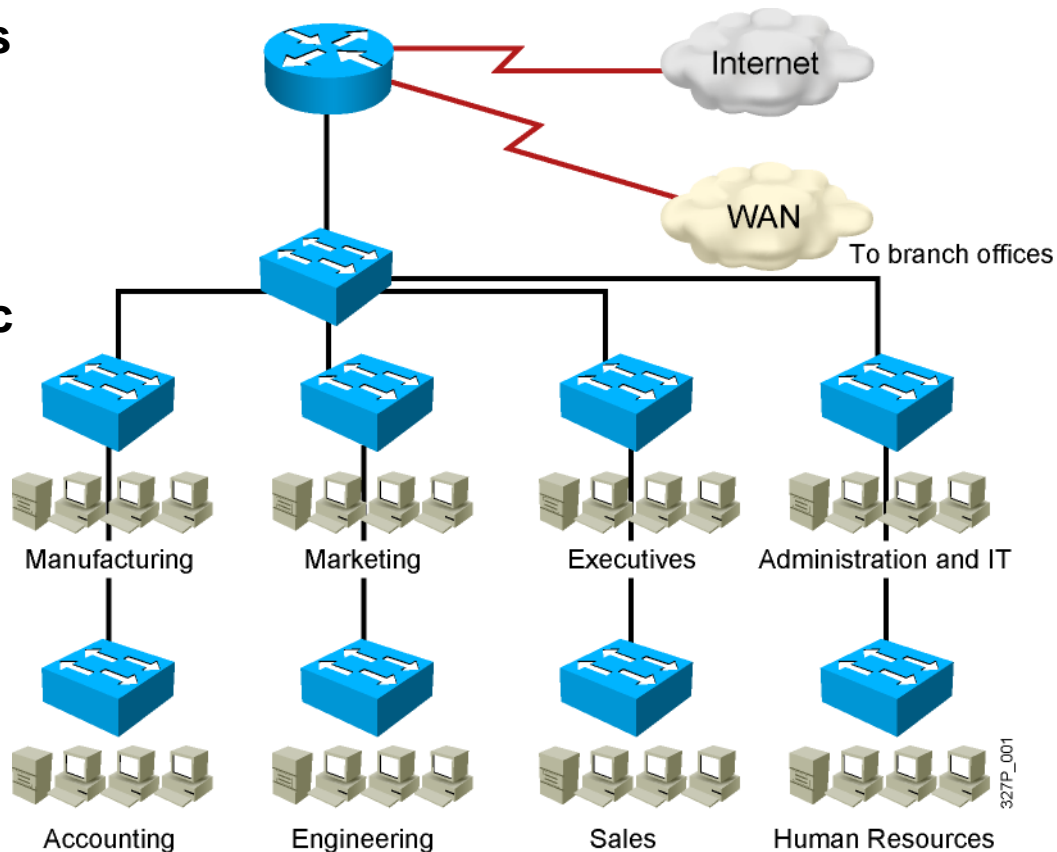# Implementing VLANs and Trunks
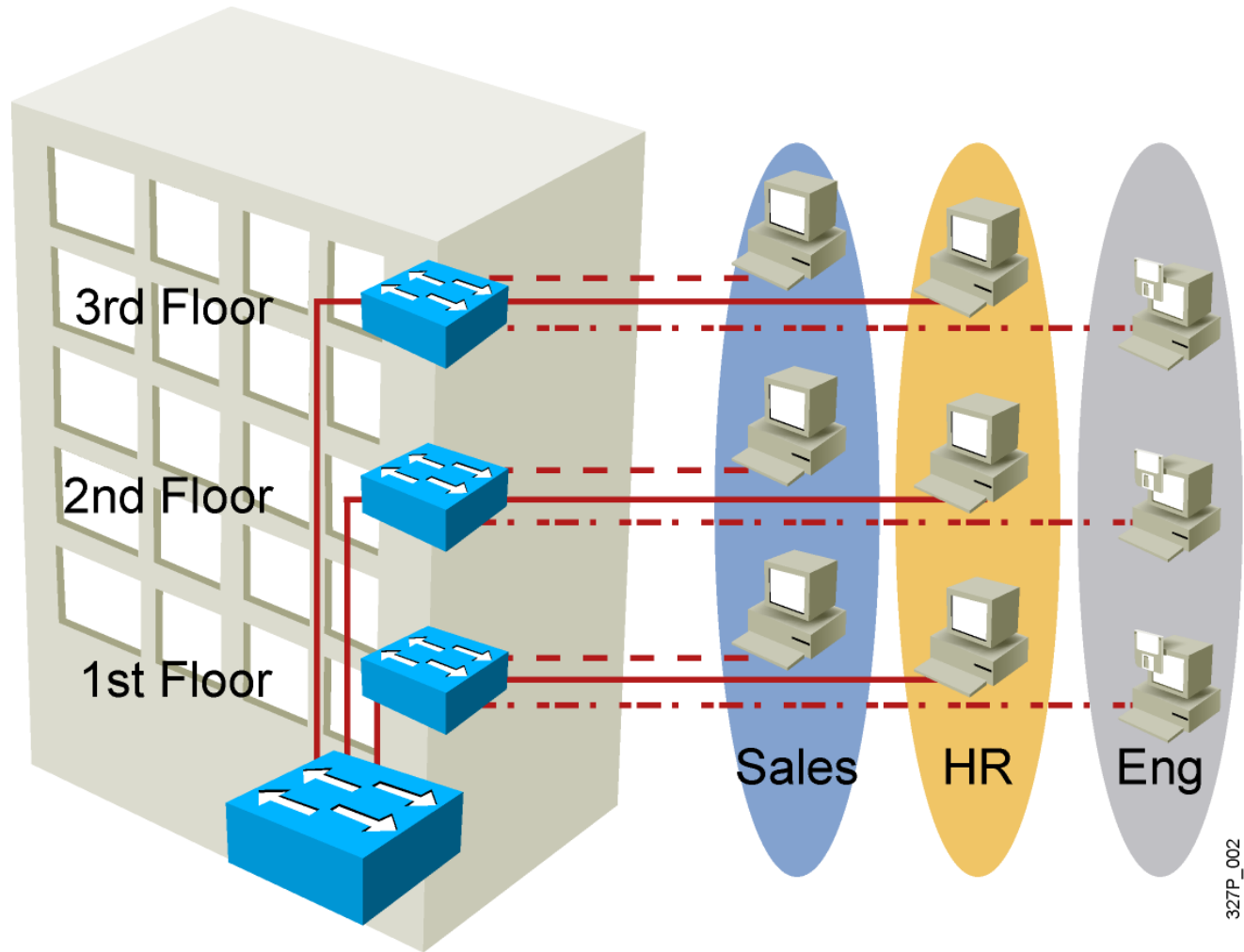
Issues in a Poorly Designed Network

