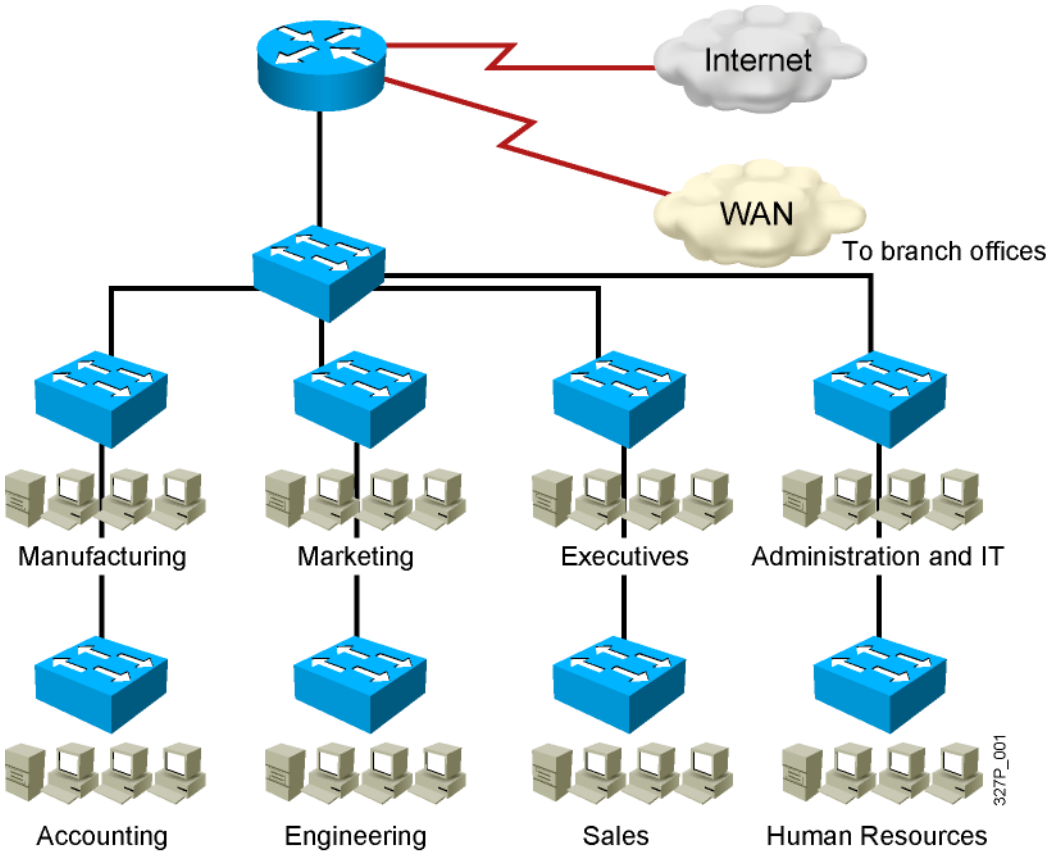
Implementing VLANs and Trunks

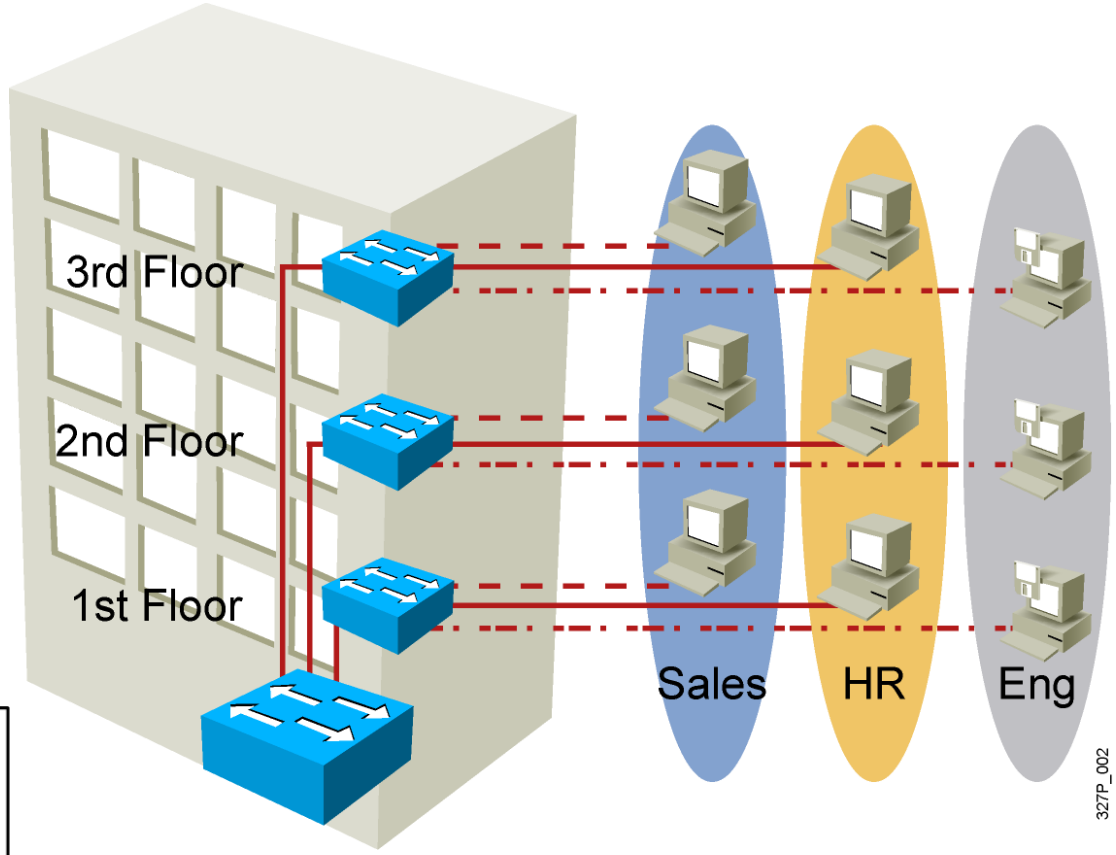
Issues in a Poorly Designed Network

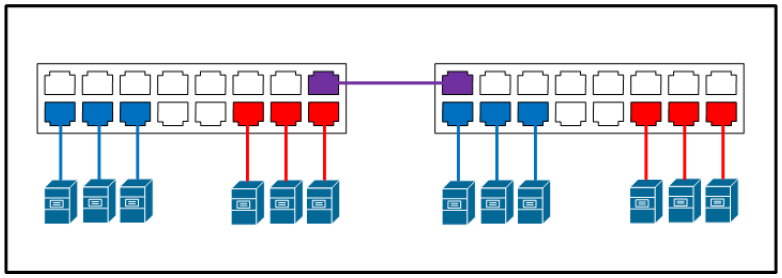
- Unbounded failure domains
- Large broadcast domains
- Large amount of unknown MAC unicast traffic
- Unbounded multicast traffic
- Management and support challenges
- Possible security vulnerabilities



