ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

パスの決定

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定します。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を模倣しているため、そのトラフィック パターンを適切に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。

ルーティングでサポートされ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。

- Routing Information Protocol（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。

- ボーダー ゲートウェイ プロトコル（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。

ルーティングテーブル

ASA はデータ トラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティング テーブルを使用します。ここでは、ルーティングテーブルの仕組みについて説明します。管理ルーティングテーブルの詳細については、管理トラフィック用ルーティングテーブル （12 ページ）も参照してください。

ルーティング テーブルへの入力方法

ASAルーティングテーブルには、静的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 デバイスは、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 デバイスが、（RIP などの）1 つのルーティングプロトコル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 デバイスが、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に複数の異なるルートがある場合に、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、他のプロトコルと異なるアルゴリズムに基づいた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つのルートのいずれが最適パスであるかは、必ずしも判別できません。

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でサポートされてい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
VPN ルート	1
スタティック ルート	1
EIGRP集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカルBGP	200
不明	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。

VPN アドバタイズされたルート（V-Route/RRI）は、デフォルトのアドミニストレーティブ ディスタンス 1 のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

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 を通じ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。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけ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、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。

ダイナミック ルーロとフローティング スタティック ルートのバックアップ

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した場合は、パケットが、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た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でインターフェイスに到着するとします。

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

この場合、192.168.32.1 は 192.168.32.0/24 ネットワーク内にあるため、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。もうひとつのルートにもあてはまりますが、192.168.32.0/24 の方が長いプレフィックスを持つためです（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る。

（注） 既存の接続は、新しい同様の接続がルートの変更により異なる動作になる場合でも、引き続き確立されたインターフェイスを使用します。

ダイナミック ルーティングおよび 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

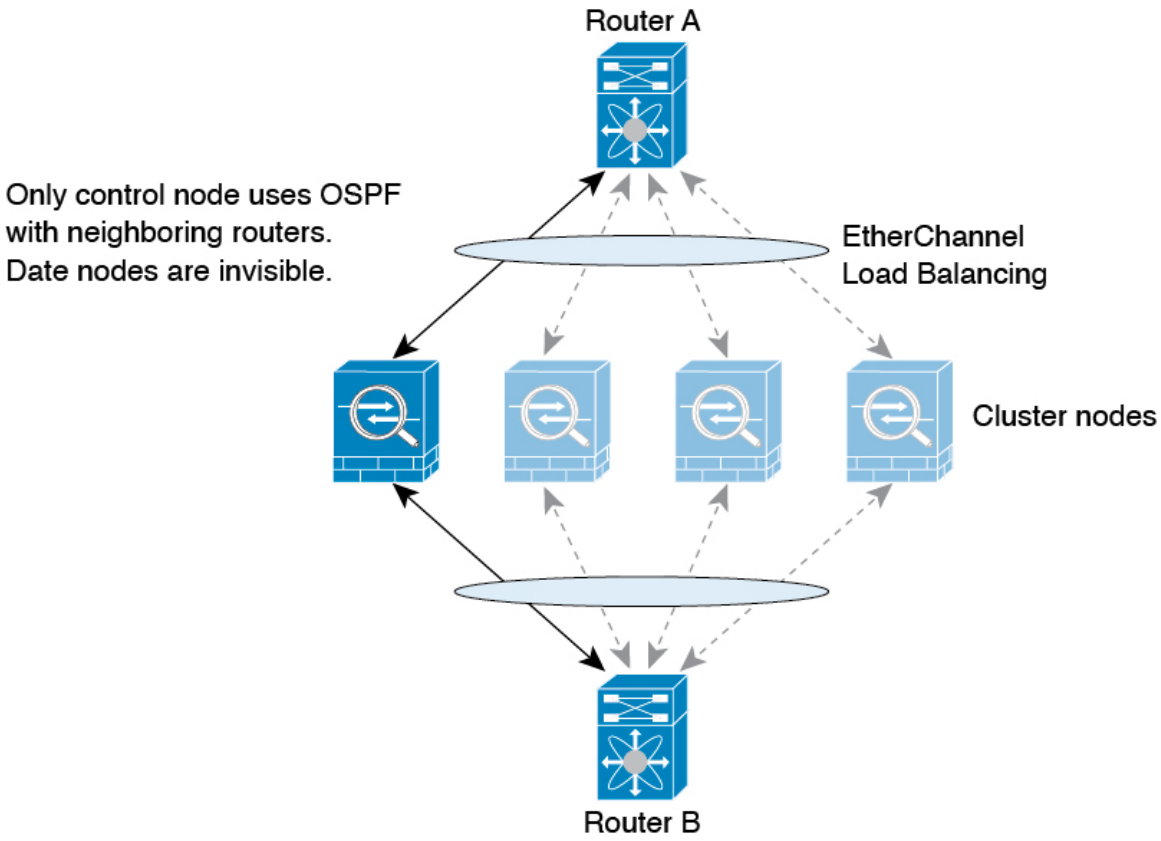
ここでは、クラスタリングでダイナミックルーティングを使用する方法について説明します。

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。

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *1* : スパンド *EtherChannel* モードでのダイナミック ルーティング



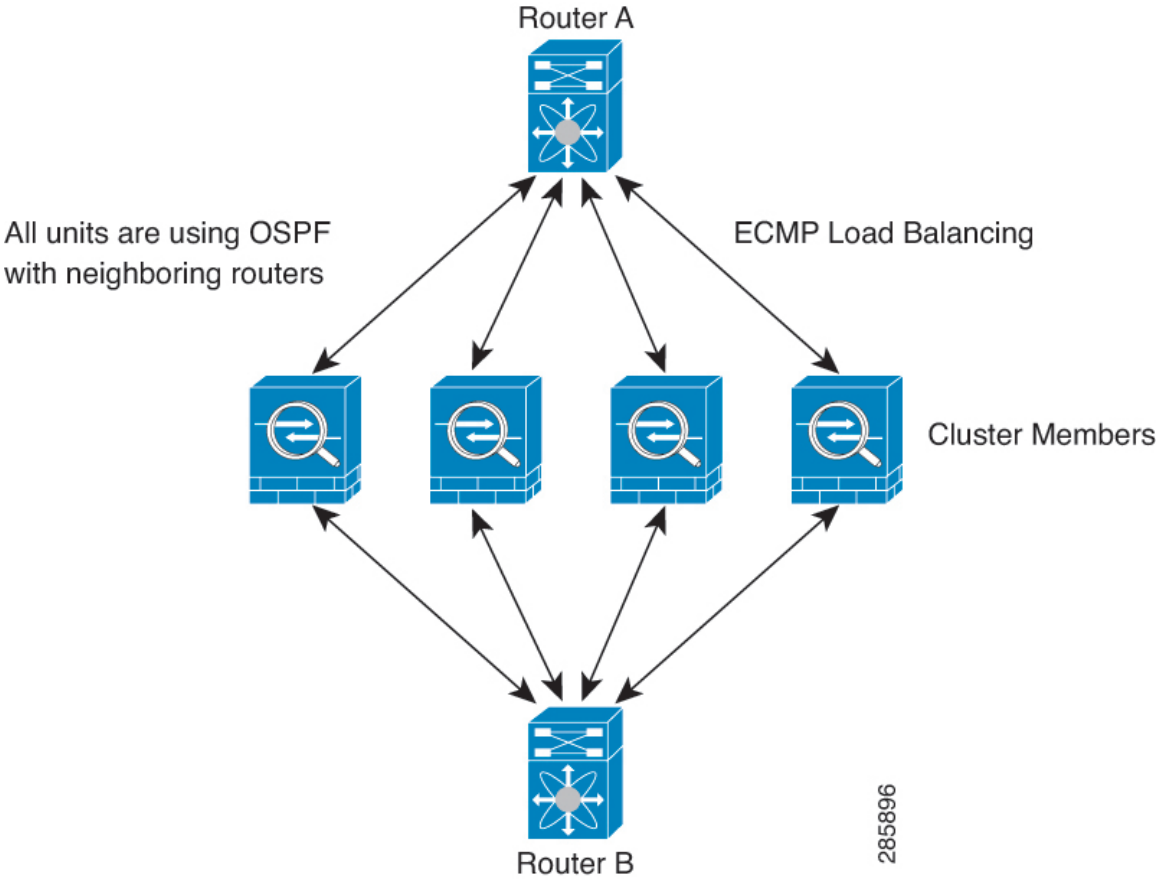
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバー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、各ノード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、各ノードが個別に行います。

図 *2:* 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 つのノードを通過します。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。各ノードは、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、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ 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 ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。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ノード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対策として、多くの場合、（デバイスからの）管理トラフィックをデータトラフィックから分離する必要があります。この分離を実現するために、ASA デバイス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。個別のルーティングテーブルを使用することで、データと管理用に別のデフォルトルートを作成できます。

各ルーティングテーブルのトラフィックのタイプ

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス発信トラフィックでは、タイプに応じて、デフォルトで管理専用ルーティングテーブルまたはデータルーティングテーブルが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

- 管理専用テーブルのデバイス発信トラフィックには、HTTP、SCP、TFTP、**copy** コマンド、スマートライセンス、Smart Call Home、**trustpoint**、**trustpool** などを使用してリモートファイルを開く機能が含まれています。
- データテーブルのデバイス発信トラフィックには、ping、DNS、DHCP などの他のすべての機能が含まれます。

管理専用ルーティングテーブルに含まれるインターフェイス

管理専用インターフェイスには、すべての Management 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。

他のルーティングテーブルへのフォールバック

デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デフォルト以外のルーティングテーブルの使用

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。ASA は、指定されたインターフェイスのルートのみをチェックします。たとえば、管理専用インターフェイスから ping を送信する必要がある場合は、ping 機能でインターフェイスを指定します。他方、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

ダイナミック ルーティング

管理専用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 テーブルから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際、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。

VPN 要件の管理アクセス機能

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)#
```

Equal-Cost Multipath（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 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、および10.1.1.4間の外部インターフェイスでロードバランシングされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポート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。

トラフィックゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストの静的または動的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、等コストルートを自動的に設定できます。ASA 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のトラフィックのロードバランシングを行います。

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。

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。各行は 1 つのルートを表します。

ルート概要の履歴

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 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 タそれぞれの専用ルーティング テーブルは IPv4 と Ipv6 の ASA の各コンテキストごとに作成されます。さらに、ASA トに対して、RIB と FIB の両方に 2 つの予備のルーティン 加されます。 次の画面が更新されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。