



# アクセスインターフェイスとトランクインターフェイスの設定

---

この章の内容は、次のとおりです。

- [アクセスインターフェイスとトランク インターフェイスについて, 1 ページ](#)
- [アクセスインターフェイスとトランク インターフェイスの設定, 5 ページ](#)
- [インターフェイスの設定の確認, 11 ページ](#)

## アクセスインターフェイスとトランクインターフェイスについて

### アクセス インターフェイスとトランク インターフェイスの概要

イーサネット インターフェイスは、次のように、アクセス ポートまたはトランク ポートとして設定できます。

- アクセスポートはインターフェイス上に設定された1つのVLANだけに対応し、1つのVLANのトラフィックだけを伝送します。
- トランクポートはインターフェイス上に設定された2つ以上のVLANに対応しているため、複数のVLANのトラフィックを同時に伝送できます。



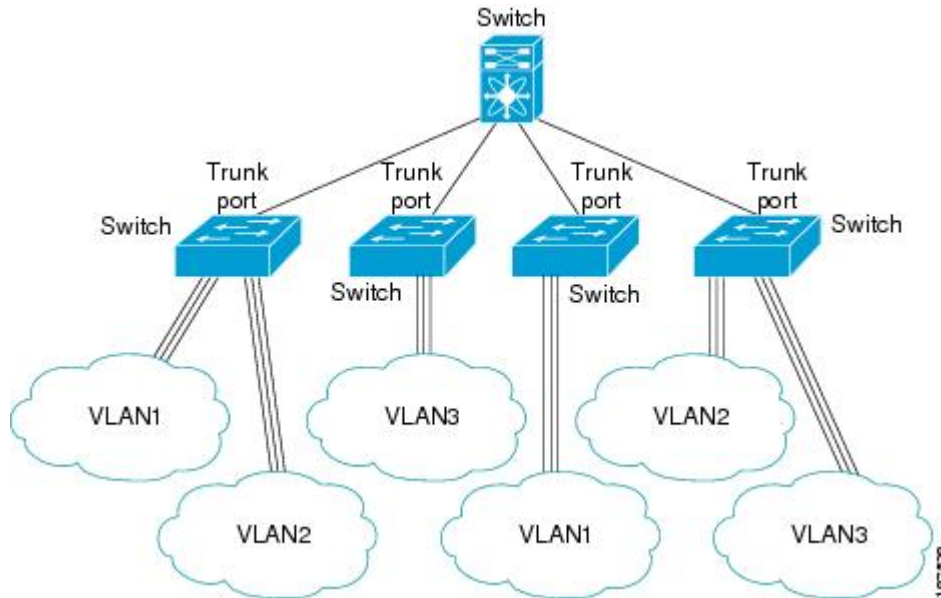
---

(注) Cisco NX-OS では、IEEE 802.1Q タイプの VLAN トランク カプセル化だけをサポートしています。

---

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2つ以上の VLAN のトラフィックを伝送します。

図 1: トランキング環境におけるデバイス



複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化（タギング）方式が使用されます。

アクセスポートでのパフォーマンスを最適化するには、そのポートをホストポートとして設定します。ホストポートとして設定されたポートは、自動的にアクセスポートとして設定され、チャンネルグループ化はディセーブルになります。ホストポートを使用すると、指定ポートがパケットの転送を開始するための所要時間を短縮できます。



(注) ホストポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセスポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。