VLAN Overview

- Segmentation
- Flexibility
- Security



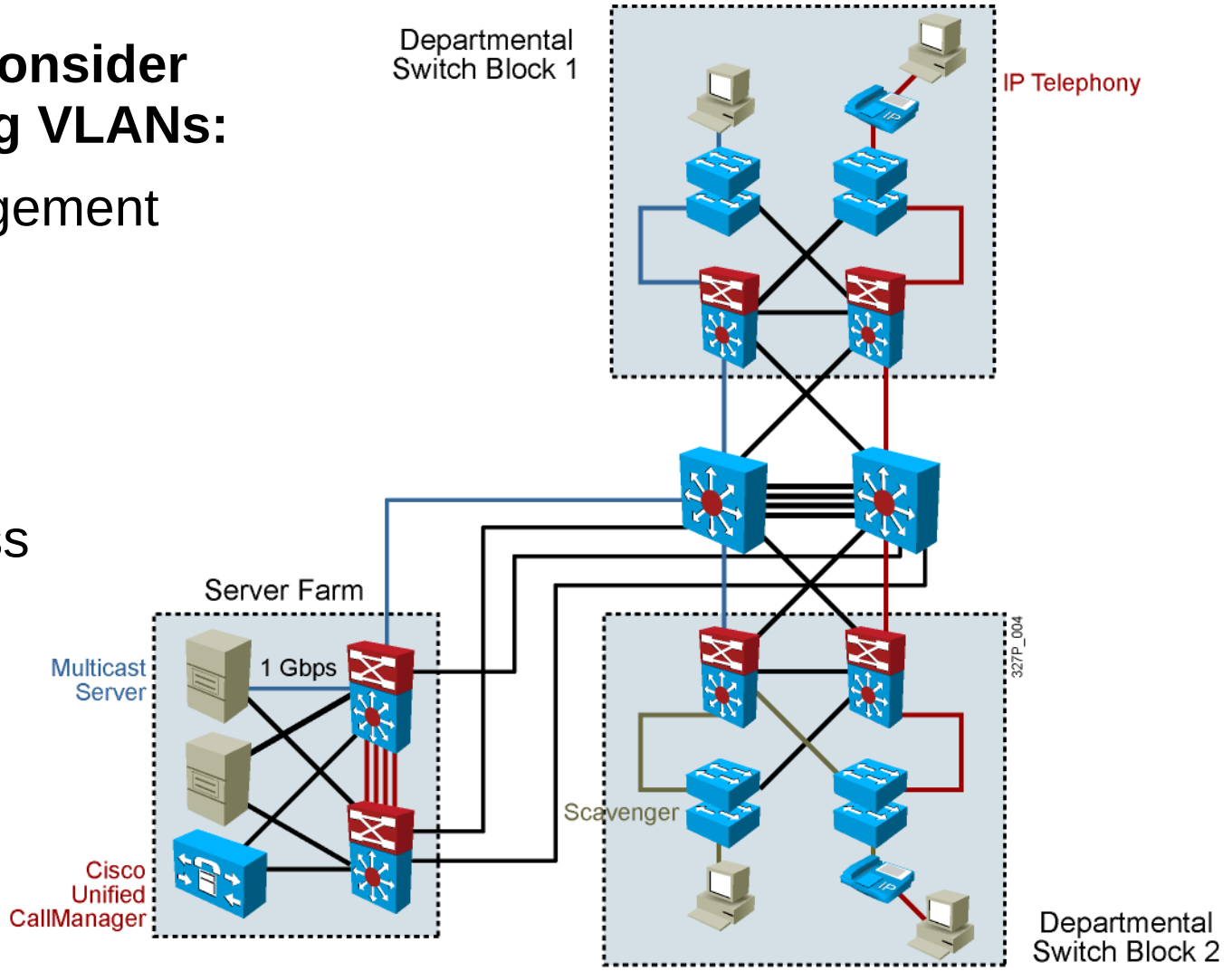


VLAN (Virtual LAN) = Broadcast Domain = Logical Network (Subnet)

Network Traffic Types

Traffic types to consider when designating VLANs:

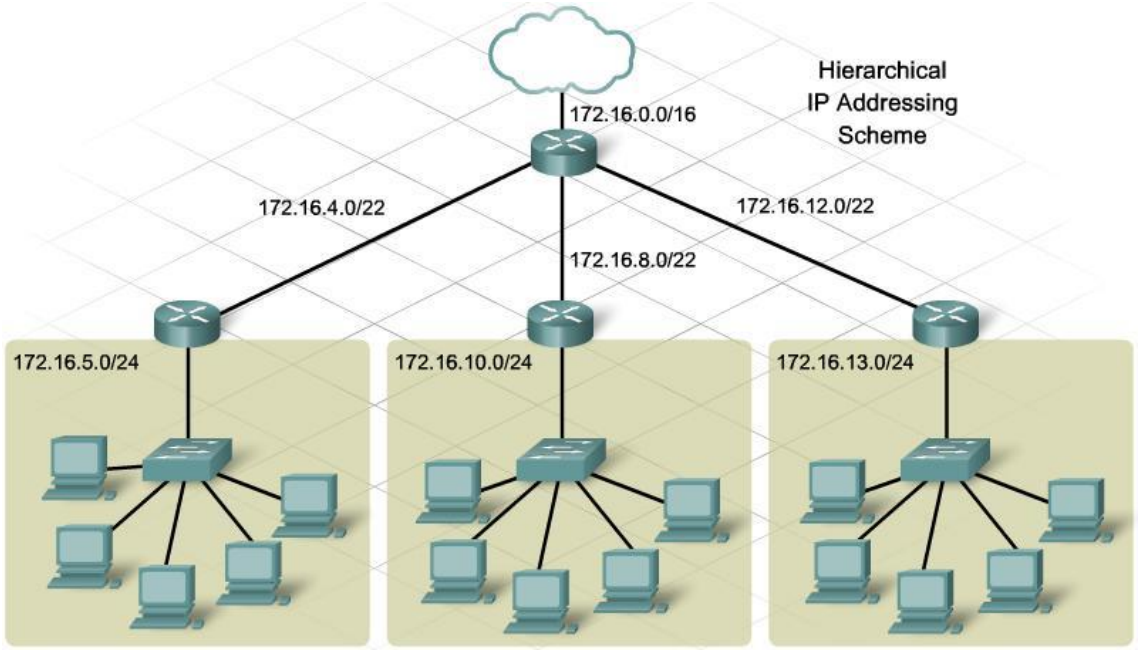
- Network management
- IP telephony
- IP Multicast
- Normal data
- Scavenger class



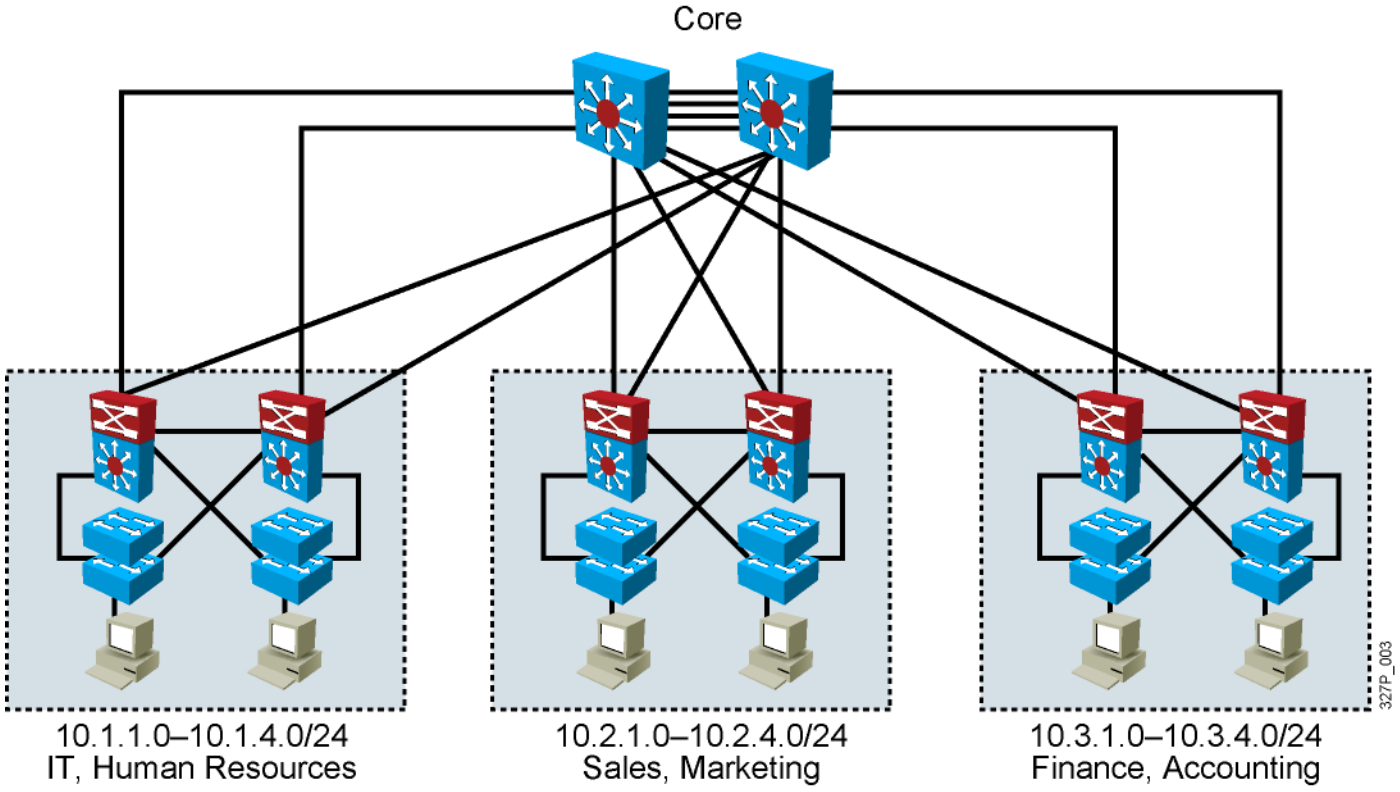
Designing VLANs for an Organization

- **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.

