Configuring VLANs

This chapter describes how to configure virtual LANs (VLANs) on CIsco NX-OS devices.

For more information about the Data Center Network Manager (DCNM) features, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.2*.

.

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 bridge or a router.

The Cisco NX-OS release that is running on a managed device many not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

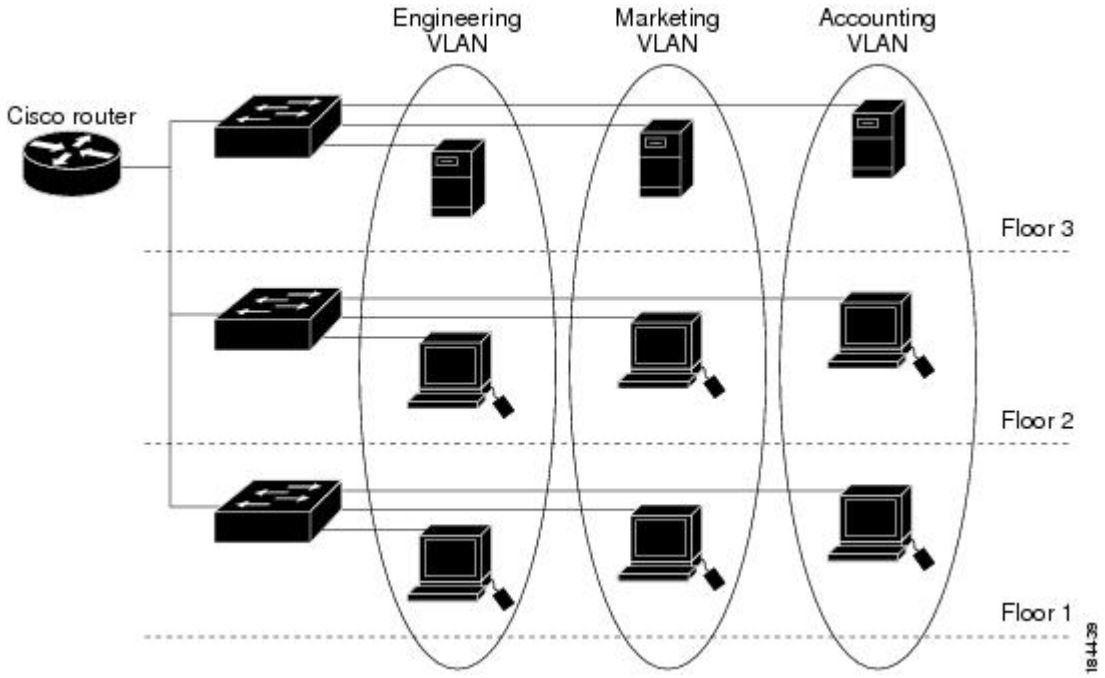
VLANs Overview

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.

This 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.

Note See the Cisco DCNM Interfaces Configuration Guide, Release 4.2 for complete information on configuring VLAN network interfaces and subinterfaces, as well as assigning IP addresses. This feature must be enabled before you can configure VLAN network interfaces.

VLAN Ranges

Note The extended system ID is always automatically enabled in Cisco NX-OS devices.

The device supports up to 4094 VLANs in accordance with the IEEE 802.1Q standard in each VDC. The software organizes these VLANs into ranges, and you use each range slightly differently.

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.
1006—3967 and 4048—4093	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.
3968-4047 and 4094	Internally allocated	These 80 VLANs and VLAN 4094 are allocated for internal device use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.

Note VLANs 3968 to 4047 and 4094 are reserved for internal use in each VDC; you cannot change or use these VLANs.

The software allocates a group of 80 VLAN numbers for those features, like multicast and diagnostics, that need to use internal VLANs for their operation. By default, the system allocates VLANs 3968 to 4047 for internal use. VLAN 4094 is also reserved for internal use by the device.

You cannot use, modify, or delete any of the VLANs in the reserved group. You can display the VLANs that are allocated internally and their associated use.

Creating, Deleting, and Modifying VLANs

Note By default, all Cisco NX-OS ports are Layer 3 ports.

