VLANs

この章では、強化サービスまたは拡張サービスをサポートする仮想ローカルエリアネットワーク（VLAN）の設定について説明します。製品固有や機能固有の「アドミニストレーション ガイド」には、VLAN を使用する可能性のあるシステムでのサービスの設定例と手順が記載されています。次に説明する手順を使用する前に、サービスモデルに最適な設定例を選択する必要があります。

- 概要 （1 ページ）
- VLAN および StarOS （3 ページ）
- VLAN およびハイパーバイザ （3 ページ）
- VLAN および KVM ハイパーバイザ （4 ページ）
- VLAN 対応 VM （5 ページ）
- VLAN および VMware （5 ページ）
- VLAN タグの設定 （6 ページ）
- ポート設定の確認 （7 ページ）
- サブスクライバ VLAN の関連付けの設定 （8 ページ）
- VLAN 関連の CLI コマンド （9 ページ）

概要

仮想 LAN（VLAN）は、コンテキストおよびサービスの設定と使用の柔軟性を高めます。

これらはポートごとに「タグ」として設定され、より複雑な設定を実装することができます。VLAN タグを使用すると、1 つの物理ポートを複数の論理インターフェイスにバインドして、異なるコンテキスト内に設定できます。したがって、各イーサネットポートは、VLAN タグが使用されている場合は多くの論理ポートが含まれているように表示されることがあります。

VLAN は、ハイパーバイザレベルと StarOS レベルで作成できます。VLAN を作成する場所は、特定のネットワーク要件によって異なります。

オーバーラッピング IP アドレスプールのサポート：GGSN

IPアドレスプールの重複により、オペレータは、物理的に分離されたルータや仮想ルータに高価な投資をすることなく、同じプライベート IP アドレス空間を持つ複数の企業の VPN 顧客を柔軟にサポートできます。

システムは、次の 2 種類の重複プールをサポートしています。

- リソースプールはダイナミック割り当て専用に設計されており、VPN トンネル（GRE トンネルなど）を使用して、VPN との間でプライベート IP アドレスを転送および受信します。
- 重複プールは、ダイナミックアドレッシングとスタティックアドレッシングの両方に使用でき、VLAN とネクストホップ転送アドレスを使用して VPN カスタマに接続できます。

ダウンストリーム トラフィックを正しい PDP コンテキストに転送するために、GGSN は GRE トンネル ID または VLAN ID のいずれかを使用してパケットを照合します。トラフィックをアップストリームに転送する場合、GGSN は IP プール設定でトンネルおよび転送情報を使用します。重複するプールは、このようなインスタンスの APN で設定する必要があります。

PDP コンテキストが作成されると、IP アドレスが IP プールから割り当てられます。この場合、転送ルールも GGSN に設定されます。アドレスが静的に割り当てられている場合、GGSN が APN で設定されたプールから IP アドレスを確認すると、転送ルールも適用されます。

GGSN は、コンテキストごとの VLAN インターフェイスと同じ数の実際の重複プールに合わせて拡張でき、GGSN ごとに複数のコンテキストが存在することがあります。制限は IP プールの数です。この拡張性により、顧客のプライベート IP アドレス空間を使用して VPN サービスを顧客に提供するオペレータが、ハードウェアコストの増加や複雑な設定について心配する必要がなくなります。

RADIUS VLAN サポート：Enhanced Charging サービス

VPN のお客様は、多くの場合、他の顧客と簡単にオーバーラップできるプライベートアドレス空間を使用しています。サブスクライバアドレスは、同じ仮想ルーティングコンテキスト内で設定できるオーバーラッピングプールでサポートされています。

RADIUS サーバーと NAS の IP アドレスが別々のコンテキスト内である必要がないため、APN と RADIUS の設定とネットワーク設計がシンプルになります。この機能を使用すると、同じコンテキスト内に次のシナリオを定義できます。

- さまざまな APN を表すさまざまな RADIUS サーバーグループの RADIUS NAS-IP アドレスのオーバーラッピング
- さまざまな RADIUS サーバーグループの RADIUS サーバー IP アドレスのオーバーラッピング

オーバーラッピング NAS-IP アドレスすべてに固有のネクストホップアドレスが指定されて、固有の VLAN にバインドされるインターフェイスにバインドされます。これにより、同じコンテキストにこの設定が存在できるようになります。

