Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 3-16.

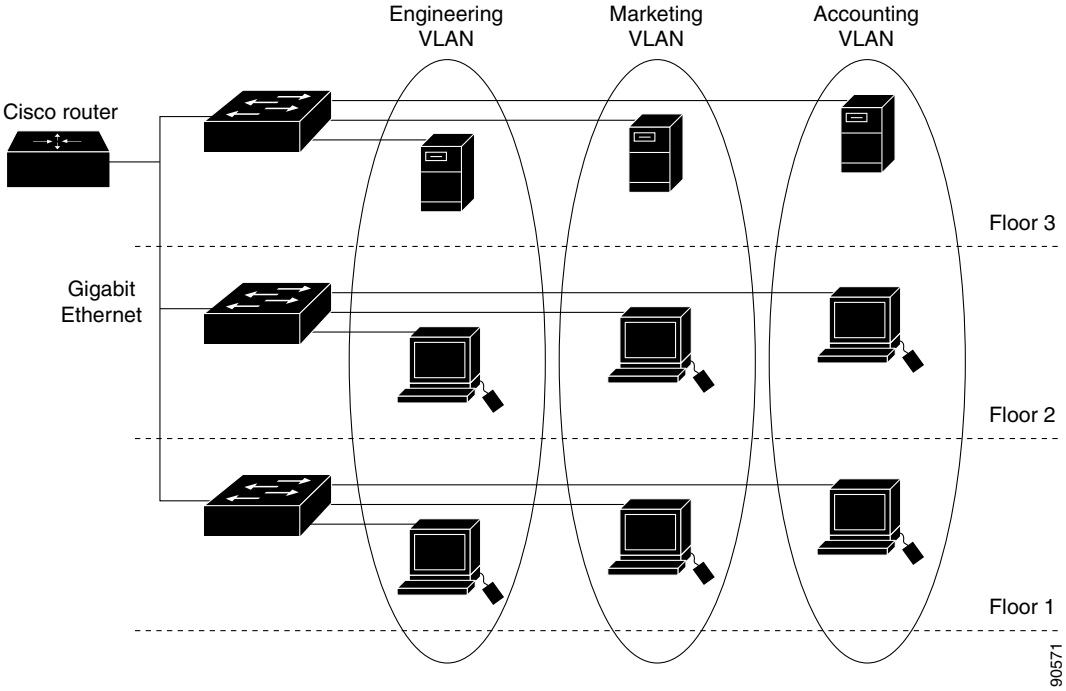
This chapter includes the following sections:

Information About VLANs

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 switch 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, as shown in Figure 3-1. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree. (See Chapter 11, "Configuring STP.")

Figure 3-1 shows an example of VLANs segmented into logically defined networks.

Figure 3-1 VLANs as Logically Defined Networks



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 switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed. Switches that are running the IP services image can route traffic between VLANs by using switch virtual interfaces (SVIs). To route traffic between VLANs, an SVI must be explicitly configured and assigned an IP address. For more information, see the "Switch Virtual Interfaces" section and the "Configuring Layer 3 Interfaces" section in the *Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

This section includes the following topics:

Supported VLANs

VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware.

The switch supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

Note Network node interfaces (NNIs) support STP by default. Enhanced network interfaces (ENIs) can be configured to support STP. User network interfaces (UNIs) do not support STP and by default are always in a forwarding state.

See the "Guidelines and Limitations" section on page 3-7 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. 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.)

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in flash memory.

Caution You can cause inconsistency in the VLAN database if you try to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release.

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)

Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- 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
- Private VLAN. Configure the VLAN as a primary or secondary private VLAN. For information about private VLANs, see Chapter 7, "Configuring Private VLANs."
- Remote SPAN VLAN. Configure the VLAN as the Remote Switched Port Analyzer (RSPAN) VLAN for a remote SPAN session. For more information on remote SPAN, see the "Configuring SPAN and RSPAN" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
- UNI-ENI VLAN configuration

For extended-range VLANs, you can configure only MTU, private VLAN, remote SPAN VLAN, and UNI-ENI VLAN parameters.

