VPN 間のルートリーク

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1*：機能の履歴

機能名	リリース情報	説明
グローバル VRF とサービス VPN 間のルートリーク	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、グローバル VRF とサービス VPN の間でルートを双方向にリークできます。ルートリークにより、ハブのバイパスが可能になり、移行されたブランチが移行されていないブランチに直接アクセスできるため、サービスの共有が可能になり、移行のユースケースで役立ちます。
OSPF、EIGRP プロトコルへの複製された BGP ルートの再配布	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能を使用すると、グローバル VRF とサービス VPN の間で BGP ルートをリーク（または複製）し、リークした BGP ルートを再配布できます。EIGRP および OSPF プロトコルにリークされたルートの再配布は、対応する VRF に BGP ルートを複製した後に行われます。

機能名	リリース情報	説明
BGP、OSPF、および EIGRP プロトコルへの複製ルートの再配布	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能を使用すると、次の項目を設定できます。 Cisco IOS XE Catalyst SD-WAN デバイス上の BGP、OSPF、および EIGRP プロトコルのグローバル VRF とサービス VPN 間のリークまたは複製ルートの再配布 MPLS ルートよりも OMP ルートを優先する OMP アドミニストレーティブ ディスタンス オプション リークされたルートが到達可能かどうかを追跡する VRRP トラッキング。
サービス VPN 間のルートリーク	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、同じエッジデバイスのサービス VPN 間でルートをリークできます。 ルートリーク機能により、Cisco IOS XE Catalyst SD-WAN デバイス での接続、スタティック、BGP、OSPF、および EIGRP について、サービス VPN 間で複製されたルートを再配布できます。

サポートされているプロトコル

グローバル VRF とサービス VPN 間のルートリークに対して、次のプロトコルがサポートされています。

- 接続されている状態
- スタティック
- BGP
- OSPF
- EIGRP

次のプロトコルは、サービス VPN とグローバル VRF 間のルートの再配布でサポートされる宛先および送信元プロトコルです。

送信元プロトコル

- 接続されている状態
- スタティック
- BGP
- OSPF
- EIGRP

宛先プロトコル

- BGP
- OSPF
- EIGRP

（注） EIGRP プロトコルは、サービス VPN でのみ使用でき、グローバル VRF では使用できません。したがって、ルートリークは、サービス VPN からグローバル VRF へのルートに対してのみサポートされます。

ルートリークと再配布の制約事項

- EIGRP プロトコルは、サービス VRF でのみ使用でき、グローバル VRF では使用できません。したがって、グローバル VRF からサービス VRF へのルート、および EIGRP プロトコルのサービス VRF 間のルートでは、ルートリークはサポートされません。
- サービス側 NAT は、グローバル VRF とサービス VRF の間のルートリークではサポートされません。
- NAT は、トランスポート VRF ルートリークではサポートされません。
- IPv6 アドレスファミリはサポートされません。

- 各サービス VRF は、最大 1000 ルートをリーク（インポートおよびエクスポート）できます。
- リークされたルートのフィルタリングに使用されるルートマップでは、プレフィックスリスト、タグ、およびメトリックのみを照合できます。
- マルチテナント機能を備えた Cisco IOS XE Catalyst SD-WAN デバイスでのサービス VRF 間ルートリークはサポートされません。
- オーバーレイループを防止するために、Overlay Management Protocol（OMP）ルートは VRF ルートリークに参加しません。
- Cisco SD-WAN のエクスポートポリシーを使用したさまざまなデバイスまたはサイト間のルートリークはサポートされません。
- EIGRP での再配布では、ベストパスを選択するために帯域幅、負荷、信頼性、遅延、および MTU の設定が必要です。
- **all** キーワードを使用したルート複製は推奨されません。
- 集中型ポリシーを使用したルートリークはサポートされません。
- VRF のルートリークを設定する際には、ルートループを防止するために、**global-address-family ipv4** コマンドの下の **route-replicate** コマンドで、unicast オプションのプロトコルとしてキーワード **all** を指定しないでください。

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast all
```

- この例に示されているように、キーワード all を特定のプロトコル名に置き換える必要があります。

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast connected
```

ルートリークに関する情報

グローバル VRF とサービス VPN 間のルートリーク

Cisco Catalyst SD-WAN ソリューションを使用すると、VPN を使用してネットワークをセグメント化できます。グローバルまたはデフォルト VRF（トランスポート VPN）とサービス VPN 間のルートリークにより、複数の VPN がアクセスする必要がある共通サービスを共有できます。この機能を使用すると、グローバル VRF（別名、トランスポート VPN）とサービス VPN の間で双方向のルートリークを介してルートが複製されます。VRF 間のルートリークは、ルーティング情報ベース（RIB）を使用して行われます。

（注） Cisco Catalyst SD-WAN のコンテキストでは、VRF と VPN という用語は同じ意味で使用されます。Cisco IOS XE Catalyst SD-WAN デバイスは、セグメンテーションとネットワーク分離に VRF を使用しますが、VPN 機能テンプレートは、Cisco SD-WAN Manager を使用してこれらを設定するために使用されます。Cisco SD-WAN Manager を使用して Cisco IOS XE Catalyst SD-WAN デバイスの VPN を設定すると、Cisco SD-WAN Manager は自動的に VPN 設定を VRF 設定に変換します。

ルーティングネイバーにルートをリークするには、グローバル VRF とサービス VPN の間でリークされたルートを再配布します。

リークされたルートの OMP アドミニストレーティブ ディスタンス

Cisco SD-WAN オーバーレイ管理プロトコル（OMP）アドミニストレーティブディスタンスを低い値に設定すると、ブランチ間ルーティングシナリオでリークされたルートよりも優先して、OMP ルートを優先ルートおよびプライマリルートとして設定できます。

次の点に基づいて、Cisco IOS XE Catalyst SD-WAN デバイスの OMP アドミニストレーティブディスタンスを設定します。

- グローバル VRF レベルとサービス VRF レベルの両方で OMP アドミニストレーティブディスタンスを設定すると、VRF レベルの設定でグローバル VRF レベルの設定がオーバーライドされます。
- サービス VRF をグローバル VRF よりも低いアドミニストレーティブ ディスタンスで設定すると、サービス VRF を除き、残りすべての VRF でグローバル VRF からのアドミニストレーティブ ディスタンスの値が使用されます。

