



# IP ルーティングおよび DHCP サービス の設定

---

この章では、FWSM で IP ルーティングと DHCP を設定する方法について説明します。内容は次のとおりです。

- [スタティック ルートおよびデフォルト ルートの設定 \(p.8-2\)](#)
- [OSPF の設定 \(p.8-5\)](#)
- [RIP の設定 \(p.8-18\)](#)
- [マルチキャスト ルーティングの設定 \(p.8-20\)](#)
- [非対称ルーティング サポートの設定 \(p.8-28\)](#)
- [DHCP の設定 \(p.8-30\)](#)

## スタティック ルートおよびデフォルト ルートの設定

ここでは、FWSM でスタティック ルートとデフォルト ルートを設定する方法を説明します。

マルチコンテキスト モードはダイナミック ルーティングをサポートしないので、ネットワークと FWSM の間にルータが配置されている場合など、FWSM が直接接続されていないネットワークには、スタティック ルートを使用する必要があります。

シングルコンテキスト モードでスタティック ルートを使用する状況は、次のとおりです。

- ネットワークで RIP または OSPF 以外の Router Discovery Protocol を使用する場合
- ネットワークが小規模で、スタティック ルートの管理が容易な場合
- ルーティング プロトコルに伴うトラフィックまたは CPU のオーバーヘッドが望ましくない場合

最も単純なオプションは、デフォルト ルートを設定してすべてのトラフィックをアップストリーム ルータへ送り、トラフィックのルーティングをルータに任せてしまうことです。ただし、デフォルト ゲートウェイが宛先ネットワークに到達できない場合もあるので、より具体的なスタティック ルートを設定することも必要です。たとえば、デフォルト ゲートウェイが外部の場合、FWSM に直接接続されていない内部ネットワークには、デフォルト ルートからトラフィックを転送できません。

透過ファイアウォール モードでは、FWSM を発信元とする、直接接続されていないネットワークを宛先とするトラフィックには、どのインターフェイスからトラフィックを送信するのかを FWSM が認識できるように、デフォルト ルートまたはスタティック ルートのどちらかを設定する必要があります。FWSM が発信元になるトラフィックには、システム ログ サーバ、Websense/N2H2 サーバ、AAA サーバなどへの通信が含まれます。単一のデフォルト ルートから到達できないサーバがある場合は、スタティック ルートを設定しなければなりません。



(注)

管理トラフィックの戻りパスを指定するために必要な、透過ファイアウォールのデフォルト ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにのみ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別するスタティック ルートを指定する必要があります。

FWSM は、インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまでサポートするので、負荷分散が可能です。

ここでは、次の内容について説明します。

- [スタティック ルートの設定 \(p.8-3\)](#)
- [デフォルト ルートの設定 \(p.8-4\)](#)

IPv6 スタティック / デフォルト ルートの設定の詳細については、「[IPv6 デフォルト / スタティック ルートの設定](#)」(p.9-6) を参照してください。

## スタティック ルートの設定

スタティック ルートを追加するには、次のコマンドを入力します。

```
hostname(config)# route if_name dest_ip mask gateway_ip [distance]
```

*dest\_ip* と *mask* は宛先ネットワークの IP アドレスで、*gateway\_ip* はネクストホップ ルータのアドレスです。

*distance* はルートの管理ディスタンスです。値を指定しなかった場合、デフォルトの 1 が使用されます。管理ディスタンスは、異なるルーティング プロトコル間のルートを比較するためのパラメータです。スタティック ルートのデフォルト管理ディスタンスは 1 で、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優先します。ただし、直接接続されたルートには優先しません。OSPF によって検出されたルートのデフォルト管理ディスタンスは 110 です。スタティック ルートのデフォルト管理ディスタンスがダイナミック ルートと同じ場合、スタティック ルートが優先します。接続されたルートは常に、スタティック ルートまたは動的に検出されたルートに優先します。

指定したゲートウェイが使用不能になった場合でも、スタティック ルートはルーティング テーブルに残ります。指定したゲートウェイが使用不能になった場合、スタティック ルートをルーティング テーブルから手動で削除する必要があります。ただし、関連するインターフェイスがダウンすると、スタティック ルートはルーティング テーブルから削除されます。インターフェイスが元に戻ると、スタティック ルートは復旧します。



(注)

管理ディスタンスの値を FWSM 上で実行されているルーティング プロトコルの管理ディスタンスよりも大きくしてスタティック ルートを作成すると、このルーティング プロトコルによって検出された指定の宛先へのルートは、スタティック ルートに優先します。スタティック ルートは、動的に検出されたルートがルーティング テーブルから削除された場合にのみ使用されます。

次に、10.1.1.0/24 宛てのすべてのトラフィックを、内部インターフェイスに接続されたルータ (10.1.2.45) に送信するスタティック ルートを作成する例を示します。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまで定義できます。ECMP は複数のインターフェイス間ではサポートされていません。ECMP では、トラフィックは必ずしもルート間で均等に分割されるわけではありません。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。

次に、外部インターフェイス上の 3 台のゲートウェイにトラフィックを転送する、コストの等しいスタティック ルートの例を示します。FWSM は、指定したゲートウェイ間にトラフィックを分配します。

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

## デフォルト ルートの設定

デフォルト ルートでは、FWSM が、学習したルートまたはスタティック ルートのないすべての IP パケットを送信するゲートウェイ IP アドレスを識別します。デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。特定の宛先が識別されたルートは、デフォルト ルートに優先されます。

デバイスごとに、コストの等しいデフォルト ルート エントリを 3 つまで定義できます。コストの等しいデフォルト ルート エントリを複数定義すると、デフォルト ルートに送信されたトラフィックは、指定したゲートウェイ間に分配されます。複数のデフォルト ルートを定義する場合、各エントリに対して同じインターフェイスを指定する必要があります。

コストの等しいデフォルト ルート エントリを 3 つより多く定義しようとする、または定義済みのデフォルト ルートとは異なるインターフェイスでデフォルト ルートを定義しようとする、**「ERROR: Cannot add route entry, possible conflict with existing routes.」** というメッセージが表示されず。

デフォルト ルートを定義するには、次のコマンドを入力します。

```
hostname(config)# route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance]
```



### ヒント

宛先ネットワーク アドレスおよびマスクに、0.0.0.0 0.0.0.0 ではなく 00 を入力できます。例を示します。

```
hostname(config)# route outside 0 0 192.168.1 1
```

次に、コストの等しい 3 つのデフォルト ルートが設定された FWSM の例を示します。FWSM が受信したトラフィックで、スタティック ルートまたは学習したルートのないものは、IP アドレス 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイ間に分配されます。

```
hostname(config)# route outside 0 0 192.168.2.1
hostname(config)# route outside 0 0 192.168.2.2
hostname(config)# route outside 0 0 192.168.2.3
```

## OSPF の設定

ここでは、OSPF の設定方法について説明します。内容は次のとおりです。

- [OSPF の概要 \(p.8-5\)](#)
- [OSPF のイネーブル化 \(p.8-6\)](#)
- [OSPF プロセス間でのルートの再分配 \(p.8-7\)](#)
- [OSPF インターフェイスパラメータの設定 \(p.8-9\)](#)
- [OSPF エリアパラメータの設定 \(p.8-11\)](#)
- [OSPF NSSA の設定 \(p.8-12\)](#)
- [OSPF エリア間のルート集約の設定 \(p.8-13\)](#)
- [OSPF へのルート再分配時のルート集約の設定 \(p.8-14\)](#)
- [デフォルトルートの生成 \(p.8-14\)](#)
- [ルート計算タイマーの設定 \(p.8-15\)](#)
- [ネイバのアップまたはダウンのロギング \(p.8-16\)](#)
- [OSPF アップデートパケットペーシングの表示 \(p.8-16\)](#)
- [OSPF のモニタリング \(p.8-17\)](#)
- [OSPF プロセスの再起動 \(p.8-17\)](#)

## OSPF の概要

OSPF では、リンクステートアルゴリズムを使用し、既知のすべての宛先に到達する最短経路を作成して算出します。OSPF エリア内の各ルータには同じリンクステートデータベースが与えられます。このデータベースは、ルータが使用できるインターフェイスと到達できるネイバを個々に指定したリストです。

OSPF over RIP の利点は、次のとおりです。

- OSPF リンクステートデータベースのアップデートは、RIP のアップデートほど頻繁には送信されません。また、リンクステートデータベースの場合、古い情報は期限切れになるので、アップデートが緩慢ではなく瞬間的に行われます。
- ルーティングはコストに基づいて決定されます。コストとは、パケットを特定のインターフェイスに送信するために必要なオーバーヘッドを指します。FWSM は、宛先へのホップ数ではなくリンクの帯域幅に基づいてコストを計算します。優先経路を指定する目的で、コストを設定できます。

