Chapter 3: Campus Network Architecture

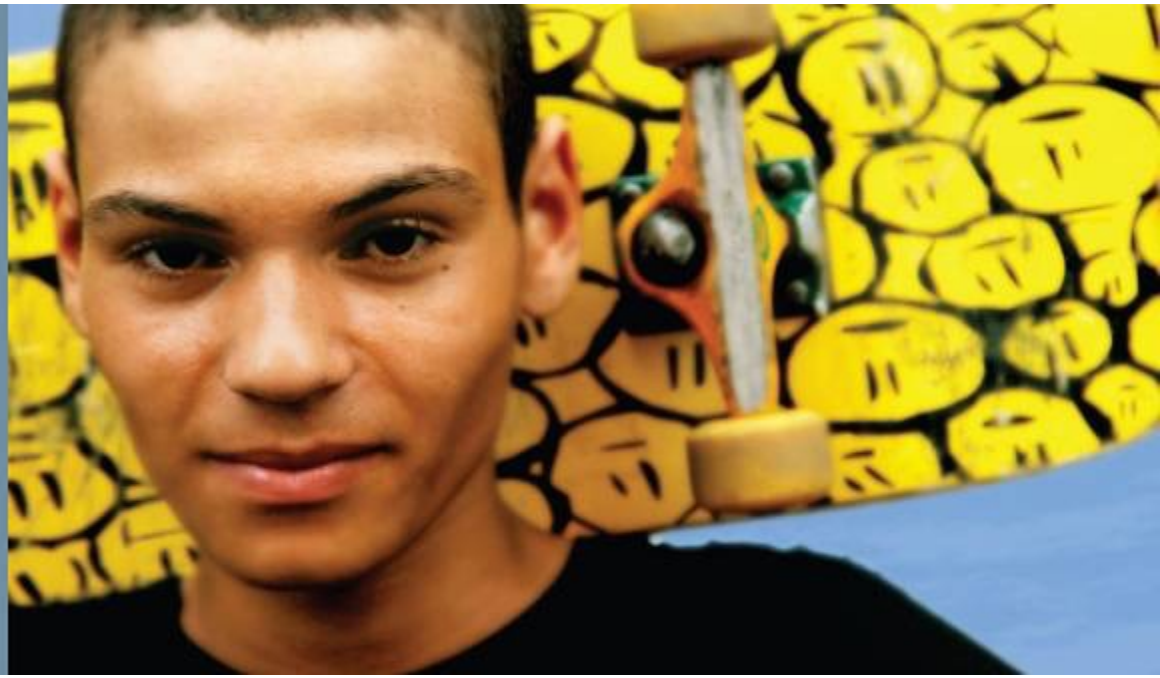
CCNP SWITCH: Implementing Cisco IP Switched Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3 Objectives

- Implementing VLANs and trunks in campus switched architecture
- Private VLANs
- Understanding the concept of VTP and its limitation and configurations
- Implementing and configuring EtherChannel

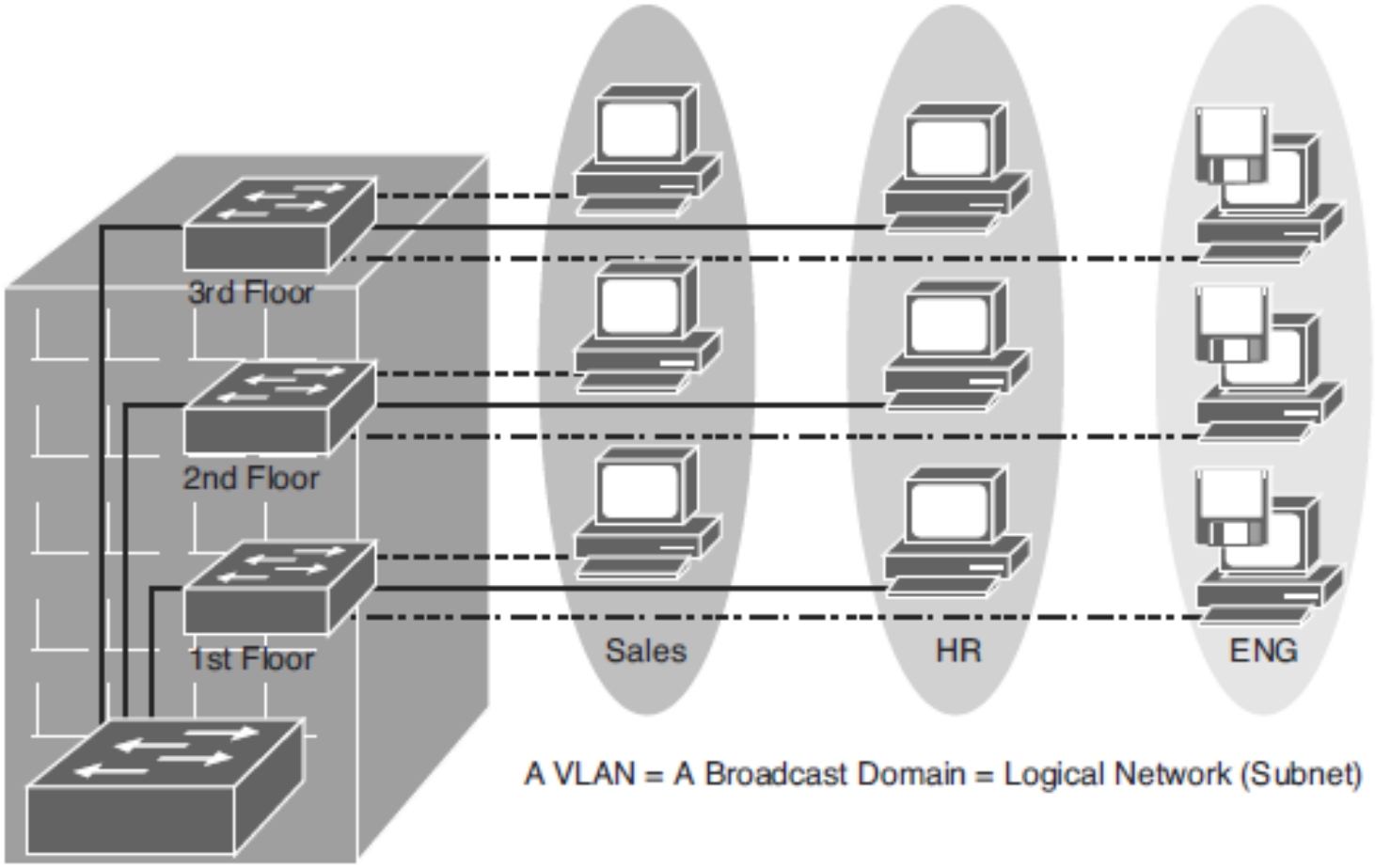
Implementing VLANs and Trunks in Campus Environment



