



レイヤ 3 仮想化の設定

この章では、Cisco NX-OS デバイスでレイヤ 3 仮想化を設定する方法について説明します。

この章は、次の項で構成されています。

- [レイヤ 3 仮想化について \(1 ページ\)](#)
- [VRF の前提条件 \(5 ページ\)](#)
- [VRF の注意事項および制約事項 \(6 ページ\)](#)
- [VRF ルート リークの注意事項と制約事項 \(7 ページ\)](#)
- [デフォルト設定 \(7 ページ\)](#)
- [VRF の設定 \(8 ページ\)](#)
- [VRF の設定の確認 \(15 ページ\)](#)
- [VRF の設定例 \(15 ページ\)](#)
- [その他の参考資料 \(22 ページ\)](#)

レイヤ 3 仮想化について

Cisco NX-OS は、複数の仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。各 VRF には、IPv4 および IPv6 に対応するユニキャストおよびマルチキャスト ルート テーブルを備えた、独立したアドレス空間が 1 つずつあり、他の VRF と無関係にルーティングを決定できます。

ルータごとに、デフォルト VRF および管理 VRF があります。

管理 VRF

- 管理 VRF は管理専用です。
- mgmt 0 インターフェイスのみが、管理 VRF にいることができます。
- mgmt 0 インターフェイスは、異なる VRF に割り当てられることはできません。
- ルーティング プロトコルは、管理 VRF (スタティックのみ) で動作できません。

デフォルト VRF

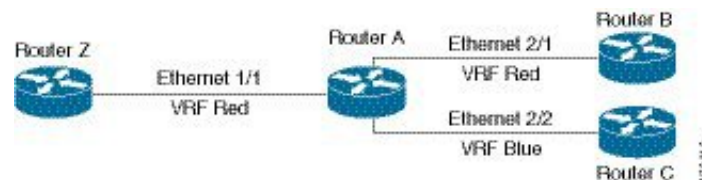
- すべてのレイヤ3 インターフェイスは、別の VRF に割り当てられるまでデフォルト VRF に存在します。
- 異なる VRF コンテキストが指定されない限り、ルーティング プロトコルはデフォルトの VRF コンテキストで実行されます。
- デフォルト VRF は、すべての show コマンドに対してデフォルトのルーティング コンテキストを使用します コマンドにも表示されません。
- デフォルト VRF は、Cisco IOS のグローバルルーティング テーブルの概念に似ています。

VRF およびルーティング

すべてのユニキャストおよびマルチキャストルーティングプロトコルは VRF をサポートします。VRF でルーティングプロトコルを設定する場合は、同じルーティングプロトコルインスタンスの別の VRF のルーティングパラメータに依存しないルーティングパラメータをその VRF に設定します。

VRF にインターフェイスおよびルーティングプロトコルを割り当てることによって、仮想レイヤ3 ネットワークを作成できます。インターフェイスが存在する VRF は1つだけです。次の図は、1つの物理ネットワークが2つの VRF からなる2つの仮想ネットワークに分割されている例を示しています。ルータ Z、A、および B は、VRF Red にあり、1つのアドレスドメインを形成しています。これらのルータは、Router C が含まれないルート更新を共有します。Router C は別の VRF で設定されているからです。

図 1: ネットワーク内の VRF



デフォルトで、着信インターフェイスの VRF を使用して、ルート検索に使用するルーティングテーブルを選択します。ルートポリシーを設定すると、この動作を変更し、Cisco NX-OS が着信パケットに使用する VRF を設定できます。

Cisco NX-OS は VRF 間のルートリーク（インポートまたはエクスポート）をサポートします。

デフォルトの VRF からのルートリークとルートのインポート

Cisco NX-OS は VRF 間のルートリーク（インポートまたはエクスポート）をサポートします。

インポートポリシーを使用して、グローバルルーティングテーブル（デフォルト VRF）から他の VRF に IP プレフィックスをインポートできます。VRF インポートポリシーはルートマップを使用して、VRF にインポートされるプレフィックスを指定します。ポリシーは、IPv4 および IPv6 ユニキャストプレフィックスをインポートできます。



- (注) BGPデフォルトVRFのルートは直接インポートできます。デフォルトVRFの他のルートは、最初にBGPに再配布する必要があります。

IPプレフィックスは、標準のルートポリシーフィルタリングメカニズムでインポートルートマップの一致基準として定義されます。たとえば、IPプレフィックスリストまたはas-pathフィルタを作成してIPプレフィックスまたはIPプレフィックス範囲を定義し、そのプレフィックスリストまたはas-pathフィルタをルートマップのmatch句で使用できます。ルートマップを通過したプレフィックスは、インポートポリシーを使用して指定されたVRFにインポートされます。このインポートポリシーによってVRFにインポートされたIPプレフィックスは、別のVRFに再インポートできません。