システムは、RADIUS アクセス要求やアカウンティングメッセージを、その NAS-IP に定義されているネクストホップに転送します。接続されているルータがそのメッセージを RADIUS サーバーに転送します。ネクストホップアドレスによって、使用するインターフェイスと VLAN が決まります。サーバーからのトラフィックは、ポートや VLAN の組み合わせによって特定の NAS-IP に属しているものとして識別されます。

設定可能な RADIUS NAS-IP アドレスの数は、設定可能なループバックアドレスの数によって制限されます。

APN サポート：PDN ゲートウェイ（P-GW）

P-GWアクセスポイント名（APN）は、APNに対する広範なパラメータ設定の柔軟性をサポートします。APN では VLAN タグを選択できますが、APN とは別に、P-GW で設定されます。

VLAN および StarOS

StarOS は、いくつかのゲートウェイ製品の VLAN をサポートしています。

（注） VLAN は、サブスクライバ vNIC トラフィックポート 1-10 ～ 1-21 とあわせてサポートされています。StarOSは、付録の「エンジニアリングルール」で説明されているように、VLANの設定制限をサポートしています。

VLAN およびハイパーバイザ

ネットワークを介して処理されているパケットのタイプに応じて、ハイパーバイザは VPC-SI 仮想マシン（VM）とパケットを交換する前に、さまざまな VLAN タスクを実行します。

- **管理パケット** MGMT パケットはタグなしで着信し、ハイパーバイザはこれらのパケットを追加の VLAN 処理なしで VM と交換します。
- **アクセスパケット** は、VLAN タグ付きで物理ネットワークから着信します。ハイパーバイザは、VLANタグをVMに転送する前に削除します。受信したパケットは、物理ネットワークを介して送信される前に再度タグ付けされます。
- **トランキング**パケットは、VLANタグ付きで物理ネットワークを介して発着信します。ハイパーバイザは、タグ付きのパケットを追加処理のために VM に送信する前に、タグをフィルタ処理します。

管理、アクセス、およびトランキングの各パケットは、個別のコンテキストで定義し、一意のインターフェイスにバインドする必要があります。ハイパーバイザは、適切なタイプのVLANタグ付けを行うか、またはパケットタイプに基づいたフィルタ処理を行うように設定する必要があります。

詳細については、VLANサポートと送信元を簡単に説明している次の項を参照してください。

• VLAN および KVM ハイパーバイザ （4 ページ）
• VLAN および VMware （5 ページ）

VLAN および KVM ハイパーバイザ

ネットワークの分離

Ubuntu ネットワーキングスタックの実装により、KVM ホストは、単純なレイヤ 2 ブリッジ（イーサネットスイッチ）、転送または NAT ルータ、ステートフルファイアウォール、またはこれらのロールの任意の組み合わせとして機能できます。

VLAN 対ブリッジインターフェイス

KVM 仮想化のシナリオでは、VLAN 使用率をシンプルなブリッジインターフェイス共有の拡張と見なすことができます。違いは、ブリッジセットに参加するインターフェイスです。標準動作モード（イーサネットブリッジとのネットワークポート共有の例を参照）では、物理インターフェイス（eth0、eth1... など）はブリッジにバインドされ、各ゲストが使用します。これらのインターフェイスは、VLAN ID タグの有無にかかわらず、外部から着信するか、または内部で生成された未変更のパケットを伝送します。

サブインターフェイスを作成することで、特定のVLAN IDを伝送していないすべてのパッケージを除外できます。これらのサブインターフェイスは、特定の VLAN ID によって定義された VLAN の一部になります。

この概念をブリッジされたインターフェイスの共有方式に適用するには、バインドされた物理インターフェイスを、特定の VLAN セグメンテーションの一部であるサブインターフェイスに置き換える必要があります。このようにして、このブリッジにバインドされたインターフェイスを持つすべての仮想マシンゲストは、その特定の VLAN の一部になります。シンプルなイーサネットブリッジ環境と同様に、提供されるネットワークは透過的です。

（注） すべての vNIC タイプがブリッジへの VLAN トランキングをサポートしているわけではありません。これは多くの場合、ハードウェアで VLAN が除外されためです。

その他の情報

KVM ハイパーバイザを使用した VLAN の設定の詳細については、次の URL を参照してください。

• *802.1q VLAN* の設定：
https://www.ibm.com/support/knowledgecenter/linuxonibm/liaat/liaatkvmsecconfvlans.htm