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 vlan-id
SwitchX(config-vlan)# name vlan-name
```

Example:

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

Assigning Switch Ports to a VLAN

```
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport access vlan vlan-id
```

Example:

```
SwitchX# configure terminal
SwitchX(config)# interface fastethernet0/2
SwitchX(config-if)# switchport mode access
SwitchX(config-if)# switchport access vlan 2
```

from to

```
SwitchX(config)# interface range fastethernet 0/3 - 5
SwitchX(config-if-range)# switchport mode access
SwitchX(config-if-range)# switchport access vlan 2
```

Or:

```
SwitchX(config)# interface range fastethernet0/3-5
```

Verifying VLAN Membership

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

```
SwitchX# show vlan brief
VLAN Name                         Status    Ports
---- -------------------          --------- -------------------------------
1    default                      active    Fa0/1, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                            Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    switchlab99                  active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

Verifying VLAN Membership (Cont.)

```
SwitchX# show interfaces interface switchport
```

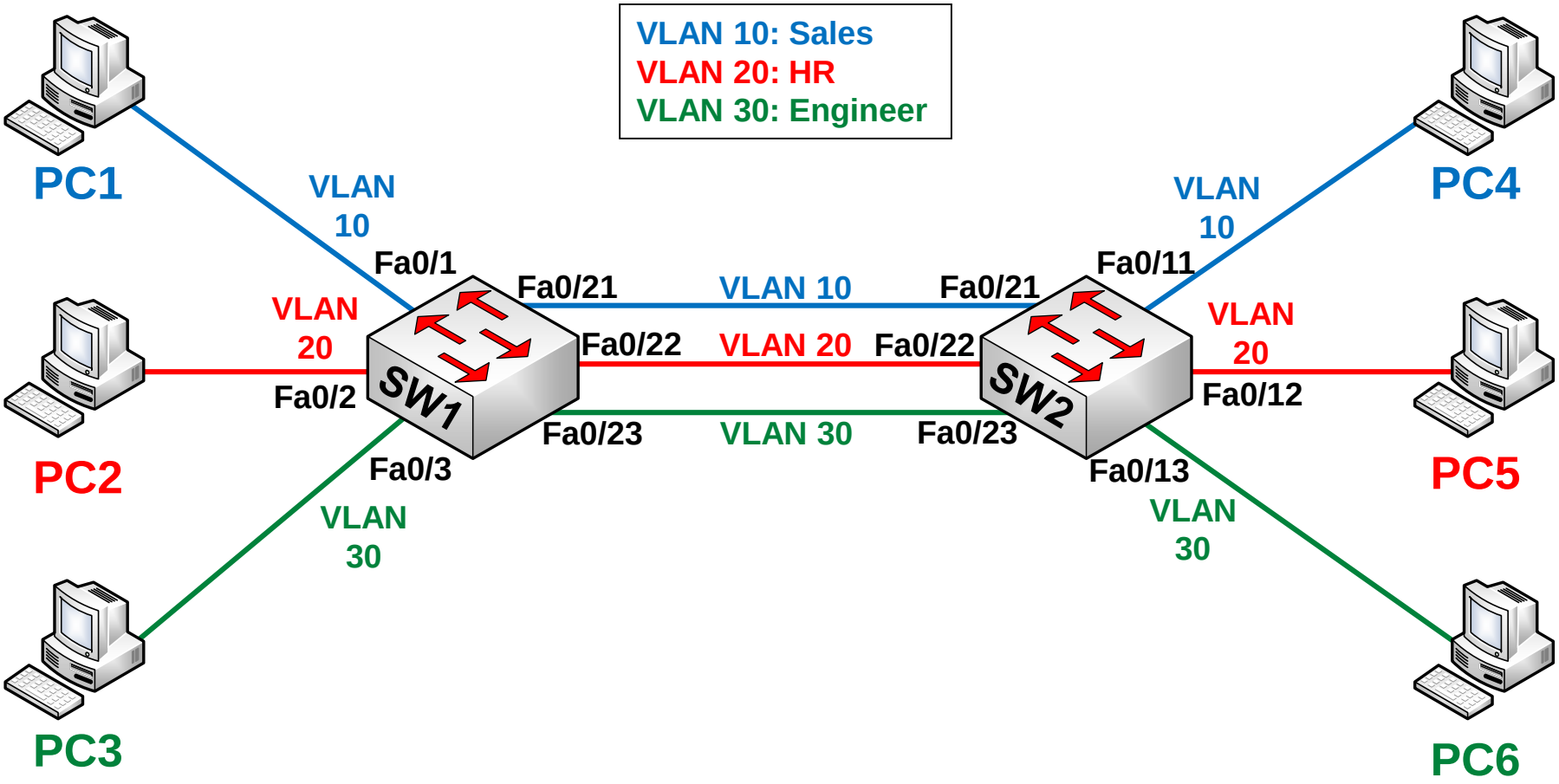
```
SwitchX# show interfaces fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (switchlab99)
Trunking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

Verifying a VLAN

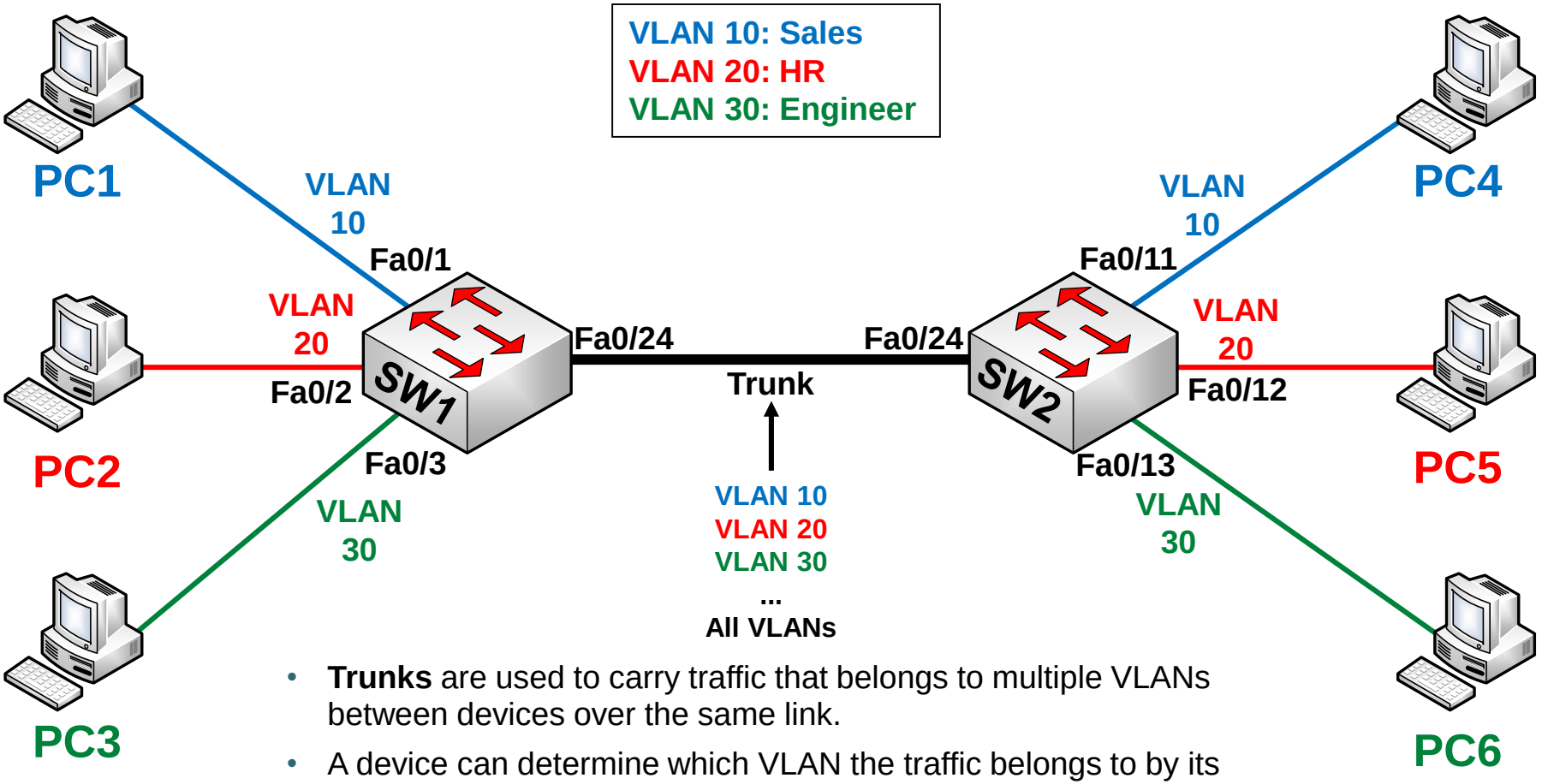
```
SwitchX# show vlan [brief | id vlan-id || name vlan-name]
```

```
SwitchX# show vlan id 2

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------
-----------------
2    switchlab99                         active    Fa0/2, Fa0/3,
Fa0/4, Fa0/5