詳細については、「[VRF ルート リークの注意事項と制約事項](#)」セクションを参照してください。

IPv6 専用環境の BGP VRF ルーター ID

router-id を取得するソースを優先順に次に示します。

1. VRF レベル router-id コマンド
2. IPv4 アドレスが設定された VRF インターフェイス
3. デフォルトの VRF ルータ ID 設定からデフォルト以外の VRF ルータ ID を継承



- (注) router-id の 3 番目のソースの優先度は最も低く、1 番目と 2 番目のソースが利用できない場合にのみ適用されます。



- (注) router-id がない場合、BGP OPEN メッセージを送信できません。

VRF 認識サービス

Cisco NX-OS アーキテクチャの基本的な特徴として、すべての IP ベースの機能が VRF を認識することがあげられます。

次の VRF 認識サービスは、特定の VRF を選択することにより、リモートサーバへの接続や、選択した VRF に基づいた情報のフィルタリングを可能にします。

- AAA : 詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』を参照してください)。
- Call Home : 詳細については、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。

- DNS（ドメインネームシステム）：詳細については、[DNS の設定](#)を参照してください。
- HSRP：詳細については、[『Configuring HSRP』](#)を参照してください。
- HTTP：詳細については、[『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』](#)を参照してください。
- NTP：詳細については、[『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』](#)を参照してください。
- Ping と Traceroute：詳細については、[『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』](#)を参照してください。
- RADIUS：詳細については、[『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』](#)を参照してください。
- SNMP：詳細については、[『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』](#)を参照してください。
- SSH：詳細については、[『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』](#)を参照してください。
- Syslog：詳細については、[『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』](#)を参照してください。
- TACAS+：詳細については、[『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』](#)を参照してください。
- TFTP：詳細については、[『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』](#)を参照してください。
- VRRP（仮想ルータ冗長プロトコル）：詳細については、[VRRP の設定](#)を参照してください。
- XML：詳細については、[『Cisco NX-OS XML Management Interface User Guide』](#)を参照してください。

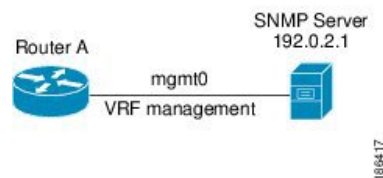
各サービスでVRFサポートを設定する詳細については、各サービスの適切なコンフィギュレーションガイドを参照してください。

Reachability

到達可能性は、サービスを提供するサーバに到達するために必要なルーティング情報がどのVRFにあるかを示します。たとえば、管理VRFで到達可能なSNMPサーバを設定できます。ルータにサーバアドレスを設定する場合は、サーバに到達するためにCisco NX-OSが使用するべきVRFも設定します。

次の図は、管理VRFを介して到達可能なSNMPサーバを示しています。SNMPサーバホスト192.0.2.1には管理VRFを使用するように、ルータAを設定します。

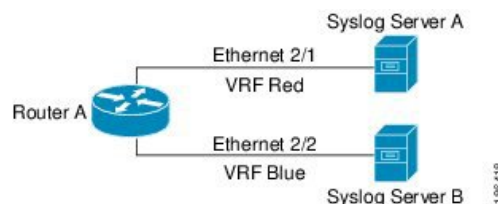
図 2: サービス VRF の到達可能性



フィルタリング

フィルタリングにより、VRF に基づいて VRF 認識サービスに渡される情報のタイプを制限できます。たとえば、Syslog サーバが特定の VRF をサポートするように設定できます。下に示す 2 つの Syslog サーバは、それぞれ 1 つの VRF をサポートしています。Syslog サーバ A は VRF Red で設定されているので、Cisco NX-OS は VRF Red で生成されたシステム メッセージだけを Syslog サーバ A に送信します。

図 3: サービス VRF のフィルタリング

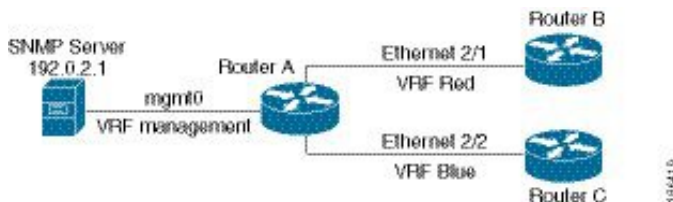


到達可能性とフィルタリングの組み合わせ

VRF 認識サービスの到達可能性とフィルタリングを組み合わせることができます。サービスに接続するために Cisco NX-OS が使用する VRF とともに、そのサービスがサポートする VRF も設定できます。デフォルト VRF でサービスを設定する場合は、任意で、すべての VRF をサポートするようにサービスを設定できます。

次の図は、管理 VRF を介して到達可能な SNMP サーバを示しています。たとえば、SNMP サーバが VRF Red からの SNMP 通知だけをサポートするように設定できます。

図 4: サービス VRF の到達可能性とフィルタリング



VRF の前提条件

デフォルト VDC 以外の仮想デバイス コンテキスト (VDC) を使用するには、Advanced Services ライセンスをインストールする必要があります。VRF のライセンス要件は VDC と同じです。

