



## Configuring VLANs

---

This chapter describes how to configure Ethernet, Token Ring, and private VLANs on the Catalyst 6000 family switches.



**Note**

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family Command Reference* publication.

---



**Note**

---

The Catalyst 6000 family switch 10/100 Ethernet switching modules support auxiliary VLANs. You can plug an externally powered IP phone into a 10/100 port and then add that port to an auxiliary VLAN using the **set port auxiliaryvlan** command. For complete details on configuring auxiliary VLANs, see Chapter 36, “Configuring a Voice-over-IP Network.”

---

This chapter consists of these sections:

- Configuring Ethernet and Token Ring VLANs, page 9-1
- Configuring Private VLANs, page 9-14

## Configuring Ethernet and Token Ring VLANs

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

These sections describe how VLANs work:

- Understanding VLANs in a VTP Domain, page 9-2
- Understanding Token Ring VLANs, page 9-3
- VLAN Default Configuration, page 9-6
- VLAN Configuration Guidelines, page 9-6
- Configuring Ethernet and Token Ring VLANs, page 9-7

## Understanding VLANs in a VTP Domain

VLANs allow you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out other ports belonging to that VLAN.

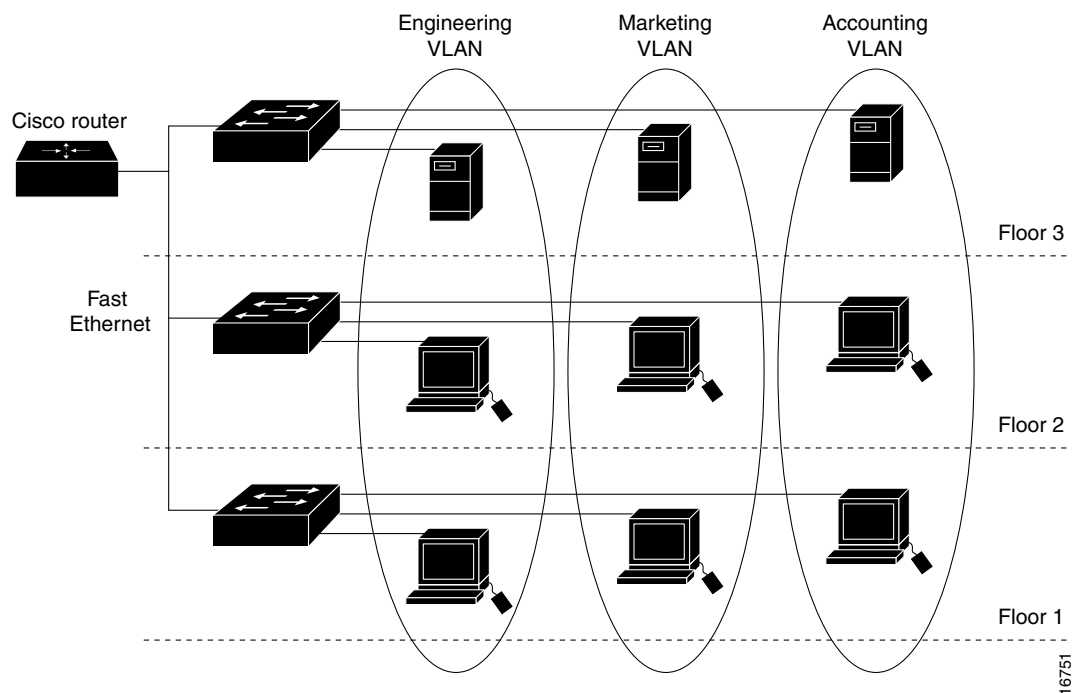


### Note

Before you create VLANs, you must decide whether to use VTP to maintain global VLAN configuration information for your network. For complete information on VTP, see Chapter 8, “Configuring VTP.”

Figure 9-1 shows an example of VLANs segmented into logically defined networks.

**Figure 9-1** 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. Traffic between VLANs must be routed. Port VLAN membership on the switch is assigned manually on a port-by-port basis. When you assign switch ports to VLANs using this method, it is known as port-based, or static, VLAN membership.

The in-band (sc0) interface of a switch can be assigned to any VLAN, so you can access another switch on the same VLAN directly without a router. Only one IP address at a time can be assigned to the in-band interface. If you change the IP address and assign the interface to a different VLAN, the previous IP address and VLAN assignment are overwritten.

You can set these parameters when you create a VLAN in the management domain:

- VLAN number
- VLAN name
- VLAN type (Ethernet, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF)
- 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

**Note**

When translating from one VLAN type to another, the switch software requires a different VLAN number for each media type.

