



## 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 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 Normal-Range VLANs on the Switch, page 11-5](#)
- [Configuring Extended-Range VLANs on the Switch, page 11-6](#)
- [Mapping VLANs to VLANs, page 11-8](#)
- [Assigning Switch Ports to a VLAN, page 11-12](#)
- [Deleting a VLAN, page 11-13](#)
- [Configuring Private VLANs on the Switch, page 11-14](#)
- [Configuring FDDI VLANs on the Switch, page 11-24](#)
- [Configuring Token Ring VLANs on the Switch, page 11-25](#)
- [Configuring VLANs for the Firewall Services Module, page 11-31](#)

## 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 end stations even if they are not located physically on the same LAN segment.

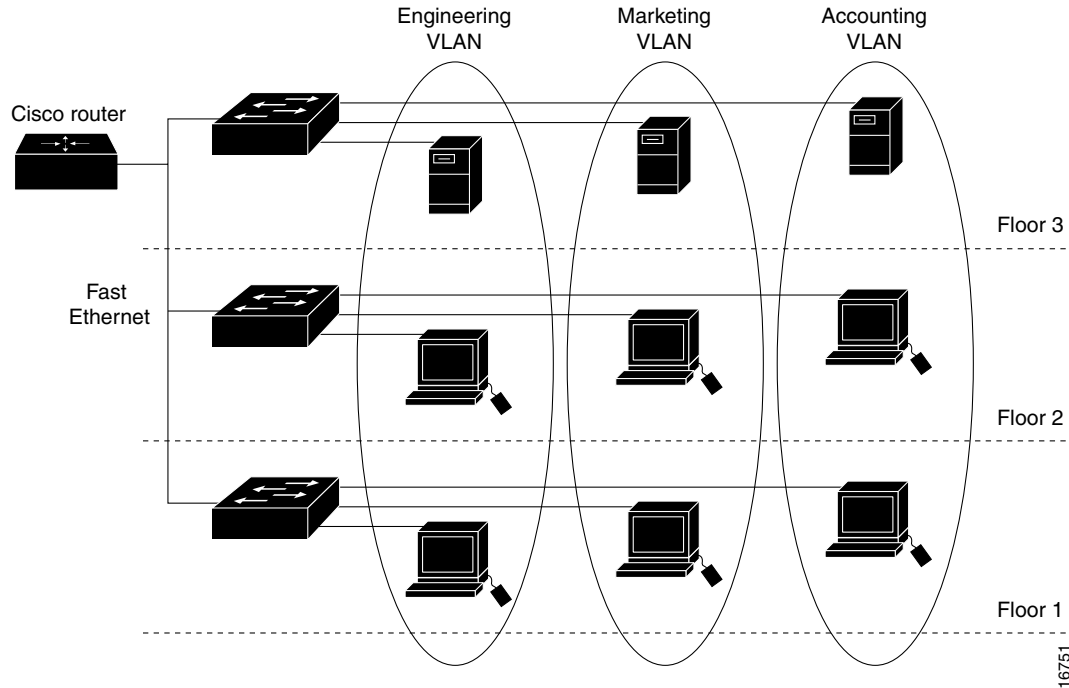
VLANs allow you to group ports on a switch to limit unicast, multicast, and broadcast traffic flooding. Flooded traffic originating from a particular VLAN is only flooded out ports belonging to that VLAN.

[Figure 11-1](#) shows an example of VLANs segmented into logically defined networks.

These sections describe VLANs:

- [VLAN Ranges, page 11-2](#)
- [Configurable VLAN Parameters, page 11-3](#)
- [Default VLAN Configuration, page 11-4](#)

Figure 11-1 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.

## VLAN Ranges

Catalyst 6500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several 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.

There are three ranges of VLANs:

- Normal-range VLANs: 1–1000
- Extended-range VLANs: 1025–4094
- Reserved-range VLANs: 0, 1002–1024, 4095

Table 11-1 describes the VLAN ranges.

**Table 11-1 VLAN Ranges**

VLANs	Range	Usage	Propagated by VTP (Y/N)
0, 4095	Reserved range	For system use only. You cannot see or use these VLANs.	N/A
1	Normal range	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1000	Normal range	Used for Ethernet VLANs; you can create, use, and delete these VLANs.	Yes
1001	Normal range	You cannot create or use this VLAN. May be available in the future.	Yes
1002–1005	Reserved range	Cisco defaults for FDDI and Token Ring. Not supported on Catalyst 6500 series switches. You cannot delete these VLANs.	N/A
1006–1009	Reserved range	Cisco defaults. Not currently used but may be used for defaults in the future. You can map nonreserved VLANs to these reserved VLANs when necessary.	N/A
1010–1024	Reserved range	You cannot see or use these VLANs but you can map nonreserved VLANs to these reserved VLANs when necessary.	N/A
1025–4094	Extended range	For Ethernet VLANs only. You can create, use, and delete these VLANs, with the following exception:  FlexWAN modules and routed ports automatically allocate a sequential block of internal VLANs starting at VLAN 1025. If you use these devices, you must allow the required number of VLANs for them.	No

## 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.

- 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 11-2 shows the default VLAN configuration for the Catalyst 6500 series switches.

**Table 11-2 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, 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

**Table 11-2 VLAN Default Configuration (continued)**

Feature	Default Value
TrCRF bridge mode	SRB
Remote switched port analyzer (RSPAN)	Disabled

## Configuring Normal-Range VLANs on the Switch

These sections describe how to configure normal-range VLANs 2–1000:

- [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 normal-range VLANs 2–1000 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.)
- 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; VLAN names must be unique.

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

	Task	Command
<b>Step 1</b>	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> ]
<b>Step 2</b>	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</i> ]

This example shows how to create 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> { <b>active</b>   <b>suspend</b> }] [ <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 11-7](#)
- [Creating Extended-Range VLANs, page 11-7](#)

## Extended-Range VLAN Configuration Guidelines

This section describes the guidelines for creating extended-range VLANs 1025–4094:

- You can only create Ethernet-type VLANs in the extended range.
- You must enable MAC address reduction in order to use extended-range VLANs.
- You can only create and delete extended-range VLANs from the CLI or SNMP.
- You cannot use VTP to manage these VLANs; they must be statically configured on each switch.
- You cannot use extended-range VLANs if you have dot1q-to-isl mappings.
- You can configure private VLAN parameters and RSPAN for extended-range VLANs; however, all other parameters for 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 VLANs for routed ports or FlexWAN modules. The block of VLANs is always allocated starting from VLAN 1025. If you have any VLANs within the range that is required by the FlexWAN module, all of the VLANs that are required will not be allocated, because VLANs are never allocated from the user's VLAN area.

**Caution**

FlexWAN modules and routed ports automatically allocate a sequential block of internal VLANs starting at VLAN 1025. If you use these devices, you *must* allow the required number of VLANs for them and *must* not use the lower-range VLANs starting with VLAN 1025. If not enough VLANs are available for the FlexWAN module, some ports may not work. You *must* use the highest VLANs first. For example, use VLAN 4090, then VLAN 4089, and so forth.

**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 extended-range VLANs, you must first enable MAC address reduction, which provides IDs for 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 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 11-11 for more information.

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

You can map VLANs to other VLANs on the Catalyst 6500 series switches in two ways:

1. From non-Cisco devices in your network using VLANs 1006–1024 to nonreserved VLANs on the Catalyst 6500 series switches.
2. From VLANs on non-Cisco devices on 802.1Q trunks to ISL trunks on the Catalyst 6500 series switches.



### Note

If you use method 1, you can use extended-range VLANs (1025–4094) on the switch; if you use method 2, you can retain mappings from a previous Catalyst 6500 series software release but you cannot use extended-range VLANs.

This section describes how to map VLANs to VLANs:

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

## Mapping Reserved VLANs to Nonreserved VLANs

You can map reserved-range VLANs to any nonreserved VLANs that are not in use. Nonreserved VLANs are any VLANs that are not reserved by Cisco; this includes normal-range and extended-range VLANs.



### Note

If you have dot1q-to-isl VLAN mappings from a previous Catalyst 6500 series switch software release, you cannot use the mapped VLANs to map reserved VLANs to nonreserved VLANs. Optionally, you can clear the dot1q-to-isl mappings and then use those reserved VLANs.

These restrictions apply when mapping reserved VLANs to nonreserved VLANs:

- You can create up to eight reserved-to-nonreserved VLAN mappings on the switch.
- You can only map Ethernet VLANs to Ethernet VLANs.
- Reserved VLAN mappings are local to each switch. You must configure the VLAN mappings on all applicable switches in the network.

To map a reserved VLAN to a nonreserved VLAN, perform this task in privileged mode:

	Task	Command
Step 1	If necessary, clear old dot1q-to-isl VLAN mappings.	<b>clear vlan mapping dot1q all</b>
Step 2	Map a reserved VLAN to a nonreserved VLAN.	<b>set vlan mapping reserved {reserved_vlan} non-reserved {nonreserved_vlan}</b>
Step 3	Verify the VLAN mapping.	<b>show vlan mapping</b>

This example shows how to clear old VLAN mappings, map a reserved VLAN, and verify the mappings on the mapping table:

```

Console> (enable) clear vlan mapping dot1q all
All dot1q vlan mapping entries deleted
Console> (enable) set vlan mapping reserved 1020 non-reserved 4070
Vlan 1020 successfully mapped to 4070.
Console> (enable) show vlan mapping
Reserved vlan   Non-Reserved vlan   Effective
-----
1008            63                  false
1010            4065                 true
1011            4066                 true
1020            4070                 true

```

The Effective column in the mapping table indicates whether the mapping has taken effect (that is, *true* or *false*). Mappings that are marked true can be used by the system. Mappings that are marked false cannot be used by the system.

**Note**

Reserved VLAN mappings are entered on the table in the order in which you map them. If you delete a mapping, the line where it existed will not display on the table. However, the next mapping you create will appear where the old one was deleted.

## Deleting Reserved-to-Nonreserved VLAN Mappings

To delete the mappings for reserved-to-nonreserved VLAN mappings, you can delete the mappings one at a time or all at once.

When you delete all entries from the mapping table at once, the table is completely cleared and the nonreserved VLANs still exist in the list of VLANs.

To delete reserved VLAN mappings, perform this task in privileged mode:

	Task	Command
Step 1	Delete the reserved VLAN.	<b>clear vlan mapping reserved</b> { <i>reserved_vlan</i>   <b>all</b> }
Step 2	Delete the nonreserved VLAN.	<b>clear vlan</b> <i>vlan</i>
Step 3	Verify that the mapping table entry has been cleared.	<b>show vlan mapping</b>

This example shows how to delete a single mapping:

```
Console> (enable) clear vlan mapping reserved 1010
Vlan 1010 mapping entry deleted
Console> (enable)
```

This example shows how to delete all reserved VLAN mappings:

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

## Mapping 802.1Q VLANs to ISL VLANs

Your network might have non-Cisco devices that are connected to the Catalyst 6500 series switches through 802.1Q trunks or traffic from a non-Cisco switch that has VLANs in the Catalyst 6500 series reserved range, 1002–1024.

The valid range of user-configured Inter-Switch Link (ISL) VLANs is 1 to 1000 and 1025 to 4094. The valid range of VLANs that are specified in the IEEE 802.1Q standard is 0–4095. In a network environment with non-Cisco devices that are connected to Cisco switches through 802.1Q trunks, you can map 802.1Q VLAN numbers greater than 1000 to ISL VLAN numbers. Note that 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.

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:

- 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 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 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
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)

```

## 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 {<i>dot1q_vlan</i>   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)
```