VRFの注意事項および制約事項

VRF設定時の注意事項と制約事項は次のとおりです。

- プレフィックスリスト内の名前は、大文字と小文字が区別されません。一意の名前を使用することを推奨します。大文字と小文字を変更しただけの名前は使用しないでください。たとえば、CTCPPrimaryNetworks と CtcPrimaryNetworks は2つの異なるエントリではありません。
- インターフェイスを既存のVRFのメンバにすると、Cisco NX-OSはあらゆるレイヤ3設定を削除します。VRFにインターフェイスを追加したあとで、すべてのレイヤ3パラメータを設定する必要があります。
- 管理VRFにmgmt0インターフェイスを追加し、そのあとでmgmt0のIPアドレスおよびその他のパラメータを設定します。
- VRFが存在しないうちにVRFのインターフェイスを設定した場合は、VRFを作成するまで、そのインターフェイスは運用上のダウンになります。
- Cisco NX-OSはデフォルトで、デフォルトと管理VRFを作成します。mgmt0は管理VRFのメンバにする必要があります。
- この項で説明している **write erase boot** コマンドを実行しても、管理VRFの設定は削除されません。**write erase** を使用する必要があります。コマンドを使用し、**write erase boot** コマンドを使用する必要があります。
- ルートターゲットには、次の注意事項と制約事項があります。
 - レイヤ2とレイヤ3に異なるルートターゲットを割り当てるのがベストプラクティスです。
 - 自動ルートターゲット生成では、ルートターゲットはEVIから生成されます。レイヤ2とレイヤ3で異なるEVI範囲を使用して、レイヤ2とレイヤ3のEVIが同じ識別子を使用しないようにすることをお勧めします。
- Cisco NX-OS リリース 10.3(1)F以降、マルチVRFがCisco Nexus 9808プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F以降、マルチVRFがCisco Nexus 9804プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F以降、マルチVRFは、Cisco Nexus 9808および9804スイッチを搭載したN9KX98900CD-AおよびN9KX9836DM-Aラインカードでサポートされます。

VRF ルート リークの注意事項と制約事項

VRF ルート リークには次の設定注意事項と制限があります。

- ルート リークは、任意の2つのデフォルト以外の VRF間、およびデフォルト VRF からデフォルト以外の VRF にサポートされます。



(注) VRF 間のルート リークは、MPLS セグメント ルーティング (SR-MPLS) ではサポートされません。

VRF 間のルート リークは BGP ではサポートされません。BGP スピーカーは、異なる VRF を介してルーティングされるピア IP には接続できません。

- デフォルト VRF へのルート リークは、グローバル VRF であるため使用できません。
- 指定した IP アドレスにマッチするルート マップのフィルタを使用して、特定のルートに対してルート リークを制限できます。
- デフォルトでは、デフォルト VRF からデフォルト以外の VRF にインポートできる (逆も可能) IP プレフィックスの最大数は 1000 ルートです。
- 2つの非デフォルト VRF間でリークできるルートの数に制限はありません。
- Cisco NX-OS リリース 10.3(1)F 以降、VRF 間のルート リークは Cisco Nexus 9808 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、VRF 間のルート リークは Cisco Nexus 9804 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、VRF 間のルート リークは、Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードでサポートされます。

デフォルト設定

次の表に、VRF パラメータのデフォルト設定値を示します。

表 1: デフォルトの VRF パラメータ

パラメータ	デフォルト
設定されている VRF	デフォルト、管理
ルーティング コンテキスト	デフォルト VRF

VRFの設定



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

VRFの作成

VRF を作成できます。



(注) グローバル設定モードで使用できるコマンドはすべて、VRF 設定モードでも使用できます。

手順の概要

1. **configure terminal**
2. **[no] vrf context name**
3. (任意) **ip route {ip-prefix | ip-addr ip-mask} {[next-hop | nh-prefix] | [interface next-hop | nh-prefix]} [tag tag-value [preference]**
4. (任意) **show vrf [vrf-name]**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] vrf context name 例： switch(config)# vrf context Enterprise switch(config-vrf)#	新しい VRF を作成し、VRF 設定モードを開始します。 <i>name</i> には最大 32 文字の英数字を使用できます。 大文字と小文字は区別されます。 このコマンドで no オプションを使用すると、VRF と、関連するすべての設定が削除されます。
ステップ 3	(任意) ip route {ip-prefix ip-addr ip-mask} {[next-hop nh-prefix] [interface next-hop nh-prefix]} [tag tag-value [preference] 例：	スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。任意でネクスト ホップ アドレスを設定できます。 <i>preference</i> 値でアドミニストレーティブディスタンスを設定します。範囲は 1 ~ 255 です。デフォルトは 1 です。