## Understanding Token Ring VLANs

Two Token Ring VLAN types are supported on switches running VTP version 2:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

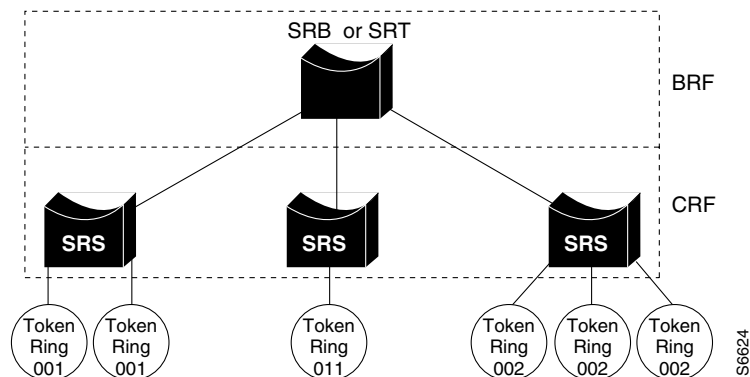
**Note**

Catalyst 6000 family switches do not support ISL-encapsulated Token Ring frames.

### Token Ring TrBRF VLANs

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see Figure 9-2). The TrBRF can be extended across a network of switches interconnected via trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

**Figure 9-2 Interconnected Token Ring TrBRF and TrCRF VLANs**



For source routing, the switch appears as a single bridge between the logical rings. The TrBRF can function as a source-route bridge (SRB) or source-route transparent (SRT) bridge running either the IBM or IEEE STP. If SRB is used, you can define duplicate MAC addresses on different logical rings.

The Token Ring software runs an instance of STP for each TrBRF VLAN and each TrCRF VLAN. For TrCRF VLANs, STP removes loops in the logical ring. For TrBRF VLANs, STP interacts with external bridges to remove loops from the bridge topology, similar to STP operation on Ethernet VLANs.

**Caution**

Certain parent TrBRF STP and TrCRF bridge mode configurations can place the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF in a blocked state. For more information, see the “VLAN Configuration Guidelines” section on page 9-6.

For source routing, the switch appears as a single bridge between the logical rings. The TrBRF can function as an SRB or SRT bridge running either the IBM or IEEE STP. If SRB is used, duplicate MAC addresses can be defined on different logical rings.

To accommodate IBM System Network Architecture (SNA) traffic, you can use a combination of SRT and SRB modes. In a mixed mode, the TrBRF considers some ports (logical ports connected to TrCRFs) to operate in SRB mode while others operate in SRT mode.

## Token Ring TrCRF VLANs

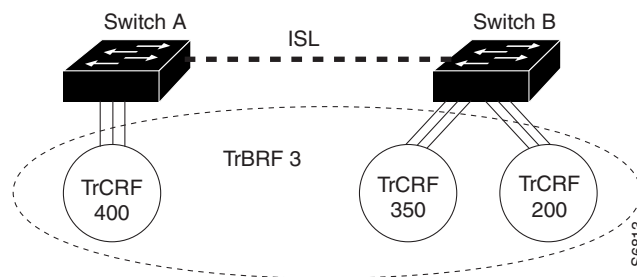
Token Ring Concentrator Relay Function (TrCRF) VLANs define port groups with the same logical ring number. You can configure two types of TrCRFs in your network: undistributed and backup.

Typically, TrCRFs are undistributed, which means each TrCRF is limited to the ports on a single switch. Multiple undistributed TrCRFs on the same or separate switches can be associated with a single parent TrBRF (see Figure 9-3). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

**Note**

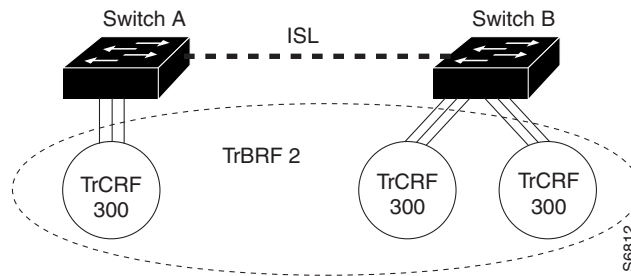
To pass data between rings located on separate switches, you can associate the rings to the same TrBRF and configure the TrBRF for SRB.

**Figure 9-3 Undistributed TrCRFs**

**Note**

By default, Token Ring ports are associated with the default TrCRF (VLAN 1003, trcrf-default), which has the default TrBRF (VLAN 1005, trbrf-default) as its parent. In this configuration, a distributed TrCRF is possible (see Figure 9-4), and traffic is passed between the default TrCRFs located on separate switches provided that the switches are connected through an ISL trunk.

Figure 9-4 Distributed TrCRF



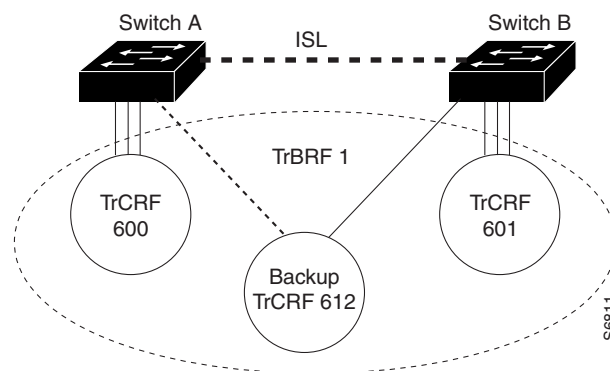
Within a TrCRF, source-route switching forwards frames based on either MAC addresses or route descriptors. The entire VLAN can operate as a single ring, with frames switched between ports within a single TrCRF.