- **Unbounded failure domains**
- **Large broadcast domains**
- **Large amount of unknown MAC unicast traffic**
- **Unbounded multicast traffic**
- **Management and support challenges**
- **Possible security vulnerabilities**

VLAN Overview

- **Segmentation**
- **Flexibility**
- **Security**

VLAN = Broadcast Domain = Logical Network (Subnet)

Designing VLANs for an Organization

- **VLAN design must take into consideration the implementation of a hierarchical network addressing scheme.**
- **The benefits of hierarchical addressing are:**
  - **Ease of management and troubleshooting**
  - **Minimization of errors**
  - **Reduced number of routing table entries**

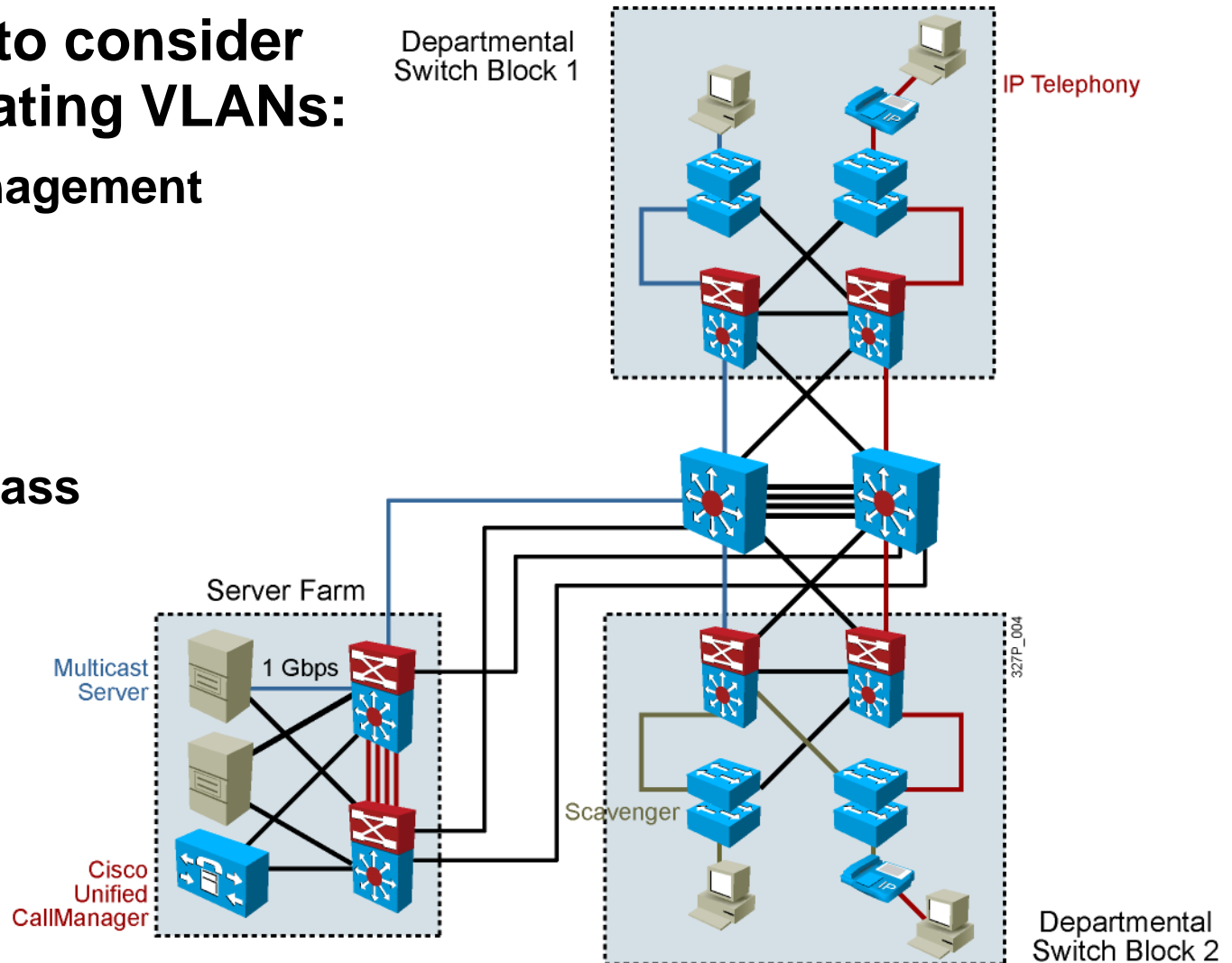# Guidelines for Applying IP Address Space
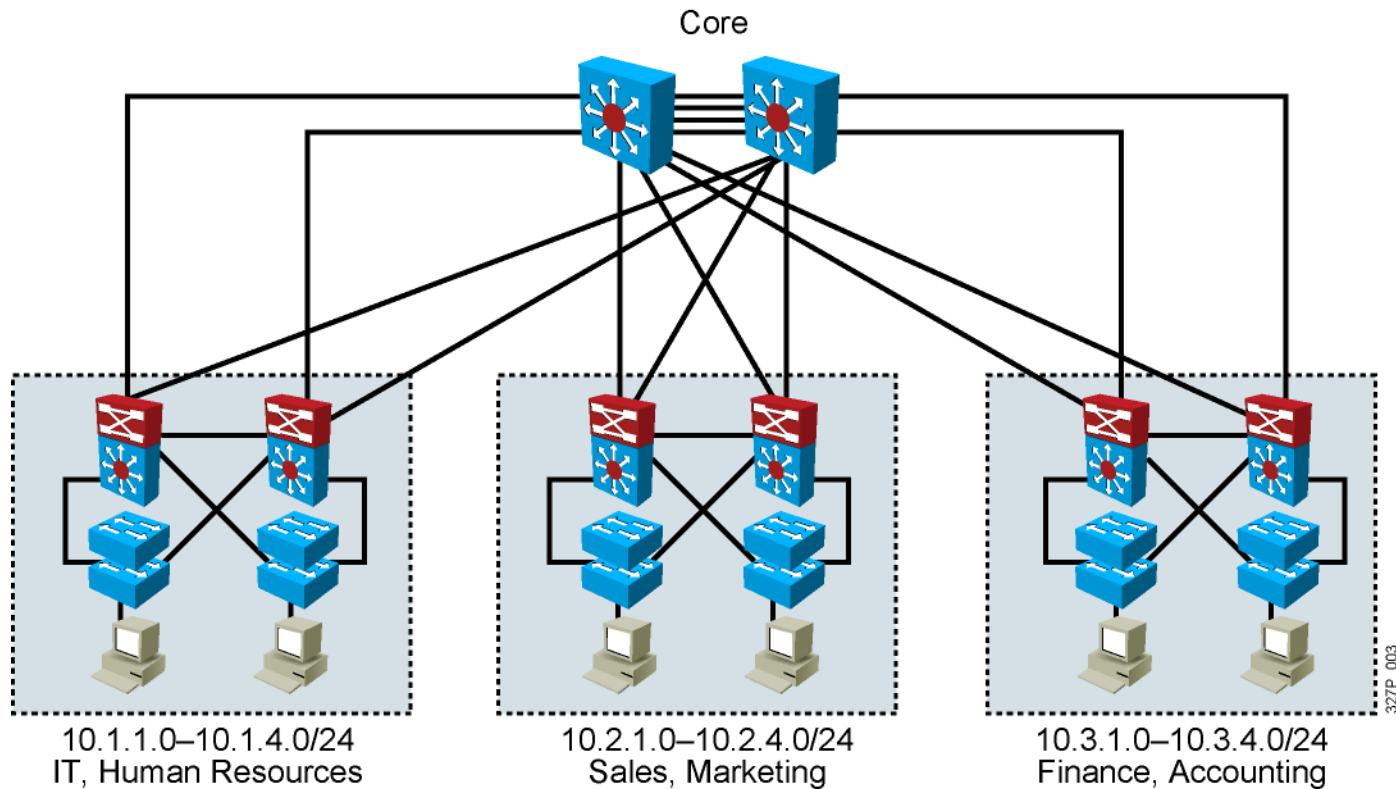
- **Allocate one IP subnet per VLAN.**
- **Allocate IP address spaces in contiguous blocks.**