最短経路を優先させるアルゴリズムの短所は、多くの CPU サイクルとメモリが必要になることです。

FWSM は、OSPF プロトコルのプロセスを 2 つ同時に、異なるインターフェイスセット上で実行できます。複数のインターフェイスで同じ IP アドレスを使用する場合に、2 つのプロセスを実行しなければならない場合があります (NAT はこのようなインターフェイスの共存を認めますが、OSPF はアドレスのオーバーラップを認めません)。または、一方のプロセスを内部で、他方を外部で実行し、2 つのプロセス間でルートのサブセットを再分配したいという場合もあります。プライベートアドレスをパブリックアドレスから隔離しなければならないこともあります。

2 つの OSPF プロセス間での再分配がサポートされます。FWSM では、OSPF がイネーブルのインターフェイス上で設定したスタティックルートと接続ルートを、OSPF プロセスに再分配することもできます。OSPF がイネーブルの場合、FWSM で RIP をイネーブルにすることはできません。RIP と OSPF 間の再分配はサポートされません。

FWSM は次の OSPF 機能をサポートします。

- エリア内ルート、エリア間ルート、および外部（タイプ I、タイプ II）ルートのサポート
- 仮想リンクのサポート
- OSPF LSA フラッドイング
- OSPF パケットの認証（パスワードおよび MD5 認証の両方）
- FWSM を指定ルータまたは指定バックアップ ルータとして設定。FWSM を Area Boundary Router（ABR; エリア境界ルータ）として設定することもできますが、FWSM を ASBR として設定する機能はデフォルト情報のみ（デフォルトルートの導入など）に限定されています。
- スタブエリアおよび Not-So-Stubby-Area のサポート
- ABR タイプ 3 LSA フィルタリング
- スタティック アドレス変換およびグローバルアドレス変換のアドバタイズ

## OSPF のイネーブル化

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、ルーティング プロセスに対応する IP アドレス範囲を指定し、さらに IP アドレス範囲に対応するエリア ID を割り当てる必要があります。



(注)

RIP がイネーブルの場合、OSPF をイネーブルにすることはできません。

OSPF を設定する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、OSPF ルーティング プロセスを作成します。

```
hostname(config)# router ospf process_id
```

このコマンドによって、この OSPF プロセスに対応するルータ コンフィギュレーション モードが開始されます。

*process\_id* は、このルーティング プロセスを識別するための内部 ID です。任意の正の整数を指定できます。内部で使用するだけなので、この ID を他のデバイスの ID と一致させる必要はありません。最大 2 つのプロセスを使用できます。

**ステップ 2** 次のコマンドを入力して、OSPF を実行する IP アドレスを定義し、さらにそのインターフェイスのエリア ID を定義します。

```
hostname(config-router)# network ip_address mask area area_id
```

次に、OSPF をイネーブルに設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0
```

## OSPF プロセス間でのルートの再分配

FWSM は、OSPF ルーティング プロセス間におけるルートの再分配を制御できます。FWSM は、**redistribute** コマンドの設定値に従って、またはルート マップを使用することによって、ルートを照合して変更します。ルート マップのその他の用途については、「[デフォルト ルートの生成 \(p.8-14\)](#)」も参照してください。



(注) FWSM は、ルーティング プロトコル間ではルートを再分配できません。ただし、FWSM はスタティック ルートと接続ルートを再分配できます。

ここでは、次の内容について説明します。

- ルート マップの追加 (p.8-7)
- OSPF プロセスへのスタティック ルート、接続ルート、または OSPF ルートの再分配 (p.8-8)

### ルート マップの追加

ルート マップを定義する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、ルート マップ エントリを作成します。

```
hostname(config)# route-map name {permit | deny} [sequence_number]
```

ルート マップ エントリは順番に読み取られます。*sequence\_number* オプションを使用すると、順番を指定できます。順番を指定しなかった場合、FWSM はエントリが追加された順番に従います。

**ステップ 2** 1 つまたは複数の **match** コマンドを入力します。

- 宛先ネットワークが標準アクセス リストと一致するルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match ip address acl_id [acl_id] [...]
```

複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。

- メトリックが指定されたルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match metric metric_value
```

*metric\_value* には 0 ~ 4,294,967,295 を指定できます。

- ネクスト ホップ ルータ アドレスが標準アクセス リストと一致するルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match ip next-hop acl_id [acl_id] [...]
```

複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。

- ネクスト ホップ インターフェイスが指定されているルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match interface if_name
```

複数のインターフェイスを指定した場合、いずれかのインターフェイスが一致するルートを検出します。

- 標準アクセス リストと一致するルータによってアドバタイズされたルートを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

複数のアクセス リストを指定した場合、いずれかのアクセス リストが一致するルートを検出します。

- ルート タイプを照合する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# match route-type {internal | external [type-1 | type-2]}
```

**ステップ 3** 1 つまたは複数の **set** コマンドを入力します。

ルートが **match** コマンドと一致すると、次の **set** コマンドによって、再分配の前にルートに対して実行するアクションが決まります。

- メトリックを設定する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# set metric metric_value
```

*metric\_value* には 0 ~ 294,967,295 の任意の値を指定できます。

- メトリック タイプを設定する場合は、次のコマンドを入力します。

```
hostname(config-route-map)# set metric-type {type-1 | type-2}
```

次に、ホップ カウントが 1 のルートを再分配する例を示します。FWSM は、メトリックが 5、メトリック タイプが Type 1、タグが 1 の外部 LSA として、これらのルートを再分配します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
```

## OSPF プロセスへのスタティック ルート、接続ルート、または OSPF ルートの再分配

ある OSPF プロセスから別の OSPF プロセスにスタティック ルート、接続ルート、または OSPF ルートを再分配する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、再分配先の OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

**ステップ 2** 次のコマンドを入力して、再分配するルートを指定します。

```
hostname(config-router)# redistribute {ospf process_id
[match {internal | external 1 | external 2}] | static | connect} [metric metric-value]
[metric-type {type-1 | type-2}] [tag tag_value] [subnets] [route-map map_name]
```

**ospf process\_id**、**static**、および **connect** キーワードでは、どこからルートを再分配するかを指定します。



このコマンドのオプションを使用して、ルートプロパティを照合したり設定したりできます。またはルートマップを使用することもできます。**tag** オプションおよび **subnets** オプションに相当するオプションは、**route-map** コマンドにはありません。ルートマップと **redistribute** コマンドのオプションを両方とも使用する場合は、両方を一致させる必要があります。

メトリックが 1 のルートと照合することによって、OSPF プロセス 1 から OSPF プロセス 2 にルートを再分配する例を示します。FWSM はメトリックが 5、メトリックタイプが Type 1、タグが 1 の外部 LSA として、これらのルートを再分配します。

```
hostname(config)# route-map 1-to-2 permit
hostname(config-route-map)# match metric 1
hostname(config-route-map)# set metric 5
hostname(config-route-map)# set metric-type type-1
hostname(config-route-map)# set tag 1
hostname(config-route-map)# router ospf 2
hostname(config-router)# redistribute ospf 1 route-map 1-to-2
```

次に、指定した OSPF プロセスのルートが OSPF プロセス 109 に再分配される例を示します。OSPF メトリックは 100 に再マッピングされます。

```
hostname(config)# router ospf 109
hostname(config-router)# redistribute ospf 108 metric 100 subnets
```

次に、リンクステートコストが 5、メトリックタイプが外部に設定されたルートの再分配の例を示します。この場合、内部メトリックよりプライオリティが下がります。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute ospf 2 metric 5 metric-type external
```

## OSPF インターフェイスパラメータの設定

必要に応じて、インターフェイス固有の OSPF パラメータを一部変更できます。これらのパラメータは、特に変更する必要はありませんが、次のインターフェイスパラメータについては、接続先ネットワーク上のすべてのルータで一致している必要があります。**ospf hello-interval**、**ospf dead-interval**、および **ospf authentication-key** です。これらのパラメータを設定する場合には、ネットワーク上のすべてのルータのコンフィギュレーションに矛盾しない値が設定されていることを確認してください。

OSPF インターフェイスパラメータを設定する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、インターフェイスコンフィギュレーションモードを開始します。

```
hostname(config)# interface if_name
```

**ステップ 2** 次のコマンドを任意で入力します。

- インターフェイスの認証タイプを指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf authentication [message-digest | null]
```
- OSPF 簡易パスワード認証を使用するネットワークセグメント上で、近接する OSPF ルータが使用するパスワードを割り当てる場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf authentication-key key
```

*key* には、長さ 8 バイトまでの連続する任意の文字列を指定できます。

このコマンドによって作成されたパスワードは、FWSM のソフトウェアがルーティングプロトコルパケットを発信するときに、OSPF ヘッダーに直接挿入するキーとして使用されます。インターフェイス単位で、ネットワークごとに異なるパスワードの割り当てが可能です。OSPF 情報を交換できるように、同一ネットワーク上のすべての近接ルータに、同じパスワードを与える必要があります。

- OSPF インターフェイス上でのパケット送信コストを明示的に指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf cost cost
```

