Configuring VLANs

- Information About VLANs, on page 1
- Prerequisites for Configuring VLANs, on page 5
- Guidelines and Limitations for Configuring VLANs, on page 6
- Default Settings for VLANs, on page 7
- Configuring a VLAN, on page 7
- Verifying the VLAN Configuration, on page 16
- Displaying and Clearing VLAN Statistics, on page 17
- Configuration Example for VLANs, on page 17
- Additional References for VLANs, on page 17

Information About VLANs

You can use VLANs to divide the network into separate logical areas at the Layer 2 level. VLANs can also be considered as broadcast domains.

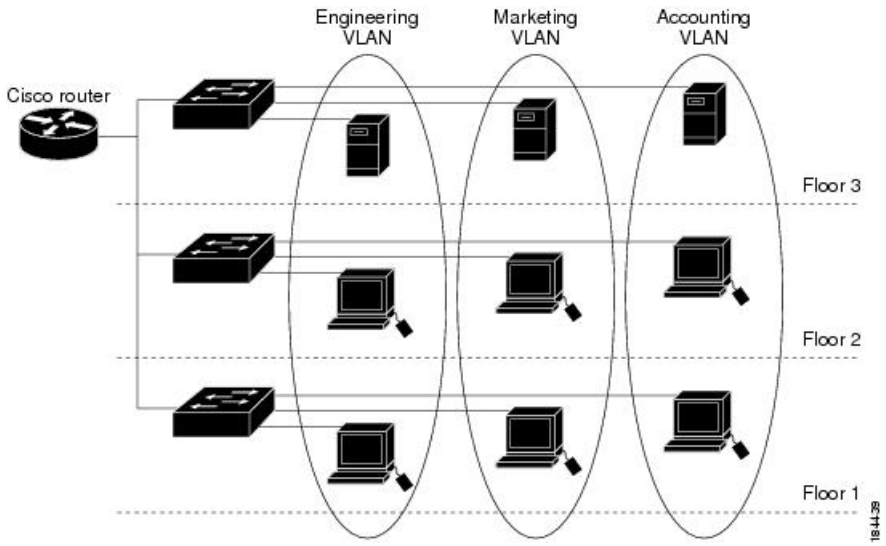
Any switch port can belong to a VLAN, and unicast broadcast and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

Understanding VLANs

A VLAN is a group of end stations in a switched network that is logically segmented by function or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered as a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router. The following figure shows VLANs as logical networks. The stations in the engineering department are assigned to one VLAN, the stations in the marketing department are assigned to another VLAN, and the stations in the accounting department are assigned to another VLAN.

Figure 1: VLANs as Logically Defined Networks



VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. To communicate between VLANs, you must route the traffic.

By default, a newly created VLAN is operational; that is, the newly created VLAN is in the no shutdown condition. Additionally, you can configure VLANs to be in the active state, which is passing traffic, or the suspended state, in which the VLANs are not passing packets. By default, the VLANs are in the active state and pass traffic.

A VLAN interface, or switched virtual interface (SVI), is a Layer 3 interface that is created to provide communication between VLANs. In order to route traffic between VLANs, you must create and configure a VLAN interface for each VLAN. Each VLAN requires only one VLAN interface.

VLAN Ranges

Note The extended system ID is always automatically enabled in Cisco Nexus 9000 devices.

The device supports up to 4095 VLANs in accordance with the IEEE 802.1Q standard. The software organizes these VLANs into ranges, and you use each range slightly differently.

For information about configuration limits, see the verified scalability limits documentation for your switch.

This table describes the VLAN ranges.

Table 1: VLAN Ranges

VLANs Numbers	Range	Usage
1	Normal	Cisco default. You can use this VLAN, but you cannot modify or delete it.
2—1005	Normal	You can create, use, modify, and delete these VLANs.

VLANs Numbers	Range	Usage
1006—3967	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: • The state is always active. • The VLAN is always enabled. You cannot shut down these VLANs.
3968-4095	Internally allocated	These reserved VLANs are allocated for internal device use.