Network Traffic Types

Traffic types to consider when designating VLANs:

- **Network management**
- **IP telephony**
- **IP Multicast**
- **Normal data**
- **Scavenger class**

802.1Q Trunking

Cisco Catalyst
Series Switch

802.1Q
Trunk

802.1Q
Trunk

802.1Q
Trunk

802.1Q
Trunk

Catalyst
Series Switch

Catalyst
Series Switch

Catalyst
Series Switch

Catalyst
Series Switch

VLAN 1

VLAN 2

VLAN 3

VLAN 2

VLAN 1

VLAN 3

327P_507

802.1Q Frame

Dest	Src	Len/Etype	Data	~~FCS~~	Original Frame

Dest	Src	Tag	Len/Etype	Data	FCS	Tagged Frame

EtherType (0x8100)	PRI		VLAN ID

↑ Token Ring Encapsulation Flag

327P_077
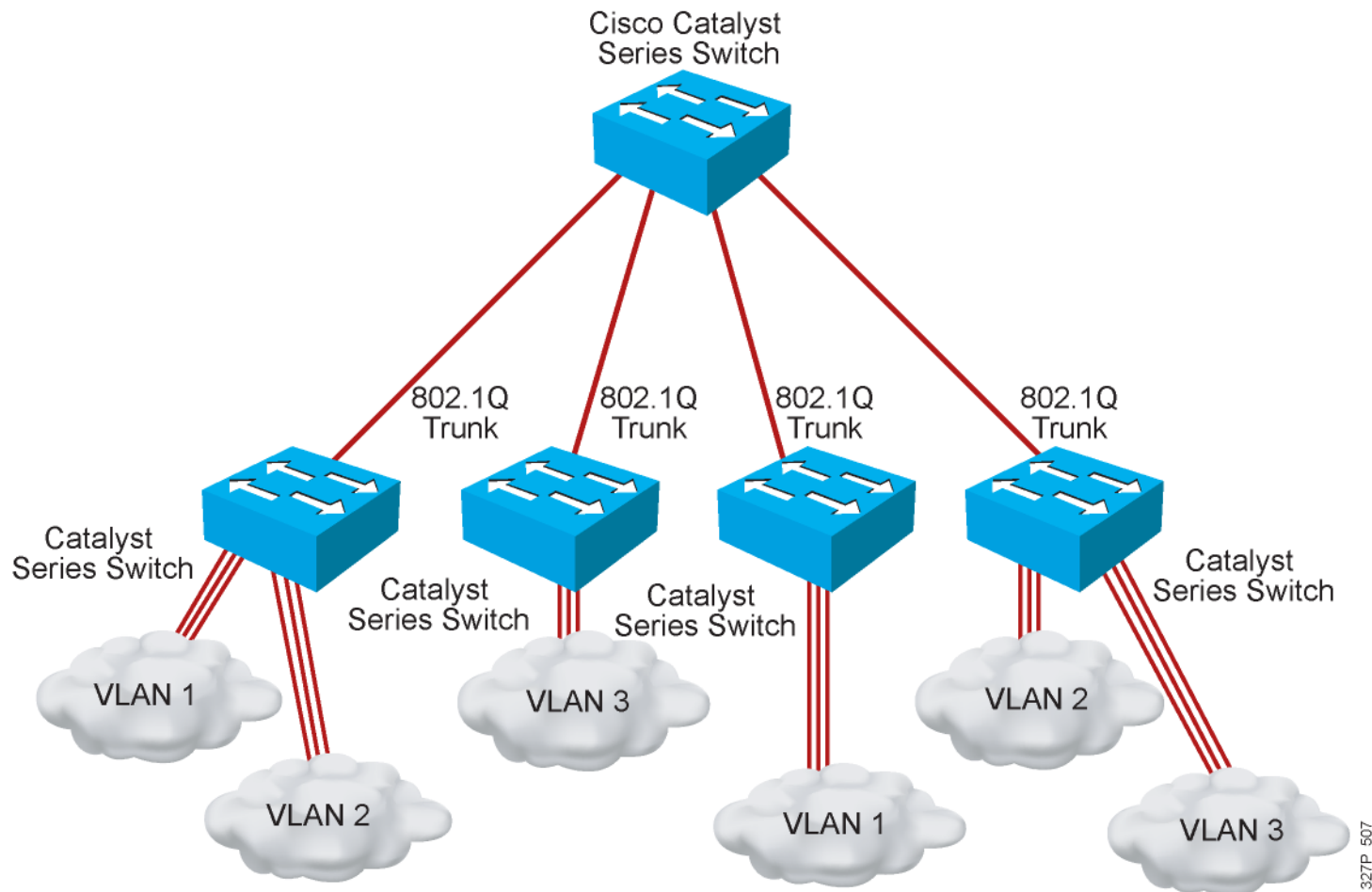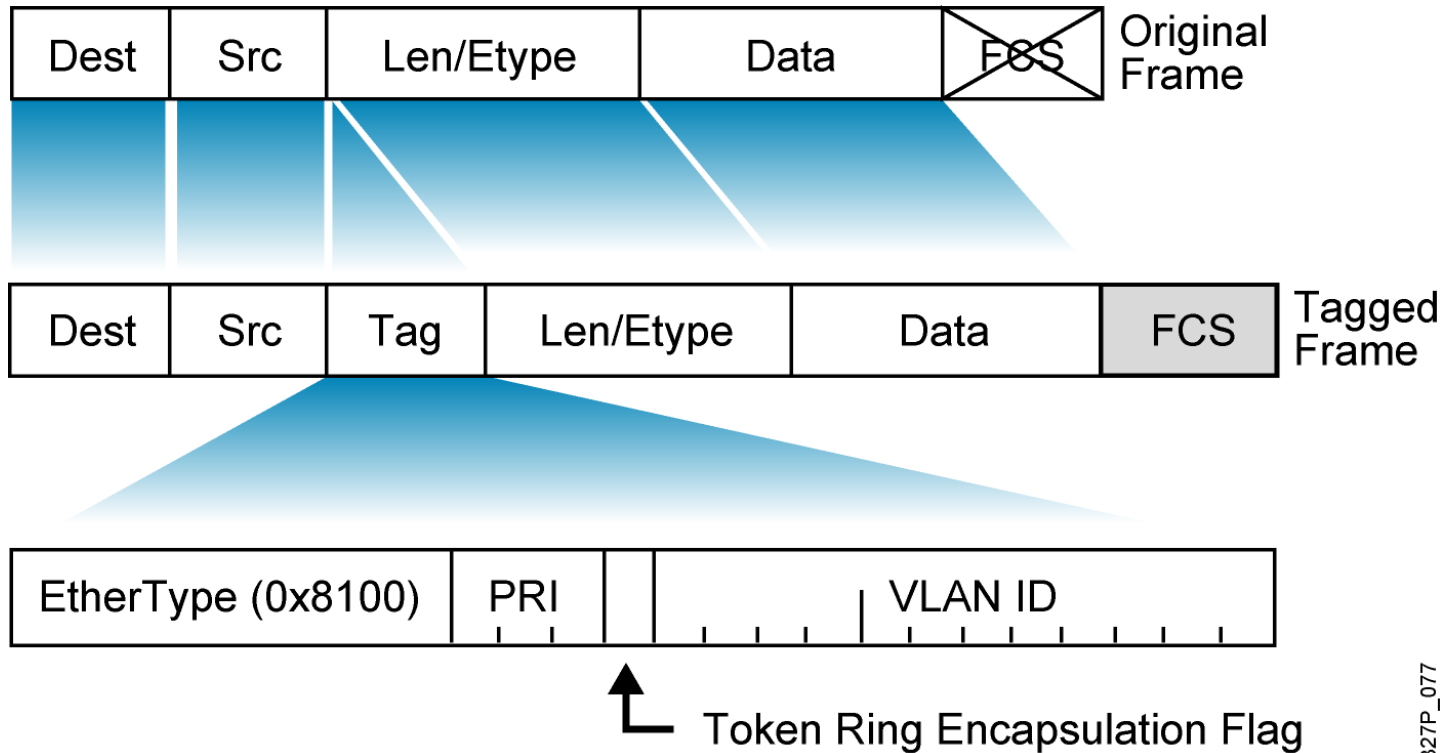
ISL Encapsulation
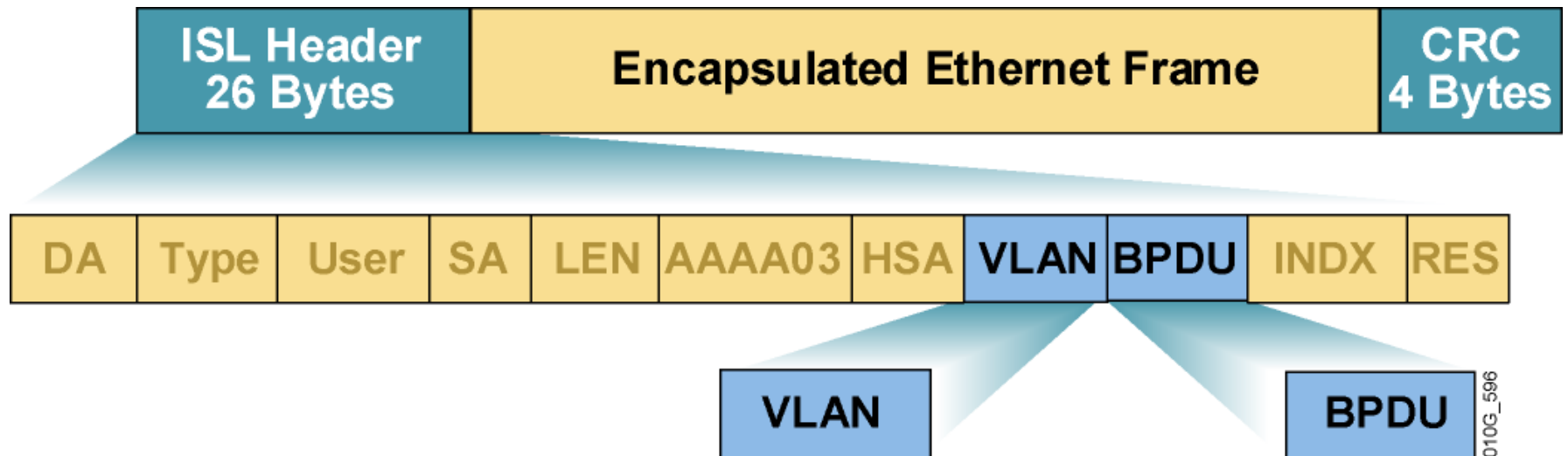
Understanding Native VLANs