*cost* は 1 ~ 65,535 の整数です。

- hello パケットの最後の受信から、デバイスで近接する OSPF ルータのダウンを宣言するまでの待機時間 (秒) を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf dead-interval seconds
```

この値は、ネットワーク上のすべてのノードで一致させる必要があります。

- FWSM が OSPF インターフェイス上で送信する hello パケットの時間間隔を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf hello-interval seconds
```

この値は、ネットワーク上のすべてのノードで一致させる必要があります。

- OSPF MD5 認証をイネーブルにするには、次のコマンドを入力します。

```
hostname(config-interface)# ospf message-digest-key key_id md5 key
```

次の値を設定します。

- *key\_id* — 1 ~ 255 の範囲の ID
- *key* — 最大 16 バイトの英数字パスワード

通常、1 つのインターフェイスに 1 つのキーを使用して、パケットの送信時に認証情報を生成し、着信パケットを認証します。近接するルータの同じキー ID には同じキー値を与える必要があります。

1 つのインターフェイスに複数のキーを使用しないことを推奨します。新しいキーを追加するたびに古いキーを削除し、ローカルシステムが、古いキーを知っている好ましくないシステムといつまでも通信しないようにしてください。古いキーを削除することによって、ロールオーバー時のオーバーヘッドも軽減されます。

- ネットワーク用の OSPF 指定ルータを決定するときに役立つプライオリティを設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf priority number_value
```

*number\_value* は 0 ~ 255 です。

- OSPF インターフェイスに属している隣接ノードへの LSA 再送信間隔 (秒) を指定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf retransmit-interval seconds
```

*seconds* は、接続ネットワーク上の 2 つのルータ間で予期される往復遅延より大きくする必要があります。値の範囲は 1 ~ 65,535 秒です。デフォルトは 5 秒です。

- OSPF インターフェイス上でリンク ステート アップデート パケットを送信するときに必要な推定秒数を設定する場合は、次のコマンドを入力します。

```
hostname(config-interface)# ospf transmit-delay seconds
```

*seconds* は 1 ~ 65,535 秒です。デフォルトは 1 秒です。

次に、OSPF インターフェイスを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# network 2.0.0.0 255.0.0.0 area 0
hostname(config-router)# interface inside
hostname(config-interface)# ospf cost 20
hostname(config-interface)# ospf retransmit-interval 15
hostname(config-interface)# ospf transmit-delay 10
hostname(config-interface)# ospf priority 20
hostname(config-interface)# ospf hello-interval 10
hostname(config-interface)# ospf dead-interval 40
hostname(config-interface)# ospf authentication-key cisco
hostname(config-interface)# ospf message-digest-key 1 md5 cisco
hostname(config-interface)# ospf authentication message-digest
```

次に、**show ospf** コマンドの出力例を示します。

```
hostname(config)# show ospf

Routing Process "ospf 2" with ID 20.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x      0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x 209a3
    Number of opaque link LSA 0. Checksum Sum 0x      0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

## OSPF エリア パラメータの設定

複数のエリア パラメータを設定できます。これらのエリア パラメータ（次の作業手順を参照）には、認証の設定、スタブ エリアの定義、およびデフォルトの集約ルートへの特定コストの割り当てが含まれます。認証により、エリアへの不正アクセスに対して、パスワードベースの保護が提供されます。

スタブ エリアは、外部ルート情報が送信されないエリアです。その代わりに、スタブ エリアには、Autonomous System (AS; 自律システム) 外部の宛先について、ABR が生成したデフォルトの外部ルートが設定されます。OSPF のスタブ エリア サポートを有効に利用するには、スタブ エリアでデフォルトのルーティングを使用する必要があります。スタブ エリアに送信される LSA 数を減らすには、ABR に **area stub** コマンドの **no-summary** キーワードを設定して、ABR からスタブ エリアへの集約リンク アドバタイズ (LSA タイプ 3) の送信を阻止できます。

ネットワークのエリア パラメータを指定する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

**ステップ 2** 次のコマンドを任意で入力します。

- OSPF エリアの認証をイネーブルにするには、次のコマンドを入力します。  
hostname(config-router)# area area-id authentication
  - OSPF エリアの MD5 認証をイネーブルにするには、次のコマンドを入力します。  
hostname(config-router)# area area-id authentication message-digest
  - エリアをスタブ エリアとして定義するには、次のコマンドを入力します。  
hostname(config-router)# area area-id stub [no-summary]
  - スタブ エリアで使用するデフォルトの集約ルートに、特定のコストを割り当てるには、次のコマンドを入力します。  
hostname(config-router)# area area-id default-cost cost
- cost* は 1 ～ 65,535 の整数です。デフォルトは 1 です。

次に、OSPF エリア パラメータを設定する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# area 0 authentication
hostname(config-router)# area 0 authentication message-digest
hostname(config-router)# area 17 stub
hostname(config-router)# area 17 default-cost 20
```

## OSPF NSSA の設定

OSPF NSSA は OSPF スタブ エリアと似ています。NSSA では、コアからエリアへのタイプ 5 外部 LSA のフラッドは実行されませんが、限定された方法で、AS の外部ルートをエリア内にインポートできます。

NSSA では、再分配により、NSSA エリア内にタイプ 7 AS 外部ルートをインポートします。これらのタイプ 7 LSA は、NSSA の ABR によってタイプ 5 LSA に変換され、ルーティング ドメイン全体へフラッドされます。変換時には、集約およびフィルタリングがサポートされます。

OSPF を使用している中央サイトから別のルーティング プロトコルを使用しているリモートサイトに接続する必要がある ISP またはネットワーク管理者は、NSSA を使用して管理を簡素化できます。

スタブ エリアにはリモートサイトのルートが再分配されないため、NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続に OSPF スタブ エリアを利用できず、2 つのルーティング プロトコルを維持する必要がありました。一般的には RIP などの簡易プロトコルを使用し、再分配を行っていました。NSSA の実装により、企業ルータとリモート ルータ間のエリアを NSSA として定義することで、リモート接続にも OSPF を適用できます。

OSPF NSSA の設定に必要なネットワークのエリア パラメータを指定する手順は、次のとおりです。

- ステップ1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

- ステップ2** 次のコマンドを任意で入力します。

- NSSA エリアを定義するには、次のコマンドを入力します。

```
hostname(config-router)# area area-id nssa [no-redistribution]  
[default-information-originate]
```

- アドレス グループを集約するには、次のコマンドを入力します。

```
hostname(config-router)# summary address ip_address mask [not-advertise] [tag tag]
```

このコマンドは、ルーティング テーブルの容量縮小に有効です。OSPF にこのコマンドを使用すると、OSPF ASBR によって、アドレスに含まれるすべての再分配ルートを集約したものとして、外部ルートが1つアドバタイズされます。

OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

次の例では、集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれていません。外部 Link State Advertisement (LSA; リンク ステート アドバタイズメント) では、アドレス 10.1.0.0 だけがアドバタイズされます。

```
hostname(config-router)# summary-address 10.1.1.0 255.255.0.0
```

この機能を使用する前に、次の注意事項を考慮してください。

- 外部の宛先に到達するためのタイプ7デフォルトルートを設定できます。この設定により、ルータは NSSA または NSSA の ABR が使用するタイプ7デフォルトルートを生成します。
- 同じエリア内のすべてのルータは、そのエリアが NSSA であることを認識している必要があります。認識していないと、ルータ間の通信ができません。

## OSPF エリア間のルート集約の設定

ルート集約は、アドバタイズされたアドレスの統合を意味します。この機能により、ABR から他のエリアに、1つの集約ルートだけをアドバタイズできます。OSPF では、ABR が1つのエリアのネットワークを別のエリアにアドバタイズします。1つのエリア内のネットワーク番号が連続して割り当てられている場合、そのエリア内のすべてのネットワークが指定範囲内に収まる1つの集約ルートを生成し、そのルートだけがアドバタイズされるように、ABR を設定できます。

ルート集約のアドレス範囲を定義する手順は、次のとおりです。

- ステップ1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

- ステップ2** 次のコマンドを入力して、アドレス範囲を設定します。

```
hostname(config-router)# area area-id range ip-address mask [advertise | not-advertise]
```

次に、OSPF エリア間のルート集約を設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# area 17 range 12.1.0.0 255.255.0.0
```

## OSPF へのルート再分配時のルート集約の設定

他のプロトコルからのルートが OSPF に再分配される場合、各ルートは外部 LSA により個別にアドバタイズされます。ただし、ネットワーク アドレスとマスクの範囲を指定することにより、範囲内のすべての再分配ルートを含む単一ルートがアドバタイズされるように、FWSM を設定できます。この設定により、OSPF リンク ステート データベースのサイズを縮小できます。

指定したネットワーク アドレスとマスクの範囲内のすべての再分配ルートを 1 つの集約ルートとしてアドバタイズする手順は、次のとおりです。

- ステップ 1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 次のコマンドを入力して、集約アドレスを設定します。

```
hostname(config-router)# summary-address ip_address mask [not-advertise] [tag tag]
```

