Cisco LAN Switching Configuration Handbook

Second Edition

A complete, concise reference for implementing the most important features of the Cisco Catalyst family of switches

Stephen McQuerry, CCIE® No. 6108
David Jansen
David Hucaby, CCIE No. 4594

ciscopress.com

Cisco LAN Switching Configuration Handbook

Steve McQuerry, CCIE No. 6108
David Jansen, CCIE No. 5952
Dave Hucaby, CCIE No. 4594

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Chapter 6

VLANs and Trunking

See the following sections for configuration information about these topics:

- **6-1: VLAN Configuration:** Describes the method for configuring, creating, and configuring VLANs on a switch
- **6-2: VLAN Port Assignments:** Explains how to assign a port to a VLAN using static or dynamic methods
- **6-3: Trunking:** Covers the method for extending a VLAN beyond the boundaries of a single switch through tagging mechanisms
- **6-4: VLAN Trunking Protocol:** Describes the Cisco proprietary protocol for maintaining a forwarding path between switches that are trunking and how to prune for unused VLANs
- **6-5: Private VLANs:** Explains the feature that allows for more granular traffic control within the VLAN using the private VLAN structure

6-1: VLAN Configuration

- *VLANs* are broadcast domains defined within switches to enable control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.
- VLANs are defined on a switch in an internal database known as the *VLAN Trunking Protocol (VTP) database*. After a VLAN has been created, ports are assigned to the VLAN.
- VLANs are assigned numbers for identification within and between switches. Cisco switches have two ranges of VLANs, the *normal range* and *extended range*.
- VLANs have a variety of configurable parameters, including name, type, and state.
- Several VLANs are reserved, and some can be used for internal purposes within the switch.

Creation of an Ethernet VLAN

VLANs are created on Layer 2 switches to control broadcasts and enforce the use of a Layer 3 device for communications. Each VLAN is created in the local switch's database for use. If a VLAN is not known to a switch, that switch cannot transfer traffic across any of its ports for that VLAN. VLANs are created by number, and there are two ranges of usable VLAN numbers (normal range 1 to 1000 and extended range 1025 to 4096). When a VLAN is created, you can also give it certain attributes such as a VLAN name, VLAN type, and its operational state. To create a VLAN, use the following steps.

1. Configure VTP.

VTP is a protocol used by Cisco switches to maintain a consistent database between switches for trunking purposes. VTP is not required to create VLANs; however, Cisco has set it up to act as a conduit for VLAN configuration between switches as a default to make administration of VLANs easier. Because of this, you must first either configure a VTP with a domain name or disable VTP on the switch. VTP is explained in detail in section "6-4: VLAN Trunking Protocol."

- Specify a VTP name:

```
(global) vtp domain domain-name
```

By default, the VTP is in server mode and must be configured with a domain name before any VLANs can be created. These commands specify the VTP domain name.

OR

- Disable VTP synchronization:

```
(global) vtp mode transparent
```

Another option is to disable VTP synchronization of the databases. Disabling it enables you to manage your local VTP database without configuring and relying on VTP. You can configure the VTP parameters in global configuration mode as well.

2. Create the VLAN.

VLANs are created by number. The two ranges of VLANs are as follows:

- The standard range consists of VLANs 1 to 1000.
- The extended range consists of VLANs 1025 to 4096.

Extended VLANs are supported in switches running IOS software. When you create a VLAN, you have many options to consider, several of which are valid only for FDDI and Token Ring VLANs. Some of the items configured deal with options, such as private VLANs, which are discussed in other sections in this book. VLANs are created using the **vlan** command in global mode. For Ethernet VLANs, you can also configure the standard parameters, as shown in Table 6-1.

Table 6-1 *Configurable VLAN Parameters*

Parameter	Description
`name`	A description of the VLAN up to 32 characters. If none is given, it defaults to VLAN00XXX, where XXX is the VLAN number.
`mtu`	The maximum transmission unit (packet size in bytes) that the VLAN can use; valid values are from **576** to **18190**. The MTU can extend up to 1500 for Ethernet, but beyond for Token Ring or FDDI. The default is **1500**.
`state`	Used to specify whether the state of the VLAN is active or suspended. All ports in a suspended VLAN will be suspended and not allowed to forward traffic. The default state is **active**.

a. Create a VLAN in the standard range:

```
(global) vlan vlan-id [name vlan-name] [state {suspend | active}] [mtu
  mtu-size]
```

The **vlan-id** specifies the VLAN by number. You can create VLANs in global configuration mode if the switch is in VTP transparent mode. To do this, enter the **vlan** *vlan-id* command to move to vlan-config mode. From vlan-config mode, you can manage the parameters of the VLANs.

Note You cannot modify any of the parameters for VLAN 1.

b. Create a VLAN in the extended range.

Extended VLANs support VLANs up to 4096 in accordance with the 802.1Q standard.

3. Enable spanning-tree MAC reduction:

```
(global) vlan internal allocation policy descending
```

You can instruct the Catalyst 6500 series switch to start to borrow VLANs from the top, and descend from 4096, or from bottom, and ascend from 1006, with the use the global config mode **vlan allocation policy** command.

Note After you create a VLAN in the extended range, you cannot disable this feature unless you first delete the VLAN.

4. Create a VLAN in the extended range:

```
(global) vlan vlan-id [name vlan-name] [state {suspend | active}] [mtu
  mtu-size]
```

Here the *vlan-id* would be a number from 1025 to 4096. Numbers 1001 to 1024 are reserved by Cisco and cannot be configured.

Caution For Catalyst 6000 series switches with FlexWAN cards, the system identifies these ports internally with VLAN numbers starting with 1025. If you have any FlexWAN modules, be sure to reserve enough VLAN numbers (starting with VLAN 1025) for all the FlexWAN ports you want to install. You cannot use these extended VLANs if you install FlexWAN ports.

Feature Example

In this example, the switches Access_1 and Distribution_1 are going to be configured with VLANs 5, 8, and 10 with the names Cameron, Logan, and Katie, respectively. Also the distribution switch will be configured with VLAN 2112 with the name Rush.

An example of the configuration for Distribution 1 follows:

```
Distribution_1# conf t
Distribution_1 (config)# vtp mode transparent
Distribution_1 (config)# vlan 5
Distribution_1 ((config-vlan)# name Cameron
Distribution_1 ((config-vlan)# vlan 8
Distribution_1 ((config-vlan)# name Logan
Distribution_1 ((config-vlan)# vlan 10
Distribution_1 ((config-vlan)# name Katie
Distribution_1 ((config-vlan)# vlan 2112
Distribution_1 ((config-vlan)# name Rush
Distribution_1 ((config-vlan)# end
Distribution_1 # copy running-config startup-config
```

An example of the Layer 2 configuration for Access 1 follows:

```
Access_1(config)# vlan 5
Access_1(config-vlan)# name Cameron
Access_1(config-vlan)# vlan 8
Access_1(config-vlan)# name Logan
Access_1(config-vlan)# vlan 10
Access_1(config-vlan)# name Katie
```

```
Access_1(config-vlan)# end
Access_1 #copy running-config startup-config
```

6-2: VLAN Port Assignments

- VLANs are assigned to individual switch ports.
- Ports can be statically assigned to a single VLAN or dynamically assigned to a single VLAN.
- All ports are assigned to VLAN 1 by default.
- Ports are active only if they are assigned to VLANs that exist on the switch.
- Static port assignments are performed by the administrator and do not change unless modified by the administrator, whether the VLAN exists on the switch.
- Dynamic VLANs are assigned to a port based on the MAC address of the device plugged into a port.
- Dynamic VLAN configuration requires a *VLAN Membership Policy Server* (VMPS) client, server, and database to operate properly.

Configuring Static VLANs

On a Cisco switch, ports are assigned to a single VLAN. These ports are referred to as *access ports* and provide a connection for end users or node devices, such as a router or server. By default all devices are assigned to VLAN 1, known as the *default VLAN*. After creating a VLAN, you can manually assign a port to that VLAN, and it can communicate only with or through other devices in the VLAN. Configure the switch port for membership in a given VLAN as follows:

1. Statically assign a VLAN:

```
(global) interface type mod/port
(interface) switchport access vlan number
```

For the device, you must first select the port or port range and then use the **switchport access vlan** command followed by the VLAN *number*.

Caution If the VLAN that the port is assigned to does not exist in the database, the port is disabled until the VLAN is created.

Configuring Dynamic VLANs

Although static VLANs are the most common form of port VLAN assignments, it is possible to have the switch dynamically allocate a VLAN based on the authentication. The IEEE 802.1X standard defines a client and server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN. Until the client is authenticated, 802.1X access control enables only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port. Use the following steps to configure dynamic VLANs using 802.1x with VLAN assignment:

1. Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server.

   ```
   (global) RADIUS configuration

   (global) radius-server host ip_address

   (global) radius-server key key

   (global) aaa new-model

   (global) aaa authentication dot1x default group radius

   (global) aaa authorization default group radius

   (global) aaa authorization config-commands
   ```

2. Enable 802.1x authentication:

   ```
   (global) dot1x system-auth-control

   (global) dot1x max-req

   (global) dot1x timeout quiet-period

   (global) dot1x timeout tx-period

   (global) dot1x timeout re-authperiod

   (global) dot1x re-authentication
   ```

Note The VLAN assignment feature is automatically enabled when you configure 802.1X authentication on an access port.

3. Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch: [64] Tunnel-Type = VLAN [65] Tunnel-Medium-Type = 802 [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID.

Note The dynamic VLAN mechanism:

- RADIUS AV-Pairs used to send back VLAN configuration information to authenticator.