Note This chapter does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the documents listed in the "Related Documents" section on page 3-16.

Extended-Range VLANs

You can create extended-range VLANs (in the range 1006 to 4094) to 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. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch supports 4094 VLAN IDs, the actual number of VLANs supported is 1005.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic that the port carries and the number of VLANs to which it can belong. Table 3-1 lists the membership modes and characteristics.

Table 3-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 3-11.
Trunk (802.1Q)	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. For information about configuring trunk ports, see the "Configuring VLAN Trunks" section on page 4-3.

Table 3-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Dynamic-access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a Cisco Connected Grid switch. The Cisco Connected Grid switch is a VMPS client. See Chapter 6, "Configuring VMPS." **Note** Only UNIs or ENIs can be dynamic-access ports. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch. For configuration information, see the "Configuring Dynamic-Access Ports on VMPS Clients" section on page 6-57.
Private VLAN	A private VLAN port is a host or promiscuous port that belongs to a primary or secondary private VLAN. Only NNIs can be configured as promiscuous ports. For information about private VLANs, see Chapter 7, "Configuring Private VLANs."
Tunnel (**dot1q-tunnel**)	Tunnel ports are used for 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch in the service-provider network and connect it to an 802.1Q trunk port on a customer interface, creating an assymetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling. For more information about tunnel ports, see Chapter 10, "Configuring Layer 2 Protocol Tunneling."

For more detailed definitions of access and trunk modes and their functions, see Table 4-1 in Chapter 4, "Configuring VLAN Trunks."

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Table" section of the "Administering the Switch" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

UNI-ENI VLANs

The switch is the boundary between customer networks and the service-provider network, with user network interfaces (UNIs) and enhanced network interfaces (ENIs) connected to the customer side of the network. When customer traffic enters or leaves the service-provider network, the customer VLAN ID must be isolated from other customers' VLAN IDs. You can achieve this isolation by several methods, including using private VLANs. On the switch, this isolation occurs by default by using UNI-ENI VLANs.

There are two types of UNI-ENI VLANs:

- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch. Local switching does not occur among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN. This configuration is designed for cases when different customers are connected to UNIs or ENIs on the same switch. However, switching is allowed among UNIs or ENIs on different switches even though they belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch that belong to the same community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch packets between the ports, you can configure the common VLAN as a UNI-ENI

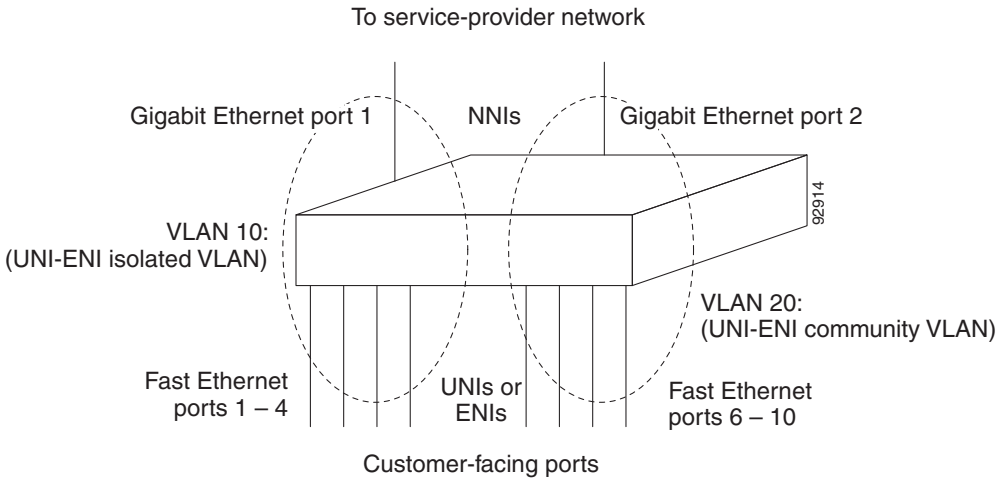
community VLAN. There is no local switching between the ports in a UNI-ENI community VLAN and ports outside of the VLAN. The switch supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN.

