NX-OSを使用したプライベートVLANの設定

この章では、Cisco NX-OS デバイスでプライベート VLAN を設定する手順について説明します。プライベート VLAN は、レイヤ 2 レベルでさらなる保護機能を提供します。

この章は、次の内容で構成されています。

Information About Private VLANs

（注） A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port.

（注） Beginning with Cisco NX-OS Release 5.0(2), the system supports private VLAN promiscuous trunk ports and isolated trunk ports. Private VLAN community ports cannot be trunk ports.

（注） You must enable the private VLAN feature before you can configure this feature.

In certain instances where similar systems do not need to interact directly, private VLANs provide additional protection at the Layer 2 level. Private VLANs are an association of primary and secondary VLANs.

A primary VLAN defines the broadcast domain with which the secondary VLANs are associated. The secondary VLANs may either be isolated VLANs or community VLANs. Hosts on isolated VLANs communicate only with associated promiscuous ports in primary VLANs, and hosts on community VLANs communicate only among themselves and with associated promiscuous ports but not with isolated ports or ports in other community VLANs.

In configurations that use integrated switching and routing functions, you can assign a single Layer 3 VLAN network interface to each private VLAN to provide routing. The VLAN network interface is created for the primary VLAN. In such configurations, all secondary VLANs communicate at Layer 3 only through a mapping with the VLAN network interface on the primary VLAN. Any VLAN network interfaces previously created on the secondary VLANs are put out-of-service.

プライベート VLAN の概要

デバイスでプライベート VLAN 機能を適用するには、プライベート VLAN をイネーブルにする必要があります。

プライベート VLAN モードで動作しているポートがデバイスに設定されている場合は、プライベート VLAN をディセーブルにすることはできません。

（注） 特定の VLAN をプライマリまたはセカンダリのどちらかのプライベート VLAN として設定するには、事前に VLAN を作成しておく必要があります。

Primary and Secondary VLANs in Private VLANs

The private VLAN feature addresses two problems that users encounter when using VLANs:

- Each VDC supports up to 4096 VLANs. If a user assigns one VLAN per customer, the number of customers that the service provider can support is limited.
- To enable IP routing, each VLAN is assigned with a subnet address space or a block of addresses, which can result in wasting the unused IP addresses and creating IP address management problems.

Using private VLANs solves the scalability problem and provides IP address management benefits and Layer 2 security for customers.

The private VLAN feature allows you to partition the Layer 2 broadcast domain of a VLAN into subdomains. A subdomain is represented by a pair of private VLANs: a primary VLAN and a secondary VLAN. A private VLAN domain can have multiple private VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another.

（注） A private VLAN domain has only one primary VLAN.

Secondary VLANs provide Layer 2 isolation between ports within the same private VLAN. The following two types are secondary VLANs within a primary VLAN:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other community VLANs or in any isolated VLANs at the Layer 2 level.

Private VLAN Ports

（注） Both community and isolated private VLAN ports are labeled as PVLAN host ports. A PVLAN host port is either a community PVLAN port or an isolated PVLAN port depending on the type of secondary VLAN with which it is associated.

The types of private VLAN ports are as follows:

- Promiscuous port—A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. You can have several promiscuous ports in a primary VLAN. Each promiscuous port can have several secondary VLANs, or no secondary VLANs, associated to that port. You can associate a secondary VLAN to more than one promiscuous port, as long as the promiscuous port and secondary VLANs are within the same primary VLAN. You may want to do this association for load balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port, but these secondary VLANs cannot communicate to the Layer 3 interface.

  Beginning with Cisco NX-OS Release 5.0(2), the primary VLAN becomes inactive after you remove all the mapped secondary VLANs to that primary VLAN.

- Promiscuous trunk—Beginning with Cisco NX-OS Release 5.0(2) and Cisco DCNM Release 5.1(1), on the Cisco Nexus 7000 Series devices, you can configure a promiscuous trunk port to carry traffic for multiple primary VLANs. You map the private VLAN primary VLAN and either all or selected associated VLANs to the promiscuous trunk port. Each primary VLAN and one associated and secondary VLAN is a private VLAN pair, and you can configure a maximum of 16 private VLAN pairs on each promiscuous trunk port.

  （注） Private VLAN promiscuous trunk ports carry traffic for normal VLANs as well as for primary private VLANs.

- Isolated port—An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete Layer 2 isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous

ports. You can have more than one isolated port in a specified isolated VLAN, and each port is completely isolated from all other ports in the isolated VLAN.

- Isolated or secondary trunk—Beginning with Cisco NX-OS Release 5.0(2) and Cisco DCNM Release 5.1(1) on the Cisco Nexus 7000 Series devices, you can configure an isolated trunk port to carry traffic for multiple isolated VLANs. Each secondary VLAN on an isolated trunk port must be associated with a different primary VLAN. You cannot put two secondary VLANs that are associated with the same primary VLAN on an isolated trunk port. Each primary VLAN and one associated secondary VLAN is a private VLAN pair, and you can configure a maximum of 16 private VLAN pairs on each isolated trunk port.

（注） Private VLAN isolated trunk ports carry traffic for normal VLANs as well as for secondary private VLANs.

- Community port—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from all isolated ports within the private VLAN domain.

（注） Because trunks can support the VLANs that carry traffic between promiscuous, isolated, and community ports, the isolated and community port traffic might enter or leave the device through a trunk interface.