Cisco SD-WAN Manager を使用して OMP アドミニストレーティブ ディスタンスを設定するには、「Configure Basic VPN Parameters」および「Configure OMP Using SD-WAN Manager Templates」を参照してください。

CLI を使用して OMP アドミニストレーティブ ディスタンスを設定するには、「CLI を使用した OMP の設定」の「OMP アドミニストレーティブ ディスタンスの設定」を参照してください。

サービス VRF 間ルートリーク

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1。

サービス VRF 間ルートリーク機能は、サービス VRF 間の選択的ルートを同じサイト上の発信元デバイスにリークする機能を提供します。

Cisco SD-WAN コントローラを使用するときに発生するルーティング拡張性の課題を解決するために、エッジデバイスで VRF 間のルートをリークできます。

Cisco SD-WAN Manager を使用してサービス VRF 間ルートリーク機能を設定するには、「サービス VRF 間のルートリークの設定」を参照してください。

CLI を使用してサービス VRF 間ルートリーク機能を設定するには、「CLI を使用したサービス VRF 間のルートリークの設定」を参照してください。

リークされたサービス VPN に VRRP トラッカーを使用する

Virtual Router Redundancy Protocol（VRRP）は、リークされたルートが到達可能かどうかをトラックできます。トラック対象ルートに到達できない場合、VRRP は、VRRP グループの優先順位を変更します。VRRP は新しいプライマリルータの選択をトリガーできます。VRRP トラッカーは、VRRP 設定に含まれるルーティングインスタンスのルーティングテーブル内のルートの存在に基づいて、ルートが到達可能かどうかを判断します。

Cisco SD-WAN Manager を使用してリークされたサービス VPN を追跡するように VRRP トラッカーを設定するには、「Configure VRRP for Cisco VPN Interface Ethernet template」を参照してください。

CLI を使用してリークされたサービス VPN を追跡するように VRRP トラッカーを設定するには、「CLI を使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定」を参照してください。

ルートリークの機能

- グローバル VRF とサービス VPN 間のルートを直接リークできます。
- 複数のサービス VPN がグローバル VRF にリークされる可能性があります。
- 複数のサービス VRF の同じサービス VRF へのリークがサポートされています。
- グローバル VRF とサービス VPN の間でルートがリークまたは複製される場合、メトリック、送信元 VPN 情報、タグ、アドミニストレーティブ ディスタンス、ルートの起点などのルートプロパティは保持されます。
- ルートマップを使用して、リークされたルートを制御できます。
- ルートマップでは、照合操作を使用して、ルートをリークする前にルートをフィルタリングできます。
- この機能は、Cisco SD-WAN Manager と CLI の両方で設定できます。

ルートリークのユースケース

- **サービスプロバイダーのセントラルサービス**：MPLS の SP セントラルサービスは、VPN ごとに複製することなく直接アクセスできます。これにより、セントラルサービスへのアクセスがより簡単かつ効率的になります。
- **移行**：ルートリークにより、Cisco SD-WAN に移行したブランチは、ハブをバイパスして移行されていないブランチに直接アクセスできるため、アプリケーションの SLA が向上します。
- **集中型ネットワーク管理**：コントロールプレーンとサービス側の機器をアンダーレイで管理できます。

- **PCI 準拠に関する小売業者の要件**：サービス VRF のルートリークは、VRF トラフィックが、PCIに準拠しながら、同じブランチルータ上のゾーンベースファイアウォールを通過する場合に使用されます。

ルートプリファレンスの特定方法

グローバル VRF とサービス VPN の間でルートが複製またはリークされた場合、次のルールによってルートプリファレンスが決まります。

あるデバイスが 2 つの送信元からルートを受信し、両方のルートで同じ送信元 VRF が使用されていて一方のルートが複製される場合、複製されないルートが優先されます。

前述のルールが適用されない場合、次のルールに従い、以下の順番でルートプリファレンスが決まります。

1. アドミニストレーティブ ディスタンスが小さいルートが優先されます。
2. 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ルートが優先されます。
3. レプリケートされたルートよりもレプリケートされていないルートが優先されます。
4. 元の VRF 名を比較します。辞書の観点から VRF 名が小さいルートが優先されます。
5. 元のサブアドレスファミリを比較します。マルチキャストルーティングよりもユニキャストルーティングが優先されます。
6. 最も古いルートが優先されます。

Cisco SD-WAN Manager を使用したルートリーク設定のワークフロー

1. ローカライズ型ポリシーを設定し、有効にして、ルートポリシーを添付します。
2. グローバル VPN とサービス VPN 間のルートリーク機能を設定して有効にします。
3. サービス VPN 間のルートリーク機能を設定して有効にします。
4. サービス側の VPN 機能テンプレートをデバイステンプレートに添付します。

ローカライズされたルートポリシーの設定

ルートポリシーの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [ローカライズ側ポリシー（Localized Policy）] を選択します。

3. [Custom Options] ドロップダウンの [Localized Policy] で [Route Policy] を選択します。
4. [Add Route Policy] をクリックし、[Create New] を選択します。
5. ルートポリシーの名前と説明を入力します。
6. 左側のペインで、[シーケンスタイプの追加（Add Sequence Type）] をクリックします。
7. 右側のペインで、[シーケンスルールの追加（Add Sequence Rule）] をクリックして、ポリシーに単一のシーケンスを作成します。デフォルトでは [マッチ（Match）] が選択されています。
8. [Protocol] ドロップダウンリストから目的のプロトコルを選択します。オプションは、[IPv4]、[IPv6]、またはその両方です。
9. マッチ条件をクリックします。
10. 左側に、マッチ条件の値を入力します。
11. 右側に、ポリシーが一致した場合に実行するアクションを入力します。
12. [マッチとアクションの保存（Save Match and Actions）] をクリックして、シーケンスルールを保存します。
13. どのルート ポリシー シーケンス ルールにも一致するパケットがない場合、デフォルトのアクションはパケットをドロップすることです。デフォルトのアクションを変更するには、次の手順を実行します。
    1. 左側のペインで [Default Action] をクリックします。
    2. [鉛筆（Pencil）] アイコンをクリックします。
    3. デフォルトのアクションを [Accept] に変更します。
    4. [Save Match and Actions] をクリックします。
14. [Save Route Policy] をクリックします。