VLANs are numbered from 1 to 4094 for each VDC. 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

Note See the Cisco DCNM Interfaces Configuration Guide, Release 4.2 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 are shut down 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 VLANs 3968 to 4047 and 4094 are reserved for internal use in each VDC; you cannot change or use these VLANs.

VTP

The VLAN Trunking Protocol (VTP) is disabled by default on the device. You enable and configure VTP using the command-line interface (CLI). When VTP is disabled, the device does not relay any VTP protocol packets.

For information about enabling and configuring VTP, see the Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2.

VTP is a Layer 2 messaging protocol that maintains VLAN consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain is made up of one or more network devices that share the same VTP domain name and that are connected with trunk interfaces. Each network device can be in only one VTP domain.

Layer 2 trunk interfaces, Layer 2 port channels, and virtual port channels (vPCs) support VTP functionality.

Note In the Cisco Nexus 7000 Series devices, VTP works only in transparent mode, allowing you to extend a VTP domain across the device.

When the device is in the VTP transparent mode, the device relays all VTP protocol packets it receives on a trunk port to all other trunk ports. When you create or modify a VLAN that is in VTP transparent mode, those VLAN changes affect only the local device. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

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 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.2 for complete information on high availability features.

Virtualization Support for VLANs

The software supports virtual device contexts (VDCs), and VLAN configuration and operation are local to the VDC.

Note See the Cisco DCNM Virtual Device Context Configuration Guide, Release 4.2 for complete information on VDCs and assigning resources.

When you create a new VDC, the device automatically creates a new default VLAN, VLAN1, and internally reserves VLANs 3968 to 4047 and 4094 for device use.

One or more VLANs can be associated with a role to either allow or disallow the user to configure it. When a VLAN is associated with a role, the corresponding interfaces will also be subjected to the same check. For instance, if a role is allowed to access VLAN1, then that role also has access to the interfaces that have that VLAN. If an interface does not have the VLAN associated with a role, that interface is not accessible to that role.

Licensing Requirements for VLANs

The following table shows the licensing requirements for this feature.

	License Requirement
DCNM	VLANs require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you..
NX-OS	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 NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*.

However, using VDCs requires an Advanced Services license.

Prerequisites for Configuring VLANs

The following are prerequisites for configuring VLANs:

- 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

Follow these guidelines and limitations when configuring VLANs:

- The maximum number of VLANs per VDC is 4094.
- 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 4094 are always in the active state and are always enabled. You cannot suspend the state or shut down these VLANs.

Configuring a VLAN

Note See the Cisco DCNM Fundamentals Configuration Guide, Release 4.2, for information on using the Topology feature with VLANs

Note See the Cisco DCNM Interfaces Configuration Guide, Release 4.2, for information on assigning Layer 2 interfaces to VLANs (access or trunk ports). All interfaces are in VLAN 1 by default.