Implementing VLANs and Trunks in Campus Environment

- Within the switched internetwork, VLANs provide segmentation and organizational flexibility.
- VLANs help administrators to have the end node or workstations group that are segmented logically by functions, project teams, and applications, without regard to the physical location of the users.
- VLANs allow you to implement access and security policies to particular groups of users and limit the broadcast domain.
- The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS).

VLAN Overview



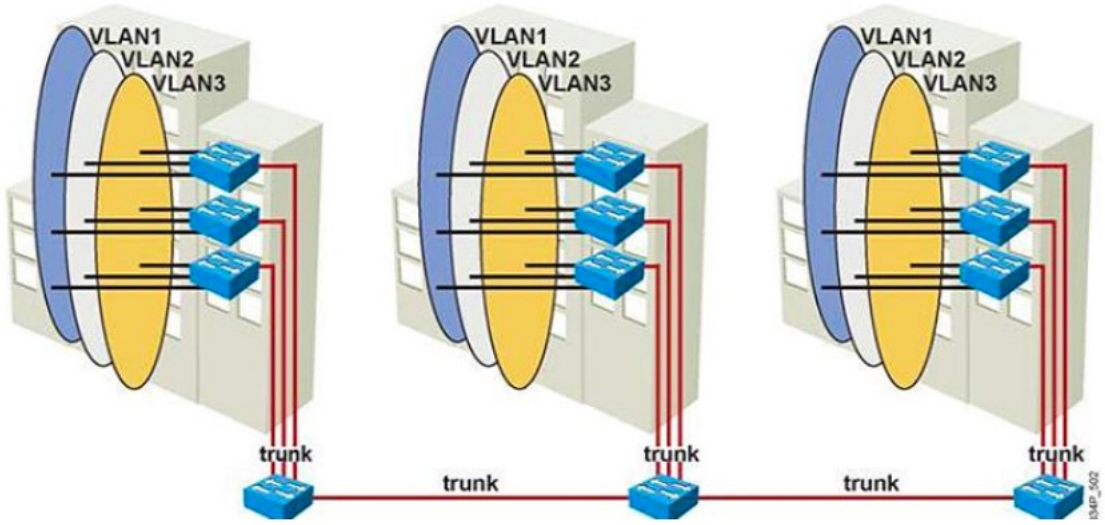
A VLAN = A Broadcast Domain = Logical Network (Subnet)

VLAN Segmentation

- Larger flat networks generally consist of many end devices in which broadcasts and unknown unicast packets are flooded on all ports in the network.
- One advantage of using VLANs is the capability to segment the Layer 2 broadcast domain. All devices in a VLAN are members of the same broadcast domain. If an end device transmits a Layer 2 broadcast, all other members of the VLAN receive the broadcast.
- Switches filter the broadcast from all the ports or devices that are not part of the same VLAN.
- In a campus design, a network administrator can design a campus network with one of two models:
  - **End-to-End VLANs**
  - **Local VLANs**.
- Each model has its own advantages and disadvantages.

End-to-End VLANs

- *End-to-End VLAN* refers to a single VLAN that is associated with switch ports widely dispersed throughout an enterprise network on multiple switches.
- pôvodný koncept - pravidlo 80/20
- VLAN sa rozprestiera po celej sieti naprieč A-D-C
- VLAN boli vytvorené na báze pracovných skupín