- *KVM/Networking*：https://help.ubuntu.com/community/KVM/Networking

VLAN 対応 VM

VLAN 対応 VM インスタンスは、単一の vNIC を介して VLAN タグ付きトラフィックを送受信します。VLAN 対応は、VLAN タグ付きトラフィックを予期している NFV アプリケーション（VNF）に役立ち、単一の vNIC で複数のサービスを提供できます。トランクインターフェイスを備えた VLAN 対応 VM を使用すると、接続が中断されることなく、ネットワークの自動追加と削除を容易に行うことができます。

VLAN トランクは、VLAN を単一のトランクポートに結合することで、VLAN 対応インスタンスをサポートします。VLAN タグ付きトラフィックのトランクを実装するには、次の手順を実行します。

- 親ポートを作成し、新しいポートを既存の Neutron ネットワークに接続します。新しいポートを接続すると、OpenStack ネットワーキング（Neutron）は、作成した親ポートにトランク接続を追加します。
- サブポートを作成します。これらのサブポートは VLAN をインスタンスに接続してトランクへの接続を可能にします。

OpenStack ネットワーキングサービス（Neutron）がサブポートに割り当てた MAC アドレスを使用するように VM インスタンスを展開します。Elastic Services Controller（ESC）5.8 バージョンは、この VLAN 対応 VM をサポートしています。

制限事項：

SRIOV VF を介した VLAN 対応の VM に対する Red Hat での既知の RFE 障害により、VPC DI の展開時および親ポートを VM に接続する際の VLAN 対応には次の 2 つの制限があります。

- VLAN 対応 VM 設定の一部として作成された Neutron トランクポートのステータスは DOWN です。
- 複数の VLAN ID で作成されたサブポートは Detached 状態です。

VLAN および VMware

VMware は、ネットワーク展開入要件を満たすために VLAN の設定をサポートしています。

VLAN の設定

VLAN を使用すると、単一の物理 LAN セグメントをさらに分割して、ポートのグループが物理的に異なるセグメント上にあるかのように分離することができます。

次の理由により、VLAN ありの ESXi を設定することを推奨します。

- これにより、ホストが既存の環境に統合されます。

- これにより、ホストが既存の環境に統合されます。
- これにより、ネットワークトラフィックの輻輳が軽減されます。
- iSCSI トラフィックには、隔離されたネットワークが必要です。

外部スイッチタグ（EST）、仮想スイッチタグ（VST）、および仮想ゲストタグ（VGT）の 3 つの方法で、ESXi で VLAN を設定できます。

- EST を使用すると、パケットのすべての VLAN タグ付けが物理スイッチで実行されます。ホストネットワークアダプタは、物理スイッチのアクセスポートに接続されています。仮想スイッチに接続されているポートグループは、VLAN ID を 0 に設定する必要があります。

VST を使用すると、ホストを離れる前にパケットのすべての VLAN タグ付けが仮想スイッチによって実行されます。ホストネットワークアダプタは、物理スイッチのトランクポートに接続されている必要があります。また、仮想スイッチに接続されているポートグループには、適切な VLAN ID が指定されている必要があります。

VGT を使用すると、すべての VLAN タグ付けが仮想マシンによって実行されます。VGT の場合、VLAN ID = 4095 です。仮想スイッチとの間でフレームが渡されると、仮想マシンのネットワーキングスタックと外部スイッチの間で VLAN タグが保持されます。物理スイッチポートは、トランクポートに設定されます。

その他の情報

VMware ハイパーバイザを使用した VLAN の設定の詳細については、次のドキュメントを参照してください。

- UCS および VMware での VLAN の設定
- VLAN の設定については、VMware のドキュメントを参照してください。
- ESXi ホストへの VLAN ID の割り当てについては、VMware のドキュメントを参照してください。
- 仮想スイッチ、物理スイッチ、および仮想マシンでの VLAN の構成については、VMware のドキュメントを参照してください。

VLAN タグの設定

ポートで VLAN を作成し、既存のインターフェイスにバインドするには、次の例を使用します。インターフェイスの作成については、「システムインターフェイスとポート」を参照してください。

```
config
  port ethernet slot/port
    no shutdown
    vlan vlan_tag_ID
    no shutdown
```

```
bind interface interface_name context_name
end
```