Creating and Deleting a VLAN

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

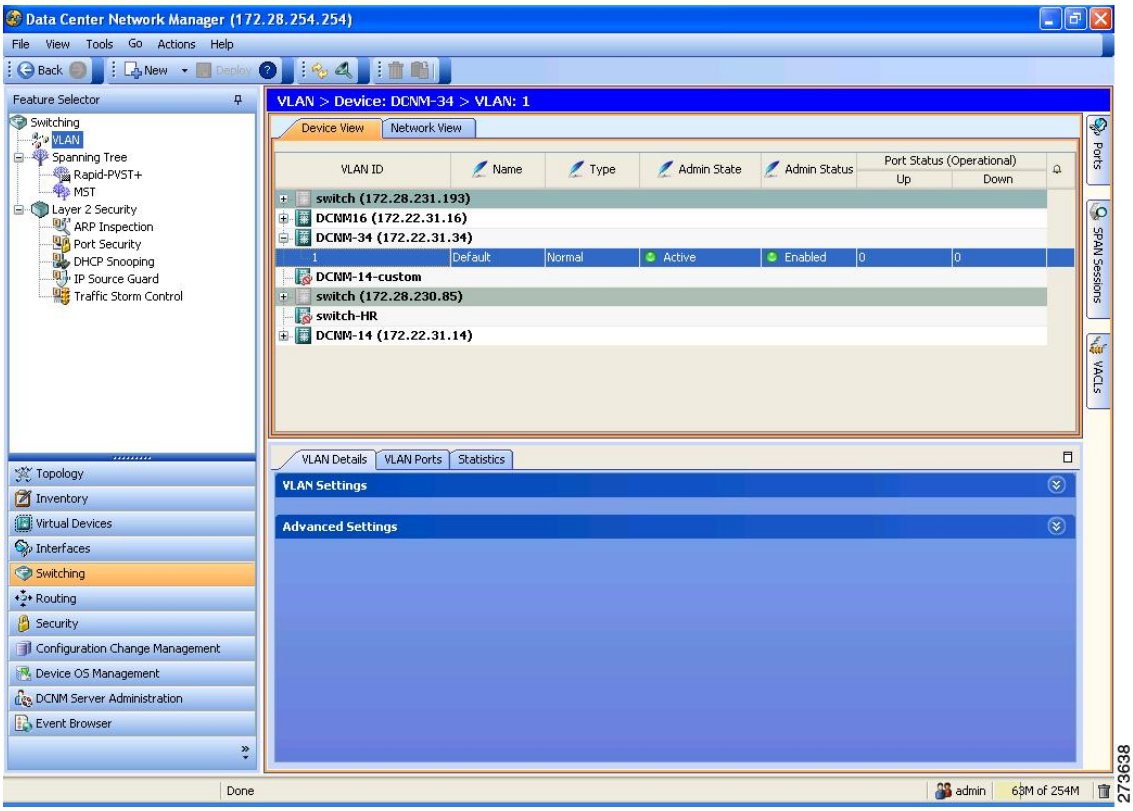
Once a VLAN is created, it is automatically in the active state.

Note When you delete a VLAN, ports associated to that VLAN shut down. 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.

This figure shows the VLAN pane that you use to create VLANs.

Figure 2: Configuring VLAN Details



To create or delete a VLAN, follow these steps:

Configuring or Modifying the Basic Settings for a VLAN

You can use the VLAN pane to modify the basic VLAN settings (see Figure 2: Configuring VLAN Details, page 8).

To modify the basic settings for a VLAN, follow these steps:

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ VLAN** to open the VLAN pane.

Step 2 In the Summary pane, click the **Device View** tab.

Step 3 Click the device that you want to configure.
The system highlights the device in the Summary pane, and tabs appear in the Details pane.

Step 4 Expand the view for the device.
The system lists the VLANs configured on that device.

Step 5 Highlight the VLAN that you want to configure.

Step 6 In the Details pane, click the **VLAN Details** tab.

Step 7 Click the **VLAN Settings** tab.

Note Do not change the dimmed value in the Media row from Ethernet. Ethernet is the only supported media.

Step 8 Enter the name in the VLAN Name field.

Step 9 Choose the type of VLAN that you want and the administrative state and status from the drop-down lists.

Step 10 (Optional) Beginning with Cisco NX-OS Release 4.2(3), if you want to enable this VLAN for the Chassis Internal Network (CIN), click the Enable VLAN CIN checkbox.

Note See the *Cisco Nexus 4001 Switch Module Configuration Guide* for information on CIN.

Step 11 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Copying the VLAN from One Device to Another

You can copy and paste the VLAN, along with its VLAN ID, name, type, admin stat, and admin status, from one device to another.

To copy and paste a VLAN from one device to another, follow these steps:

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ VLAN** to open the VLAN pane.

Step 2 In the Summary pane, click the **Device View** tab.

Step 3 Click the device from which you want to copy the VLAN.

Step 4 Expand the view for the device.
The system lists the VLANs configured on that device.

Step 5 Highlight the VLAN that you want to copy.

Step 6 From the menu bar, choose **Actions ➤ Copy**.

Step 7 In the Summary pane, click the device to which you want to paste the VLAN.

Step 8 From the menu bar, choose **Actions ➤ Paste**.

Step 9 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Displaying VLAN Statistics

- VLAN Traffic Statistics—Displays information on VLAN traffic such as Layer 2 unicast, multicast, and broadcast traffic, Layer 3 unicast and multicast traffic, and so forth.