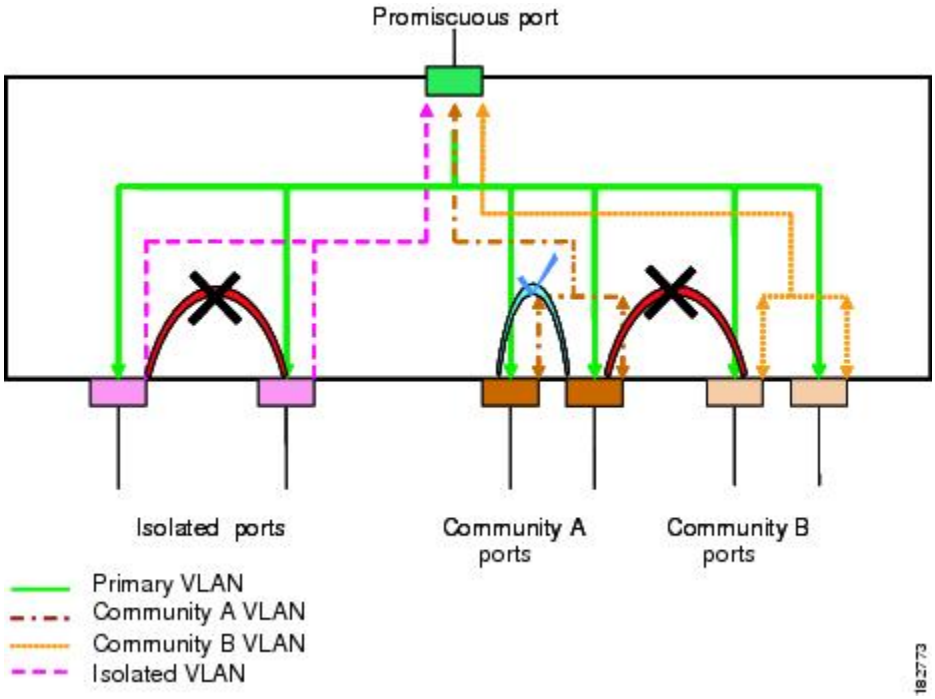
Primary, Isolated, and Community Private VLANs

Because the primary VLAN has the Layer 3 gateway, you associate secondary VLANs with the primary VLAN in order to communicate outside the private VLAN. Primary VLANs and the two types of secondary VLANs, isolated VLANs and community VLANs, have these characteristics:

- Primary VLAN— The primary VLAN carries traffic from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.
- Isolated VLAN —An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the Layer 3 gateway. You can configure multiple isolated VLANs in a private VLAN domain, and all the traffic remains isolated within each one. In addition, each isolated VLAN can have several isolated ports, and the traffic from each isolated port also remains completely separate.
- Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.

This figure shows the Layer 2 traffic flows within a primary, or private VLAN, along with the types of VLANs and types of ports.

図 *1* : ***Private VLAN Layer 2 Traffic Flows***



（注） The private VLAN traffic flows are unidirectional from the host ports to the promiscuous ports. Traffic that egresses the promiscuous port acts like the traffic in a normal VLAN, and there is no traffic separation among the associated secondary VLAN.

A promiscuous port can serve only one primary VLAN, but it can serve multiple isolated VLANs and multiple community VLANs. (Layer 3 gateways are connected to the device through a promiscuous port.) With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private VLAN servers from an administration workstation.

（注） Beginning with Cisco NX-OS Release 5.0(2) for the Nexus 7000 Series devices, you can configure private VLAN promiscuous and isolated trunk ports. These promiscuous and isolated trunk ports carry traffic for multiple primary and secondary VLANs as well as normal VLAN.

Although you can have several promiscuous ports in a primary VLAN, you can have only one Layer 3 gateway per primary VLAN.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

（注） You must enable the VLAN interface feature before you can configure the Layer 3 gateway. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』 for complete information on VLAN network interfaces and IP addressing.

プライマリ VLAN とセカンダリ VLAN のアソシエーション

セカンダリ VLAN 内のホスト ポートでプライベート VLAN 外と通信するには、セカンダリ VLAN をプライマリ VLAN に関連付ける必要があります。 関連付けが正常に動作していない場合、セカンダリ VLAN のホスト ポート（独立ポートおよびコミュニティ ポート）はダウン ステートになります。

（注） セカンダリ VLAN は、1 つのプライマリ VLAN のみにアソシエートすることができます。

アソシエーションの操作を可能にするには、次の条件を満たす必要があります。

- プライマリ VLAN が存在する。
- セカンダリ VLAN が存在する。
- プライマリ VLAN がプライマリ VLAN として設定されている。
- セカンダリ VLAN が、独立 VLAN またはコミュニティ VLAN として設定されている。

（注） アソシエーションが動作していることを確認するには、**show** コマンドの出力を調べます。 関連付けが動作していなくても、エラー メッセージは発行されません

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。 指定の VLAN をプライベート VLAN モードに再変換すると、元の関連付けが回復します。

関連付けがプライベート VLAN トランク ポートで動作していない場合、ポート全体はダウンせずに、その VLAN だけがダウンします。

no private-vlan コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN 上の関連付けはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままになります。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けられたすべてのプライベート VLAN は失われます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN のアソシエーションは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

（注） この動作は、Catalyst デバイスの動作と異なります。

セカンダリ VLAN とプライマリ VLAN の関連付けを変更するには、現在の関連付けを削除してから目的の関連付けを追加します。

Broadcast Traffic in Private VLANs

Broadcast traffic from ports in a private VLAN flows in the following ways:

- The broadcast traffic flows from all promiscuous ports to all ports in the primary VLAN. This broadcast traffic is distributed to all ports within the primary VLAN, including those ports that are not configured with private VLAN parameters.
- The broadcast traffic from all isolated ports is distributed only to those promiscuous ports in the primary VLAN that are associated to that isolated port.
- The broadcast traffic from community ports is distributed to all ports within the port's community and to all promiscuous ports that are associated to the community port. The broadcast packets are not distributed to any other communities within the primary VLAN or to any isolated ports.