注：

- オプション：VLANサブスクライバの関連付けを設定します。詳細については、サブスクライバ VLAN の関連付けの設定 （8 ページ） を参照してください。
- ポートの追加の VLAN を設定するには、必要に応じてこの手順を繰り返します。
- 詳細については、VLAN 関連の CLI コマンド （9 ページ）および『*Command Line Interface Reference*』を参照してください。
- 「設定の確認と保存」の章の説明に従って、設定を保存します。

ポート設定の確認

次のコマンドを実行してポート設定を確認します。

```
[local]host_name# show port info slot/port
```

ポートに対して少なくとも 1 つの VLAN が設定されている場合のこのコマンドの出力例を次に示します。

```
Port: 5/11
  Port Type               : 10G Ethernet
  Role                    : Service Port
  Description             : (None Set)
  Redundancy Mode         : Port Mode
  Redundant With          : 6/11
  Preferred Port          : Non-Revertive
  Physical ifIndex        : 85262336
  Administrative State    : Enabled
  Configured Duplex       : Auto
  Configured Speed        : Auto
  Fault Unidirection Mode : 802_3ae clause 46
  Configured Flow Control : Enabled
  Interface MAC Address   : 64-9E-F3-69-5B-EA
  SRP Virtual MAC Address : None
  Fixed MAC Address       : 64-9E-F3-69-5B-CA
  Link State              : Up
  Link Duplex             : Full
  Link Speed              : 10 Gb
  Flow Control            : Enabled
  Link Aggregation Group  : None
  Untagged:
    Logical ifIndex       : 85262337
    Operational State     : Up, Active
  Tagged VLAN: VID 10
    Logical ifIndex       : 285278210
    VLAN Type             : Standard
    VLAN Priority         : 0
    Administrative State  : Enabled
    Operational State     : Up, Active
  Number of VLANs         : 1
  SFP Module              : Present (10G Base-SR)
```

注：

- 必要に応じてこの手順を繰り返して、追加ポートを確認します。
- オプション：VLANサブスクライバの関連付けを設定します。詳細については、サブスクライバ VLAN の関連付けの設定 （8 ページ） を参照してください。
- 追加情報については、VLAN 関連の CLI コマンド （9 ページ）を参照してください。
- 「設定の確認と保存」の章の説明に従って、設定を保存します。

サブスクライバ VLAN の関連付けの設定

サブスクライバトラフィックは、ユーザープロファイルの設定に基づいて特定のVLANにルーティングできます。この機能によって、指定した VLAN を介してサブスクライバからすべてのトラフィックをルーティングするメカニズムが実現します。また、サブスクライバ宛のすべてのパケットは VLAN 上で有効な IP アドレスのみを使用して送信する必要があります。そうでない場合はドロップされます。

使用される RADIUS 属性

次の RADIUS 属性を RADIUS サーバー上のサブスクライバプロファイル内で設定して、特定の VLAN をサブスクライバに関連付けることができます。

- **SN-Assigned-VLAN-ID**：Starent VSA ディクショナリ内
- **SN1-Assigned-VLAN-ID**： Starent VSA1 ディクショナリ内

重要 サブスクライバプロファイルの設定手順は RADIUS サーバーアプリケーション間で異なるため、この項では、サブスクライバプロファイルに追加できる個々の属性についてのみ説明します。サブスクライバの設定手順については、RADIUSサーバーに付属のマニュアルを参照してください。

ローカルサブスクライバのプロファイルの設定

システム上のローカルサブスクライバのプロファイル内でVLANの関連付けを設定するには、次の設定例を使用します。

重要 これらの手順は、VLAN タグの設定 （6 ページ） に記載されている手順に従って、サブスクライバタイプの VLAN タグがすでに設定されていることを前提としています。

```
config
  context context_name
    subscriber name user_name
```

```
ip vlan vlan_id
end
```

サブスクライバのプロファイル設定の確認

サブスクライバプロファイルの設定を表示するには、次のコマンドを使用します。

```
[local]host_name# show subscriber configuration username user_name
```

注：

- 各サブスクライバに対してこのコマンドを繰り返します。
- 「設定の確認と保存」の章の説明に従って、設定を保存します。

VLAN 関連の CLI コマンド

VLAN 関連の機能は、いくつかの CLI コマンドモードでサポートされています。次の表に、VLAN 関連の機能の設定とモニタリングに関連するコマンドを示します。