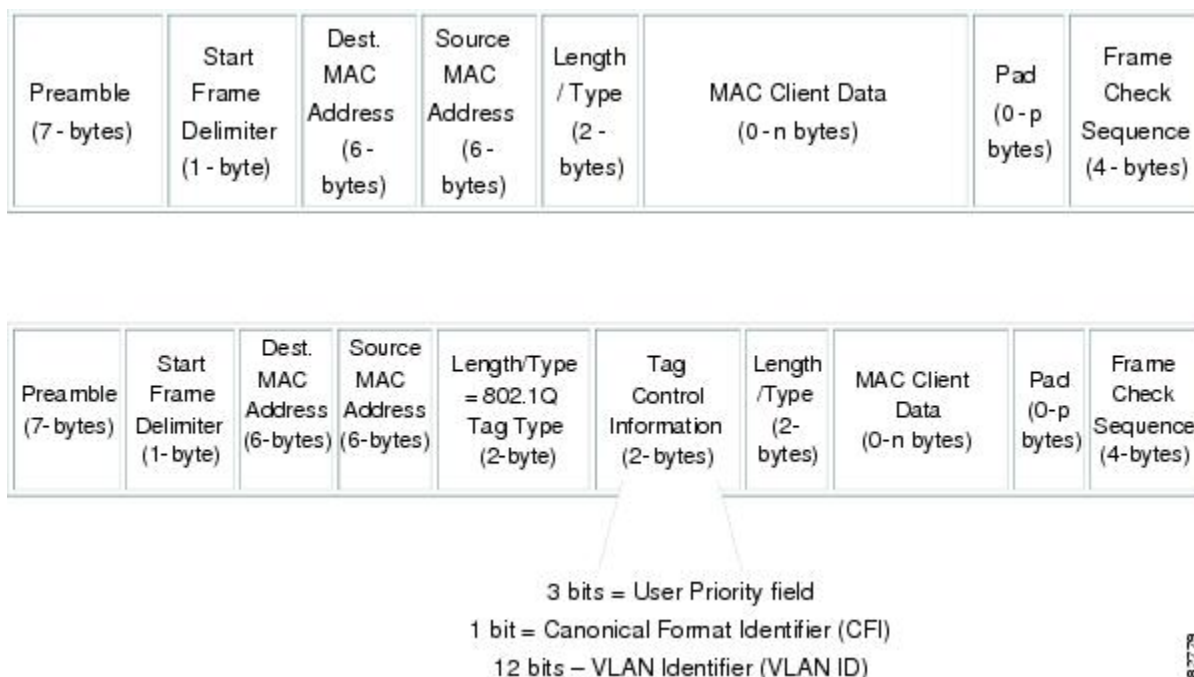
(注) イーサネット インターフェイスはアクセスポートまたはトランクポートとして動作できますが、両方のポートタイプとして同時に動作することはできません。

## IEEE 802.1Q カプセル化の概要

トランクは、デバイスと他のネットワーク デバイス間のポイントツーポイントリンクです。トランクは1つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

複数の VLAN に対応するトランク ポートでトラフィックが正しく送信されるようにするため、デバイスでは IEEE 802.1Q カプセル化 (タグging) 方式が使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、VLAN タグのカプセル化を使用すると、同じ VLAN 上のネットワークを経由するエンドツーエンドでトラフィックを転送できます。

図 2: 802.1Q タグが含まれているヘッダーと含まれていないヘッダー



162798

## アクセス VLAN の概要

アクセスモードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセスモードのポート (アクセスポート) 用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN (VLAN1) のトラフィックだけを伝送します。

VLAN のアクセスポートメンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセスポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセスポート上のアクセス VLAN を、まだ作成されていない VLAN に変更すると、システムはそのアクセスポートをシャットダウンします。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。



- (注) アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートが、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信するようになります。

## トランク ポートのネイティブ VLAN ID の概要

トランク ポートは、タグなしのパケットと 802.1Q タグ付きのパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。ネイティブ VLAN ID とは、トランク ポート上でタグなしトラフィックを伝送する VLAN のことです。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされません。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。



- (注) ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

## 許可 VLAN の概要

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。トランク経由でトラフィックを伝送したい VLAN を後でリストに戻すこともできます。

デフォルト VLAN の Spanning Tree Protocol (STP; スパニング ツリー プロトコル) トポロジを分割するには、許可 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1 (デフォルトでは、すべてのポートでイネーブル) が非常に大きな STP トポロジを形成し、STP の収束中に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

## ネイティブ 802.1Q VLAN の概要

802.1Q トランク ポートを通過するトラフィックのセキュリティを高めるため、`vlan dot1q tag native` コマンドが導入されました。この機能により、802.1Q トランク ポートから送信されるすべての