	コマンドまたはアクション	目的
	<code>switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4</code>	
ステップ4	(任意) show vrf [<i>vrf-name</i>] 例： <code>switch(config-vrf)# show vrf Enterprise</code>	VRF 情報を表示します。
ステップ5	(任意) copy running-config startup-config 例： <code>switch(config-vrf)# copy running-config startup-config</code>	この設定変更を保存します。

例

次に、VRF を作成し、VRF にスタティック ルートを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip route 192.0.2.0/8 ethernet 1/2
switch(config-vrf)# exit
switch(config)# copy running-config startup-config
```

インターフェイスへのVRFメンバーシップの割当て

インターフェイスをVRFのメンバにできます。

始める前に

VRF用のインターフェイスを設定したあとで、インターフェイスにIPアドレスを割り当てます。

手順の概要

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **vrf member** *vrf-name*
4. **ip address** *ip-prefix/length*
5. (任意) **show vrf** *vrf-name interface interface-type number*
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	switch# <code>configure terminal</code> switch(config)#	
ステップ2	interface <i>interface-type slot/port</i> 例： switch(config)# <code>interface ethernet 1/2</code> switch(config-if)#	インターフェイス設定モードを開始します。
ステップ3	vrf member <i>vrf-name</i> 例： switch(config-if)# <code>vrf member RemoteOfficeVRF</code>	このインターフェイスをVRFに追加します。
ステップ4	ip address <i>ip-prefix/length</i> 例： switch(config-if)# <code>ip address 192.0.2.1/16</code>	このインターフェイスのIPアドレスを設定します。 このステップは、このインターフェイスをVRFに割り当てたあとに行う必要があります。
ステップ5	(任意) show vrf <i>vrf-name interface interface-type number</i> 例： switch(config-vrf)# <code>show vrf Enterprise interface ethernet 1/2</code>	VRF情報を表示します。
ステップ6	(任意) copy running-config startup-config 例： switch(config-vrf)# <code>copy running-config startup-config</code>	この設定変更を保存します。

例

次に、VRFにインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# copy running-config startup-config
```

ルーティングプロトコル用のVRFパラメータの設定

1つまたは複数のVRFにルーティングプロトコルを関連付けることができます。ルーティングプロトコルに関するVRFの設定については、該当する章を参照してください。ここでは、詳細な設定手順の例として、OSPFv2プロトコルを使用します。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **vrf vrf-name**
4. (任意) **maximum-paths paths**
5. **exit**
6. **exit**
7. **interface interface-type slot/port**
8. **vrf member vrf-name**
9. **ip address ip-prefix/length**
10. **ip router ospf instance-tag area area-id**
11. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ2	router ospf instance-tag 例： switch (config-vrf)# router ospf 201 switch(config-router)#	インスタスタグが設定された新しいOSFPv2インスタンスを作成します。
ステップ3	vrf vrf-name 例： switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	VRF 設定モードを開始します。
ステップ4	(任意) maximum-paths paths 例： switch(config-router-vrf)# maximum-paths 4	この VRF のルート テーブル内の宛先への、同じ OSPFv2 パスの最大数を設定します。このコマンドはロード バランシングに使用されます。
ステップ5	exit 例： switch(config-router-vrf)# exit switch(config-router)#	VRF設定モードを終了します。
ステップ6	exit 例： switch(config-router)# exit switch(config)#	ルータ設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	interface <i>interface-type slot/port</i> 例： switch(config)# interface ethernet 1/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 8	vrf member <i>vrf-name</i> 例： switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 9	ip address <i>ip-prefix/length</i> 例： switch(config-if)# ip address 192.0.2.1/16	このインターフェイスの IP アドレスを設定します。 このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 10	ip router ospf <i>instance-tag area area-id</i> 例： switch(config-if)# ip router ospf 201 area 0	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 11	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# vrf context RemoteOfficeVRF
switch(config-vrf)# exit
switch(config)# router ospf 201
switch(config-router)# vrf RemoteOfficeVRF
switch(config-router-vrf)# maximum-paths 4
switch(config-router-vrf)# interface ethernet 1/2
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config-if)# exit
switch(config)# copy running-config startup-config
```

VRF 認識サービスの設定

VRF 認識サービスの到達可能性とフィルタリングを設定できます。

ここでは、サービスの詳細な設定手順の例として、SNMP および IP ドメイン リストを使用します。

手順の概要

1. **configure terminal**
2. **snmp-server host ip-address [filter-vrf vrf-name] [use-vrf vrf-name]**
3. **vrf context vrf-name**
4. **ip domain-list domain-name [all-vrfs] [use-vrf vrf-name]**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server host ip-address [filter-vrf vrf-name] [use-vrf vrf-name] 例： switch(config)# snmp-server host 192.0.2.1 use-vrf Red	グローバル SNMP サーバを設定し、サービスに到達するために Cisco NX-OS が使用する VRF を設定します。選択した VRF からこのサーバへの情報をフィルタリングするには、 filter-vrf キーワードを使用します。
ステップ 3	vrf context vrf-name 例： switch(config)# vrf context Blue switch(config-vrf)#	新しい VRF を作成します。
ステップ 4	ip domain-list domain-name [all-vrfs] [use-vrf vrf-name] 例： switch(config-vrf)# ip domain-list List all-vrfs use-vrf Blue	VRF でドメインリストを設定し、必要に応じて、リスト内のドメイン名に到達するために Cisco NX-OS が使用する VRF を設定します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config-vrf)# copy running-config startup-config	この設定変更を保存します。

例

次の例は、VRF Red 上の到達可能な SNMP ホスト 192.0.2.1 に、すべての VRF の SNMP 情報を送信する方法を示しています。