Field Descriptions for Configuring VLANs

Device View Device Global Settings: Global Settings Section

Table 2: Device View: Device: Global Settings: Global Settings Section

Field	Description
Dot1Q Native Tag	Tagging of the packets on the native VLAN maintained on all trunk ports on the device. The default is disabled.

Device View VLAN VLAN Details VLAN Settings Section

Table 3: Device View: VLAN: VLAN Details: VLAN Settings: Normal VLANs

Field	Description
VLAN ID	*Display only*. VLAN ID. The default is the VLAN plus the number of the VLAN (VLANXXXX).
Device	*Display only.* Hostname or IP address for the device for this VLAN.
VLAN Name	Name of the VLAN. The default name is the VLAN plus the number of the VLAN (VLANXXXX).
VLAN Type	VLAN type set as normal. Valid values are as follows: • Normal • Primary • Community • Isolated
Media	This field is not supported.
Admin State	Administrative state. Valid values are as follows: • Active • Suspended The default is Active.
Admin Status	Administrative status. Valid values are as follows:

Field	Description
	• Enabled • Disabled The default is Enabled.
VLAN Network Interface Settings	
Description	Description of the VLAN network interface. The value is any printable string.
IP Address	IP address for the VLAN network interface. The value is a valid IP address in dotted decimal notation (A:B:C:D).
Netmask	Network mask for the VLAN network interface. The value is in dotted decimal notation.
Admin State	Administrative state of the VLAN network interface. Valid values are as follows: • Down • Up The default is Up.
Oper Status	*Display only*. Operational status of this VLAN network interface.

Table 4: Device View: VLAN: VLAN Details: VLAN Settings: Primary VLANs

Field	Description
VLAN ID	*Display only*. VLAN ID. The default is the VLAN plus the number of the VLAN (VLANXXXX).
Device	*Display only.* Hostname or IP address for the device for this VLAN.
VLAN Name	Name of the VLAN. The default name is the VLAN plus the number of the VLAN (VLANXXXX).
VLAN Type	VLAN type set as a primary VLAN. The primary VLAN carries downstream traffic from the router to the private VLAN host ports. Valid values are as follows: • Normal • Primary

Field	Description
	• Community • Isolated
Media	This field is not supported.
Admin State	Administrative state. Valid values are as follows: • Active • Suspended The default is Active.
Admin Status	Administrative status. Valid values are as follows: • Enabled • Disabled The default is Enabled.
Oper Status	*Display only*. Operational status of this VLAN.
Secondary VLANs **Note** Multiple secondary VLANs can be associated with each primary VLAN.	
VLAN Id	*Display only.* Isolated and community VLANs configured on the device.
Type	*Display only.* Type of the secondary VLAN. Valid values are as follows: • Community • Isolated
VLAN Network Interface Settings	
Description	Description of the VLAN network interface. The value is any printable string
IP Address	IP address for the VLAN network interface. The value is a valid IP address in dotted decimal notation (A:B:C:D).
Netmask	Network mask for the VLAN network interface. The value is in dotted decimal notation.

Field	Description
Admin State	Administrative state of the VLAN network interface. Valid values are as follows: • Down • Up The default is Up.

Table 5: Device View: VLAN: VLAN Details: VLAN Settings: Community VLANs

Field	Description
VLAN ID	*Display only*. VLAN ID. The default is the VLAN plus the number of the VLAN (VLANXXXX).
Device	*Display only.* Hostname or IP address for the device for this VLAN.
VLAN Name	Name of the VLAN. The default name is the VLAN plus the number of the VLAN (VLANXXXX).
VLAN Type	VLAN set as a community VLAN. Valid values are as follows: • Normal • Primary • Community • Isolated
Primary VLAN ID	*Display only.* Displays the primary VLAN with which this community VLAN is associated. **Note** If you have not associated a primary VLAN, the system displays Not Configured.
Media	This field is not supported.
Admin State	Valid values are as follows: • Active • Suspended The default is Active.
Admin Status	Valid values are as follows: • Enabled

Field	Description
	• Disabled The default is Enabled.
VLAN Network Interface Settings **Note** When a community VLAN is associated with a primary VLAN, this VLAN network interface is not supported. With private VLANs, only the VLAN network interface on the primary VLAN is operational.	
Description	Description of the VLAN network interface. The value is any printable string.
IP Address	IP address for the VLAN network interface. The value is a valid IP address in dotted decimal notation (A:B:C:D).
Netmask	Network mask for the VLAN network interface. The value is in dotted decimal notation.
Admin State	Administrative state of the VLAN network interface. Valid values are as follows: • Down • Up The default is Up.
Oper Status	*Display only*. Operational status of this VLAN network interface.