ルートポリシーの追加

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Localized Policy] を選択します。
3. [Add Policy] をクリックします。
4. ローカルポリシーウィザードで、[Configure Route Policy] オプションが表示されるまで [Next] をクリックします。
5. [Add Route Policy] をクリックし、[Import Existing] を選択します。
6. [Policy] ドロップダウンから、作成されたルートポリシーを選択します。[Import] をクリックします。

7. [Next] をクリックします。
8. [Policy Name] にポリシー名を入力し、[Description] に説明を入力します。
9. [Preview] をクリックして、CLI 形式でポリシー設定を表示します。
10. [Save Policy] をクリックします。

デバイステンプレートへのローカライズ型ポリシーの関連付け

（注） 以前に作成したローカライズ型ポリシーを利用するための最初の手順は、デバイステンプレートに関連付けることです。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックし、目的のテンプレートを選択します。
3. [...] をクリックして、[Edit] をクリックします。
4. [Additional Templates] をクリックします。
5. [Policy] ドロップダウンから、作成された**ローカライズ型ポリシー**を選択します。
6. [Update] をクリックします。

（注） ローカライズ型ポリシーがデバイステンプレートに追加されると、[Update] オプションを選択することにより、このデバイステンプレートに関連付けられているすべてのデバイスに設定変更がすぐにプッシュされます。複数のデバイスがデバイステンプレートに関連付けられている場合は、複数のデバイスが変更されていることを示す警告メッセージが表示されます。

7. [Next] をクリックし、[Configure Devices] をクリックします。
8. 検証プロセスが完了するまで待って、Cisco SD-WAN Manager からデバイスに設定をプッシュします。

グローバル VRF とサービス VPN 間のルートリークの設定および有効化

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. ルートリークを設定するには、[Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

次のいずれかを実行します。

- 機能テンプレートを作成するには、次の手順を実行します。

1. [Add template] をクリックします。デバイスのリストからデバイスを選択します。選択したデバイスで使用可能なテンプレートが右側のペインに表示されます。
2. 右側のペインから **[Cisco VPN]** テンプレートを選択します。

（注） ルートリークはサービス VPN にのみ設定できますしたがって、[Basic Configuration] の下の [VPN] フィールドに入力する番号は、1 ー 511 または 513 ー 65527 のいずれかです。

基本設定、DNS、Virtual Router Redundancy Protocol（VRRP）トラッキングなどのさまざまな VPN パラメータの設定の詳細については、「Configure a VPN Template」を参照してください。ルートリーク機能に固有の詳細については、ステップ c に進みます。

3. [Template Name] と [Description] に機能テンプレートの名前と説明をそれぞれ入力します。
4. [Description] フィールドの下にある [Global Route Leak] をクリックします。
5. グローバル VRF からルートをリークするには、[Add New Route Leak from Global VPN to Service VPN] をクリックします。
    1. [Route Protocol Leak from Global to Service] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
    2. [Route Policy Leak from Global to Service] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能なルートポリシーのいずれかを選択します。
    3. [Redistribute to protocol (in Service VPN)] フィールドで、[Add Protocol] をクリックします。

        [Protocol] ドロップダウン リストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

        [Redistribution Policy] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。
    4. [Add] をクリックします。
6. サービス VPN からグローバル VRF にルートをリークするには、[Add New Route Leak from Service VPN to Global VPN] をクリックします。

1. [Route Protocol Leak from Service to Global] ドロップダウンリストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。
2. [Route Policy Leak from Service to Global] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能なルートポリシーのいずれかを選択します。
3. [Redistribute to protocol (in Global VPN)] フィールドで、[Add Protocol] をクリックします。

   [Protocol] ドロップダウン リストで、[Global] を選択してプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

   [Redistribution Policy] ドロップダウンリストで、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。
4. [Add] をクリックします。

7. [Save/Update] をクリックします。設定は、機能テンプレートがデバイステンプレートに添付されるまで有効になりません。
8. リークされたルートを、Cisco SD-WAN Manager を使用して再配布するには、CLI アドオン機能テンプレートを使用して、使用環境に適した設定を入力します。次に例を示します。

```
Device(config)# router ospf 65535
Device(config-router)# redistribute vrf 1 ospf 103

Device(config)# router eigrp vpn
Device(config-router)# address-family ipv4 vrf 1 autonomous-system
 50
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global  ospf 65535

metric  1 2 3 4 5
```

   CLI アドオンテンプレートを作成したら、ルートを再配布するプロトコルテンプレートに添付する必要があります。この例では、EIGRP テンプレートに添付します。

- 既存の機能テンプレートを変更するには、次の手順を実行します。

1. 変更する機能テンプレートを選択します。
2. テーブルの行の横にある [...] をクリックし、[Edit] をクリックします。
3. [Global Route Leak] をクリックします。

4. 情報を編集するには、[Add New Route Leak from Global VPN to Service VPN] または [Add New Route Leak from Service VPN to Global VPN] の下にあるテーブルで、[Edit] をクリックします。

   [Update Route Leak] ダイアログボックスが表示されます。

5. 機能テンプレートを作成するステップ d のすべての操作を実行します。

   機能テンプレートを作成するステップ c のすべての操作を実行します。

6. [Save Changes] をクリックします。

7. [更新（Update）] をクリックします。

（注）
- 設定は、サービス VPN 機能テンプレートがデバイステンプレートに添付されるまで有効になりません。

サービス VPN 間のルートリークの設定

サポート対象の最小リリース：Cisco vManage リリース 20.9.1

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. デバイスの **Cisco VPN** テンプレートに移動します。

（注） **VPN** テンプレートを作成するには、「VPN テンプレートの作成」を参照してください。

4. [Route Leak] をクリックします。
5. [Route Leak between Service VPN] をクリックします。
6. [Add New Inter Service VPN Route Leak] をクリックします。
7. [Source VPN] ドロップダウンリストから、[Global] を選択して、ルートをリークするサービス VPN を設定します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

   Cisco IOS XE Catalyst SD-WAN デバイスのサービス側データトラフィック用に、VPN 1 ～ 511 および 513 ～ 65530 の範囲内でサービス VPN を設定できます（VPN 512 は、ネットワーク管理トラフィック用に予約済みです。VPN 0 は、設定された WAN トランスポート インターフェイスを使用した制御トラフィック用に予約済みです）。

8. [Route Protocol Leak to Current VPN] ドロップダウンリストから、[Global] を選択して、現在の VPN へのルートリークを有効にするルートプロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