You can specify the maximum hop count for All-Routes and Spanning-Tree Explorer frames for each TrCRF. This limits the maximum number of hops an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of hops specified, it does not forward the frame. The TrCRF determines the number of hops an explorer has traversed based on the number of bridge hops in the route information field.

A backup TrCRF enables you to configure an alternate route for traffic between undistributed TrCRFs located on separate switches that are connected by a TrBRF, in the event that the ISL connection between the switches fails. Only one backup TrCRF for a TrBRF is allowed, and only one port per switch can belong to a backup TrCRF.

If the ISL connection between the switches fails, the port in the backup TrCRF on each affected switch automatically becomes active, rerouting traffic between the undistributed TrCRFs through the backup TrCRF. When the ISL connection is reestablished, all but one port in the backup TrCRF is disabled. Figure 9-5 illustrates the backup TrCRF.

Figure 9-5 Backup TrCRF



## VLAN Default Configuration

Table 9-1 shows the default VLAN configuration.

**Table 9-1** VLAN Default Configuration

Feature	Default Value
Native (default) VLAN	VLAN 1
Port VLAN assignments	All ports assigned to VLAN 1 Token Ring ports assigned to VLAN 1003 (trcrf-default)
VLAN state	Enabled
MTU size	1500 bytes 4472 bytes for Token Ring VLANs
SAID value	100,000 plus the VLAN number (for example, the SAID for VLAN 3 is 100003)
Pruning eligibility	VLANs 2–1000 are pruning eligible
Default FDDI VLAN	VLAN 1002
Default FDDI NET VLAN	VLAN 1004
Default Token Ring TrBRF VLAN	VLAN 1005 (trbrf-default) with bridge number 0F
Default Token Ring TrCRF VLAN	VLAN 1003 (trcrf-default)
TrBRF STP	IBM
TrCRF bridge mode	SRB

## VLAN Configuration Guidelines

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

- A maximum of 1000 VLANs can be active at any time.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain. For information on configuring VTP, see Chapter 8, “Configuring VTP.”
- The default TrBRF (VLAN 1005) can only be the parent of the default TrCRF (VLAN 1003). You cannot specify the default TrBRF as the parent of a user-configured TrCRF.
- You must configure a TrBRF before you configure the TrCRF (the parent TrBRF VLAN you specify must exist).
- In a Token Ring environment, the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF are placed in a blocked state if either of these conditions exists:
  - The TrBRF is running the IBM STP, and the TrCRF is in SRT mode.
  - The TrBRF is running the IEEE STP, and the TrCRF is in SRB mode.

## Configuring Ethernet and Token Ring VLANs



### Note

VLANs support a number of parameters that are not discussed in detail in this section. For complete information on the **set vlan** command and its parameters, refer to the *Catalyst 6000 Family Command Reference* publication.

These sections describe how to configure VLANs:

- Creating or Modifying an Ethernet VLAN, page 9-7
- Creating or Modifying an FDDI VLAN, page 9-8
- Creating or Modifying a Token Ring TrBRF VLAN, page 9-8
- Creating or Modifying a Token Ring TrCRF VLAN, page 9-9
- Assigning Switch Ports to a VLAN, page 9-11
- Mapping 802.1Q VLANs to ISL VLANs, page 9-12
- Clearing 802.1Q-to-ISL VLAN Mappings, page 9-13
- Deleting a VLAN, page 9-13

### Creating or Modifying an Ethernet VLAN

To create a new Ethernet VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Create a new Ethernet VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan_num</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]



### Note

The default VLAN type is Ethernet; if you do not specify the VLAN type, the VLAN is an Ethernet VLAN.

This example shows how to create an Ethernet VLAN and verify the configuration:

```

Console> (enable) set vlan 500 name Engineering
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name                Status      IfIndex Mod/Ports, Vlans
-----
500 Engineering          active     344
VLAN Type  SAID      MTU   Parent RingNo BrdgNo  Stp   BrdgMode Trans1 Trans2
-----
500 enet  100500   1500  -     -     -     -     -     0     0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

To modify the VLAN parameters on an existing Ethernet VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Modify an existing Ethernet VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>translation</b> <i>vlan_num</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

## Creating or Modifying an FDDI VLAN

To create a new FDDI VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Create a new FDDI or FDDI NET-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] <b>type</b> { <b>fdi</b>   <b>fdinet</b> } [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

To modify the VLAN parameters on an existing FDDI VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Modify an existing FDDI or FDDI NET-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

## Creating or Modifying a Token Ring TrBRF VLAN



### Note

You must enable VTP version 2 before you create Token Ring VLANs. For information on enabling VTP version 2, see Chapter 8, “Configuring VTP.”

To create a new Token Ring TrBRF VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Create a new Token Ring TrBRF-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] <b>type</b> <b>trbrf</b> [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] <b>bridge</b> <i>bridge_number</i> [ <b>stp</b> { <b>ieee</b>   <b>ibm</b> }]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]



### Note

You must specify a bridge number when creating a new TrBRF.

This example shows how to create a new Token Ring TrBRF VLAN and verify the configuration:

```

Console> (enable) set vlan 999 name TrBRF_999 type trbrf bridge a
Vlan 999 configuration successful
Console> (enable) show vlan 999
VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
999 TrBRF_999              active
VLAN Type SAID          MTU    Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
999 trbrf 100999      4472  -      -      0xa   ibm  -      0      0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

To modify the VLAN parameters on an existing Token Ring TrBRF VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Modify an existing Token Ring TrBRF-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>bridge</b> <i>bridge_number</i> ] [ <b>stp</b> { <b>ieee</b>   <b>ibm</b> }]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

## Creating or Modifying a Token Ring TrCRF VLAN



**Note** You must enable VTP version 2 before you create Token Ring VLANs. For information on enabling VTP version 2, see Chapter 8, “Configuring VTP.”

