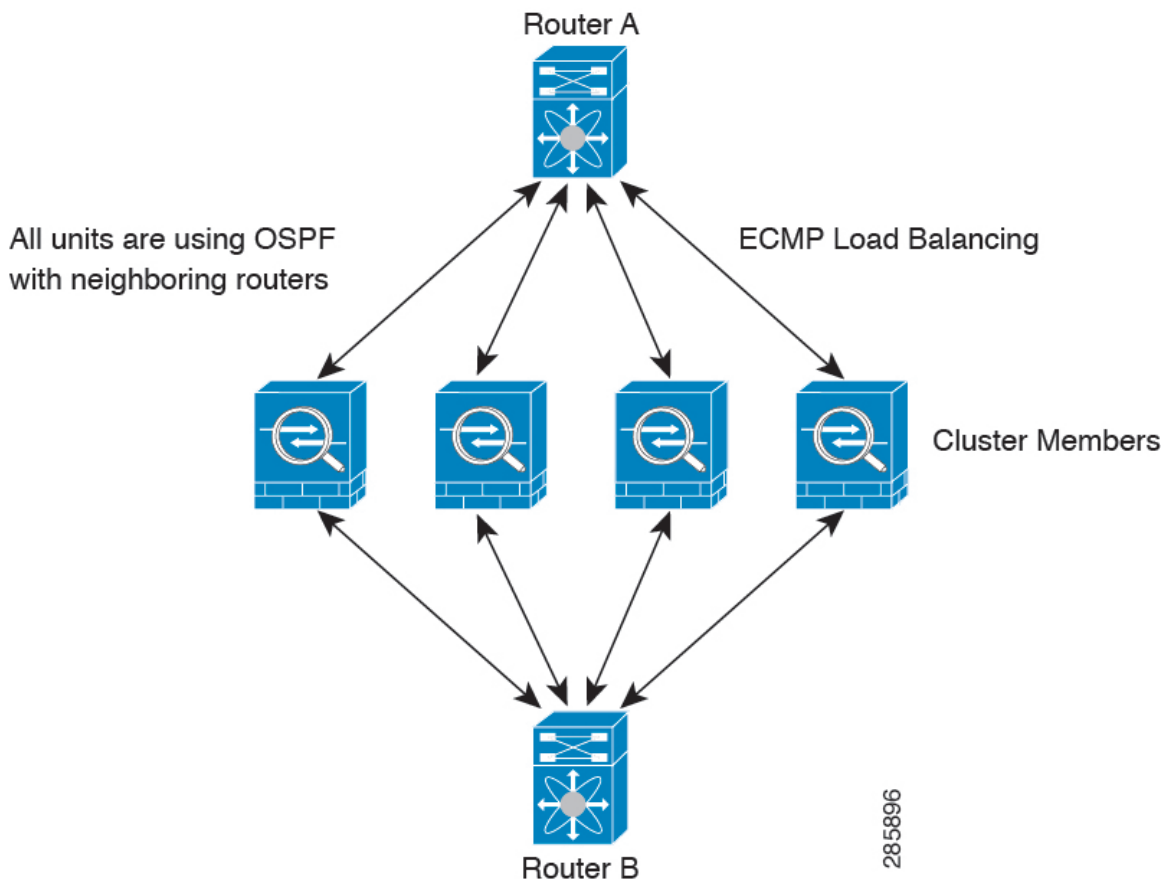
スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイス モードでは、各ユニットがスタンドアロン ルータとしてルーティング プロトコルを実行します。ルートの学習は、各ユニットが個別に行います。

図 3: 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ユニットが別のルータ ID を使用できるように、ルータ ID のクラスター プールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスターピアとのネイバー関係を形成しません。