   ルートリークについては、[Connected]、[Static]、[OSPF]、[BGP]、および [EIGRP] プロトコルを選択できます。

9. [Route Policy Leak to Current VPN] ドロップダウンリストから、[Global] を選択して、現在の VPN へのルートリークを有効にするルートポリシーを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

   利用可能なルートポリシーがない場合、このフィールドは無効になります。

10. [Redistribute to protocol (in Service VPN)] を設定するには、[Add Protocol] をクリックします。

    [Protocol] ドロップダウンリストから、[Global] を選択して、プロトコルを選択します。それ以外の場合は、[Device-Specific] を選択してデバイス固有の値を使用します。

    再配布については、[Connected]、[Static]、[OSPF]、[BGP]、および [EIGRP] プロトコルを選択できます。

    （任意）[Redistribution Policy] ドロップダウンリストから、[Global] を選択します。次に、ドロップダウンリストから使用可能な再配布ポリシーのいずれかを選択します。

    利用可能なルートポリシーがない場合、このフィールドは無効になります。

11. [Add] をクリックします。

12. [Save] をクリックします。

サービス側の VPN 機能テンプレートのデバイステンプレートへの添付

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。

2. [Device Templates] をクリックし、目的のテンプレートを選択します。

3. [...] をクリックして、[Edit] をクリックします。

4. [Service VPN] をクリックします。

5. [Add VPN] をクリックします。[Available VPN Templates] ペインに示されているサービス VPN 機能テンプレートを選択します。右矢印をクリックしてテンプレートを [Selected VPN Templates] リストに追加します。

6. テンプレートが左側（[Available VPN Templates]）から右側（[Selected VPN Templates]）に移動したら、[Next] をクリックします。

7. [Add] をクリックします。

8. [更新（Update）] をクリックします。

9. [Next] をクリックし、[Configure Devices] をクリックします。

10. 最後に、検証プロセスが完了するのを待って、Cisco SD-WAN Manager からデバイスに設定をプッシュします。

CLI を使用したルートリークの設定と確認

例：グローバル VRF とサービス VPN 間のルートリーク

次に、グローバル VRF とサービス VPN 間のルートリークを設定する例を示します。この例では、VRF 103 がサービス VPN です。次に、接続ルートがグローバル VRF から VRF 103 にリークされる例を示します。同様に、同じ接続ルートが VRF 103 からグローバル VRF にリークされます。

```
vrf definition 103
 !
  address-family ipv4
   route-replicate from vrf global unicast connected
!
global-address-family ipv4
  route-replicate from vrf 103 unicast connected
  exit-address-family
```

設定の確認

（注） 出力では、リークされたルートは、リークされたルートの横にある+記号で表されます。例：C+ は、接続ルートがリークされたことを示します。

```
Device#show ip route
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O 10.1.14.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.15.0/24 is directly connected, GigabitEthernet1
L 10.1.15.15/32 is directly connected, GigabitEthernet1
O 10.1.16.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.17.0/24 is directly connected, GigabitEthernet2
L 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
[170/10880] via 192.168.24.17(103), 01:04:13, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C + 192.0.2.0/24  is directly connected, GigabitEthernet5.103
```

```
L & 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 203.0.113.0/24 is directly connected, GigabitEthernet6
L 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 198.51.100.0/24 is directly connected, GigabitEthernet7
L 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
O E2 100.100.100.100 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets
O E2 172.16.255.14 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
```

グローバル VRF からサービス VRF テーブルにリークされたルートの表示

show ip route vrf <*vrf id*> コマンドを使用して、グローバル VRF からサービス VRF テーブルにリークされたルートを表示します。

（注） 出力では、リークされたルートは、リークされたルートの横にある+記号で示されます。例：C+ は、接続ルートがリークされたことを示します。

```
Device#show ip route vrf 103
Routing Table: 103
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C + 10.0.1.0/24 is directly connected, GigabitEthernet9
L & 10.0.1.15/32 is directly connected, GigabitEthernet9
C + 10.0.20.0/24 is directly connected, GigabitEthernet4
L & 10.0.20.15/32 is directly connected, GigabitEthernet4
C + 10.0.100.0/24 is directly connected, GigabitEthernet8
L & 10.0.100.15/32 is directly connected, GigabitEthernet8
C + 10.1.15.0/24 is directly connected, GigabitEthernet1
L & 10.1.15.15/32 is directly connected, GigabitEthernet1
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
D EX 172.16.20.20
[170/10880] via 192.168.24.17, 01:04:07, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.0/24 is directly connected, GigabitEthernet5.103
L 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 203.0.113.0/24 is directly connected, GigabitEthernet6
L & 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 198.51.100.0/24 is directly connected, GigabitEthernet7
```

```
L & 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
```

例：リーク前のルートのフィルタリング

グローバル VRF とサービス VRF の間でリークされたルートをさらにフィルタリングするには、次の例に示すようにルートマップを適用できます。

```
vrf definition 103
 !
  address-family ipv4
   route-replicate from vrf global unicast connected route-map myRouteMap permit 10
    match ip address prefix-list pList seq 5 permit 10.1.17.0/24
!
```

設定の確認

（注） 出力では、リークされたルートは、リークされたルートの横にある+記号で示されます。例：C+ は、接続ルートがリークされたことを示します。

```
Device#show ip route vrf 103

Routing Table: 1
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
m 10.1.18.0/24 [251/0] via 172.16.255.14, 19:01:28, Sdwan-system-intf
m 10.2.2.0/24 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
m 10.2.3.0/24 [251/0] via 172.16.255.11, 17:26:50, Sdwan-system-intf
C 10.20.24.0/24 is directly connected, GigabitEthernet5
L 10.20.24.15/32 is directly connected, GigabitEthernet5
m 10.20.25.0/24 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
172.16.0.0/32 is subnetted, 3 subnets
m 172.16.255.112 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
O E2 172.16.255.117 [110/20] via 10.20.24.17, 1d11h, GigabitEthernet5
m 172.16.255.118 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
```

