CHAPTER 25

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の概念と、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。

この章は、次の項で構成されています。

ルーティングに関する情報

ルーティングは、発信元から宛先にインター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情報グループ（通常はパケットと呼ばれる）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。ルーティング プロセスのコンテキストでは、後者のアクティビティがパケット スイッチングと呼ばれます。パケット スイッチングは比較的単純ですが、パスの決定は非常に複雑になることがあります。

この項は、次の内容で構成されています。

スイッチング

スイッチング アルゴリズムは比較的単純で、ほとんどのルーティング プロトコルで同じです。ほとんどの場合は、別のホストにパケットを送信しなければならないことをホストが決定します。何らかの方法でルータのアドレスを取得すると、送信元ホストは、ルータの物理（メディア アクセス コントロール（MAC）レイヤ）アドレスだけに向けてパケットを送信します。この場合は、宛先ホストのプロトコル（ネットワーク層）アドレスとともに送信されます。

パケットの宛先プロトコル アドレスを確認するときに、ルータは、ネクスト ホップへのパケットの転送方法を認識しているかどうかを確認します。ルータがパケットの転送方法を認識していない場合は、通常はパケットをドロップします。ルータがパケットの転送方法を認識している場合は、宛先の物理アドレスをネクスト ホップのアドレスに変更し、パケットを送信します。

ネクスト ホップが最終的な宛先ホストであることもあります。最終的な宛先ホストでない場合、ネクスト ホップは通常は別のルータであり、このルータが、同じスイッチング決定プロセスを実行します。パケットがインターネットワークを移動すると、その物理アドレスは変化しますが、プロトコル アドレスは一定のままです。

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、ルート情報が含まれるルーティング 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。宛先ホップまたはネクスト ホップの関連付けは、最後の宛先に達するまで、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をルータに示します。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、他の情報を含めることもできます。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は、マルチ コンテキスト モードのアクティブ/アクティブ フェールオーバーでのみサポートされます。詳細については、「アクティブ/アクティブ フェールオーバーの設定」（P.10-9）を参照してください。

サポートされるルート タイプ

ルータで使用可能な複数のルート タイプがあります。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

スタティック ルーティング アルゴリズムは実際にはアルゴリズムではなく、ルーティングの開始前にネットワーク管理者によって確立されるテーブル マッピングです。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）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、一般にロード シェアリングと呼ばれ、スループットと信頼性が大幅に向上することです。

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、ルーティング テーブルと XLATE テーブルの両方をルーティングの決定に使用します。宛先 IP 変換トラフィック、つまり、変換されていないトラフィックを処理するために、ASA は既存の XLATE またはスタティック変換を検索して出力インターフェイスを選択します。

この項は、次の内容で構成されています。

出力インターフェイスの選択プロセス

選択プロセスは次のとおりです。

1. 宛先 IP を変換する XLATE がすでに存在する場合は、パケットの出力インターフェイスは、ルーティング テーブルではなく XLATE テーブルから決定されます。
2. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換が存在する場合は、出力インターフェイスはスタティック ルートから決定されて XLATE が作成され、ルーティング テーブルは使用されません。
3. 宛先 IP を変換する XLATE が存在せず、一致するスタティック変換も存在しない場合は、パケットの宛先 IP 変換は実行されません。ASA は、ルートをルックアップして出力インターフェイスを選択することでこのパケットを処理し、次に発信元 IP 変換が（必要に応じて）実行されます。

   通常のダイナミック発信 NAT では、最初の発信パケットは、ルート テーブルを使用し、XLATE を作成することでルーティングされます。着信返送パケットは、既存の XLATE だけを使用して転送されます。スタティック NAT では、宛先変換された着信パケットは、常に既存の XLATE またはスタティック変換ルールを使用して転送されます。

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ると、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。古いルートが古いインターフェイスから削除され、ルーティング プロセスで別のインターフェイスに接続する場合は、誤ったインターフェイスに転送されるか、生成されたレベル 6 の syslog メッセージ 110001（ホストへのルートなし）でドロップされる可能性があります。

