VLANs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Related Topics

Feature History and Information for Troubleshooting Software Configuration

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

- Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.
- If you plan to configure many VLANs on the controller and to not enable routing, you can set the Switch Database Management (SDM) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses.
- Controllers running the LAN Base feature set support only static routing on SVIs.

- A VLAN should be present in the controller to be able to add it to the VLAN group.

Restrictions for VLANs

The following are restrictions for VLANs:

- In the Cisco Catalyst 4500E Supervisor Engine, the number of controller per-VLAN spanning-tree (PVST) or rapid PVST is based on the number of trunks on the switch multiplied by the number of active VLANs on the trunks, plus the number of non-trunking interfaces on the switch (trunks * VLANS + non-trunk ports). For MSTP, the maximum number of MST instances supported is 4094.
- The controller supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- Configuring an interface VLAN router's MAC address is not supported. The interface VLAN already has an MAC address assigned by default.
- Private VLANs are not supported on the controller.
- You cannot have a switch stack containing a mix of Catalyst 3850 and Catalyst 3650 switches.

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 and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. 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.

Traffic between VLANs must be routed.

The controller can route traffic between VLANs by using controller virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

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. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. All of the VLANs except 1002 to 1005 are available for user configuration.

There are 3 VTP versions: VTP version 1, version 2, and version 3. All VTP versions support both normal and extended range VLANs, but only with VTP version 3, does the controller propagate extended range VLAN configuration information. When extended range VLANs are created in VTP versions 1 and 2, their configuration information is not propagated. Even the local VTP database entries on the controller are not updated, but the extended range VLANs configuration information is created and stored in the running configuration file.

You can configure up to 4049 VLANs on the controller.

Related Topics

Creating or Modifying an Ethernet VLAN (CLI), on page 7
Deleting a VLAN (CLI), on page 10
Assigning Static-Access Ports to a VLAN (CLI), on page 13
Monitoring VLANs, on page 17
Creating an Extended-Range VLAN (CLI), on page 15
Creating an Extended-Range VLAN with an Internal VLAN ID

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. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the 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 controllers over trunk links.

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Dynamic access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VLAN Member Policy Server (VMPS). You can have dynamic-access ports and trunk ports on the same controller, but you must connect the dynamic-access port to an end station or hub and not to another controller.	VTP is required. Configure the VMPS and the client with the same VTP domain name. To participate in VTP, at least one trunk port on the controller must be connected to a trunk port of a second controller .
Voice VLAN	A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.	VTP is not required; it has no effect on a voice VLAN.

Related Topics

Assigning Static-Access Ports to a VLAN (CLI), on page 13
Monitoring VLANs, on page 17

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.
- From image 15.0(02)SE6, on vtp transparent and off modes, vlans get created from startup-config even if they are not applied to the interface.

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

Normal-range VLANs are VLANs with IDs from 1 to 1005.

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 numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- 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 controller 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.
- Before you can create a VLAN, the controller must be in VTP server mode or VTP transparent mode. If the controller is a VTP server, you must define a VTP domain or VTP will not function.
- The controller does not support Token Ring or FDDI media. The controller does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The controller supports 128 spanning tree instances. If a controller has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs.

  If you have already used all available spanning-tree instances on a controller, adding another VLAN anywhere in the VTP domain creates a VLAN on that controller that is not running spanning-tree. If you have the default allowed list on the trunk ports of that controller (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent controllers that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of controllers that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the controller exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your controller to map multiple VLANs to a single spanning-tree instance.

Related Topics

Creating or Modifying an Ethernet VLAN (CLI), on page 7
Monitoring VLANs, on page 17
Deleting a VLAN (CLI), on page 10
Assigning Static-Access Ports to a VLAN (CLI), on page 13

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

Related Topics

Creating an Extended-Range VLAN (CLI), on page 15
Monitoring VLANs, on page 17
Creating an Extended-Range VLAN with an Internal VLAN ID

Information About VLAN Groups

Whenever a client connects to a wireless network (WLAN), the client is placed in a VLAN that is associated with the WLAN. In a large venue, such as an auditorium, a stadium, or a conference room where there are numerous wireless clients, having only a single WLAN to accommodate many clients might be a challenge.

The VLAN Groups feature uses a single WLAN that can support multiple VLANs. The clients can get assigned to one of the configured VLANs. This feature maps a WLAN to a single VLAN or multiple VLANs using the VLAN groups. When a wireless client associates to the WLAN, the VLAN is derived by an algorithm based on the MAC address of the wireless client. A VLAN is assigned to the client and the client gets the IP address from the assigned VLAN. This feature also extends the current AP group architecture and AAA override architecture, where the AP groups and AAA override can override a VLAN or a VLAN group to which the WLAN is mapped.

The system marks VLAN as *Dirty* for 30 minutes when the clients are unable to receive IP addresses using DHCP. The system might not clear the *Dirty* flag from the VLAN even after 30 minutes for a VLAN group. After 30 minutes, when the VLAN is marked non-dirty, new clients in the IP Learn state can get assigned with IP addresses from the VLAN if free IPs are available in the pool and DHCP scope is defined correctly. This is the expected behavior because the timestamp of each interface has to be checked to see if it is greater than 30 minutes, due to which there is a lag of 5 minutes for the global timer to expire.