Note Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

Network node interfaces (NNIs) are not affected by the type of UNI-ENI VLAN to which they belong. Switching can occur between NNIs and other NNIs or UNIs or ENIs on the switch or other switches that are part of the same VLAN, regardless of VLAN type.

In the configuration in Figure 3-2, if VLAN 10 is a UNI-ENI isolated VLAN and VLAN 20 is a UNI-ENI community VLAN, local switching does not take place among Fast Ethernet ports 1–4, but local switching can occur between Fast Ethernet ports 6–10. The NNIs in both VLAN 10 and VLAN 20 can exchange packets with the UNIs or ENIs in the same VLAN.

Figure 3-2 UNI-ENI Isolated and Community VLANs in the Switch



A UNI or ENI can be an access port, a trunk port, a private VLAN port, or an 802.1Q tunnel port. It can also be a member of an EtherChannel.

When a UNI or ENI configured as an 802.1Q trunk port belongs to a UNI-ENI isolated VLAN, the VLAN on the trunk is isolated from the same VLAN ID on a different trunk port or an access port. Other VLANs on the trunk port can be of different types (private VLAN, UNI-ENI community VLAN, and so on). For example, a UNI access port and one VLAN on a UNI trunk port can belong to the same UNI-ENI isolated VLAN. In this case, isolation occurs between the UNI access port and the VLAN on the UNI trunk port. Other access ports and other VLANs on the trunk port are isolated because they belong to different VLANs.

UNIs, ENIs, and NNIs are always isolated from ports on different VLANs.

Prerequisites

- Be familiar with the information in the "Information About VLANs" section on page 3-1 and "Guidelines and Limitations" section on page 3-7.
- Ensure that your network strategy and planning for your network are complete.

Guidelines and Limitations

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

- The switch supports 1005 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database and in the switch running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU, RSPAN VLAN, private VLAN, and UNI-ENI VLAN. Extended-range VLANs are not saved in the VLAN database.
- Spanning Tree Protocol (STP) is enabled by default for only NNIs on all VLANs. You can configure STP on ENIs. NNIs and ENIs in the same VLAN are in the same spanning-tree instance. The switch supports 128 spanning-tree instances. If a switch 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 switch, adding another VLAN creates a VLAN on that switch that is not running spanning tree. If you have the default allowed list on the trunk ports of that switch (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 switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

  If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance. For more information about MSTP, see Chapter 12, "Configuring MSTP."

  Note MSTP is supported only on NNIs on ENIs on which STP has been enabled.

- Each routed port on the switch creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.

  - Before configuring extended-range VLANs, enter the **show vlan internal usage** privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the "Creating an Extended-Range VLAN with an Internal VLAN ID" section on page 3-12.
- Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

UNI-ENI VLAN

These are the guidelines for UNI-ENI VLAN configuration:

- UNI-ENI isolated VLANs have no effect on NNI ports.
- A UNI-ENI community VLAN is like a traditional VLAN except that it can include no more than a combination of eight UNIs and ENIs.
- To change a VLAN type, first enter the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode:
  - To change a VLAN from UNI-ENI isolated VLAN to a private VLAN, enter the **private-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **private-vlan** VLAN configuration command.
  - To change a VLAN from a UNI-ENI isolated VLAN to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **rspan-vlan** VLAN configuration command.
  - To change a private VLAN to a UNI-ENI VLAN, you must first remove the private VLAN type by entering the **no private-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command.
  - To change an RSPAN VLAN to a UNI-ENI VLAN, you must first remove the RSPAN VLAN type by entering the **no rspan-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command
- The switch supports a total of eight UNIs and ENIs in a community VLAN. You cannot configure a VLAN as a UNI-ENI community VLAN if more than eight UNIs and ENIs belong to the VLAN.
- If you attempt to add a UNI or ENI static-access port to a UNI-ENI community VLAN that has a combination of eight UNIs and ENIs, the configuration is refused. If a UNI or ENI dynamic access port is added to a UNI-ENI community VLAN that has eight UNIs or ENIs, the port is error-disabled.
- Use caution when configuring ENIs and UNIs in the same community VLAN. Local switching takes place between the ENIs and UNIs in the community VLAN and ENIs can support spanning tree while UNIs do not.

Default Settings

The switch supports only Ethernet interfaces. The following table shows the default configuration for Ethernet VLANs.

Note On extended-range VLANs, you can change only the MTU size, the private VLAN, the remote SPAN, and the UNI-ENI VLAN configuration. All other characteristics must remain at the default conditions.

Parameter	Default	Range
VLAN ID	1	1 to 4094 **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1 to 4294967294
MTU size	1500	1500 to 9198
Translational bridge 1	0	0 to 1005
Translational bridge 2	0	0 to 1005
VLAN state	active	active, suspend
Remote SPAN	disabled	enabled, disabled
Private VLANs	none configured	2 to 1001, 1006 to 4094
UNI-ENI VLAN	UNI-ENI isolated VLAN	2 to 1001, 1006 to 4094 VLAN 1 is always a UNI-ENI isolated VLAN.

Configuring VLANs

You use VLAN configuration mode, accessed by entering the **vlan** global configuration command, to create VLANs and to modify some parameters. 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.

This section includes the following topics:

For more efficient management of the MAC address table space available on the switch, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the "Disabling MAC Address Learning on a VLAN" section of the "Administering the Switch" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches* for more information.

Creating or Modifying an Ethernet VLAN

To access VLAN configuration mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration (see the "Default Settings" section on page 3-9) or enter commands to configure the VLAN.

Note Extended-range VLANs use the default Ethernet VLAN characteristics and the MTU, the private VLAN, the RSPAN, and the UNI-ENI VLAN configurations are the only parameters you can change.

For more information about commands available in this mode, see the **vlan** command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file) with a VLAN number and name and in the switch running configuration file. Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the VLAN configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

BEFORE YOU BEGIN

Before you create an extended-range VLAN, verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to release it, go to the "Creating an Extended-Range VLAN with an Internal VLAN ID" section on page 3-12 before creating the extended-range VLAN.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. The available VLAN ID range for this command is 1 to 4094. **Note** When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN.

	Command	Purpose
Step 3	**name** *vlan-name*	(Optional and supported on normal-range VLANs only) Enter a name for the VLAN. If no name is entered for the VLAN, the default in the VLAN database is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries. The **name** option is only valid for VLAN IDs 1 to 1005.
Step 7	**copy running-config startup config**	(Optional) Save the configuration in the switch startup configuration file.

To delete a VLAN, use the **no vlan** *vlan-id* global configuration command. You cannot delete VLAN 1 or 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.

To return the VLAN name to the default settings, use the **no name** or **no mtu** VLAN configuration command.

EXAMPLE

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN.

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 3-10.)

