



Understanding and Configuring VLANs

This chapter describes how to configure virtual LANs (VLANs) on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter contains these major sections:

- [Understanding How VLANs Work, page 10-1](#)
- [VLAN Default Configuration, page 10-4](#)
- [VLAN Configuration Guidelines, page 10-4](#)
- [Configuring VLANs, page 10-5](#)
- [Configuring Private VLANs, page 10-12](#)

Understanding How VLANs Work

A VLAN is a group of end stations with a common set of requirements, independent of physical location. A VLANs 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 other ports belonging to that VLAN.

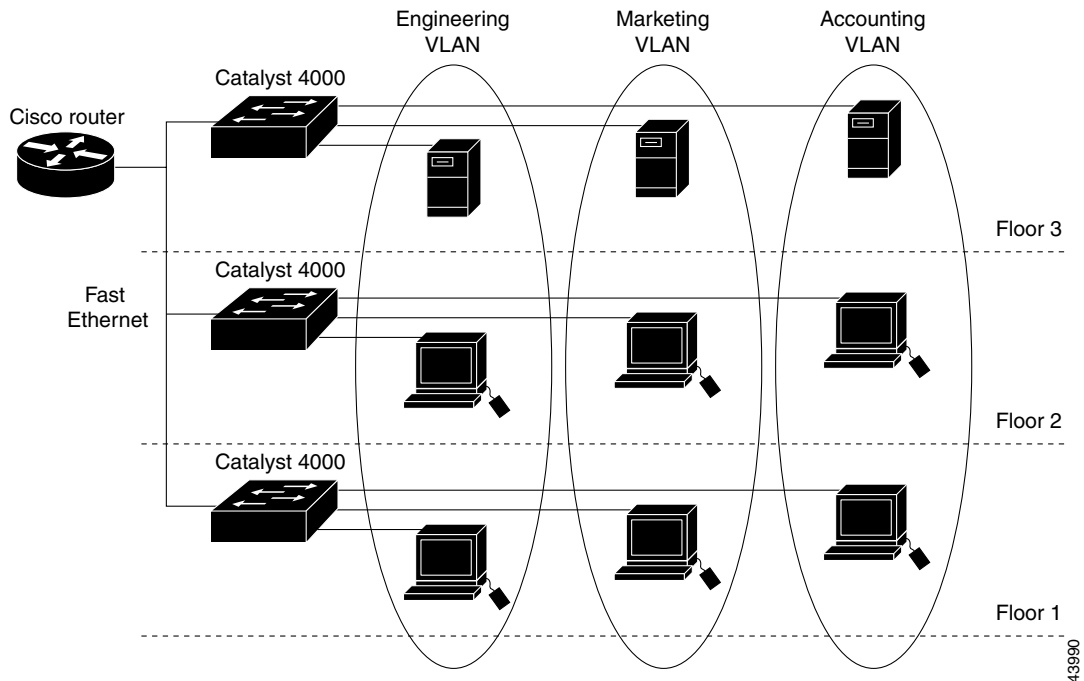


Note

Before you create VLANs, you must decide whether to use VTP or VMPS to maintain global VLAN configuration information for your network. For complete information on VTP, see [Chapter 9, “Configuring VTP.”](#) For complete information on VMPS, see [Chapter 12, “Configuring Dynamic VLAN Membership with VMPS.”](#)

[Figure 10-1](#) shows an example of VLANs segmented into logically defined networks.

Figure 10-1 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.

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

- VLAN number
- VLAN name
- VLAN type (Ethernet)
- 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

**Note**

When translating from one VLAN type to another, you must create a different VLAN number for each media type.

VLAN Ranges

Catalyst 4000 family 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 10-1 describes the VLAN ranges.

Table 10-1 VLAN Ranges

| VLAN Number | Range | Usage | Propagated by VTP ? |
|-------------|----------|--|---------------------|
| 0, 4095 | Reserved | For system use only. You cannot see or use these VLANs. | N/A |
| 1 | Normal | Cisco default. You can use this VLAN, but you cannot delete it. | Yes |
| 2–1000 | Normal | Used for Ethernet VLANs; you can create, use, and delete these VLANs. | Yes |
| 1001 | Normal | You cannot create or use this VLAN. | Yes |
| 1002–1005 | Reserved | Cisco defaults for FDDI and Token Ring. Not supported on Catalyst 4000 family switches. You cannot delete these VLANs. | N/A |
| 1006–1009 | Reserved | Cisco defaults. Not currently used. You can map nonreserved VLANs to these reserved VLANs when necessary. | N/A |
| 1010–1024 | Reserved | You cannot see or use these VLANs, but you can map nonreserved VLANs to these reserved VLANs when necessary. | N/A |
| 1025–4094 | Extended | For Ethernet VLANs only. You can create, use, and delete these VLANs. | No |

Configurable VLAN Parameters

When you create VLANs 2–1000 or modify VLANs 2–1005, you can set the parameters as follows:

- VLAN number
- VLAN name
- VLAN type: Ethernet, FDDI, and FDDINET
- VLAN state: active or suspended
- Multi-Instance Spanning Tree Protocol (MISTP) instance
- Private VLAN type: primary, isolated, community, two-way community, or none

- SAID
- MTU for the VLAN
- 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
- Remote Switched Port Analyzer (RSPAN)

**Note**

Ethernet VLANs 1 and 1025–4094 can use the defaults only.

VLAN Default Configuration

Table 10-2 shows the default VLAN configuration.

Table 10-2 VLAN Default Configuration

| Feature | Default Value |
|-----------------------|--|
| Native (default) VLAN | VLAN 1 |
| Port VLAN assignments | All ports assigned to VLAN 1 |
| VLAN state | Enabled |
| MTU size | 1500 bytes |
| SAID value | 100,000 plus the VLAN number (for example, the SAID for VLAN 3 is 100,003) |
| Pruning eligibility | VLANs 2–1000 are eligible for pruning |

VLAN Configuration Guidelines

Keep the following in mind when creating and modifying VLANs in your network:

- Before you can create a normal-range VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain. For information on configuring VTP, see [Chapter 9, “Configuring VTP.”](#)
- Since VTP does not work on extended-range VLANs, you can create extended-range VLANs (1025-4094) even when the VTP mode is set to client.
- You can create normal-range VLANs one at a time or you can create a range of VLANs.
- You cannot specify a VLAN name when you create a VLAN range, because VLAN names must be unique.
- VLAN numbers are always ISL VLAN identifiers, not 802.1Q VLAN identifiers.
- Always specify a VLAN type when configuring the VLAN or, by default, the VLAN will be an Ethernet VLAN.

Follow these additional guidelines when creating or modifying extended-range VLANs:

- You can create only extended-range Ethernet VLANs.
- You can create and delete only 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.

**Note**

The Catalyst 4000 family switch 10/100 Ethernet switching modules support auxiliary VLANs in software release 5.5(1) and later. You can plug an externally powered IP phone into a 10/100 port and then add that port to an auxiliary VLAN using the **set port auxiliaryvlan** command. For complete details on configuring auxiliary VLANs, refer to the “Configuring a Voice-over-IP Network” chapter in the *Catalyst 6000 Family Software Configuration Guide*.

Configuring VLANs

VLANs are either normal range or extended range. VLANs in the normal range are VLANs 2–1000. VLANs in the extended range are VLANs 1025–4094.

When you configure normal-range VLANs, VLANs 2–1000, you can configure one VLAN at a time or a range of VLANs, all with a single command. If you configure a range of VLANs, you cannot specify a name, because VLAN names must be unique.

**Note**

You cannot configure or modify normal-range VLAN 1.

You can use VTP to manage global normal-range VLAN configuration information on your network; but not extended-range VLAN configuration information. In order to use VTP, you must configure it before you create any normal-range VLANs. For more information about configuring VTP, see [Chapter 9, “Configuring VTP”](#).

Before configuring extended-range VLANs, VLANs 1025–4094, you must first enable MAC address reduction. When you enable MAC address reduction the system commits the 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 first delete the mappings. See the “[Clearing 802.1Q-to-ISL VLAN Mappings](#)” section on [page 10-11](#) for more information.

Creating or Modifying an Ethernet VLAN

To create a new Ethernet VLAN, perform this procedure in privileged mode:

| | Task | Command |
|--------|--------------------------------|--|
| Step 1 | Create a new Ethernet VLAN. | set vlan <i>vlan_num</i> [name <i>name</i>] [said <i>said</i>] [mtu <i>mtu</i>] [translation <i>vlan_num</i>] |
| Step 2 | Verify the VLAN configuration. | show vlan [<i>vlan_num</i>] |

**Note**

The default VLAN type is Ethernet; if you do not specify the type, the VLAN is an Ethernet VLAN.

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

```

Console> (enable) set vlan 500 name Engineering
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
500 Engineering                          active    344
VLAN Type SAID      MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
500 enet  100500   1500 -     -     -     -     -         0      0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

To modify the VLAN parameters on an existing Ethernet VLAN, perform this procedure in privileged mode:

| | Task | Command |
|--------|-----------------------------------|---|
| Step 1 | Modify an existing Ethernet VLAN. | set vlan <i>vlan_num</i> [name <i>name</i>] [state { active suspend }] [said <i>said</i>] [mtu <i>mtu</i>] [translation <i>vlan_num</i>] |
| Step 2 | Verify the VLAN configuration. | show vlan [<i>vlan_num</i>] |

This example shows how to change the vlan 500 name from Engineering to Development and verify the configuration:

```

Console> (enable) set vlan 500 name Development
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
500 Development                          active    344
VLAN Type SAID      MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
500 enet  100500   1500 -     -     -     -     -         0      0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)

```

Creating or Modifying a Normal-Range Ethernet VLAN

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

| | Task | Command |
|--------|--------------------------------------|--|
| Step 1 | Create a normal-range Ethernet VLAN. | set vlan <i>vlan</i> [name <i>name</i>] [said <i>said</i>] [mtu <i>mtu</i>] [translation <i>vlan</i>] |
| Step 2 | Verify the VLAN configuration. | show vlan [<i>vlan</i>] |

This example shows how to create normal-range VLANs 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)
```

This example shows how to verify that the switch is in PVST+ mode:

```
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)
```

To modify VLAN parameters on an existing normal-range VLAN, do this procedure in privileged mode:

| | Task | Command |
|--------|---------------------------------------|---|
| Step 1 | Modify an existing normal-range VLAN. | set vlan <i>vlan</i> [name <i>name</i>] [state { active suspend }] [said <i>said</i>] [mtu <i>mtu</i>] [translation <i>vlan</i>] |
| Step 2 | Verify the VLAN configuration. | show vlan [<i>vlan</i>] |

This example shows how to change the state of an Ethernet VLAN and verify the configuration:

```
Console> (enable) set vlan 500 state suspend
Vlan 500 configuration successful
Console> (enable) show vlan 500
VLAN Name                               Status      IfIndex Mod/Ports, Vlans
-----
500  Engineering          suspend     344
VLAN Type  SAID      MTU    Parent  RingNo  BrdgNo  Stp   BrdgMode  Trans1  Trans2
-----
500  enet  100500   1500   -       -       -    -         0       0
VLAN AREHops STEHops Backup CRF
-----
Console> (enable)
```

Creating or Modifying an Extended-Range VLAN

To create an extended-range Ethernet VLAN, perform this procedure in privileged mode:

| | Task | Command |
|--------|--------------------------------|---|
| Step 1 | Enable MAC address reduction. | set spantree macreduction { enable disable } |
| Step 2 | Create a VLAN. | set vlan <i>vlan</i> |
| Step 3 | Verify the VLAN configuration. | show vlan [<i>vlan</i>] |

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

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

```

To modify the VLAN parameters on an existing extended-range VLAN, perform this procedure in privileged mode:

| | Task | Command |
|--------|---|---|
| Step 1 | Modify an existing extended-range VLAN. | set vlan <i>vlan</i> [name <i>name</i>] [state { active suspend }] [said <i>said</i>] [mtu <i>mtu</i>] [translation <i>vlan</i>] |
| Step 2 | Verify the VLAN configuration. | show vlan [<i>vlan</i>] |

This example shows how to change the state of an extended-range Ethernet VLAN and verify the configuration:

```

Console> (enable) set vlan 2000 state suspend
Vlan 2000 configuration successful
Console> (enable) show vlan 2000
VLAN Name                               Status    IfIndex Mod/Ports, Vlans
-----
2000 VLAN2000                            suspend    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

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

```

Assigning Switch Ports to a VLAN

A VLAN created in a management domain remains unused until you assign one or more switch ports to the VLAN. If you specify a VLAN that does not exist, the VLAN is created and the specified ports are assigned to it.

To assign one or more switch ports to a VLAN, perform this procedure in privileged mode:

| | Task | Command |
|--------|--|--|
| Step 1 | Assign one or more switch ports to a VLAN. | set vlan <i>vlan_num mod_num/port_num</i> |
| Step 2 | Verify the port VLAN membership. | show vlan [<i>vlan_num</i>] show port [<i>mod_num[/port_num]</i>] |

This example shows how to assign switch ports to a VLAN and verify the assignment:

```

Console> (enable) set vlan 500 2/4
VLAN 500 modified.
VLAN 560 modified.
VLAN Mod/Ports
-----
500 2/4
Console> (enable) show vlan 500
VLAN Name                               Status   IfIndex Mod/Ports, Vlans
-----
500 Engineering                          active   59      2/4

VLAN Type SAID      MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
-----
500 enet  100500    1500 -     -     -     -     -     0     0

VLAN AREHops STEHops Backup CRF
-----
Console> (enable) show port 2/4
Port Name                               Status   Vlan     Level Duplex Speed Type
-----
2/4                                           notconnect 500     normal  auto  auto 10/100BaseTX

Port Security Secure-Src-Addr Last-Src-Addr Shutdown Trap IfIndex
-----
2/4 disabled                                           No      disabled 12

Port Status Channel Channel Neighbor Neighbor
      mode status device
-----
2/4 notconnect auto not channel

```

```

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
-----
 2/4          -          0          0          0          0

Port  Single-Col Multi-Coll  Late-Coll  Excess-Col  Carri-Sen  Runts    Giants
-----
 2/4          0          0          0          0          0          0        0

Last-Time-Cleared
-----
Wed Jul 26 2000, 19:44:05
Console> (enable)

```

Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1–1000. The valid range of VLANs specified in the IEEE 802.1Q standard is 0–4095. In a network environment with non-Cisco devices connected to Cisco switches through 802.1Q trunks, you must map 802.1Q VLAN numbers greater than 1000 to ISL VLAN numbers.

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.

Keep the following in mind when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to seven 802.1Q-to-ISL VLAN mappings on the switch.
- You must 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 you configure the same VLAN mappings on all appropriate switches in the network.
- You cannot use dot1q-to-isl mappings if you have extended-range VLANs.

To map an 802.1Q VLAN to an ISL VLAN, perform this procedure 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. | set vlan mapping dot1q <i>dot1q_vlan</i> isl <i>isl_vlan</i> |
| Step 2 | Verify the VLAN mapping. | show vlan mapping |

This example shows how to map 802.1Q VLANs 2000, 3000, and 4000 to ISL VLANs 200, 300, and 400 respectively and how to 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)

```

Clearing 802.1Q-to-ISL VLAN Mappings

To clear an 802.1Q-to-ISL VLAN mapping, perform this procedure in privileged mode:

| | Task | Command |
|--------|--------------------------------------|--|
| Step 1 | Clear an 802.1Q-to-ISL VLAN mapping. | clear vlan mapping dot1q { <i>dot1q_vlan</i> all } |
| Step 2 | Verify the VLAN mapping. | show vlan mapping |

This example shows how to clear 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 clear all 802.1Q-to-ISL VLAN mappings:

```

Console> (enable) clear vlan mapping dot1q all
All vlan mapping entries deleted
Console> (enable)

```

Deleting a VLAN

When you delete a VLAN in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN in VTP transparent mode, the VLAN is deleted only on the current switch. When you are on a VTP client, you can only delete a VLAN on the local switch.



Caution

When you delete a VLAN, any ports assigned to that VLAN become inactive. Such ports remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

To delete a VLAN on the switch, perform this task in privileged mode:

| Task | Command |
|----------------|-----------------------------------|
| Delete a VLAN. | clear vlan <i>vlan_num</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 500
in the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 500 deleted
Console> (enable)

```

Configuring Private VLANs

A private VLAN is a VLAN you configure to have some Layer 2 isolation from other ports within the same private VLAN. Ports belonging to a private VLAN are associated with a common set of supporting VLANs that are used to create the private VLAN structure. You can configure private VLANs and normal VLANs from the same Catalyst 4000 family switch.

There are three types of private VLAN ports: promiscuous, isolated, and community.

- A promiscuous port communicates with all other private VLAN ports and is the port you use to communicate with routers, LocalDirector, the CSS11000, backup servers, and administrative workstations.
- An isolated port has complete Layer 2 separation, including broadcasts, from other ports within the same private VLAN with the exception of the promiscuous port.
- Community 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. Broadcasts propagate only between associated community ports and the promiscuous port.

Privacy is granted at the Layer 2 level by blocking outgoing traffic to all isolated ports. All isolated ports are assigned to an isolated VLAN where this hardware function occurs. Traffic received from an isolated port is forwarded to all promiscuous ports only.

Within a private VLAN are three distinct classifications of VLANs: a single primary VLAN, a single isolated VLAN, and a series of community VLANs.

Define each supporting VLAN within a private VLAN structure before configuring the private VLAN:

- Primary VLAN—Conveys incoming traffic from the promiscuous port to all other promiscuous, isolated, and 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 and can be received only by promiscuous ports.
- Community VLAN—Used by a group of community ports to communicate among themselves and transmit traffic outside the group via the designated promiscuous port.

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, a second VLAN is designated as either an isolated VLAN, community VLAN, or two-way community VLAN. You can 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 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 only 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 inter-server communication at Layer 2.
- Designate as promiscuous the ports to which the default gateway(s), backup server, or LocalDirector are attached, to allow all stations to have access to these gateways.
- Reduce VLAN consumption. You need to allocate only one IP subnet to the entire group of stations, because all stations reside in one common private VLAN.

- Conserve public address space. Servers are now isolated from one another using private VLANs, which eliminates the necessity of creating multiple IP subnets. Multiple IP subnets waste public IP addresses on multiple subnet and broadcast addresses. As a result, all servers can be members of the same IP subnet, but they remain isolated from one another.

Private VLAN Configuration Guidelines

Follow these guidelines to configure private VLANs:

- Designate one VLAN as the primary VLAN.
- Designate one VLAN as an isolated VLAN. If you want to use private VLAN communities, 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 nontrunk ports as promiscuous ports.
- You must set VTP to transparent mode.
- Once you configure a private VLAN, you cannot change the VTP mode to client or server mode, because VTP does not support private VLAN types or 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 assigned to it.
- An isolated or community VLAN can have only one primary VLAN associated with it.
- Private VLANs can use VLANs 2 through 1000 and 1025 through 4096.
- If you delete either the primary or isolated VLAN, the ports associated with the VLAN become inactive.
- When configuring private VLANs, note these hardware and software restrictions:
 - You can use the sc0 interface in a private VLAN assigned to either an isolated or community VLAN, but not as a promiscuous port to a primary VLAN.
 - You cannot set private VLAN ports to trunking mode or channeling or have dynamic VLAN memberships. If you attempt such a configuration, a warning message is displayed and the command is rejected.
- Isolated and community ports should run BPDU guard features to prevent spanning tree loops caused by misconfigurations.
- Primary VLANs and associated isolated/community VLANs must have the same spanning tree configuration. This configuration maintains consistent spanning tree topologies among associated primary, isolated, and community VLANs and avoids connectivity loss. These priorities and parameters automatically propagate from the primary VLAN to isolated and community VLANs.