Table 6: Device View: VLAN: VLAN Details: VLAN Settings: Isolated VLANs

Field	Description
VLAN ID	*Display only*. VLAN ID. The default is the VLAN plus the number of the VLAN (VLANXXXX).
Device	*Display only.* Hostname or IP address for the device for this VLAN.
VLAN Name	Name of the VLAN. The maximum number of characters is XXX. The default name is VLAN plus the numerical value of the VLAN: VLANXXXX.
VLAN Type	VLAN type set as an isolated VLAN. Valid values are as follows:

Field	Description
	• Normal • Primary • Community • Isolated
Primary VLAN ID	*Display only.* Displays the primary VLAN with which this community VLAN is associated. **Note** If you have not associated a primary VLAN, the system displays Not Configured.
Media	This field is not supported.
Admin State	Administrative state. Valid values are as follows: • Active • Suspended The default is Active.
Admin Status	Administrative status. Valid values are as follows: • Enabled • Disabled The default is Enabled.
Oper Status	Operational status of this VLAN.
VLAN Network Interface Settings **Note** When an isolated VLAN is associated with a primary VLAN, this VLAN network interface is not supported. With private VLANs, only the VLAN network interface on the primary VLAN is operational.	
Description	Description of the VLAN network interface. The value is any printable string
IP Address	IP address for the VLAN network interface. The value is a valid IP address in dotted decimal notation (A:B:C:D).
Netmask	Network mask for the VLAN network interface. The value is in dotted decimal notation.

Field	Description
Admin State	Administrative state of the VLAN network interface. Valid values are as follows: • Down • Up The default is Up.

Device View VLAN VLAN Details Advanced Settings Section

Table 7: Device View: VLAN: VLAN Details: Advanced Settings Section

Field	Description
SPAN Settings	
RSPAN VLAN	Status of whether there is a remote SPAN (RSPAN) VLAN or not.
SPAN Source Settings	
Session ID	*Display only.* SPAN session ID where interface is applied.
Type	*Display only.* Session type.
Direction: Ingress	Monitor ingress packets.
Direction: Egress	Monitor egress packets.
Security Settings	
DAI	*Display only.* Whether Dynamic ARP Inspection (DAI) is enabled or disabled.
DHCP Snooping	*Display only.* Whether DHCP snooping is enabled or disabled.
VACL	VLAN access map that filters ingress traffic on the VLAN.

Device View VLAN VLAN Ports for Normal VLANs Access Ports Section

Table 8: Device View: VLAN: VLAN Ports for Normal VLANs: Access Ports Section

Field	Description
Interface Name	*Display only*. Name of the access interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Device View VLAN VLAN Ports for Normal VLANs Trunk Ports Section

Table 9: Device View: VLAN: VLAN Ports for Normal VLANs: Trunk Ports Section

Field	Description
Interface Name	*Display only*. Name of the trunk interfaces. This can be a physical port or a port channel.
Description	*Display only.* Description configured for interface. The default is blank.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Device View VLAN Primary VLAN Ports for Primary VLANs Promiscuous Ports Section

Table 10: Device View: VLAN: VLAN Ports for Primary VLANs: Promiscuous Ports Section

Field	Description
Interface Name	*Display only*. Name of the interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Secondary VLANs	Secondary VLANs that are associated to this promiscuous port for the primary VLAN.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Device View VLAN Secondary VLAN Ports Tab for Secondary VLANs PVLAN Host Ports Section

Table 11: Device View: VLAN: VLAN Ports for Secondary VLANs: PVLAN Hosts Ports Section

Field	Description
Interface Name	*Display only*. Name of the interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Port Status	Secondary VLAN to which port is associated. *Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Network View: Device: VLAN Details: VLAN Settings Section