Private VLAN Port Isolation

You can use private VLANs to control access to end stations as follows:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

Private VLANs and VLAN Interfaces

A VLAN interface to a Layer 2 VLAN is also called a switched virtual interface (SVI). Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs.

Configure VLAN network interfaces only for primary VLANs. Do not configure VLAN interfaces for secondary VLANs. VLAN network interfaces for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN. You will see the following actions if you misconfigure the VLAN interfaces:

- If you try to configure a VLAN with an active VLAN network interface as a secondary VLAN, the configuration is not allowed until you disable the VLAN interface.
- If you try to create and enable a VLAN network interface on a VLAN that is configured as a secondary VLAN, that VLAN interface remains disabled and the system returns an error.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLANs. For example, if you assign an IP subnet to the VLAN network interface on the primary VLAN, this subnet is the IP subnet address of the entire private VLAN.

（注） You must enable the VLAN interface feature before you configure VLAN interfaces. See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on VLAN interfaces and IP addressing.

Private VLANs Across Multiple Devices

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private VLAN configuration and to avoid other uses of the VLANs configured to be private VLANs, configure private VLANs on all intermediate devices, including devices that have no private VLAN ports.

High Availability for Private VLANs

The software supports high availability for both stateful and stateless restarts, as during a cold reboot, for private VLANs. For the stateful restarts, the software supports a maximum of three retries. If you try more than 3 times within 10 seconds of a restart, the software reloads the supervisor module.

You can upgrade or downgrade the software seamlessly, with respect to private VLANs.

Beginning with Cisco NX-OS Release 5.0(2), if you configure private VLAN promiscuous or isolated trunk ports, you must unconfigure those ports in order to downgrade the software.

（注） See the 『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』, for complete information on high-availability features.

Virtualization Support for Private VLANs

The software supports virtual device contexts (VDCs).

（注） See the 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』, for complete information on VDCs and assigning resources.

Each VLAN must have all of its private VLAN ports for both the primary VLAN and all secondary VLANs in the same VDC. Private VLANs cannot cross VDCs.

Licensing Requirements for Private VLANs

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Private VLANs require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the 『*Cisco NX-OS Licensing Guide*』.

However, using VDCs requires an Advanced Services license.

Prerequisites for Private VLANs

Private VLANs have the following prerequisites:

- You must be logged onto the device.
- If necessary, install the Advanced Services license and enter the desired VDC.
- You must enable the private VLAN feature.

Guidelines and Limitations for Configuring Private VLANs

Private VLANs have the following configuration guidelines and limitations:

- You must enable private VLANs before the device can apply the private VLAN functionality.
- You must enable the VLAN interface feature before the device can apply this functionality.
- Shut down the VLAN network interface for all VLANs that you plan to configure as secondary VLANs before you configure these VLANs.
- You cannot configure a shared interface to be part of a private VLAN. For more details, see the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』.

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring secondary or primary VLANs in private VLANs:

- You cannot configure the default VLAN (VLAN1) or any of the internally allocated VLANs as primary or secondary VLANs.
- You must use VLAN configuration (config-vlan) mode to configure private VLANs.
- A primary VLAN can have multiple isolated and community VLANs associated with it. An isolated or community VLAN can be associated with only one primary VLAN.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.

- When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN, such as bridge priorities, are propagated to the secondary VLAN. However, STP parameters do not necessarily propagate to other devices. You should manually check the STP configuration to ensure that the spanning tree topologies for the primary, isolated, and community VLANs match exactly so that the VLANs can properly share the same forwarding database.
- For normal trunk ports, note the following:
  - There is a separate instance of STP for each VLAN in the private VLAN.
  - STP parameters for the primary and all secondary VLANs must match.
  - The primary and all associated secondary VLANs should be in the same MST instance.
- For nontrunking ports, note the following:
  - STP is aware only of the primary VLAN for any private VLAN host port; STP does not run on secondary VLANs on a host port.

（注） We recommend that you enable BPDU Guard on all ports that you configure as a host port; do not enable this feature on promiscuous ports.

- For private VLAN promiscuous trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each promiscuous trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN primary VLAN. You cannot configure a private VLAN secondary VLAN as the native VLAN for a private VLAN promiscuous trunk port.
  - To downgrade a system that has private VLAN promiscuous trunk ports configured, you must unconfigure these ports.
- For private VLAN isolated trunk ports, note the following:
  - You can configure a maximum of 16 private VLAN primary and secondary VLAN pairs on each isolated trunk port.
  - The native VLAN must be either a normal VLAN or a private VLAN secondary VLAN. You cannot configure a private VLAN primary port as the native VLAN for a private VLAN isolated trunk port.
  - To downgrade a system that has private VLAN isolated trunk ports configured, you must unconfigure these ports.
- You can apply different Quality of Service (QoS) configurations to primary, isolated, and community VLANs.
- To apply a VACL to all private VLAN traffic, map the secondary VLANs on the VLAN network interface of the primary VLAN, and then configure the VACLs on the VLAN network interface of the primary VLAN.

