Configuring VLANs

This chapter describes how to configure VLANs on the Cisco 7600 series routers.

Note For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html

This chapter contains these sections:

Understanding How VLANs Work

The following sections describe how VLANs work:

VLAN Overview

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

VLANs are usually 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. LAN port VLAN membership is assigned manually on an port-by-port basis.

VLAN Ranges

Note   You must enable the extended system ID to use 4096 VLANs (see the "Understanding the Bridge ID" section on page 19-2).

Cisco 7600 series routers 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 the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so you must configure extended-range VLANs manually on each network device.

Table 14-1 describes the VLAN ranges.

Table 14-1   VLAN Ranges

VLANs	Range	Usage	Propagated by VTP
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.	—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1001	Normal	For Ethernet VLANs; you can create, use, and delete these VLANs.	Yes
1002–1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.	Yes
1006–4094	Extended	For Ethernet VLANs only.	No

The following information applies to VLAN ranges:

- Layer 3 LAN ports, WAN interfaces and subinterfaces, and some software features use internal VLANs in the extended range. You cannot use an extended range VLAN that has been allocated for internal use.

- To display the VLANs used internally, enter the **show vlan internal usage** command.

- You can configure ascending internal VLAN allocation (from 1006 and up) or descending internal VLAN allocation (from 4094 and down).

- Switches running the Catalyst operating system do not support configuration of VLANs 1006–1024. If you configure VLANs 1006–1024, ensure that the VLANs do not extend to any switches running Catalyst software.

- You must enable the extended system ID to use extended range VLANs (see the "Understanding the Bridge ID" section on page 19-2).

Configurable VLAN Parameters

> **Note**
> - Ethernet VLAN 1 uses only default values.
> - Except for the VLAN name, Ethernet VLANs 1006 through 4094 use only default values.
> - You can configure the VLAN name for Ethernet VLANs 1006 through 4094.

You can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type (Ethernet, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF)
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

Understanding Token Ring VLANs

The following section describes the two Token Ring VLAN types supported on network devices running VTP version 2:

> **Note**
> Cisco 7600 series routers do not support Inter-Switch Link (ISL)-encapsulated Token Ring frames. When a Cisco 7600 series router is configured as a VTP server, you can configure Token Ring VLANs from the router.

Token Ring TrBRF VLANs

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see Figure 14-1). The TrBRF can be extended across a network devices interconnected via trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port*.

Figure 14-1   Interconnected Token Ring TrBRF and TrCRF VLANs
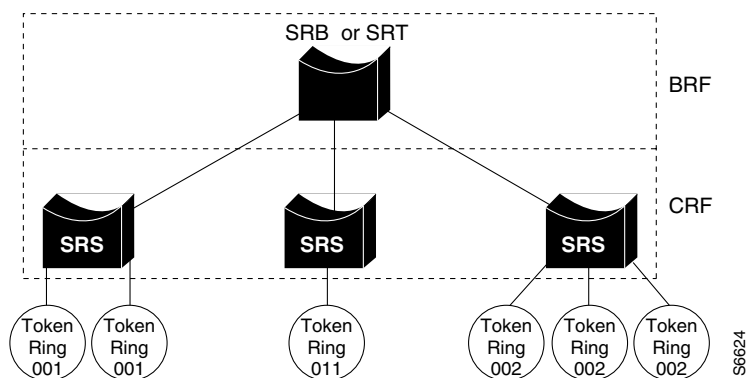
For source routing, the Cisco 7600 series router appears as a single bridge between the logical rings. The TrBRF can function as a source-route bridge (SRB) or a source-route transparent (SRT) bridge running either the IBM or IEEE STP. If an SRB is used, you can define duplicate MAC addresses on different logical rings.

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

Caution   Certain parent TrBRF STP and TrCRF bridge mode configurations can place the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF in a blocked state. For more information, see the "VLAN Interaction with Bridged Routed Encapsulation within an Automatic Protection Switching Group" section on page 14-8.

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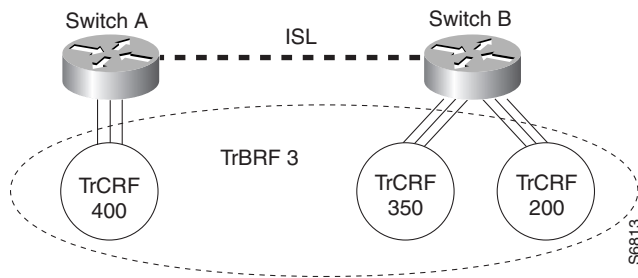
Token Ring TrCRF VLANs

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

TrCRFs typically are undistributed, which means each TrCRF is limited to the ports on a single network device. Multiple undistributed TrCRFs on the same or separate network devices can be associated with a single parent TrBRF (see Figure 14-2). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

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

Figure 14-2 **Undistributed TrCRFs**

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 14-3), and traffic is passed between the default TrCRFs located on separate network devices if the network devices are connected through an ISL trunk.

Figure 14-3 **Distributed TrCRF**
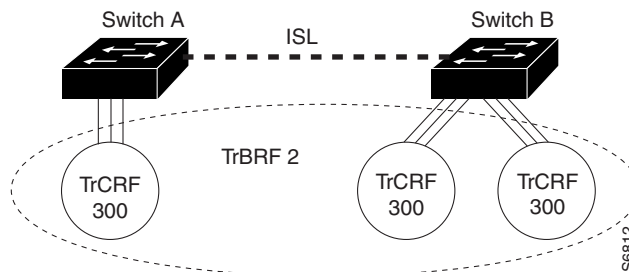
Within a TrCRF, source-route switching forwards frames based on either MAC addresses or route descriptors. The entire VLAN can operate as a single ring, with frames switched between ports within a single TrCRF.

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

If the ISL connection between network devices fails, you can use a backup TrCRF to configure an alternate route for traffic between undistributed TrCRFs. Only one backup TrCRF for a TrBRF is allowed, and only one port per network device can belong to a backup TrCRF.

If the ISL connection between the network devices fails, the port in the backup TrCRF on each affected network device 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 14-4 illustrates the backup TrCRF.

Figure 14-4   Backup TrCRF
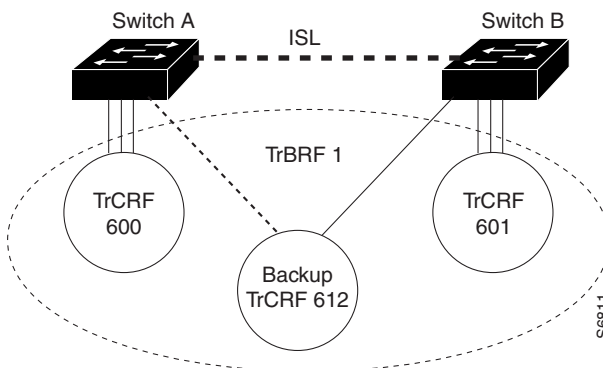
VLAN Default Configuration

Tables 14-2 through 14-6 show the default configurations for the different VLAN media types.

Table 14-2   Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094
VLAN name	"default" for VLAN 1 "VLAN*vlan_ID*" for other Ethernet VLANs	—
802.10 SAID	10*vlan_ID*	100001–104094
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Pruning eligibility	VLANs 2–1001 are pruning eligible; VLANs 1006–4094 are not pruning eligible.	—

Table 14-3   FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	"fddi-default"	—
802.10 SAID	101002	1–4294967294
MTU size	1500	1500–18190
Ring number	0	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005

Table 14-3   FDDI VLAN Defaults and Ranges (continued)

Parameter	Default	Range
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 14-4   Token Ring (TrCRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	"token-ring-default"	—
802.10 SAID	101003	1–4294967294
Ring Number	0	1–4095
MTU size	VTPv1 default 1500 VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Table 14-5   FDDI-Net VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	"fddinet-default"	—
802.10 SAID	101004	1–4294967294
MTU size	1500	1500–18190
Bridge number	1	0–15
STP type	ieee	auto, ibm, ieee
VLAN state	active	active, suspend

Table 14-6   Token Ring (TrBRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	"trnet-default"	—
802.10 SAID	101005	1–4294967294

Table 14-6   Token Ring (TrBRF) VLAN Defaults and Ranges (continued)

Parameter	Default	Range
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	1	0–15
STP type	ibm	auto, ibm, ieee
VLAN state	active	active, suspend

VLAN Interaction with Bridged Routed Encapsulation within an Automatic Protection Switching Group

In a Bridged Routed Encapsulation (BRE) scenario, an IP routed AAL5SNAP packet is bridged over the Ethernet side, adding a MAC header with a fake SRC MAC and configured distributed storage (DST). The ATM PVC traffic is relayed over an IP and not Ethernet. However, you cannot configure more than one virtual connection (VC) on the same VLAN. To configure more than one VC, customers configure two different VLANS on the protect and working interface of the Automatic Protection Switching (APS) group. This workaround is not a viable long- term solution because it results in high convergence time and an inefficient use of the VLANS. To resolve these limitations, you can use the BRE+APS feature to configure two VCs for the same VLAN, provided their parent interfaces too belong to the same Automatic Protection Switching (APS) group.

For information on configuring an APS group, see Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide at
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

Supported Line Cards

This feature is supported on the SIP-200 and SIP-400 line cards. For more information on the SIP implementation, see Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide at
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw.html.

Requirements and Restrictions

Follow these requirements and restrictions when you configure the BRE+APS feature:

- You can configure BRE-Connect VLANS for two different VCs if the new VC:
    - belongs to the same APS group to which the first VC belongs.
    - does not belong to the same ATM interface as the first VC.
- Before you change the APS parameters of an interface (changing the APS group or removing the APS configurations), first ensure that the BRE configurations on the interface are removed.
- When you configure BRE on an ATM interface, you cannot configure a L2 IP address at the BRE end, but you can configure an IP address at the L3 non BRE end.

Table 14-7   Show command for ATM VLAN BRE

	Command	Purpose
Step 1	Router(config)# **show atm vlan bre**	Verifies the configuration and displays the status of the PVC. An Active VC is displayed as **UP** and an inactive VC as **DN** (down).

This example shows how to verify the configuration of BRE ATM VLAN:

```
Router# show atm vlan bre
Interface      Bre VCD         VPI/VCI   Vlan Learned MAC    Virtual MAC    State
ATM3/0/0.1     1               0/11      100 0000.0000.0000 0000.0300.0001  UP
ATM3/0/0.2     2               1/13      200 0000.0000.0000 0000.0300.0002  UP
ATM4/0/0.2     2               1/13      300 0000.0000.0000 0000.0400.0002  DN
```

Warning Messages

Consider instances where you have configured APS on the main interface, and have configured BRE within a main interface and subinterface. The warning message "%ATM2/0/0 - Remove BRE configs on this interface before changing APS configs"appears when you attempt to modify the APS configurations in the main interface, without removing the BRE configurations first.

VLAN Configuration Guidelines and Restrictions

When creating and modifying VLANs in your network, follow these guidelines and restrictions:

- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file** *file_name* command on a router that has a redundant supervisor engine.

- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.

- VLAN database mode, which was available in Release 12.2(18)SXD and earlier releases, is no longer supported. In addition, RPR+ redundancy does not support configurations entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

- Before you can create a VLAN, the Cisco 7600 series router must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see Chapter 13, "Configuring VTP."

- The VLAN configuration is stored in the vlan.dat file, which is stored in nonvolatile memory. You can cause inconsistency in the VLAN database if you manually delete the vlan.dat file. If you want to modify the VLAN configuration or VTP, use the commands described in this guide and in the *Cisco 7600 Series Router Cisco IOS Command Reference* publication.

- To do a complete backup of your configuration, include the vlan.dat file in the backup.

- Cisco 7600 series routers do not support Token Ring or FDDI media. The router does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it can propagate the VLAN configuration through VTP.

- When a Cisco 7600 series router is configured as a VTP server, you can configure FDDI and Token Ring VLANs from the router.

- You must configure a TrBRF before you configure the TrCRF (the parent TrBRF VLAN you specify must exist).

- In a Token Ring environment, the logical interfaces (the connection between the TrBRF and the TrCRF) of the TrBRF are placed in a blocked state if either of these conditions exists:

– The TrBRF is running the IBM STP, and the TrCRF is in SRT mode.

– The TrBRF is running the IEEE STP, and the TrCRF is in SRB mode.

Configuring VLANs

These sections describe how to configure VLANs:

- VLAN Configuration Background Information, page 14-10
- Creating or Modifying an Ethernet VLAN, page 14-10
- Assigning a Layer 2 LAN Interface to a VLAN, page 14-14
- Configuring the Internal VLAN Allocation Policy, page 14-14
- Configuring VLAN Translation, page 14-15
- Mapping 802.1Q VLANs to ISL VLANs, page 14-18

Note VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Cisco 7600 Series Router Cisco IOS Command Reference* publication.

VLAN Configuration Background Information

If the router is in VTP server or transparent mode (see the "Configuring VTP" section on page 13-8), you can configure VLANs in global and config-vlan configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the vlan.dat files. To display the VLAN configuration, enter the **show vlan** command.

If the router is in VLAN transparent mode, use the copy **running-config startup-config** command to save the VLAN configuration to the startup-config file. After you save the running configuration as the startup configuration, use the **show running-config** and **show startup-config** commands to display the VLAN configuration.

Note • When the router boots, if the VTP domain name and VTP mode in the startup-config and vlan.dat files do not match, the router uses the configuration in the vlan.dat file.

- VLAN database mode, which was available in Release 12.2(18)SXD and earlier releases, is no longer supported.

- RPR+ redundancy does not support configurations entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

Creating or Modifying an Ethernet VLAN

User-configured VLANs have unique IDs from 1 to 4094, except for reserved VLANs (see Table 14-1 on page 14-2). Enter the **vlan** command with an unused ID to create a VLAN. Enter the **vlan** command for an existing VLAN to modify the VLAN (you cannot modify an existing VLAN that is being used by a Layer 3 port or a software feature).

See the "VLAN Default Configuration" section on page 14-6 for the list of default parameters that are assigned when you create a VLAN. If you do not specify the VLAN type with the **media** keyword, the VLAN is an Ethernet VLAN.

To create or modify a VLAN, perform this task:

	Command	Purpose
Step 1	Router# **configure terminal** or Router# **vlan database**	Enters VLAN configuration mode.
Step 2	Router(config)# **vlan** *vlan_ID*{[-*vlan_ID*]|[,*vlan_ID*]) Router(config-vlan)# or Router(vlan)# **vlan** *vlan_ID*	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).
	Router(config)# **no vlan** *vlan_ID* Router(config-vlan)# or Router(vlan)# **no vlan** *vlan_ID*	Deletes a VLAN.
Step 3	Router(config-vlan)# **end** or Router(vlan)# **exit**	Updates the VLAN database and returns to privileged EXEC mode.
Step 4	Router# **show vlan** [**id** | **name**] *vlan*	Verifies the VLAN configuration.

When you create or modify an Ethernet VLAN, note the following information:

- RPR+ redundancy does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094.
- Layer 3 ports and some software features use extended-range VLANs. If the VLAN you are trying to create or modify is being used by a Layer 3 port or a software feature, the router displays a message and does not modify the VLAN configuration.

When deleting VLANs, note the following information:

- You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.
- When you delete a VLAN, any LAN ports configured as access ports assigned to that VLAN become inactive. The ports remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

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

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active
```

```
VLAN Type  SAID       MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ------ ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500   -      -      -        -    -        0      0

Primary Secondary Type             Interfaces
------- --------- ---------------- ----------------------------------------
```

This example shows how to verify the configuration:

```
Router# show vlan name VLAN0003
VLAN Name                             Status    Ports
---- -------------------------------- --------- --------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
Router#
```

You can also use the **sh vlan free** and **sh vlan free summary** command to To list and view the total number of free vlans and display the vlan usage summary information in the system.

```
Router#show vlan free ?
  Summary  Total number of free vlans in the system
  |        Output modifiers
  <cr>

Router#show vlan free

Free VLANs
----------
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Router#show vlan free ?
  Summary  Total number of free vlans in the system
  |        Output modifiers
Router#show vlan free summ
Router#show vlan free summary ?
  |  Output modifiers

Router#show vlan free summary

======= VLAN free/usage Summary =======

Total number of available vlans = 4094

Total number of free vlans = 4074

Total number of used vlans = 20

Router#
```

Assigning a Layer 2 LAN Interface to a VLAN

A VLAN created in a management domain remains unused until you assign one or more LAN ports to the VLAN.

> **Note**   Make sure you assign LAN ports to a VLAN of the appropriate type. Assign Ethernet ports to Ethernet-type VLANs.

To assign one or more LAN ports to a VLAN, complete the procedures in the "Configuring LAN Interfaces for Layer 2 Switching" section on page 10-6.

Configuring the Internal VLAN Allocation Policy

For more information about VLAN allocation, see the "VLAN Ranges" section on page 14-2.

> **Note**   The internal VLAN allocation policy is applied only following a reload.

To configure the internal VLAN allocation policy, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan internal allocation policy {ascending	descending}`	Configures the internal VLAN allocation policy.
	`Router(config)# no vlan internal allocation policy`	Returns to the default (ascending).
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# reload`	Applies the new internal VLAN allocation policy. ⚠ **Caution** You need not enter the **reload** command immediately. Enter the **reload** command during a planned maintenance window.

When you configure the internal VLAN allocation policy, note the following information:

- Enter the **ascending** keyword to allocate internal VLANs from 1006 and up.
- Enter the **descending** keyword to allocate internal VLAN from 4094 and down.

This example shows how to configure descending as the internal VLAN allocation policy:

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

Configuring VLAN Translation

On trunk ports, you can translate one VLAN number to another VLAN number, which transfers all traffic received in one VLAN to the other VLAN.

These sections describe VLAN translation:

Note   To avoid spanning tree loops, be careful not to misconfigure the VLAN translation feature.

VLAN Translation Guidelines and Restrictions

When translating VLANs, follow these guidelines and restrictions:

- A VLAN translation configuration is inactive if it is applied to ports that are not Layer 2 trunks.

- Do not configure translation of ingress native VLAN traffic on an 802.1Q trunk. Because 802.1Q native VLAN traffic is untagged, it cannot be recognized for translation. You can translate traffic from other VLANs to the native VLAN of an 802.1Q trunk.

- If you enable a vlan translation within an interface, the inteface is reset.

- Do not remove the VLAN to which you are translating from the trunk.

- The VLAN translation configuration applies to all ports in a port group. VLAN translation is disabled by default on all ports in a port group. Enable VLAN translation on ports as needed.

- The following table lists:
  - The modules that support VLAN translation
  - The port groups to which VLAN translation configuration applies
  - The number of VLAN translations supported by the port groups
  - The trunk types supported by the modules

Note   LAN ports on OSMs support VLAN translation. LAN ports on OSMs are in a single port group.

Product Number	Number of Ports	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-SUP720-3BXL WS-SUP720-3B WS-SUP720	2	1	1–2	32	802.1Q
WS-SUP32-10GE	3	2	1, 2–3	16	ISL 802.1Q
WS-SUP32-GE	9	1	1–9	16	ISL 802.1Q
WS-X6704-10GE	4	4	1 port in each group	128	ISL 802.1Q
WS-X6708-10GE	8	8	1 port in each group	16	ISL 802.1Q
WS-X6502-10GE	1	1	1 port in 1 group	32	802.1Q
WS-X6724-SFP	24	2	1–12 13–24	128	ISL 802.1Q
WS-X6816-GBIC	16	2	1–8 9–16	32	802.1Q
WS-X6516A-GBIC	16	2	1–8 9–16	32	802.1Q
WS-X6516-GBIC	16	2	1–8 9–16	32	802.1Q
WS-X6748-GE-TX	48	4	1-23 odd 25-47 odd 2-24 even 26-48 even	128	ISL 802.1Q
WS-X6516-GE-TX	16	2	1–8 9–16	32	802.1Q
WS-X6524-100FX-MM	24	1	1–24	32	ISL 802.1Q
WS-X6548-RJ-45	48	1	1–48	32	ISL 802.1Q
WS-X6548-RJ-21	48	1	1–48	32	ISL 802.1Q

Note For a WS-X6748-GE-TX card, the ports are grouped in an odd and even fashion per ASIC and number of VLAN mappings per port group is 128. Since the VLAN mapping configuration is applicable to all ports in a port group, the total number of VLAN mappings done are 22.

> **Note** To configure a port as a trunk, see the "Configuring a Layer 2 Switching Port as a Trunk" section on page 10-7.

Configuring VLAN Translation on a Trunk Port

To translate VLANs on a trunk port, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the Layer 2 trunk port to configure.
Step 2	Router(config-if)# **switchport vlan mapping enable**	Enables VLAN translation.
Step 3	Router(config-if)# **switchport vlan mapping** *original_vlan_ID translated_vlan_ID*	Translates a VLAN to another VLAN. The valid range is 1 to 4094.
	Router(config-if)# **no switchport vlan mapping** {**all** | *original_vlan_ID translated_vlan_ID*}	Deletes the mapping.
Step 4	Router(config-if)# **end**	Exits configuration mode.
Step 5	Router# **show interface** *type*[1] *slot/port* **vlan mapping**	Verifies the VLAN mapping. **Note** The vlan option is available although it may not be displayed in the listed options for the **show interface** command.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to map VLAN 1649 to VLAN 755 Gigabit Ethernet port 5/2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping 1649 755
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show interface gigabitethernet 5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
------------- ---------------
   1649          755
```