To create a new Token Ring TrCRF VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Create a new Token Ring TrCRF-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] <b>type</b> <b>trcrf</b> [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] { <b>ring</b> <i>hex_ring_number</i>   <b>decring</b> <i>decimal_ring_number</i> } [ <b>parent</b> <i>vlan_num</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]



**Note** You must specify a ring number (either in hexadecimal or in decimal) and a parent TrBRF VLAN when creating a new TrCRF.

This example shows how to create a Token Ring TrCRF VLAN and verify the configuration:

```

Console> (enable) set vlan 998 name TrCRF_998 type trcrf decring 10 parent 999
Vlan 998 configuration successful
Console> (enable) show vlan 998
VLAN Name                Status      IfIndex Mod/Ports, Vlans
-----
998 TrCRF_998              active     352
VLAN Type SAID      MTU   Parent RingNo BrdgNo Stp   BrdgMode Trans1 Trans2
-----
998 trcrf 100998 4472 999   0xa   -     -    srb      0      0
VLAN AREHops STEHops Backup CRF
-----
998 7      7      off
Console> (enable)

```

To modify the VLAN parameters on an existing Token Ring TrCRF VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Modify an existing Token Ring TrCRF-type VLAN.	<b>set vlan</b> <i>vlan_num</i> [ <b>name</b> <i>name</i> ] [ <b>state</b> { <b>active</b>   <b>suspend</b> }] [ <b>said</b> <i>said</i> ] [ <b>mtu</b> <i>mtu</i> ] [ <b>ring</b> <i>hex_ring_num</i> ] [ <b>decring</b> <i>decimal_ring_num</i> ] [ <b>bridge</b> <i>bridge_num</i> ] [ <b>parent</b> <i>vlan_num</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

To create a backup TrCRF, assign one port on each switch that the TrBRF traverses to the backup TrCRF.

To configure a TrCRF VLAN as a backup TrCRF, perform this task in privileged mode:

	Task	Command
Step 1	Configure a TrCRF VLAN as a backup TrCRF.	<b>set vlan</b> <i>vlan_num</i> <b>backuperf on</b>
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]



#### Caution

If the backup TrCRF port is attached to a Token Ring multistation access unit (MSAU), it does not provide a backup path unless the ring speed and port mode are set by another device. We recommend that you configure the ring speed and port mode for the backup TrCRF.

To specify the maximum number of hops for All-Routes Explorer frames or Spanning-Tree Explorer frames in the TrCRF, perform this task in privileged mode:

	Task	Command
Step 1	Specify the maximum number of hops for All-Routes Explorer frames in the TrCRF.	<b>set vlan</b> <i>vlan_num</i> <b>aremaxhop</b> <i>hopcount</i>
Step 2	Specify the maximum number of hops for Spanning-Tree Explorer frames in the TrCRF.	<b>set vlan</b> <i>vlan_num</i> <b>stemaxhop</b> <i>hopcount</i>
Step 3	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan_num</i> ]

This example shows how to limit All-Routes Explorer frames and Spanning-Tree Explorer frames to ten hops and how to verify the configuration:

```

Console> (enable) set vlan 998 aremaxhop 10 stemaxhop 10
Vlan 998 configuration successful
Console> (enable) show vlan 998
VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
998  VLAN0998                active    357

VLAN Type  SAID      MTU   Parent RingNo BrdgNo  Stp  BrdgMode Trans1 Trans2
-----
998  trcrf  100998    4472  999   0xff   -    -    srb     0     0

VLAN AREHops STEHops Backup CRF
-----
998  10      10      off
Console> (enable)

```

## Assigning Switch Ports to a VLAN

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN. If you specify a VLAN that does not exist, the VLAN is created and the specified ports are assigned to it.



### Note

Make sure you assign switch ports to a VLAN of the proper type. Assign Ethernet, Fast Ethernet, and Gigabit Ethernet ports to Ethernet-type VLANs.