パケットが必ずタグ付けされるとともに、タグなしのパケットが 802.1Q トランク ポートで受信されないようにすることができるようになりました。

この機能がない場合、802.1Q トランク ポートで受信されたタグ付き入力フレームは、許可 VLAN のリストに含まれる限り受信が許可され、それらのタグは維持されます。タグなしフレームについては、トランク ポートのネイティブ VLAN ID でタグ付けされたうえで、それ以降の処理が行われます。出力フレームは、その VLAN タグが 802.1Q トランク ポートで許可される範囲内に属する場合に限って受信されます。フレームの VLAN タグが、トランク ポートのネイティブ VLAN のタグと一致した場合、その VLAN タグは取り除かれ、フレームはタグなしで送信されます。

この動作は、ハッカーがフレームを別の VLAN へジャンプさせる「VLAN ホッピング」に利用される可能性があります。また、タグなしパケットを 802.1Q トランク ポートへ送信することにより、トラフィックをネイティブ VLAN の一部にすることもできます。

こうした問題を解決するため、`vlan dot1q tag native` コマンドでは次のような機能を実行できるようになっています。

- 入力側では、タグなしのデータ トラフィックをすべてドロップする。
- 出力側では、すべてのトラフィックをタグ付ける。ネイティブ VLAN に属するトラフィックは、ネイティブ VLAN ID でタグ付けされます。

この機能は、直接接続されている Cisco Nexus 3000 シリーズ スイッチのすべてのイーサネット インターフェイスおよび EtherChannel インターフェイスでサポートされています。



(注) `vlan dot1q tag native` コマンドは、グローバル コンフィギュレーション モードで発行することによりイネーブルにすることができます。

## アクセスインターフェイスとトランクインターフェイスの設定

### イーサネット アクセス ポートとしての LAN インターフェイスの設定

イーサネット インターフェイスはアクセス ポートとして設定できます。アクセス ポートは、パケットを、1つのタグなし VLAN 上だけで送信します。管理者は、そのインターフェイスで伝送する VLAN トラフィックを指定します。アクセス ポートの VLAN を指定しないと、そのインターフェイスは、デフォルト VLAN だけのトラフィックを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセスポートをシャットダウンします。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {{*type slot/port*} | {**port-channel number**}}
3. switch(config-if)# **switchport mode** {**access** | **trunk**}
4. switch(config-if)# **switchport access vlan** *vlan-id*

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>interface</b> {{ <i>type slot/port</i> }   { <b>port-channel number</b> }}	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport mode</b> { <b>access</b>   <b>trunk</b> }	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。アクセスポートは、1つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセスポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセスポートを設定するには、 <b>switchport access vlan</b> コマンドを使用します。
ステップ 4	switch(config-if)# <b>switchport access vlan</b> <i>vlan-id</i>	このアクセスポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセスポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセスポートがトラフィックを伝送する VLAN を変更できます。

次に、指定された VLAN のみのトラフィックを送受信するイーサネット アクセスポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

## アクセス ホスト ポートの設定

スイッチポートホストを使用することにより、アクセスポートをスパンニングツリーエッジポートにすることが可能であり、BPDU フィルタリングおよび BPDU ガードを同時にイネーブルにすることができます。

## はじめる前に

設定を行うインターフェイスが適切であることを確認します。対象となるインターフェイスは、エンドステーションに接続されている必要があります。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **switchport host**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>interface type slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport host</b>	インターフェイスをスパニングツリー ポートタイプ エッジに設定し、BPDU フィルタリングおよび BPDU ガードをオンにします。  (注) このコマンドは、ホストに接続されたスイッチポートに対してのみ使用してください。

次に、EtherChannel がディセーブルにされたイーサネット アクセス ホスト ポートとしてインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

## トランク ポートの設定

イーサネット ポートをトランク ポートとして設定できます。トランク ポートは、ネイティブ VLAN のタグなしパケット、および複数の VLAN のカプセル化されたタグ付きパケットを伝送します