```
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 for-all-vrfs use-vrf Red
switch(config)# copy running-config startup-config
```

次の例は、VRF Red 上の到達可能な SNMP ホスト 192.0.2.12 に対して、VRF Blue の SNMP 情報をフィルタリングする方法を示しています。

```
switch# configure terminal
switch(config)# vrf context Blue
switch(config-vrf)# snmp-server host 192.0.2.12 use-vrf Red
switch(config)# copy running-config startup-config
```

VRF スコープの設定

すべての EXEC コマンド (**show** コマンドなど) の VRF スコープを設定できます。そうすることで、EXEC コマンド出力の範囲が設定された VRF に自動的に限定されます。この範囲は、一部の EXEC コマンドで使用できる VRF キーワードによって上書きできます。

手順の概要

1. `routing-context vrf vrf-name`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	routing-context vrf vrf-name 例 : <pre>switch# routing-context vrf red switch%red#</pre>	すべての EXEC コマンドに対応するルーティング コンテキストを設定します。デフォルトのルーティング コンテキストはデフォルト VRF です。 (注) routing-context vrf default コマンドを使用し、コマンドを使用して、デフォルトの VRF スコープに戻ります。

例

デフォルトの VRF スコープに戻すには、EXEC モードで次のコマンドを使用します。

コマンド	目的
routing-context vrf default 例 : <pre>switch%red# routing-context vrf default switch#</pre>	デフォルトのルーティング コンテキストを設定します。



(注) BGP 構成を使用して VPN VRF をシャットダウンすると、シャットダウンプロセスが完了するまでに約 50 秒かかります。

VRF の設定の確認

VRF 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show bgp process vrf [<i>vrf-name</i>]	すべてまたは1つの VRF の情報を表示します。
show vrf [<i>vrf-name</i>]	すべてまたは1つの VRF の情報を表示します。
show vrf [<i>vrf-name</i>] detail	すべてまたは1つの VRF の詳細情報を表示します。
show vrf [<i>vrf-name</i>] [interface <i>interface-type</i> <i>slot/port</i>]	インターフェイスの VRF ステータスを表示します。

VRF の設定例

次に、VRF Red を設定して、その VRF に SNMP サーバを追加し、VRF Red に OSPF インスタンスを追加する例を示します。

```
vrf context Red
  snmp-server host 192.0.2.12 use-vrf Red
  router ospf 201

vrf Red
  interface ethernet 1/2
  vrf member Red
  ip address 192.0.2.1/16
  ip router ospf 201 area 0
```

次に、VRF Red および Blue を設定し、各 VRF に OSPF インスタンスを追加して、各 OSPF インスタンスの SNMP コンテキストを作成する例を示します。

```
vrf context Red
vrf context Blue
vrf context Green

feature ospf
  router ospf Lab
  vrf Red

router ospf Production
  vrf Blue
  router-id 1.1.1.1
  vrf Green
  router-id 2.2.2.2
```

```
interface ethernet 1/2
  vrf member Red
  ip address 192.0.2.1/16
  ip router ospf Lab area 0
  no shutdown

interface ethernet 10/2
  vrf member Blue
  ip address 192.0.2.1/16
  ip router ospf Production area 0
  no shutdown

interface ethernet 10/3
  vrf member Green
  ip address 192.0.2.1/16
  ip router ospf Production area 0
  no shutdown

snmp-server user admin network-admin auth md5 nbv-12345
snmp-server community public ro

snmp-server context lab instance Lab vrf Red
snmp-server context production instance Production vrf Blue
```

この例で、VRF Red の OSPF インスタンス Lab の OSPF-MIB 値にアクセスするには、SNMP コンテキスト **lab** を使用します。

次に、デフォルト以外の2つのVRF間、およびデフォルトVRFからデフォルト以外のVRFにルートリークを設定する例を示します。

```
feature bgp
vrf context Green
  ip route 33.33.33.33/32 35.35.1.254
  address-family ipv4 unicast
  route-target import 3:3
  route-target export 2:2
  export map test
  import map test
  import vrf default map test

interface Ethernet1/7
  vrf member Green
  ip address 35.35.1.2/24

vrf context Shared
  ip route 44.44.44.44/32 45.45.1.254
  address-family ipv4 unicast
  route-target import 1:1
  route-target import 2:2
  route-target export 3:3
  export map test
  import map test
  import vrf default map test

interface Ethernet1/11
  vrf member Shared
  ip address 45.45.1.2/24

router bgp 100
  address-family ipv4 unicast
  redistribute static route-map test
  vrf Green
  address-family ipv4 unicast
```



