VLAN サブインターフェイス

この章では、VLAN サブインターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

VLAN サブインターフェイスについて

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイスまたは EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチコンテキストモードで特に便利です。

1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN を設定できます。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。

VLAN サブインターフェイスのライセンス

モデル	ライセンス要件
Firepower 1010	Essentials ライセンス：60
Firepower 1120	Essentials ライセンス：512
Firepower 1140、1150	Essentials ライセンス：1024
Secure Firewall 1210、1220	Essentials ライセンス：1024
Secure Firewall 1230、1240、1250	Essentials ライセンス：1024
Cisco Secure Firewall 3100	Essentials ライセンス：1024
Firepower 4100	Essentials ライセンス：1024
Cisco Secure Firewall 4200	Essentials ライセンス：1024
Firepower 9300	Essentials ライセンス：1024
ASA 仮想	スループット機能： 100 Mbps：25 1 Gbps：50 2 Gbps：200 10 Gbps：1024
ISA 3000	Essentials ライセンス: 5 Security Plus ライセンス：100

（注） VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 たとえば、次のようになります。

```
interface gigabitethernet 0/0.100
  vlan 100
```

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- Firepower 1010 および Cisco Secure Firewall 1210/1220：VLAN サブインターフェイスは、スイッチポートおよび VLAN インターフェイスではサポートされていません。
- ASA モデルでは、管理インターフェイスのサブインターフェイスを設定できません。サブインターフェイスのサポートについては、管理スロット/ポート インターフェイスを参照してください。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、アクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイスまたは EtherChannel インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイスまたは EtherChannel インターフェイスを通過しないように、**nameif** コマンドを除外してください。物理インターフェイスまたは EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常どおり **amenameif** コマンドを設定できます。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- ASA は Dynamic Trunking Protocol（DTP）をサポートしていないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。一意の MAC アドレスを自動的に生成できます。MAC アドレスの自動割り当てを参照してください。

（注） MAC アドレスを手動で割り当てる場合は、予期しない動作や停止を避けるために、同じ物理インターフェイス上のすべてのサブインターフェイスに MAC アドレスを割り当てるようにしてください。

VLAN サブインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLANサブインターフェイスを物理インターフェイスまたはEtherChannelインターフェイスに追加します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 新しいサブインターフェイスを指定します。

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。

subinterface ID は、1 ～ 4294967293 の整数です。

ステップ 2 サブインターフェイスの VLAN を指定します。

vlan *vlan_id* [**secondary** *vlan_range*]

例：

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

vlan_id は、1 ～ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。

セカンダリ VLAN は、（連続する範囲について）スペース、カンマ、およびダッシュで区切ることができます。ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。

同じ VLAN を複数のサブインターフェイスに関連付けることはできません。VLAN を物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。リストからいくつかのセカンダリ VLAN を削除するには、**no** コマンドを使用して削除する VLAN のみをリストすることができます。リストされた VLAN のみを選択的に削除できます。たとえば、範囲内の 1 つの VLAN を削除することはできません。

例

次に、一連のセカンダリ VLAN を VLAN 200 にマップする例を示します。

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

次に、リストからセカンダリ VLAN 503 を削除する例を示します。

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
 no ip address
```

関連トピック

VLAN サブインターフェイスのライセンス （2 ページ）

VLAN サブインターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show vlan mapping**

  マップされるインターフェイス、セカンダリ VLAN およびプライマリ VLAN を表示します。

VLAN のサブインターフェイスの例

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

次に、Catalyst 6500 でどのように VLAN マッピングが機能するのかを示します。ノードを PVLANS に接続する方法については、Catalyst 6500 の設定ガイドを参照してください。

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
```

```
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

VLAN サブインターフェイスの履歴

表 *1 : VLAN* サブインターフェイスの履歴

機能名	バージョン	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。

機能名	バージョン	機能情報
セカンダリ VLAN のプライマリ VLAN へのマッピングのサポート	9.5(2)	サブ インターフェイスで、1 つ以上のセカンダリ VLAN を設定できるようになりました。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。 次のコマンドを導入または変更しました。**vlan secondary**、**show vlan mapping**
ISA 3000 の VLAN 数の増加	9.13(1)	Security Plus ライセンスが有効な ISA 3000 について、最大 VLAN 数が 25 から 100 に増えました。

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。