

Configure VLAN

A Virtual Local Area Network (VLAN) is a logical grouping that segments a network into smaller broadcast domains. VLANs allow you to separate network devices into distinct groups, even if those devices connect to the same physical switch or to different switches. This segmentation enhances network performance, security, and manageability.

- Feature History for VLAN, on page 1
- Prerequisites for VLANs, on page 2
- Restrictions for VLANs, on page 2
- Benefits of VLANs, on page 3
- Information about Voice VLAN, on page 3
- How to Configure VLANs, on page 7
- Monitoring VLANs, on page 13
- Where to Go Next, on page 14
- Additional References, on page 14

Feature History for VLAN

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	VLAN: VLAN feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	A VLAN on Cisco switches segments a physical switch into multiple logical broadcast domains by assigning ports to VLANs. This isolates traffic within each VLAN, enhancing security and reducing broadcast traffic. VLANs improve network management and require routing for inter-VLAN communication	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

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 template, which configures system resources to support the maximum number of unicast MAC addresses.
- 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:

- The number of Spanning Tree Protocol (STP) virtual ports in the per-VLAN spanning-tree (PVST) or rapid PVST mode is based on the number of trunks, multiplied by the number of active VLANs, plus the number of access ports.

  STP virtual ports = trunks * active VLANs on trunk + number of non-trunk ports.

  Consider the following examples:

  - If a switch has 40 trunk ports (100 active VLANs on each trunk) and 8 access ports, the number of STP virtual ports on this switch would be: 40 * 100 + 8 = 4,008.
  - If a switch has 8 trunk ports (200 active VLANs on each trunk) and 40 access ports, the number of STP virtual ports on this switch would be: 8 * 200 + 40 = 1,640

- The device supports IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.
- The interface VLAN already has an MAC address assigned by default. You can override the interface VLAN MAC address by using thee **mac-address** command. If this command is configured on a single SVI or router port that requires Layer 3 injected packets, all other SVIs or routed ports on the device also must be configured with the same first four most significant bits (4MSB) of the MAC address. For example, if you set the MAC address of any SVI to xxxx.yyyy.zzzz, set the MAC address of all other SVIs to start with xxxx.yyyy. If Layer 3 injected packets are not used, this restriction does not apply.



Note This applies to all Layer 3 ports, SVIs, and routed ports. This does not apply to GigabitEthernet0/0 port.

- Once a range of interfaces has been bundled, any VLAN interface configuration change must be done only on a port channel. Otherwise, the interfaces will get suspended.

VLAN has these restrictions and limitations when implementing VLANs:

- VLAN ID range: Standard Ethernet (802.1Q) supports VLAN IDs from 1 to 4094. Switches typically support a subset of these, with some IDs reserved for internal use.

- Default VLAN (VLAN 1) security: You cannot remove VLAN 1, and it carries control plane traffic. Therefore, avoid using it for user data or management traffic to minimize security risks, such as VLAN hopping attacks.
- Native VLAN mismatch: A common misconfiguration on trunk links occurs when the Native VLAN IDs do not match. This can lead to traffic misdirection or security vulnerabilities.
- VLAN hopping attacks: Although VLANs provide segmentation, misconfigurations (such as Native VLAN mismatch or Dynamic Trunking Protocol (DTP) vulnerabilities) can allow an attacker to send traffic to VLANs they are not authorized to access.
- Spanning Tree Protocol (STP) overhead: STP typically runs an instance per VLAN (PVST+ or Rapid PVST+). This can increase CPU and memory utilization on switches, especially in networks with many VLANs.
- Broadcast domain size: While VLANs reduce broadcast domains, a poorly designed VLAN with too many devices can still become a large broadcast domain, impacting performance.
- Inter-VLAN communication requires routing: VLANs provide Layer 2 isolation. Communication between different VLANs always requires a Layer 3 routing device. This means adding complexity and potential bottlenecks if not properly designed.
- Management complexity: As the number of VLANs and inter-VLAN routing rules grows, network design and troubleshooting can become more complex.
- Traffic prioritization: While Voice VLANs help, effective QoS across the network requires careful planning and configuration beyond just VLAN assignment.