Native VLAN–untagged

327P_504
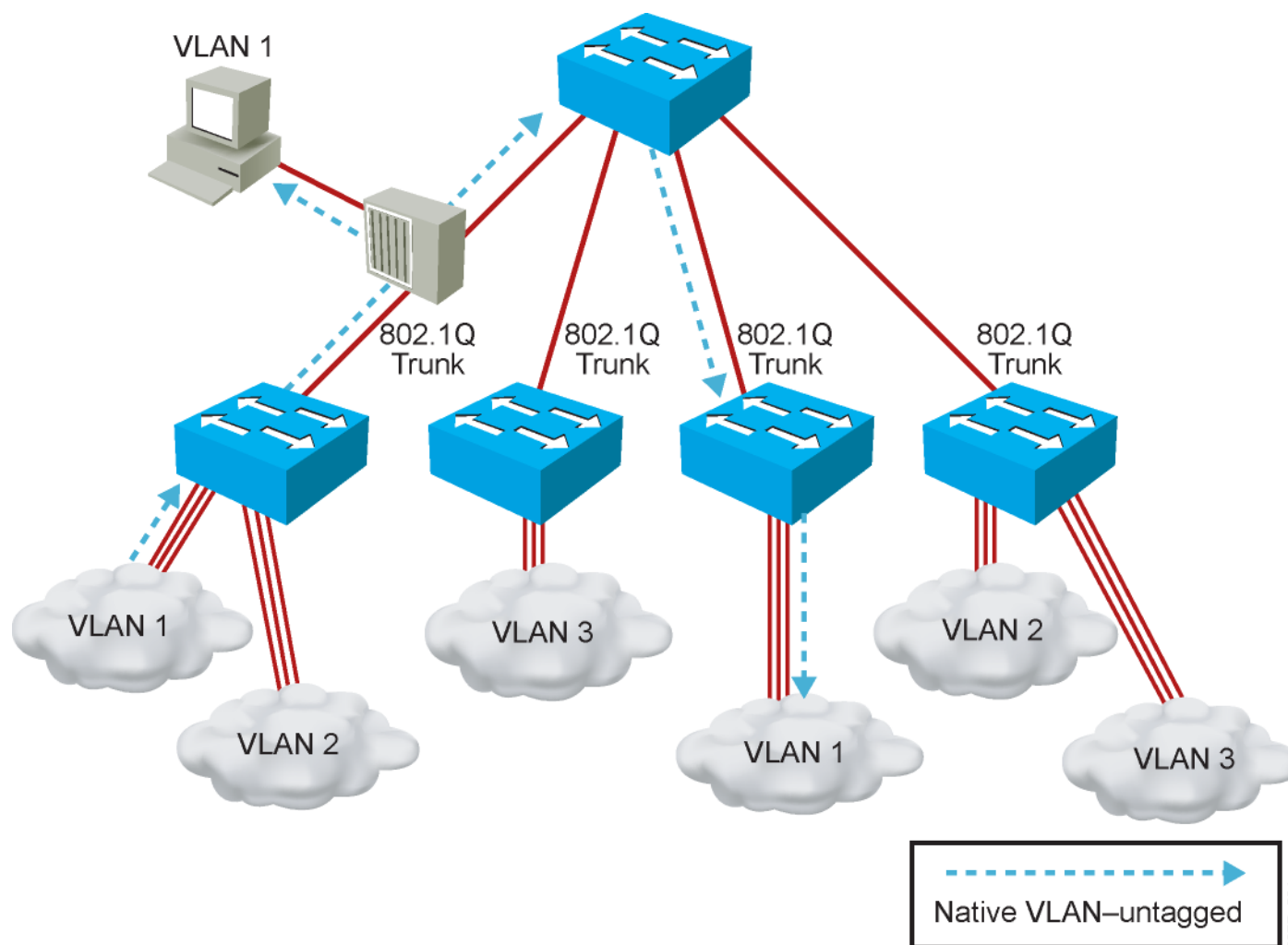
VTP Features

VTP Domain
ICND

VTP Server

1. VLAN added/deleted

2. Change propagated

802.1Q Trunk
802.1Q Trunk
802.1Q Trunk
802.1Q Trunk

VTP Client
VTP Client
VTP Client
VTP Client

3. Synch to latest change

327P_005

VTP Modes

- **Create VLANs**
- **Modify VLANs**
- **Delete VLANs**
- **Sends and forwards advertisements**
- **Synchronizes**

Server

Client

Transparent

- **Cannot create, change, or delete VLANs**
- **Sends and forwards advertisements**
- **Synchronizes**

- **Create local VLANs only**
- **Modify local VLANs only**
- **Delete local VLANs only**
- **Forwards advertisements**
- **Does not synchronize**

327P_078
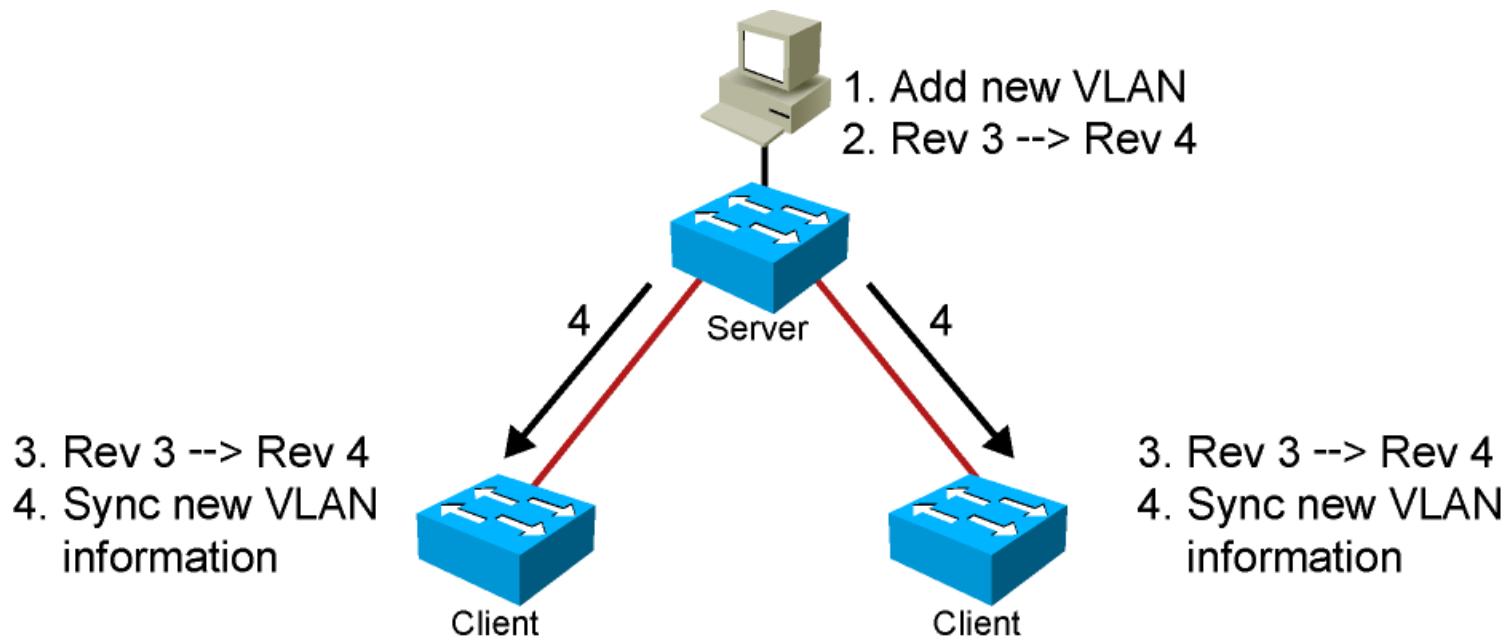
VTP Operation

- **VTP advertisements are sent as multicast frames.**
- **VTP servers and clients are synchronized to the latest revision number.**
- **VTP advertisements are sent every 5 minutes or when there is a change.**

VTP Pruning
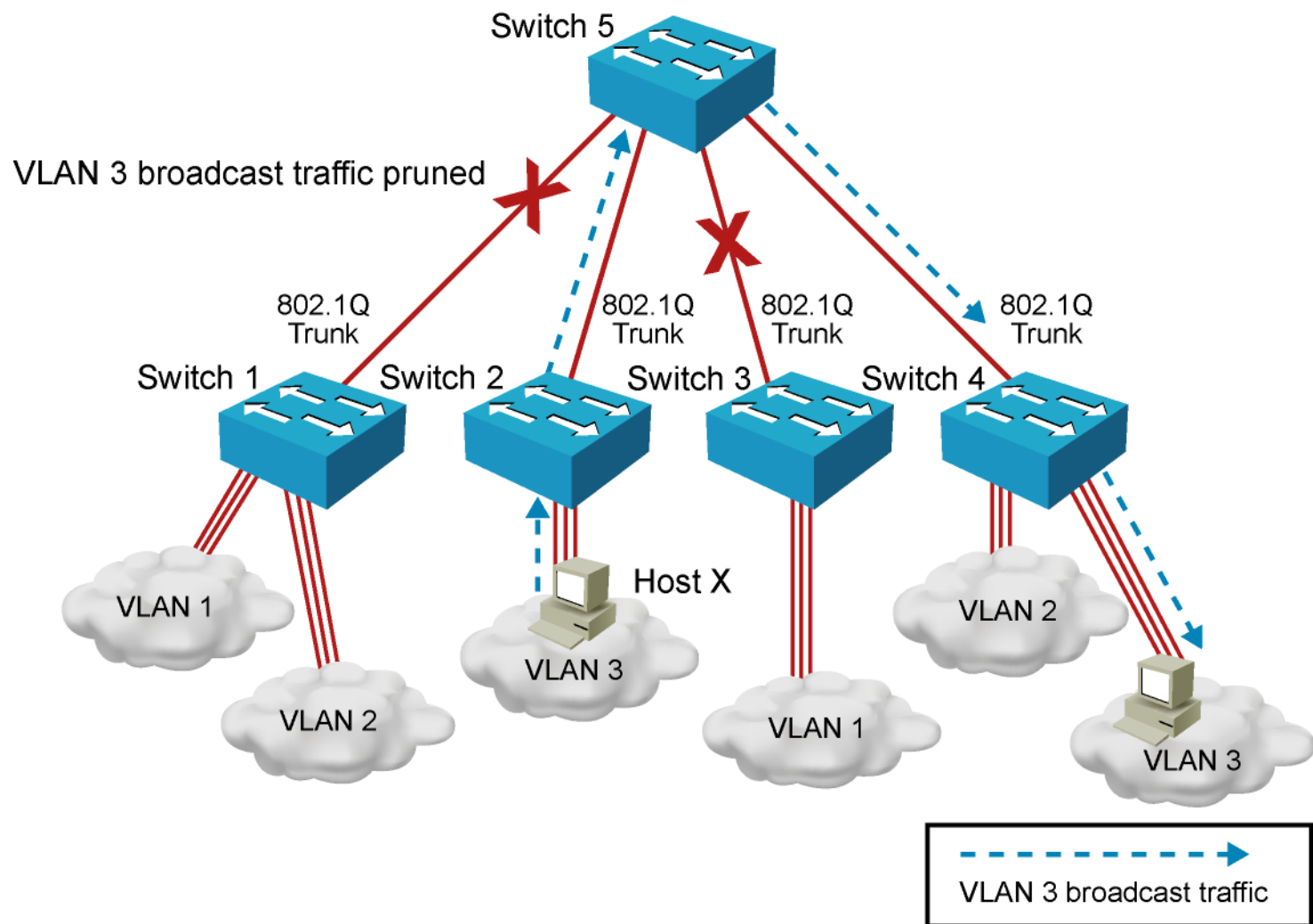
Configuring VLANs and Trunks

1. Configure and verify VTP.

2. Configure and verify 802.1Q trunks.

3. Create or modify a VLAN on the VTP server switch.

4. Assign switch ports to a VLAN and verify.

5. Execute adds, moves, and changes.

6. Save the VLAN configuration.

VTP Configuration Guidelines

- **VTP defaults for the Cisco Catalyst switch:**
  - **VTP domain name: None**
  - **VTP mode: Server mode**
  - **VTP pruning: Enabled or disabled (model specific)**
  - **VTP password: Null**
  - **VTP version: Version 1**
- **A new switch can automatically become part of a domain once it receives an advertisement from a server.**
- **A VTP client can overwrite a VTP server database if the client has a higher revision number.**
- **A domain name cannot be removed after it is assigned; it can only be reassigned.**

Creating a VTP Domain

```
SwitchX# configure terminal
SwitchX(config)# vtp mode [ server | client | transparent ]
SwitchX(config)# vtp domain domain-name
SwitchX(config)# vtp password password
SwitchX(config)# vtp pruning
SwitchX(config)# end
```
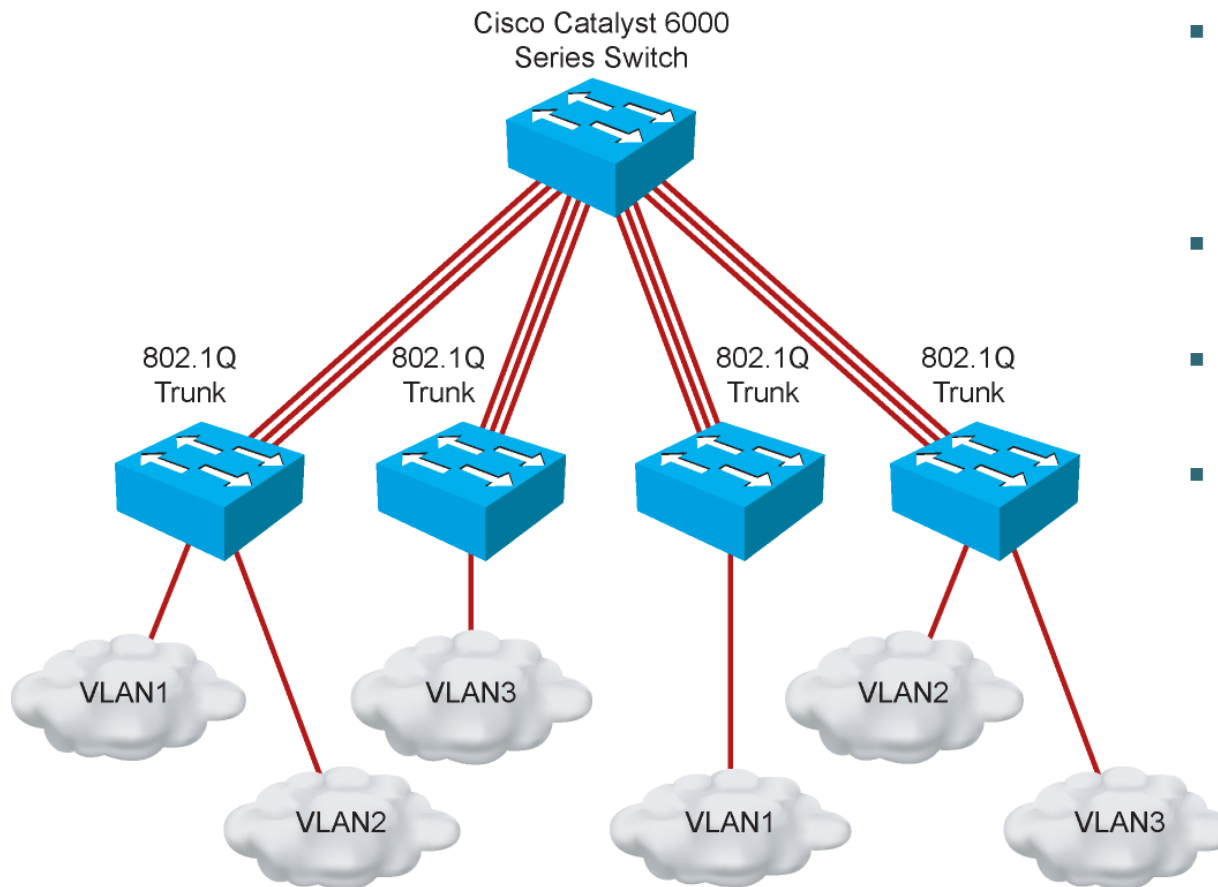
VTP Configuration and Verification Example

```
SwitchX(config)# vtp domain ICND
Changing VTP domain name to ICND
SwitchX(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
SwitchX(config)# end

SwitchX# show vtp status
VTP Version                      : 2
Configuration Revision           : 0
Maximum VLANs supported locally  : 64
Number of existing VLANs         : 17
VTP Operating Mode               : Transparent
VTP Domain Name                  : ICND
VTP Pruning Mode                 : Disabled
VTP V2 Mode                      : Disabled
VTP Traps Generation             : Disabled
MD5 digest                       : 0x7D 0x6E 0x5E 0x3D 0xAF 0xA0 0x2F 0xAA
Configuration last modified by 10.1.1.4 at 3-3-93 20:08:05
SwitchX#
```

