ルーティングとサブネット範囲

この章は、次の内容で構成されています。

- L3Out EPG スコープと制御パラメータ （1 ページ）
- セキュリティ インポート ポリシー （2 ページ）

L3Out EPG スコープと制御パラメータ

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジドメインで設定されるデフォルトのゲートウェイには影響しません。

インポート ルート コントロール サブネット：このコントロールは、インポート ルート制御の強制が設定されている場合、ルートを Border Gateway Protocol（BGP）と Open Shortest Path First（OSPF） でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティ インポート サブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラフィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC が許可済みリスト モデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG 間の全データ プレーン トラフィックをドロップするというものです。この許可済みリスト モデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークされる必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『*Cisco APIC* レイヤ *3* ネットワーキング構成定ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポート ルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィックスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0/0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。ルート マップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで設定されます。

セキュリティ インポート ポリシー

静的 L3Out EPG

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ファブリックは許可リスト モデルで動作します。そのデフォルトの動作は、契約によって明示的に許可されていない限り、エンドポイント グループ間のすべてのデータプレーン トラフィックをドロップするというものです。この許可リスト モデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナント トラフィックとは、セキュリティ ポリシーの設定方法と実装方法が少し異なります。

中継セキュリティ ポリシー

- プレフィックス フィルタリングを使用します。
- リリース 2.0(1m) 以降では、Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタのサポートが利用できるようになりました。
- セキュリティ インポート サブネット（プレフィックス）と外部 EPG で設定されたコントラクトを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングは使用しないでください。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。
- テナント EPG←→EPG およびテナント EPG←→外部 EPG でサポートされます。

外部プレフィックス ベースの EPG 間に契約が存在しない場合、トラフィックはドロップされます。2 つの外部 Epg の間のトラフィックを許可するには、契約とセキュリティ プレフィックスを設定する必要があります。プレフィックスフィルタリングのみがサポートされるため、契約ではデフォルト フィルタを使用できます。

外部 L3Out 接続契約

L3Out 接続が展開されているすべてのリーフ ノードでは、L3Out 接続のプレフィックスの結合がプログラムされます。3 つ以上の L3Out 接続が展開されている場合、集約ルール 0.0.0.0/0 を使用すると、契約のない L3Out 接続間でもトラフィックのフローが許可されます。

L3Out インスタンス プロファイル (instP) で、プロバイダーとコンシューマの契約の関連づけとセキュリティ インポート サブネットを設定します。

セキュリティ インポート サブネットが設定されており、集約ルール、0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は、 10.0.0.0～10.255.255.255 の範囲のすべてのアドレスに適合します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

3 つ以上の L3Out 接続が同じ VRF 内に設定されている場合は、ルールの結合が問題となるため、セキュリティ インポート サブネットを設定するときに注意する必要があります。

同じ L3Out で入出力する中継トラフィック フローは、0.0.0.0/0 セキュリティ インポート サブネットを設定すると、ポリシーによってドロップされます。この動作は、ダイナミックまたはスタティック ルーティングに当てはまります。この動作を防ぐためには、より詳細なサブネットを定義してください。

ダイナミック L3Out EPG 分類

Cisco APIC 5.2(4) リリースより前は、外部サブネットは外部 EPG の下で構成されていたため、外部サブネットの pcTag は外部 EPG の pcTag から派生していました。ルーティングが変更されると、外部サブネットは別の L3Out または外部 EPG から学習されました。 pcTag は、ルーティングが変更されても変更されません。

Cisco APIC 5.2(4) リリース以降、動的 L3Out EPG 分類 (DEC) 機能が導入され、ルーティングの変更に伴う pcTag の動的な変更が可能になりました。

この機能により、管理者はサブネットまたは BGP コミュニティを照合することにより、ルート マップを使用して外部 EPG を設定することもできます。外部 EPG 設定が設定されたルート マップは、デフォルト インポートを使用して L3Out に、またはルート制御プロファイルを使用して BGP ピアに適用できます。L3Out の外部 EPG および契約設定は以前と同じままです。

ルート マップに基づいて、特定の外部 EPG および関連する契約がプレフィックスに対して決定されます。

（注） ルート マップによる外部 EPG の選択は、L3Out で設定された外部 EPG サブネットよりも優先されます。たとえば、ルート マップ構成が 10.1.1.0/24 を外部 *EPG1* に関連付け、サブネット *10.1.1.0/24* が外部 *EPG2* に構成されている場合、外部 *EPG1* はルート マップによる外部 EPG 決定が優先されるため、*10.1.1.0/24* のハードウェアでプログラムされます。

DEC の注意事項と制限事項

- この機能は、BGP と OSPF のみをサポートします。
- DEC は、L3Out デフォルト インポート ルート マップまたは BGP ピア インポート ルート マップでのみサポートされます。
- 共有セキュリティを有効にするには、共有する共有セキュリティ フラグとサブネットを使用して外部 EPG を構成します。
- DEC は次の機能をサポートしていません。
  - サイト間
  - 浮動 L3Out との統合
  - スタティックルーティング
  - EIGRP
  - セグメント ルーティング
  - 午前
  - 浮動 L3Out を使用した BGP ネクストホップ伝達
  - Cisco ACI GOLF、SR-MPLS、およびフォールバック ルートとの共存