```

        redistribute static route-map test
        vrf Shared
        address-family ipv4 unicast
        redistribute static route-map test

ip prefix-list test seq 5 permit 0.0.0.0/0 le 32
    route-map test permit 10
    match ip address prefix-list test

ip route 100.100.100.100/32 55.55.55.1
switch# show ip route vrf all
IP Route Table for VRF "default"
 '*' denotes best ucast next-hop
 *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

55.55.55.0/24, ubest/mbest: 1/0, attached
 *via 55.55.55.5, Lo0, [0/0], 00:07:59, direct
 55.55.55.5/32, ubest/mbest: 1/0, attached
 *via 55.55.55.5, Lo0, [0/0], 00:07:59, local
 100.100.100.100/32, ubest/mbest: 1/0
 *via 55.55.55.1, [1/0], 00:07:42, static

IP Route Table for VRF "management"
 '*' denotes best ucast next-hop
 *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
 *via 10.29.176.1, [1/0], 12:53:54, static
 10.29.176.0/24, ubest/mbest: 1/0, attached
 *via 10.29.176.233, mgmt0, [0/0], 13:11:57, direct
 10.29.176.233/32, ubest/mbest: 1/0, attached
 *via 10.29.176.233, mgmt0, [0/0], 13:11:57, local

IP Route Table for VRF "Green"
 '*' denotes best ucast next-hop
 *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>
 33.33.33.33/32, ubest/mbest: 1/0
 *via 35.35.1.254, [1/0], 00:23:44, static
 35.35.1.0/24, ubest/mbest: 1/0, attached
 *via 35.35.1.2, Eth1/7, [0/0], 00:26:46, direct
 35.35.1.2/32, ubest/mbest: 1/0, attached
 *via 35.35.1.2, Eth1/7, [0/0], 00:26:46, local
 44.44.44.44/32, ubest/mbest: 1/0
 *via 45.45.1.254%Shared, [20/0], 00:12:08, bgp-100, external, tag 100
 100.100.100.100/32, ubest/mbest: 1/0
 *via 55.55.55.1%default, [20/0], 00:07:41, bgp-100, external, tag 100

IP Route Table for VRF "Shared"
 '*' denotes best ucast next-hop
 *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

33.33.33.33/32, ubest/mbest: 1/0
 *via 35.35.1.254%Green, [20/0], 00:12:34, bgp-100, external, tag 100
 44.44.44.44/32, ubest/mbest: 1/0
 *via 45.45.1.254, [1/0], 00:23:16, static
 45.45.1.0/24, ubest/mbest: 1/0, attached

```

```

*via 45.45.1.2, Eth1/11, [0/0], 00:25:53, direct
45.45.1.2/32, ubest/mbest: 1/0, attached
*via 45.45.1.2, Eth1/11, [0/0], 00:25:53, local
100.100.100.100/32, ubest/mbest: 1/0
*via 55.55.55.1%default, [20/0], 00:07:41, bgp-100, external, tag 100
switch(config)#

```

次に、「`export vrf default`」コマンドで導入されたインポート済みルート of の再インポートを許可し、VPN インポート済みルートを `default-VRF` に再インポートできるようにする例を示します。

```

vrf context vpn1
  address-family ipv4 unicast
    export vrf default [<prefix-limit>] map <route-map> [allow-vpn]
  address-family ipv6 unicast
    export vrf default [<prefix-limit>] map <route-map> [allow-vpn]

```

次に、`border-leaf` 設定例を示します。

```

ip prefix-list DEFAULT_ROUTE seq 5 permit 0.0.0.0/0
route-map NO_DEFAULT_ROUTE deny 5
  match ip address prefix-list DEFAULT_ROUTE
route-map NO_DEFAULT_ROUTE permit 10
route-map allow permit 10

vrf context vni100
  vni 100
  ip route 0.0.0.0/0 Null0
  rd auto
  address-family ipv4 unicast
    route-target import 100:200
    route-target import 100:200 evpn
    route-target both auto
    route-target both auto evpn
  import vrf default map allow
  export vrf default map NO_DEFAULT_ROUTE allow-vpn
vrf context vni200
  vni 200
  ip route 0.0.0.0/0 Null0
  rd auto
  address-family ipv4 unicast
    route-target import 100:100
    route-target import 100:100 evpn
    route-target both auto
    route-target both auto evpn
  import vrf default map allow
  export vrf default map NO_DEFAULT_ROUTE

router bgp 100
  address-family ipv4 unicast
    redistribute direct route-map allow
  address-family ipv6 unicast
    redistribute direct route-map allow
  neighbor 101.101.101.101
    remote-as 100
  update-source loopback0
  address-family l2vpn evpn
    send-community extended
  neighbor 30.0.0.2
    remote-as 300
  address-family ipv4 unicast
  vrf vni100

```