To assign one or more switch ports to a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Assign one or more switch ports to a VLAN.	<b>set vlan</b> <i>vlan_num mod_num/port_num</i>
Step 2	Verify the port VLAN membership.	<b>show vlan</b> [ <i>vlan_num</i> ] <b>show port</b> [ <i>mod_num[/port_num]</i> ]

This example shows how to assign switch ports to a VLAN and verify the assignment:

```

Console> (enable) set vlan 560 4/10
VLAN 560 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
560  4/10

Console> (enable) show vlan 560
VLAN Name                Status    IfIndex Mod/Ports, Vlans
-----
560  Engineering                active    348     4/10
VLAN Type  SAID      MTU   Parent RingNo BrdgNo  Stp  BrdgMode Trans1 Trans2
-----
560  enet  100560    1500  -    -    -    -    -     0     0
VLAN AREHops STEHops Backup CRF
-----

```

```

Console> (enable) show port 4/10
Port Name                Status      Vlan      Level Duplex Speed Type
-----
4/10                    notconnect 560       normal half   10 10BaseT

<...output truncated...>

Last-Time-Cleared
-----
Wed Jun 24 1998, 12:16:41
Console> (enable)

```

## Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configured Inter-Switch Link (ISL) VLANs is 1–1000. The valid range of VLANs specified in the IEEE 802.1Q standard is 0–4095. In a network environment with non-Cisco devices connected to Cisco switches through 802.1Q trunks, you must map 802.1Q VLAN numbers greater than 1000 to ISL VLAN numbers.

802.1Q VLANs in the range 1–1000 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers greater than 1000 must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco switches.

These restrictions apply when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to 16 802.1Q-to-ISL VLAN mappings on the switch.
- You can only map 802.1Q VLANs to Ethernet-type ISL VLANs.
- Do not enter the native VLAN of any 802.1Q trunk in the mapping table.
- When you map an 802.1Q VLAN to an ISL VLAN, traffic on the 802.1Q VLAN corresponding to the mapped ISL VLAN is blocked. For example, if you map 802.1Q VLAN 2000 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each switch. Make sure you configure the same VLAN mappings on all appropriate switches in the network.

To map an 802.1Q VLAN to an ISL VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Map an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for <i>dot1q_vlan</i> is 1001–4095. The valid range for <i>isl_vlan</i> is 1–1000.	<b>set vlan mapping dot1q</b> <i>dot1q_vlan</i> <b>isl</b> <i>isl_vlan</i>
Step 2	Verify the VLAN mapping.	<b>show vlan mapping</b>

This example shows how to map 802.1Q VLANs 2000, 3000, and 4000 to ISL VLANs 200, 300, and 400 and how to verify the configuration:

```

Console> (enable) set vlan mapping dot1q 2000 isl 200
802.1q vlan 2000 is existent in the mapping table
Console> (enable) set vlan mapping dot1q 3000 isl 300
Vlan mapping successful
Console> (enable) set vlan mapping dot1q 4000 isl 400
Vlan mapping successful
Console> (enable) show vlan mapping
802.1q vlan      ISL vlan      Effective
-----
2000             200           true
3000             300           true
4000             400           true
Console> (enable)

```

## Clearing 802.1Q-to-ISL VLAN Mappings

To clear an 802.1Q-to-ISL VLAN mapping, perform this task in privileged mode:

	Task	Command
Step 1	Clear an 802.1Q-to-ISL VLAN mapping.	<b>clear vlan mapping dot1q {dot1q_vlan   all}</b>
Step 2	Verify the VLAN mapping.	<b>show vlan mapping</b>

This example shows how to clear the VLAN mapping for 802.1Q VLAN 2000:

```

Console> (enable) clear vlan mapping dot1q 2000
Vlan 2000 mapping entry deleted
Console> (enable)

```

This example shows how to clear all 802.1Q-to-ISL VLAN mappings:

```

Console> (enable) clear vlan mapping dot1q all
All vlan mapping entries deleted
Console> (enable)

```

## Deleting a VLAN

When you delete a VLAN in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.



### Caution

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

To delete a VLAN on the switch, perform this task in privileged mode:

Task	Command
Delete a VLAN.	<code>clear vlan <i>vlan_num</i></code>

**Note**

You cannot delete a Token Ring TrBRF VLAN without first reassigning its child TrCRFs to another parent TrBRF, or deleting the child TrCRFs.

This example shows how to delete a VLAN (in this case, the switch is a VTP server):

```
Console> (enable) clear vlan 500
This command will deactivate all ports on vlan 500
in the entire management domain
Do you want to continue(y/n) [n]?y
Vlan 500 deleted
Console> (enable)
```

## Configuring Private VLANs

These sections describe how private VLANs work:

- Software Requirements for Private VLANs, page 9-14
- Understanding Private VLANs, page 9-14
- Private VLAN Configuration Guidelines, page 9-16
- Creating a Private VLAN, page 9-18
- Deleting a Private VLAN, page 9-21
- Deleting an Isolated or Community VLAN, page 9-21
- Deleting a Private VLAN Mapping, page 9-22

## Software Requirements for Private VLANs

To configure private VLANs you need supervisor engine software release 5.4(1) or later. If you have an MSFC installed, use Release 12.0(7)XE1 or later.

## Understanding Private VLANs

Private VLANs provide Layer-2 isolation between ports within the same private VLAN on the Catalyst 6000 family switches. Ports belonging to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure.

There are three types of private VLAN ports: promiscuous, isolated, and community.

- A promiscuous port communicates with all other private VLAN ports and is the port used to communicate with devices such as routers, LocalDirector, backup servers, and administrative workstations.

- An isolated port has complete Layer 2 separation from other ports within the same private VLAN with the exception of the promiscuous port.
- Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports within their private VLAN.