Table 12: Network View: Device: VLAN Details: VLAN Settings: Normal VLANs

Field	Description
VLAN ID	*Display only*. VLAN ID. The default is the VLAN plus the number of the VLAN (VLANXXXX).
Device	*Display only.* Hostname or IP address for the device for this VLAN.
VLAN Name	Name of the VLAN. The maximum number of characters is XXX. The default name is VLAN plus the numerical value of the VLAN: VLANXXXX.
VLAN Type	VLAN type set as a normal VLAN. Valid values are as follows: • Normal • Primary • Community • Isolated
Media	This field is not supported.
Admin State	Administrative state. Valid values are as follows: • Active • Suspended The default is Active.
Admin Status	Administrative status. Valid values are as follows: • Enabled • Disabled The default is Enabled.
VLAN Network Interface Settings	
Description	Description of the VLAN network interface. The value is any printable string.

Field	Description
IP Address	IP address for the VLAN network interface. The value is a valid IP address in dotted decimal notation (A:B:C:D).
Netmask	Network mask for the VLAN network interface. The value is in dotted decimal notation.
Admin State	Administrative state of the VLAN network interface. Valid values are as follows: • Down • Up The default is Up.
Oper Status	*Display only*. Operational status of this VLAN network interface.

Network View: Device: VLAN Details: Advanced Settings Section

Table 13: Network View: Device: VLAN Details: Advanced Settings Section

Field	Description
SPAN Settings	
RSPAN VLAN	Status of whether there is a remote SPAN (RSPAN) VLAN or not.
SPAN Source Settings	
Session ID	*Display only.* SPAN session ID where interface is applied.
Type	*Display only.* Session type.
Direction: Ingress	Monitor ingress packets.
Direction: Egress	Monitor egress packets.
Security Settings	
DAI	*Display only.* Status of whether Dynamic ARP Inspection (DAI) is enabled or disabled.
DHCP Snooping	*Display only.* Status of whether DHCP snooping is enabled or disabled.

Field	Description
VACL	VLAN access map that filters ingress traffic on the VLAN.

Network View: Device: VLAN Ports: Access Ports Section

Table 14: Network View: Device: VLAN Ports for Normal VLANs: Access Ports Section

Field	Description
Interface Name	*Display only*. Name of the access interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Network View: Device: VLAN Ports: Trunk Ports Section

Table 15: Network View: VLAN: VLAN Ports for Normal VLANs: Trunk Ports Section

Field	Description
Interface Name	*Display only*. Name of the trunk interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Network View: Device: Primary VLAN Ports: Promiscuous Ports Section

Table 16: Network View: Device: Primary VLAN Ports: Promiscuous Ports Section

Field	Description
Interface Name	*Display only*. Name of the interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Secondary VLANs	Secondary VLANs that are associated to this promiscuous port for the primary VLAN.
Port Status	*Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Network View: Device: Secondary VLAN Ports: PVLAN Host Ports Section

Table 17: Network View: Device: Secondary VLAN Ports: PVLAN Host Ports Section

Field	Description
Interface Name	*Display only*. Name of the interfaces. This interface can be a physical port or a port channel.
Description	*Display only.* Description configured for the interface. The default is blank.
Port Status	Secondary VLAN to which the port is associated. *Display only.* Status of the port. Valid values are as follows: • Admin Down • Up • Down

Additional References for VLANs

Related Documents

Related Topic	Document Title
NX-OS Layer 2 switching configuration	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2
Interfaces, VLAN network interfaces, IP addressing and port channels	Cisco DCNM Interfaces Configuration Guide, Release 4.2
DCNM fundamentals	Cisco DCNM Fundamentals Configuration Guide, Release 4.2
Multicast routing	Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.2
High availability	Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.2
System management	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.2
VDCs	Cisco DCNM Virtual Device Context Configuration Guide, Release 4.2
Release notes	Cisco DCNM Release Notes, Release 4.2

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: vmMembershipTable-MIB vmMembershipSummaryTable-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for Configuring VLANs - DCNM

This figure lists the release history for this feature.

Table 18: Feature History for Configuring STP Enhancements

Feature Name	Releases	Feature Information
VLANs	4.1(2)	Ability to copy and paste VLANs from one device to another.
No change.	4.2(1)	-