リークされたルートをモニタするには、**show ip cef** コマンドを使用します。出力には、複製またはリークされたルートが表示されます。

```
Device#show ip cef 10.1.17.0 internal
10.1.17.0/24, epoch 2, flags [rcv], refcnt 6, per-destination sharing
[connected cover 10.1.17.0/24 replicated from 1]
```

```
sources: I/F
feature space:
Broker: linked, distributed at 4th priority
subblocks:
gsb Connected receive chain(0): 0x7F6B4315DB80
Interface source: GigabitEthernet5 flags: none flags3: none
Dependent covered prefix type cover need deagg, cover 10.20.24.0/24
ifnums: (none)
path list 7F6B47831168, 9 locks, per-destination, flags 0x41 [shble, hwcn]
path 7F6B3D9E7B70, share 1/1, type receive, for IPv4
receive for GigabitEthernet5
output chain:
receive
```

例：OSPF および EIGRP プロトコルへの BGP ルートの再配布

次に、BGP ルートをグローバル VRF からサービス VRF に複製する例を示します。

```
Device#config-transaction
Device(config)# vrf definition 2
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 1
Router(config-ipv4)# commit
```

グローバル VRF の BGP ルートをサービス VRF の EIGRP に再配布するための設定

（注） 他のプロトコルへの BGP ルートの再配布は、bgp redistribute-internal 設定が BGP ルートに存在する場合にのみサポートされます。

```
Device#config-transaction
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast vrf 2 autonomous-system 100
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 1 metric 10000 100 200 1
 1500
Device(config-ipv4)# commit

* Here we are redistributing BGP routes in global VRF to EIGRP in VRF 2.
* Routes replication must be done before doing inter VRF redistribution.
------------------------------------------------------------------------------
```

設定の確認

設定前にグローバル VRF に存在する BGP ルートの表示

```
Device#show ip route bgp
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected
```

```
Gateway of last resort is not set

10.0.0.0/9 is subnetted, 1 subnets
B 172.16.255.1 [200/20] via 10.1.15.14, 00:00:25
Device#

* We have a BGP route in the global VRF.
```

設定前にサービス VRF に存在しない BGP ルートの表示

show ip route vrf <*vrf id*> [**protocol**] コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```
Device#show ip route vrf 2 bgp

Routing Table: 2
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

Device#

* We do not have any BGP route in VRF 2.
```

設定後の BGP ルートの表示

show running config [*configuration-hierarchy*] | **details** コマンドを使用して、レプリケーションコンフィギュレーションが存在するかどうかを確認します。

```
Device#show running-config | section vrf definition 2
vrf definition 2
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
  route-replicate from vrf global unicast bgp 1
 exit-address-family
Device#

* We have successfully applied the route-replicate configuration.
* In our example we are replicating bgp 1 routes from global VRF to VRF 2.
-------------------------------------------------------------------------------
```

設定後にグローバル VRF からサービス VRF に複製される BGP ルートの表示

show ip route vrf <*vrf id*> [**protocol**] コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```
Device#show ip route vrf 2 bgp
```

```
Routing Table: 2
Codes: L - local, C - connected, S - static, 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, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/9 is subnetted, 1 subnets
B   +    172.16.255.1 [200/20] via 10.1.15.14, 00:04:01
Device#

* After route replication, we can see that the BGP route in the global VRF has been
replicated into VRF 2.
* + sign indicates replicated routes.
------------------------------------------------------------------------------
```

BGP 再配布情報のない EIGRP 設定の表示

```
Device#show running-config | section router eigrp
router eigrp test
 !
 address-family ipv4 unicast vrf 2 autonomous-system 100
  !
  topology base
  exit-af-topology
  network 10.0.0.0
 exit-address-family
Router#
```

EIGRP トポロジ テーブルの表示

show eigrp address-family ipv4 vrf<*vrf-num*>**topology** コマンドを使用して、サービス VRF テーブルの BGP ルートを表示します。

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
          Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.0.0/8, 1 successors, FD is 1310720
        via Connected, GigabitEthernet2

Device#

* EIGRP 100 is running on VRF 2.
------------------------------------------------------------------------------
```

BGP 再配布後の EIGRP ルートの表示

show eigrp address-family ipv4 vrf<*vrf-num*>**topology** コマンドを使用して、EIGRP プロトコルに再配布される BGP ルートを表示します。

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
          Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.0/8, 1 successors, FD is 1310720
        via Connected, GigabitEthernet2
P 172.16.0.0/12, 1 successors, FD is 131072000
        via +Redistributed (131072000/0)

-Device#

* BGP route has been redistributed into EIGRP.
```

CLI を使用したグローバル VRF とサービス VPN 間のルート再配布の設定

1. グローバル コンフィギュレーション モードを開始して、BGP ルーティングプロセスを作成します。

（注） **router eigrp** または **router ospf** を使用して、特定のルーティングプロトコルのルーティングプロセスを設定できます。次に、BGP ルーティングプロトコルの構文の例を示します。さまざまなプロトコルのコマンド構文については、Cisco IOS XE SD-WAN 認定コマンドリファレンスガイド [英語] を参照してください。

```
Device# config-transaction
Device(config)# router bgp autonomous-system-number
```

2. サービス VPN の IPv4 アドレスファミリを設定します。次に、BGP および EIGRP プロトコルのコマンド構文の例を示します。

   - BGP プロトコル：

     ```
     Device(config-router-af)# address-family ipv4 [unicast][vrf vrf-name]
     ```

   - EIGRP プロトコル：

     ```
     Device(config-router-af)# address-family ipv4 vrf vrf-number
     ```

3. グローバル VRF とサービス VPN 間のルートを再配布します。ここでは、BGP、OSPF、および EIGRP プロトコルの構文を示します。

   - サービス VPN からグローバル VRF にルートを再配布します。

     - BGP プロトコル：

       ```
       Device(config-router-af)# redistribute vrf vrf-name src_protocol
       [src_protocol_id] [route-map route-map-name]
       ```

- OSPF プロトコル：

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol
[src_protocol_id] [match {internal|external 1|external 2}] [metric
 {metric-value}] [subnets] [route-map route-map-name]
```

- EIGRP プロトコル：

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric
 effective-bandwidth-metric mtu-bytes] [route-map route-map-name]
```

- グローバル VRF からサービス VPN へのルートを再配布します。
  - BGP プロトコル：

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [route-map route-map-name]
```

  - OSPF プロトコル：

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [match {internal|external 1|external 2}]
[subnets] [route-map route-map-name]
```