GUI を使用したダイナミック L3Out EPG 分類の設定

この手順では、ダイナミック L3Out EPG 分類（DEC）を構成し、BGP を使用してレイヤー 3 外部ネットワーク接続を構成していることを前提としています。OSPF を使用して設定された L3Out に対してこれらのタスクを実行することもできます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。

- テナント ネットワークのレイヤ 3 Outside が作成されていること。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 **[作業（Work）]** ペインで、テナント名をダブルクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name[*** の順に展開します。

ステップ 4 *[Layer3_Outside_name]* を右クリックして、**[ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control）]** をクリックします。

ステップ 5 [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、次のアクションを実行します。

a) [**名前（Name**）] フィールドから、[**default-import**] を選択します。
選択内容に応じて、特定の L3Out でアドバタイズされている内容が自動的に使用されます。

b) **Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。

c) **[コンテキスト（Contexts）]** 領域で、**[+]** をクリックして **[ルート制御コンテキストの作成（Create Route Control Context）]** ウィンドウを表示します。

ステップ 6 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) **[関連する一致したルール（Associated Matched Rules）]** テーブルで、**[+]** をクリックします。

d) **[セット ルール（Set Rule）]** ドロップダウン リストから、**[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択します。

e) **[ルート マップの一致ルールの作成（Create Match Rule for Route Map）]** ダイアログボックスの **[名前（Name）]** フィールドに、一致ルールの名前を入力します。

f) 必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。

一致コミュニティ ファクタでは、名前、コミュニティ、および範囲を指定する必要があります。

g) **[送信（Submit）]** をクリックします。

h) **[セット ルール（Set Rule）]** ドロップダウン リストから、**[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択します。

i) **[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** ダイアログボックスの **[名前（Name）]** フィールドに、ルールの名前を入力します。

j) **[外部 EPG の設定（Set External EPG）]** チェックボックスをオンにして、**[外部 EPG（External EPG）]** ドロップダウン リストで EPG を選択して、**[完了（Finish）]** をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。

k) [**ルート制御コンテキストの作成（Create Route Control Context**）] ダイアログボックスで、[**OK**] をクリックします。

l) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

ステップ 7 **[作業（Work）]** ペインで、**[ポリシー（Policy）]** > **[メイン（Main）]**タブを選択します。
Work ウィンドウに、**Properties** が表示されます。

ステップ 8 （任意） **[ルート制御の強化（Route Control Enforcement）]** フィールドのとなりの **[インポート（Import）]** チェック ボックスをオンにして、インポート ポリシーを有効にして **[送信（Submit）]** をクリックします。

インポート制御ポリシーはデフォルトで無効になっています。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザーがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、プロトコルは自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。また、ネイバー インポート ルート マップごとに BGP を設定する場合は、インポート ポリシーの **[インポート（Import）]** チェックボックスをオンにする必要はありません。

（注）
BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 9 カスタマイズされたエクスポート ポリシーを作成するには、**[ナビゲーション（Navigation）]** ペインで、**[ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control）]** を右クリックし、**[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）]** をクリックし、次のアクションを実行します。

a) [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**名前（Name**）] ドロップダウン リストから、エクスポート ポリシーを選択するか、名前を入力します。

b) **[コンテキスト（Contexts）]** 領域で、**[+]** をクリックして **[ルート制御コンテキストの作成（Create Route Control Context）]** ダイアログを開きます。

c) **[ルート制御コンテキストの作成（Create Route Control Context）]** ダイアログボックスの **[注文（Order）]** フィールドに、値を入力します。

d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

e) （任意） **[関連する一致ルール（Associated Match Rules）]** テーブルで、**[+]** をクリックし、**[ルール名（Route Name）]** ドロップダウン リストから **[ルート マップの一致ルールを作成（Create Match Rule For a Route Map）]** を選択し、必要に応じてフィールドに入力して、**[送信（Submit）]** をクリックします。

f) [**セット ルール（Set Rule**）] ドロップダウン リストから、[**ルート マップのセット ルールの作成（Create Set Rules For a Route Map**）] を選択します。

または、既存のセット ルールを選択できます。

g) **[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択した場合は、**[ルート マップのセット ルールの作成（Create Set Rules For A Route Map）]** ダイアログ ボックスで、**[名前（Name）]** フィールドにセット ルールの名前を入力し、設定するルールのチェック ボックスをオンにして、次のように入力します。ルールに適切な値を入力し、**[完了（Finish）]** をクリックします。
[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。

h) **OK** をクリックします。

i) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注）
エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 10 **[ナビゲーション（Navigation）]** ペインで ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[外部 EPG（External EPGs）]** > ***[external_EPG_name]*** の順に展開して、次のアクションを実行します。

a) **ルート制御プロファイル** テーブルで、+ をクリックします。

b) **[名前（Name）]** フィールドのドロップダウン リストから、前に作成したポリシーを選択します。

c) **[方向（Direction）]** フィールドのドロップダウン リストから、**[ルート エクスポート ポリシー（Route Export Policy）]** を選択します。

d) **Update** をクリックします。

e) [Submit] をクリックします。

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。