Privacy is granted at the Layer 2 level by blocking outgoing traffic to all isolated ports. All isolated ports are assigned to an isolated VLAN where this hardware function occurs. Traffic received from an isolated port is forwarded to all promiscuous ports only.

A private VLAN comprises pairs of VLANs that share a primary VLAN. Within a private VLAN, there are three distinct classifications of VLANs: a single primary VLAN, a single isolated VLAN, and a series of community VLANs.

You must define each supporting VLAN within a private VLAN structure before you can configure the private VLAN:

- Primary VLAN—Conveys incoming traffic from the promiscuous port to all other promiscuous, isolated, and community ports.
- Isolated VLAN—Used by isolated ports to communicate to the promiscuous ports. The traffic from an isolated port is blocked on all adjacent ports and can only be received by promiscuous ports.
- Community VLAN—Used by a group of community ports to communicate among themselves and transmit traffic to outside the group via the designated promiscuous port.

To create a private VLAN, you assign two or more normal VLANs in the normal VLAN range: one VLAN is designated as a primary VLAN, a second VLAN is designated as either an isolated or community VLAN. If you choose to, you can then designate additional VLANs as separate isolated or community VLANs in this private VLAN. After designating the VLANs, you must bind them together and associate them to the promiscuous port.

Private VLANs can be extended across multiple Ethernet switches by trunking the primary, isolated, and any community VLANs to other switches that support private VLANs.

In an Ethernet-switched environment where it is desirable to have Layer 2 isolation between individual or groups of stations, you can assign an individual VLAN and associated IP subnet to each individual or common group of stations. In many environments, the servers only require the ability to communicate with a default gateway to gain access to end points outside the VLAN itself. By incorporating these stations, regardless of ownership, into one private VLAN, you achieve these benefits:

- Designating the server ports as isolated prevents any interserver communication at Layer 2.
- Designating the ports to which the default gateway(s), backup server, or LocalDirector are attached as promiscuous, allows all stations to have access to these gateways.
- VLAN consumption is reduced. You only need to allocate one IP subnet to the entire group of stations because all stations reside in one common private VLAN.

On a Multilayer Switch Feature Card (MSFC) port or a nontrunk promiscuous port, you can remap as many community VLANs as desired; however, while a nontrunk promiscuous port can remap to only one primary VLAN, an MSFC port does not have this limitation. Another difference between the two types of promiscuous ports, is that an MSFC port can only connect an MSFC router, while with a nontrunk promiscuous port you can connect a wide range of devices as “access points” to a private VLAN. For example, you can connect a nontrunk promiscuous port to the “server port” of a LocalDirector to remap a number of community VLANs to the server VLAN so that the LocalDirector can load balance the servers present in the communities, or you can use a nontrunk promiscuous port to monitor and/or back up all the private VLAN servers from an administration workstation.

## Private VLAN Configuration Guidelines

This section contains configuration guidelines for private VLANs:

- Designate one VLAN as the primary VLAN.
- You have the option of designating one VLAN as an isolated VLAN; there can only be one isolated VLAN.
- You have the option of using private VLAN communities, you need to designate a community VLAN for each community.
- Bind the isolated and/or community VLAN(s) to the primary VLAN and assign the isolated or community ports. Doing this results in:
  - Isolated/community VLAN spanning tree properties are set to those of the primary VLAN.
  - VLAN membership becomes static.
  - Access ports become host ports.
  - BPDU guard protection is activated.
- Set up the automatic VLAN translation that maps the isolated and community VLANs to the primary VLAN on the promiscuous port(s). Set nontrunk ports or the MFSC ports as promiscuous ports.
- You must set VTP to transparent mode.
- Once you configure a private VLAN, you cannot change the VTP mode to client or server mode, because VTP does not support private VLAN types and mapping propagation.
- VLANs can be configured as primary, isolated, or community only if no access ports are currently assigned to the VLAN. Use the **show port** command to verify that the VLAN has no access ports assigned to it.
- A primary VLAN can have one isolated VLAN and/or multiple communities associated with it.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- Private VLANs cannot use VLANs 1, 1001, 1002, 1003, 1004, or 1005.
- If you delete either the primary or secondary VLAN, the ports associated with the VLAN become inactive.
- When configuring private VLANs, note the hardware and software interactions:
  - You cannot set private VLAN ports to trunking mode, channeling, or have dynamic VLAN memberships, with the exception of MSFC ports that always have trunking activated.
  - You cannot set ports belonging to the same ASIC where one port is set to trunking or promiscuous mode or is a SPAN destination and another port is set to isolated or community port for the modules listed in Table 9-2.

If you attempt such a configuration, a warning message displays and the command is rejected.

**Table 9-2** Modules with Ports Listed by ASIC Groups

Module Number	Description	Ports by ASIC
WS-X6224-100FX-MT	24-port 100FX Multimode MT-RJ	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6248-RJ-45	48-port 10/100TX RJ-45	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6248-TEL	48-Port 10/100TX RJ-21	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6348-RJ-45	48-port 10/100TX RJ-45	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6024-10FL-MT	24-port 10BaseFL MT-RJ	Ports 1–12 Ports 13–24

- Isolated and community ports should run BPDU guard features to prevent spanning tree loops due to misconfigurations.
- Primary VLANs and associated isolated/community VLANs must have the same spanning tree configuration. This configuration maintains consistent spanning tree topologies between associated primary, isolated, and community VLANs and avoids possible loss of connectivity. These priorities and parameters automatically propagate from the primary VLAN to the isolated and community VLANs.
- BPDU guard mode is system wide and is enabled once the first port is added to a private VLAN.