  - EIGRP プロトコル：

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric
 effective-bandwidth-metric mtu-bytes]
```

次に、グローバル VRF とサービス VPN 間のルート再配布の設定例を示します。この例では、VRF 103 と VRF 104 がサービス VPN です。次に、BGP ルートがグローバル VRF から VRF 103、VRF 104 に再配布される例を示します。

```
config-transaction
router bgp 100

address-family ipv4 vrf 103
redistribute vrf global bgp 100 route-map test2
!
address-family ipv4 vrf 104
redistribute vrf global bgp 100 route-map test2
!
```

次に、グローバル VRF 65535 からサービス VRF に再配布される OSPF 内部ルートおよび外部ルートの設定例を示します。

この場合、**internal** および **external** キーワードの両方を使用して、すべての OSPF ルートがサービス VRF に再配布されます。

```
config-transaction
router ospf 1
redistribute vrf global ospf 65535 match internal external 1 external 2 subnets route-map
 ospf-route-map
```

次に、サービス VPN からグローバル VRF に再配布される OSPF 内部ルートおよび外部ルートの設定例を示します。

```
config-transaction
router ospf 101
redistribute vrf 101 ospf 101 match internal external 1 external 2 metric 1 subnets
route-map ospf-route-map
```

次に、サービス VPN からグローバル VRF に再配布される BGP ルートの設定例を示します。

```
config-transaction
router bgp 50000
address-family ipv4 unicast
redistribute vrf 102 bgp 50000 route-map BGP-route-map
```

次に、グローバル VRF からサービス VPN に再配布される BGP ルートの設定例を示します。

```
config-transaction
router bgp 50000
address-family ipv4 vrf 102
redistribute vrf global bgp 50000
```

次に、EIGRP ルーティングプロセスでの設定時に、グローバル VRF から VRF 1 への BGP プロトコル、接続プロトコル、OSPF プロトコル、および静的プロトコルのルート再配布の設定例を示します。

```
config-transaction
router eigrp 101
address-family ipv4 vrf 1
redistribute vrf global bgp 50000 metric 1000000 10 255 1 1500
redistribute vrf global connected metric 1000000 10 255 1 1500
redistribute vrf global ospf 65535 match internal external 1 external 2 metric 1000000
10 255 1 1500
redistribute vrf global static metric 1000000 10 255 1 1500
```

ルートの再配布の確認

例 1:

次に、**show ip bgp** コマンドで **internal** キーワードを使用した場合の出力例を示します。次に、VRF 102 からのルートが複製された後、グローバル VRF に正常に再配布される例を示します。

```
Device# show ip bgp 10.10.10.10 internal

BGP routing table entry for 10.10.10.10/8, version 515
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
700000 70707
10.10.14.17 from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 77775522, metric 7777, localpref 100, weight 32768, valid,
sourced, replicated, best
Community: 0:7227 65535:65535
Extended Community: SoO:721:75 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB320235DC0, path: 0x7FB320245DF8, pathext: 0x7FB3203A4660
flags: net: 0x0, path: 0x808040003, pathext: 0x81
attribute: 0x7FB38E5B6258, ref: 14
Updated on Jul 1 2021 01:16:36 UTC
vm5#
```

この出力では、ルートは VRF 102 からグローバル VRF に再配布されます。

次に、再配布のために複製されたルートを示す **show ip route** コマンドの出力例を示します。

```
Device# show ip route 10.10.10.10

Routing entry for 10.10.10.10/8
Known via "bgp 50000", distance 60, metric 7777
Tag 700000, type external,
replicated from topology(102)
Redistributing via ospf 65535, bgp 50000
Advertised by ospf 65535
bgp 50000 (self originated)
Last update from 10.10.14.17 5d15h ago
Routing Descriptor Blocks:
* 10.10.14.17 (102), from 10.10.14.17, 5d15h ago
opaque_ptr 0x7FB3202563A8
Route metric is 7777, traffic share count is 1
AS Hops 2
Route tag 700000
MPLS label: none
```

例 2：

次に、**show ip bgp vpnv4 vrf** コマンドで **internal** キーワードを使用した場合の出力例を示します。

```
Device# show ip bgp vpnv4 vrf 102 209.165.201.0 internal

BGP routing table entry for 1:102:10.10.10.10/8, version 679
BGP routing table entry for 1:209.165.201.0/27, version 679
Paths: (1 available, best #1, table 102)
Advertised to update-groups:
4
Refresh Epoch 1
7111 300000
10.1.15.13 (via default) from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 5755, metric 900, localpref 300, weight 32768, valid, sourced,
replicated, best
Community: 555:666
Large Community: 1:2:3 5:6:7 412789:412780:755
Extended Community: SoO:533:53 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB38E5C5718, path: 0x7FB3202668D8, pathext: 0x7FB38E69E960
flags: net: 0x0, path: 0x808040007, pathext: 0x181
attribute: 0x7FB320256798, ref: 7
Updated on Jul 6 2021 16:43:04 UTC
```

この出力では、ルートはグローバル VRF から VRF 102 に再配布されます。

次に、VRF 102 の再配布用に複製されたルートを示す **show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 102 209.165.201.0

Routing Table: 102
Routing entry for 209.165.201.0/27
Known via "bgp 50000", distance 20, metric 900
Tag 7111, type external,
replicated from topology(default)
Redistributing via bgp 50000
Advertised by bgp 50000 (self originated)
Last update from 10.1.15.13 00:04:57 ago
Routing Descriptor Blocks:
* 10.1.15.13 (default), from 10.1.15.13, 00:04:57 ago
```

```
opaque_ptr 0x7FB38E5B5E98
Route metric is 900, traffic share count is 1
AS Hops 2
Route tag 7111
MPLS label: none
```

CLIテンプレートを使用したサービスVPN間のルートリークの設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

CLI テンプレートの使用の詳細については、「CLI Add-on Feature Templates」および「CLI Templates」を参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

ここでは、Cisco IOS XE Catalyst SD-WAN デバイスでサービス VPN 間ルートリークを設定する CLI 設定例を示します。

- 同じデバイス上のサービス VRF 間でルートを複製します。

  vrf definition *vrf-number*
  address-family ipv4
  route-replicate from vrf *source-vrf-name* **unicast protocol** [**route-map** *map-tag*]

- サービス VPN 間で複製されたルートを再配布します。

  サブネットは、bgp、nhrp、ospf、ospfv3、および static プロトコルタイプについてのみ設定できます。

  router ospf *process-id* **vrf** *vrf-number*
  redistribute vrf *vrf-name protocol* **subnets**[**route-map** *map-tag*]