Related Topics

Creating a VLAN Group (CLI), on page 11

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
  - Fiber Distributed Data Interface [FDDI]
  - FDDI network entity title [NET]
  - TrBRF or TrCRF
  - Token Ring
  - Token Ring-Net
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type 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 (CLI)

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. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other controllers.

Although the controller does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported controllers. Controllers running VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

SUMMARY STEPS

1. **configure terminal**
2. **vlan** *vlan-id*

3. **name** *vlan-name*
4. **media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** }
5. **remote-span**
6. **end**
7. **show vlan** {**name** *vlan-name* | **id** *vlan-id*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	**vlan** *vlan-id* **Example:** `Controller(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. Additional **vlan** command options include: • **access-map**—Creates VLAN access-maps or enters the vlan access map command mode. • **configuration**—Enters the vlan feature configuration mode. • **dot1q**—Configures VLAN dot1q tag native parameters. • **filter**—Applies a VLAN filter map to a VLAN list. • **group**—Creates a VLAN group.
Step 3	**name** *vlan-name* **Example:** `Controller(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. The following additional VLAN configuration command options are available: • **are**—Sets the maximum number of All Router Explorer (ARE) hops for the VLAN. • **backupcrf**—Enables or disables the backup concentrator relay function (CRF) mode for the VLAN. • **bridge**—Sets the value of the bridge number for the FDDI net or Token Ring net type VLANs.

	Command or Action	Purpose
		• **exit**—Applies changes, bumps the revision number, and exits. • **media**—Sets the media type of the VLAN. • **no**—Negates the command or default. • **parent**—Sets the value of the ID for the parent VLAN for FDDI or Token Ring type VLANs. • **remote-span**—Configures a remote SPAN VLAN. • **ring**—Sets the ring number value for FDDI or Token Ring type VLANs. • **said**—Sets the IEEE 802.10 SAID value. • **shutdown**—Shuts down the VLAN switching. • **state**—Sets the operational VLAN state to active or suspended. • **ste**—Sets the maximum number of Spanning Tree Explorer (STE) hops for the VLAN. • **stp**—Sets the Spanning Tree characteristics of the VLAN.
Step 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } **Example:** `Controller(config-vlan)# media ethernet`	Configures the VLAN media type. Command options include: • **ethernet**—Sets the VLAN media type as Ethernet. • **fd-net**—Sets the VLAN media type as FDDI net. • **fddi**—Sets the VLAN media type as FDDI. • **tokenring**—Sets the VLAN media type as Token Ring. • **trn-net**—Sets the VLAN media type as Token Ring net.
Step 5	**remote-span** **Example:** `Controller(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see the *Catalyst 3850 Network Management Configuration Guide*. (Optional) Configures the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see the *Catalyst 3650 Network Management Configuration Guide*.
Step 6	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Controller(config)# end`	
Step 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*} **Example:** `Controller# show vlan name test20 id 20`	Verifies your entries.

Related Topics

Normal-Range VLAN Configuration Guidelines, on page 5
Monitoring VLANs, on page 17
Supported VLANs, on page 2

Deleting a VLAN (CLI)

When you delete a VLAN from a controller that is in VTP server mode, the VLAN is removed from the VLAN database for all controllers in the VTP domain. When you delete a VLAN from a controller that is in VTP transparent mode, the VLAN is deleted only on that specific controller .

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no vlan** *vlan-id*
4. **end**
5. **show vlan brief**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 3	**no vlan** *vlan-id* **Example:** `Controller(config)# no vlan 4`	Removes the VLAN by entering the VLAN ID.
Step 4	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vlan brief** **Example:** `Controller# show vlan brief`	Verifies the VLAN removal.
Step 6	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Monitoring VLANs, on page 17
Supported VLANs, on page 2
Normal-Range VLAN Configuration Guidelines, on page 5

Creating a VLAN Group (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **vlan group** *WORD* **vlan-list** *vlan-ID*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**vlan group** *WORD* **vlan-list** *vlan-ID* **Example:** `Controller(config)#vlan group vlangrp1 vlan-list 91-95`	Creates a VLAN group with the given group name (vlangrp1) and adds all the VLANs listed in the command. The VLAN list ranges from 1 to 4096 and the recommended number of VLANs in a group is 32.
Step 3	**end** **Example:** `Controller(config)#end`	Exits the global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit the global configuration mode.

Related Topics

Information About VLAN Groups, on page 6

Adding a VLAN Group to a WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *WORD number*
3. **client vlan** *WORD*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global command mode.
Step 2	**wlan** *WORD number* **Example:** `Controller(config)#wlan wlanname 512`	Enables the WLAN to map a VLAN group using an identifier. The WLAN identifier values range from 1 to 512.
Step 3	**client vlan** *WORD* **Example:** `Controller(config-wlan)#client vlan vlangrp1`	Maps the VLAN group to the WLAN by entering the VLAN identifier, VLAN group, or the VLAN name.
Step 4	**end** **Example:** `Controller(config-wlan)#end`	Exits global configuration mode and returns to privileged EXEC mode. Alternatively, press **CTRL-Z** to exit global configuration mode.