(注) Cisco NX-OS は、IEEE 802.1Q カプセル化だけをサポートしています。

トランク ポートを設定する手順は、次のとおりです。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface {type slot/port | port-channel number}**
3. switch(config-if)# **switchport mode {access | trunk}**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>interface</b> { <i>type slot/port</i>   <b>port-channel number</b> }	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport mode</b> { <b>access</b>   <b>trunk</b> }	インターフェイスをイーサネット トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、 <b>switchport trunk allowed vlan</b> コマンドを使用します。

次の例は、インターフェイスをイーサネットトランクポートとして設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport mode trunk
```

## 802.1Q トランク ポートのネイティブ VLAN の設定

このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {*type slot/port* | **port-channel number**}
3. switch(config-if)# **switchport trunk native vlan vlan-id**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>interface</b> { <i>type slot/port</i>   <b>port-channel number</b> }	設定するインターフェイスを指定し、インターフェイス 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
ステップ 3	switch(config-if)# <b>switchport trunk native vlan <i>vlan-id</i></b>	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ~ 4094 です（ただし、内部使用に予約されている VLAN は除きます）。デフォルト値は VLAN 1 です。

次の例は、イーサネット トランク ポートに対してネイティブ VALN を設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk native vlan 5
```

## トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface {*type slot/port* | **port-channel number**}**
3. switch(config-if)# **switchport trunk allowed vlan {*vlan-list all* | **none** [**add** | **except** | **none** | **remove** {*vlan-list*}]}**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>interface {<i>type slot/port</i>   <b>port-channel number</b>}</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport trunk allowed vlan {<i>vlan-list all</i>   <b>none</b> [<b>add</b>   <b>except</b>   <b>none</b>   <b>remove</b> {<i>vlan-list</i>}]}</b>	トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。

	コマンドまたはアクション	目的
		(注) 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとすると、メッセージが返されます。

次の例は、イーサネット トランク ポートの許可 VLAN のリストにいくつかの VLAN を追加する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk allow vlan 15-20
```

## ネイティブ 802.1Q VLAN の設定

通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタギングが取り除かれます。この設定によって、タグなしトラフィックおよび制御トラフィックは Cisco Nexus 3000 シリーズ スイッチを通過することができます。ネイティブ VLAN ID の値と一致する 802.1Q タグを持つ、スイッチに着信するパケットも、同様にタギングが取り除かれます。

ネイティブ VLAN でのタギングを維持し、タグなしトラフィックをドロップする場合は、**vlan dot1q tag native** コマンドを入力します。スイッチによって、ネイティブ VLAN で受信したトラフィックがタグ付けされ、802.1Q タグが付けられたフレームのみが許可され、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックはドロップされます。

**vlan dot1q tag native** コマンドがイネーブルになっていても、トランク ポートのネイティブ VLAN のタグなし制御トラフィックは引き続き許可されます。



(注) **vlan dot1q tag native** コマンドはグローバル ベースでイネーブルになります。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan dot1q tag native**
3. (任意) switch(config)# **no vlan dot1q tag native**
4. (任意) switch# **show vlan dot1q tag native**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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	switch(config)# <b>vlan dot1q tag native</b>	Cisco Nexus 3000 シリーズ スイッチ上の全トランキング ポートを対象に、そのネイティブ VLAN すべてに対して dot1q (IEEE 802.1Q) タギングをイネーブルにします。デフォルトでは、この機能はディセーブルになっています。
ステップ 3	switch(config)# <b>no vlan dot1q tag native</b>	(任意) スイッチ上の全トランキングポートを対象に、そのネイティブ VLAN すべてに対して dot1q (IEEE 802.1Q) タギングをイネーブルにします。
ステップ 4	switch# <b>show vlan dot1q tag native</b>	(任意) ネイティブ VLAN のタギングのステータスを表示します。

次の例は、スイッチ上の 802.1Q タギングをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch(config)# exit
switch# show vlan dot1q tag native
vlan dot1q native tag is enabled
```

## インターフェイスの設定の確認

アクセスインターフェイスとトランクインターフェイスの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# <b>show interface</b>	インターフェイス設定を表示します。
switch# <b>show interface switchport</b>	すべてのイーサネットインターフェイス (アクセスインターフェイスとトランクインターフェイスを含む) の情報を表示します。
switch# <b>show interface brief</b>	インターフェイス設定情報を表示します。

