



# CHAPTER 11

## Configuring VLANs

---

This chapter describes how to configure VLANs for the Catalyst 6500 series switches.



**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

---

This chapter consists of these sections:

- [Understanding How VLANs Work, page 11-1](#)
- [Configuring VLANs on the Switch, page 11-4](#)
- [Configuring Extended-Range VLANs on the Switch, page 11-6](#)
- [Mapping VLANs to VLANs, page 11-8](#)
- [Allocating Internal VLANs, page 11-10](#)
- [Assigning Switch Ports to a VLAN, page 11-10](#)
- [Enabling or Disabling VLAN Port-Provisioning Verification, page 11-12](#)
- [Deleting a VLAN, page 11-13](#)
- [Configuring VLAN Mappings on a Per-Port or Per-ASIC Basis, page 11-14](#)
- [Configuring Private VLANs on the Switch, page 11-19](#)
- [Configuring FDDI VLANs on the Switch, page 11-30](#)
- [Configuring Token Ring VLANs on the Switch, page 11-31](#)
- [Configuring VLANs for the Firewall Services Module, page 11-37](#)

## Understanding How VLANs Work

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

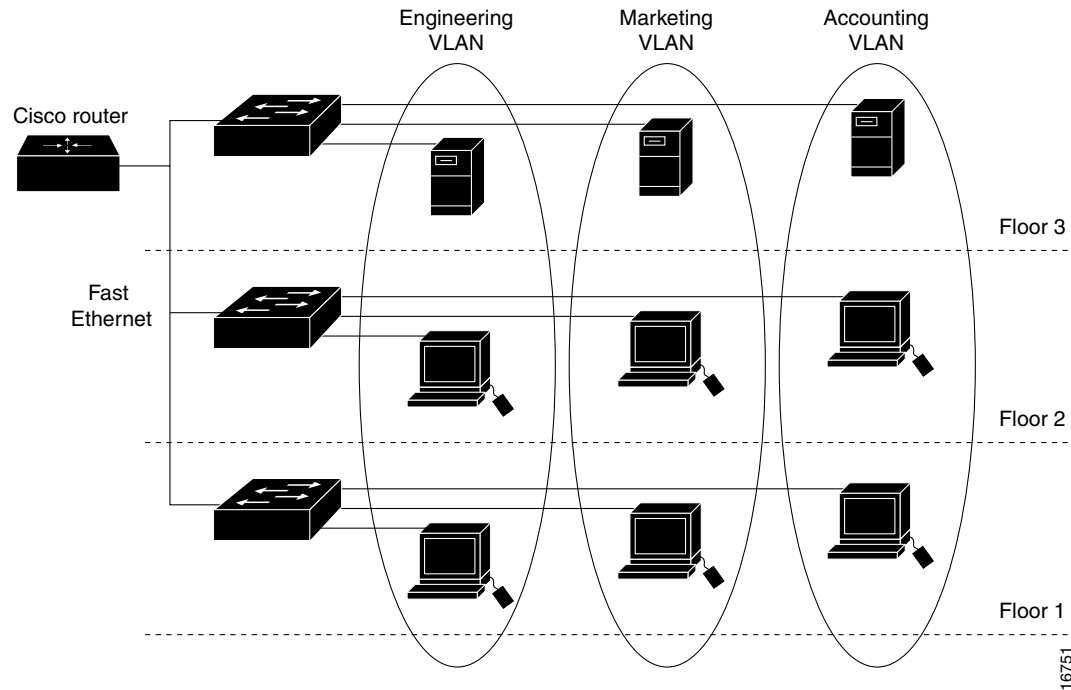
A VLAN allows you to group the ports on a switch to limit the unicast, multicast, and broadcast traffic flooding. The flooded traffic that originates from a particular VLAN is flooded only out the ports that belong to that VLAN.

**Figure 11-1** shows an example of VLANs that are segmented into logically defined networks.

These sections describe VLANs:

- [VLAN Ranges, page 11-2](#)
- [Configurable VLAN Parameters, page 11-3](#)
- [Default VLAN Configuration, page 11-3](#)

**Figure 11-1** VLANs as Logically Defined Networks



VLANs are often associated with the IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. The traffic between the VLANs must be routed. Port VLAN membership on the switch is assigned manually on a port-by-port basis. When you assign the switch ports to the 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 that 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.

## VLAN Ranges

Catalyst 6500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into two ranges; you use each range slightly differently. Some of these VLANs are propagated to other switches in the network when you use a management protocol, such as the VLAN Trunking Protocol (VTP). Other VLANs are not propagated and you must configure them on each applicable switch.

VLANs are divided into the following two ranges:

- Normal-range VLANs: 1–1023

- Extended-range VLANs: 1024–4094

**Note**

With VTP version 3, you can manage VLANs 1006–4094. These VLANs are propagated with VTP version 3.

## Configurable VLAN Parameters

Whenever you create or modify VLANs 2–1005, you can set the parameters as follows:

**Note**

Ethernet VLANs 1 and 1025–4094 can use the defaults only.

**Note**

With software release 8.3(1) and later releases, you can name all user VLANs. This capability is independent of any VTP version or mode.

- VLAN number
- VLAN name
- VLAN type: Ethernet, FDDI, FDDINET, Token Ring Bridge Relay Function (TrBRF), or Token Ring Concentrator Relay Function (TrCRF)
- VLAN state: active or suspended
- Multi-Instance Spanning Tree Protocol (MISTP) instance
- Private VLAN type: primary, isolated, community, two-way community, or none
- Security Association Identifier (SAID)
- Maximum transmission unit (MTU) for the VLAN
- Ring number for FDDI and TrCRF VLANs
- Bridge identification number for TrBRF VLANs
- Parent VLAN number for TrCRF VLANs
- STP type for TrCRF VLANs: IEEE, IBM, or auto
- VLAN to use when translating from one VLAN media type to another (VLANs 1–1005 only); requires a different VLAN number for each media type
- Source routing bridge mode for Token Ring VLANs: source-routing bridge (SRB) or source-routing transparent bridge (SRT)
- Backup for TrCRF VLAN
- Maximum hops VLAN All-Routes Explorer frames (ARE) and Spanning Tree Explorer frames (STE) for Token Ring
- Remote Switched Port Analyzer (RSPAN)

## Default VLAN Configuration

Table 11-1 shows the default VLAN configuration for the Catalyst 6500 series switches.

**Table 11-1** 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	Active
MTU size	1500 bytes 4472 bytes for Token Ring VLANs
SAID value	100,000 plus the VLAN number (for example, the SAID for VLAN 8 is 100008, and the SAID for VLAN 4050 is 104050)
Pruning eligibility	VLANs 2–1000 are pruning eligible; VLANs 1025-4094 are not pruning eligible
MAC address reduction	Disabled
Spanning-tree mode	PVST+
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)
Spanning Tree Protocol (STP) version for TrBRF VLAN	IBM
VLAN port-provisioning verification	Disabled
TrCRF bridge mode	SRB
Remote switched port analyzer (RSPAN)	Disabled

## Configuring VLANs on the Switch

These sections describe how to configure user VLANs 1–4094:

- [Normal-Range VLAN Configuration Guidelines, page 11-5](#)
- [Creating Normal-Range VLANs, page 11-5](#)
- [Modifying Normal-Range VLANs, page 11-6](#)



### Note

You cannot configure or modify normal-range VLAN 1.

## Normal-Range VLAN Configuration Guidelines

This section describes the guidelines for creating and modifying the user VLANs in your network:

- The default VLAN type is Ethernet; if you do not specify a VLAN type, the VLAN will be an Ethernet VLAN.
- If you wish to use VTP to maintain global VLAN configuration information on your network, configure VTP before you create any normal-range VLANs. See [Chapter 10, “Configuring VTP”](#) for configuring VTP. (You cannot use VTP to manage extended-range VLANs 1025–4094.)



**Note** With VTP version 3, you can manage VLANs 1006–4094. These VLANs are propagated with VTP version 3.

- The FlexWAN modules and routed ports automatically allocate a number of VLANs for their own use, starting at VLAN 1025. If you use these devices, you must allow for the number of VLANs required.

## Creating Normal-Range VLANs

You can create one VLAN at a time or you can create a range of VLANs with a single command. If you create a range of VLANs, you cannot specify a name; the VLAN names must be unique.

To create a normal-range VLAN, perform this task in privileged mode:

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

This example shows how to create the normal-range VLANs and verify the configuration when the switch is in Per VLAN Spanning Tree + (PVST+) mode:

```
Console> (enable) set vlan 500-520
Vlan 500 configuration successful
Vlan 501 configuration successful
Vlan 502 configuration successful
Vlan 503 configuration successful
Vlan 520 configuration successful
```

```
Console> (enable) show vlan 500-520
VLAN Name                Status      IfIndex  Mod/Ports, Vlans
-----
500                       active     342
501                       active     343
502                       active     344
503                       active     345
520                       active     362
```

```

VLAN Type SAID MTU Parent RingNo BrdgNo Stp BrdgMode Trans1 Trans2
-----
500 enet 100500 1500 - - - - - 0 0
501 enet 100501 1500 - - - - - 0 0
502 enet 100502 1500 - - - - - 0 0
503 enet 100503 1500 - - - - - 0 0
520 enet 100520 1500 - - - - - 0 0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

## Modifying Normal-Range VLANs

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

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

## Configuring Extended-Range VLANs on the Switch

These sections explain how to configure extended-range VLANs 1025–4094:

- [Extended-Range VLAN Configuration Guidelines, page 11-6](#)
- [Creating Extended-Range VLANs, page 11-7](#)

## Extended-Range VLAN Configuration Guidelines

This section describes the guidelines for creating extended-range VLANs 1024–4094:

- You can create only Ethernet-type VLANs in the extended range.
- You must enable MAC address reduction in order to use the extended-range VLANs.
- You can only create and delete the extended-range VLANs from the CLI or SNMP.
- You cannot use VTP to manage these VLANs; they must be statically configured on each switch.



### Note

With VTP version 3, you can manage VLANs 1006–4094. These VLANs are propagated with VTP version 3. For configuration purposes, the extended range consists of VLANs 1025–4094.

- You cannot use the extended-range VLANs if you have dot1q-to-isl mappings.

- You can configure the private VLAN parameters and RSPAN for the extended-range VLANs; however, all other parameters for the extended-range VLANs use the system defaults only.
- The switch may allocate a block of VLANs from the extended range for internal purposes; for example, the switch may allocate the VLANs for the routed ports or FlexWAN modules. The block of VLANs is always allocated starting from VLAN 1006 up. If you have any VLANs within the range that are required by the FlexWAN module, all of the VLANs that are required will not be allocated, because the VLANs are never allocated from the user's VLAN area.

**Caution**

The FlexWAN modules and routed ports automatically allocate a sequential block of internal VLANs starting at VLAN 1006. If you use these devices, you *must* allow the required number of VLANs for them. If not enough VLANs are available for the FlexWAN module, some ports may not work. Refer to the *Catalyst 6500 Series and Cisco 7600 Series Router FlexWAN Module Installation and Configuration Note* for more information.

**Caution**

If you move a FlexWAN module from one slot to another on the same switch, it will allocate another block of VLANs without deleting the previous block. You should reboot the switch if you move the FlexWAN module.

## Creating Extended-Range VLANs

To create the extended-range VLANs, you must first enable MAC address reduction, which provides the IDs for the extended-range VLANs. After you enable MAC address reduction, you cannot disable it as long as any extended-range VLANs exist.

**Note**

If you wish to use the extended-range VLANs and you have existing 802.1Q-to-ISL mappings in your system, you must delete the mappings. See the [“Deleting 802.1Q-to-ISL VLAN Mappings” section on page 11-10](#) for more information.

**Note**

With software release 8.1(1) and later releases, you can name the extended-range VLANs. This capability is independent of any VTP version or mode.

To enable MAC address reduction and create an Ethernet VLAN in the extended range, perform this task in privileged mode:

	Task	Command
Step 1	Enable MAC address reduction.	<b>set spantree macreduction {enable   disable}</b>
Step 2	Create a VLAN.	<b>set vlan <i>vlan</i></b>
Step 3	Verify the VLAN configuration.	<b>show vlan [<i>vlan</i>]</b>

This example shows how to enable MAC address reduction and create an extended-range Ethernet VLAN:

```

Console> (enable) set spantree macreduction enable
MAC address reduction enabled
Console> (enable) set vlan 2000
Vlan 2000 configuration successful
Console> (enable) show vlan 2000
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
2000 VLAN2000                           active    61

VLAN Type  SAID      MTU   Parent RingNo BrdgNo Stp   BrdgMode Trans1 Trans2
-----
2000 enet   102000    1500  -      -      -     -     -         0      0

VLAN Inst DynCreated  RSPAN
-----
2000 -    static    disabled
Console> (enable)

```

This example shows how to display a summary of active, suspended, and extended VLANs:

```

Console> (enable) show vlan summary

Vlan status   Count  Vlans
-----
VTP Active    504    1-100,102-500,1000,1002-1005

VTP Suspended  1      101

Extended      1      2000
Console> (enable)

```

## Mapping VLANs to VLANs



### Note

To configure the VLAN mappings on a per-port or per-ASIC basis, see the [“Configuring VLAN Mappings on a Per-Port or Per-ASIC Basis”](#) section on page 11-14.



### Note

With software release 8.3(1) and later releases, the global VLAN mapping feature is not needed because ISL trunks now support the entire VLAN range (1 to 4094).

You can map the VLANs from the 802.1Q trunks that are connected to the VLANs on the non-Cisco devices to the ISL trunks that are connected to the other VLANs on the Catalyst 6500 series switches.



### Note

If you map the 802.1Q VLANs to the ISL VLANs, you can retain the mappings from a previous Catalyst 6500 series software release but you cannot use the extended-range VLANs.

This section describes how to map the VLANs to VLANs:

- [Mapping 802.1Q VLANs to ISL VLANs, page 11-9](#)
- [Deleting 802.1Q-to-ISL VLAN Mappings, page 11-10](#)

## Mapping 802.1Q VLANs to ISL VLANs

Your network might have non-Cisco devices that are connected to the Catalyst 6500 series switches through the 802.1Q trunks.

The valid range of the user-configured Inter-Switch Link (ISL) VLANs is 1–1000 (and 1002–1005) and 1025–4094. The valid range of VLANs that is specified in the IEEE 802.1Q standard is 0–4095. In a network environment with the non-Cisco devices that are connected to the Cisco switches through the 802.1Q trunks, you can map the 802.1Q VLAN numbers that are greater than 1000 to the ISL VLAN numbers. If you use any VLANs in the extended range (1025–4094) for dot1q mappings, you cannot use any of the extended-range VLANs for any other purpose.

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

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

- The global VLAN mapping feature and the per-port/per-ASIC VLAN mapping features (see the [“Configuring VLAN Mappings on a Per-Port or Per-ASIC Basis”](#) section on page 11-14) are mutually exclusive; only one feature can be enabled at any time.
- If there are any extended-range VLANs present on the switch, you cannot map any new 802.1Q VLANs-to-ISL VLANs.
- You can configure up to eight 802.1Q-to-ISL VLAN mappings on the switch.
- You can only map the 802.1Q VLANs to the 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, the 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, the traffic on 802.1Q VLAN 200 is blocked.
- The VLAN mappings are local to each switch. Make sure that 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 <i>dot1q_vlan</i> isl <i>isl_vlan</i></b>
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 verify the configuration:

```
Console> (enable) set vlan mapping dot1q 2000 isl 200
Vlan mapping successful
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)

```

## Deleting 802.1Q-to-ISL VLAN Mappings

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

	Task	Command
Step 1	Delete 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 delete 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 delete all 802.1Q-to-ISL VLAN mappings:

```

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

```

## Allocating Internal VLANs

The VLANs are classified as either user VLANs or internal VLANs. A user VLAN can be any VLAN from 1–4094 created by a user. The internal VLANs are the VLANs that are used by the software features that require the dedicated VLANs in order to function. The internal VLANs are allocated by the VLAN Manager as needed using VLANs 1006–4094. The internal VLANs are allocated in ascending order, starting at VLAN 1006. You should assign the user VLANs as close to VLAN 4094 as possible in order to avoid conflicts between the user VLANs and the internal VLANs.



### Note

Because the number of available VLANs is fixed, make sure that a sufficient number of VLANs remains available for internal VLAN allocation after you have assigned the user VLANs.

## Assigning Switch Ports to a VLAN

A VLAN that is created in a management domain remains unused until you assign one or more switch ports to the VLAN. You can create a new VLAN and then specify the module and ports later, or you can create the VLAN and specify the module and ports in a single step.

**Note**

Make sure that you assign the switch ports to a VLAN of the proper type. For example, assign the Ethernet, Fast Ethernet, and Gigabit Ethernet ports to the 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 mod/port</i>
Step 2	Verify the port VLAN membership.	<b>show vlan</b> [ <i>vlan</i> ] <b>show port</b> [ <i>mod[/port]</i> ]

This example shows how to assign the 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     Duplex Speed Type
-----
4/10                               connected 560      a-half a-100 10/100BaseTX

Port AuxiliaryVlan AuxVlan-Status
-----
4/10 none           none

.
.
.

Last-Time-Cleared
-----
Tue Jun 6 2000, 16:45:18
Console> (enable)

```

## Enabling or Disabling VLAN Port-Provisioning Verification

When VLAN port-provisioning verification is enabled, you must specify the VLAN name *in addition to* the VLAN number when assigning the switch ports to the VLANs. Because you are required to specify both the VLAN name and the VLAN number, this verification feature helps to ensure that the ports are not inadvertently placed in the wrong VLAN.

When the feature is enabled, you can still create new VLANs by entering the **set vlan *vlan mod/port*** command but you cannot add additional ports to the VLAN without specifying both the VLAN number and the VLAN name. The feature does not affect assigning ports to VLANs using other features such as SNMP, dynamic VLANs, and 802.1X. VLAN port-provisioning verification is disabled by default.

To enable or disable VLAN port-provisioning verification, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable VLAN port-provisioning verification.	<b>set vlan verify-port-provisioning {enable   disable}</b>
Step 2	Verify the VLAN port-provisioning verification status.	<b>show vlan verify-port-provisioning</b>

This example shows how to enable VLAN port-provisioning verification:

```
Console> (enable) set vlan verify-port-provisioning enable
vlan verify-port-provisioning feature enabled
Console> (enable)
```

This example shows how to verify the status of VLAN port-provisioning verification:

```
Console> (enable) show vlan verify-port-provisioning
Vlan Verify Port Provisioning feature enabled
Console> (enable)
```

This example shows how to create VLAN 150 and add port 3/16 (with VLAN port-provisioning verification enabled):

```
Console> (enable) set vlan 150 3/16
Vlan 150 configuration successful
VLAN 150 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
150 3/16
Console> (enable)
```

This example shows what happens when you try to add port 3/17 to VLAN 150 with VLAN port-provisioning verification enabled:

```
Console> (enable) set vlan 150 3/17
Port Provisioning Verification is enabled on the switch.
To move port(s) into the VLAN, use 'set vlan <vlan> <port> <vlan_name>' command.
Console> (enable)
```

This example shows how to add port 3/17 to VLAN 150 with VLAN port-provisioning verification enabled:

```

Console> (enable) set vlan 150 name Eng
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 150 configuration successful
Console> (enable)

Console> (enable) set vlan 150 3/17 Eng
VLAN 150 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
150 3/16-17
Console> (enable)

```

## Deleting a VLAN

This section describes the guidelines for deleting the VLANs:

- When you delete a normal-range Ethernet VLAN in VTP server mode, the VLAN is removed from all switches in the VTP domain.
- When you delete a normal-range VLAN in VTP transparent mode, the VLAN is deleted only on the current switch.
- You can delete an extended-range VLAN only on the switch where it was created.
- You cannot delete the default VLANs.
- To delete a Token Ring TrBRF VLAN, you must first reassign its child TrCRFs to another parent TrBRF, or delete the child TrCRFs.



### Caution

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

You can delete a single VLAN or a range of VLANs. To delete a VLAN on the switch, perform this task in privileged mode:

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

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(s) 500
Do you want to continue(y/n) [n]?y
Vlan 500 deleted
Console> (enable)

```