OSPF は **summary-address 0.0.0.0 0.0.0.0** をサポートしません。

次に、ルート集約を設定する例を示します。集約アドレス 10.1.0.0 にアドレス 10.1.1.0、10.1.2.0、10.1.3.0 などが含まれています。外部 LSA では、アドレス 10.1.0.0 だけがアドバタイズされます。

```
hostname(config)# router ospf 1
hostname(config-router)# summary-address 10.1.0.0 255.255.0.0
```

## デフォルトルートの生成

ASBR に、OSPF ルーティング ドメインへのデフォルト ルートを強制的に生成させることができます。OSPF ルーティング ドメインへのルート再分配を明確に設定すると、ルータは自動的に ASBR になります。ただし、ASBR のデフォルトでは、OSPF ルーティング ドメインへのデフォルト ルートは生成されません。

デフォルト ルートを生成する手順は、次のとおりです。

- ステップ 1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

**ステップ 2** 次のコマンドを入力して、ASBR にデフォルト ルートを強制的に生成させます。

```
hostname(config-router)# default-information originate [always] [metric metric-value]
[metric-type {1 | 2}] [route-map map-name]
```

---

次に、デフォルト ルートを生成する例を示します。

```
hostname(config)# router ospf 2
hostname(config-router)# default-information originate always
```

## ルート計算タイマーの設定

OSPF がトポロジー変更を受信してから、SPF の計算を開始するまでの遅延時間を設定できます。また、2 つの連続する SPF 計算の間隔となるホールドタイムを設定できます。

ルート計算タイマーを設定する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

**ステップ 2** 次のコマンドを入力して、ルート計算時間を設定します。

```
hostname(config-router)# timers spf spf-delay spf-holdtime
```

*spf-delay* には、OSPF がトポロジー変更を受信してから、SPF 計算を開始するまでの遅延時間（秒）を指定します。0 ～ 65,535 の整数を指定できます。デフォルトは 5 秒です。0 の値は遅延がないことを意味するので、SPF 計算がただちに開始されます。

*spf-holdtime* で、連続する 2 回の SPF 計算の最小間隔（秒）を指定します。0 ～ 65,535 の整数を指定できます。デフォルトは 10 秒です。0 を指定すると遅延は発生しません。1 つの SPF 計算の終了後、ただちに次の SPF 計算が開始されます。

次に、ルート計算タイマーを設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# timers spf 10 120
```

## ネイバのアップまたはダウンのロギング

デフォルトでは、OSPF ネイバがアップまたはダウンになると、システム メッセージが送信されません。

**debug ip ospf adjacency** コマンドを実行しないで、OSPF ネイバのアップまたはダウンを調べる場合には、ロギングを設定します。**log-adj-changes** ルータ コンフィギュレーション コマンドを使用すると、少ない出力で、高いレベルのピア関係情報が得られます。各ステート変更のメッセージを表示する場合には、**log-adj-changes detail** を設定します。

ネイバのアップまたはダウンをロギングする手順は、次のとおりです。

- ステップ 1** 次のコマンドを入力して、設定する OSPF プロセスに対応するルータ コンフィギュレーション モードを開始します（まだ開始していない場合）。

```
hostname(config)# router ospf process_id
```

- ステップ 2** 次のコマンドを入力して、ネイバのアップ / ダウンに関するロギングを設定します。

```
hostname(config-router)# log-adj-changes [detail]
```



- (注) 送信するネイバのアップ / ダウン メッセージに対して、ロギングをイネーブルにする必要があります。

次に、ネイバのアップ / ダウン メッセージをロギングする例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# log-adj-changes detail
```

## OSPF アップデート パケット ペーシングの表示

OSPF アップデート パケットは、自動的にペーシングされるので、最低 33 ミリ秒の間隔をあけて送信されます。ペーシングが実行されないと、リンクが遅い状況で一部のアップデート パケットが失われたり、ネイバが適切な速度でアップデートを受信できなかったり、ルータのバッファ スペースが不足したりする可能性があります。たとえば、次のいずれかのトポロジーの場合、ペーシングを行わないと、パケットが廃棄されることがあります。

- ポイントツーポイント リンクを使用して高速ルータを低速ルータに接続する場合
- フラッドイング中に、複数のネイバが 1 つのルータに同時にアップデートを送信する場合

再送信の場合にも、効率を向上させて再送信時の損失を最小限に抑えるために、ペーシングが使用されます。インターフェイスからの送待を待機している LSA を表示することもできます。ペーシングには、OSPF のアップデート パケットと再送信パケットをより効率的に送信できるという利点があります。

この機能は自動的にサポートされるので、設定を行う必要はありません。

指定したインターフェイス上でフラッドイングされる待機中 LSA のリストを表示し、OSPF パケット ペーシングを確認するには、次のコマンドを入力します。

```
hostname# show ospf flood-list if_name
```



## OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の統計情報を表示できます。提供された情報を使用して、リソース利用状況を判別したり、ネットワークの問題を解決したりできます。また、ノードへの到達可能性情報を表示したり、デバイスのパケットがネットワーク上で使用しているルーティングパスを検出したりすることもできます。

各種のルーティング統計情報を表示するには、必要に応じて、次のいずれかの作業を行います。

- OSPF ルーティング プロセスに関する一般情報を表示するには、次のコマンドを入力します。  
`hostname# show ospf [process-id [area-id]]`
- ABR および ASBR への内部 OSPF 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 ospf border-routers`
- 特定のルータについて、OSPF データベース関連の情報リストを表示するには、次のコマンドを入力します。  
`hostname# show ospf [process-id [area-id]] database`
- (OSPF パケット ペーシングを確認するために) 指定したインターフェイス上でフラッディングを待機中の LSA のリストを表示するには、次のコマンドを入力します。  
`hostname# show ospf flood-list if-name`
- OSPF 関連のインターフェイス情報を表示するには、次のコマンドを入力します。  
`hostname# show ospf interface [if_name]`
- OSPF ネイバ情報をインターフェイス単位で表示するには、次のコマンドを入力します。  
`hostname# show ospf neighbor [if-name] [neighbor-id] [detail]`
- ルータが要求したすべての LSA のリストを表示するには、次のコマンドを入力します。  
`hostname# show ospf request-list neighbor if_name`
- 再送信待ちになっているすべての LSA のリストを表示するには、次のコマンドを入力します。  
`hostname# show ospf retransmission-list neighbor if_name`
- OSPF プロセスに基づいて設定したすべての集約アドレス再分配情報のリストを表示するには、次のコマンドを入力します。  
`hostname# show ospf [process-id] summary-address`
- OSPF 関連の仮想リンク情報を表示するには、次のコマンドを入力します。  
`hostname# show ospf [process-id] virtual-links`

## OSPF プロセスの再起動

OSPF プロセスを再起動し、再分配またはカウンタを消去するには、次のコマンドを入力します。

```
hostname(config)# clear ospf pid {process | redistribution | counters  
[neighbor [neighbor-interface] [neighbor-id]]}
```

## RIP の設定

ここでは、RIP の設定方法について説明します。内容は次のとおりです。

- [RIP の概要 \(p.8-18\)](#)
- [RIP のイネーブル化 \(p.8-18\)](#)

## RIP の概要

RIP をサポートするデバイスは、定期的におよびネットワーク トポロジー変更時に、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 RIP パケットには、装置が到達できるネットワークに関する情報とともに、パケットが宛先アドレスに到達するまでの間に通過するルータまたはゲートウェイの数が含まれます。RIP の方が OSPF より多くのトラフィックを生成しますが、初期設定は容易です。

RIP は、初期設定が容易であり、トポロジーの変更時にコンフィギュレーションを更新する必要がないので、スタティック ルートより有利です。RIP の短所は、スタティック ルーティングよりネットワークおよび処理のオーバーヘッドが増えることです。

FWSM では、限定バージョンの RIP を使用します。FWSM が到達できるネットワークを示す RIP アップデートは送信されません。ただし、次の方法の一方または両方を使用できます。

- **パッシブ RIP** — FWSM は、RIP アップデートを待ち受けませんが、インターフェイスからはネットワークに関するアップデートを送出しません。

パッシブ RIP を使用すると、FWSM は直接接続されていないネットワークについて学習できません。

- **デフォルトルートアップデート** — FWSM を介して到達可能なあらゆるネットワークを示した通常の RIP アップデートを送信する代わりに、FWSM は FWSM をデフォルトゲートウェイとして認識する参加デバイスまでのデフォルトルートを送信します。

デフォルトルート オプションは、パッシブ RIP と組み合わせて使用することも、単独で使用することもできます。FWSM 上でスタティック ルートを使用し、なおかつダウンストリームルータ上でスタティック ルートを設定しない場合は、デフォルトルート オプションを単独で使用します。通常、外部インターフェイスではデフォルトルート オプションをイネーブルにしません。FWSM がアップストリームルータのデフォルトゲートウェイになることはあまりないからです。

## RIP のイネーブル化

インターフェイス上で RIP をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# rip if_name {default | passive} [version {1 | 2}
[authentication {text | md5} key key_id]]
```

**rip** コマンドをそれぞれの方法について 1 回ずつ入力することで、インターフェイス上の RIP のパッシブ モードおよびデフォルト モードの両方をイネーブル化できます。コマンドの入力例を示します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpius 1
hostname(config)# rip inside passive version 2 authentication md5 scorpius 1
```