- The VACLs that you apply to the VLAN network interface of a primary VLAN automatically apply to the associated isolated and community VLANs only after you have configured the mapping.
- If you do not map the secondary VLAN to the VLAN network interface of the primary VLAN, you can have different VACLs for primary and secondary VLANs, which can cause problems.
- Because traffic in a private VLAN flows in different directions in different VLANs, you can have different VACLs for ingressing traffic and different VACLs for egressing traffic prior to configuring the mapping.

（注） You must keep the same VACLs for the primary VLAN and all secondary VLANs in the private VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, the DHCP configuration is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- Before you configure a VLAN as a secondary VLAN, you must shut down the VLAN network interface for the secondary VLAN.
- To prevent interhost communication in isolated private VLANs with a promiscuous port, configure a role-based ACL (RBACL) that disallows hosts in that subnet from communicating with each other.

Private VLAN Port Configuration

Follow these guidelines when configuring private VLAN ports:

- Use only the private VLAN configuration commands to assign ports to primary, isolated, or community VLANs.
- The Layer 2 access ports that are assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private VLAN configuration. Layer 2 trunk interfaces, which may carry private VLANs, are active and remain part of the STP database.
- Do not configure ports that belong to a port-channel group as private VLAN ports. While a port is part of the private VLAN configuration, any port-channel configuration for it is inactive.
- If you delete a VLAN used in the private VLAN configuration, the private VLAN ports that are associated with the VLAN become inactive.

Limitations with Other Features

Consider these configuration limitations with other features when configuring private VLANs:

（注） In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- IGMP runs only on the primary VLAN and uses the configuration of the primary VLAN for all secondary VLANs.

- Any IGMP join request in the secondary VLAN is treated as if it is received in the primary VLAN.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- Private VLAN host or promiscuous ports cannot be a SPAN destination port.
- A destination SPAN port cannot be an isolated port. (However, a source SPAN port can be an isolated port.)
- You can configure SPAN to span both primary and secondary VLANs or to span either one if the user is interested only in ingress or egress traffic.
- After you configure the association between the primary and secondary VLANs, the dynamic MAC addresses that learned the secondary VLANs are flushed.
- After you configure the association between the primary and secondary VLANs, all static MAC addresses that were created on the secondary VLANs are inserted into the primary VLAN. If you delete the association, the static MAC addresses revert to the secondary VLANs only.
- After you configure the association between the primary and secondary VLANs, you cannot create static MAC addresses for the secondary VLANs.
- After you configure the association between the primary and secondary VLANs, if you delete the association, all static MAC addresses that were created on the primary VLANs remain on the primary VLAN only.
- Port security features are not supported with private VLANs.
- In private VLANs, STP controls only the primary VLAN.

（注） See the 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』 for information on configuring static MAC addresses.

プライベート VLAN のデフォルト設定

次の表に、プライベート VLAN のデフォルト設定を示します。

表 *1*：プライベート *VLAN* のデフォルト設定

パラメータ	デフォルト
プライベート VLAN	ディセーブル

Configuring a Private VLAN

You must have already created the VLAN before you can assign the specified VLAN as a private VLAN.

See the 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』, for information on assigning IP addresses to VLAN interfaces.

（注） If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

プライベート VLAN のイネーブル化（CLI バージョン）

プライベート VLAN 機能を使用するには、デバイス上でプライベート VLAN をイネーブルにする必要があります。

（注） プライベート VLAN コマンドは、プライベート VLAN 機能をイネーブルにするまで表示されません。

手順の概要

1. **config t**
2. **feature private-vlan**
3. **exit**
4. （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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**feature private-vlan**
	
	例：
	`switch(config)# feature private-vlan`
	`switch(config)#`
		デバイス上でプライベート VLAN 機能をイネーブルにします。
		（注） プライベート VLAN モードのデバイスに動作可能なポートがある場合、**no feature private-vlan** コマンドを適用できません。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、デバイス上でプライベート VLAN 機能をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature private-vlan
switch(config)#
```

プライベート VLAN としての VLAN の設定（CLI バージョン）

（注） VLAN をセカンダリ VLAN（つまり、コミュニティ VLAN または独立 VLAN のいずれか）として設定する前に、まず VLAN ネットワーク インターフェイスをシャットダウンする必要があります。

VLAN は、プライベート VLAN として設定できます。

プライベート VLAN を作成するには、最初に VLAN を作成して、その VLAN をプライベート VLAN として設定します。

プライベート VLAN 内で、プライマリ VLAN、コミュニティ VLAN、または独立 VLAN として使用するすべての VLAN を作成します。 そのあとで、複数の独立 VLAN および複数のコミュニティ VLAN を 1 つのプライマリ VLAN に関連付けます。 複数のプライマリ VLAN と関連付けを設定できます。つまり、複数のプライベート VLAN を設定できます。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

プライベート VLAN トラック ポート上でセカンダリ VLAN またはプライマリ VLAN のいずれかを削除した場合、その特定の VLAN だけが非アクティブになり、トランク ポートはアップしたままです。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show vlan private-vlan** [*type*]
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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** {*vlan-id*	*vlan-range*}
		
		例：
		`switch(config)# vlan 5`
		`switch(config-vlan)#`
			VLAN 設定サブモードにします。

ステップ 3	次のいずれかのコマンドを入力します。	

オプション	説明
private-vlan {**community** | **isolated** | **primary**}	VLAN を、コミュニティ VLAN、独立 VLAN、またはプライマリ プライベート VLAN として設定します。 プライベート VLAN には、1 つのプライマリ VLAN を設定する必要があります。 複数のコミュニティ VLAN と独立 VLAN を設定することができます。
no private-vlan {**community** | **isolated** | **primary**}	指定した VLAN からプライベート VLAN の設定を削除し、通常の VLAN モードに戻します。 プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

	コマンドまたはアクション	目的
	例： `switch(config-vlan)# private-vlan primary`	

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション サブモードを終了します。

ステップ 5	**show vlan private-vlan** [*type*] 例： `switch# show vlan private-vlan`	（任意） プライベート VLAN の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次の例は、VLAN 5 をプライマリ VLAN としてプライベート VLAN に割り当てる方法を示しています。

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)#
```