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。

この問題は、フローの最初のパケットの方向に応じて、実質的にすべてのトラフィックを発信元変換または宛先変換できる一部のセキュリティ トラフィック構成では、高い確率で発生します。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ことも、XLATE のタイムアウトによって自動的に解決することもできます。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、ASA を通じて常に同じ方法で転送されるようにします。

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、ルーティングに複数のインターネット 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。

  EIGRP の設定方法の詳細については、「EIGRP の設定」（P.30-3）を参照してください。

- 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。

OSPF の設定方法の詳細については、「OSPFv2 の設定」（P.28-5）を参照してください。

- 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。

  RIP の設定方法の詳細については、「RIP の設定」（P.29-4）を参照してください。

ルーティング テーブルに関する情報

この項は、次の内容で構成されています。

ルーティング テーブルの表示

ルーティング テーブルのエントリを表示するには、次のコマンドを入力します。

```
hostname# 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 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

ASA 5505 では、次のルートも表示されます。これは、内部ループバック インターフェイスであり、VPN ハードウェア クライアント機能によって個々のユーザ認証に使用されます。

```
C 127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
```

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 RIP、EIGRP、OSPF の各ルーティング 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、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。表 25-1 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 25-1　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
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
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。

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 および RIP 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、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、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し、そのエントリのネットワーク プレフィックス長がすべて同じ場合、同一のネットワーク プレフィックスおよび異なるインターフェイスを持つ 2 つのエントリはルーティング テーブル上で共存できません。
- 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、そのエントリのネットワーク プレフィックス長が異なる場合、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 ASA のインターフェイスに到着したとします。

```
hostname# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 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。

ダイナミック ルーティングとフェールオーバー

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）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。

アクティブ装置上でルーティング テーブルの変更がある場合、ダイナミック ルートはスタンバイ装置上で同期化されます。これは、アクティブ装置上のすべての追加、削除、または変更がすぐにスタンバイ装置に伝播されることを意味します。プライマリ装置が一定期間アクティブであった後にスタンバイ装置がアクティブになると、ルートがフェールオーバー バルク同期プロセスの一部として同期化されます。そのためアクティブ/スタンバイ フェールオーバー ペア上では、ルーティング テーブルが同じように表示されます。

スタティック ルートとそれらの設定方法の詳細については、「スタティック ルートおよびデフォルト ルートの設定」（P.26-3）を参照してください。

ダイナミック ルーティングおよびクラスタリング

ダイナミック ルーティングは、クラスタに完全に統合され、ルートはユニットで共有されます（クラスタでは最大 8 ユニットを使用できます）。ルーティング テーブル エントリは、クラスタのユニットにも複製されます。

1 つのユニットがスレーブからマスターに遷移すると、RIB テーブルのエポック番号（32 ビット シーケンス番号）が増加します。遷移後、新しいマスター ユニットには、まず以前のマスター ユニットのミラー イメージである RIB テーブル エントリが含まれます。さらに、再コンバージェンス タイマーが新しいマスター ユニットで開始されます。RIB テーブルのエポック番号が増加された場合、既存のすべてのエントリは古いと見なされます。IP パケットの転送は通常どおりに継続されます。新しいマスター ユニットで、ダイナミック ルーティング プロトコルが既存のルート エントリの更新または新しいエポック番号を持つ新しいルート エントリの作成を開始します。変更されたエントリまたは現在のエポック番号を持つ新しいエントリは、更新され、すべてのスレーブ ユニットと同期化されていることを示します。再コンバージェンス タイマーの期限が切れると、RIB テーブルの古いエントリが削除されます。OSPF ルート、RIP ルート、EIGRP ルートの RIB テーブル エントリはスレーブ ユニットに同期化されます。