BEFORE YOU BEGIN

Review the "Information About VLANs" section on page 3-1 and "Guidelines and Limitations" section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface to add to the VLAN.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 5	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 8	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

EXAMPLE

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

Creating an Extended-Range VLAN with an Internal VLAN ID

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message appears, and the extended-range VLAN is rejected. To manually release an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**show vlan internal usage**	Display the VLAN IDs being used internally by the switch. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**interface** *interface-id*	Specify the interface ID for the routed port that is using the VLAN ID, and enter interface configuration mode.
Step 4	**shutdown**	Shut down the port to release the internal VLAN ID.
Step 5	**exit**	Return to global configuration mode.
Step 6	**vlan** *vlan-id*	Enter the new extended-range VLAN ID, and enter config-vlan mode.
Step 7	**exit**	Exit from config-vlan mode, and return to global configuration mode.
Step 8	**interface** *interface-id*	Specify the interface ID for the routed port that you shut down in Step 4, and enter interface configuration mode.
Step 9	**no shutdown**	Re-enable the routed port. It will be assigned a new internal VLAN ID.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to release internal VLAN ID 1030:

```
Switch# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# vlan 1030
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# no shutdown
Switch(config-if)# end
```

Configuring UNI-ENI VLANs

By default, every VLAN configured on the switch is a UNI-ENI isolated VLAN. You can change VLAN configuration to that of a UNI-ENI community VLAN, a private VLAN, or an RSPAN VLAN. You can also change the configuration of one of these VLANs to the default of a UNI-ENI isolated VLAN.

For procedures for configuring private VLANs or RSPAN VLANs, see Chapter 7, "Configuring Private VLANs" and the "Configuring SPAN and RSPAN" chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

BEFORE YOU BEGIN

Review the "UNI-ENI VLANs" section on page 3-5 and the UNI-ENI VLAN configuration guidelines in the "Guidelines and Limitations" section on page 3-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. By default, the VLAN is a UNI-ENI isolated VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.
Step 3	**uni-vlan** {**community** | **isolated**}	Configure the UNI-ENI VLAN type. • Enter **community** to change from the default to a UNI-ENI community VLAN. • Enter **isolated** to return to the default UNI-ENI isolated VLAN. **Note** VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs 1002 to 1005 are not Ethernet VLANs.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vlan uni-vlan** [**type**]	Display UNI-ENI VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI-ENI VLAN.
Step 6	**copy running-config startup config**	(Optional) Save the configuration in the switch startup configuration file.

Use the **no uni-vlan** VLAN configuration command to return to the default (UNI-ENI isolated VLAN). Entering **uni-vlan isolated** command has the same effect as entering the no **uni-vlan** VLAN configuration command. The **show vlan** and **show vlan** *vlan-id* privileged EXEC commands also display UNI-ENI VLAN information, but only UNI-ENI community VLANs appear. To display both isolated and community VLANs, use the **show vlan uni-vlan type** command.

EXAMPLE

This example configures VLAN 20 as a community VLAN:

```
Switch(config)# vlan 20
Switch (config-vlan)# uni-vlan community
Switch (config-vlan)# end
```

Verifying Configuration

Command	Purpose
show interfaces [**vlan** *vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show vlan [**id** *vlan-id*]	Display parameters for all VLANs or the specified VLAN on the switch.
show vlan [*vlan-name*] **uni-vlan type**	Display UNI-ENI isolated or UNI-ENI community VLANs by VLAN name.
show vlan uni-vlan	Display UNI-ENI community VLANs and associated ports on the switch.
show vlan uni-vlan type	Display UNI-ENI isolated and UNI-ENI community VLANs on the switch by VLAN ID.

Configuration Example

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

This example shows how to release internal VLAN ID 1030:

```
Switch# show vlan internal usage

VLAN Usage
---- --------------------
1025 -
1026 -
1027 -
1028 -
```

```
1029 Port-channel6
1030 GigabitEthernet1/2
1032 FastEthernet3/20
1033 FastEthernet3/21
1129 -
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# shutdown
Switch(config-if)# exit
Switch(config)# vlan 1030
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet1/2
Switch(config-if)# no shutdown
Switch(config-if)# end
```

This example configures VLAN 20 as a community VLAN:

```
Switch(config)# vlan 20
Switch (config-vlan)# uni-vlan community
Switch (config-vlan)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS LAN Switching Command Reference
- Cisco IOS Interface and Hardware Component Command Reference
- Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 Switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX