

Configuring VLANs, VTP, and VMPS

This chapter describes VLANs on Catalyst 4500 series switches. It also describes how to enable the VLAN Trunking Protocol (VTP) and to configure the Catalyst 4500 series switch as a VMPS client.

This chapter includes the following major sections:

- [VLANs, page 13-1](#)
 - [VLAN Trunking Protocol, page 13-7](#)
 - [VLAN Membership Policy Server, page 13-16](#)

VLANs

- [Overview of VLANs, page 13-1](#)
- [VLAN Configuration Guidelines and Restrictions, page 13-3](#)
 - [VLAN Default Configuration, page 13-4](#)
 - [Configuring VLANs, page 13-4](#)

**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference*

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/index.htm>.

Overview of VLANs

attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.

You can define one or many virtual bridges within a switch. Each virtual bridge you create in the switch defines a new broadcast domain (VLAN). Traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. To interconnect two different VLANs, you must use routers or Layer 3 switches. See the [“Overview of Layer 3 Interfaces” section on page 25-1](#) for information on inter-VLAN routing on Catalyst 4500 series switches.

[Figure 13-1](#) shows an example of three VLANs that create logically defined networks.

Figure 13-1 Sample VLANs



VLANs are often associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. You must assign LAN interface VLAN membership on an interface-by-interface basis (this is known as interface-based or static VLAN membership).

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

- VLAN number
- VLAN name
- VLAN type
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- VLAN number to use when translating from one VLAN type to another



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

VLAN Configuration Guidelines and Restrictions

-
- **end**
Ctrl-Z

VLAN Ranges


Note

You must enable the extended system ID to use 4094 VLANs. See the [“Understanding the Bridge ID” section on page 17-2](#).

With Cisco IOS Release 12.2(25)EWA and later, Catalyst 4500 series switches support 4096 VLANs in compliance with the IEEE 802.1Q standard. These VLANs are organized into three ranges: reserved, normal, and extended.

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 13-1](#) describes the uses for VLAN ranges.

Table 13-1 VLAN Ranges

VLANs	Range	Usage	Propagated by VTP
			—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1001	Normal	Used 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. When configuring extended-range VLANs, note the following: Layer 3 ports and some software features require internal VLANs. Internal VLANs are allocated from 1006 and up. You cannot use a VLAN that has been allocated for such use. To display the VLANs used internally, enter the show vlan internal usage	

Configurable Normal-Range VLAN Parameters


Note

-
-
-
-
-

VLAN Default Configuration

Table 13-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Valid Values
	x x	


Note

Configuring VLANs


Note



vlan.dat

vlan.dat

Configuring VLANs in Global Configuration Mode

running-config startup-config

show vlan

copy running-config startup-config

startup-config
show running-config

show startup-config



vlan.dat

startup-config

vlan.dat

running-config
show running-config

vlan
show vlan id *ID*

media

	Command	Purpose
Step 1		
Step 2	<code>vlan_ID</code>	Switch(config-vlan)#,
Step 3		
Step 4	<code>show vlan [id name] vlan_name</code>	

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# end
Switch# 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
-----
Switch#
```

Assigning a Layer 2 LAN Interface to a VLAN



Note

VLAN Trunking Protocol

-
-
-
-

Overview of VTP

-
-
-
-
-

Understanding the VTP Domain

Understanding VTP Modes

-

-

configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive on their trunking LAN interfaces. VTP transparent is the default mode.



Catalyst 4500 series switches automatically change from VTP server mode to VTP client mode if the switch detects a failure while writing configuration to NVRAM. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.

Understanding VTP Advertisements



FDDI, FDDI-Net, Token Ring Concentrator Relay Function [TrCRF], or Token Ring Bridge Relay Function [TrBRF] traffic, but it does propagate the VLAN configuration via VTP.

VTP version 2 supports the following features, which are not supported in version 1:

Token Ring support—VTP version 2 supports Token Ring LAN switching and VLANs (TrBRF and TrCRF).

Unrecognized Type-Length-Value (TLV) Support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM.

Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent network device inspects VTP messages for the domain name and version, and forwards a message only if the version and domain name match. Because only one domain is supported in the supervisor engine software, VTP version 2 forwards VTP messages in transparent mode, without checking the version.

Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, and unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled.

For VTP pruning to be effective, all devices in the management domain must either support VTP pruning or, on devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.

Figure 13-2 shows a switched network without VTP pruning enabled. Interface 1 on Switch 1 and Interface 2 on Switch 4 are assigned to the Red VLAN. A broadcast is sent from the host connected to Switch 1. Switch 1 floods the broadcast and every network device in the network receives it, even though Switches 3, 5, and 6 have no interfaces in the Red VLAN.

You can enable pruning globally on the Catalyst 4500 series switch (see the [“Enabling VTP Pruning”](#) section on page 13-12).

Flooding Traffic without VTP Pruning



Figure 13-3 Flooding Traffic with VTP Pruning



switchport trunk pruning vlan


Caution

-
-
-
-

VTP Default Configuration

VTP Default Configuration

Feature	Default Value

Configuring VTP

-
-
-
-
-

Configuring VTP Global Parameters

-
-
-

Configuring a VTP Password

Command	Purpose
<i>password_string</i>	