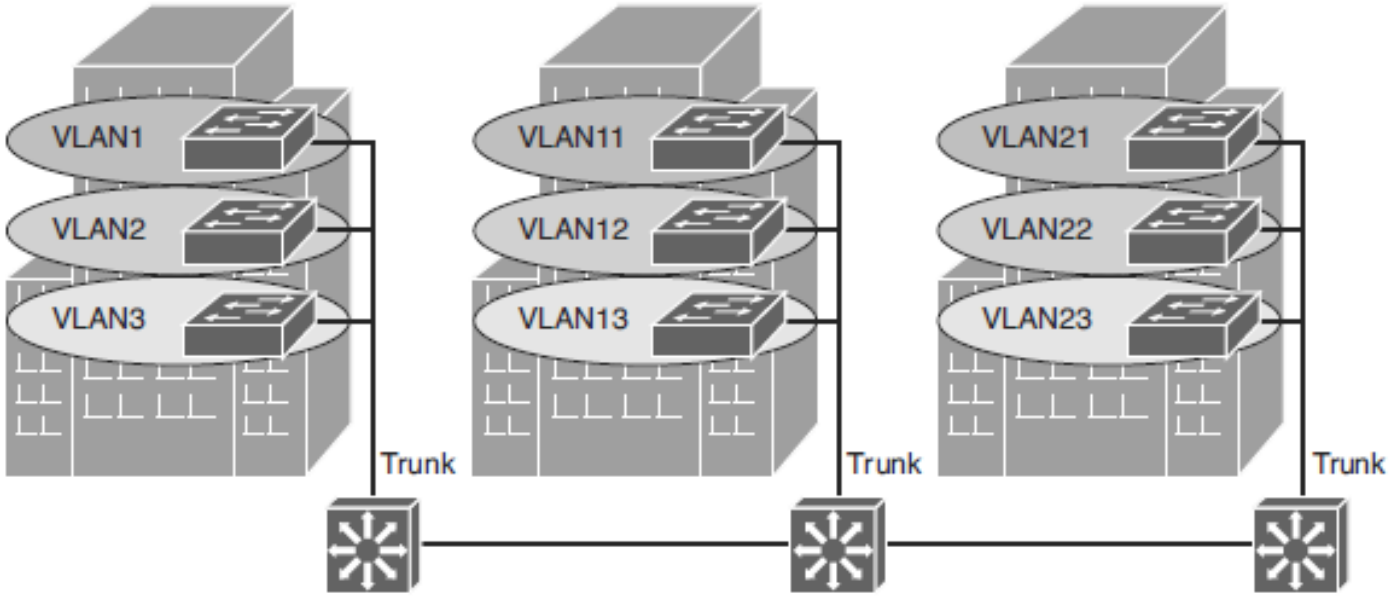


End-to-End VLAN Model Characteristics

- Each VLAN is dispersed geographically throughout the network.
- Users are grouped into each VLAN regardless of the physical location.
- As a user moves throughout a campus, the VLAN membership of that user remains the same, regardless of the physical switch to which this user attaches.
- Users are typically associated with a given VLAN for network management reasons. This is why they are kept in the same VLAN, therefore the same group, as they move through the campus.
- All devices on a given VLAN typically have addresses on the same IP subnet.
- Switches commonly operate in a server/client VTP mode.

Local VLANs

- In a local VLAN model, all users of a set of geographically common switches are grouped into a single VLAN, regardless of the organizational function of those users.
- odráža pravidlo 80/20
- D prepínač zabezpečuje smerovaním prístup medzi VLAN



Local VLAN Model Characteristics

- The network administrator should create local VLANs with physical boundaries in mind rather than the job functions of the users on the end devices.
- Generally, local VLANs exist between the ACC and DIS levels.
- Traffic from a local VLAN is routed at the distribution and core levels to reach destinations on other networks.
- Configure the VTP mode in transparent mode because VLANs on a given access switch should not be advertised to all other switches in the network, nor do they need to be manually created in any other switch VLAN databases.
- A network that consists entirely of local VLANs can benefit from increased convergence times offered via routing protocols, instead of a spanning tree for Layer 2 networks.
- It is usually recommended to have 1 to 3 VLANs per ACC layer switch.

Comparison of End-to-End VLANs and Local VLANs

Reasons for implementing the **end-to-end** design:

- **Grouping users**
  - Users can be grouped on a common IP segment, even though they are geographically dispersed.
- **Security**
  - A VLAN can contain resources that should not be accessible to all users on the network, or there might be a reason to confine certain traffic to a particular VLAN.
- **Applying quality of service (QoS)**
  - Traffic can be a higher- or lower-access priority to network resources from a given VLAN.

Comparison of End-to-End VLANs and Local VLANs

Reasons for implementing the **end-to-end** design (cont.):

- **Routing avoidance**
  - If much of the VLAN user traffic is destined for devices on that same VLAN.
- **Special-purpose VLAN**
  - Sometimes a VLAN is provisioned to carry a single type of traffic that must be dispersed throughout the campus (for example, multicast, voice, or visitor VLANs).
- **Poor design**
  - For no clear purpose, users are placed in VLANs that span the campus or even span WANs. Sometimes when a network is already configured and running, organizations are hesitant to improve the design because of downtime or other political reasons.

Comparison of End-to-End VLANs and Local VLANs

- Reasons for implementing the **Local Vlan** design:
- **Deterministic traffic flow**
  - The simple layout provides a predictable Layer 2 and Layer 3 traffic path.
- **Active redundant paths**
  - When implementing Per-VLAN Spanning Tree (PVST) or Multiple Spanning Tree (MST) because there is no loop, all links can be used to make use of the redundant paths.
- **High availability (HA)**
  - Redundant paths exist at all infrastructure levels.
- **Finite failure domain**
  - If VLANs are local to a switch block, and the number of devices on each VLAN is kept small, failures at Layer 2 are confined to a small subset of users.
- **Scalable design**
  - Following the enterprise campus architecture design, new access switches can be easily incorporated, and new submodules can be added when necessary.

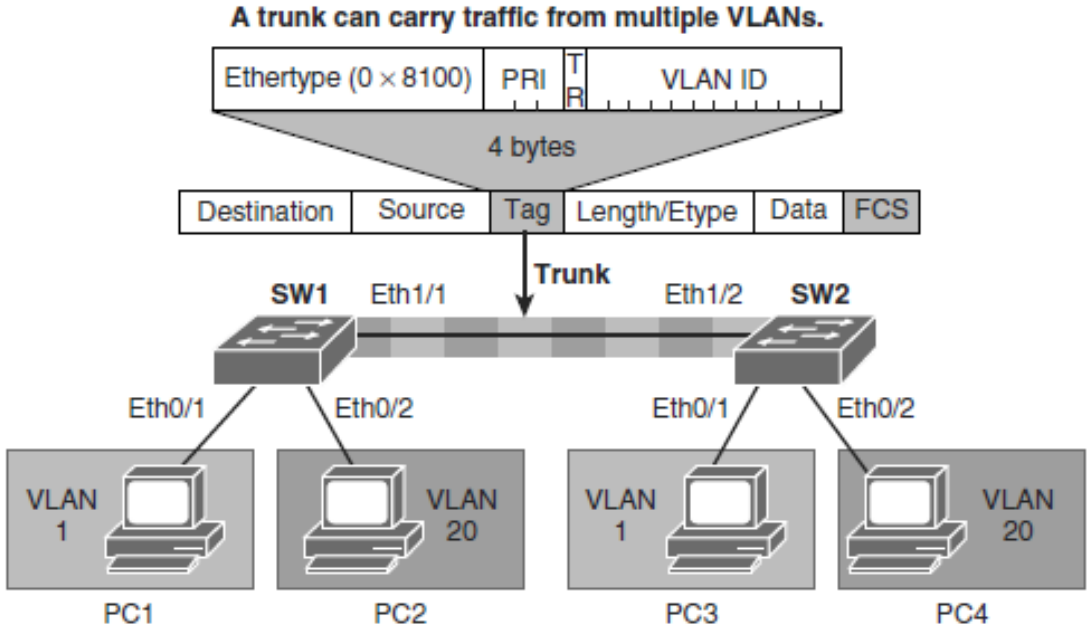
Comparison of End-to-End VLANs and Local VLANs

End-to-End VLANs drawbacks:

- Switch ports are provisioned for each user and associated with a given VLAN. Because users on an end-to-end VLAN can be anywhere in the network, all switches must be aware of that VLAN. This means that all switches carrying traffic for end-to-end VLANs are required to have those specific VLANs defined in each switch's VLAN database.
- Flooded traffic for the VLAN is, by default, passed to every switch even if it does not currently have any active ports in the particular end-to-end VLAN.
- Troubleshooting devices on a campus with end-to-end VLANs can be challenging because the traffic for a single VLAN can traverse multiple switches in a large area of the campus, and that can easily cause potential spanning-tree problems.

Implementing a Trunk in a Campus Environment

- A trunk is a point-to-point link that carries the traffic for multiple VLANs across a single physical link between the two switches or any two devices.
- Trunking is used to extend Layer 2 operations across an entire network.



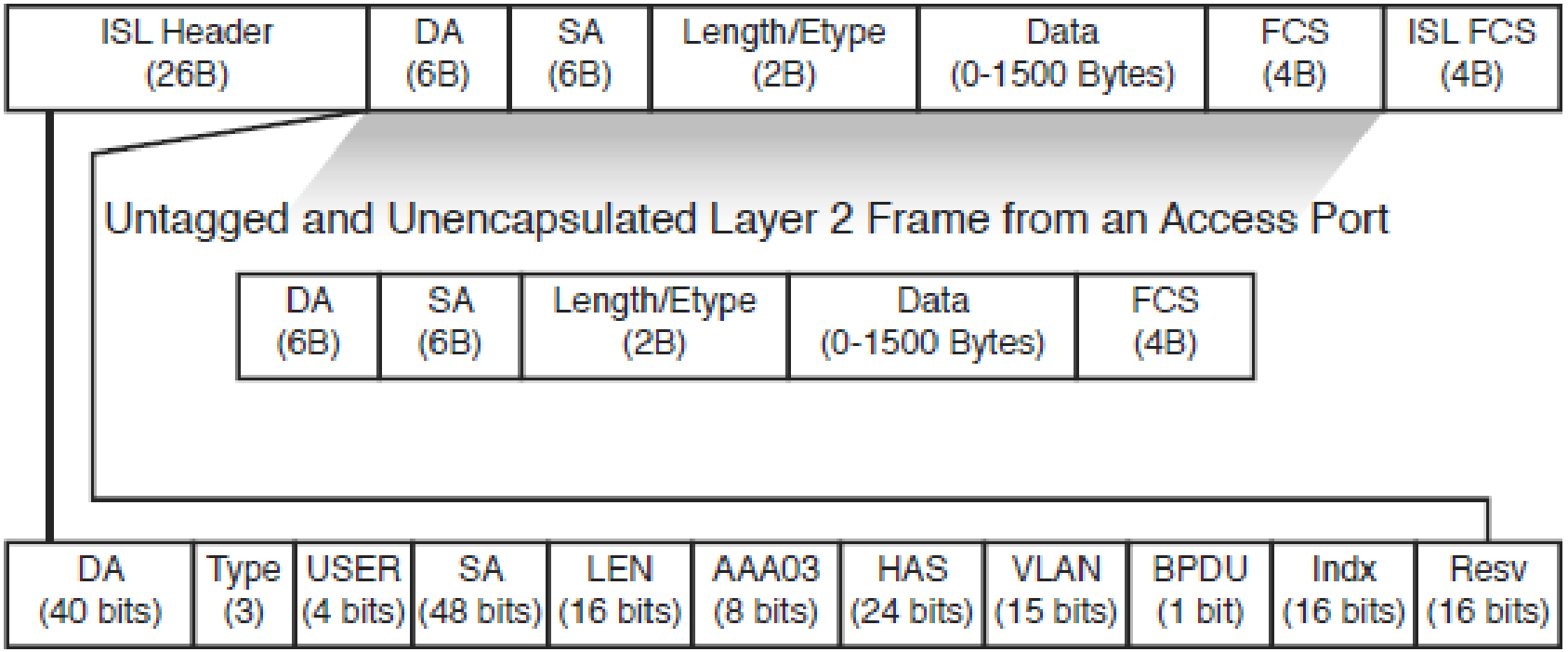
Trunking Protocols

- A special protocol is used to carry multiple VLANs over a single link between two devices.

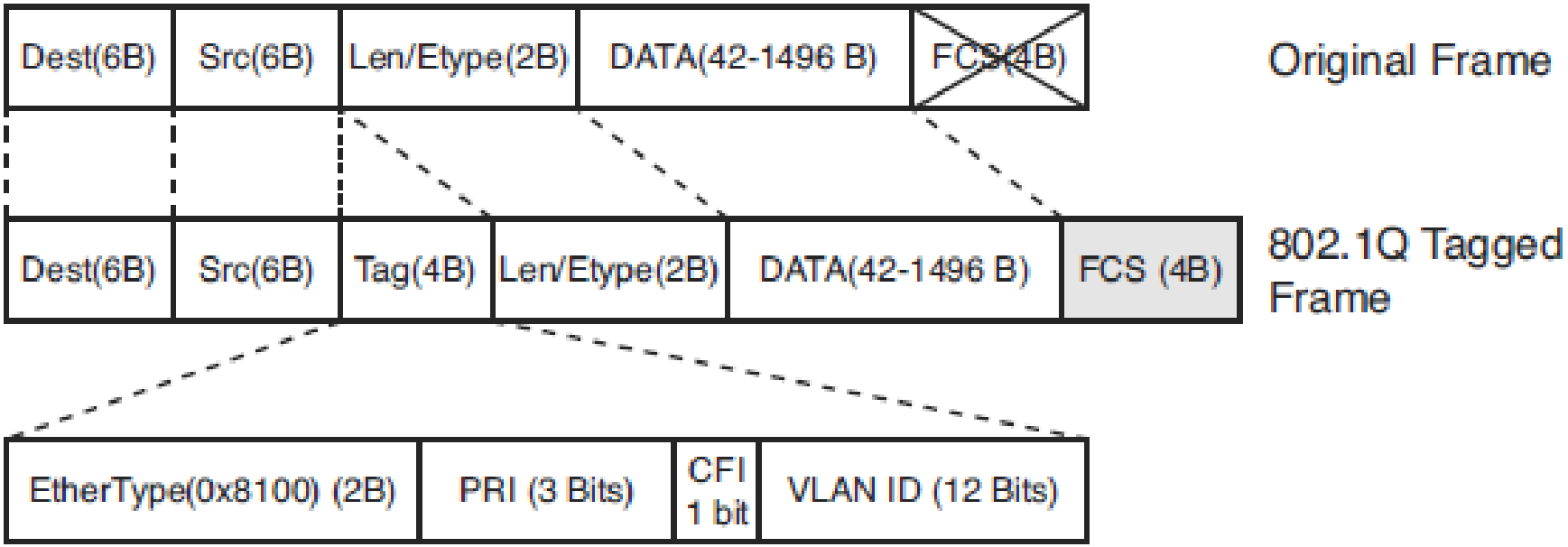
There are two trunking technologies:

- **Inter-Switch Link (ISL):** A Cisco proprietary trunking encapsulation
- **IEEE 802.1Q:** An industry-standard trunking method

ISL Frame



802.1Q Frame



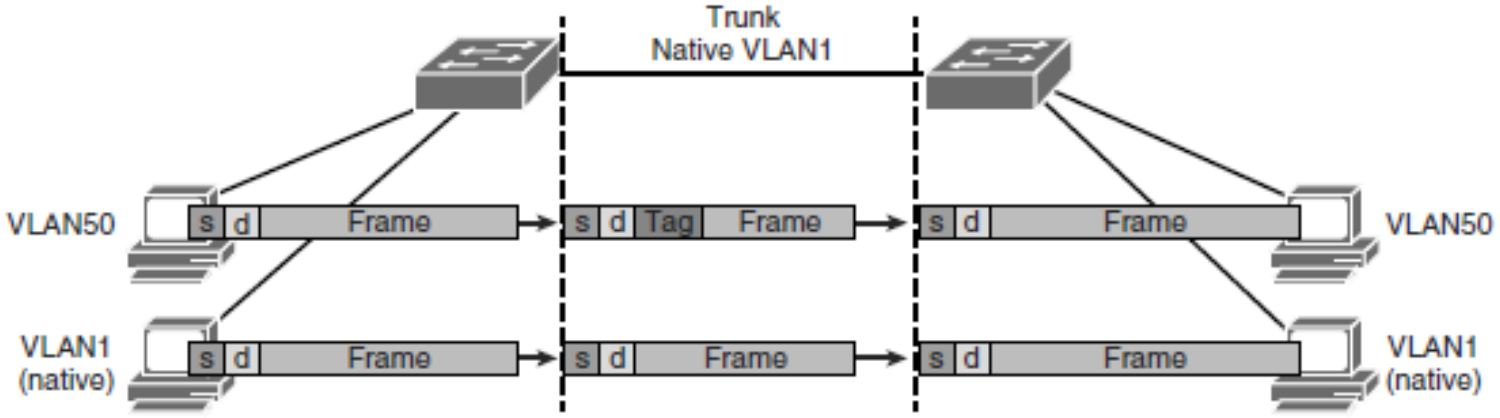
IEEE 802.1Q/802.1p advantages over ISL

- 802.1Q has smaller frame overhead than ISL. As a result, 802.1Q is more efficient than ISL, especially in the case of small frames. 802.1Q overhead is 4 bytes, whereas ISL is 30 bytes.
- 802.1Q is a widely supported industry standard protocol.
- 802.1Q has the support for 802.1p fields for QoS.

802.1Q tag

- Inserted 802.1Q tag (4 bytes, detailed here)
  - **EtherType(TPID):** Set to 0x8100 to specify that the 802.1Q tag follows.
  - **PRI:** 3-bit 802.1p priority field.
  - **CFI:** Canonical Format Identifier is always set to 0 for Ethernet switches and to 1 for Token Ring-type networks.
  - **VLAN ID:** 12-bit VLAN field. Of the 4096 possible VLAN IDs, the maximum number of possible VLAN configurations is 4094. A VLAN ID of 0 indicates priority frames, and value 4095 (FFF) is reserved.
  - If a non-802.1Q-enabled device or an access port receives an 802.1Q frame, the tag data is ignored, and the packet is switched at Layer 2 as a standard Ethernet frame
  - Baby giants: 1500B < MTU < 2000B

Understanding Native VLAN in 802.1Q Trunking



- A frequent configuration error is to have different native VLANs. The native VLAN that is configured on each end of an 802.1Q trunk must be the same.
- Cisco switches use Cisco Discovery Protocol (CDP) to warn of a native VLAN mismatch
- By default, the native VLAN will be VLAN 1.

- `Switch(config-if)# switchport trunk native vlan vlan-id`

Understanding DTP

Mode in Cisco IOS	Function
Access	Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.
Trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.
Nonegotiate	Prevents the interface from generating DTP frames. You must configure the local and neighboring interface manually as a trunk interface to establish a trunk link. Use this mode when connecting to a device that does not support DTP.
Dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.
Dynamic auto	Makes the interface willing to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is the default mode for all Ethernet interfaces in Cisco IOS.

