



Configuring VLANs

To configure VLANs on your Catalyst 6000 family switch, perform these steps:

-
- Step 1** Configure VLAN Trunk Protocol—Create a VLAN Trunk Protocol (VTP) domain and set the VTP mode on the switch.
 - Step 2** Configure VLANs—Create VLANs in the VTP domain and place the switch ports in those VLANs.
 - Step 3** Configure VLAN Trunks—Configure trunk ports between switches to transport traffic from multiple VLANs.
-

Configure VLAN Trunk Protocol

VTP propagates information about the VLAN configuration throughout the switched network. A Catalyst 6000 family switch can operate in any one of these three VTP modes:

- **Server**—VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.

- Client—VTP clients are similar to VTP servers, except that you cannot create, change, or delete VLANs on a VTP client.
- Transparent—VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements.

**Note**

Before you configure VLANs on the switch, you should decide whether to use VTP. If you choose to use VTP, decide if the switch should function as a VTP client or a VTP server. If you are connecting the switch to an existing network, make sure your VTP configuration is compatible with the rest of the network.

Configure the Switch as a VTP Server

When you configure a switch as a VTP server, you must define a VTP domain before you can create VLANs.

To configure a switch as a VTP server, perform these steps in privileged mode:

	Task	Command
Step 1	Assign a name to the VTP management domain.	set vtp domain <i>name</i>
Step 2	Set the VTP mode.	set vtp mode server
Step 3	Verify the VTP configuration.	show vtp domain

This example shows how to configure a switch as a VTP server:

```

Console> (enable) set vtp domain BigCorp
VTP domain BigCorp modified
Console> (enable) set vtp mode server
VTP domain BigCorp modified
Console> (enable) show vtp domain
-----
Domain Name                               Domain Index VTP Version Local Mode Password
-----
BigCorp                                   1             2             server      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
9           1023             0             enabled

Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
172.20.52.40 disabled disabled 2-1000
Console> (enable)

```

Configure the Switch as a VTP Client

When you configure a switch as a VTP client, you cannot configure VLANs on the switch; instead, you configure VLANs on a VTP server in the same VTP domain as the client. The VTP client synchronizes its VLAN configuration to the configuration of the server.

To configure a switch as a VTP client, perform these steps in privileged mode:

	Task	Command
Step 1	Assign a name to the VTP management domain.	set vtp domain <i>name</i>
Step 2	Set the VTP mode.	set vtp mode client
Step 3	Verify the VTP configuration. (It might take a few minutes before a VTP client learns the VTP and VLAN configuration information from neighboring switches.)	show vtp domain

Configure VLAN Trunk Protocol

This example shows how to configure a switch as a VTP client:

```

Console> (enable) set vtp domain BigCorp
VTP domain BigCorp modified
Console> (enable) set vtp mode client
VTP domain BigCorp modified
Console> (enable) show vtp domain
-----
Domain Name                Domain Index VTP Version Local Mode Password
-----
BigCorp                    1            2            client      -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
9           1023             0            enabled

Last Updater    V2 Mode Pruning PruneEligible on Vlans
-----
172.20.52.40   disabled disabled 2-1000
Console> (enable)

```

Configure the Switch as VTP Transparent

When you configure a switch as VTP transparent, you must configure VLAN information manually on the switch. A VTP-transparent switch does not advertise VLAN information to other switches and will ignore VTP updates from VTP clients and servers.

To configure a switch for VTP transparent mode, perform these steps in privileged mode:

	Task	Command
Step 1	Set the VTP mode.	set vtp mode transparent
Step 2	Verify the VTP configuration.	show vtp domain

This example shows how to configure a switch as VTP transparent:

```

Console> (enable) set vtp mode transparent
VTP domain modified
Console> (enable) show vtp domain
Domain Name                               Domain Index VTP Version Local Mode Password
-----
                                           1             2             Transparent -

Vlan-count Max-vlan-storage Config Revision Notifications
-----
9           1023             0             enabled

Last Updater   V2 Mode Pruning PruneEligible on Vlans
-----
172.20.52.40   disabled disabled 2-1000
Console> (enable)

```

Configure VLANs

When you properly configure a switch for VTP, you can create, modify, and delete VLANs on the switch (unless you configured the switch as a VTP client). When you configure a VLAN on a VTP server, the configuration information is distributed to switches throughout the VTP domain.

VTP clients and servers in the same domain update their VLAN configuration based on the advertised configuration. VTP transparent switches do not act on VTP updates; you must make changes to the VLAN configuration locally on such switches.

Typically, in an IP network, each VLAN is associated with a single IP subnetwork. That is, all of the hosts in a given VLAN belong to a single subnet, use the same subnet mask, and use one or more default gateways connected to that subnetwork. Stations in different VLANs cannot communicate with one another without either a router configured to route between the different VLANs or manually configured (static) routes configured on the switches.

The Catalyst 6000 family software supports many VLAN types, including Ethernet, FDDI, ATM, and Token Ring.



Note Two Token Ring VLAN types are supported on switches running VTP version 2: Token Ring TrBRF VLANs and Token Ring TrCRF VLANs. Catalyst 6000 family switches do not support ISL-encapsulated Token Ring frames.

This section describes how to configure Ethernet VLANs only. For information about configuring other types of VLANs, refer to the *Catalyst 6000 Family Software Configuration Guide*.

Create VLANs

To configure an Ethernet VLAN in a VTP domain, perform these steps in privileged mode:

	Task	Command
Step 1	Create a VLAN by assigning it a VLAN number and, if desired, a VLAN name.	set vlan <i>vlan_num</i> [name <i>name</i>]
Step 2	Verify the VLAN configuration.	show vlan <i>vlan_num</i>

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

```

Console> (enable) set vlan 100 name Pubs
Vlan 100 configuration successful
Console> (enable) show vlan 100
VLAN Name                Status      Mod/Ports, Vlans
-----
100  Pubs                    active

VLAN Type  SAID      MTU   Parent RingNo BrdgNo  Stp   BrdgMode Trans1  Trans2
-----
100  enet    100100   1500  -     -     -     -     -     0     0

VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

Assign Switch Ports to VLANs

After you create a VLAN, you can assign one or more switch ports to the VLAN. Devices connected to those ports will belong to that VLAN. Make sure the connected device is properly configured with an IP address, subnet mask, and default gateway in the subnet used for the VLAN.

To add a switch port to a VLAN, perform these steps in privileged mode:

	Task	Command
Step 1	Add one or more switch ports to a VLAN.	set vlan <i>vlan_num</i> <i>mod_num/port_num</i>
Step 2	Verify that the ports are properly assigned to the VLAN.	show vlan <i>vlan_num</i>
Step 3	Check to which VLAN a particular port belongs.	show port [<i>mod_num/port_num</i>]

Configure VLAN Trunks

This example shows how to assign ports to a VLAN and how to verify to which VLAN the ports belong:

```
Console> (enable) set vlan 100 2/1-4
```

```
VLAN 100 modified.
```

```
VLAN 1 modified.
```

```
VLAN Mod/Ports
```

```
-----
100 2/1-4
```

```
Console> (enable) show vlan 100
```

```
VLAN Name                               Status    Mod/Ports, Vlans
```

```
-----
100 Pubs                                 active    2/1-4
```

```
VLAN Type SAID      MTU    Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
100 enet  100100   1500  -      -      -    -      -      0      0
```

```
VLAN AREHops STEHops Backup CRF
```

```
Console> (enable) show port 2
```

```
Port Name                               Status    Vlan    Level Duplex Speed Type
```

```
-----
2/1                                     notconnect 100     normal half 100 100BaseTX
2/2                                     notconnect 100     normal half 100 100BaseTX
2/3                                     notconnect 100     normal half 100 100BaseTX
2/4                                     notconnect 100     normal half 100 100BaseTX
2/5                                     notconnect 1       normal half 100 100BaseTX
```

```
<... output truncated ...>
```

```
Console> (enable)
```

Configure VLAN Trunks

VLAN trunks are point-to-point links that carry the traffic of multiple VLANs. Trunk ports are useful in the network backbone, where traffic from many VLANs is handled.

All Ethernet ports can use Inter-Switch Link (ISL) or IEEE 802.1Q encapsulation for trunking.

By default, all Ethernet ports are set to **negotiate** and attempt to use ISL encapsulation.

If the port on the other end of the link is set to **desirable** or **on**, a port set to **auto** automatically becomes a trunk port. (For complete information on the various trunk modes and encapsulation types, refer to the *Catalyst 6000 Family Software Configuration Guide*.)

To configure an Ethernet port as a trunk, perform these steps in privileged mode:

	Task	Command
Step 1	Configure a port as a trunk. A message appears on the console indicating that the port has become a trunk.	set trunk <i>mod_num/port_num</i> { on desirable auto } { isl dot1q negotiate }
Step 2	Verify that the trunk configuration is correct.	show trunk

This example shows how to configure a port to become a trunk and how to verify the trunk configuration (this example assumes that the port on the other end of the link is set to **auto**):

```

Console> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
Console> (enable) 07/22/1998,10:16:58:DTP-5:Port 1/2 has become isl trunk
07/22/1998,10:16:58:PAGP-5:Port 1/2 left bridge port 1/2.
07/22/1998,10:17:09:PAGP-5:Port 1/2 joined bridge port 1/2.
Console> (enable) show trunk 1/2
Port      Mode           Encapsulation  Status      Native vlan
-----
1/2      desirable     isl            trunking    523
Port      Vlans allowed on trunk
-----
1/2      1-1005
Port      Vlans allowed and active in management domain
-----
1/2      1,10,105,152,521-524
Port      Vlans in spanning tree forwarding state and not pruned
-----
1/2      1,10,105,152,521-524
Console> (enable)

```