Assigning Static-Access Ports to a VLAN (CLI)

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 the Cisco Catalyst 9500 Series Switches, if you are assigning a port on a cluster member controller to a VLAN, first use the **rcommand** privileged EXEC command to log in to the cluster member switch.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode access**
5. **switchport access vlan** *vlan-id*
6. **end**
7. **show running-config interface** *interface-id*
8. **show interfaces** *interface-id* **switchport**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode
Step 3	**interface** *interface-id* **Example:** `Controller(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.
Step 4	**switchport mode access** **Example:** `Controller(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).

	Command or Action	Purpose
Step 5	**switchport access vlan** *vlan-id* **Example:** `Controller(config-if)# switchport access vlan 2`	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end** **Example:** `Controller(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id* **Example:** `Controller# show running-config interface gigabitethernet2/0/1`	Verifies the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Controller# show interfaces gigabitethernet2/0/1 switchport`	Verifies your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 9	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

VLAN Port Membership Modes, on page 3
Monitoring VLANs, on page 17
Supported VLANs, on page 2
Normal-Range VLAN Configuration Guidelines, on page 5

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.

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Creating an Extended-Range VLAN (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **exit**
6. **interface vlan**
7. **ip mtu** *mtu-size*
8. **end**
9. **show vlan id** *vlan-id*
10. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Controller> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.

Step 3	**vlan** *vlan-id*
	Example:
	`Controller(config)# vlan 2000`
	`Controller(config-vlan)#`
		Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.

Step 4	**remote-span** **Example:** `Controller(config-vlan)# remote-span`	(Optional) Configures the VLAN as the RSPAN VLAN.
Step 5	**exit** **Example:**	Returns to configuration mode.

	Command or Action	Purpose
	`Controller(config-vlan)# exit` `Controller(config)#`	

Step 6	**interface vlan**
	Example:
	`Controller(config)# interface vlan 200`
	`Controller(config-if)#`
		Enters the interface configuration mode for the selected VLAN.

Step 7	**ip mtu** *mtu-size*
	Example:
	`Controller(config-if)# ip mtu 1024`
	`Controller(config-if)#`
		(Optional) Modifies the VLAN by changing the MTU size. You can configure the MTU size between 68 to 1500 bytes.
		Note Although all VLAN commands appear in the CLI help, only the **ip mtu** *mtu-size* and **remote-span** commands are supported for extended-range VLANs.

Step 8	**end** **Example:** `Controller(config)# end`	Returns to privileged EXEC mode.
Step 9	**show vlan id** *vlan-id* **Example:** `Controller# show vlan id 2000`	Verifies that the VLAN has been created.
Step 10	**copy running-config startup-config** **Example:** `Controller# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Extended-Range VLAN Configuration Guidelines, on page 6
Monitoring VLANs, on page 17
Supported VLANs, on page 2

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** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	Displays parameters for all VLANs or the specified VLAN on the controller. The following command options are available: • **access-map**—Displays the VLAN access-maps. • **brief**—Displays VTP VLAN status in brief. • **dot1q**—Displays the dot1q parameters. • **filter**—Displays VLAN filter information. • **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. • **remote-span**–Displays the remote SPAN VLANs. • **summary**—Displays a summary of VLAN information.

Related Topics

Creating or Modifying an Ethernet VLAN (CLI), on page 7
Normal-Range VLAN Configuration Guidelines, on page 5
Deleting a VLAN (CLI), on page 10
Assigning Static-Access Ports to a VLAN (CLI), on page 13
VLAN Port Membership Modes, on page 3
Creating an Extended-Range VLAN (CLI), on page 15
Extended-Range VLAN Configuration Guidelines, on page 6
Supported VLANs, on page 2
Creating an Extended-Range VLAN with an Internal VLAN ID

Where to Go Next

After configuring VLANs, you can configure the following:

- VLAN groups

- VLAN groups
- VLAN Trunking Protocol (VTP)
- VLAN trunks
- Voice VLANs

Additional References

Related Documents

Related Topic	Document Title
CLI commands	*Layer 2/3 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)VLAN Command Reference (Catalyst 3650 Switches)*
VLAN access-maps	*Security Configuration Guide, Cisco IOS Release 3SE (Catalyst 3850 Switches)* *Security Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
Cisco Flexible NetFlow	*Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
IGMP Snooping	*IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *IP Multicast Routing Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
IPv6	*Catalyst 3850 IPv6 Configuration Guide, Release 3.2SE* *IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*
SPAN	*Network Management Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)* *Network Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Related Documents

Related Topic	Document Title
CLI commands	*VLAN Command Reference (Catalyst 3850 Switches) VLAN Command Reference (Cisco WLC 5700 Series)VLAN Command Reference (Catalyst 3650 Switches)*

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management
RFC 2021	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for VLANs

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced
Cisco IOS XE 3.3SE	VLAN GUI support.
Cisco IOS XE Everest 16.5.1a	This feature was introduced.