```

address-family ipv4 unicast
  network 0.0.0.0/0
  advertise l2vpn evpn
  redistribute direct route-map allow
vrf vni200
  address-family ipv4 unicast
  network 0.0.0.0/0
  advertise l2vpn evpn
  redistribute direct route-map allow

```

次に、BGP IPv4 ユニキャスト設定の例を示します。

```

bl1(config-vrf)# show bgp ipv4 unicast 11.11.11.11/32
BGP routing table information for VRF default, address family IPv4 Unicast
BGP routing table entry for 11.11.11.11/32, version 14
Paths: (1 available, best #1)
Flags: (0x08041a) on xmit-list, is in urib, is best urib route, is in HW

```

```

Advertised path-id 1
Path type: internal, path is valid, is best path, in rib
  Imported from 3.3.3.3:11.11.11.11/32 (VRF vni100)
AS-Path: 150 , path sourced external to AS
  1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
  Origin incomplete, MED 0, localpref 100, weight 0
  Received label 100
  Extcommunity:
    RT:100:100
    ENCAP:8
    Router MAC:5254.004e.a437
  Originator: 1.1.1.1 Cluster list: 101.101.101.101

```

```

Path-id 1 advertised to peers:
  30.0.0.2

```

```

bl1(config-vrf)# show bgp vrf vni100 ipv4 unicast 11.11.11.11/32
BGP routing table information for VRF vni100, address family IPv4 Unicast
BGP routing table entry for 11.11.11.11/32, version 8
Paths: (1 available, best #1)
Flags: (0x08041e) on xmit-list, is in urib, is best urib route, is in HW
  vpn: version 19, (0x100002) on xmit-list

```

```

Advertised path-id 1, VPN AF advertised path-id 1
Path type: internal, path is valid, is best path, in rib
  Imported from 1.1.1.1:3:[5]:[0]:[0]:[32]:[11.11.11.11]:[0.0.0.0]/224
AS-Path: 150 , path sourced external to AS
  1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
  Origin incomplete, MED 0, localpref 100, weight 0
  Received label 100
  Extcommunity:
    RT:100:100
    ENCAP:8
    Router MAC:5254.004e.a437
  Originator: 1.1.1.1 Cluster list: 101.101.101.101

```

```

VRF advertise information:
Path-id 1 not advertised to any peer

```

```

VPN AF advertise information:
Path-id 1 not advertised to any peer

```

次に、BGP IPv6 ユニキャスト設定の例を示します。

```

b11(config-vrf)# show bgp ipv6 unicast 11::11/128
BGP routing table information for VRF default, address family IPv6 Unicast
BGP routing table entry for 11::11/128, version 13
Paths: (1 available, best #1)
Flags: (0x08041a) on xmit-list, is in u6rib, is best u6rib route, is in HW

  Advertised path-id 1
  Path type: internal, path is valid, is best path
             Imported from 3.3.3.3:3:11::11/128 (VRF vni100)
AS-Path: 150 , path sourced external to AS
::ffff:1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
  Origin incomplete, MED 0, localpref 100, weight 0
  Received label 100
  Extcommunity:
    RT:100:100
    ENCAP:8
    Router MAC:5254.004e.a437
    Originator: 1.1.1.1 Cluster list: 101.101.101.101

  Path-id 1 advertised to peers:
    30::2

b11(config-vrf)# show bgp vrf vni100 ipv6 unicast 11::11/128
BGP routing table information for VRF vni100, address family IPv6 Unicast
BGP routing table entry for 11::11/128, version 6
Paths: (1 available, best #1)
Flags: (0x08041e) on xmit-list, is in u6rib, is best u6rib route, is in HW
      vpn: version 7, (0x100002) on xmit-list

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: internal, path is valid, is best path
             Imported from 1.1.1.1:3:[5]:[0]:[0]:[128]:[11::11]:[0::]/416
AS-Path: 150 , path sourced external to AS
::ffff:1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
  Origin incomplete, MED 0, localpref 100, weight 0
  Received label 100
  Extcommunity:
    RT:100:100
    ENCAP:8
    Router MAC:5254.004e.a437
    Originator: 1.1.1.1 Cluster list: 101.101.101.101

VRF advertise information:
Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 not advertised to any peer

```

次に、`show route isis` コマンドの出力例を示します。

```

b11(config-if)# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

0.0.0.0/0, ubest/mbest: 1/0
  *via vrf vni100, Null0, [20/0], 1d04h, bgp-100, external, tag 100
1.1.1.1/32, ubest/mbest: 1/0
  *via 103.0.0.1, Eth1/1, [110/81], 1d04h, ospf-100, intra
2.2.2.2/32, ubest/mbest: 1/0
  *via 103.0.0.1, Eth1/1, [110/81], 1d04h, ospf-100, intra
3.3.3.3/32, ubest/mbest: 2/0, attached

```

