



Configuring VLANs

- [Finding Feature Information, on page 1](#)
- [Prerequisites for VLANs, on page 1](#)
- [Restrictions for VLANs, on page 2](#)
- [Information About VLANs, on page 2](#)
- [How to Configure VLANs, on page 5](#)
- [Monitoring VLANs, on page 12](#)
- [Where to Go Next, on page 13](#)
- [Additional References, on page 14](#)
- [Feature History and Information for VLANs, on page 15](#)

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.

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 device 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.
- Devices running the LAN Base feature set support only static routing on SVIs.
- A VLAN should be present in the device 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 device 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 device 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.
- 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 device 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 device supporting fallback bridging. In a device stack, VLANs can be formed with ports across the stack. 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 device is assigned manually on an interface-by-interface basis. When you assign device interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

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

Supported VLANs

The device 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 device 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 device are not updated, but the extended range VLANs configuration information is created and stored in the running configuration file.

You can configure up to 4094 VLANs on the device.

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 device 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 device or the device stack connected to a trunk port of a second device or device stack.
Trunk (IEEE 802.1Q) : <ul style="list-style-type: none"> • 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 devices over trunk links.
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.

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 device running configuration file.

In a device stack, the whole stack uses the same vlan.dat file and running configuration. On some devices, the vlan.dat file is stored in flash memory on the active device.

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 device, the device 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

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 device running configuration file.
- If the device 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 device must be in VTP server mode or VTP transparent mode. If the device is a VTP server, you must define a VTP domain or VTP will not function.
- The device does not support Token Ring or FDDI media. The device does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The device supports 128 spanning tree instances. If a device 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 device, adding another VLAN anywhere in the VTP domain creates a VLAN on that device that is not running spanning-tree. If you have the default allowed list on the trunk ports of that device (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 devices that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of devices that have used up their allocation of spanning-tree instances.

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

- When a device in a stack learns a new VLAN or deletes or modifies an existing VLAN (either through VTP over network ports or through the CLI), the VLAN information is communicated to all stack members.
- When a device joins a stack or when stacks merge, VTP information (the vlan.dat file) on the new devices will be consistent with the active device.

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.
- In a device stack, the whole stack uses the same running configuration and saved configuration, and extended-range VLAN information is shared across the stack.

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

Before you begin

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

The device 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 devices.

Although the device does not support Token Ring connections, a remote device with Token Ring connections could be managed from one of the supported devices. Devices 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: Device# configure terminal	Enters global configuration mode.
Step 2	vlan <i>vlan-id</i> 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.
Step 3	name <i>vlan-name</i> 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 <i>vlan-id</i> value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	media { ethernet fd-net fddi tokenring trn-net } Example: Device(config-vlan)# media ethernet	Configures the VLAN media type. Command options include: <ul style="list-style-type: none"> • 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: Device(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 <i>Catalyst 3650 Network Management Configuration Guide</i> .
Step 6	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 7	show vlan {name <i>vlan-name</i> id <i>vlan-id</i>} Example:	Verifies your entries.

	Command or Action	Purpose
	Device# <code>show vlan name test20 id 20</code>	

Deleting a VLAN

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

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: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	no vlan <i>vlan-id</i> Example: Device(config)# <code>no vlan 4</code>	Removes the VLAN by entering the VLAN ID.

	Command or Action	Purpose
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	show vlan brief Example: Device# show vlan brief	Verifies the VLAN removal.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

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).

If you are assigning a port on a cluster member device 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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode
Step 3	interface <i>interface-id</i> Example: Device(config)# <code>interface gigabitethernet2/0/1</code>	Enters the interface to be added to the VLAN.
Step 4	switchport mode access Example: Device(config-if)# <code>switchport mode access</code>	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 5	switchport access vlan <i>vlan-id</i> Example: Device(config-if)# <code>switchport access vlan 2</code>	Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	end Example: Device(config-if)# <code>end</code>	Returns to privileged EXEC mode.
Step 7	show running-config interface <i>interface-id</i> Example: Device# <code>show running-config interface gigabitethernet2/0/1</code>	Verifies the VLAN membership mode of the interface.
Step 8	show interfaces <i>interface-id</i> switchport Example: Device# <code>show interfaces gigabitethernet2/0/1 switchport</code>	Verifies your entries in the <i>Administrative Mode</i> and the <i>Access Mode VLAN</i> fields of the display.
Step 9	copy running-config startup-config Example: Device# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

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 device 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, private VLAN, and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

Creating an Extended-Range VLAN

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	vlan <i>vlan-id</i> Example: <pre>Device(config)# vlan 2000 Device(config-vlan)#</pre>	Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.
Step 4	remote-span Example:	(Optional) Configures the VLAN as the RSPAN VLAN.

	Command or Action	Purpose
	Device(config-vlan) # remote-span	
Step 5	exit Example: Device(config-vlan) # exit Device(config) #	Returns to configuration mode.
Step 6	end Example: Device(config) # end	Returns to privileged EXEC mode.
Step 7	show vlan id <i>vlan-id</i> Example: Device# show vlan id 2000	Verifies that the VLAN has been created.
Step 8	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring VLANs

Table 2: Privileged EXEC show Commands

Command	Purpose
show interfaces [vlan <i>vlan-id</i>]	Displays characteristics for all interfaces or for the specified VLAN configured on the device .

Command	Purpose
<pre>show vlan [access-map name brief dot1q { tag native } filter [access-map vlan] group [group-name name] id vlan-id ifindex mtu name name private-vlan remote-span summary]</pre>	<p>Displays parameters for all VLANs or the specified VLAN on the device. The following command options are available:</p> <ul style="list-style-type: none"> • 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. • private-vlan—Displays private VLAN information. • remote-span—Displays the remote SPAN VLANs. • summary—Displays a summary of VLAN information. <p>Note The private-vlan command option that appears in the device CLI is not supported.</p>

Where to Go Next

After configuring VLANs, you can configure the following:

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

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	<i>VLAN Command Reference (Catalyst 3650 Switches)</i> <i>Layer 2/3 Command Reference (Catalyst 3650 Switches)</i>
VLAN access-maps	<i>Security Configuration Guide (Catalyst 3650 Switches)</i> <i>Security Command Reference (Catalyst 3650 Switches)</i>
VLAN and Mobility Agents	<i>Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i>
Cisco Flexible NetFlow	<i>Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i> <i>Flexible Netflow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i>
IGMP Snooping	<i>IP Multicast Routing Command Reference (Catalyst 3650 Switches)</i> <i>IP Multicast Routing Configuration Guide (Catalyst 3650 Switches)</i>
IPv6	<i>IPv6 Configuration Guide (Catalyst 3650 Switches)</i> <i>IPv6 Command Reference (Catalyst 3650 Switches)</i>
SPAN	<i>Network Management Command Reference (Catalyst 3650 Switches)</i> <i>Network Management Configuration Guide (Catalyst 3650 Switches)</i>
Platform-independent configuration information	<i>Identity Based Networking Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)</i>

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 1573	Evolution of the Interfaces Group of MIB-II
RFC 1757	Remote Network Monitoring Management

Standard/RFC	Title
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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for VLANs

Release	Modification
Cisco IOS XE 3.3SE	VLAN GUI support.