次に、サービス VRF 間のルート複製および再配布の完全な設定例を示します。

```
vrf definition 2
 rd 1:2
 !
 address-family ipv4
  route-replicate from vrf 1 unicast static route-map VRF1_TO_VRF2
 exit-address-family
 !
!
ip prefix-list VRF1_TO_VRF2 seq 5 permit 10.10.10.97/32
!
route-map VRF1_TO_VRF2 permit 1
 match ip address prefix-list VRF1_TO_VRF2
!
```

```
router ospf 2 vrf 2
 redistribute vrf 1 static route-map VRF1_TO_VRF2
```

CLI を使用したサービス VPN 間ルートリーク設定の確認

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a

次に、VRF 2 への再配布のために複製されたルートを示す **show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 2
Routing Table: 2
Codes: L - local, C - connected, S - static, 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S   +    10.10.10.97/32 [1/0] via 10.20.1.2 (1)
C        10.20.2.0/24 is directly connected, GigabitEthernet5
L        10.20.2.1/32 is directly connected, GigabitEthernet5
```

次に、VRF 1 から複製されたルートを示す **show ip cef vrf** コマンドの出力例を示します。

```
Device# show ip cef vrf 2 10.10.10.97 internal
10.10.10.97/32, epoch 0, RIB[S], refcnt 6, per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00048000
    Broker: linked, distributed at 3rd priority
  subblocks:
    Replicated from VRF 1
  ifnums:
    GigabitEthernet3(9): 10.20.1.2
  path list 7F890C8E2F20, 7 locks, per-destination, flags 0x69 [shble, rif, rcrsv, hwcn]

    path 7F890FB18F08, share 1/1, type recursive, for IPv4
     recursive via 10.20.1.2[IPv4:1], fib 7F890B609578, 1 terminal fib, v4:1:10.20.1.2/32

      path list 7F890C8E3148, 2 locks, per-destination, flags 0x49 [shble, rif, hwcn]
          path 7F890FB19178, share 1/1, type adjacency prefix, for IPv4
           attached to GigabitEthernet3, IP adj out of GigabitEthernet3, addr 10.20.1.2
 7F890FAE4CD8
  output chain:
    IP adj out of GigabitEthernet3, addr 10.20.1.2 7F890FAE4CD8
```

CLI を使用したリークされたサービス VPN を追跡するための VRRP トラッカーの設定

トラックを設定します。

1. グローバル コンフィギュレーション モードを開始し、IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

```
Device# config-transaction
Device(config)# track object-number {ip} route address|prefix-length  {
reachability  | metric threshold}
```

2. VPN ルーティングおよび転送（VRF）テーブルを設定します。

```
Device(config-track)# ip vrf vrf-name
```

3. 特権 EXEC モードに戻ります。

```
Device(config-track)# end
```

VRRP バージョン 2（VRRPv2）を設定します。

1. ギガビットイーサネットなどのインターフェイスタイプを設定します。

```
Device(config)# interface type number [name-tag]
```

2. VRF インスタンスをギガビット イーサネット インターフェイスに関連付けます。

```
Device(config-if)# vrf forwarding vrf-name
```

3. ギガビット イーサネット インターフェイスのプライマリ IP アドレスを設定します。

```
Device(config-if)# ip address ip-address [mask]
```

4. ギガビット イーサネット インターフェイスの速度、デュプレックスモード、およびフロー制御を自動ネゴシエーションプロトコルで設定できるようにします。

```
Device(config-if)# negotiation auto
```

5. VRRP グループを作成し、VRRP コンフィギュレーション モードを開始します。

```
Device(config-if)# vrrp group address-family ipv4
```

6. VRRP バージョン 3 と同時に VRRP バージョン 2 のサポートを有効にします。

```
Device(config-if-vrrp)# vrrpv2
```

7. VRRP の優先順位レベルを設定します。

```
Device(config-if-vrrp)# priority level
```

8. インターフェイス リスト トラッキングを単一のエンティティとして設定します。

```
Device(config-if-vrrp)# track track-list-name [decrement priority]
```

9. 優先順位の高いデバイスが引き継ぐ前に最低限の期間待機するように、プリエンプション遅延を設定します。

```
Device(config-if-vrrp)# preempt delay minimum seconds
```

10. VRRP のプライマリ IP アドレスを指定します。

```
Device(config-if-vrrp)# address ip-address primary
```

VRF を設定します。

1. VRF ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。

```
Device(config)# vrf definition vrf-number
```

2. VRF コンフィギュレーション モードで、アドレスファミリ IPv4 を設定します。

```
Device(config-vrf)# address-family ipv4
```

3. アドレスファミリ コンフィギュレーション モードを終了します。

```
Device(config-ipv4)# exit-address-family
```

次に、VRRP トラッキングの設定例を示します。

VRF red にトラックを追加するには、次の設定を使用します。

```
config-transaction
track 1 ip route 10.1.15.13 255.255.255.0 reachability
ip vrf red
```

インターフェイストラッキングを設定し、デバイスの優先順位を下げるには、次の設定を使用します。

```
interface GigabitEthernet 1.101
vrf forwarding 100
 ip address 10.1.15.13 255.255.255.0
 negotiation auto
 vrrp 2 address-family ipv4
  vrrpv2
  priority 220
  track 1 decrement 25
  preempt delay minimum 30
  address 10.1.15.100 primary
exit
```

設定された VRF の VRF ルーティング テーブル インスタンスを設定するには、次の設定を使用します。

```
vrf definition 100
!
 address-family ipv4
 exit-address-family
```

VRRP トラッキングの確認

例 1:

次に、Cisco IOS XE Catalyst SD-WAN デバイスに設定された VRRP グループのステータスを表示する **show vrrp details** コマンドの出力例を示します。