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

.    .    .
SwitchX#
```

Trunking


VLAN 10: Sales
VLAN 20: HR
VLAN 30: Engineer
PC1
PC2
PC3
PC4
PC5
PC6
SW1
SW2
VLAN 10
VLAN 20
VLAN 30
Fa0/1
Fa0/2
Fa0/3
Fa0/21
Fa0/22
Fa0/23
Fa0/11
Fa0/12
Fa0/13

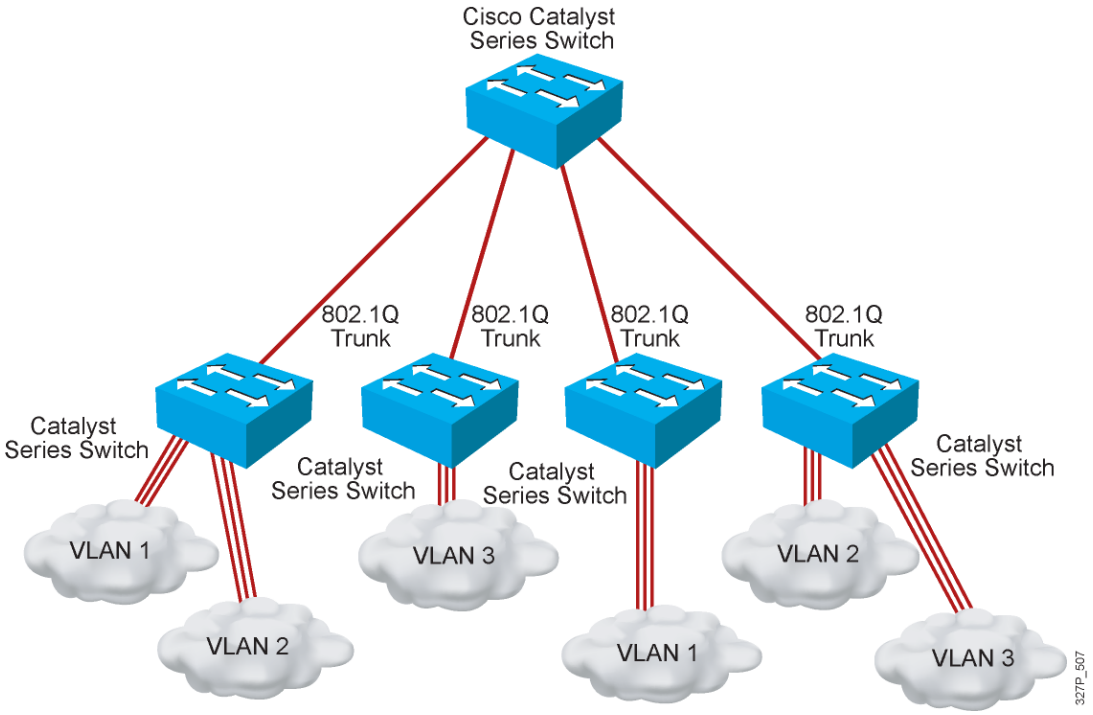
Trunking (Cont.)



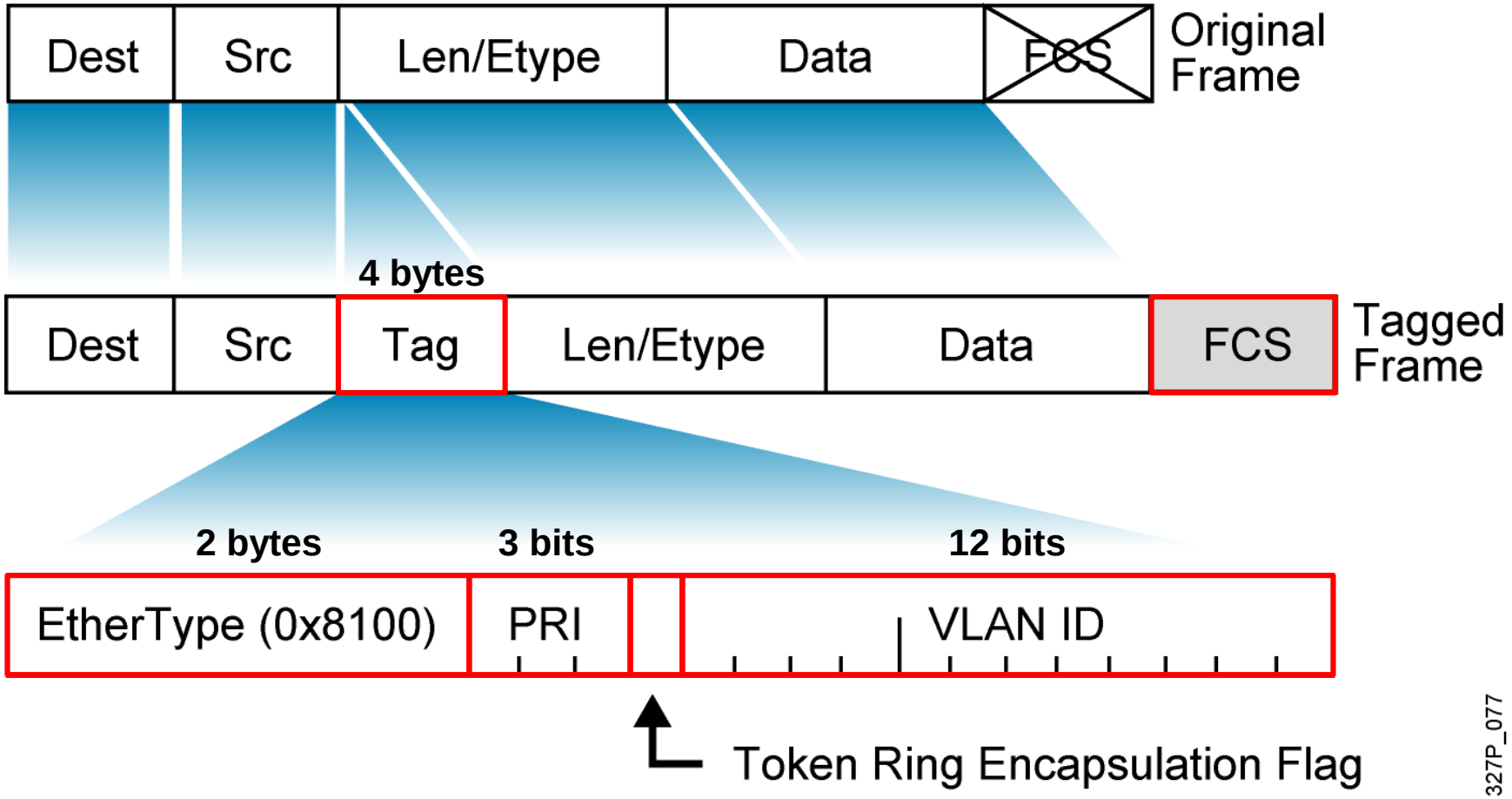
- **Trunks** are used to carry traffic that belongs to multiple VLANs between devices over the same link.
- A device can determine which VLAN the traffic belongs to by its **VLAN identifier**. The **VLAN identifier** is a tag that is encapsulated with the data.

Encapsulation Types

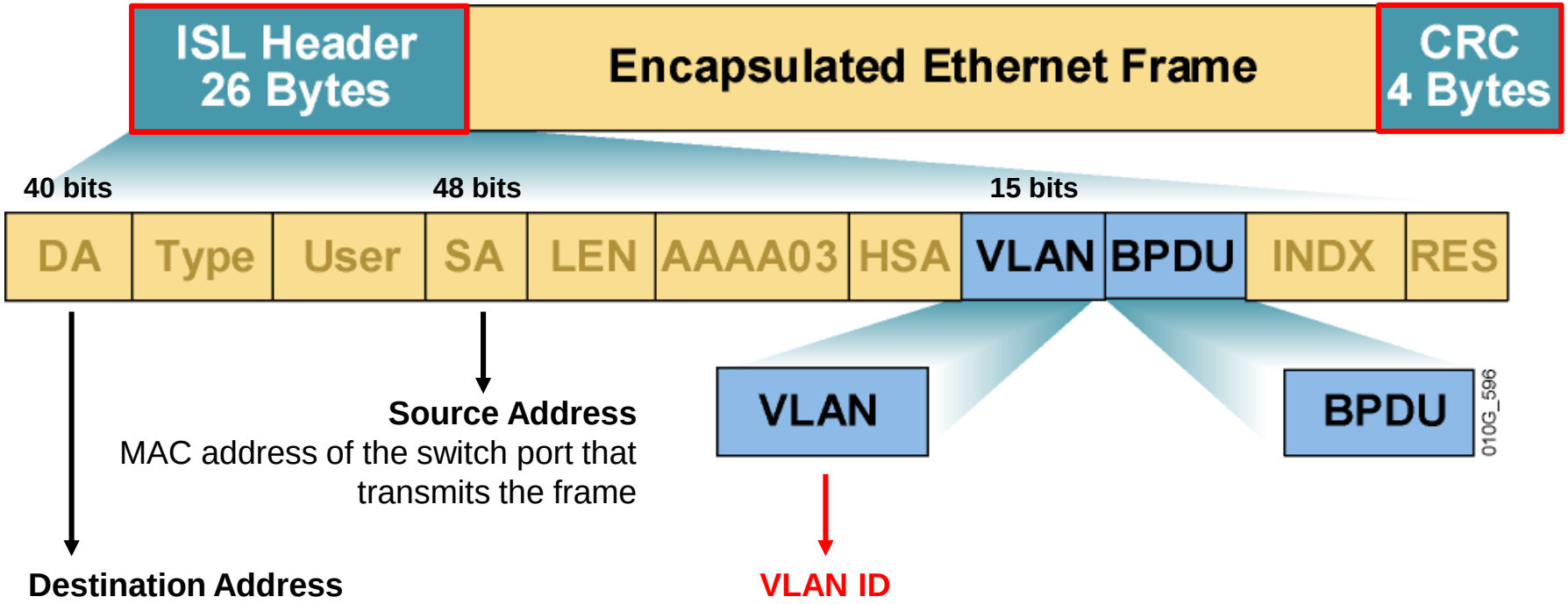
- **802.1Q (dot1Q)** and **ISL (Inter-Switch Link)** are two types of encapsulation that are used to carry data from multiple VLANs over trunk links (VLAN tagging).
  - **802.1Q** is the ***IEEE standard*** for tagging frames on a trunk.
  - **ISL** is a ***Cisco proprietary*** protocol for the interconnection of multiple switches and maintenance of VLAN information as traffic goes between switches.



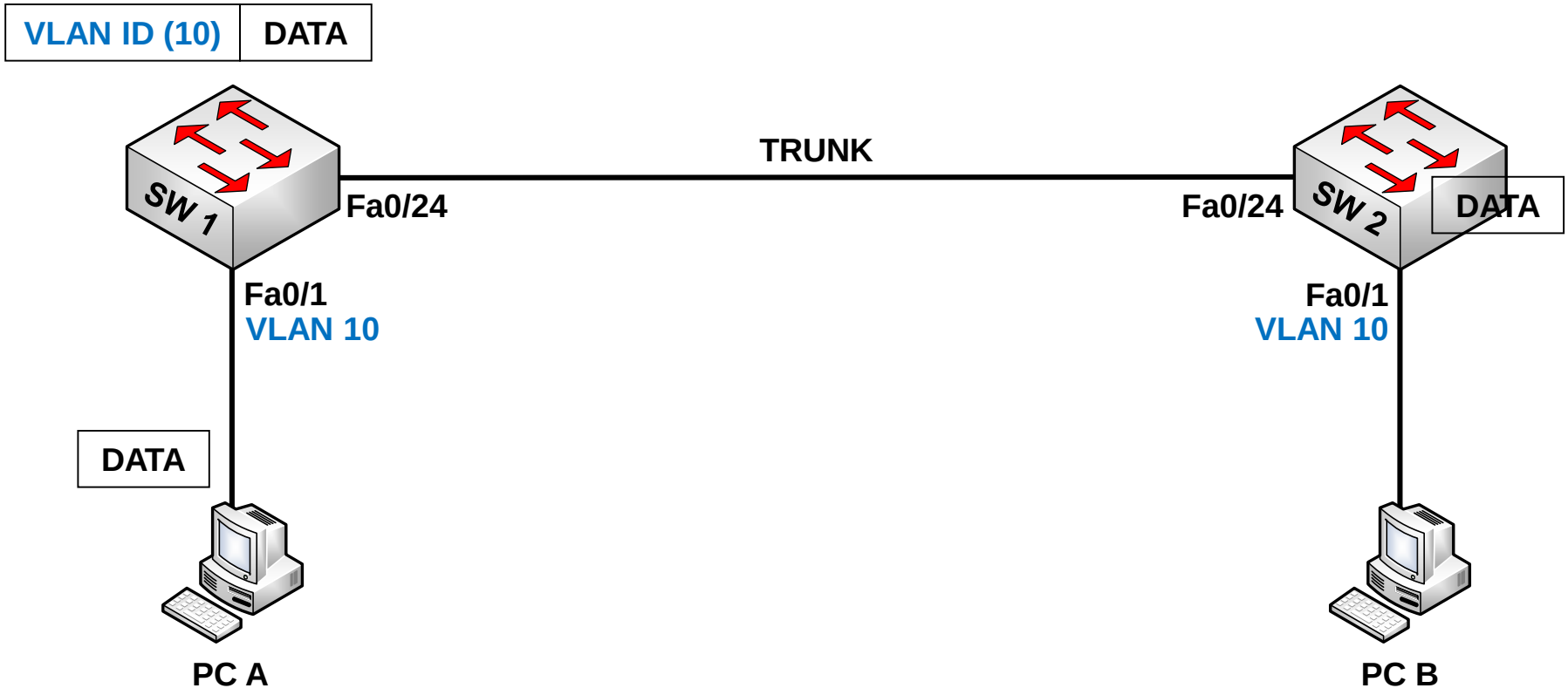
802.1Q Frame


Dest
Src
Len/Etype
Data
FCS
Original Frame
4 bytes
Dest
Src
Tag
Len/Etype
Data
FCS
Tagged Frame
2 bytes
3 bits
12 bits
EtherType (0x8100)
PRI
VLAN ID
Token Ring Encapsulation Flag
327P_077

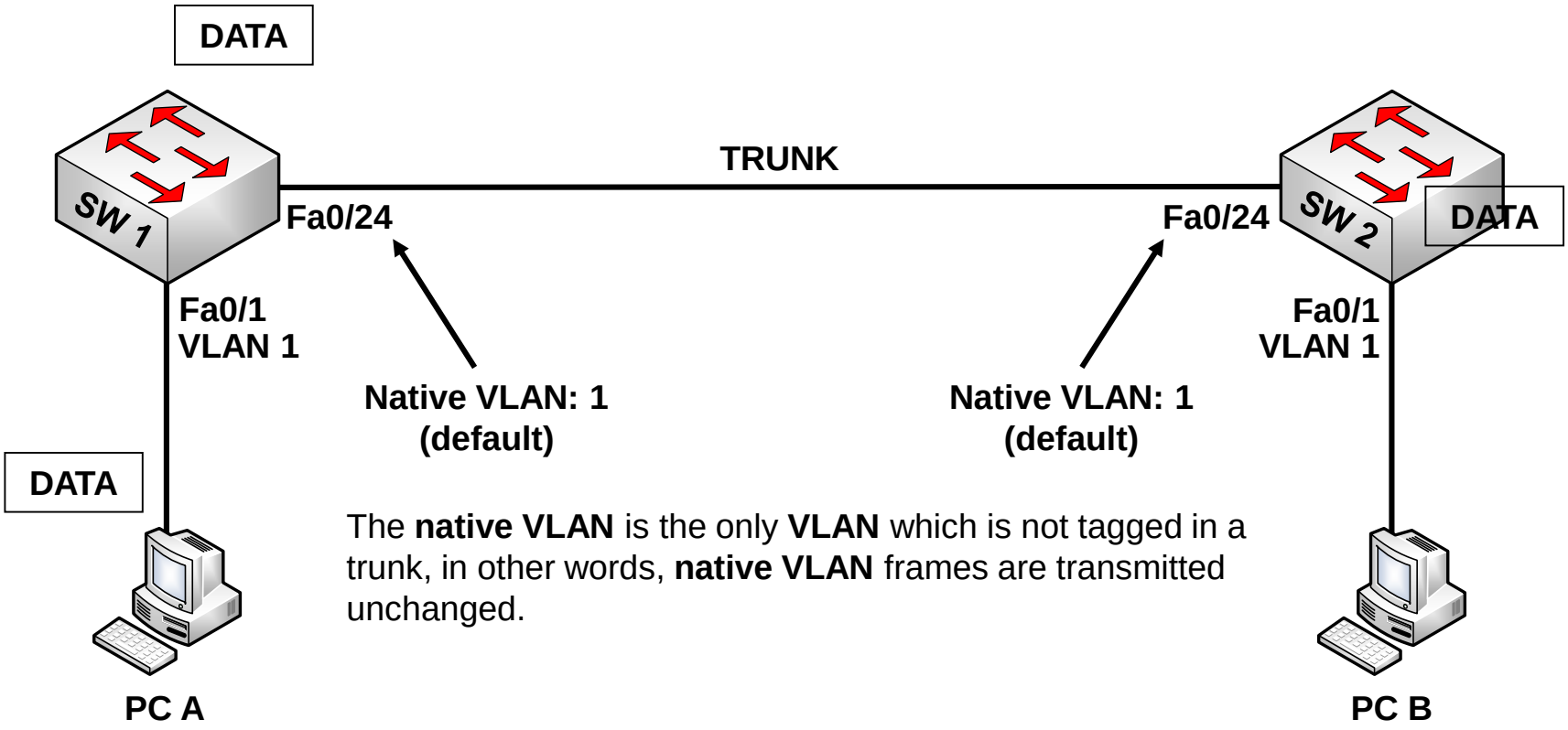
ISL Encapsulation



Understanding Native VLANs

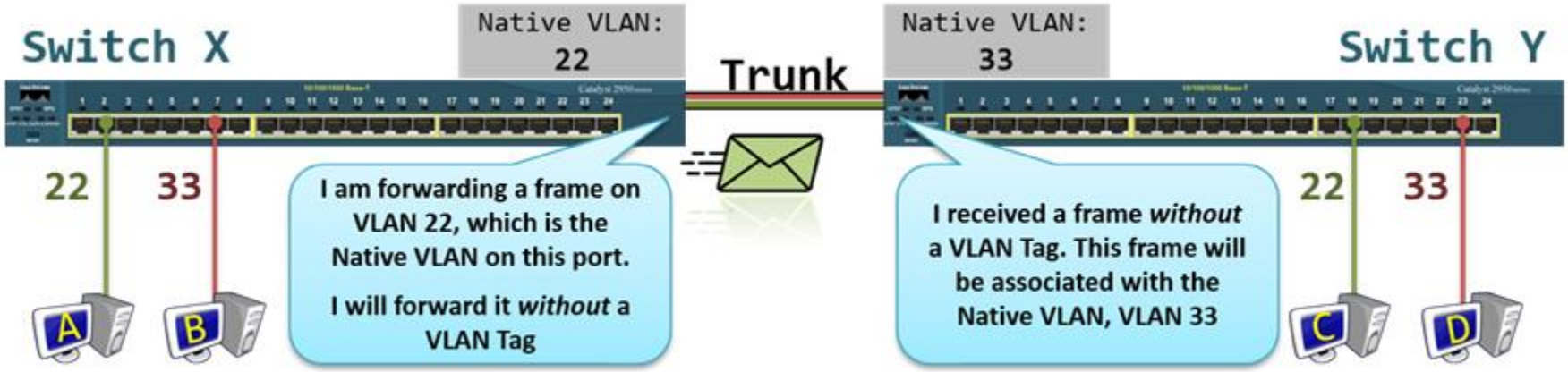


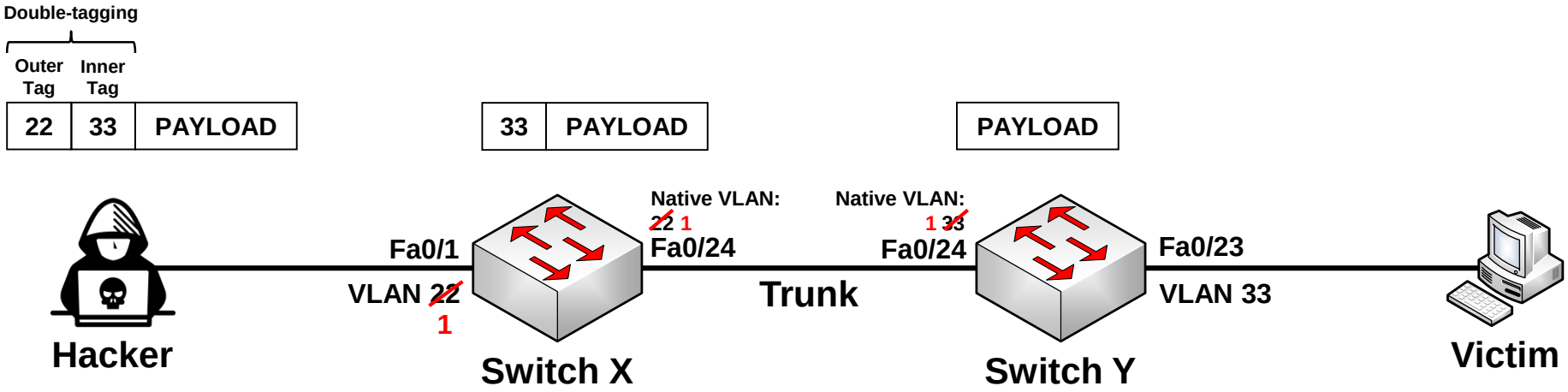
Understanding Native VLANs (Cont.)



The **native VLAN** is the only **VLAN** which is not tagged in a trunk, in other words, **native VLAN** frames are transmitted unchanged.

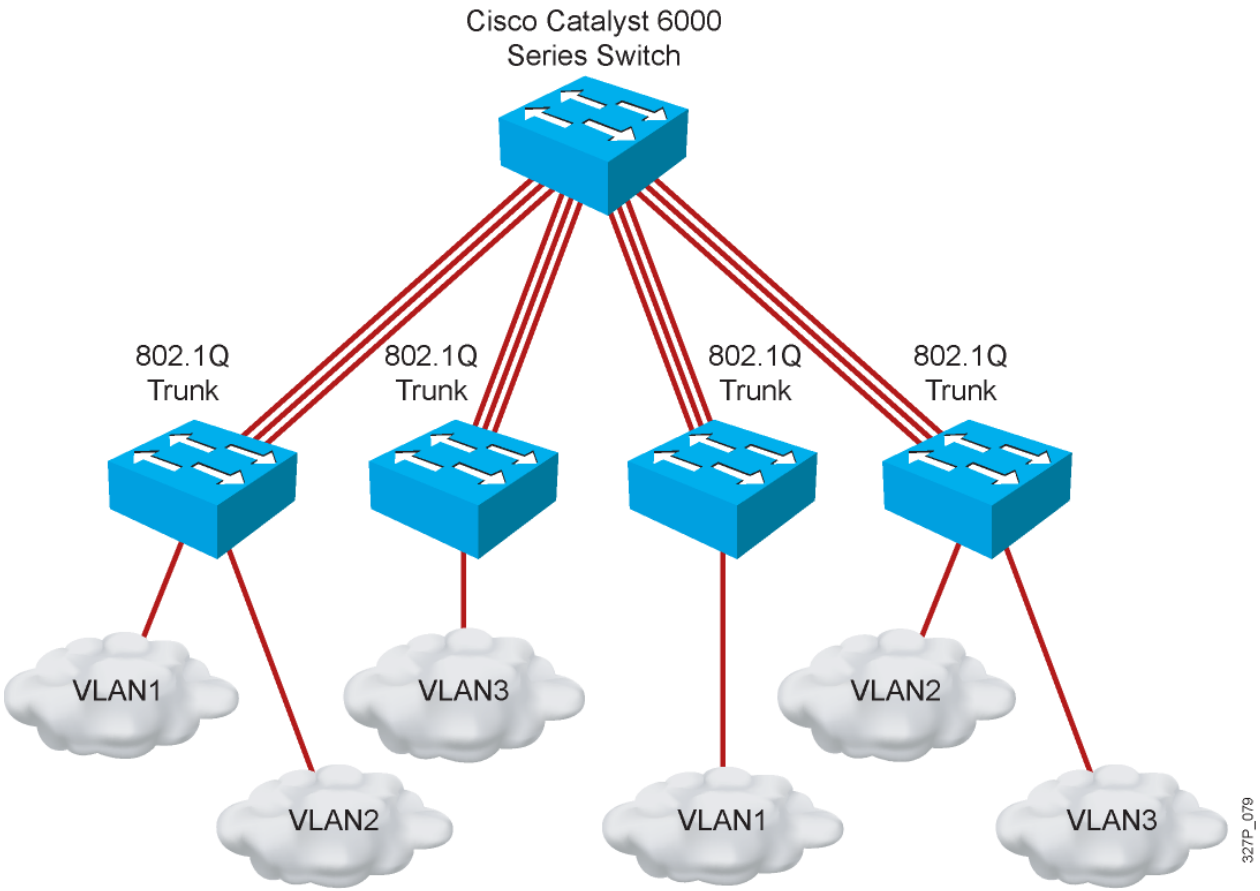
Native VLAN Mismatch





VLAN Hopping

802.1Q Trunking Issues



- 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.

Dynamic Trunking Protocol (DTP)

- The ***Dynamic Trunking Protocol (DTP)*** is used to negotiate forming a trunk between two Cisco devices.
- DTP is a Cisco proprietary protocol. Switches from other vendors do not support DTP.
- DTP causes increased traffic, and is enabled by default, but may be disabled.
- DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP.
- To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk but not generate DTP frames.

Negotiated Interface Modes

- **switchport mode access**: The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.
- **switchport mode dynamic auto**: Makes the interface able to convert the link to a trunk link. The default switchport mode for newer Cisco switch Ethernet interfaces is dynamic auto.
- **switchport mode dynamic desirable**: Makes the interface actively attempt to convert the link to a trunk link. This is the default switchport mode on older switches, such as the Catalyst 2950 and 3550 Series switches.
- **switchport mode trunk**: Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link.
- **switchport nonegotiate**: Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Trunking Modes

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Configuring 802.1Q Trunking