バルク同期は、ユニットがクラスタに参加し、マスター ユニットから参加ユニットへのユニットである場合にのみ行われます。

ダイナミック ルーティング アップデートの場合、マスター ユニットが OSPF、RIP、または EIGRP によって取得した新しいルートを学習すると、マスター ユニットは、信頼できるメッセージ送信を介してすべてのスレーブ ユニットにアップデートを送信します。スレーブ ユニットはクラスタのルート アップデート メッセージを受信した後に RIB テーブルを更新します。

サポートされるダイナミック ルーティング プロトコル（OSPF、RIP、EIGRP）の場合、スレーブ ユニットのレイヤ 2 ロード バランシングのインターフェイスからのルーティング パケットがマスター ユニットに転送されます。マスター ユニットだけがダイナミック ルーティング プロトコル パケットを確認し、処理します。スレーブ ユニットがバルク同期を要求すると、レイヤ 2 ロード バランシングのインターフェイスを介して学習されたすべてのルーティング エントリが複製されます。

新しいルーティング エントリがマスター ユニットのレイヤ 2 ロード バランシングのインターフェイスを介して学習される場合、新しいエントリはすべてのスレーブ ユニットにブロードキャストされます。既存のルーティング エントリがネットワーク トポロジの変更が原因で変更された場合、変更されたエントリもすべてのスレーブ ユニットに同期化されます。既存のルーティング エントリがネットワーク トポロジの変更が原因で削除された場合、削除されたエントリもすべてのスレーブ ユニットに同期化されます。

レイヤ 2 およびレイヤ 3 ロード バランシングのインターフェイスの組み合わせがダイナミック ルーティング用に展開され、設定されている場合は、レイヤ 2 ロード バランシングのインターフェイスのマスター ユニットから RIB テーブルのエントリのみが同期化されるため、スレーブ ユニットは部分的なトポロジおよびルーティング プロセスのネイバー情報（レイヤ 3 ロード バランシングのインターフェイスを介して取得された詳細を含む）のみを持ちます。レイヤ 2 およびレイヤ 3 が異なるルーティング プロセスに属し、各ルーティング プロセスからの負荷を再配布するようにネットワークを設定する必要があります。

表 25-2 に、サポートされている設定の概要を示します。Yes は、2 つのプロセスの組み合わせ（レイヤ 2 に対する 1 つのプロセスおよびレイヤ 3 に対する 1 つのプロセス）が機能していることを示し、No は、2 つのプロセスの組み合わせが機能していないことを示しています。

表 25-2　サポートされている設定の概要

レイヤ 2 またはレイヤ 3	OSPF（レイヤ 3）	EIGRP（レイヤ 3）	RIP（レイヤ 3）
OSPF（レイヤ 2）	Yes	Yes	Yes
EIGRP（レイヤ 2）	Yes	No	Yes
RIP（レイヤ 2）	Yes	Yes	No

クラスタ内のすべてのユニットは、同じモード（シングル モードまたはマルチ コンテキスト モード）である必要があります。マルチ コンテキスト モードでは、マスタースレーブ同期は、同期メッセージにすべてのコンテキストおよびすべてのコンテキストの RIB テーブル エントリを含めます。

クラスタリングでは、レイヤ 3 インターフェイスを設定した場合は、router-id プール設定を実行設定する必要があります。

ダイナミック ルーティングおよびクラスタリングの詳細については、第 7 章「ASA のクラスタの設定」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 およびプレフィックス 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。	N/A
システム コンテキストでディセーブルになっています。		N/A
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。	N/A
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。	N/A
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。	N/A

（続き）EIGRP	OSPFv2 （続き）	ルート マップ およびプレフィックス リスト
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 クラスが導入されました。このリソース 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。

プロキシ ARP 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アクセス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、の 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 をディセーブルにしなければならない場合があります。

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、デフォルトにより、すべてのインターフェイス上でプロキシ ARP 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 が不要なインターフェイスに対してプロキシ ARP をディセーブルにする必要があります。

プロキシ ARP をディセーブルにするには、次のコマンドを入力します。

コマンド	目的
sysopt noproxyarp *interface* **例：** `hostname(config)# sysopt noproxyarp exampleinterface`	プロキシ ARP をディセーブルにする。