Benefits of VLANs

VLANs offer several advantages for network design and operation:

- Reduced broadcast domains: Each VLAN operates as its own broadcast domain, which limits the scope of broadcast traffic and reduces network congestion.
- Enhanced security: Devices in one VLAN cannot directly communicate with devices in another VLAN without a Layer 3 routing device. This provides isolation and improves security.
- Improved performance: By reducing broadcast traffic and segmenting the network, VLANs contribute to better overall network performance.
- Simplified network management: VLANs enable flexible network design. This makes it easier to manage and reorganize network resources without extensive recabling.

Information about Voice VLAN



Note Voice VLAN is not supported on Cisco C9550 Series Smart Switches and Cisco C9610 Series Smart Switches.

These sections provide information about Voice VLAN:

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. 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.

By default, VTP versions 1 and 2 support 20 characters for the VLAN name. VTP version 3 supports 128 characters.

Types of VLAN

VLANs are categorized based on their common use cases:

- Data VLAN: Carries ordinary user-generated network traffic, such as web browsing, file transfers, and email. This is the most common type of VLAN.
- Voice VLAN: Specifically carries Voice over IP (VoIP) traffic for IP phones. You can prioritize voice traffic using Quality of Service (QoS) mechanisms to ensure clear communication. IP phones often include a mini-switch that allows a PC to connect through the phone. The phone's traffic goes into the Voice VLAN, and the PC's traffic goes into a Data VLAN.
- Management VLAN: Provides a dedicated path for network device management traffic, such as accessing switches and routers via Telnet, SSH, SNMP, or a web interface. Separating management traffic enhances security and ensures management access even during high network utilization.
- Native VLAN: On a trunk link, the Native VLAN is the VLAN whose traffic is sent untagged. All other VLANs' traffic on the trunk link is typically sent with a VLAN tag (e.g., 802.1Q tag). Ensure that the Native VLAN ID matches on both ends of a trunk link to avoid connectivity issues and security vulnerabilities. By default, VLAN 1 is often the Native VLAN.
- Default VLAN (VLAN 1): On Cisco switches, VLAN 1 is the factory-default VLAN. All switch ports are initially members of VLAN 1. You cannot delete or rename VLAN 1. It typically carries control plane traffic (like CDP, STP, VTP) by default. It is a common security practice to avoid using VLAN 1 for user data.

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) : • 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.)
- 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.
- 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.

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.

How to Configure VLANs

The following sections provide information about configuring Normal-Range VLANs and Extended-Range 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

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 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** *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. **Note** By default, VTP versions 1 and 2 support 20 characters for the VLAN name. VTP version 3 supports 128 characters.

	Command or Action	Purpose
Step 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } **Example:** `Device(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	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Step 7	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}
	Example:
	`Device# show vlan name test20`
	`or`
	`Device# show vlan id 20`
		Verifies your entries.

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 .

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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no vlan** *vlan-id* **Example:** `Device(config)# no vlan 4`	Removes the VLAN by entering the VLAN ID.
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 assign an interface to a VLAN that does not exist, the new VLAN is created. In case of interface templates, make sure to create the VLAN explicitly before applying the command via templates.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Enters the interface to be added to the VLAN.
Step 4	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Defines the VLAN membership mode for the port (Layer 2 access port).
Step 5	**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 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id* **Example:** `Device# show running-config interface gigabitethernet2/0/1`	Verifies the VLAN membership mode of the interface.

	Command or Action	Purpose
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Device# 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:** `Device# copy running-config startup-config`	(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.

Creating an Extended-Range VLAN

Procedure

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

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

	Command or Action	Purpose

Step 4	**exit**
	Example:
	`Device(config-vlan)# exit`
	`Device(config)#`
		Returns to configuration mode.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vlan id** *vlan-id* **Example:** `Device# show vlan id 2000`	Verifies that the VLAN has been created.
Step 7	**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** *vlan-id*]	Displays characteristics for all interfaces or for the specified VLAN configured on the device .

Command	Purpose
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**]	Displays parameters for all VLANs or the specified VLAN on the device. 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. • **private-vlan**—Displays private VLAN information. • **remote-span**–Displays the remote SPAN VLANs. • **summary**—Displays a summary of VLAN information.

Where to Go Next

After configuring VLANs, you can configure the following:

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

Additional References

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