802.1Q Trunking Issues

Cisco Catalyst 6000 Series Switch

802.1Q Trunk

VLAN1

VLAN2

VLAN3

VLAN2

VLAN1

VLAN3

327P_079

- **Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link.**

- **Note that native VLAN frames are untagged.**

- **A trunk port cannot be a secure port.**

- **All 802.1Q trunking ports in an EtherChannel group must have the same configuration.**

Configuring 802.1Q Trunking

`SwitchX(config-if)#`

```
switchport mode {access |  dynamic {auto | desirable} | trunk}
```

- **Configures the trunking characteristics of the port**

`SwitchX(config-if)#`

```
switchport mode trunk
```

- **Configures the port as a VLAN trunk**

Verifying a Trunk

```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
 . . .
```

```
SwitchX# show interfaces fa0/11 trunk

Port          Mode            Encapsulation    Status         Native vlan
Fa0/11        desirable       802.1q           trunking       1

Port          Vlans allowed on trunk
Fa0/11        1-4094

Port          Vlans allowed and active in management domain
Fa0/11        1-13
```

VLAN Creation Guidelines

- The maximum number of VLANs is switch-dependent.

- Most Cisco Catalyst desktop switches support 128 separate spanning-tree instances, one per VLAN.

- VLAN 1 is the factory default Ethernet VLAN.

- Cisco Discovery Protocol and VTP advertisements are sent on VLAN 1.

- The Cisco Catalyst switch IP address is in the management VLAN (VLAN 1 by default).

- If using VTP, the switch must be in VTP server or transparent mode to add or delete VLANs.

Adding a VLAN

```
SwitchX# configure terminal
SwitchX(config)# vlan 2
SwitchX(config-vlan)# name switchlab99
```

Verifying a VLAN

```
SwitchX# show vlan [brief | id vlan-id || name vlan-name]
```

```
SwitchX# show vlan id 2

VLAN Name                             Status     Ports
---- -------------------------------- ---------- -------------------------------
2    switchlab99                      active     Fa0/2, Fa0/12

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0


.   .   .
SwitchX#
```

Assigning Switch Ports to a VLAN

`SwitchX(config-if)#`

```
switchport access [vlan vlan# | dynamic]
```

```
SwitchX# configure terminal
SwitchX(config)# interface range fastethernet 0/2 - 4
SwitchX(config-if)# switchport access vlan 2

SwitchX# show vlan

VLAN Name                              Status     Ports
---- -------------------------------- --------- ------------------------
1    default                          active     Fa0/1
2    switchlab99                      active     Fa0/2, Fa0/3, Fa0/4
```

Verifying VLAN Membership

```
SwitchX# show vlan brief
```

```
SwitchX# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- ------------------------------
1    default                          active    Fa0/1
2    switchlab99                       active    Fa0/2, Fa0/3, Fa0/4
3    vlan3                            active
4    vlan4                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup

VLAN Name                             Status    Ports
---- -------------------------------- --------- ------------------------------
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Verifying VLAN Membership (Cont.)

SwitchX(config-if)#

```
show interfaces interface switchport
```

```
SwitchX# show interfaces fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (switchlab99)
Trunking Native Mode VLAN: 1 (default)
--- output omitted ----
```

Executing Adds, Moves, and Changes for VLANs

- **When using VTP, the switch must be in VTP server or transparent mode to add, change, or delete VLANs.**

- **When you make VLAN changes from a switch in VTP server mode, the change is propagated to other switches in the VTP domain.**

- **Changing VLANs typically implies changing IP networks.**

- **After a port is reassigned to a new VLAN, that port is automatically removed from its previous VLAN.**

- **When you delete a VLAN, any ports in that VLAN that are not moved to an active VLAN will be unable to communicate with other stations.**