すべてのインターフェイスでパッシブ RIP をイネーブルにし、デフォルト ルートに関しては内部インターフェイスに限定してイネーブルにするという場合は、次のコマンドを入力します。

```
hostname(config)# rip inside default version 2 authentication md5 scorpius 1
hostname(config)# rip inside passive version 2 authentication md5 scorpius 1
hostname(config)# rip outside passive version 2 authentication md5 scorpius 1
```



(注)

コンフィギュレーションをテストする前に、FWSM に接続されたすべてのルータ上で、ARP キャッシュをフラッシュしてください。Cisco ルータの場合、**clear arp** コマンドを使用して ARP キャッシュをフラッシュします。

OSPF がイネーブルの場合、RIP をイネーブルにすることはできません。

## マルチキャスト ルーティングの設定

ここでは、マルチキャスト ルーティングの設定方法について説明します。内容は次のとおりです。

- [マルチキャスト ルーティングの概要 \(p.8-20\)](#)
- [マルチキャスト ルーティングのイネーブル化 \(p.8-20\)](#)
- [IGMP 機能の設定 \(p.8-21\)](#)
- [スタブ マルチキャスト ルーティングの設定 \(p.8-24\)](#)
- [スタティック マルチキャスト ルートの設定 \(p.8-24\)](#)
- [PIM 機能の設定 \(p.8-25\)](#)
- [マルチキャスト ルーティングの詳細について \(p.8-27\)](#)

### マルチキャスト ルーティングの概要

FWSM はスタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートします。ただし、1 つの FWSM で両方を同時に設定することはできません。

スタブ マルチキャスト ルーティングでは動的なホスト登録が行われるため、マルチキャスト ルーティングが効率化されます。スタブ マルチキャスト ルーティング用に設定された場合、FWSM は IGMP プロキシ エージェントとして機能します。FWSM はマルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージを、マルチキャスト データの配信を設定するアップストリームのマルチキャスト ルータに転送します。FWSM をスタブ マルチキャスト ルーティング用に設定した場合、PIM 用には設定できません。

FWSM は PIM-SM および双方向 PIM の両方をサポートします。PIM-SM は、ユニキャスト ルーティング情報ベースまたは別個のマルチキャスト 対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。マルチキャスト グループごとに、単一の Rendezvous Point (RP; ランデブー ポイント) をルートとする単方向の共有ツリーを作成します。また、任意でマルチキャストの送信元ごとに最短パス ツリーを作成します。

双方向 PIM は PIM-SM のバリエーションで、マルチキャストの送信元とレシーバーを接続する双方向の共有ツリーを作成します。双方向ツリーは、マルチキャスト トポロジーの各リンクで実行される DF 選定プロセスを使用して作成します。マルチキャスト データは DF を使用して送信元から RP へ、そして共有ツリーからレシーバーへ転送されます。送信元固有のステートは必要ありません。DF 選定は RP 検出時に行われ、RP へのデフォルト ルートを指定します。



(注)

FWSM が PIM RP の場合、FWSM の変換されていない外部アドレスを RP アドレスとして使用します。

### マルチキャスト ルーティングのイネーブル化

マルチキャスト ルーティングをイネーブル化すると、FWSM でマルチキャスト パケットを転送できます。マルチキャスト ルーティングをイネーブル化すると、すべてのインターフェイスで PIM と IGMP が自動的にイネーブルになります。マルチキャスト ルーティングをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# multicast-routing
```

マルチキャスト ルーティング テーブルのエントリ数は、システムの RAM の容量に制限されます。表 8-1 に、FWSM の RAM 容量に基づく、特定のマルチキャスト テーブルの最大エントリ数を示します。最大エントリ数に達すると、新規エントリはすべて廃棄されます。

表 8-1 マルチキャスト テーブルのエントリ制限

テーブル	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

## IGMP 機能の設定

IP ホストは IGMP を使用して、グループ メンバーシップを直接接続されているマルチキャストルータにレポートします。IGMP は、グループ アドレス (クラス D IP アドレス) をグループ ID として使用します。ホスト グループ アドレスには 224.0.0.0 ~ 239.255.255.255 の範囲を指定できます。アドレス 224.0.0.0 は、どのグループにも割り当てられません。アドレス 224.0.0.1 は、サブネット上のすべてのシステムに割り当てられます。アドレス 224.0.0.2 は、サブネット上のすべてのルータに割り当てられます。

FWSM でマルチキャストルーティングをイネーブルにすると、すべてのインターフェイスで IGMP Version 2 が自動的にイネーブルになります。



(注)

**show run** コマンドを使用すると、**no igmp** コマンドのみがインターフェイス コンフィギュレーションに表示されます。**multicast-routing** コマンドがデバイス コンフィギュレーションに表示されると、すべてのインターフェイスで自動的に IGMP がイネーブルになります。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。内容は次のとおりです。

- [インターフェイス上での IGMP のディセーブル化 \(p.8-21\)](#)
- [グループ メンバーシップの設定 \(p.8-22\)](#)
- [静的に加入するグループの設定 \(p.8-22\)](#)
- [マルチキャスト グループへのアクセスの制御 \(p.8-22\)](#)
- [インターフェイス上の IGMP ステート数の制限 \(p.8-23\)](#)
- [クエリー間隔とクエリータイムアウトの変更 \(p.8-23\)](#)
- [クエリー応答時間の変更 \(p.8-24\)](#)
- [IGMP バージョンの変更 \(p.8-24\)](#)

### インターフェイス上での IGMP のディセーブル化

特定のインターフェイスで IGMP をディセーブルにできます。これは、特定のインターフェイスにマルチキャスト ホストがないことがわかっていて、FWSM からそのインターフェイスにホストクエリーメッセージを送信しないようにする場合に役立ちます。

インターフェイス上で IGMP をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no igmp
```

インターフェイス上で IGMP を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# igmp
```



(注) `no igmp` コマンドのみがインターフェイス コンフィギュレーションに表示されます。

## グループ メンバーシップの設定

FWSM をマルチキャスト グループのメンバーにするように設定できます。FWSM をマルチキャスト グループに参加するように設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を保持して、そのグループのパスをアクティブにし続けます。

FWSM をマルチキャスト グループに参加させるには、次のコマンドを入力します。

```
hostname(config-if)# igmp join-group group-address
```

## 静的に加入するグループの設定

グループ メンバーがグループのメンバーシップをレポートできなかつたり、ネットワーク セグメントにグループのメンバーが存在しない場合でも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメントに送信しなければならないことがあります。このような場合、次のいずれかの方法で、そのグループのマルチキャスト トラフィックをセグメントに送信できます。

- `igmp join-group` コマンドを使用（「グループ メンバーシップの設定」 [p.8-22] を参照）。FWSM はマルチキャスト パケットを受信して転送することができます。
- `igmp static-group` コマンドを使用。FWSM はマルチキャスト パケットを受信せずに、指定されたインターフェイスに転送します。

静的に加入するマルチキャスト グループをインターフェイス上で設定するには、次のコマンドを入力します。

```
hostname(config-if)# igmp static-group group-address
```

## マルチキャスト グループへのアクセスの制御

FWSM インターフェイスのホストが参加できるマルチキャスト グループを制御するには、次の手順を実行します。

**ステップ 1** マルチキャスト トラフィックのアクセス リストを作成します。1 つのアクセス リストに複数のエントリを作成できます。拡張アクセス リストまたは標準アクセス リストを使用できます。

- 標準アクセス リストを作成するには、次のコマンドを入力します。

```
hostname(config)# access-list name standard [permit | deny] ip_addr mask
```

`ip_addr` 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

- 拡張アクセス リストを作成するには、次のコマンドを入力します。

```
hostname(config)# access-list name extended [permit | deny] protocol src_ip_addr  
src_mask dst_ip_addr dst_mask
```

`dst_ip_addr` 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

**ステップ 2** 次のコマンドを入力して、アクセスリストをインターフェイスに適用します。

```
hostname(config-if)# igmp access-group acl
```

*acl* 引数は、標準または拡張 IP アクセスリストの名前です。

## インターフェイス上の IGMP ステート数の制限

IGMP メンバーシップ レポートから生成される IGMP ステート数を、インターフェイス単位で制限できます。設定した制限を超えるメンバーシップ レポートは IGMP キャッシュに保存されず、超過したメンバーシップ レポートのトラフィックは転送されません。

インターフェイスの IGMP ステート数を制限するには、次のコマンドを入力します。

