VLANs

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, 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 controller port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the 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 or a controller supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information.

VLANs are often associated with IP subnet. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the controller is assigned manually on an interface-by-interface basis. When you assign controller interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

The controller supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN 1 is the default VLAN and is created during system initialization. All of the VLANs except 1002 to 1005 are available for user configuration.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the controller learns and manages the addresses associated with the port on a per-VLAN basis.

Table 1: Port Membership Modes and Characteristics

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the controller connected to a trunk port of a second controller.
Trunk IEEE 802.1Q) : • IEEE 802.1Q—Industry-standard trunking encapsulation.	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other controller over trunk links.

Note If a client VLAN has two subnets, a primary subnet and a secondary subnet, the static IP address is not supported on the secondary subnet.

Consider the following SVI configuration example:

interface VlanX

ip address a.b.c.254 255.255.255.0 secondary

ip address a.d.e.254 255.255.255.0

In this scenario, you can't allocate the secondary subnet for clients with static IP addresses.

VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory. If the VTP mode is transparent, they are also saved in the controller running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the controller, the controller configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

Note Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using **write erase** command. This ensures that the switch reboots correctly on a reset.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the running configuration file.
- If the controller is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)
- Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode.

If clients are unable to connect to the controller due to a VLAN failure, try one of the following options:

- Configure *ip4 dhcp required* in the policy profile forcing the client to initiate a DHCP request.
- Configure the RADIUS server to send VLAN group (having the client's static IP VLAN) information allowing the client to use static IP.
- Configure *aaa-override vlan fallback* under the policy profile forcing the controller to check for the client's static IP VLAN in other VLAN groups as well. The client can join the network if the client's static IP VLAN is part of the configured VLAN group under the policy profile.

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

Follow these guidelines when creating extended-range VLANs:

- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the device is running VTP version 3.
- You cannot include extended-range VLANs in the pruning eligible range.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the device boots up in VTP transparent

mode. Otherwise, you lose the extended-range VLAN configuration if the device resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- To configure VLAN through the Web UI, you must change the number of available Virtual Terminal (VTY) sessions to 50. Web UI uses VTY lines for processing HTTP requests. At times, when multiple connections are open, the default VTY lines of 15 set by the device gets exhausted. Therefore, you must change the VTY lines to 50 before using the Web UI.

Note To increase the VTY lines in a device, run the following command in the configuration mode:

```
Device# configure terminal
Device(config)# service tcp-keepalives in
Device(config)# service tcp-keepalives out

Device# configure terminal
Device(config)# line vty 16-50
```

Note The maximum number of SSH VTY sessions supported on the standby controller is eight.

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.
- Before adding a VLAN to a VLAN group, you should first create it on the device.

Restrictions for VLANs

The following are restrictions for VLANs:

- You cannot delete a wireless management interface, if the associated VLAN interface is already deleted. To avoid this scenario, you should delete the wireless management interface before deleting the VLAN interface.
- The device supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- When client VLAN is not configured for a policy profile, AP native VLAN is used.
- The behavior of VLAN 1 changes depending on the AP mode. These scenarios are described below:
  - **Local mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the wireless management interface.
  - **FlexConnect mode AP**: If you use *vlan-name*, clients are assigned to VLAN 1. However, if you use *vlan-id* 1, clients are assigned to the native VLAN defined in the flex profile.

By default, the policy profile assigns vlan-id 1 so that clients can use the wireless management VLAN.

- You cannot use the same VLAN on the same SSID for local switching and central switching.

How to Configure VLANs

How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type
  - Ethernet
  - TrBRF or TrCRF
- VLAN state (active or suspended)
- Parent VLAN number for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, follow the procedures in this section.

Creating or Modifying an Ethernet VLAN

Before you begin

With VTP version 1 and 2, if the controller is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

The controller supports only Ethernet interfaces.

Procedure

	Command or Action	Purpose
Step 1	**vlan** *vlan-id* **Example:** `Device(config)# vlan 20`	Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.

	Command or Action	Purpose
Step 2	**name** *vlan-name* **Example:** `Device(config-vlan)# name test20`	(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**media** { **ethernet** | **fd-net** | **trn-net** } **Example:** `Device(config-vlan)# media ethernet`	Configures the VLAN media type.
Step 4	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Device# show vlan name test20 id 20`	Verifies your entries.

Assigning Static-Access Ports to a VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN** > **VLAN**

Step 2 Click the **VLAN** tab.

Step 3 To assign **Port Members**, click the interfaces that are to be included as port members from the **Available** list and click on the arrow to move it to the **Associated** list.

Step 4 Click **Update & Apply to Device**.

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode). For more information on static-access ports, see *VLAN Port Membership Modes*.

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode

	Command or Action	Purpose
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.
Step 3	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id* **Example:** `Device# copy running-config startup-config`	Verifies the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces gigabitethernet2/0/1`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.

How to Configure Extended-Range VLANs

Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the controller running configuration file, and you can

save the configuration in the startup configuration file. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

Creating an Extended-Range VLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Layer2** > **VLAN**.

Step 2 In the VLAN page, click **ADD**.

Step 3 Enter the extended range VLAN ID in the **VLAN ID** field.

The extended range is between range is 1006 and 4094.

Step 4 Enter a VLAN name in the **Name** field.

Step 5 Save the configuration.

Creating an Extended-Range VLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Device(config)# vlan 2000`	Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.
Step 3	**show vlan id** *vlan-id* **Example:** `Device# show vlan id 2000`	Verifies that the VLAN has been created.

Monitoring VLANs

Table 2: Privileged EXEC show Commands

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the controller.
show vlan [**access-map** *name* | **brief** | **group** |**id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **summary**]	Displays parameters for all VLANs or the specified VLAN on the controller. The following command options are available: • **brief**—Displays VTP VLAN status in brief. • **group**—Displays the VLAN group with its name and the connected VLANs that are available. • **id**—Displays VTP VLAN status by identification number. • **ifindex**—Displays SNMP ifIndex. • **mtu**—Displays VLAN MTU information. • **name**—Displays the VTP VLAN information by specified name. • **summary**—Displays a summary of VLAN information.