DTP Modes Combination

	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

VLAN Ranges and Mappings

- ISL supports VLAN numbers in the range of 1 to 1005, whereas 802.1Q VLAN numbers are in the range of 1 to 4094.
- The default behavior of VLAN trunks is to permit all normal and extended-range VLANs across the link if it is an 802.1Q interface and to permit normal VLANs in the case of an ISL interface.

Supported VLAN on Catalyst Switchs

Type of Switch	Maximum Number of VLANs	VLAN ID Range
Catalyst 2940	4	1–1005
Catalyst 2950/2955	250	1–4094
Catalyst 2960	255	1–4094
Catalyst 2970/3550/3560/3750	1005	1–4094
Catalyst 2848G/2980G/4000/4500	4094	1–4094
Catalyst 6500	4094	1–4094

VLAN Ranges

VLAN Range	Range Usage	Propagated via VTP
0, 4095	Reserved for system use only. You cannot see or use these VLANs.	—
1	Normal Cisco default. You can use this VLAN, but you cannot delete it.	Yes
2–1001	Normal For Ethernet VLANs. You can create, use, and delete these VLANs.	Yes
1002–1005	Normal Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.	Yes
1006–1024	Reserved for system use only. You cannot see or use these VLANS.	—
1025–4094	Extended for Ethernet VLANs only.	Not supported in VTP Versions 1 and 2. The switch must be in VTP transparent mode to configure extended-range VLANS. This range is only supported in Version 3.

Configuring, Verifying, and Troubleshooting VLANs and Trunks

Step 1. Enter global configuration mode:

- `Switch# configure terminal`

Step 2. Create a new VLAN with a particular ID number:

- `Switch(config)# vlan vlan-id`

Step 3. (Optional.) Name the VLAN:

- `Switch(config-vlan)# name vlan-name`

```
Switch# configure terminal
Switch(config)# vlan 5
Switch(config-vlan)# name Engineering
Switch(config-vlan)# exit
```

```
Switch# configure terminal
Switch(config)# no vlan 3
Switch(config)# end
```

Assigning an Access Port to a VLAN

Step 1. From global configuration mode, enter the configuration mode for the particular port you want to add to the VLAN:

- `Switch(config)# interface interface-id`

Step 2. Specify the port as an access port:

- `Switch(config-if)# switchport mode access`
- `Switch(config-if)# switchport host`

```
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

Step 3. Remove or place the port in a particular VLAN:

- `Switch(config-if)# [ no ] switchport access vlan vlan-id`

Assigning an Access Port to a VLAN

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet 5/6
Switch(config-if)# description PC A
Switch(config-if)# switchport
Switch(config-if)# switchport host
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 200
Switch(configif)# no shutdown
Switch(config-if)# end
```

Verifying the VLAN Configuration

```
SW1#show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Et1/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

SW1#
```

```
SW1# show vlan name VLAN0003

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active    Et1/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

SW1#
```

Verifying the VLAN Configuration

Field	Description
VLAN	VLAN number
Name	Name, if configured, of the VLAN
Status	Status of the VLAN (active or suspended)
Ports	Ports that belong to the VLAN
Type	Media type of the VLAN
SAID	Security association ID value for the VLAN
MTU	Maximum transmission unit size for the VLAN
Parent	Parent VLAN, if one exists
RingNo	Ring number for the VLAN, if applicable
BridgNo	Bridge number for the VLAN, if applicable
Stp	Spanning Tree Protocol type used on the VLAN
BrdgMode	Bridging mode for this VLAN
Trans1	Translation bridge 1
Trans2	Translation bridge 2
AREHops	Maximum number of hops for All-Routes Explorer frames
STEHops	Maximum number of hops for Spanning Tree Explorer frames

Displaying Information About the Interface

```
Switch# show running-config interface FastEthernet 5/6
Building configuration... !
Current configuration :33 bytes
interface FastEthernet 5/6
switchport access vlan 200
switchport mode access
end
```

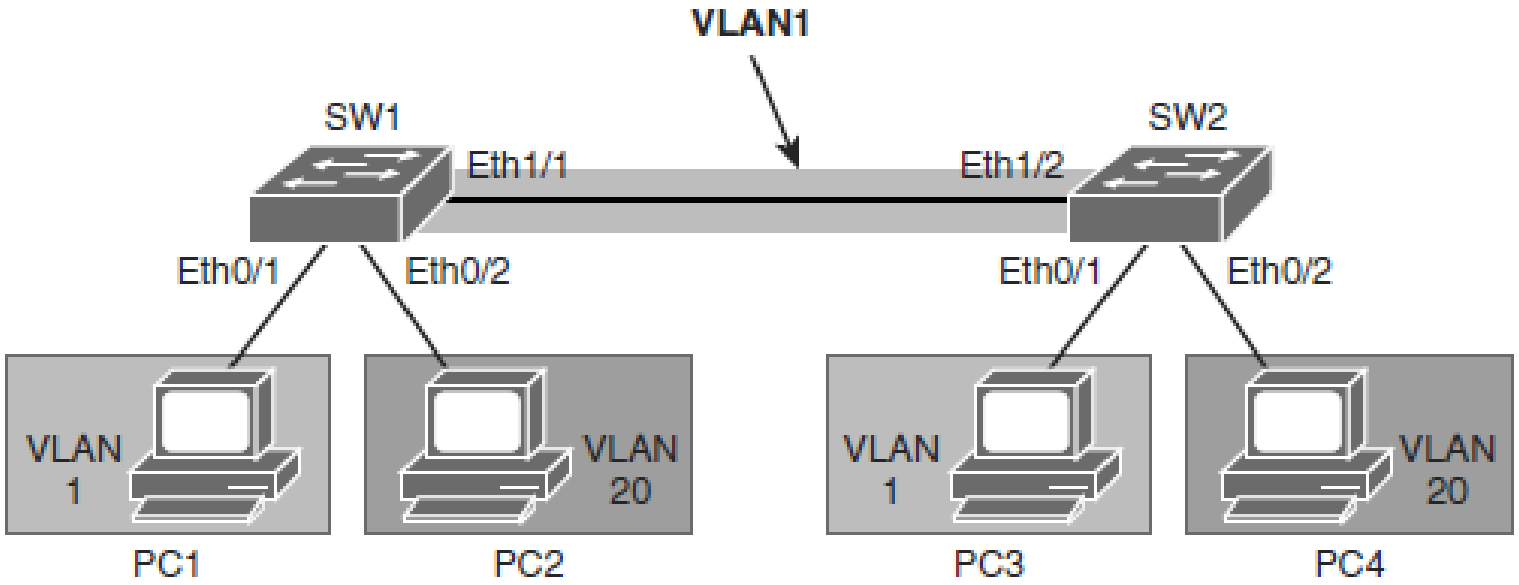
Displaying Detailed Switch Port Information

```
BXB-6500-10:8A# SW1# show int ethernet 4/1 switchport
Name: Et4/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Operational Dot1q Ethertype:  0x8100
Negotiation of Trunking: Off
Access Mode VLAN: 200 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Operational Native VLAN tagging: disabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Voice VLAN: none (Inactive)
Appliance trust: none
```

Displaying MAC Address Table Information

```
Switch# show mac-address-table interface GigabitEthernet 0/1 vlan 1
SW1# show mac address-table interface Gigabitethernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    aabb.cc01.0600    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 1
```

Topology to Configure VLAN and Trunking



Device	Device IP	Device Interface	Device Neighbor	Interface on the Neighbor
PC1	192.168.1.100	Eth0/0	SW1	Eth0/1
PC2	192.168.20.101	Eth0/0	SW1	Eth0/2
PC3	192.168.1.110	Eth0/0	SW2	Eth0/1
PC4	192.168.20.110	Eth0/0	SW2	Eth0/2

Configuring VLANs and Trunks

Step 1. Create VLAN 20 on both switches.

- `SW1(config)# vlan 20`
- `SW1(config-vlan)# exit`
- `% Applying VLAN changes may take few minutes. Please wait...`

Step 2. On SW1/2 configure port Ethernet 0/2 to be an access port and assign it to VLAN 20

- `SW1(config)# interface ethernet 0/2`
- `SW1(config-if)# switchport mode access`
- `SW1(config-if)# switchport access vlan 20`

Step 3. Configure ports that connect SW1 and SW2 as trunks. Use the dot1Q encapsulation.

- Trunk configuration on SW1:
- `SW1(config)# interface Ethernet 1/1`
- `SW1(config-if)# switchport trunk encapsulation dot1q`
- `SW1(config-if)# switchport trunk allowed vlan 1,20`
- `SW1(config-if)# switchport mode trunk`
- Trunk configuration on SW2:
- `SW2(config)# interface Ethernet 1/2`
- `SW2(config-if)# switchport trunk encapsulation dot1q`
- `SW2(config-if)# switchport trunk allowed vlan 1,20`
- `SW2(config-if)# switchport mode trunk`

Verify Trunking

```
SW1# show interfaces trunk

Port            Mode         Encapsulation  Status        Native vlan
Et1/1           on           802.1q         trunking      1

Port            Vlans allowed on trunk
Et1/1           1,20

Port            Vlans allowed and active in management domain
Et1/1           1,20

Port            Vlans in spanning tree forwarding state and not pruned
Et1/1           1,20
```

Best Practices for VLANs and Trunking

- For the Local VLANs model, it is usually recommended to have only one to three VLANs per access module.
- Avoid using VLAN 1 as the black hole for all unused ports.
- Try to always have separate voice VLANs, data VLANs, management VLANs, native VLANs, black hole VLANs, and default VLANs (VLAN 1).
- In the local VLANs model, avoid VTP; it is feasible to use manually allowed VLANs in a network on trunks.
- For trunk ports, turn off DTP and configure it manually.
- Use IEEE 802.1Q rather than ISL because it has better support for QoS and is a standard protocol.
- Manually configure access ports that are not specifically intended for a trunk link.
- Prevent all; only permit control protocols to run on VLAN 1 (data traffic from VLAN1 DTP, VTP, STP bridge protocol data units [BPDUs], Port Aggregation Protocol [PAgP], Link Aggregation Control Protocol [LACP], Cisco Discovery Protocol [CDP], and such.).
- Avoid using Telnet because of security risks; enable Secure Shell (SSH) support on management VLANs.