セカンダリ VLAN とプライマリ プライベート VLAN の関連付け（CLI バージョン）

セカンダリ VLAN をプライマリ VLAN に関連付けるときは、次の注意事項に従ってください。

- *secondary-vlan-list* パラメータには、スペースを含めないでください。 カンマで区切った複数の項目を含めることができます。 各項目は、単一のセカンダリ VLAN ID、またはセカンダリ VLAN ID をハイフンでつないだ範囲にできます。
- *secondary-vlan-list* パラメータには、複数のコミュニティ VLAN ID と独立 VLAN ID を含めることができます。
- セカンダリ VLAN をプライマリ VLAN にアソシエートするには、*secondary-vlan-list* と入力するか、*secondary-vlan-list* に **add** キーワードを入力します。
- セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアするには、*secondary-vlan-list* に **remove** キーワードを入力します。

- セカンダリ VLAN とプライマリ VLAN とのアソシエーションを変更するには、既存のアソシエーションを削除し、次に必要なアソシエーションを追加します。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

no private-vlan コマンドを入力すると、VLAN は通常の VLAN モードに戻ります。 その VLAN 上の関連付けはすべて一時停止されますが、インターフェイスはプライベート VLAN モードのままになります。

指定の VLAN をプライベート VLAN モードに再変換すると、元の関連付けが回復します。

プライマリ VLAN に対して **no vlan** コマンドを入力すると、その VLAN に関連付けされたすべてのプライベート VLAN は失われます。 ただし、セカンダリ VLAN に対して **no vlan** コマンドを入力した場合、その VLAN とプライベート VLAN の関連付けは一時停止します。この VLAN を再作成して以前のセカンダリ VLAN として設定すると元に戻ります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **vlan** *primary-vlan-id*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show vlan private-vlan** [**type**]
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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**vlan** *primary-vlan-id*
	
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		プライベート VLAN の設定作業を行うプライマリ VLAN の番号を入力します。

ステップ 3	次のいずれかのコマンドを入力します。	

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td>
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>private-vlan association {[add] secondary-vlan-list | remove secondary-vlan-list}</td><td>セカンダリ VLAN をプライマリ VLANに関連付けます。</td></tr>
<tr><td>no private-vlan association</td><td>プライマリ VLAN からすべてのアソシエーションを削除し、通常の VLAN モードに戻します。</td></tr>
</table>
例：
<code>switch(config-vlan)# private-vlan association 100-105,109</code></td><td></td></tr>
<tr><td>ステップ 4</td><td>exit
例：
<code>switch(config-vlan)# exit
switch(config)#</code></td><td>VLAN コンフィギュレーション サブモードを終了します。</td></tr>
<tr><td>ステップ 5</td><td>show vlan private-vlan [type]
例：
<code>switch# show vlan private-vlan</code></td><td>（任意）
プライベートVLANの設定を表示します。</td></tr>
<tr><td>ステップ 6</td><td>copy running-config startup-config
例：
<code>switch(config)# copy running-config startup-config</code></td><td>（任意）
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。</td></tr>
</table>

次に、コミュニティ VLAN 100 ～ 105 および独立 VLAN 109 をプライマリ VLAN 5 に関連付ける例を示します。

```
switch(config)# vlan 5
switch(config-vlan)# private-vlan association 100-105, 109
switch(config-vlan)# exit
switch(config)#
```

プライマリ VLAN の VLAN インターフェイスへのセカンダリ VLAN のマッピング（CLI バージョン）

（注） プライベート VLAN 内のプライマリ VLAN の VLAN インターフェイスへの IP アドレスの割り当てについては、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』を参照してください。

セカンダリ VLAN を、プライマリ VLAN の VLAN インターフェイスにマッピングします。 独立 VLAN およびコミュニティ VLAN は、ともにセカンダリ VLAN と呼ばれます。 プライベート VLAN の入力トラフィックをレイヤ 3 で処理するには、セカンダリ VLAN をプライマリ VLAN の VLAN ネットワーク インターフェイスにマッピングします。

（注） VLAN ネットワーク インターフェイスを設定する前に、VLAN ネットワーク インターフェイスをイネーブルにする必要があります。 プライマリ VLAN に関連付けられたコミュニティ VLAN または独立 VLAN 上の VLAN ネットワーク インターフェイスは、アウト オブ サービスになります。 稼働するのは、プライマリ VLAN 上の VLAN ネットワーク インターフェイスだけです。

はじめる前に

- プライベート VLAN 機能をイネーブルにする。
- VLAN インターフェイス機能をイネーブルにする。
- 正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。
- セカンダリ VLAN のマッピング先となる正しいプライマリ VLAN レイヤ 3 インターフェイスで作業をしていること。

手順の概要

1. **config t**
2. **interface vlan** *primary-vlan-ID*
3. 次のいずれかのコマンドを入力します。
4. **exit**
5. （任意） **show interface vlan** *primary-vlan-id* **private-vlan mapping**
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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**interface vlan** *primary-vlan-ID*
	
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		プライベート VLAN の設定作業を行うプライマリ VLAN の番号を入力します。 プライマリ VLAN のインターフェイス コンフィギュレーション モードが開始されます。

ステップ 3	次のいずれかのコマンドを入力します。 **private-vlan mapping** {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}：セカンダリ VLAN を、プライマリ VLAN の SVI またはレイヤ 3 インターフェイスにマッピングします。 これにより、プライベート VLAN 入力トラフィックのレイヤ 3 スイッチングが可能になります。 **no private-vlan mapping**：セカンダリ VLAN とプライマリ VLAN 間のレイヤ 3 インターフェイスへのマッピングを消去します。 例： `switch(config-if)# private-vlan mapping 100-105, 109`	

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show interface vlan** *primary-vlan-id* **private-vlan mapping** 例： `switch(config)# show interface vlan 101 private-vlan mapping`	（任意） インターフェイスのプライベート VLAN 情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、セカンダリ VLAN 100 ～ 105 および 109 を、プライマリ VLAN 5 のレイヤ 3 インターフェイスにマッピングする例を示します。

```
switch #config t
switch(config)# interface vlan 5
switch(config-if)# private-vlan mapping 100-105, 109
switch(config-if)# exit
switch(config)#
```

プライベート VLAN ホスト ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN のホスト ポートとして設定できます。 プライベート VLAN では、ホスト ポートがセカンダリ VLAN の一部です。セカンダリ VLAN は、コミュニティ VLAN または独立 VLAN のいずれかです。

（注） ホスト ポートとして設定されているすべてのインターフェイスで、BPDU ガードをイネーブルにすることを推奨します。

次に、ホスト ポートを、プライマリ VLAN とセカンダリ VLAN の両方にアソシエートします。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **interface** *type slot/port*
3. **switchport mode private-vlan host**
4. 次のいずれかのコマンドを入力します。
5. **exit**
6. （任意） **show interface switchport**
7. （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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**interface** *type slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN ホスト ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport mode private-vlan host**
	
	例：
	`switch(config-if)# switchport mode private-vlan host`
	`switch(config-if)#`
		レイヤ 2 ポートをプライベート VLAN のホスト ポートとして設定します。

ステップ 4	次のいずれかのコマンドを入力します。	

オプション	説明
switchport private-vlan host-association {*primary-vlan-id*} {*secondary-vlan-id*}	レイヤ 2 ホスト ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。 セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
no switchport private-vlan host-association	プライベート VLAN のアソシエーションをポートから削除します。

	コマンドまたはアクション	目的
	例： `switch(config-if)# switchport private-vlan host-association 10 50`	

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、レイヤ 2 ポート 2/1 をプライベート VLAN のホスト ポートとして設定し、プライマリ VLAN 10 およびセカンダリ VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan host
switch(config-if)# switchport private-vlan host-association 10 50
switch(config-if)# exit
switch(config)#
```

プライベートVLAN独立トランクポートとしてのレイヤ2インターフェイスの設定

Cisco NX-OS Release 5.0(2) から、レイヤ 2 インターフェイスをプライベート VLAN 独立トランク ポートとして設定できるようになりました。これらの独立トランク ポートは、複数のセカンダリ VLAN と通常の VLAN のトラフィックを伝送します。

（注） プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 独立トランク ポート上で動作可能になる前に関連付ける必要があります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk secondary**
5. （任意） **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. 次のいずれかのコマンドを入力します。
8. **exit**
9. （任意） **show interface switchport**
10. （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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**interface** {*type slot/port*}
	
	例：
	`switch(config)# interface ethernet 2/11`
	`switch(config-if)#`
		プライベート VLAN 独立トランク ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport**
	
	例：
	`switch(config-if)# switchport`
	`switch(config-if)#`
		レイヤ 2 ポートをスイッチ ポートとして設定します。

ステップ 4	**switchport mode private-vlan trunk secondary**
	
	例：
	`switch(config-if)# switchport mode private-vlan trunk secondary`
	`switch(config-if)#`
		レイヤ2ポートを、複数の独立VLANのトラフィックを伝送する独立トランク ポートとして設定します。
		（注） コミュニティ VLAN は独立トランク ポートにはできません。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	（任意） 802.1Q トランクのネイティブ VLAN を設定します。有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。デフォルト値は 1 です。 （注） プライベート VLAN を独立トランク ポートのネイティブ VLAN として使用している場合は、セカンダリ VLAN または標準 VLAN の値を入力する必要があります。プライマリ VLAN をネイティブ VLAN として設定することはできません。

ステップ 6	**switchport private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	
	例：
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		プライベート VLAN 独立トランク インターフェイスの許容 VLAN を設定します。 有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。
		プライベート プライマリ VLAN およびセカンダリ VLAN を独立トランク ポートにマッピングすると、すべてのプライマリ VLAN がこのポートの許可される VLAN リストに自動的に追加されます。
		（注） ネイティブ VLAN が許可される VLAN リストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上の VLAN が許可されないため、ネイティブ VLAN トラフィックを通過させるには、ネイティブ VLAN を許可される VLAN として設定する必要があります（関連する VLAN として追加済みでない場合）。

ステップ 7	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的

オプション	説明
switchport private-vlan association trunk {*primary-vlan-id*} {*secondary-vlan-id*}	レイヤ 2 独立トランク ポートを、プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN に関連付けます。セカンダリ VLAN は独立 VLAN である必要があります。 各独立トランク ポートに対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアを関連付けられます。 作業中のプライマリ VLAN とセカンダリ VLAN のペアごとに、コマンドを再入力する必要があります。 （注） 独立トランク ポートの各セカンダリ VLAN は、別々のプライマリ VLAN に関連付ける必要があります。 同じプライマリ VLAN に関連付けられた 2 つの独立 VLAN を、プライベート VLAN 独立トランク ポートに接続することはできません。 これを行った場合、最新のエントリが前のエントリを上書きします。
no switchport private-vlan association trunk [*primary-vlan-id* [*secondary-vlan-id*]]	プライベート VLAN 独立トランク ポートからプライベート VLAN の関連付けを削除します。

例：