```

    *via 3.3.3.3, Lo0, [0/0], 1d04h, local
    *via 3.3.3.3, Lo0, [0/0], 1d04h, direct
9.9.9.9/32, ubest/mbest: 1/0, attached
    *via 9.9.9.9%vni100, Lo9, [20/0], 1d03h, bgp-100, external, tag 100
10.0.0.0/24, ubest/mbest: 1/0
    *via 1.1.1.1, [200/0], 1d04h, bgp-100, internal, tag 100 (evpn) segid: 100 tunnelid:
    0x1010101 encap: VXLAN
11.11.11.11/32, ubest/mbest: 1/0
    *via 1.1.1.1, [200/0], 1d04h, bgp-100, internal, tag 150 (evpn) segid: 100 tunnelid:
    0x1010101 encap: VXLAN
20.0.0.0/24, ubest/mbest: 1/0
    *via 2.2.2.2, [200/0], 1d04h, bgp-100, internal, tag 100 (evpn) segid: 200 tunnelid:
    0x2020202 encap: VXLAN
22.22.22.22/32, ubest/mbest: 1/0
    *via 2.2.2.2, [200/0], 1d04h, bgp-100, internal, tag 250 (evpn) segid: 200 tunnelid:
    0x2020202 encap: VXLAN
30.0.0.0/24, ubest/mbest: 1/0, attached
    *via 30.0.0.1, Eth1/2, [0/0], 1d04h, direct
30.0.0.1/32, ubest/mbest: 1/0, attached
    *via 30.0.0.1, Eth1/2, [0/0], 1d04h, local
33.33.33.33/32, ubest/mbest: 1/0
    *via 30.0.0.2, [20/0], 1d04h, bgp-100, external, tag 300
100.0.0.0/24, ubest/mbest: 1/0, attached
    *via 100.0.0.3%vni100, Vlan100, [20/0], 1d04h, bgp-100, external, tag 100
101.0.0.0/24, ubest/mbest: 1/0
    *via 103.0.0.1, Eth1/1, [110/80], 1d04h, ospf-100, intra
101.101.101.101/32, ubest/mbest: 1/0
    *via 103.0.0.1, Eth1/1, [110/41], 1d04h, ospf-100, intra
102.0.0.0/24, ubest/mbest: 1/0
    *via 103.0.0.1, Eth1/1, [110/80], 1d04h, ospf-100, intra
103.0.0.0/24, ubest/mbest: 1/0, attached
    *via 103.0.0.2, Eth1/1, [0/0], 1d04h, direct
103.0.0.2/32, ubest/mbest: 1/0, attached

```

show ipv6 route コマンドの出力例を示します。

```

b11(config-vrf)# show bgp ipv6 unicast 11::11/128
BGP routing table information for VRF default, address family IPv6 Unicast
BGP routing table entry for 11::11/128, version 13
Paths: (1 available, best #1)
Flags: (0x08041a) on xmit-list, is in u6rib, is best u6rib route, is in HW

```

```

Advertised path-id 1
Path type: internal, path is valid, is best path
    Imported from 3.3.3.3:3:11::11/128 (VRF vni100)
AS-Path: 150 , path sourced external to AS
::ffff:1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
    Origin incomplete, MED 0, localpref 100, weight 0
    Received label 100
    Extcommunity:
        RT:100:100
        ENCAP:8
        Router MAC:5254.004e.a437
    Originator: 1.1.1.1 Cluster list: 101.101.101.101

```

```

Path-id 1 advertised to peers:
30::2

```

```

b11(config-vrf)# show bgp vrf vni100 ipv6 unicast 11::11/128
BGP routing table information for VRF vni100, address family IPv6 Unicast
BGP routing table entry for 11::11/128, version 6
Paths: (1 available, best #1)
Flags: (0x08041e) on xmit-list, is in u6rib, is best u6rib route, is in HW

```

```

vpn: version 7, (0x100002) on xmit-list

Advertised path-id 1, VPN AF advertised path-id 1
Path type: internal, path is valid, is best path
    Imported from 1.1.1.1:3:[5]:[0]:[0]:[128]:[11::11]:[0::]/416
AS-Path: 150 , path sourced external to AS
::ffff:1.1.1.1 (metric 81) from 101.101.101.101 (101.101.101.101)
  Origin incomplete, MED 0, localpref 100, weight 0
  Received label 100
  Extcommunity:
    RT:100:100
    ENCAP:8
    Router MAC:5254.004e.a437
  Originator: 1.1.1.1 Cluster list: 101.101.101.101

VRF advertise information:
Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 not advertised to any peer

```

その他の参考資料

仮想化の実装に関する詳細情報については、次の項を参照してください。

VRF の関連資料

関連項目	マニュアル タイトル
VRF	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』 『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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。