```

This command will deactivate all ports on vlan(s) 10
All ports on normal range vlan(s) 10
will be deactivated in the entire management domain.
Do you want to continue(y/n) [n]?

```

# Configuring VLAN Mappings on a Per-Port or Per-ASIC Basis

These sections describe how to configure VLAN mapping on a per-port or per-ASIC basis:

- [Understanding VLAN Mapping, page 11-14](#)
- [Configuration Guidelines and Restrictions, page 11-14](#)
- [Enabling or Disabling VLAN Mapping on an Individual Port, page 11-17](#)
- [Configuring VLAN Mapping on an Individual Port, page 11-17](#)
- [Clearing the VLAN Mapping, page 11-18](#)
- [Displaying the VLAN Mapping Information, page 11-19](#)

## Understanding VLAN Mapping

With software release 8.4(1) and later releases, VLAN mapping has been enhanced to allow you to map *any* type of VLAN to any other type of VLAN without any VLAN range restrictions. VLAN mapping is now configurable on a per-port or per-ASIC basis.

**Note**

---

Before software release 8.4(1), VLAN mapping was configured globally. For detailed information, see the [“Mapping VLANs to VLANs” section on page 11-8](#).

---

## Configuration Guidelines and Restrictions

This section describes the configuration guidelines and restrictions for configuring VLAN mapping:

- With VLAN mapping, you have the following options depending on the type of ASIC on the switching module or supervisor engine (for the individual module ASIC specifics, see [Table 11-2](#)):
  - VLAN mapping is not supported.
  - Per-port VLAN mapping is supported.
  - Per-ASIC VLAN mapping *without* the ability to enable or disable VLAN mapping on an individual port basis is supported.
  - Per-ASIC VLAN mapping *with* the ability to enable or disable VLAN mapping on an individual port basis is supported.
- If a module does not support per-port VLAN mapping and supports only per-ASIC VLAN mapping, VLAN mapping is applied to all the ports in the ASIC. If you change the mapping for any port in the ASIC, the change is applied to all the ports in the ASIC.
- Global VLAN mapping

The global VLAN mapping feature (see the [“Mapping VLANs to VLANs” section on page 11-8](#)) and the per-port/per-ASIC VLAN mapping features are mutually exclusive; only one feature can be enabled at any time.

If global VLAN mapping is configured for any of the VLANs and you try to configure per-port/per-ASIC VLAN mapping, the command is rejected and an error message is displayed. Conversely, if per-port/per-ASIC VLAN mapping is configured for any of the VLANs and you try to configure global VLAN mapping, the command is rejected and an error message is displayed.

Global VLAN mapping supports a maximum of eight VLANs. If VLAN X is mapped to VLAN Y, VLAN Y is mapped to a discarded VLAN internally. Per-port/per-ASIC VLAN mapping does not work that way. If VLAN X is mapped to VLAN Y, all the internally switched traffic to a port on VLAN Y is mapped to VLAN X.

- VLAN mapping is applied in both directions. For example, if port P has a VLAN mapping of VLAN x to VLAN y, all the traffic received by port P on VLAN X is mapped and processed in VLAN Y, and all the traffic internally tagged with VLAN Y that leaves port P, is tagged with VLAN X.
- EtherChannel  
VLAN mapping is supported on EtherChannels, both PAgP and LACP. If you enable or disable VLAN mapping on one port of the channel, the feature is enabled or disabled on all the ports in the channel. Similarly, if you configure a VLAN mapping on one port in the channel, the mapping is applied to all ports in the channel.

All the ports in the EtherChannel must have the same port ASIC capability in terms of VLAN mapping. If you try to configure a VLAN mapping on an EtherChannel where some of the ports in the channel do not have the same port ASIC capabilities, the command is rejected.

- SPAN and RSPAN

If per-port VLAN mapping is enabled on a port, the port ASIC changes the source VLAN to the translated VLAN. Any SPAN configuration works on the translated VLAN.

The RSPAN VLAN cannot be translated; you must not configure the RSPAN VLAN to be mapped to any VLAN. Similarly, the translated VLAN cannot be used as an RSPAN VLAN.

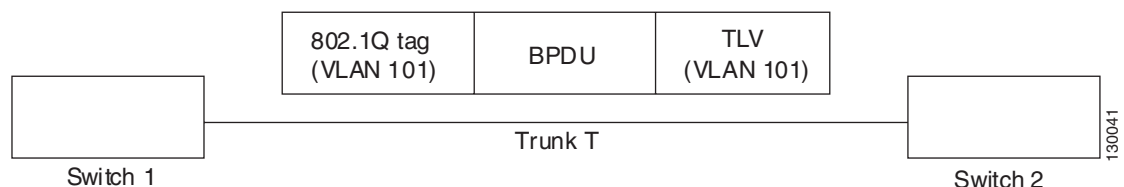
- Spanning tree

In the PVST+ implementation, spanning-tree BPDUs are tagged with a TLV of “VLAN ID” on each trunk port. This TLV helps spanning tree in determining the port VLAN ID consistency. In PVST+ and Rapid-PVST+, this VLAN ID is equal to the spanning-tree instance number (the VLAN ID).

With Shared Spanning Tree Protocol (SSTP), be careful when per-port/per-ASIC VLAN mapping is enabled on a port. For example, in [Figure 11-2](#), switch 1 and switch 2 are connected using trunk T that carries VLAN 101. On switch 2, per-port/per-ASIC VLAN mapping is enabled on trunk port P and one of the mappings is VLAN 101 to VLAN 202. As shown in [Figure 11-2](#), on the trunk link, the BPDU has the 802.1Q VLAN and the TLV VLAN as VLAN 101. When this BPDU reaches port P, its 802.1Q VLAN is changed to VLAN 202 because of the mapping but the TLV VLAN still remains VLAN 101. When the BPDU reaches the spanning-tree process, spanning tree concludes that the VLAN 101 BPDU is received on VLAN 202 and thinks that it is inconsistent and reports this as an inconsistent port.

To correct this problem, the spanning tree processes this BPDU in VLAN 202 and the TLV VLAN is mapped to the translated VLAN and checked for consistency. When that occurs, the spanning-tree instance 101 of switch 1 is merged with the spanning-tree instance 202 of switch 2. This process is also done on the transmit side.

**Figure 11-2 Understanding VLAN Mapping and Spanning Tree**



**Tip**

Before designing your spanning-tree topology, you should take into account the way in which VLANs are merged. You should clear the source VLAN from the port on which VLAN mapping is enabled and clear the translated VLAN from the neighboring end. Doing this ensures that the source VLAN of the customer port and the translated VLAN of the provider port are merged.

**Table 11-2 Per-Module Port ASIC VLAN Mapping Capabilities**

Module	Maximum Number of Per-Port VLAN Mappings Supported	Capabilities/Limitations
WS-X6548-RJ-45 WS-X6548-RJ-21 WS-X6148X2-RJ-45 WS-X6148X2-45AF WS-X6196-RJ-21 <sup>1</sup>	32	Per-ASIC VLAN mapping. Mapping can be enabled or disabled on a per-port basis on ISL trunks. Mapping is always on for 802.1Q trunks and there is no way to disable it. Mapping is supported for ISL and 802.1Q trunks.
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2 WS-X6K-S2-PFC2 WS-SUP720-3B WS-SUP720-3BXL WS-SUP720 WS-X6516A-GBIC <sup>2</sup> WS-X6516-GE-TX	32	Per-ASIC VLAN mapping. Mapping can be enabled or disabled on individual ports in the ASIC. Supports any-to-any type of VLAN translation. Supported only on 802.1Q trunks. <sup>3</sup>
WS-X6748-SFP <sup>4</sup> WS-X6724-SFP WS-X6748-GE-TX	128	Per-ASIC VLAN mapping. Mapping can be enabled or disabled on individual ports in the ASIC. Supports any-to-any type of VLAN translation. Mapping is supported for ISL and 802.1Q trunks.
WS-X6148A-GE-TX WS-X6148A-GE-45A WS-X6148-FE-SFP WS-X6148A-RJ-45 WS-X6148A-45AF WS-X6704-10GE <sup>5</sup>	8	Per-port VLAN mapping. Supports any-to-any type of VLAN translation. Mapping is supported for ISL and 802.1Q trunks.
WS-X6502-10GE	16	Per-port VLAN mapping. Supports any-to-any type of VLAN translation. Supported only on 802.1Q trunks.
WS-SUP32-GE-3B	16	Per-port VLAN mapping. Supports any-to-any type of VLAN translation. Mapping is supported for ISL and 802.1Q trunks.

1. WS-X6196-RJ-21 does not have per-ASIC VLAN mapping. VLAN mapping is per-two ASICs: Ports 1 through 96 (instead of only 48 ports per ASIC).
2. WS-X6516A-GBIC does not have per-ASIC VLAN mapping. VLAN mapping is per-two ASICs: Ports 1 through 8 and ports 9 through 16 (instead of only 4 ports per ASIC).
3. The ASICs in these modules have the following limitation: When dot1q-all-tagged is disabled, VLAN translation does not occur for packets transmitted on the native VLAN.

4. WS-X6748-SFP does not have per-ASIC VLAN mapping. VLAN mapping is per-two ASICs: Ports 1 through 24 and ports 25 through 48 (instead of only 12 ports per ASIC).
5. WS-X6704-10GE: Mapping can be enabled or disabled on individual ports in the ASIC. 128 per-port VLAN mappings supported.

## Enabling or Disabling VLAN Mapping on an Individual Port



### Note

Before using the **set port vlan-mapping** command to configure VLAN mapping on an individual port, you must enable port VLAN mapping by entering the **set port vlan-mapping mod/port enable** command.

Enter the **set port vlan-mapping mod/port {enable | disable}** command to enable or disable VLAN mapping on an individual port. VLAN translation occurs only when the mapping is enabled and the port is trunking. For the ASICs that support VLAN mapping only on a per-ASIC basis, but with the ability to enable or disable VLAN mapping on an individual port basis, this command is applied to the port configuration only and not to the ASIC. If you disable VLAN mapping, the mapping is still preserved. VLAN mapping is disabled by default.

To enable or disable VLAN mapping on an individual port, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable VLAN mapping on an individual port.	<b>set port vlan-mapping mod/port {enable   disable}</b>
Step 2	Display VLAN mapping configuration.	<b>show port vlan-mapping [mod   mod/port]</b>

This example shows how to enable VLAN mapping on an individual port:

```
Console>(enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console>(enable)
```

## Configuring VLAN Mapping on an Individual Port



### Note

Before using the **set port vlan-mapping** command, you must enable the port VLAN mapping by entering the **set port vlan-mapping mod/port enable** command.



### Note

The source VLAN is the trunk VLAN (external to the switch) and the translated VLAN is internal to the switch.

Enter the **set port vlan-mapping mod/port source-vlan-id translated-vlan-id** command to configure VLAN mapping on an individual port. This command causes the traffic on the *source-vlan-id* to be translated to the *translated-vlan-id*. All traffic that is internally tagged with the *translated-vlan-id* is tagged with the *source-vlan-id* before leaving the port. The VLAN translation occurs only if the port is trunking. This command accepts the full range of ports.

To configure VLAN mapping on an individual port, perform this task in privileged mode:

	Task	Command
Step 1	Enable the port VLAN mapping.	<b>set port vlan-mapping</b> <i>mod/port</i> { <b>enable</b>   <b>disable</b> }
Step 2	Configure VLAN mapping on an individual port.	<b>set port vlan-mapping</b> <i>mod/port source-vlan-id translated-vlan-id</i>
Step 3	Display VLAN mapping configuration.	<b>show port vlan-mapping</b> [ <i>mod</i>   <i>mod/port</i> ]

This example shows how to enable the port VLAN mapping and configure VLAN mapping on an individual port. In this example, module 7 is the 48-port 10/100/1000 switching module (WS-X6748-GE-TX). This module supports per-ASIC VLAN mapping; 1 ASIC supports 12 ports.