```
hostname(config-if)# igmp limit number
```

有効値の範囲は 0 ~ 500 で、500 がデフォルト値です。値を 0 に設定すると、学習したグループは追加されませんが、(**igmp join-group** および **igmp static-group** コマンドを使用して) 手で定義したメンバーシップは追加できます。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

## クエリー間隔とクエリー タイムアウトの変更

FWSM はクエリー メッセージを送信して、インターフェイスに接続されたネットワーク上でメンバーを持つマルチキャスト グループを検出します。メンバーが IGMP レポート メッセージに応答した場合、そのメンバーは特定グループのマルチキャスト パケットを受信したいことを示します。クエリー メッセージは、アドレスが 224.0.0.1 で Time To Live (TTL) の値が 1 の全システムのマルチキャスト グループ宛てに送信されます。

FWSM に保存されているメンバーシップ情報をリフレッシュするために、これらのメッセージは定期的に送信されます。FWSM はインターフェイスに接続されているマルチキャスト グループのローカル メンバーがいなくなったことを検出すると、そのグループのマルチキャスト パケットを接続されているネットワークに転送することをやめて、Prune メッセージをそのパケットの送信元に送り返します。

デフォルトでは、サブネット上の PIM 指定ルータがクエリー メッセージの送信を担当します。デフォルトでは、メッセージは 125 秒ごとに送信されます。この間隔を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-interval seconds
```

FWSM が指定したタイムアウト値 (デフォルトは 255 秒) の間インターフェイスでクエリー メッセージを受信しない場合、FWSM が指定ルータになり、クエリー メッセージの送信を開始します。このタイムアウト値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-timeout seconds
```



(注) **igmp query-timeout** および **igmp query-interval** コマンドでは IGMP Version 2 が必要です。

## クエリー応答時間の変更

デフォルトでは、IGMP クエリーでアドバタイズされる最大クエリー応答時間は 10 秒です。FWSM がこの時間内にホストクエリーへの応答を受信しない場合、そのグループを削除します。

最大クエリー応答時間を変更するには、次のコマンドを入力します。

```
hostname(config-if)# igmp query-max-response-time seconds
```

## IGMP バージョンの変更

デフォルトでは、FWSM は IGMP Version 2 を実行します。このプロトコルにより、**igmp query-timeout** や **igmp query-interval** コマンドなど複数の追加機能がイネーブルになります。

サブネット上のすべてのマルチキャスト ルータで、同じバージョンの IGMP がサポートされている必要があります。FWSM は Version 1 のルータを自動的に検出せず、Version 1 に切り替えます。ただし、サブネット上に IGMP Version 1 と Version 2 ホストを混在させることができます。すなわち、IGMP Version 1 ホストが存在する場合、IGMP Version 2 を実行する FWSM は正しく機能します。

インターフェイスで実行する IGMP のバージョンを制御するには、次のコマンドを入力します。

```
hostname(config-if)# igmp version {1 | 2}
```

## スタブ マルチキャスト ルーティングの設定

スタブ エリアへのゲートウェイとして機能する FWSM は、PIM に参加する必要はありません。代わりに、IGMP プロキシエージェントとして動作し、あるインターフェイスに接続されているホストから別のインターフェイス上のアップストリーム マルチキャスト ルータに IGMP メッセージを転送するように設定できます。FWSM を IGMP プロキシエージェントとして設定するには、ホスト ジョインを転送して、スタブ エリア インターフェイスからアップストリーム インターフェイスにメッセージを残します。

ホスト ジョインを転送してメッセージを残すには、スタブ エリアに接続されたインターフェイスから次のコマンドを入力します。

```
hostname(config-if)# igmp forward interface if_name
```



(注) スタブ マルチキャスト ルーティングと PIM は同時にはサポートされません。

## スタティック マルチキャスト ルートの設定

PIM を使用する場合、FWSM は同一インターフェイス上でのパケット受信を予期します（このインターフェイスからユニキャスト パケットを送信元に返します）。マルチキャスト ルーティングをサポートしないルートバイパスする場合など、ユニキャスト パケットとマルチキャスト パケットに別々のパスを使用させたいことがあります。

スタティック マルチキャスト ルートはアドバタイズまたは再分配されません。

PIM 用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask input_if_name [distance]
```



スタブ エリア用のスタティック マルチキャスト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name]
[distance]
```



(注) *dense output\_if\_name* キーワードと引数のペアは、スタブ マルチキャストルーティングに対してのみサポートされます。

## PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送する転送テーブルを管理します。FWSM でマルチキャストルーティングをイネーブルにすると、すべてのインターフェイスで PIM と IGMP が自動的にイネーブルになります。



(注) PIM は PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルでのみ動作するためです。

ここでは、任意の PIM 設定を行う方法について説明します。内容は次のとおりです。

- [インターフェイス上での PIM のディセーブル化 \(p.8-25\)](#)
- [スタティック RP アドレスの設定 \(p.8-26\)](#)
- [指定ルータのプライオリティの設定 \(p.8-26\)](#)
- [PIM Register メッセージのフィルタリング \(p.8-26\)](#)
- [PIM メッセージ間隔の設定 \(p.8-27\)](#)

## インターフェイス上での PIM のディセーブル化

特定のインターフェイスで PIM をディセーブルにできます。インターフェイス上で PIM をディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# no pim
```

インターフェイス上で PIM を再びイネーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# pim
```



(注) **no pim** コマンドのみがインターフェイス コンフィギュレーションに表示されます。

## スタティック RP アドレスの設定

一般的な PIM sparse (疎) モードまたは bidir ドメイン内のすべてのルータは、PIM RP アドレスを知っている必要があります。このアドレスは、**pim rp-address** コマンドを使用して静的に設定されます。



(注) FWSM は Auto-RP や PIM BSR をサポートしないため、ユーザは **pim rp-address** コマンドを使用して RP アドレスを指定する必要があります。

FWSM を複数グループの RP として設定できます。アクセスリストで指定されているグループ範囲によって、PIM RP グループ マッピングが決定されます。アクセスリストが指定されていない場合、そのグループの RP がマルチキャスト グループ範囲全体 (224.0.0.0/4) に適用されます。

PIM RP のアドレスを設定するには、次のコマンドを入力します。

```
hostname(config)# pim rp-address ip_address [acl] [bidir]
```

*ip\_address* 引数は、PIM RP となるルータのユニキャスト IP アドレスです。*acl* 引数は、RP を使用するマルチキャスト グループを指定するアクセスリストの名前または番号です。**bidir** キーワードを除外すると、グループは PIM sparse (疎) モードで動作します。



(注) 実際の bidir 設定に関係なく、FWSM は常に bidir 機能を PIM の hello メッセージでアドバタイズします。

## 指定ルータのプライオリティの設定

DR は、PIM レジスタ、ジョイン、Prune メッセージの RP への送信を担当します。ネットワーク セグメントに複数のマルチキャストルータがある場合、DR のプライオリティに基づいて DR を選択する選定プロセスが行われます。複数のデバイスが同じ DR プライオリティの場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、FWSM は DR プライオリティ 1 を持ちます。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim dr-priority num
```

*num* 引数には 1 ~ 4,294,967,294 の任意の値を指定できます。

## PIM Register メッセージのフィルタリング

PIM Register メッセージをフィルタリングするように FWSM を設定できます。PIM Register メッセージをフィルタリングするには、次のコマンドを入力します。

```
hostname(config)# pim accept-register {list acl | route-map map-name}
```

## PIM メッセージ間隔の設定

ルータ クエリー メッセージを使用して PIM DR を選定します。PIM DR はルータ クエリー メッセージの送信を担当します。デフォルトでは、ルータ クエリー メッセージは 30 秒ごとに送信されます。次のコマンドを入力して、この値を変更できます。

```
hostname(config-if)# pim hello-interval seconds
```

*seconds* 引数の有効値の範囲は 1 ～ 3600 秒です。

FWSM は 60 秒ごとに PIM ジョイン /Prune メッセージを送信します。この値を変更するには、次のコマンドを入力します。

```
hostname(config-if)# pim join-prune-interval seconds
```

*seconds* 引数の有効値の範囲は 10 ～ 600 秒です。

## マルチキャスト ルーティングの詳細について

次の Internet Engineering Task Force (IETF) による RFC には、SMR 機能を実装するための、IGMP 規格およびマルチキャスト ルーティング規格に関する技術的な詳細が示されています。

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP マルチキャストとファイアウォール
- RFC 2113 IP ルータ アラート オプション
- IETF draft-ietf-idmr-igmp-proxy-01.txt

## 非対称ルーティング サポートの設定

セッションの戻りトラフィックが、発信元と異なるインターフェイスを経由してルーティングされることもあります。フェールオーバー コンフィギュレーションでは、ある装置から発信された接続の戻りトラフィックが、ピア装置を経由して返送されることがあります。これは一般に、1 つの FWSM 上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つの FWSM が別々のサービス プロバイダーに接続され、発信接続で NAT アドレスを使用しない場合に起こります。FWSM では、戻りトラフィックは接続情報がないためデフォルトでは廃棄されます。

廃棄が発生する可能性のあるインターフェイス上で **asr-group** コマンドを使用して、戻りトラフィックの廃棄を阻止できます。**asr-group** コマンドで設定したインターフェイスがセッション情報のないパケットを受信すると、同一グループ内の他のインターフェイスのセッション情報を確認します。



(注)