**Note** For more information on spanning tree and setting BPDU-guard protection, see Chapter 6, “Configuring Spanning Tree.”

- You cannot configure a destination SPAN port as a private VLAN port and vice versa.
- A source SPAN port can belong to a private VLAN.
- You can use VSPAN to span primary, isolated, and community VLANs together, or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- A remote SPAN VLAN (RSPAN) cannot be used for a private VLAN.



**Note** For more information on SPAN, see Chapter 32, “Configuring SPAN and RSPAN.”

- IGMP snooping and multicast shortcuts are not supported in private VLANs.
- You cannot enable EtherChannel on isolated, community, or promiscuous ports.
- If you apply an ACL to a primary VLAN, it propagates to all the associated isolated and community VLANs. The opposite is not allowed as this would not conform to the ACL model, which is not direction based. Primary and secondary VLANs, instead, are mostly unidirectional. However, you can configure ACLs “on a community basis,” but you will need to set up IOS ACLs and/or QoS ACLs address by address or, if a range of addresses is assigned to each community, you can set up the ACLs for each range/community. Note that VACLs always apply to the entire private VLAN.



**Note** For more information on ACLs, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

- You can stop Layer 3 switching on an isolated or community VLAN by destroying the binding of that VLAN with its primary VLAN. Deleting the corresponding mapping is not sufficient.

## Creating a Private VLAN

To create a private VLAN, perform this task in privileged mode:

	<b>Task</b>	<b>Command</b>
<b>Step 1</b>	Create the primary VLAN.	<b>set vlan</b> <i>vlan_num</i> <b>pvlan-type primary</b>
<b>Step 2</b>	Set the isolated or community VLAN(s).	<b>set vlan</b> <i>vlan_num</i> <b>pvlan-type</b> { <b>isolated</b>   <b>community</b> }
<b>Step 3</b>	Bind the isolated or community VLAN(s) to the primary VLAN.	<b>set pvlan</b> <i>primary_vlan_num</i> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> }
<b>Step 4</b>	Associate the isolated or community port(s) to the private VLAN.	<b>set pvlan</b> <i>primary_vlan_num</i> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> } <i>mod/ports</i>
<b>Step 5</b>	Map the isolated/community VLAN to the primary VLAN on the promiscuous port.	<b>set pvlan mapping</b> <i>primary_vlan_num</i> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> } <i>mod/ports</i>
<b>Step 6</b>	Verify the private VLAN configuration.	<b>show pvlan</b> [ <i>vlan_num</i> ] <b>show pvlan mapping</b>



**Note** As a shortcut, you can bind the isolated or community port(s) and associated isolated or community port(s) to the private VLAN in one step using the **set pvlan** *primary\_vlan\_num* { *isolated\_vlan\_num* | *community\_vlan\_num* } *mod/port* command.

**Note**

Ports do not have to be on the same switch as long as the switches are trunk connected and the private VLAN has not been removed from the trunk.

**Note**

If you are using the MSFC for your promiscuous port in your private VLAN, use 15/1 as the MSFC *mod/port* number if the supervisor engine is in slot 1, or use 16/1 if the supervisor engine is in slot 2.

This example shows how to create a private VLAN using VLAN 7 as the primary VLAN, 901 as the isolated VLAN, and 902 and 903 as the community VLANs. VLAN 901 uses module 4, port 3. VLAN 902 uses module 4, ports 4 through 6. VLAN 903 uses module 4, ports 7 through 9.

This example shows how to specify VLAN 7 as the primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Vlan 7 configuration successful
Console> (enable)
```

This example shows how to specify VLAN 901 as the isolated VLAN and VLANs 902 and 903 as community VLANs:

```
Console> (enable) set vlan 901 pvlan-type isolated
Vlan 901 configuration successful
Console> (enable) set vlan 902 pvlan-type community
Vlan 902 configuration successful
Console> (enable) set vlan 903 pvlan-type community
Vlan 903 configuration successful
Console> (enable)
```

This example shows how to bind VLAN 901 to primary VLAN 7 and assign port 4/3 as the isolated port:

```
Console> (enable) set pvlan 7 901 4/3
Successfully set the following ports to Private Vlan 7,901: 4/3
Console> (enable)
```

This example shows how to bind VLAN 902 to primary VLAN 7 and assign ports 4/4 through 4/6 as the community port:

```
Console> (enable) set pvlan 7 902 4/4-6
Successfully set the following ports to Private Vlan 7,902:4/4-6
Console> (enable)
```

This example shows how to bind VLAN 903 to primary VLAN 7 and assign port 4/7 through 4/9 as the community ports:

```
Console> (enable) set pvlan 7 903
Successfully set association between 7 and 903.
Console> (enable) set pvlan 7 903 4/7-9
Successfully set the following ports to Private Vlan 7,903:4/7-9
Console> (enable)
```

This example shows how to map the isolated/community VLAN to the primary VLAN on the promiscuous port, 3/1, for each isolated or community VLAN:

```

Console> (enable) set pvlan mapping 7 901 3/1
Successfully set mapping between 7 and 901 on 3/1
Console> (enable) set pvlan mapping 7 902 3/1
Successfully set mapping between 7 and 902 on 3/1
Console> (enable) set pvlan mapping 7 903 3/1
Successfully set mapping between 7 and 903 on 3/1

```

This example shows how to verify the private VLAN configuration:

```

Console> (enable) show vlan 7
VLAN Name                Status      IfIndex Mod/Ports, Vlans
-----
7    VLAN0007                active     35      4/4-6
VLAN Type  SAID      MTU    Parent RingNo BrdgNo  Stp   BrdgMode Trans1 Trans2
-----
7    enet    100010   1500   -      -      -      -      -      0      0
VLAN DynCreated  RSPAN
-----
7    static    disabled
VLAN AREHops STEHops Backup CRF 1q VLAN
-----
Primary Secondary Secondary-Type  Ports
-----
7    901      Isolated      4/3
7    902      Community     4/4-6
7    903      Community     4/7-9

Console> (enable) show vlan 902
VLAN Name                Status      IfIndex Mod/Ports, Vlans
-----
902  VLAN0007                active     38      4/4-6
VLAN Type  SAID      MTU    Parent RingNo BrdgNo  Stp   BrdgMode Trans1 Trans2
-----
7    enet    100010   1500   -      -      -      -      -      0      0
VLAN DynCreated  RSPAN
-----
7    static    disabled
VLAN AREHops STEHops Backup CRF 1q VLAN
-----
Primary Secondary Secondary-Type  Ports
-----
7    902      Isolated      4/4-6

Console> (enable) show pvlan
Primary Secondary Secondary-Type  Ports
-----
7    901      isolated      4/3
7    902      community     4/4-6
7    903      community     4/7-9

Console> (enable) show pvlan mapping
Port Primary Secondary
-----
3/1  7      901-903

```

```

Console> (enable) show port
Port Name                Status      Vlan      Duplex Speed Type
-----
...truncated output...
4/3                      notconnect 7,901     half    100 100BaseFX MM
4/4                      notconnect 7,902     half    100 100BaseFX MM
4/5                      notconnect 7,902     half    100 100BaseFX MM
4/6                      notconnect 7,902     half    100 100BaseFX MM
4/7                      notconnect 7,903     half    100 100BaseFX MM
4/8                      notconnect 7,903     half    100 100BaseFX MM
4/9                      notconnect 7,903     half    100 100BaseFX MM
... truncated output...

```

## Deleting a Private VLAN

You can delete a private VLAN by deleting the primary VLAN. If you delete a primary VLAN, all bindings to the primary VLAN are broken, all ports in the private VLAN become inactive, and any related mappings on the promiscuous port(s) are deleted.

To delete a private VLAN, perform this task in privileged mode:

Task	Command
Delete a primary VLAN.	<b>clear vlan</b> <i>primary_vlan</i>

This example shows how to delete primary VLAN 7:

```

Console> (enable) clear vlan 7
This command will de-activate all ports on vlan 7
Do you want to continue(y/n) [n]?y
Vlan 7 deleted
Console> (enable)

```

## Deleting an Isolated or Community VLAN

If you delete an isolated or community VLAN, the binding with the primary VLAN is broken, any isolated or community ports associated to the VLAN become inactive, and any related mappings on the promiscuous port(s) are deleted.

To delete a VLAN on the switch, perform this task in privileged mode:

Task	Command
Delete an isolated or community VLAN.	<b>clear vlan</b> { <i>isolated_vlan_num</i>   <i>community_vlan_num</i> }

This example shows how to delete the community VLAN 902:

```

Console> (enable) clear vlan 902
This command will de-activate all ports on vlan 902
Do you want to continue(y/n) [n]?y
Vlan 902 deleted
Console> (enable)

```

## Deleting a Private VLAN Mapping

If you delete the private VLAN mapping, the connectivity breaks between the isolated or community ports and the promiscuous port. If you delete all the mappings on a promiscuous port, the promiscuous port becomes inactive. When a private VLAN port is set to inactive, it displays “pvlan-” as its VLAN number in the **show port** output.

A private VLAN port might be set to inactive for the following reasons:

- The primary, isolated, or community VLAN to which it belongs is cleared.
- All mappings from a non-MSFC promiscuous port are deleted.
- An error occurs during the configuration of a port to be a private VLAN port.

To delete a port mapping from a private VLAN, perform this task in privileged mode:

Task	Command
Delete the port mapping from the private VLAN.	<b>clear pvlan mapping</b> primary_vlan { <i>isolated</i>   <i>community</i> } { <i>mod/ports</i> }

This example shows how to delete the mapping of VLAN 902 to 901, previously set on ports 3/2 through 3/5:

```
Console> (enable) clear pvlan mapping 901 902 3/2-5
Successfully cleared mapping between 901 and 902 on 3/2-5
Console> (enable)
```