Note Cisco recommends that you enter the range in an increasing order, though the system accepts the range entered in decreasing order.

For example, to delete the range of VLANs from 1602 to 1607, the recommended way to enter the value is 1602-1607, rather than 1607-1602. Entering the range as 1602-7 will delete VLANs from 7 to 1602, instead of 1602 to 1607.

About Reserved VLANs

The following are notes about reserved VLANs (3968 to 4095):

- The software allocates a group of VLAN numbers for features like multicast and diagnostics, that need to use internal VLANs for their operation. By default, the system allocates a block of 128 reserved VLANs (3968 to 4095) for these internal uses.
- You can change the range of reserved VLANs with the system **vlan** *vlan-id* **reserve** command. This allows you to set a different range of VLANs to be used as the reserved VLANs. The selected VLANs must be reserved in groups of 128.
  - You may configure VLANs 3968-4092 for other purposes.
  - VLANs 4093-4095 are always reserved for internal use and cannot be used other purposes.

  For example,

  ```
  system vlan 400 reserve
  ```

  reserves VLANs 400-527.

  The new reserved range takes effect after the running configuration is saved and the device is reloaded.

  - VLANs 4093-4095 are always reserved for internal use and cannot be used other purposes.

    In the example, the result of the command would be that VLANs 400-527 are reserved and that VLANs 4093-4095 are also reserved.

- The **no system vlan** *vlan-id* **reserve** command changes the range for reserved VLANs to the default range of 3968-4095 after the device is reloaded.
- Use the **show system vlan reserved** command to verify the range of the current and future reserved VLAN ranges.

Example of VLAN Reserve

The following is an example of configuring the VLAN reserve (before and after image reload):

```
**********************************************
CONFIGURE NON-DEFAULT RANGE, "COPY R S" AND RELOAD
**********************************************
switch(config)# system vlan 400 reserve
"vlan configuration 400-527" will be deleted automatically.
Vlans, SVIs and sub-interface encaps for vlans 400-527 need to be removed by the user.
Continue anyway? (y/n) [no] y
Note: After switch reload, VLANs 400-527 will be reserved for internal use.
      This requires copy running-config to startup-config before
      switch reload.  Creating VLANs within this range is not allowed.

switch(config)# show system vlan reserved

system current running vlan reservation: 3968-4095

system future running vlan reservation: 400-527


switch(config)# copy running-config startup-config
[########################################] 100%

switch(config)# reload
This command will reboot the system. (y/n)?  [n] y

************
AFTER RELOAD
************

switch# show system vlan reserved

system current running vlan reservation: 400-527
```

Creating, Deleting, and Modifying VLANs

Note By default, all Cisco Nexus 9396 and Cisco Nexus 93128 ports are Layer 2 ports.

By default, all Cisco Nexus 9504 and Cisco Nexus 9508 ports are Layer 3 ports.

VLANs are numbered from 1 to 3967. All ports that you have configured as switch ports belong to the default VLAN when you first bring up the switch as a Layer 2 device. The default VLAN (VLAN1) uses only default values, and you cannot create, delete, or suspend activity in the default VLAN.

You create a VLAN by assigning a number to it; you can delete VLANs and move them from the active operational state to the suspended operational state. If you attempt to create a VLAN with an existing VLAN ID, the device goes into the VLAN submode but does not create the same VLAN again.

Newly created VLANs remain unused until Layer 2 ports are assigned to the specific VLAN. All the ports are assigned to VLAN1 by default.

Depending on the range of the VLAN, you can configure the following parameters for VLANs (except the default VLAN):

- VLAN name
- VLAN state
- Shutdown or not shutdown

You can configure VLAN long-names of up to 128 characters. To configure VLAN long-names, VTP must be in transparent mode.

Note See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide* for information on configuring ports as VLAN access or trunk ports and assigning ports to VLANs.

When you delete a specified VLAN, the ports associated to that VLAN become inactive and no traffic flows. When you delete a specified VLAN from a trunk port, only that VLAN is shut down and traffic continues to flow on all the other VLANs through the trunk port.

However, the system retains all the VLAN-to-port mapping for that VLAN, and when you reenable or re-create, that specified VLAN, the system automatically reinstates all the original ports to that VLAN. The static MAC addresses and aging time for that VLAN are not restored when the VLAN is reenabled.

Note Commands entered in the VLAN configuration submode are not immediately executed. You must exit the VLAN configuration submode for configuration changes to take effect.

High Availability for VLANs

The software supports high availability for both stateful and stateless restarts, as during a cold reboot, for 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 when you use VLANs.

Note See the *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*, for complete information on high availability features.

Prerequisites for Configuring VLANs

VLANs have the following prerequisites:

- You must be logged onto the device.
- You must create the VLAN before you can do any modification of that VLAN.

Guidelines and Limitations for Configuring VLANs

VLANs have the following configuration guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.
- You can configure a single VLAN or a range of VLANs.

  When you configure a large number of VLANs, first create the VLANs using the **vlan** command (for example, **vlan** *200-300*, *303-500*). After the VLANS have been successfully created, name or configure those VLANs sequentially.
- You cannot create, modify, or delete any VLANs that are within the group of VLANs reserved for internal use.
- VLAN1 is the default VLAN. You cannot create, modify, or delete this VLAN.
- VLANs 1006 to 3967 are always in the active state and are always enabled. You cannot suspend the state or shut down these VLANs.
- When the spanning tree mode is changed, the Layer 3 subinterface VLANs that share the same VLAN IDs with Layer 2 VLANs might be affected by a few micro-seconds of traffic drops as a result of the hardware re-programming.
- VLANs 3968 to 4095 are reserved for internal device use by default.
- A port *cannot* simultaneously have port-VLAN mapping and operate as a Private VLAN (PVLAN) interface in promiscuous, isolated, trunk, or host port modes due to hardware and configuration limitations. PVLAN and port-VLAN features operate independently on separate ports. You can configure and use the same VLAN for both functionalities. This is applicable on these releases.
  - Cisco NX-OS Release 10.2(9)M
  - Cisco NX-OS Release10.3(7)M
  - Cisco NX-OS Release 10.4(5)M
  - Cisco NX-OS Release 10.5(3)F
- Beginning with Cisco NX-OS Release 10.5(3)F, VLANs configuration is supported on the Cisco Nexus 93C64E-SG2-Q switch.
- Beginning with Cisco NX-OS Release 9.2(3), VLANs can be configured to have vn-segments.
- Cisco Nexus 9348GC-FX3PH switch has feature limitations due to half-duplex for ports 41-48.
- Cisco Nexus C93108TC-FX3 switch has feature limitations due to half-duplex for ports 41-48.
- QOS/ACL/SPAN are not supported on FEX HIFs.
- Beginning with Cisco NX-OS Release 9.3(9), PVLAN configuration is not allowed on vPC Peer-link interfaces.

Default Settings for VLANs

This table lists the default settings for VLAN parameters.

Table 2: Default VLAN Parameters

Parameters	Default
VLANs	Enabled
VLAN	VLAN1—A port is placed in VLAN1 when you configure it as a switch port.
VLAN ID	1
VLAN name	• Default VLAN (VLAN1)—default • All other VLANs—VLAN *vlan-id*
VLAN state	Active
STP	Enabled; Rapid PVST+ is enabled
VTP	Disabled
VTP version	1

Configuring a VLAN

Note See the *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*, for information on assigning Layer 2 interfaces to VLANs (access or trunk ports). All interfaces are in VLAN1 by default.

Note 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.

Creating and Deleting a VLAN - CLI Version

You can create or delete all VLANs except the default VLAN and those VLANs that are internally allocated for use by the device.

Once a VLAN is created, it is automatically in the active state.

Note When you delete a VLAN, ports associated to that VLAN become inactive. Therefore, no traffic flows and the packets are dropped. On trunk ports, the port remains open and the traffic from all other VLANs except the deleted VLAN continues to flow.

If you create a range of VLANs and some of these VLANs cannot be created, the software returns a message listing the failed VLANs, and all the other VLANs in the specified range are created.

Note You can also create and delete VLANs in the VLAN configuration submode.

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **exit**
4. (Optional) **show vlan**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Creates a VLAN or a range or VLANs. If you enter a number that is already assigned to a VLAN, the device puts you into the VLAN configuration submode for that VLAN. If you enter a number that is assigned to an internally allocated VLAN, the system returns an error message. However, if you enter a range of VLANs and one or more of the specified VLANs is outside the range of internally allocated VLANs, the command takes effect on only those VLANs outside the range. The range is from 2 to 3967; VLAN1 is the default VLAN and cannot be created or deleted. You cannot create or delete those VLANs that are reserved for internal use. For more information about VLAN ranges, see VLAN Ranges, on page 2

Step 3	**exit** **Example:**	Exits the VLAN mode.

	Command or Action	Purpose
	`switch(config-vlan)# exit` `switch(config)#`	
Step 4	(Optional) **show vlan** **Example:** `switch# show vlan`	Displays information and status of VLANs.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to create a range of VLANs from 15 to 20:

```
switch# config t
switch(config)# vlan 15-20
switch(config-vlan)# exit
switch(config)#
```

Entering the VLAN Configuration Submode

To configure or modify the VLAN for the following parameters, you must be in the VLAN configuration submode:

- Name
- State
- Shut down

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **exit**
4. (Optional) **show vlan**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**config t** **Example:**	Enters configuration mode.

	Command or Action	Purpose
	`switch# config t` `switch(config)#`	

Step 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Places you into the VLAN configuration submode. This submode allows you to name, set the state, disable, and shut down the VLAN or range of VLANs.
		You cannot change any of these values for VLAN1 or the internally allocated VLANs. For more information about VLAN ranges, see VLAN Ranges, on page 2

Step 3	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN configuration mode.

Step 4	(Optional) **show vlan** **Example:** `switch# show vlan`	Displays information and status of VLANs.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

This example shows how to enter and exit the VLAN configuration submode:

```
switch# config t
switch(config)# vlan 15
switch(config-vlan)# exit
switch(config)#
```

Configuring a VLAN

To configure or modify a VLAN for the following parameters, you must be in the VLAN configuration submode:

- Name
- State
- Shut down

Note You cannot create, delete, or modify the default VLAN or the internally allocated VLANs. Additionally, some of these parameters cannot be modified on some VLANs.

SUMMARY STEPS

1. **config t**
2. **vlan** {*vlan-id* | *vlan-range*}
3. **name** *vlan-name*
4. **state** {**active** | **suspend**}
5. **no shutdown**
6. **exit**
7. (Optional) **show vlan**
8. (Optional) **show vtp status**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**vlan** {*vlan-id* | *vlan-range*}
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Places you into the VLAN configuration submode. If the VLAN does not exist, the system creates the specified VLAN and then enters the VLAN configuration submode. For more information about VLAN ranges, see VLAN Ranges, on page 2

Step 3	**name** *vlan-name* **Example:** `switch(config-vlan)# name accounting`	Names the VLAN. You can enter up to 32 alphanumeric characters to name the VLAN. You cannot change the name of VLAN1 or the internally allocated VLANs. The default value is VLANxxxx where xxxx represent four numeric digits (including leading zeroes) equal to the VLAN ID number. **Note** 128-character names are supported (VLAN Long-Name).
Step 4	**state** {**active** | **suspend**} **Example:** `switch(config-vlan)# state active`	Sets the state of the VLAN to active or suspend. While the VLAN state is suspended, the ports associated with this VLAN become inactive, and that VLAN does not pass any traffic. The default state is active. You cannot suspend the state for the default VLAN or VLANs 1006 to 3967.
Step 5	**no shutdown** **Example:** `switch(config-vlan)# no shutdown`	Enables the VLAN. The default value is no shutdown (or enabled). You cannot shut down the default VLAN, VLAN1, or VLANs 1006 to 3967.

	Command or Action	Purpose

Step 6	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN configuration submode.

Step 7	(Optional) **show vlan** **Example:** `switch# show vlan`	Displays information and status of VLANs.
Step 8	(Optional) **show vtp status** **Example:** `switch# show vtp status`	Displays information and status of VLAN Trunking Protocols (VTPs).
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. **Note** Commands entered in the VLAN configuration submode are not immediately executed. You must exit the VLAN configuration submode for configuration changes to take effect.

Example

This example shows how to configure optional parameters for VLAN 5:

```
switch# config t
switch(config)# vlan 5
switch(config-vlan)# name accounting
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
switch(config)#
```

Configuring a VLAN Before Creating the VLAN

You can configure a VLAN before you create the VLAN. This procedure is used for IGMP snooping, VTP, and other configurations.

Note The **show vlan** command does not display these VLANs unless you create it using the **vlan** command.

SUMMARY STEPS

1. **config t**
2. **vlan configuration** {*vlan-id*}

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**vlan configuration** {*vlan-id*}
	Example:
	`switch(config)# vlan configuration 20`
	`switch(config-vlan-config)#`
		Allows you to configure VLANs without actually creating them.

Example

This example shows how to configure a VLAN before creating it:

```
switch# config t
switch(config)# vlan configuration 20
switch(config-vlan-config)#
```

Enabling the VLAN Long-Name

You can configure VLAN long-names of up to 128 characters.

Note When **system vlan long-name** is included in the start-up configuration, the Cisco Nexus 9000 Series switch boots up in VTP off mode.

To enable VTP transparent mode:

1. Disable VTP
2. Remove **system vlan long-name** from the start-up configuration
3. Re-enable VTP

Before you begin

VTP must be in transparent or in off mode. VTP cannot be in client or server mode. For more details about VTP, see Configuring VTP.

SUMMARY STEPS

1. **configure terminal**
2. **system vlan long-name**

3. (Optional) **copy running-config startup-config**
4. **show running-config vlan**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**system vlan long-name** **Example:** `switch(config)# system vlan long-name`	Allows you to enable VLAN names that have up to 128 characters. Use the **no** form of this command to disable this feature.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 4	**show running-config vlan** **Example:** `switch(config)# show running-config vlan`	Verifies that the system VLAN long-name feature is enabled.

Example

This example shows how to enable VLAN long-names.

```
switch# configure terminal
switch(config)# system vlan long-name
switch(config)# copy running config startup config
switch(config)# show running-config vlan
```

Configuring Inner VLAN and Outer VLAN Mapping on a Trunk Port

You can configure VLAN translation from an inner VLAN and an outer VLAN to a local (translated) VLAN on a port.

Notes for configuring inner VLAN and outer VLAN mapping:

- VLAN translation (mapping) is supported on Cisco Nexus 9000 Series switches with a Network Forwarding Engine (NFE). VLAN translation is supported on Cisco Nexus 9300-EX switches.
- Inner and outer VLAN cannot be on the trunk allowed list on a port where inner VLAN and outer VLAN is configured.

  For example:

```
switchport vlan mapping 11 inner 12 111
switchport trunk allowed vlan 11-12,111 /***Not valid because 11 is outer VLAN and 12
is inner VLAN.***/
```

- On the same port, no two mapping (translation) configurations can have the same outer (or original) or translated VLAN. Multiple inner VLAN and outer VLAN mapping configurations can have the same inner VLAN.

  For example:

```
switchport vlan mapping 101 inner 102 1001
switchport vlan mapping 101 inner 103 1002  /***Not valid because 101 is already used
as an original VLAN.***/
switchport vlan mapping 111 inner 104 1001  /***Not valid because 1001 is already used
 as a translated VLAN.***/
switchport vlan mapping 106 inner 102 1003  /***Valid because inner vlan can be the
same.***/
```

- Port VLAN mapping on a trunk port is supported on Cisco Nexus 9000 Series switches with a Network Forwarding Engine (NFE), Cisco Nexus 9200, 9300-EX, 9300-FX, and Cisco Nexus 9500 platform switches with EX/FX line cards.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type port*
3. [**no**] **switchport mode trunk**
4. **switchport vlan mapping enable**
5. **switchport vlan mapping** *outer-vlan-id* **inner** *inner-vlan-id translated-vlan-id*
6. (Optional) **copy running-config startup-config**
7. (Optional) **show interface** [*if-identifier*] **vlan mapping**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *type port*	Enters interface configuration mode.
Step 3	[**no**] **switchport mode trunk**	Enters trunk configuration mode.
Step 4	**switchport vlan mapping enable**	Enables VLAN translation on the switch port. VLAN translation is disabled by default. **Note** Use the **no** form of this command to disable VLAN translation.

	Command or Action	Purpose
Step 5	**switchport vlan mapping** *outer-vlan-id* **inner** *inner-vlan-id translated-vlan-id*	Translates inner VLAN and outer VLAN to another VLAN.
Step 6	(Optional) **copy running-config startup-config**	Copies the running configuration to the startup configuration. **Note** The VLAN translation configuration does not become effective until the switch port becomes an operational trunk port
Step 7	(Optional) **show interface** [*if-identifier*] **vlan mapping**	Displays VLAN mapping information for a range of interfaces or for a specific interface.

Example

This example shows how to configure translation of double tag VLAN traffic (inner VLAN 12; outer VLAN 11) to VLAN 111.

```
switch# config t
switch(config)# interface ethernet1/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport vlan mapping enable
switch(config-if)# switchport vlan mapping 11 inner 12 111
switch(config-if)# switchport trunk allowed vlan 101-170
switch(config-if)# no shutdown

switch(config-if)# show mac address-table dynamic vlan 111

Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*  111     0000.0092.0001   dynamic  0         F      F    nve1(100.100.100.254)
*  111     0000.0940.0001   dynamic  0         F      F    Eth1/1
```

Verifying the VLAN Configuration

To display VLAN configuration information, perform one of the following tasks:

Command	Purpose
show running-config vlan *vlan-id*	Displays VLAN information.
show vlan [**all-ports** | **brief** | **id** *vlan-id* | **name** *name* | **dot1q tag native**]	Displays VLAN information.
show vlan summary	Displays a summary of VLAN information.

Command	Purpose
show vtp status	Displays VTP information.

Displaying and Clearing VLAN Statistics

To display VLAN configuration information, perform one of the following tasks:

Command	Purpose
clear vlan [**id** *vlan-id*] **counters**	Clears counters for all VLANs or for a specified VLAN.
show vlan counters	Displays information on Layer 2 packets in each VLAN.

Configuration Example for VLANs

The following example shows how to create and name a VLAN as well as how to make the state active and administratively up:

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan)# name test
switch(config-vlan)# state active
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
switch(config)#
```

Additional References for VLANs

Related Documents

Related Topic	Document Title
NX-OS Layer 2 switching configuration	*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*
Interfaces, VLAN interfaces, IP addressing, and port channels	*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*
Multicast routing	*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*
NX-OS fundamentals	*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*

Related Topic	Document Title
High availability	*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*
System management	*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
CISCO-VLAN-MEMBERSHIP MIB: • vmMembership Table • MIBvmMembershipSummaryTable • MIBvmMembershipSummaryTable	To locate and download MIBs, go to the following URL: https://cisco.github.i supportlists/nexus9000/Nexus9000MIBSupportList.html