```
switch(config-if)# switchport private-vlan
association trunk 10 101
switch(config-if)#
```

	コマンドまたはアクション	目的

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、レイヤ 2 ポート 2/1 を、3 つの異なるプライマリ VLAN と関連セカンダリ VLAN に関連付けられたプライベート VLAN 独立トランク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan trunk
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan association trunk 10 101
switch(config-if)# switchport private-vlan association trunk 20 201
switch(config-if)# switchport private-vlan association trunk 30 102
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 無差別ポートとしてのレイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスをプライベート VLAN の無差別ポートとして設定し、その無差別ポートをプライマリ VLAN およびセカンダリ VLAN に関連付けることができます。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport mode private-vlan promiscuous**
4. 次のいずれかのコマンドを入力します。
5. **exit**
6. （任意） **show interface switchport**
7. （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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**interface** {*type slot/port*}
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN 無差別ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport mode private-vlan promiscuous** 例： `switch(config-if)# switchport mode private-vlan promiscuous`	レイヤ 2 ポートをプライベート VLAN の無差別ポートとして設定します。
ステップ 4	次のいずれかのコマンドを入力します。	

オプション	説明
switchport private-vlan mapping {*primary-vlan-id*} {*secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list*}	レイヤ 2 ポートを無差別ポートとして設定し、このポートをプライマリ VLAN および選択したセカンダリ VLAN のリストに関連付けます。セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。
no switchport private-vlan mapping	プライベート VLAN から、マッピングをクリアします。

	コマンドまたはアクション	目的
	例： `switch(config-if)# switchport private-vlan mapping 10 50`	

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、レイヤ 2 ポート 2/1 を無差別ポートとして設定し、プライマリ VLAN 10 とセカンダリ独立 VLAN 50 に関連付ける例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# switchport private-vlan mapping 10 50
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 無差別トランク ポートとしてのレイヤ 2 インターフェイスの設定

Cisco NX-OS Release 5.0(2) から、レイヤ 2 インターフェイスをプライベート VLAN 無差別トランク ポートとして設定し、その無差別トランク ポートを複数のプライマリ VLAN に関連付けることができるようになりました。 これらの無差別トランク ポートは、複数のプライマリ VLAN と通常の VLAN のトラフィックを伝送します。

（注） プライマリ VLAN とセカンダリ VLAN は、プライベート VLAN 無差別トランク ポート上で動作可能になる前に関連付ける必要があります。

はじめる前に

プライベート VLAN 機能がイネーブルであることを確認してください。

正しい VDC を開始していること（または **switchto vdc** コマンドを入力済みであること）を確認してください。 VDC が異なっていても同じ VLAN 名と ID を使用できるので、正しい VDC で作業していることを確認する必要があります。

手順の概要

1. **config t**
2. **interface** {*type slot/port*}
3. **switchport**
4. **switchport mode private-vlan trunk promiscuous**
5. （任意） **switchport private-vlan trunk native vlan** *vlan-id*
6. **switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
7. 次のいずれかのコマンドを入力します。
8. **exit**
9. （任意） **show interface switchport**
10. （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	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**interface** {*type slot/port*}
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		プライベート VLAN 無差別トランク ポートとして設定するレイヤ 2 ポートを選択します。

ステップ 3	**switchport**
	
	例：
	`switch(config-if)# switchport`
	`switch(config-if)#`
		レイヤ 2 ポートをスイッチ ポートとして設定します。

ステップ 4	**switchport mode private-vlan trunk promiscuous**
	
	例：
	`switch(config-if)# switchport mode private-vlan trunk promiscuous`
	`switch(config-if)#`
		レイヤ 2 ポートを、複数のプライベート VLAN と通常の VLAN のトラフィックを伝送するための無差別トランク ポートして設定します。

	コマンドまたはアクション	目的
ステップ 5	**switchport private-vlan trunk native vlan** *vlan-id* 例： `switch(config-if)# switchport private-vlan trunk native vlan 5`	（任意） 802.1Q トランクのネイティブ VLAN を設定します。有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。デフォルト値は 1 です。 （注） プライベート VLAN を無差別トランク ポートのネイティブ VLAN として使用している場合は、プライマリ VLAN または標準 VLAN の値を入力する必要があります。セカンダリ VLAN をネイティブ VLAN として設定することはできません。

ステップ 6	**switchport mode private-vlan trunk allowed vlan** {**add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
	
	例：
	`switch(config-if)# switchport private-vlan trunk allowed vlan add 1`
	`switch(config-if)#`
		プライベート VLAN 無差別トランク インターフェイスの許可 VLAN を設定します。 有効値の範囲は 1 ～ 3968 および 4048 ～ 4093 です。
		プライベート プライマリ VLAN およびセカンダリ VLAN を無差別トランク ポートにマッピングすると、すべてのプライマリ VLAN がこのポートの許可される VLAN リストに自動的に追加されます。
		（注） ネイティブ VLAN が許可される VLAN リストに含まれていることを確認します。このコマンドでは、デフォルトでこのインターフェイス上の VLAN が許可されないため、ネイティブ VLAN トラフィックを通過させるには、ネイティブ VLAN を許可される VLAN として設定する必要があります（関連する VLAN として追加済みでない場合）。

ステップ 7	次のいずれかのコマンドを入力します。	

	コマンドまたはアクション	目的
	オプション / 説明	
	switchport private-vlan mapping trunk *primary-vlan-id* {**add** *secondary-vlan-list* | **remove** *secondary-vlan-id*} — 無差別トランク ポートと、プライマリ VLAN および選択した関連するセカンダリ VLAN のリストをマッピングするかマッピングを削除します。 セカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN のいずれかとして設定できます。 トラフィックを通過させるには、プライマリ VLAN とセカンダリ VLAN の間のプライベート VLAN の関連付けが動作する必要があります。 各無差別トランク ポートに対し、最大 16 個のプライベート VLAN のプライマリとセカンダリのペアをマッピングできます。 作業しているプライマリ VLAN それぞれに対してコマンドを再入力する必要があります。	
	no switchport private-vlan mapping trunk [*primary-vlan-id* [*secondary-vlan-id*]] — インターフェイスからプライベート VLAN 無差別トランクマッピングを削除します。	

	例：
	`switch(config-if)# switchport private-vlan mapping trunk 4 add 5`
	`switch(config-if)#`	

ステップ 8	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show interface switchport** 例： `switch# show interface switchport`	（任意） スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、レイヤ 2 ポート 2/1 を、2 つのプライマリ VLAN とそれに関連するセカンダリ VLAN に関連付けられた無差別トランク ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan trunk allowed vlan add 1
switch(config-if)# switchport private-vlan mapping trunk 2 add 3
switch(config-if)# switchport private-vlan mapping trunk 4 add 5
switch(config-if)# switchport private-vlan mapping trunk 1 add 20
switch(config-if)# exit
switch(config)#
```