Enabling VLAN Translation on Other Ports in a Port Group

To enable VLAN translation on other ports in a port group, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	Router(config-if)# **switchport vlan mapping enable**	Enables VLAN translation.
	Router(config-if)# **no switchport vlan mapping enable**	Disables VLAN translation.

	Command	Purpose
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show interface type`[1] `slot/port vlan mapping`	Verifies the VLAN mapping.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable VLAN translation on a port:

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/2
Router(config-if)# switchport vlan mapping enable
Router(config-if)# end
Router#
```

Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1 through 1001 and 1006 through 4094. The valid range of VLANs specified in the IEEE 802.1Q standard is 1 to 4094. You can map 802.1Q VLAN numbers to ISL VLAN numbers.

802.1Q VLANs in the range 1 through 1001 and 1006 through 4094 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers corresponding to reserved VLAN numbers must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco network devices.

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

- You can configure up to eight 802.1Q-to-ISL VLAN mappings on the Cisco 7600 series router.
- 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 1007 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each Cisco 7600 series router. Make sure you configure the same VLAN mappings on all appropriate network devices.

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

	Command	Purpose
Step 1	`Router(config)# vlan mapping dot1q dot1q_vlan_ID isl isl_vlan_ID`	Maps an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for *dot1q_vlan_ID* is 1001 to 4094. The valid range for *isl_vlan_ID* is the same.
	`Router(config)# no vlan mapping dot1q {all | dot1q_vlan_ID}`	Deletes the mapping.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show vlan`	Verifies the VLAN mapping.

This example shows how to map 802.1Q VLAN 1003 to ISL VLAN 200:

```
Router# configure terminal
Router(config)# vlan mapping dot1q 1003 isl 200
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show vlan
<...output truncated...>
802.1Q Trunk Remapped VLANs:
802.1Q VLAN    ISL VLAN
-----------   -----------
   1003         200
```