## 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 switch ports to a VLAN of the proper type. For example, 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 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 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)

```

## Deleting a VLAN

Follow these guidelines for deleting 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.
- 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 thus 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 Private VLANs on the Switch

These sections describe how private VLANs work:

- [Understanding How Private VLANs Work, page 11-14](#)
- [Private VLAN Configuration Guidelines, page 11-15](#)
- [Creating a Primary Private VLAN, page 11-19](#)
- [Viewing the Port Capability of a Private VLAN Port, page 11-21](#)
- [Deleting a Private VLAN, page 11-22](#)
- [Deleting an Isolated, Community, or Two-Way Community VLAN, page 11-23](#)
- [Deleting a Private VLAN Mapping, page 11-23](#)
- [Private VLAN Support on the MSFC, page 11-24](#)

## Understanding How Private VLANs Work

Private VLANs provide Layer-2 isolation between ports within the same private VLAN on the Catalyst 6500 series 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.

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.
- **Isolated**—This port has complete Layer 2 separation from 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 outgoing traffic to all isolated ports. All isolated ports are assigned to an isolated VLAN where this hardware function occurs. 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 incoming traffic from the promiscuous port to all other promiscuous, isolated, community, and two-way 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 within its private VLAN and can only be received by its promiscuous ports.
- **Community VLAN**—Unidirectional VLAN that is used by a group of community ports to communicate among themselves and transmit traffic to outside the private VLAN through the designated promiscuous port.
- **Two-way community VLAN**—Bidirectional VLAN that is used by a group of community ports to communicate among themselves and to and from community ports from and to the Multilayer Switch Feature Card (MSFC).

**Note**

With software release 6.2(1) and later releases, you can use 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 outbound and inbound traffic can be carried on the same VLAN allowing VLAN-based features such as 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 private VLANs across multiple Ethernet switches by trunking the primary, isolated, and any community or two-way community VLANs to other switches that support 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 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 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 only be mapped 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 unidirectional community VLANs and two-way community VLANs unless specifically differentiated.

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

- You have the option of using 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.
  - 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 the nontrunk ports or the MSFC ports as promiscuous ports.
- You must set VTP to transparent mode.
- After 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.
- You can configure 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.
- 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 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 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 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.

**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

- 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 connectivity loss. These priorities and parameters automatically propagate from the primary VLAN to the isolated and community VLANs.
- You can create 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. Changes will be applied to the primary VLAN and will propagate to the isolated and community VLANs.

- In networks with some switches using MAC address reduction, and others not using MAC address reduction, 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 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* 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 primary, isolated, and community VLANs together, or use SPAN on only one VLAN to separately monitor egress or ingress traffic.
- You cannot use a remote SPAN VLAN (RSPAN) for a private VLAN.
- You cannot enable EtherChannel on isolated, community, or promiscuous ports.
- You can apply different VACLs and quality of service (QoS) ACLs to primary, isolated, and community VLANs.




---

**Note** For information on configuring ACLs, see the [“Configuring ACLs on Private VLANs” section on page 16-38](#).

---

- Output ACLs need to be configured 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 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 dynamic access control entries (ACEs) configured.
- 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 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> { <i>isolated</i>   <i>community</i>   <i>twoway-community</i> }
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 using the **set pvlan** *primary\_vlan* { *isolated\_vlan* | *community\_vlan* | *twoway\_community\_vlan* } *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.



### Note

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

- Enter the **show pvlan** command to display information about private VLANs. The **show pvlan** command displays information about 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 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 Layer 3 parameters only for primary private VLANs.
- On the supervisor engine, you cannot create isolated or community VLANs using VLAN numbers for which **interface vlan** commands have been entered on the MSFC.
- ARP entries learned on Layer 3 private VLAN interfaces are sticky ARP entries (we recommend that you display and verify private VLAN interface ARP entries).
- For security reasons, 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 private VLAN interface ARP entries if a MAC address changes.
- You can add or remove 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 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>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</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 switches running VTP version 2:

- [Understanding How Token Ring TrBRF VLANs Work](#), page 11-25
- [Understanding How Token Ring TrCRF VLANs Work](#), page 11-26
- [Token Ring VLAN Configuration Guidelines](#), page 11-28
- [Creating or Modifying a Token Ring TrBRF VLAN](#), page 11-28
- [Creating or Modifying a Token Ring TrCRF VLAN](#), page 11-29

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



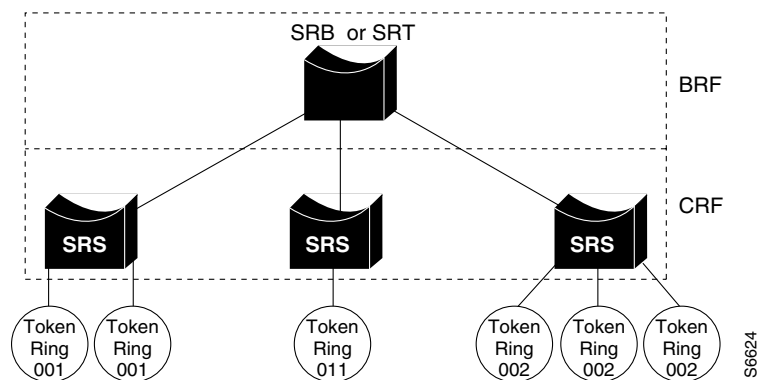
**Note**

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

## Understanding How Token Ring TrBRF VLANs Work

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see [Figure 11-2](#)). The TrBRF can be extended across a network of switches interconnected through trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

**Figure 11-2 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 as a 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 “[Default VLAN Configuration](#)” section on page 11-4.

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.

## Understanding How Token Ring TrCRF VLANs Work

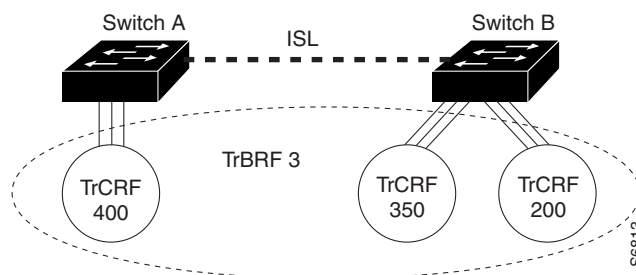
TrCRF VLANs define port groups with the same logical ring number. You can configure two TrCRF types in your network: undistributed and backup.

Typically, 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 11-3](#)). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

**Note**

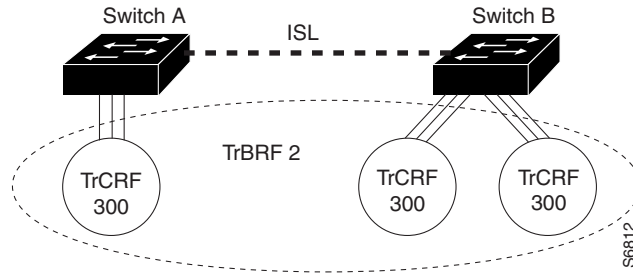
To pass data between rings that are located on separate switches, you can associate the rings to the same TrBRF and configure the TrBRF for SRB.

**Figure 11-3 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 11-4](#)), and traffic is passed between the default TrCRFs that are located on separate switches if the switches are connected through an ISL trunk.

Figure 11-4 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 that are switched between ports within a single TrCRF.

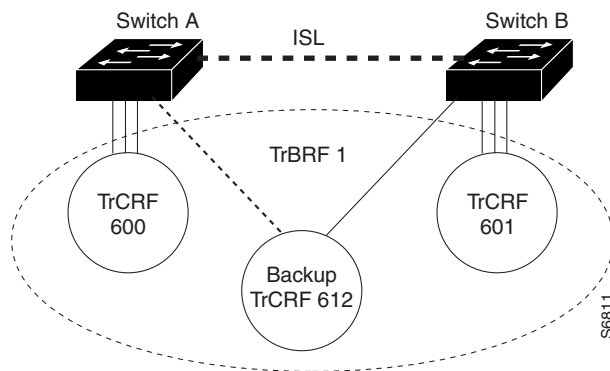
You can specify the maximum hop count for All-Routes and Spanning Tree Explorer frames for each TrCRF to limit the maximum number of hops that an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of hops specified, it does 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 11-5 shows the backup TrCRF.

Figure 11-5 Backup TrCRF



## Token Ring VLAN Configuration Guidelines

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

- For 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 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.	<code>set vlan <i>vlan</i> [<i>name name</i>] type <i>trbrf</i> [<i>said said</i>] [<i>mtu mtu</i>] <i>bridge</i> <i>bridgeber</i> [<i>stp {ieee   ibm}</i>]</code>
Step 2	Verify the VLAN configuration.	<code>show vlan [<i>vlan</i>]</code>

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 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 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 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</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</i> <b>stemaxhop</b> <i>hopcount</i>
Step 3	Verify the VLAN configuration.	<b>show vlan</b> [ <i>vlan</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)

```

## Configuring VLANs for the Firewall Services Module

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

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. 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.

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.

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)

```



### Note

---

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

---

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/fwsm/index.htm)

---