プライベート VLAN 設定の確認

プライベート VLAN 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
show running-config vlan *vlan-id*	VLAN 情報を表示します。
show vlan private-vlan [*type*]	プライベート VLAN に関する情報を表示します。
show interface private-vlan mapping	プライベート VLAN マッピングのインターフェイスの情報を表示します。
show interface vlan *primary-vlan-id* **private-vlan mapping**	プライベート VLAN マッピングのインターフェイスの情報を表示します。
show interface switchport	スイッチポートとして設定されているすべてのインターフェイスに関する情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』を参照してください。

プライベート VLAN の統計情報の表示とクリア

プライベート VLAN 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
clear vlan [**id** *vlan-id*] **counters**	すべての VLAN または指定した VLAN のカウンタをクリアします。
show vlan counters	各 VLAN のレイヤ 2 パケット情報を表示します。

プライベート VLAN の設定例

次に、3 種類のプライベート VLAN を作成し、セカンダリ VLAN をプライマリ VLAN に関連付け、プライベート VLAN のホスト ポートと無差別ポートを作成して適正な VLAN に関連付け、VLAN インターフェイスまたは SVI を作成して、プライマリ VLAN がネットワーク全体と通信できるように設定する例を示します。

```
switch# configure terminal
switch(config)# vlan 2
switch(config-vlan)# private-vlan primary
switch(config-vlan)# exit
switch(config)# vlan 3
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 4
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit

switch(config)# vlan 2
switch(config-vlan)# private-vlan association 3,4
switch(config-vlan)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan host
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# exit

switch(config)# interface ethernet 1/11
switch(config-if)# switchport private-vlan host-association 2 3
switch(config-if)# exit
switch(config)# interface ethernet 1/12
switch(config-if)# switchport private-vlan mapping 2 3,4
switch(config-if)# exit

switch(config)# interface vlan 2
switch(config-vlan)# private-vlan mapping 3,4
switch(config-vlan)# exit
switch(config)#
```

プライベート VLAN の追加情報（CLI バージョン）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
VLAN インターフェイス、IP アドレス指定	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x*』
スタティック MAC アドレス、セキュリティ	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*』
Cisco NX-OS の基礎	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x*』
ハイ アベイラビリティ	『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』
システム管理	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x*』
仮想デバイス コンテキスト（VDC）	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 6.x*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB のリンク
• CISCO-PRIVATE-VLAN-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

プライベート VLAN 設定の機能履歴（CLI バージョン）

次の表に、この機能のリリースの履歴を示します。

表 *2*：プライベート *VLAN* 設定の機能履歴

機能名	リリース	機能情報
プライベート VLAN 無差別トランク ポートと独立トランク ポート	5.0(2)	この機能では、無差別ポートから複数のプライベート VLAN および通常の VLAN のトラフィックを伝送でき、独立ポートから複数の独立 VLAN および通常の VLAN のトラフィックを伝送できます。
変更なし	4.2(1)	–
デバイス上でイネーブルになっている機能の表示	4.1(2)	次のコマンドを入力すると、デバイス上でイネーブルになっている機能を表示できます。 • **show feature**