```

Console>(enable) set port vlan-mapping 7/1 enable
VLAN mapping enabled on port 7/1.
Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7.1. 7/1-12.
Console>(enable) show port vlan-mapping 7/1
Mod/Port Source VLAN Translated VLAN State Max Allowed (Current) Entries
-----
7/1      2002      3003      Enabled      128 (1)
Console>(enable)

```

In this example, module 5 is the 1-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6502-10GE). This module supports per-port VLAN mapping.

```

Console>(enable) set port vlan-mapping 5/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on port 5/1.
Console>(enable)

```

In this example, module 7 is the 48-port 10/100/1000 switching module (WS-X6748-GE-TX). This module supports per-ASIC VLAN mapping; 1 ASIC supports 12 ports. In this example, ports 7/1-4 are part of an EtherChannel.

```

Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12.
Console>(enable)

```

In this example, module 7 and module 8 are the 48-port 10/100/1000 switching modules (WS-X6748-GE-TX). These modules support per-ASIC VLAN mapping; 1 ASIC supports 12 ports. In this example, ports 7/1-4 and ports 8/1-4 are part of an EtherChannel.

```

Console>(enable) set port vlan-mapping 7/1 2002 3003
VLAN 2002 mapped to VLAN 3003 on ports 7/1-12,8/1-12.
Console>(enable)

```

## Clearing the VLAN Mapping

Enter the **clear port vlan-mapping** command to clear the VLAN mapping on an individual port, on all ports, or on a specific source VLAN ID. On some modules, VLAN mapping is supported on a per-ASIC basis; the mapping is not stored on a per-port basis. For these modules, entering the **clear port vlan-mapping** *mod/port* command clears the VLAN mapping on all ports on the ASIC. When you enter a *source\_vlan\_id* argument, only the VLAN mapping for that source VLAN is cleared from the VLAN mapping table of the specified port or ASIC (if ASIC-based port).

To clear VLAN mapping, perform this task in privileged mode:

Task	Command
Clear VLAN mapping.	<code>clear port vlan-mapping mod/port all</code> <code>clear port vlan-mapping mod/port [source-vlan-id]</code> <code>clear port vlan-mapping all</code>

This example shows how to clear the VLAN mapping from port 7/1:

```
Console>(enable) clear port vlan-mapping 7/1 2002
VLAN mapping for VLAN 2002 removed from port 7/1-12.
Console>(enable)
```

## Displaying the VLAN Mapping Information

Enter the `show port vlan-mapping [mod | mod/port]` command to display the VLAN mapping information.

To display VLAN mapping information, perform this task in normal mode:

Task	Command
Display the VLAN mapping information.	<code>show port vlan-mapping [mod   mod/port]</code>

This example shows how to display the VLAN mapping information for port 7/1:

```
Console>(enable) show port vlan-mapping 7/1
Mod/Port Source VLAN Translated VLAN State Max Allowed (Current) Entries
-----
7/1      2002      3003      Enabled      128 (1)
Console>(enable)
```



### Note

Enter the `show port capabilities [mod | mod/port]` command to display the mapping type (per port or per ASIC) for each port. This command also displays the maximum allowed mappings for each port.

## Configuring Private VLANs on the Switch

These sections describe how the private VLANs work:

- [Understanding How Private VLANs Work](#), page 11-20
- [Private VLAN Configuration Guidelines](#), page 11-21
- [Creating a Primary Private VLAN](#), page 11-25
- [Viewing the Port Capability of a Private VLAN Port](#), page 11-27
- [Deleting a Private VLAN](#), page 11-28
- [Deleting an Isolated, Community, or Two-Way Community VLAN](#), page 11-29
- [Deleting a Private VLAN Mapping](#), page 11-29
- [Private VLAN Support on the MSFC](#), page 11-30

## Understanding How Private VLANs Work

The private VLANs provide the Layer-2 isolation between the ports within the same private VLAN on the Catalyst 6500 series switches. The ports that belong to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure.

The three types of private VLAN ports are as follows:

- Promiscuous—This port communicates with all other private VLAN ports and is the port that you use to communicate with routers, LocalDirector, backup servers, and administrative workstations.




---

**Note** If a broadcast or multicast packet comes from the promiscuous port, it is sent to all the ports in the private VLAN domain, that is, to all the community and isolated ports.

---

- Isolated—This port has complete Layer 2 separation from the other ports within the same private VLAN with the exception of the promiscuous port.
- Community—These 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 Layer 2 by blocking the outgoing traffic to all isolated ports. All isolated ports are assigned to an isolated VLAN where this hardware function occurs. The traffic that is received from an isolated port is forwarded to all promiscuous ports only.

A private VLAN has four distinct classifications: a single primary VLAN, a single isolated VLAN, and a series of community or two-way community VLANs.

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

- Primary VLAN—Conveys the incoming traffic from the promiscuous port to all other promiscuous, isolated, community, and two-way community ports.
- Isolated VLAN—Used by the isolated ports to communicate to the promiscuous ports. The traffic from an isolated port is blocked on all adjacent ports within its private VLAN and can only be received by its promiscuous ports.
- Community VLAN—A unidirectional VLAN that is used by a group of community ports to communicate among themselves and transmit the traffic to outside the private VLAN through the designated promiscuous port.
- Two-way community VLAN—A bidirectional VLAN that is used by a group of community ports to communicate among themselves and to and from the community ports from and to the Multilayer Switch Feature Card (MSFC).




---

**Note** With software release 6.2(1) and later releases, you can use the two-way community VLANs to perform an inverse mapping from the primary VLAN to the secondary VLAN when the traffic crosses the boundary of a private VLAN through an MSFC promiscuous port. Both the outbound and inbound traffic can be carried on the same VLAN allowing the VLAN-based features such as the VLAN access control lists (VACLs) to be applied in both directions on a per-community (per-customer) basis.

---

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, and a second VLAN is designated as either an isolated, community, or two-way community VLAN. If you choose, you can then designate additional VLANs as separate isolated, community, or two-way community VLANs in this private VLAN. After designating the VLANs, you must bind them together and associate them to the promiscuous port.

You can extend the private VLANs across multiple Ethernet switches by trunking the primary, isolated, and any community or two-way community VLANs to the other switches that support the private VLANs.

In an Ethernet-switched environment, you can assign an individual VLAN and associated IP subnet to each individual or common group of stations. The servers require only the ability to communicate with a default gateway to gain access to the end points outside the VLAN itself. By incorporating these stations, regardless of ownership, into one private VLAN, you can do the following:

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

On an MSFC port or a nontrunk promiscuous port, you can remap as many isolated or community VLANs as desired; however, while a nontrunk promiscuous port can remap to only one primary VLAN, an MSFC port can only connect an MSFC router. 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 isolated or community VLANs to the server VLAN so that the LocalDirector can load balance the servers that are present in the isolated or community VLANs, or you can use a nontrunk promiscuous port to monitor and/or back up all the private VLAN servers from an administration workstation.

**Note**

---

A two-way community VLAN can be mapped only on the MSFC promiscuous port (it cannot be mapped on nontrunk or other types of promiscuous ports).

---

## Private VLAN Configuration Guidelines

This section describes the guidelines for configuring private VLANs:

**Note**

---

In this section, the term *community VLAN* is used for both the unidirectional community VLANs and two-way community VLANs unless specifically differentiated.

---

**Note**

---

If VLAN port-provisioning verification is enabled, you must specify the VLAN name *in addition to the* VLAN number when assigning the switch ports to the primary and secondary VLANs. For more information, see the [“Enabling or Disabling VLAN Port-Provisioning Verification” section on page 11-12](#).

---

- Designate one VLAN as the primary VLAN.
- You have the option of designating one VLAN as an isolated VLAN, but you can use only one isolated VLAN.

- You have the option of using the private VLAN communities, but 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. You will achieve these results:
  - Isolated/community VLAN spanning-tree properties are set to those of the primary VLAN.
  - VLAN membership becomes static.
  - The access ports become the 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 the nontrunk ports or the MSFC ports as promiscuous ports.
- You must set VTP to transparent mode.




---

**Note** This restriction does not apply with VTP version 3.

---

- After you configure a private VLAN, you cannot change the VTP mode to client or server mode, because VTP does not support the private VLAN types and mapping propagation.
- You can configure the VLANs as primary, isolated, or community only if no access ports are currently assigned to the VLAN. Enter the **show port** command to verify that the VLAN has no access ports that are assigned to it.
- A primary VLAN can have one isolated VLAN and/or multiple communities that are associated with it.
- An isolated or community VLAN can have only one primary VLAN that is associated with it.
- The private VLANs can use VLANs 2–1000 and 1025–4096.
- If you delete either the primary or secondary VLAN, the ports that are associated with the VLAN become inactive.
- When configuring the private VLANs, note the hardware and software interactions as follows:
  - You cannot use the inband port, sc0, in a private VLAN.




---

**Note** With software release 6.3(1) and later releases, you can configure the sc0 port as a private VLAN port; however, you cannot configure the sc0 port as a promiscuous port.

---

- You cannot set the private VLAN ports to trunking mode, channeling, or have dynamic VLAN memberships, with the exception of the MSFC ports that always have trunking activated.
- You cannot set the 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 11-3](#). (Note that a promiscuous port can be defined in the same ASIC as a trunk port but not within the same ASIC as an isolated or community port.)

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



**Note**

---

Software release 8.6(1) and later releases provide support for configuring 802.1X with private VLANs. For more information, see the [“Configuring 802.1X Authentication with Private VLANs”](#) section on [page 40-41](#).

---

**Table 11-3** Modules with Ports Listed by ASIC Groups

Module Number	Description	Ports by ASIC
WS-X6224-100FX-MT	24-port 100BASE-FX multimode, MT-RJ	Ports 1–12 Ports 13–24
WS-X6324-100FX-SM WS-X6324-100FX-MM	24-port 100BASE-FX single mode or multimode, MT-RJ	Ports 1–12 Ports 13–24
WS-X6024-10FL-MT	24-port 10BASE-FL, MT-RJ	Ports 1–12 Ports 13–24
WS-X6248-TEL WS-X6248A-TEL WS-X6348-RJ-21(V) WS-X6148-RJ-21(V) WS-X6148-21AF	48-port 10/100BASE-TX, RJ-21	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6348-RJ-45 WS-X6348-RJ-45(V) WS-X6248-RJ-45 WS-X6248A-RJ-45 WS-X6148-RJ-45(V) WS-X6148-45AF	48-port 10/100BASE-TX, RJ-45	Ports 1–12 Ports 13–24 Ports 25–36 Ports 37–48
WS-X6148-GE-TX WS-X6148V-GE-TX WS-X6148-GE-45AF WS-X6548-GE-TX WS-X6548V-GE-TX WS-X6548-GE-45AF	48-port 10/100/1000BASE-TX, RJ-45	Ports 1–8 Ports 9–16 Ports 17–24 Ports 25–32 Ports 33–40 Ports 41–48

- The isolated and community ports should run the BPDU guard features to prevent the spanning-tree loops due to misconfigurations.
- The primary VLANs and associated isolated/community VLANs must have the same spanning-tree configuration. This configuration maintains the consistent spanning-tree topologies between the associated primary, isolated, and community VLANs and avoids possible connectivity loss. These priorities and parameters automatically propagate from the primary VLAN to the isolated and community VLANs.
- You can create the private VLANs that run in MISTP mode as follows:
  - If you disable MISTP, any change to the configuration of a primary VLAN propagates to all corresponding isolated and community VLANs, and you cannot change the isolated or community VLANs.
  - If you enable MISTP, you can only configure the MISTP instance with the primary VLAN. The changes will be applied to the primary VLAN and will propagate to the isolated and community VLANs.

- In the networks with some switches using MAC address reduction, and others not using MAC address reduction, the STP parameters do not necessarily propagate to ensure that the spanning-tree topologies match. You should manually check the STP configuration to ensure that the primary, isolated, and community VLANs' spanning-tree topologies match.
- If you enable MAC address reduction on a Catalyst 6500 series switch, you might want to enable MAC address reduction on all the switches in your network to ensure that the STP topologies of the private VLANs match. Otherwise, in a network where private VLANs are configured, if you enable MAC address reduction on some switches and disable it on others (mixed environment), you will have to use the default bridge priorities to make sure that the root bridge is *common* to the primary VLAN and to all its associated isolated and community VLANs. Be consistent with the ranges that are employed by the MAC address reduction feature regardless of whether it is enabled on the system. MAC address reduction allows only discrete levels and uses *all* intermediate values internally as a range. You should disable a root bridge with private VLANs and MAC address reduction, and configure the root bridge with any priority higher than the highest priority *range* that is used by any nonroot bridge.
- BPDU guard mode is system wide and is enabled after you add the first port to a private VLAN.
- 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 VLAN-based SPAN (VSPAN) to span the primary, isolated, and community VLANs together, or use SPAN on only one VLAN to separately monitor the egress or ingress traffic.
- You cannot use a remote SPAN VLAN (RSPAN) for a private VLAN.
- You cannot enable EtherChannel on the isolated, community, or promiscuous ports.
- You can apply the different VACLs and the quality of service (QoS) ACLs to the primary, isolated, and community VLANs.




---

**Note** For information on configuring the ACLs, see the [“Configuring ACLs on Private VLANs” section on page 15-43](#).

---

- You need to configure the output ACLs on both the two-way community VLANs and the primary VLAN in order to be applied to all outgoing traffic from the MSFC.
- If you map a Cisco IOS ACL to a primary VLAN, the Cisco IOS ACL automatically maps to the associated isolated and community VLANs.
- You cannot map the Cisco IOS ACLs to an isolated or community VLAN.
- You cannot use policy-based routing (PBR) on a private VLAN interface. You get an error message if you try to apply a policy to a private VLAN interface using the **ip policy route-map** *route\_map\_name* command.
- You cannot set a VLAN to a private VLAN if the VLAN has the dynamic access control entries (ACEs) configured.
- You can stop the 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 Primary Private VLAN

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

	Task	Command
Step 1	Create the primary private VLAN.	<b>set vlan</b> <i>vlan</i> <b>pvlan-type primary</b>
Step 2	Set the isolated, community, or two-way community VLAN(s).	<b>set vlan</b> <i>vlan</i> <b>pvlan-type</b> { <b>isolated</b>   <b>community</b>   <b>twoway-community</b> }
Step 3	Bind the isolated, community, or two-way community VLAN(s) to the primary VLAN.	<b>set pvlan</b> <i>primary_vlan</i> { <i>isolated_vlan</i>   <i>community_vlan</i>   <i>twoway_community_vlan</i> }
Step 4	Associate the isolated, community, or two-way community port(s) to the primary private VLAN.	<b>set pvlan</b> <i>primary_vlan</i> { <i>isolated_vlan</i>   <i>community_vlan</i>   <i>twoway_community_vlan</i> } [ <i>mod/ports</i>   <b>sc0</b> ]
Step 5	Map the isolated, community, or two-way community VLAN to the primary private VLAN on the promiscuous port.	<b>set pvlan mapping</b> <i>primary_vlan</i> { <i>isolated_vlan</i>   <i>community_vlan</i>   <i>twoway_community_vlan</i> } <i>mod/ports</i>
Step 6	Verify the primary private VLAN configuration.	<b>show pvlan</b> [ <i>vlan</i> ] <b>show pvlan mapping</b>



### Note

You can bind the isolated, community, or two-way community port(s) and associated isolated, community, or two-way community VLANs to the private VLAN by entering the **set pvlan** *primary\_vlan* { *isolated\_vlan* | *community\_vlan* | *twoway\_community\_vlan* } *mod/port* command.



### Note

The 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.



### Note

You must enter the **set pvlan** command everywhere that a private VLAN needs to be created, which includes the switches with the isolated, community, or two-way community ports, the switches with the promiscuous ports, and all *intermediate* switches that need to carry the private VLANs on their trunks. On the edge switches that do not have any isolated, community, two-way community, or promiscuous ports (typically, the access switches with no private ports), you do not need to create the private VLANs and you can prune the private VLANs from the trunks for security reasons.

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 ports 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 lq 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 lq 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...