```
SwitchX(config-if)#
```

```
switchport trunk encapsulation {dot1q | isl}
```

- Configures the trunking encapsulation

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

- Configures the trunking characteristics of the port

Example:

```
SwitchX(config)#interface Fa0/24
SwitchX(config-if)#switchport trunk encapsulation dot1q
SwitchX(config-if)#switchport mode trunk
```

Verifying a Trunk

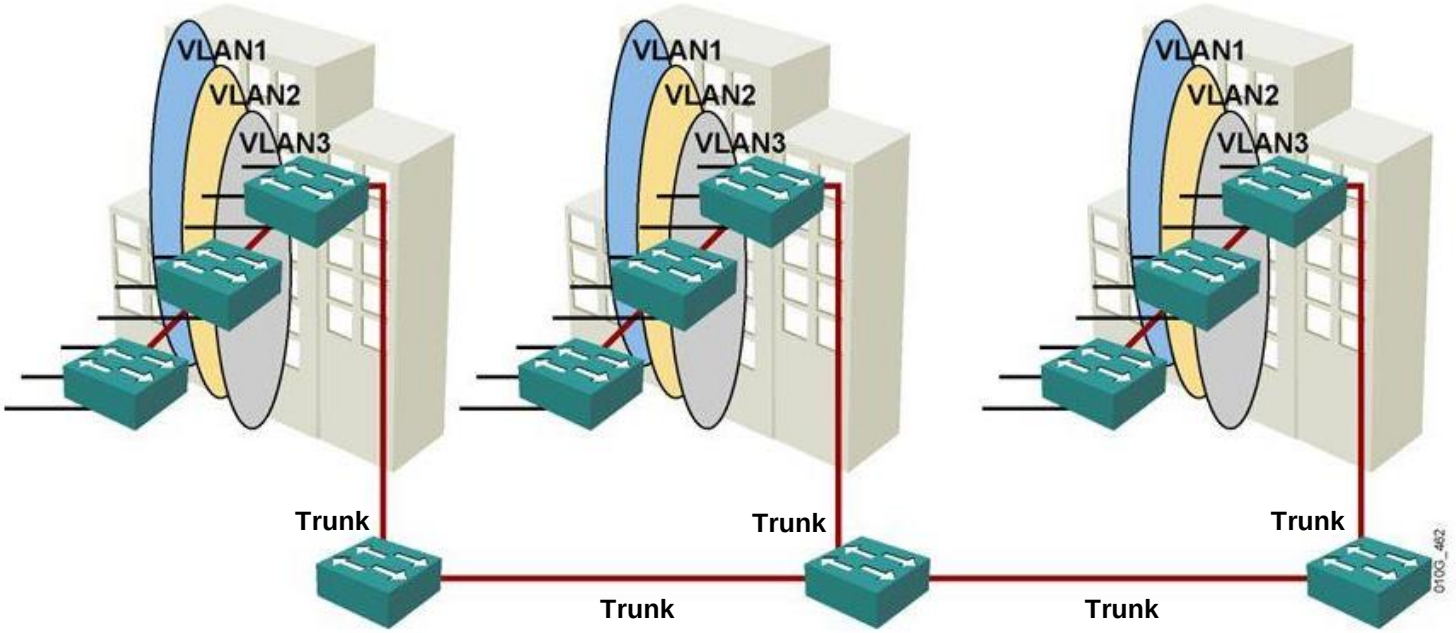
```
SwitchX# show interfaces interface [switchport | trunk]
```