次に示すコマンドの使用に関する詳細については、『*Command Line Interface Reference*』を参照してください。

表 *1 : VLAN* 関連の設定コマンド

CLI モード	コマンド	説明
AAA サーバー グループ構成モード	**radius attribute nas-ip-address address** *ip_address* **nexthop-forwarding-address** *ip_address* **vlan** *vlan_id*	単一ネクストホップ ゲートウェイ モードで実行しているシステムへのネクストホップ転送アドレスを持つ VLAN ID を提供するように RADIUS クライアントを設定します。 **注**：**vlan** キーワードにアクセスするには、グローバル構成モードで **aaa-large configuration** を有効にする必要があります。
ACS 課金アクション構成モード	**ip vlan** *vlan_id*	接続先コンテキストのサブスクライバ トラフィックに関連付ける VLAN 識別子を設定します。

CLI モード	コマンド	説明
コンテキスト構成モード	**ip pool** *pool_name* **nexthop forwarding address** *ip_address* **overlap vlanid** *vlan_id*	テクストホップ転送アドレスが設定されている場合、**overlap vlanid** を使用するとIPアドレスプールのオーバーラップが可能になり、指定した VLAN ID にプールを関連付けます。
コンテキスト構成モード	**ip routing overlap-pool**	VLAN ID を使用してプールの重複が設定されている場合、ダイナミックルーティングプロトコルでオーバーラッププールアドレスがアドバタイズされます。有効にすると、オーバーラップアドレスがインターフェイスアドレスとして追加され、アドバタイズされます。
コンテキスト構成モード	**radius attribute nas-ip-address address** *ip_address* **nexthop-forwarding-address** *ip_address* **vlan** *vlan_id*	ネクストホップ IP アドレスに関連付ける VLAN ID を指定します。
イーサネットインターフェイス構成モード	**[no] logical-port-statistics**	最初の32設定されたイーサネットまたはPVCインターフェイスタイプの論理ポート（VLAN と NPU）のバルク統計情報の収集を有効または無効にします。
イーサネットインターフェイス構成モード	**vlan-map next-hop** *ipv4_address*	単一ネクストホップ IP アドレスを設定して、複数の VLAN が単一のネクストホップゲートウェイを使用できるようにします。VLAN マップが特定のインターフェイスに関連付けられます。
イーサネット ポート構成モード	**vlan** *vlan_id*	VLAN 構成モードを開始します。
PVC 構成モード	**[no] shutdown**	指定した VLAN 上のトラフィックを有効または無効にします。次を参照してください。

CLI モード	コマンド	説明
サブスクライバ構成モード	**ip vlan** *vlan_id*	サブスクライバセッションがパケットを受信するために割り当てられたアドレスとともに使用するサブスクライバ VLAN ID を設定します。アドレスが割り当てられている IP プールが VLAN ID を使用して設定されている場合、このサブスクライバで設定された VLAN ID がそのアドレスを上書きします。
VLAN 構成モード	**bind interface** *interface_name context_name*	VLAN サービスをサポートするために、仮想インターフェイスとコンテキストをバインドします。
VLAN 構成モード	**[no] ingress-mode**	ポート入力着信モードを有効または無効にします。
VLAN 構成モード	**priority** *value*	ASN-GW サービスの 802.1p VLAN 優先順位ビットのみを設定します。
VLAN 構成モード	**[no] shutdown**	現在の VLAN 上のトラフィックを有効または無効にします。
VLAN 構成モード	**vlan-map interface** *if_name context_name*	VLAN ID を持つ IP インターフェイスをコンテキストに関連付けます。

表 *2 : VLAN* 関連のモニタリングコマンド

CLI モード	コマンド	説明
Exec モードの show コマンド	**clear port** *slot/port* **vlan** *vlan_id*	以前に設定された VLAN ID を持つポートの NPU 統計をクリアします。
Exec モードの show コマンド	**show logical-port utilization table vlan { 5-minute | hourly }**	指定された収集間隔の VLAN 使用率を表示します。
Exec モードの show コマンド	**show port info** *slot/port* **vlan** *vlan_id*	以前に設定された VLAN ID の NPU カウンタを表示します。

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。