

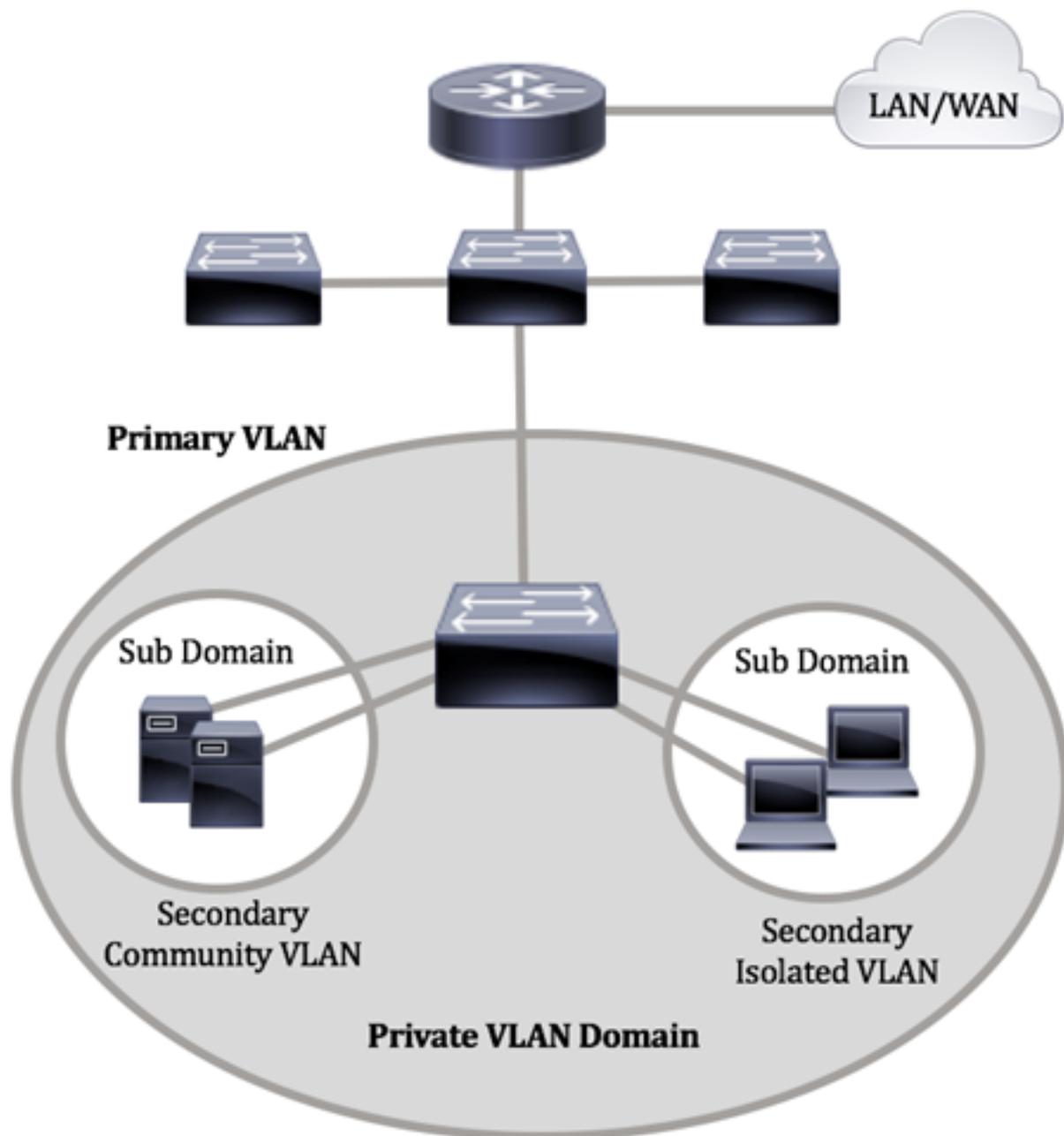
CLIを使用したスイッチでのプライベートVLANメンバーシップの設定

概要

仮想ローカルエリアネットワーク(VLAN)を使用すると、ローカルエリアネットワーク(LAN)を論理的に異なるブロードキャストドメインにセグメント化できます。機密データがネットワーク上でブロードキャストされるシナリオでは、特定のVLANにブロードキャストを指定することでセキュリティを強化するためにVLANを作成できます。VLANに属するユーザだけが、そのVLANのデータにアクセスして操作できます。また、VLANを使用して、ブロードキャストやマルチキャストを不要な宛先に送信する必要性を減らし、パフォーマンスを向上させることもできます。

注：Webベースのユーティリティを使用してスイッチのVLAN設定を構成する方法については、[ここをクリックしてください](#)。CLIベースの手順については、[ここをクリックします](#)。

プライベートVLANドメインは、1つまたは複数のVLANペアで構成されます。プライマリVLANがドメインを構成します。各VLANペアはサブドメインを構成します。ペアのVLANは、プライマリVLANとセカンダリVLANと呼ばれます。プライベートVLAN内のすべてのVLANペアには、同じプライマリVLANがあります。セカンダリVLAN IDは、サブドメインを別のサブドメインと区別します。



プライベートVLANドメインには1つのプライマリVLANしかありません。プライベートVLANドメインの各ポートは、プライマリVLANのメンバです。プライマリVLANは、プライベートVLANドメイン全体です。

セカンダリVLANは、同じプライベートVLANドメイン内のポート間を隔離します。次の2つのタイプは、プライマリVLAN内のセカンダリVLANです。

- 隔離VLAN：隔離VLAN内のポートは、レイヤ2レベルで相互に直接通信できません。
- コミュニティVLAN：コミュニティVLAN内のポートは相互に通信できますが、他のコミュニティVLAN内のポートやレイヤ2レベルの隔離VLAN内のポートとは通信できません。

プライベートVLANドメイン内には、3つのポート指定があります。各ポート指定には、同じプライベートVLANドメイン内の他の接続されたエンドポイントと通信する1つのエンドポイントの機能を規定する、独自のルールセットがあります。次に、3つのポート名称を示します。

- 混合ポート：混合ポートは、同じプライベートVLANのすべてのポートと通信できます

- 。これらのポートは、サーバとルータを接続します。
- コミュニティ (ホスト) : コミュニティポートは、同じレイヤ2ドメインのメンバーポートのグループを定義できます。これらは、他のコミュニティおよび隔離ポートからレイヤ2で隔離されます。これらのポートはホストポートを接続します。
- 隔離ポート (ホスト) : 隔離ポートは、同じプライベートVLAN内の他の隔離ポートおよびコミュニティポートから完全にレイヤ2で隔離されています。これらのポートはホストポートを接続します。

ホストトラフィックは隔離VLANおよびコミュニティVLANに送信され、サーバおよびルータのトラフィックはプライマリVLANに送信されます。

目的

プライベートVLANは、ポート間のレイヤ2分離を提供します。つまり、ブリッジトラフィックのレベルでは、IPルーティングとは異なり、同じブロードキャストドメインを共有するポートは相互に通信できません。プライベートVLANのポートは、レイヤ2ネットワーク内の任意の場所に配置できます。つまり、同じスイッチ上に配置する必要はありません。プライベートVLANは、タグなしトラフィックまたはプライオリティタグ付きトラフィックを受信し、タグなしトラフィックを送信するように設計されています。

この記事では、スイッチでプライベートVLANを設定する方法について説明します。

注 : スwitchのWebベースのユーティリティを使用してプライベートVLANを設定するには、[ここをクリックします](#)。

該当するデバイス

- Sx300シリーズ
- Sx350シリーズ
- SG350Xシリーズ
- Sx500シリーズ
- Sx550Xシリーズ

[Software Version]

- 1.4.7.06 — Sx300、Sx500
- 2.2.8.04 — Sx350、SG350X、Sx550X

CLIを使用したスイッチでのプライベートVLAN設定

プライベートプライマリVLANの作成

ステップ1 : スwitchコンソールにログインします。デフォルトのユーザ名とパスワードはcisco/ciscoです。新しいユーザ名またはパスワードを設定している場合は、クレデンシャルを入力します。

```
User Name:cisco
Password:*****
```

注：コマンドは、スイッチの正確なモデルによって異なる場合があります。この例では、SG350XスイッチにTelnetでアクセスします。

ステップ2：スイッチの特権EXECモードから、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ3：グローバルコンフィギュレーションモードで、次のように入力してインターフェイスコンフィギュレーションコンテキストを入力します。

```
SG350X(config)#interface [vlan-id]
```

- vlan-id：設定するVLAN IDを指定します。

```
SG350X#configure
SG350X(config)#interface vlan 2
SG350X(config-if)#
```

注：この例では、VLAN 2が使用されています。

ステップ4：インターフェイス設定コンテキストで、次のように入力して、VLANインターフェイスをプライマリプライベートVLANとして設定します。

```
SG350X(config-if)#private-vlan primary
```

注：デフォルトでは、スイッチにプライベートVLANは設定されていません。

```
SG350X#configure
SG350X(config)#interface vlan 2
SG350X(config-if)#private-vlan primary
SG350X(config-if)#
```

重要：プライベートVLANの設定には、次のガイドラインに注意してください。

- VLAN内にメンバーであるプライベートVLANポートがある場合、VLANタイプを変更することはできません。
- VLANタイプは、他のプライベートVLANに関連付けられている場合は変更できません。
- VLANタイプは、VLANが削除されてもVLANのプロパティとして保持されません。

ステップ5: (オプション) VLANを通常のVLAN設定に戻すには、次のように入力します。

```
SG350X(config-if)#no private-vlan
```

ステップ6: (オプション) スイッチの特権EXECモードに戻るには、次のように入力します。

```
SG350X(config-if)#end
```

```
SG350X#configure
SG350X(config)#interface vlan 2
SG350X(config-if)#private-vlan primary
SG350X(config-if)#end
```

ステップ7: (オプション) スイッチの特権EXECモードで、次のように入力して、設定した設定をスタートアップコンフィギュレーションファイルに保存します。

```
SG350X#copy running-config startup-config
```

```
[SG350X] copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?
```

ステップ8: (オプション) Overwrite file [startup-config]..プロンプトが表示されたら、キーボードでY (はい) を押し、No (いいえ) を押します。

```
SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?Y
16-May-2017 05:45:25 %COPY-I-FILECPY: Files Copy - source URL running-config destination
URL flash://system/configuration/startup-config
16-May-2017 05:45:28 %COPY-N-TRAP: The copy operation was completed successfully
SG350X#
```

これで、CLIを使用してスイッチにプライマリVLANを正常に作成できました。

セカンダリVLANの作成

ステップ1: スイッチの特権EXECモードで、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ2: グローバルコンフィギュレーションモードで、次のように入力してインターフェイスコンフィギュレーションコンテキストを入力します。

```
SG350X(config)#interface [vlan-id]
```

```
[SG350X#configure
[SG350X(config)#interface vlan 10
SG350X(config-if)#
```

注: この例では、VLAN 10が使用されています。

ステップ3: インターフェイス設定コンテキストで、次のように入力して、VLANインターフェイスをセカンダリプライベートVLANとして設定します。

```
SG350X(config-if)#private-vlan [community | isolated]
```

次のオプションがあります。

- community:VLANをコミュニティVLANとして指定します。
- isolated:VLANを隔離VLANとして指定します。

```
SG350X#configure
SG350X(config)#interface vlan 10
SG350X(config-if)#private-vlan isolated
SG350X(config-if)#
```

注：この例では、VLAN 10が隔離VLANとして設定されています。

ステップ4: (オプション) ステップ2と3を繰り返して、プライベートVLANに追加のセカンダリVLANを設定します。

```
SG350X#configure
SG350X(config)#interface vlan 10
SG350X(config-if)#private-vlan isolated
SG350X(config-if)#exit
SG350X(config)#interface vlan 20
SG350X(config-if)#private-vlan community
SG350X(config-if)#exit
SG350X(config)#interface vlan 30
SG350X(config-if)#private-vlan community
```

注：この例では、VLAN 20とVLAN 30がコミュニティVLANとして設定されています。

ステップ5: (オプション) VLANを通常のVLAN設定に戻すには、次のように入力します。

```
SG350X(config-if)#no private-vlan
```

ステップ6: (オプション) スイッチの特権EXECモードに戻るには、次のように入力します。

```
SG350X(config-if)#end
```

```
[SG350X#configure
[SG350X(config)#interface vlan 10
[SG350X(config-if)#private-vlan isolated
[SG350X(config-if)#exit
[SG350X(config)#interface vlan 20
[SG350X(config-if)#private-vlan community
[SG350X(config-if)#exit
[SG350X(config)#interface vlan 30
[SG350X(config-if)#private-vlan community
[SG350X(config-if)#end
SG350X#
```

これで、CLIを使用してスイッチにセカンダリVLANを正常に作成できました。

セカンダリVLANをプライマリプライベートVLANに関連付ける

ステップ1：スイッチの特権EXECモードで、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ2：次のように入力して、プライマリVLANのVLANインターフェイスコンフィギュレーションコンテキストを入力します。

```
SG350X(config)#vlan [primary-vlan-id]
```

```
[SG350X#configure
[SG350X(config)#interface vlan 2
SG350X(config-if)#
```

注：この例では、プライマリVLANはVLAN 2です。

ステップ3：プライマリVLANとセカンダリVLANの関連付けを設定するには、次のように入力します。

```
SG350X(config-if)#private-vlan association [add | remove]
secondary-vlan-list
```

次のオプションがあります。

- **add secondary-vlan-list**：プライマリVLANに追加するタイプsecondaryのVLAN IDのリスト。連続しないVLAN IDは、カンマで区切り、スペースは使用しません。ハイフンを使用して、IDの範囲を指定します。これがデフォルトのアクションです。
- **remove secondary-vlan-list**：プライマリVLANから関連付けを削除するタイプsecondaryのVLAN IDのリスト。連続しないVLAN IDは、カンマで区切り、スペースは使用しません。ハイフンを使用して、IDの範囲を指定します。

```
SG350X#configure
SG350X(config)#interface vlan 2
SG350X(config-if)#private-vlan association add 10,20,30
SG350X(config-if)#
```

注：この例では、セカンダリVLAN 10、20、および30がプライマリVLANに追加されています。

ステップ4：スイッチの特権EXECモードに戻るには、次のように入力します。

```
SG350X(config-if)#end
```

```
SG350X#configure
SG350X(config)#interface vlan 2
SG350X(config-if)#private-vlan association add 10,20,30
SG350X(config-if)#end
SG350X#
```

これで、CLIを使用して、セカンダリVLANをスイッチのプライマリプライベートVLANに正しく関連付けることができました。

プライマリおよびセカンダリプライベートVLANへのポートの設定

ステップ1：スイッチの特権EXECモードで、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ2：グローバルコンフィギュレーションモードで、次のように入力してインターフェイスコンフィギュレーションコンテキストを入力します。

```
SG350X(config)#interface [interface-id | range vlan vlan-range]
```

次のオプションがあります。

- interface-id：設定するインターフェイスIDを指定します。
- range vlan vlan-range:VLANのリストを指定します。カンマとスペースを使用せずに、連続しないVLANを区切ります。ハイフン(-)を使用して、VLANの範囲を指定します。

```
SG350X#configure
SG350X(config)#interface ge1/0/10
```

注：この例では、インターフェイスge1/0/10が入力されています。

ステップ3：インターフェイス設定コンテキストでswitchport modeコマンドを使用して、VLANメンバーシップモードを設定します。

```
SG350X(config-if-range)#switchport mode private-vlan  
[promiscuous | host]
```

- promiscuous : プライベートVLAN混合モードポートを指定します。このオプションを使用する場合は、ステップ5に[進みます](#)。
- host : プライベートVLANホストポートを指定します。このオプションを使用する場合は、ステップ6に[進みます](#)。

注：この例では、ポートは混合モードとして定義されています。

```
SG350X#configure  
SG350X(config)#interface ge1/0/10  
SG350X(config-if)#switchport mode private-vlan promiscuous  
SG350X(config-if)#
```

ステップ4: (オプション) ポートまたはポート範囲をデフォルト設定に戻すには、次のように入力します。

```
SG350X(config-if-range)#no switchport mode
```

[ステップ5: プロミスキュー](#)ポートとプライベートVLANのプライマリおよびセカンダリVLANの関連付けを設定するには、次のように入力します。

```
SG350X(config-if)#switchport private-vlan mapping [primary-vlan-id] add [secondary-vlan-id]
```

次のオプションがあります。

- primary-vlan-id : プライマリVLANのVLAN IDを指定します。
- secondary-vlan-id : セカンダリVLANのVLAN IDを指定します。

注：この例では、無差別インターフェイスがプライマリVLAN 2にマッピングされ、セカンダリVLAN 30に追加されています。

```
SG350X#configure  
SG350X(config)#interface ge1/0/10  
SG350X(config-if)#switchport mode private-vlan promiscuous  
SG350X(config-if)#switchport private-vlan mapping 2 add 30  
SG350X(config-if)#
```

[ステップ6: ホス](#)トポートとプライベートVLANのプライマリおよびセカンダリVLANの関連付けを設定するには、次のように入力します。

```
SG350X(config-if)#switchport private-vlan host-association  
[primary-vlan-id] [secondary-vlan-id]
```

次のオプションがあります。

- primary-vlan-id : プライマリVLANのVLAN IDを指定します。
- secondary-vlan-id : セカンダリVLANのVLAN IDを指定します。

注：この例では、ホストインターフェイスの範囲40～45がプライマリVLAN 2にマッピングされ、セカンダリVLAN 20に追加されています。

```
SG350X(config)#interface range ae1/0/40-45
SG350X(config-if-range)#switchport mode private-vlan host
SG350X(config-if-range)#switchport private-vlan host-association 2 20
```

ステップ7：インターフェイス設定コンテキストを終了するには、次のように入力します。

```
SG350X(config-if-range)#exit
```

ステップ8: (オプション) 手順2～7を繰り返して、より多くの混合モードポートとホストポートを設定し、対応するプライマリおよびセカンダリプライベートVLANに割り当てます。

注：この例では、ホストインターフェイスの範囲36～39がプライマリVLAN 2にマッピングされ、セカンダリVLAN 10に追加されています。

```
SG350X(config)#interface range ge1/0/40-45
SG350X(config-if-range)#switchport mode private-vlan host
SG350X(config-if-range)#switchport private-vlan host-association 2 20
SG350X(config-if-range)#exit
SG350X(config)#interface range ge1/0/36-39
SG350X(config-if-range)#switchport mode private-vlan host
SG350X(config-if-range)#switchport private-vlan host-association 2 10
```

ステップ9: endコマンドを入力して、特権EXECモードに戻ります。

```
SG350X(config-if)#end
```

```
SG350X(config-if-range)#exit
SG350X(config)#interface range ge1/0/36-39
SG350X(config-if-range)#switchport mode private-vlan host
SG350X(config-if-range)#switchport private-vlan host-association 2 10
SG350X(config-if-range)#end
SG350X#
```

ステップ10: (オプション) スイッチで設定されているプライベートVLANを確認するには、次のように入力します。

```
SG350X#show vlan private-vlan tag [vlan-id]
```

```
[SG350X(config-if-range)#end
[SG350X]#show vlan private-vlan
```

Primary	Secondary	Type	Ports
2		primary	gi1/0/10
2	10	isolated	gi1/0/36-39
2	20	community	gi1/0/40-45
2	30	community	gi1/0/10

```
SG350X#
```

ステップ11: (オプション) スイッチの特権EXECモードで、次のように入力して、設定をスタートアップコンフィギュレーションファイルに保存します。

```
SG350X#copy running-config startup-config
```

```
[SG350X]copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[M] ?
```

ステップ12. (オプション) Overwrite file [startup-config]..プロンプトが表示されたら、キーボードでYを押して、Noを押します。

```
SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[M] ?Y
16-May-2017 05:45:25 %COPY-I-FILECPY: Files Copy - source URL running-config destination
URL flash://system/configuration/startup-config
16-May-2017 05:45:28 %COPY-N-TRAP: The copy operation was completed successfully
SG350X#
```

これで、CLIを使用して、ホストおよび混合モードポートと、スイッチ上のプライマリおよびセカンダリプライベートVLANとの関連付けを正しく設定できました。