- You can create private VLANs that run in MISTP mode.
 - If you disable MISTP, any change to the configuration of a private VLAN propagates to all corresponding isolated and community VLANs, and you cannot change the isolated or community VLANs.
 - If you enable MISTP, you can configure only the MISTP instance with the private VLAN. Changes are applied to the primary VLAN and propagate to 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 double-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 4000 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 it 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 non-root bridge.
- BPDU guard mode and UplinkFast affect the system and are automatically enabled once the first port is added 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.
- IGMP snooping and multicast shortcuts are not supported in private VLANs.
- You cannot enable EtherChannel on isolated, community, or promiscuous ports.
- You cannot set a VLAN to a private VLAN if the VLAN has dynamic access control entries (ACEs) configured on it.
- 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 Private VLAN

You can bind isolated or community VLAN(s) to the primary VLAN without associating the isolated or community ports to the private VLAN: use the **set pvlan** *primary_vlan_num* {*isolated_vlan_num* | *community_vlan_num*} command.

You can change the isolated or community ports associated to the private VLAN without changing the isolated or community VLANs binding: use the **set pvlan** *primary_vlan_num* {*isolated_vlan_num* | *community_vlan_num*} *mod/port* command.

Ports do not have to be on the same switch as long as the switches are connected to the trunk and the private VLAN has not been removed from the trunk.

You must enter the **set pvlan** command everywhere that a private VLAN needs to be created. This includes entering the command on switches with isolated or community ports, switches with promiscuous ports, and all *intermediate* switches that need to carry private VLANs on their trunks. On the edge switches that do not have any isolated, community, or promiscuous ports (typically, access switches with no private ports), the private VLANs do not need to be created and can be pruned from the trunks for security reasons.

To create a private VLAN, perform this procedure in privileged mode:

| | Task | Command |
|---------------|---|--|
| Step 1 | Create the primary VLAN. | set vlan <i>vlan_num</i> pvlan-type primary |
| Step 2 | Set the isolated or community VLAN(s). | set vlan <i>vlan_num</i> pvlan-type {isolated community} |
| Step 3 | Bind the isolated or community VLAN(s) to the primary VLAN and associate the isolated or community port(s) to the private VLAN. | set pvlan <i>primary_vlan_num</i> {<i>isolated_vlan_num</i> <i>community_vlan_num</i>} <i>mod/ports</i> |
| Step 4 | Map the isolated/community VLAN to the primary VLAN on the promiscuous port. | set pvlan mapping <i>primary_vlan_num</i> {<i>isolated_vlan_num</i> <i>community_vlan_num</i>} <i>mod/ports</i> |
| Step 5 | Verify the private VLAN configuration. | show pvlan [<i>vlan_num</i>] show pvlan mapping |

The following example shows how to create a private VLAN using VLAN 7 as the primary VLAN, VLAN 901 as the isolated VLAN, and VLANs 902 and 903 as the community VLANs. VLAN 901 uses module 4, port 3. VLAN 902 uses module 4, ports 4 through 6. VLAN 903 uses module 4, ports 7 through 9. The router is attached to the promiscuous port 3/1.

Before starting, verify that VLANs 7, 901, 902, and 903 have no ports assigned to them, do so by using the **show vlan *vlan_num*** command. If any ports are assigned to one or more of these VLANs, set them to some other VLAN using the **set vlan *vlan_num* {*mod/port*}** command.

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 port 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 1q 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 1q 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.

These examples show 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
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.

```

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. | clear vlan <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 or Community VLAN

If you delete an isolated or community VLAN, the binding with the primary VLAN is broken, any isolated or community ports 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. | clear vlan { <i>isolated_vlan_num</i> <i>community_vlan_num</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 or 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, or community VLAN to which it belongs is cleared.
- An error occurs during the configuration of a port to be 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. | clear pvlan mapping primary_vlan { <i>isolated</i> <i>community</i> } { <i>mod/ports</i> } |

This example shows how to delete the mapping of VLAN 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)
```