```
Device# show vrrp details
GigabitEthernet1/0/1 - Group 1 - Address-Family IPv4
  State is BACKUP         <------ check states
  State duration 2 mins 13.778 secs
  Virtual IP address is 10.0.0.1
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 1 (Configured 100)    <----- shows current and configured priority
    Track object 121 state DOWN decrement 220  Master Router is 10.1.1.3, priority is
200 <---- track object state
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 2737 msec)
  FLAGS: 0/1
  VRRPv3 Advertisements: sent 27 (errors 0) - rcvd 149
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Adverts received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
    Init to master: 0
    Init to backup: 1 (Last change Wed Feb 17 23:02:04.259)
    Backup to master: 1 (Last change Wed Feb 17 23:02:07.869)  <----- check this for
flaps
    Master to backup: 1 (Last change Wed Feb 17 23:02:32.008)
    Master to init: 0
    Backup to init: 0
```

例 2：

次に、VRRP トラッキングプロセスによって追跡されるオブジェクトに関する情報を表示する **show track** コマンドの出力例を示します。

```
Device# show track 1
Track 1
  IP route 209.165.200.225 209.165.200.236 reachability
  Reachability is Down (no ip route)
    1 change, last change 1w1d
  VPN Routing/Forwarding table "vrrp"
  First-hop interface is unknown
rtr3#
```

例 3：

次に、VRRP トラッキングプロセスによって追跡されるギガビットイーサネットインターフェイスの設定を表示する **show running-config interface** コマンドの出力例を示します。

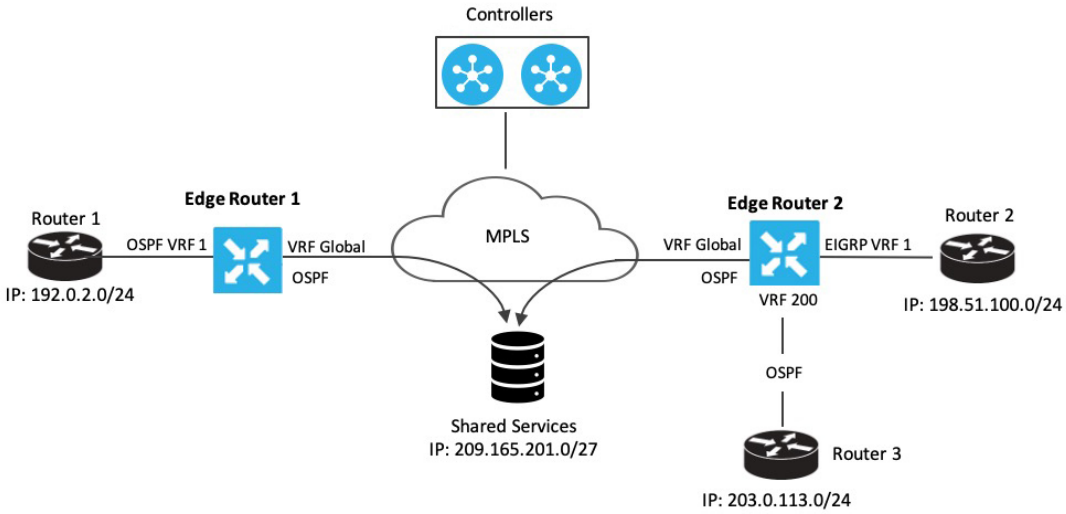
```
Device# show running-config interface GigabitEthernet 4
Building configuration...
Current configuration : 234 bytes
!
interface GigabitEthernet4
ip address 172.16.0.1 255.255.255.0
negotiation auto
vrrp 7 address-family ipv4
  priority 200
  vrrpv2
  track 5 decrement 5ß-------priority decreament
  address 172.16.0.0 primary
  exit-vrrp
no mop enabled
no mop sysid
end
```

ルートリークの設定例

ルートリークは通常、共有サービスを使用する必要があるシナリオで使用されます。ルートレプリケーションを設定すると、VRF または VPN 間の相互再配布が可能になります。ルートレプリケーションにより、ルートがグローバル VPF およびサービス VPN 間で複製またはリークされ、ある VPN に存在するクライアントが別の VPN に存在する一致するプレフィックスに到達できるため、共有サービスが可能になります。

トポロジの例

このセクションでは、ルートリーク設定を示すトポロジの例を使用します。ここでは、エッジルータ 1 と 2 がオーバーレイネットワークの 2 つの異なるサイトにあり、MPLS を介して相互に接続されています。両方のエッジルータで、アンダーレイネットワークのサービスにアクセスできるようにルートリークが設定されています。ルータ 1 は、サービス側のエッジルータ 1 の背後にあります。このサイトのローカルネットワークは OSPF を実行します。ルータ 2 は、VPN 1 に EIGRP があるネットワーク上のエッジルータ 2 の背後にあります。ルータ 3 もエッジルータ 2 の背後にあり、VRF 200 で OSPF を実行しています。



エッジルータ 1 は、ルータ 1 の送信元 IP アドレス 192.0.2.0/24 をエッジルータ 1 のグローバル VRF にインポートします。したがって、192.0.2.0/24 はグローバル VRF にリークされたルートです。エッジルータ 2 は、ルータ 2 の送信元 IP アドレス 198.51.100.0/24 とエッジルータ 3 の送信元 IP アドレス 203.0.113.0/24 をエッジルータ 2 のグローバル VRF にインポートします。

アンダーレイ MPLS ネットワークの共有サービスは、ループバックアドレス 209.21.25.18/27 を介してアクセスされます。共有サービスの IP アドレスは、OSPF を介してエッジルータ 1 および 2 のグローバル VRF にアドバタイズされます。この共有サービスの IP アドレスは、エッジルータ 1 の VRF 1 と、エッジルータ 2 の VRF 1 および VRF 200 にリークされます。ルートリークに関しては、リークされたルートは両方のエッジルータのサービス VRF にインポートされます。

（注） OMP はルートループを防止するために、リークされたルートをサービス VPN からオーバーレイネットワークにアドバタイズしません。

設定例

次に、エッジルータ 2 のグローバル VRF と VPN 1 の間で BGP および OSPF ルートリークが発生する設定の例を示します。

```
vrf definition 1
 rd 1:1
 !
  address-family ipv4
   route-replicate from vrf global unicast ospf 65535
 !
global-address-family ipv4
 route-replicate from vrf 1 unicast eigrp
 exit-address-family
```

次に、エッジルータ 2 のグローバル VRF と VPN 200 の間で BGP および OSPF ルートリークが発生する設定の例を示します。

```
vrf definition 200
 rd 1:200
 !
  address-family ipv4
   route-replicate from vrf global unicast ospf 65535
 !
global-address-family ipv4
 route-replicate from vrf 200 unicast eigrp
 exit-address-family
```

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。