```
SwitchX# show interfaces fa0/24 switchport
Name: Fa0/24
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 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
```

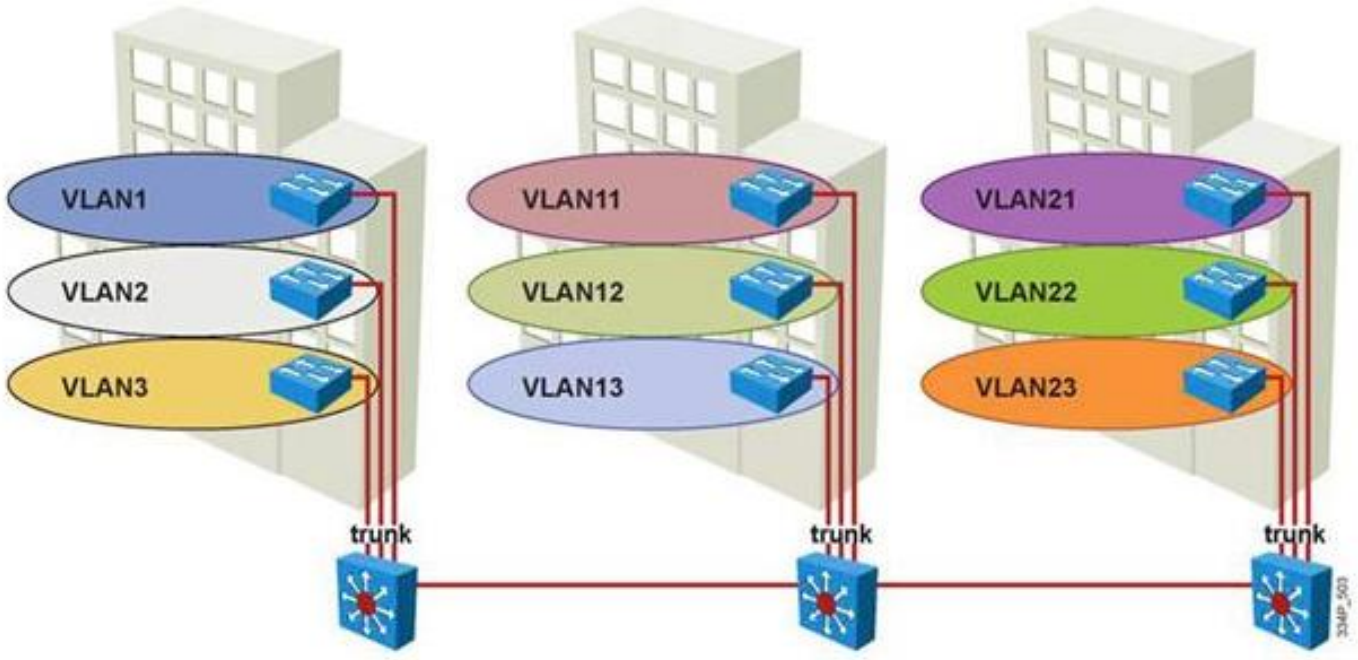
End-to-End VLANs

- Users are grouped into VLANs independent of physical location.
- If users are moved within the campus, their VLAN membership remains the same.



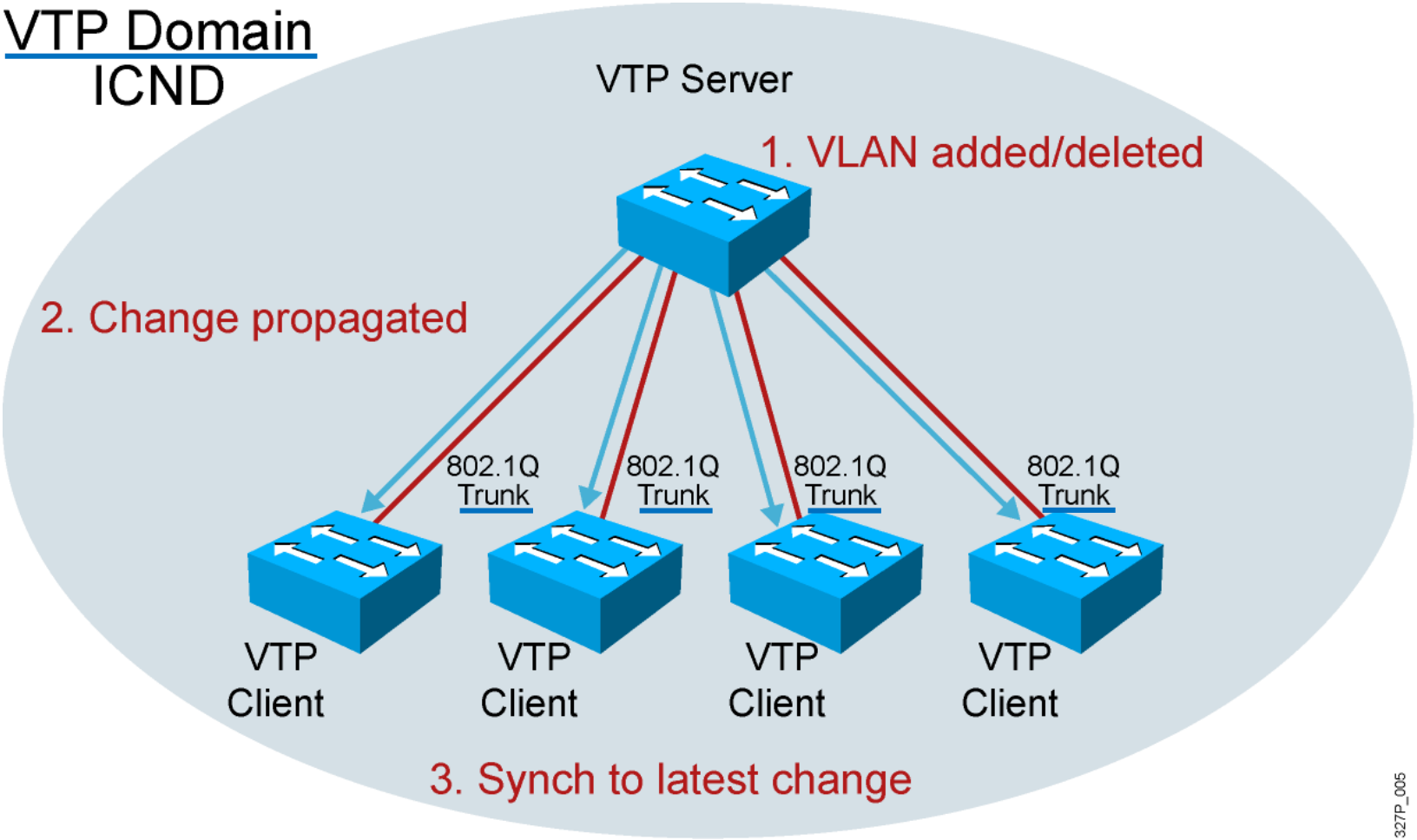
Local VLANs

- Users are grouped into VLANs depending of physical location.
- If users are moved within the campus, their VLAN membership changes.



VTP Features

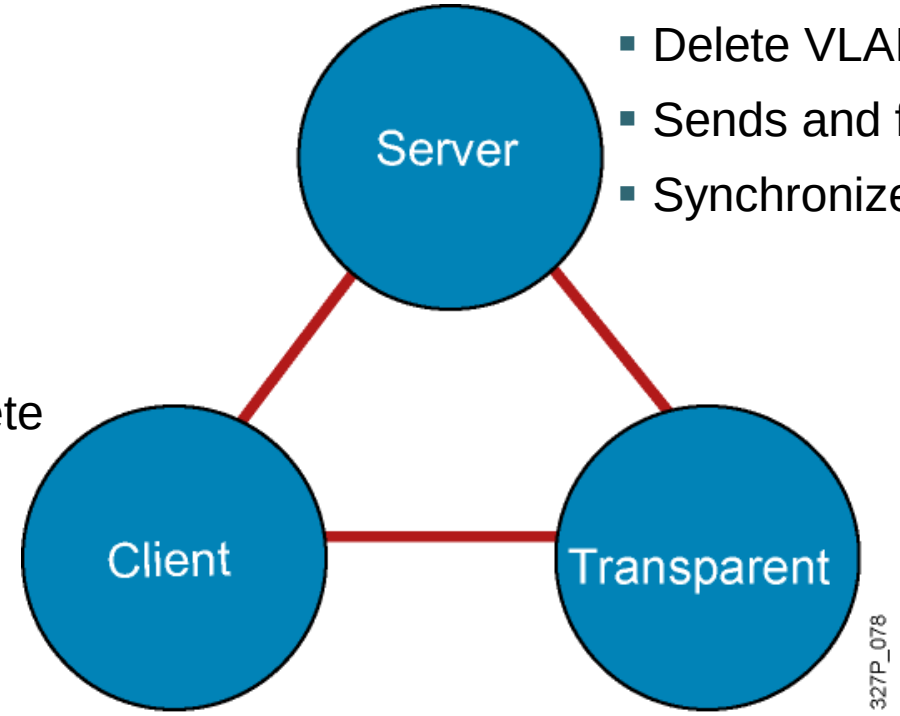
VTP (VLAN Trunking Protocol)



327P_005

VTP Modes

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

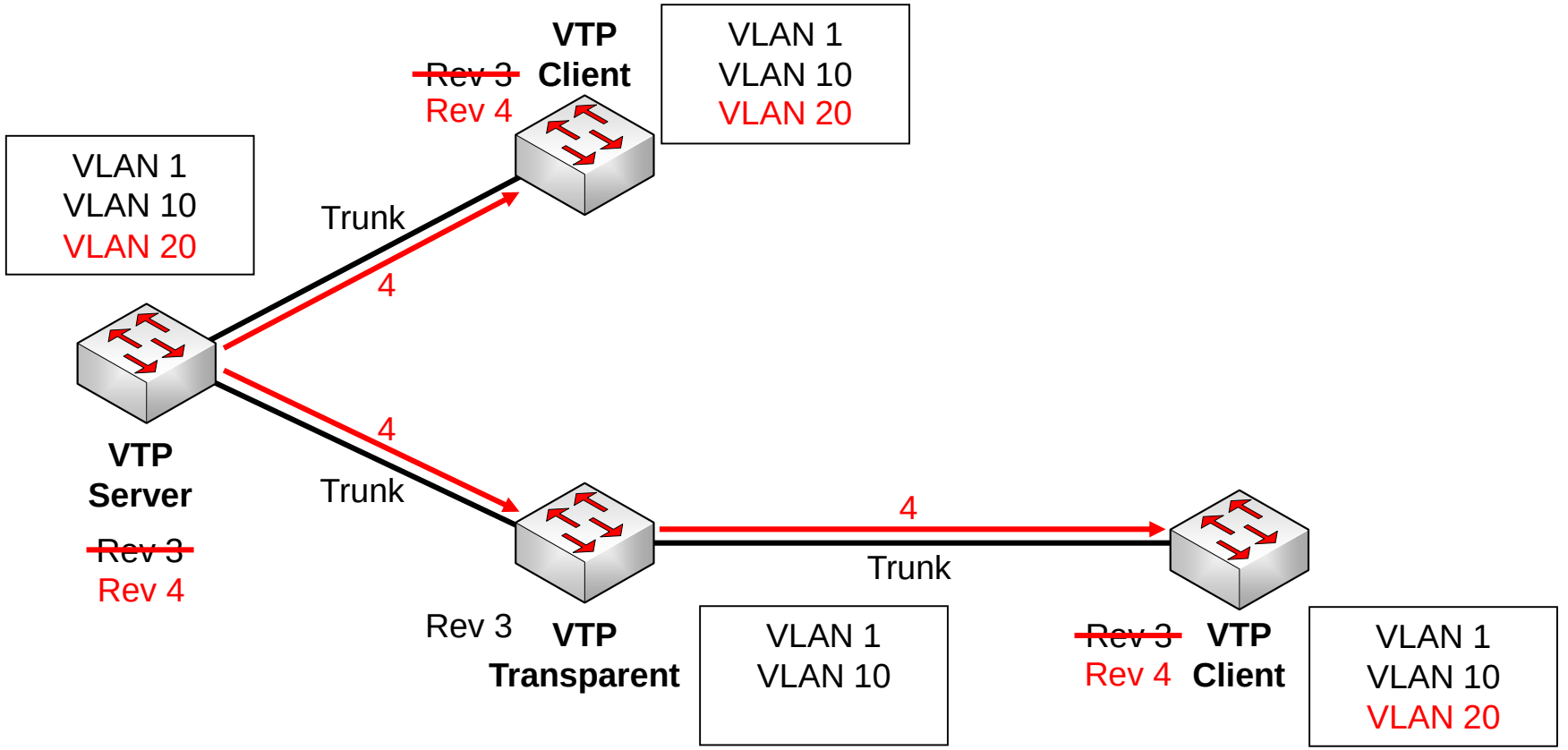


- Cannot create, change, or delete VLANs
- Sends and forwards advertisements
- Synchronizes

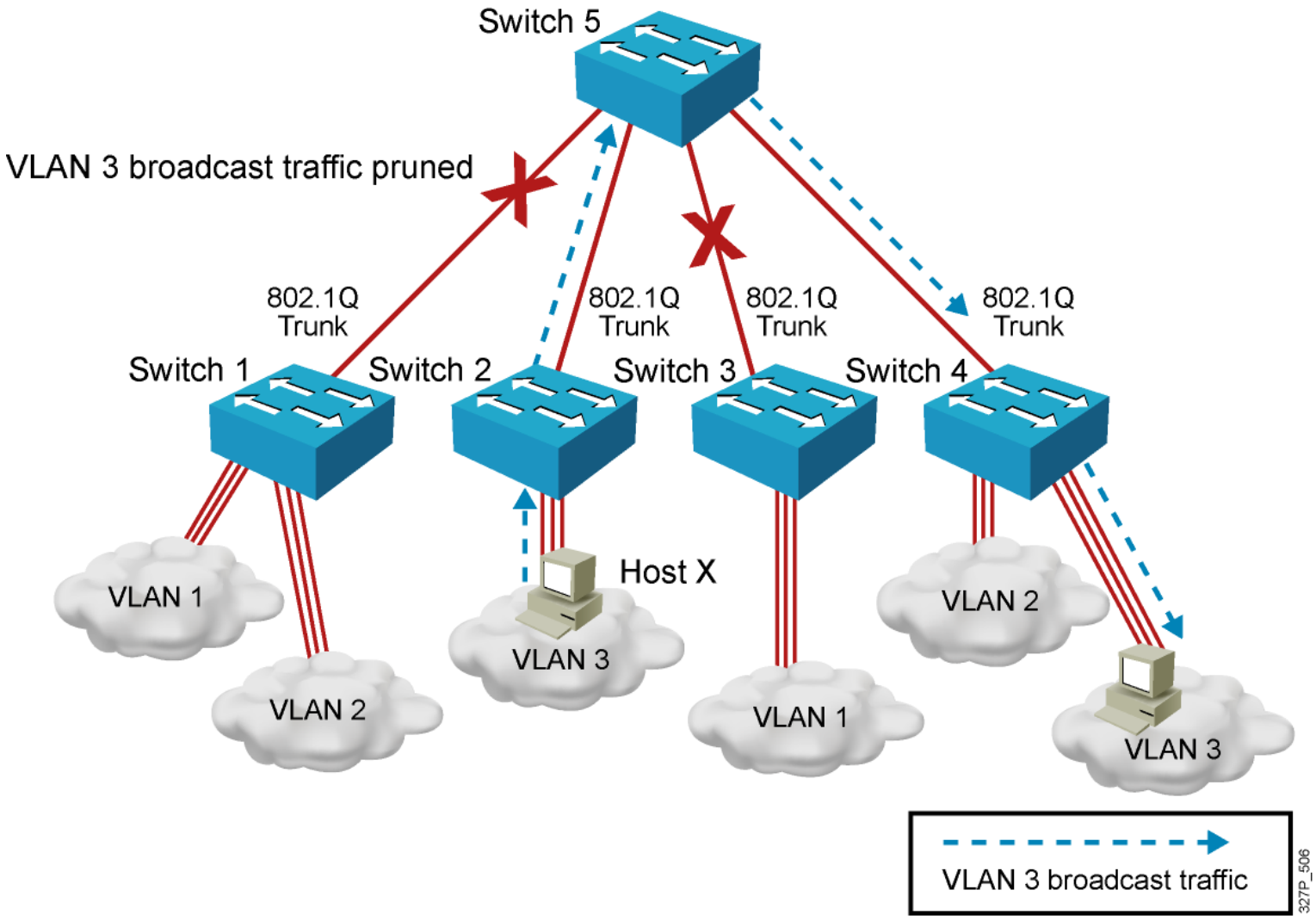
- Create local VLANs only
- Modify local VLANs only
- Delete local VLANs only
- Forwards advertisements
- Does not synchronize

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


Switch 5
VLAN 3 broadcast traffic pruned
802.1Q Trunk
802.1Q Trunk
802.1Q Trunk
802.1Q Trunk
Switch 1
Switch 2
Switch 3
Switch 4
VLAN 1
VLAN 2
Host X
VLAN 3
VLAN 1
VLAN 2
VLAN 3
VLAN 3 broadcast traffic
327P_506

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#
```

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.


CISCO