フェールオーバー コンフィギュレーションでは、スタンバイ ユニットまたはフェールオーバー グループからアクティブ ユニットまたはフェールオーバー グループに転送されるセッション情報について、ステートフル フェールオーバーをイネーブルにする必要があります。

一致が見つからない場合、パケットは廃棄されます。一致が見つかった場合、次のいずれかの処理が行われます。

- 着信トラフィックがフェールオーバー コンフィギュレーションのピア装置で発信された場合、レイヤ 2 ヘッダの一部または全部が書き換えられ、パケットは他の装置にリダイレクトされます。このリダイレクションは、セッションがアクティブなまじり続きます。
- 着信トラフィックが同一装置上の異なるインターフェイスで発信された場合、レイヤ 2 ヘッダの一部または全部が書き換えられ、パケットは再度ストリームに入れられます。



(注)

**asr-group** コマンドを使用して非対象ルーティング サポートを設定する方が、**nailed** オプションを指定して **static** コマンドを使用するよりもセキュアです。

ここでは、次の内容について説明します。

- [インターフェイスの ASR グループへの追加 \(p.8-28\)](#)
- [非対称ルーティング サポートの例 \(p.8-29\)](#)

### インターフェイスの ASR グループへの追加

次のコマンドを入力して、インターフェイスを非対象ルーティング グループに追加します。フェールオーバー コンフィギュレーションの装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。

```
hostname/ctx1(config)# interface if
hostname/ctx1(config-if)# asr-group num
```

*num* の有効値の範囲は 1 ~ 32 です。ASR グループに参加するインターフェイスごとに、コマンドを入力する必要があります。**show interface detail** コマンドを使用して、伝送された ASR パケット数、受信された ASR パケット数、またはインターフェイスによって廃棄された ASR パケット数を表示できます。

最大 32 個の ASR グループを作成し、各グループに最大 8 個のインターフェイスを割り当てることができます。



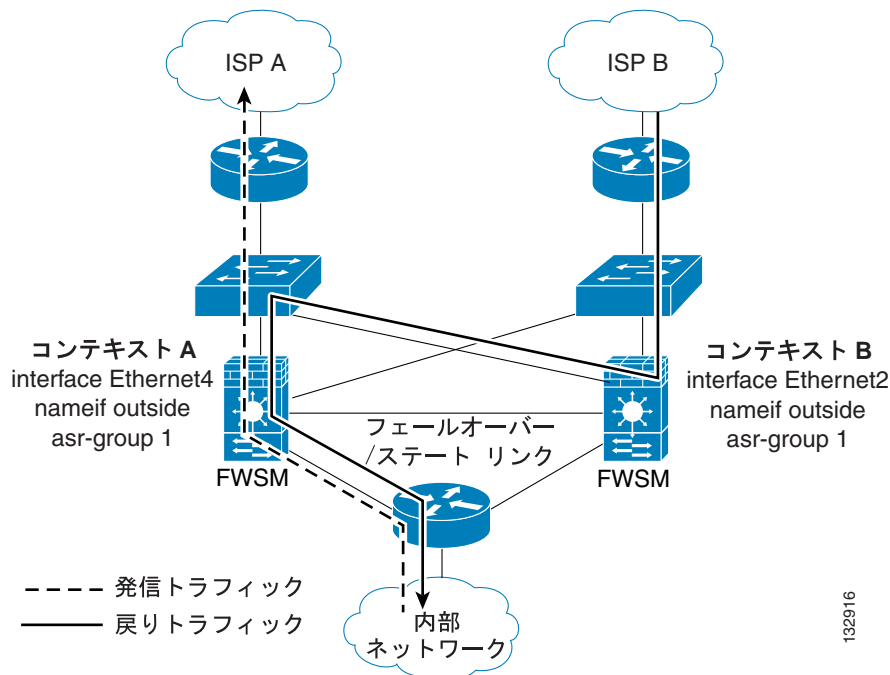
(注)

フェールオーバー コンフィギュレーションのスタンバイ ユニットからアクティブ ユニットへのパケットのリダイレクションを可能にするために、アップストリーム ルータおよびダウンストリーム ルータは、VLAN ごとに 1 つの MAC アドレスを使用し、異なる VLAN には異なる MAC アドレスを使用する必要があります。

## 非対称ルーティング サポートの例

図 8-1 に、アクティブ/アクティブ フェールオーバー コンフィギュレーションでの非対称ルーティング サポートに `asr-group` コマンドを使用する例を示します。

図 8-1 アクティブ/アクティブ フェールオーバーでの ASR の例



一方の装置でコンテキスト A がアクティブで、もう一方の装置でコンテキスト B がアクティブです。各コンテキストには「outside」という名前のインターフェイスがあり、両方とも `asr-group 1` の一部として設定されています。発信トラフィックは、コンテキスト A がアクティブな装置を經由してルーティングされます。ただし、戻りトラフィックはコンテキスト B がアクティブな装置を經由してルーティングされています。通常、装置上に戻りトラフィックのセッション情報はないため、戻りトラフィックは廃棄されます。ただし、インターフェイスは `asr-group` 番号を使用して設定されているため、装置は同じ `asr-group` が割り当てられた他のインターフェイスのセッション情報を検索します。そして、装置上でスタンバイ ステートのコンテキスト A の外部インターフェイスでセッション情報を見つけて、戻りトラフィックをコンテキスト A がアクティブな装置に転送します。

トラフィックは、コンテキスト A がスタンバイ ステートの装置上でコンテキスト A の外部インターフェイスを經由して転送され、コンテキスト A がアクティブ ステートの装置上でコンテキスト A の外部インターフェイスを經由して返送されます。転送は、セッションが終了するまで続きます。

## DHCP の設定

DHCP は、IP アドレスなどのネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。FWSM は DHCP サーバまたは DHCP リレー サービスを、FWSM インターフェイスに接続された DHCP クライアントに提供します。DHCP サーバはネットワーク コンフィギュレーション パラメータを直接 DHCP クライアントに提供します。DHCP リレーでは、あるインターフェイスで受信した DHCP 要求を、別のインターフェイスの背後に配置された外部 DHCP サーバに転送します。

ここでは、次の内容について説明します。

- [DHCP サーバの設定 \(p.8-30\)](#)
- [DHCP リレー サービスの設定 \(p.8-34\)](#)

## DHCP サーバの設定

ここでは、FWSM の DHCP サーバを設定する方法を説明します。内容は次のとおりです。

- [DHCP サーバのイネーブル化 \(p.8-30\)](#)
- [DHCP オプションの設定 \(p.8-32\)](#)
- [DHCP サーバで Cisco IP Phone を使用する方法 \(p.8-33\)](#)

## DHCP サーバのイネーブル化

FWSM は DHCP サーバとして動作可能です。DHCP は、ホスト IP アドレス、デフォルト ゲートウェイ、DNS サーバなどのネットワーク設定値をホストに供給するプロトコルです。



(注)

FWSM の DHCP サーバは BOOTP 要求をサポートしません。

マルチコンテキスト モードの場合、複数のコンテキストが使用するインターフェイス上で DHCP サーバまたは DHCP リレーをイネーブルにすることはできません。

FWSM の各インターフェイス上で DHCP サーバを設定できます。各インターフェイスは、アドレスを抽出する固有のアドレス プールを持つことができます。ただし、DNS サーバ、ドメイン名、オプション、ping タイムアウト、WINS サーバなどのその他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバで使用されます。

DHCP クライアントまたは DHCP リレー サービスを、サーバがイネーブル化されたインターフェイス上で設定することはできません。また、DHCP クライアントは、サーバがイネーブル化されたインターフェイスに直接接続する必要があります。

特定の FWSM インターフェイス上で DHCP サーバをイネーブルにする手順は、次のとおりです。

**ステップ 1** DHCP アドレス プールを作成します。次のコマンドを入力して、アドレス プールを定義します。

```
hostname(config)# dhcpd address ip_address-ip_address interface_name
```

FWSM は、このプールからアドレスを 1 つクライアントに割り当て、一定時間だけ使用できるようにします。これらのアドレスは、直接接続されたネットワークで使用する、変換されないローカルアドレスです。

アドレス プールは、FWSM インターフェイスと同じサブネットになければなりません。

- ステップ 2** (任意) 次のコマンドを入力して、クライアントに使用させる DNS サーバ (複数可) の IP アドレス (複数可) を指定します。

```
hostname(config)# dhcpd dns dns1 [dns2]
```

DNS サーバを 2 つまで指定できます。

- ステップ 3** (任意) 次のコマンドを入力して、クライアントに使用させる WINS サーバ (複数可) の IP アドレス (複数可) を指定します。

```
hostname(config)# dhcpd wins wins1 [wins2]
```

WINS サーバを 2 つまで指定できます。

- ステップ 4** (任意) 次のコマンドを入力して、クライアントに付与するリース期間を変更します。

```
hostname(config)# dhcpd lease lease_length
```

このリースとは、リース期限が切れるまでに、割り当てられた IP アドレスをクライアントが使用できる時間の長さ (秒) です。0 ~ 1,048,575 の値を入力します。デフォルトは 3600 秒です。