- (注) クラスターが、冗長性確保のために、同一ルータに対して複数の隣接関係を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。[トラフィックゾーンの設定](#)を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 および EIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキストモードでは、ルーテッドモードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティングアップデートをフィルタリングするために OSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップとプレフィックスのリスト
コンテキストごとに 1 つのインスタンスがサポートされます。	コンテキストごとに 2 つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングルモードで使用可能なすべての CLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える 1 つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルトクラスは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ実践として、データトラフィックを管理トラフィックから分離しなければならない場合があります。この分離を実現するために、ASA は管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。

管理ルーティングテーブルは、データ インターフェイスルーティングテーブルとは分離したダイナミック ルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。分離した管理ルーティングテーブルが含まれていない以前のリリースからアップグレードするとき、データインターフェイスと管理インターフェイスが混在し、同じダイナミック ルーティング プロセスを使用している場合、管理インターフェイスは破棄されます。

HTTP、SCP、TFTP などを使用してリモート ファイルを開くすべての機能に関しては、インターフェイスを指定していない場合、ASA は管理専用ルーティング テーブルを確認します。一致がない場合はデータ ルーティング テーブルを確認します。たとえば、**copy** コマンド、**Smart Call Home**、**trustpoint**、**trustpool** などがあります。

その他のすべての機能に関しては、インターフェイスを指定しなかった場合、ASA はデータルーティング テーブルを確認し、一致するものが見つからなければ、管理専用ルーティング テーブルを確認します。たとえば、**ping**、**DNS**、**DHCP** などがあります。

管理専用インターフェイスには、すべての管理 x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。



(注) VPN を使用している際に ASA で参加したインターフェイス以外のインターフェイスに管理アクセスを許可する管理アクセス機能を設定した場合、分離した管理およびデータルーティング テーブルに関するルーティングの配慮のために、VPN 終端インターフェイスと管理アクセスインターフェイスは同じタイプである必要があります。両方とも管理専用インターフェイスまたは通常のデータ インターフェイスである必要があります。

管理インターフェイスの識別

management-only で設定されたインターフェイスは、管理インターフェイスと見なされます。

次の設定では、GigabitEthernet0/0 と Management0/0 の両インターフェイスは、管理インターフェイスと見なされます。

```

a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
  management-only
  nameif inside
  security-level 100
  ip address 10.10.10.123 255.255.255.0
  ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
  management-only
  nameif mgmt
  security-level 0
  ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#

```

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピングアドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピングアドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアントアドレスプールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターントラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

ステップ 1 [Configuration] > [Device Setup] > [Routing] > [Proxy ARP/Neighbor Discovery] の順に選択します。

[Interface] フィールドにインターフェイス名が一覧表示されます。[Enabled] フィールドには、NAT グローバルアドレスに対してプロキシ ARP/ネイバー探索がイネーブルか (Yes) ディセーブルか (No) が表示されます。

- ステップ 2** 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をイネーブルにするには、[Enable] をクリックします。デフォルトでは、プロキシ ARP/ネイバー探索はすべてのインターフェイスに対してイネーブルです。
- ステップ 3** 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をディセーブルにするには、[Disable] をクリックします。
- ステップ 4** [Apply] をクリックして設定を実行コンフィギュレーションに保存します。

ルーティング テーブルの表示

ルーティング テーブル内のエントリを表示するには、次の手順を実行します

手順

ルーティング テーブルにある ASDM のすべてのルートを表示するには、[Monitoring] > [Routing] > [Routes] の順に選択します。

このペインでは、各行がそれぞれ 1 つのルートを表します。

参照先

表 2: ルート概要の履歴

機能名	プラットフォーム リリース	機能情報
管理インターフェイス用のルーティング テーブル	9.5(1)	データ トラフィックから管理トラフィックを区別して分離するため、管理トラフィック専用のルーティング テーブルが追加されました。管理とデータそれぞれの専用ルーティング テーブルは IPv4 と Ipv6 の両方に対して、ASA の各コンテキストごとに作成されます。さらに、ASA の各コンテキストに対して、RIB と FIB の両方に 2 つの予備のルーティング テーブルが追加されます。 次の画面が更新されました。