```
Switch# vtp password WATER
Setting device VLAN database password to WATER.
Switch# show vtp password
VTP Password:WATER
Switch#
```

Enabling VTP Pruning

Pruning switched ON

Switch# `show vtp status | include Pruning`

Enabling VTP Version 2



Step 1

Command	Purpose
<code>{1 }</code>	
Switch#	

`vtp version 2`

`show vtp status | include V2`

Configuring the Switch as a VTP Server

Step 5

Switch#	
Switch(config)#	
Switch(config)# <i>domain_name</i>	
Switch(config)#	

```
Switch# vtp domain Lab_Network
```

```
Setting VTP domain name to Lab_Network
```

```
Switch(config)#
```

```
Switch#
```

```
Switch#
```

```
VTP Version : running VTP1 (VTP2 capable)
```

```
Configuration Revision : 247
```

```
Maximum VLANs supported locally : 1005
```

```
Number of existing VLANs : 33
```

```
VTP Operating Mode : Server
```

```
VTP Domain Name : Lab_Network
```

```
VTP Pruning Mode : Enabled
```

```
VTP V2 Mode : Disabled
```

```
VTP Traps Generation : Disabled
```

```
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
```

```
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
```

```
Local updater ID is 172.20.52.34 on interface Gi1/1 (first interface found)
```

```
Switch#
```

Switch# configuration terminal	
Switch(config)# [no] vtp mode client	
Switch(config)# end	
Switch# show vtp status	

```
Switch#
```

```
Switch(config)#
```

```
Setting device to VTP CLIENT mode.
```

```
Switch(config)# exit
```

```
Switch#
```

```
Switch# show vtp status
```

```
VTP Version : running VTP1 (VTP2 capable)
```

```
Configuration Revision : 247
```

```
Maximum VLANs supported locally : 1005
```

```
Number of existing VLANs : 33
```

```
VTP Operating Mode : Client
```

```
VTP Domain Name : Lab_Network
```

```
VTP Pruning Mode : Enabled
```

```
VTP V2 Mode : Disabled
```

```
VTP Traps Generation : Disabled
```

MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49

Switch#

Disabling VTP (VTP Transparent Mode)

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		

Displaying VTP Statistics

Command	Purpose

```
Request advertisements received      : 0
Summary advertisements transmitted  : 997
Subset advertisements transmitted   : 13
Request advertisements transmitted  : 3
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk      Join Transmitted Join Received  Summary advts received from
-----
Fa5/8      43071             42766      5
non-pruning-capable device
```

VLAN Membership Policy Server

-
-
-
-

Overview of VMPS

-
-
-
-

Understanding the VMPS Server

-

—

—

—

, “

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/config_gd/vmps.htm

VMPS operates in three different modes. The way a VMPS server responds to illegal requests depends on the mode in which the VMPS is configured:

[Open Mode, page 13-17](#)

[Secure Mode, page 13-18](#)

[Multiple Mode, page 13-18](#)

Open Mode

-

-

-

-

Secure Mode

-

-

-

Multiple Mode



Note

Fallback VLAN

-

-

-

Illegal VMPS Client Requests

-
-

Overview of VMPS Clients

-
-
-
-
-

Understanding Dynamic VLAN Membership



Note

Default VMPS Client Configuration

Table 13-4 Default VMPS Client and Dynamic Port Configuration

Configuring a Switch as a VMPS Client

-
-
-
-
-

Configuring the IP Address of the VMPS Server

<i>ipaddress</i> <i>hostname</i>	
<i>ipaddress</i> <i>hostname</i>	
	Returns to privileged EXEC mode.
	Verifies the VMPS server entry.

```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmps server 172.20.128.179 primary
                  vmps server 172.20.128.178
                  end
    
```



Configuring Dynamic Access Ports on a VMPS Client

	Command	Purpose
Step 1	<code>configure terminal</code>	
Step 2	<code>interface <i>interface</i></code>	
Step 6	<code><i>interface</i></code>	

```

interface fa1/1
    switchport mode access
    switchport access vlan dynamic
end

show interface fa1/1 switchport

```

Voice Ports

-
-

Reconfirming VLAN Memberships

Switch#	
Switch#	

Configuring Reconfirmation Interval

Switch#	
Switch(config)#	<i>minutes</i>

```
vmmps reconfirm 60
end
show vmmps
```

VMPS Action: No Host

configure terminal	
vmps retry	
end	
show vmps	

```
vmps retry 5
end

show vmps
```

vmps reconfirm

show vmps

show vmps statistics



errdisable recovery cause vmps

Dynamic Port VLAN Membership Configuration Example

-
-
-
-
-



Figure 13-5 Dynamic Port VLAN Membership Configuration



Figure 13-6 Dynamic Port VLAN Membership Configuration



a.

b.

c.

d.

e.

Step 2

- a.
- b.
- c.
- d.
- e.

Step 3

Step 4

Step 5

Step 6

VMPS Database Configuration File Example

```

!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
  device 198.92.30.32 port Fa1/3
  device 172.20.26.141 port Fa1/4
vmps-port-group "Executive Row"
  device 198.4.254.222 port es5%Fa0/1
  device 198.4.254.222 port es5%Fa0/2
  device 198.4.254.223 all-ports
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
  vlan-name hardware
  vlan-name software
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
  port-group WiringCloset1

```

```
vmports-port-policies vlan-name Green
  device 198.92.30.32 port Fa0/9
vmports-port-policies vlan-name Purple
  device 198.4.254.22 port Fa0/10
  port-group "Executive Row"
```