- ステップ 5** (任意) 次のコマンドを入力して、クライアントが使用するドメイン名を設定します。

```
hostname(config)# dhcpd domain domain_name
```

- ステップ 6** (任意) 次のコマンドを入力して、DHCP の ping タイムアウト値を設定します。

```
hostname(config)# dhcpd ping_timeout milliseconds
```

アドレスの競合を防ぐために、FWSM はアドレスを DHCP クライアントに割り当てる前に、アドレスに 2 つの ICMP ping パケットを送信します。このコマンドは、これらのパケットのタイムアウト値を指定します。

- ステップ 7** (透過ファイアウォール モード) デフォルト ゲートウェイを定義します。DHCP クライアントに送信するデフォルト ゲートウェイを定義するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 3 ip gateway_ip
```

DHCP オプション 3 を使用してデフォルト ゲートウェイを定義しない場合、DHCP クライアントは管理インターフェイスの IP アドレスを使用します。管理インターフェイスは、トラフィックをルーティングしません。

- ステップ 8** 次のコマンドを入力して、FWSM 内の DHCP デーモンがイネーブルになったインターフェイス上で DHCP クライアント要求を待ち受けるようにします。

```
hostname(config)# dhcpd enable interface_name
```

たとえば、内部インターフェイスに接続されたホストに 10.0.1.101 ~ 10.0.1.110 の範囲を割り当てる場合、次のコマンドを入力します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 209.165.201.2 209.165.202.129
hostname(config)# dhcpd wins 209.165.201.5
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

## DHCP オプションの設定

RFC 2132 に示されている DHCP オプションの情報を送信するように FWSM を設定できます。DHCP オプションは次の 3 つのいずれかのカテゴリに属します。

- IP アドレスを返すオプション
- テキスト文字列を返すオプション
- 16 進数値を返すオプション

FWSM は、DHCP オプションの 3 つのカテゴリすべてをサポートします。DHCP オプションを設定するには、次のいずれかを実行します。

- 1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option code ip addr_1 [addr_2]
```

- テキスト文字列を返す DHCP オプションを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option code ascii text
```

- 16 進数値を返す DHCP オプションを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option code hex value
```



(注)

FWSM は、ユーザが指定したオプション タイプと値が RFC 2132 で定義されたオプション コードの予測タイプと値と一致するかどうかは確認しません。たとえば、`dhcpd option 46 ascii hello` を入力した場合、オプション 46 は RFC 2132 で 1 桁の 16 進数値として定義されているにもかかわらず、FWSM はこのコンフィギュレーションを受け付けます。オプション コードとオプション コードに対応付けられたタイプおよび予測値の詳細については、RFC 2132 を参照してください。

表 8-2 に、`dhcpd option` コマンドでサポートされない DHCP オプションを示します。

表 8-2 サポート対象外の DHCP オプション

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE



表 8-2 サポート対象外の DHCP オプション (続き)

オプションコード	説明
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

特定オプション (DHCP オプション 3、66、150) を使用して Cisco IP Phone を設定します。これらのオプションの設定については、「[DHCP サーバで Cisco IP Phone を使用する方法](#)」(p.8-33) を参照してください。

## DHCP サーバで Cisco IP Phone を使用する方法

小規模な支社で構成される企業が Cisco IP Telephony Voice over IP (VoIP) ソリューションを実装する場合、通常、セントラル オフィスに Cisco CallManager を配置して、小規模な支社の Cisco IP Phone を制御します。この方式によって、コール処理を一元化し、必要な装置数を減らし、支社で Cisco CallManager やその他のサーバを管理する余分な負担を排除できます。

Cisco IP Phone は、TFTP サーバからコンフィギュレーションをダウンロードします。Cisco IP Phone が起動したときに、IP アドレスと TFTP サーバの IP アドレスの両方があらかじめ設定されていない場合、Cisco IP Phone はオプション 150 または 66 を指定した要求を DHCP サーバへ送り、この情報を取得します。

- DHCP オプション 150 を指定すると、TFTP サーバリストの IP アドレスが得られます。
- DHCP オプション 66 を指定すると、単一 TFTP サーバの IP アドレスまたはホスト名が得られます。

Cisco IP Phone は、要求に DHCP オプション 3 を含めることもあります。この場合、デフォルトルートが設定されます。

Cisco IP Phone は、1 つの要求にオプション 150 と 66 の両方を含めることがあります。この場合、FWSM DHCP サーバは、FWSM 上で値が設定されていれば、両方のオプションに対応する値を応答として提供します。

RFC 2132 で指定されている大部分のオプションに対応する情報を送信するように、FWSM を設定できます。次に、オプション番号の構文とともに、よく使用されるオプション 66、150、および 3 の構文を示します。

- 次のコマンドを入力して、RFC 2132 の指定に従って、オプション番号が含まれている DHCP 要求に対応する情報を提供します。

```
hostname(config)# dhcpd option number value
```

- 次のコマンドを入力して、オプション 66 に対応する TFTP サーバの IP アドレスまたは名前を提供します。

```
hostname(config)# dhcpd option 66 ascii server_name
```

- 次のコマンドを入力して、オプション 150 に対応する 1 つまたは 2 つの TFTP サーバの IP アドレスまたは名前を提供します。

```
hostname(config)# dhcpd option 150 ip server_ip1 [server_ip2]
```

*server\_ip1* はプライマリ TFTP サーバの IP アドレスまたは名前です。*server\_ip2* は、セカンダリ TFTP サーバの IP アドレスまたは名前です。オプション 150 を使用して、最大 2 つの TFTP サーバを指定できます。

- デフォルト ルートを設定するには、次のコマンドを入力します。

```
hostname(config)# dhcpd option 3 ip router_ip1
```

## DHCP リレー サービスの設定

DHCP リレー エージェントを利用すると、FWSM はクライアントから異なるインターフェイスに接続されたルータへ DHCP 要求を転送できます。

DHCP リレー エージェントの利用には、次の制約があります。

- DHCP サーバ機能がイネーブルのときに、リレー エージェントをイネーブルにすることはできません。
- DHCP リレー サービスは、透過ファイアウォール モードでは使用できません。ただし、アクセスリストを使用して DHCP トラフィックを通過させることはできます。透過モードで DHCP 要求および応答が FWSM を通過できるようにするには、内部インターフェイスから外部インターフェイスへの DHCP 要求を許可するアクセスリストと、別方向のサーバからの応答を許可するアクセスリストの 2 つのアクセスリストを設定する必要があります。
- FWSM にクライアントを直接接続する必要があります。クライアントから別のリレー エージェントまたはルータを介して要求を送ることはできません。
- マルチコンテキスト モードの場合、複数のコンテキストが使用するインターフェイス上で DHCP リレーをイネーブルにすることはできません。

DHCP リレーをイネーブル化する手順は、次のとおりです。

- ステップ 1** 次のコマンドを入力して、DHCP クライアントと異なるインターフェイス上の DHCP サーバの IP アドレスを設定します。

```
hostname(config)# dhcprelay server ip_address if_name
```

このコマンドは 4 回まで使用でき、最大 4 サーバを指定できます。

- ステップ 2** 次のコマンドを入力して、クライアントに接続されたインターフェイス上で DHCP リレーをイネーブルにします。

```
hostname(config)# dhcprelay enable interface
```

- ステップ 3** (任意) 次のコマンドを入力して、リレー アドレス ネゴシエーションが可能な秒数を設定します。

```
hostname(config)# dhcprelay timeout seconds
```

- ステップ 4** (任意) 次のコマンドを入力して、DHCP サーバから FWSM インターフェイスのアドレスに送信されるパケットに組み込む、最初のデフォルト ルータ アドレスを変更します。

```
hostname(config)# dhcprelay setroute if_name
```

この作業によって、DHCP サーバで別のルータが指定されている場合でも、クライアントは FWSM に接続できるデフォルト ルートを設定できます。

パケットにデフォルト ルータ オプションが指定されていない場合、FWSM はインターフェイス アドレスが含まれているオプションを 1 つ追加します。

---

次に、FWSM が、内部インターフェイスに接続されたクライアントから外部インターフェイス上の DHCP サーバへ、DHCP 要求を転送できるようにする例を示します。

```
hostname(config)# dhcprelay server 201.168.200.4
hostname(config)# dhcprelay enable inside
hostname(config)# dhcprelay setroute inside
```

## DHCP クライアントの設定

FWSM インターフェイスを DHCP クライアントとして設定するための手順は、次のとおりです。

```
hostname(config-if)# ip address dhcp [retry num] [setroute]
```

任意の *retry num* 引数は、インターフェイスが DHCP サーバへの接続を試行する回数を指定します。デフォルト値は 4 で、最大値は 48 です。*setroute* キーワードでは、DHCP サーバが戻すデフォルト ゲートウェイを使用してデフォルト ルートが設定されます。



- (注)** DHCP クライアントとして設定されたインターフェイス上で、DHCP サーバまたは DHCP リレー サービスをイネーブル化することはできません。
-