```

## Viewing the Port Capability of a Private VLAN Port

You can view the port capability of a port in a private VLAN by entering the **show pvlan capability mod/port** command.

This example shows the port capability for several ports in the following configuration:

```

Console> (enable) set pvlan 10 20
Console> (enable) set pvlan mapping 10 20 3/1
Console> (enable) set pvlan mapping 10 20 5/2
Console> (enable) set trunk 5/1 desirable isl 1-1005,1025-4094

```

```

Console> (enable) show pvlan capability 5/20
Ports 5/13 - 5/24 are in the same ASIC range as port 5/20.

```

Port 5/20 can be made a private vlan port.

```

Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
10      20      isolated

```

```

Console> (enable) show pvlan capability 3/1
Port 3/1 cannot be made a private vlan port due to:
-----
Promiscuous ports cannot be made private vlan ports.

Console> (enable) show pvlan capability 5/1
Ports 5/1 - 5/12 are in the same ASIC range as port 5/1.

Port 5/1 cannot be made a private vlan port due to:
-----
Trunking ports are not Private Vlan capable.
Conflict with Promiscuous port(s) : 5/2

Console> (enable) show pvlan capability 5/2
Ports 5/1 - 5/12 are in the same ASIC range as port 5/2.

Port 5/2 cannot be made a private vlan port due to:
-----
Promiscuous ports cannot be made private vlan ports.
Conflict with Trunking port(s) : 5/1

Console> (enable) show pvlan capability 5/3
Ports 5/1 - 5/12 are in the same ASIC range as port 5/3.

Port 5/3 cannot be made a private vlan port due to:
-----
Conflict with Promiscuous port(s) : 5/2
Conflict with Trunking port(s) : 5/1

Console> (enable) show pvlan capability 15/1
Port 15/1 cannot be made a private vlan port due to:
-----
Only ethernet ports can be added to private vlans.

```

## 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, Community, or Two-Way Community VLAN

If you delete an isolated, community, or two-way community VLAN, the binding with the primary VLAN is broken, any isolated, community, or two-way community ports that are 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</i>   <i>community_vlan</i>   <i>twoway_community_vlan</i> }

This example shows how to delete 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, community, or two-way 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.

You might set a private VLAN port to inactive for the following reasons:

- The primary, isolated, community, or two-way community VLAN to which it belongs is cleared.
- All mappings from a non-MSFC promiscuous port are deleted.
- An error occurs when you are configuring a port as 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>twoway-community</i> } { <i>mod/ports</i> }

This example shows how to delete the mapping of VLANs 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)
```

## Private VLAN Support on the MSFC

These items describe the private VLAN support on the MSFC:

- Enter the **show pvlan** command to display information about the private VLANs. The **show pvlan** command displays information about the private VLANs only when the primary private VLAN is up.
- Entering the **set pvlan mapping** or the **clear pvlan mapping** command on the supervisor engine generates the MSFC syslog messages. See the following for an example:

```
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Created a private vlan mapping, Primary 200, Secondary 201
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 101
```

- Enter the **interface vlan** command to configure the Layer 3 parameters only for the primary private VLANs.
- On the supervisor engine, you cannot create the isolated or community VLANs using the VLAN numbers for which the **interface vlan** commands have been entered on the MSFC.
- The ARP entries that are learned on the Layer 3 private VLAN interfaces are sticky ARP entries (we recommend that you display and verify the private VLAN interface ARP entries).
- For security reasons, the private VLAN interface sticky ARP entries do not age out. Connecting new equipment with the same IP address generates a message and the ARP entry is not created.
- Because the private VLAN interface ARP entries do not age out, you must manually remove the private VLAN interface ARP entries if a MAC address changes.
- You can add or remove the private VLAN ARP entries manually as follows:

```
obelix-rp(config)# no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30

obelix-rp(config)# arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by hw:0000.5403.2356
```

- Some commands clear and recreate the private VLAN mapping as follows:

```
obelix-rp(config)# xns routing
obelix-rp(config)#
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 102
%PV-6-PV_MSG:Purged a private vlan mapping, Primary 100, Secondary 103
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 101
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 102
%PV-6-PV_MSG:Created a private vlan mapping, Primary 100, Secondary 103
```

## Configuring FDDI VLANs on the Switch

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</i> [ <b>name</b> <i>name</i> ] <b>type</b> { <b>fddi</b>   <b>fddinet</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</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.	<code>set vlan <i>vlan</i> [name <i>name</i>] [state {active   suspend}] [said <i>said</i>] [mtu <i>mtu</i>]</code>
Step 2	Verify the VLAN configuration.	<code>show vlan [<i>vlan</i>]</code>

## Configuring Token Ring VLANs on the Switch

These sections describe the two Token Ring VLAN types that are supported on the switches running VTP version 2:

- [Understanding How Token Ring TrBRF VLANs Work](#), page 11-31
- [Understanding How Token Ring TrCRF VLANs Work](#), page 11-32
- [Token Ring VLAN Configuration Guidelines](#), page 11-34
- [Creating or Modifying a Token Ring TrBRF VLAN](#), page 11-34
- [Creating or Modifying a Token Ring TrCRF VLAN](#), page 11-35

You must use VTP version 2 to configure and manage the Token Ring VLANs.



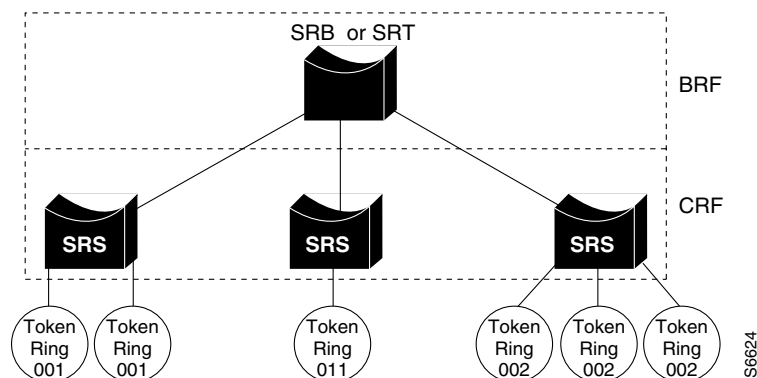
**Note**

Catalyst 6500 series switches do not support the ISL-encapsulated Token Ring frames.

## Understanding How Token Ring TrBRF VLANs Work

The Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple the Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see [Figure 11-3](#)). The TrBRF can be extended across a network of switches that are interconnected through the trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

**Figure 11-3** 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 as a source-route transparent (SRT) bridge running either the IBM or IEEE STP. If SRB is used, you can define the duplicate MAC addresses on the different logical rings.

The Token Ring software runs an instance of STP for each TrBRF VLAN and each TrCRF VLAN. For the TrCRF VLANs, STP removes loops in the logical ring. For the TrBRF VLANs, STP interacts with the external bridges to remove the loops from the bridge topology, similar to STP operation on the 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 “[Default VLAN Configuration](#)” section on page 11-3.

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, the duplicate MAC addresses can be defined on the different logical rings.

To accommodate the 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 that are connected to TrCRFs) to operate in SRB mode while others operate in SRT mode.

## Understanding How Token Ring TrCRF VLANs Work

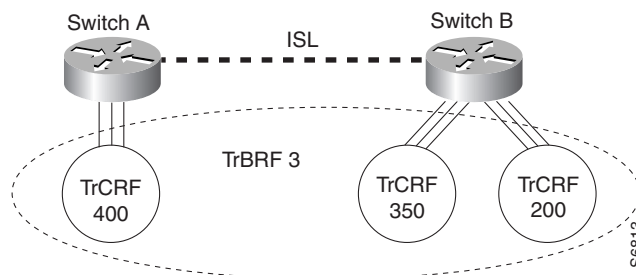
The TrCRF VLANs define the port groups with the same logical ring number. You can configure two TrCRF types in your network: undistributed and backup.

Typically, the TrCRFs are undistributed, which means that 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 11-4](#)). The parent TrBRF acts as a multiport bridge, forwarding the traffic between the undistributed TrCRFs.

**Note**

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

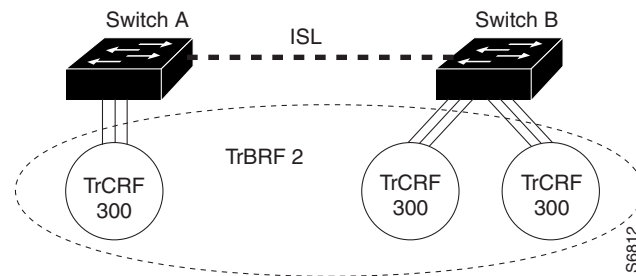
**Figure 11-4** Undistributed TrCRFs



**Note**

By default, the 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 11-5](#)), and the traffic is passed between the default TrCRFs that are located on separate switches if the switches are connected through an ISL trunk.

**Figure 11-5 Distributed TrCRF**



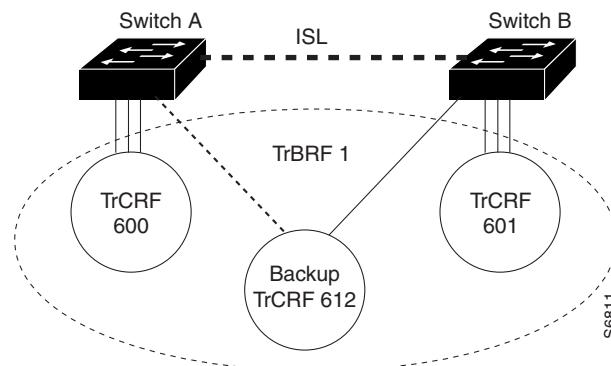
Within a TrCRF, source-route switching forwards the frames that are based on either the MAC addresses or the route descriptors. The entire VLAN can operate as a single ring, with frames that are switched between the ports within a single TrCRF.

You can specify the maximum hop count for the All-Routes and Spanning Tree Explorer frames for each TrCRF to limit the maximum number of hops that an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of specified hops, it does not forward the frame. The TrCRF determines the number of hops that 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 the traffic between the undistributed TrCRFs located on separate switches that are connected by a TrBRF if 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 the 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 11-6](#) shows the backup TrCRF.

**Figure 11-6 Backup TrCRF**



## Token Ring VLAN Configuration Guidelines

This section describes the guidelines for creating or modifying the Token Ring VLANs:

- For the Token Ring VLANs, 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; that is, the parent TrBRF VLAN you specify for the TrCRF must already exist.
- In a Token Ring environment, the logical ports of the TrBRF (the connection between the TrBRF and the TrCRF) 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.

## Creating or Modifying a Token Ring TrBRF VLAN

You must enable VTP version 2 before you create the Token Ring VLANs. For information on enabling VTP version 2, see [Chapter 10, “Configuring VTP.”](#)

You must specify a bridge number when you create a new TrBRF.

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</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>bridgeber</i> [ <b>stp</b> { <b>ieee</b>   <b>ibm</b> }]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</i> ]

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</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>bridgeber</i> ] [ <b>stp</b> { <b>ieee</b>   <b>ibm</b> }]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</i> ]

## Creating or Modifying a Token Ring TrCRF VLAN



**Note** You must enable VTP version 2 before you create the Token Ring VLANs. For information on enabling VTP version 2, see [Chapter 10, “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</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_ringber</i>   <b>decring</b> <i>decimal_ringber</i> } <b>parent</b> <i>vlan</i>
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</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 VLAN.	<b>set vlan</b> <i>vlan</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</i> ] [ <b>decring</b> <i>decimal_ring</i> ] [ <b>bridge</b> <i>bridge</i> ] [ <b>parent</b> <i>vlan</i> ]
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</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</i> <b>backupcrf on</b>
Step 2	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</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 the All-Routes Explorer frames or the Spanning Tree Explorer frames in the TrCRF, perform this task in privileged mode:

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

This example shows how to limit the 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)

```

# Configuring VLANs for the Firewall Services Module

Enter the **set vlan {vlans} firewall-vlan {mod}** command to specify the VLANs that are secured by a Firewall Services Module (WS-SVC-FWM-1-K9). Enter the **show vlan firewall-vlan mod** command to display the VLANs that are secured by the Firewall Services Module.

To secure a range of VLANs on a Firewall Services Module, these conditions must be satisfied:



## Note

VLAN 1 cannot be secured to the Firewall Services Module.

1. The port membership must be defined for the VLANs, and the VLANs must be in the active state.
2. The VLANs cannot have a Layer 3 interface in the active state on the MSFC.
3. The VLANs cannot be reserved VLANs.

The VLANs that do not satisfy condition number 2 in the list above are discarded from the range of VLANs that you attempt to secure on the Firewall Services Module.

The VLANs that meet condition number 2 and condition number 3 but do not meet condition number 1 are stored in the supervisor engine database; these VLANs are sent to the Firewall Services Module as soon as they meet condition number 1.

This example shows how to secure a range of VLANs on a Firewall Services Module:

```
Console> (enable) set vlan 2-55 firewall-vlan 7
Console> (enable)
```

Enter the **set firewall multiple-vlan-interfaces {enable | disable}** command to set the multiple VLAN interface feature for a Firewall Services Module. Disabling the multiple VLAN interface feature sets the Firewall Services Module to single VLAN interface mode. The multiple VLAN interface feature is disabled by default. An example is as follows:

```
Console> (enable) set firewall multiple-vlan-interfaces enable
This command will enable multiple-vlan-interfaces feature for all firewall
modules in the chassis.
It can result in traffic bypassing the firewall module.
Do you want to continue (y/n) [n]? y
multiple-vlan-interfaces feature enabled for firewall module 5.
Console> (enable)
```

With software release 8.4(1) and later releases, you can enter the **set vlan {vlan} firewall-vlan {mod} msfc-fwsm-interface** command to make the specified VLAN the secured interface between the MSFC and the Firewall Services Module. This command is available only in the single VLAN interface mode and cannot be entered when multiple VLAN interfaces are enabled. An example is as follows:

```
Console> (enable) set vlan 3 firewall-vlan 5 msfc-fwsm-interface
Vlan 3 declared as Secure Vlan interface for module 5
Vlan 3 declared secure for firewall module 5
Console> (enable)
```



## Note

For detailed Firewall Services Module configuration information, refer to the Firewall Services Module documentation at this URL:

[http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd\\_products\\_support\\_model\\_home.html](http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html)