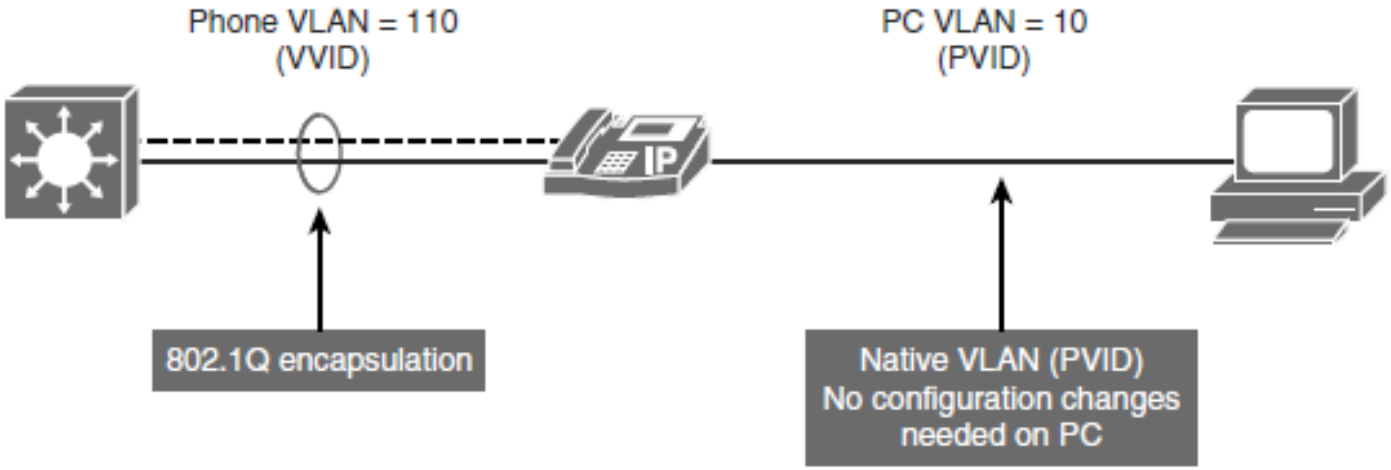
Best Practices for VLANs and Trunking

- DTP is useful when the status of the switch on the other end of the link is uncertain or might be changing over time. When the link is to be set to trunk in a stable manner, changing both ends to trunk nonegotiate accelerates the convergence time, saving up to 2 seconds upon boot time. We recommend this mode on stable links between switches that are part of the same core infrastructure.
- On trunk links, it is recommended to manually prune the VLANs that are not used.
- It is also a good practice to have an unused VLAN as a native VLAN on the trunk links to prevent DTP spoofing.
- If trunking is not used on a port, you can disable it with the interface level command **switchport host** .

Voice VLAN Overview

- Multiservice switches support a new parameter for IP telephony support that makes the access port a multi-VLAN access port.
- The new parameter is called a *voice* or *auxiliary VLAN* . Every Ethernet 10/100/1000 port in the switch is associated with two VLANs:
  - A native VLAN for data service that is identified by the PVID
  - A voice VLAN that is identified by the voice VLAN ID (VVID)
- During the initial CDP exchange with the access switch, the IP phone is configured with a VVID.
- The IP phone is also supplied with a QoS configuration using CDP.

Voice VLAN Overview



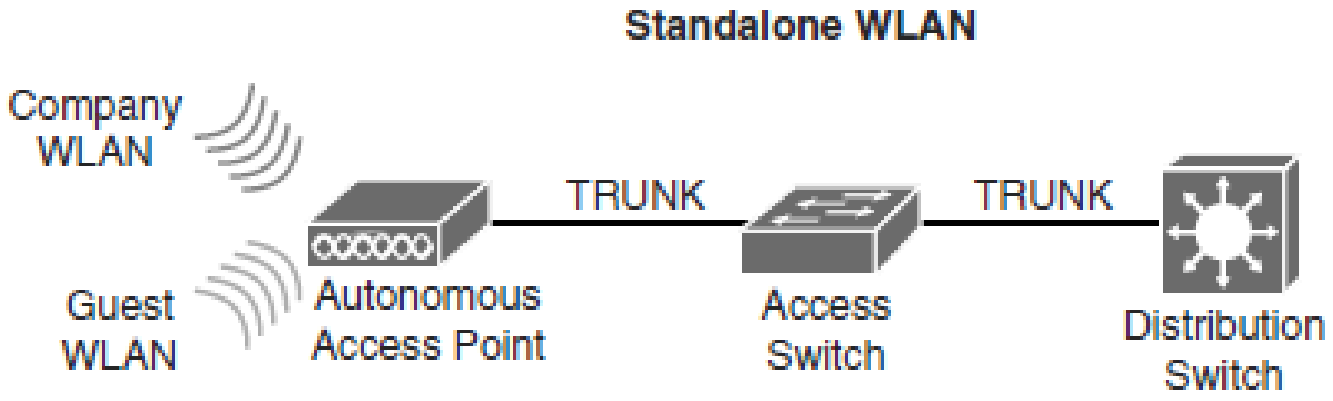

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport voice vlan 110
```

Switch Configuration for Wireless Network Support

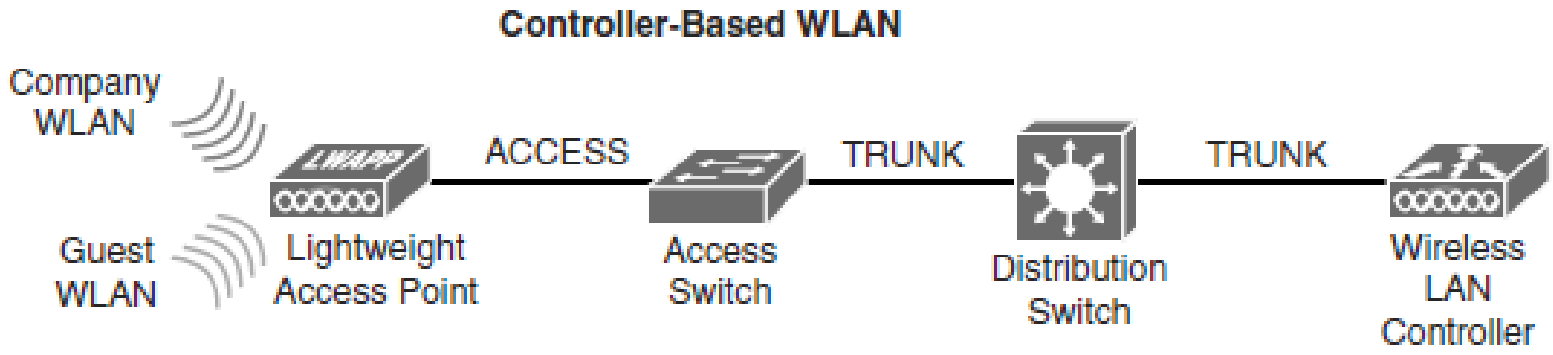
- Cisco offers the following two WLAN implementations:
  - The standalone WLAN solution is based on autonomous (standalone) access points (APs).
  - The controller-based WLAN solution is based on controller-based APs and WLCs (Wireless LAN Controllers).

Autonomous WLAN

- In the autonomous (or standalone) solution, each AP operates independently and acts as a transition point between the wireless media and the 802.3 media.
- The data traffic between two clients flows via the Layer 2 switch when on the same subnet from a different AP infrastructure. As the AP converts the IEEE 802.11 frame into an 802.3 frame, the wireless client MAC address is transferred to the 802.3 headers and appears as the source for the switch.
- The destination, also a wireless client, appears as the destination MAC address.

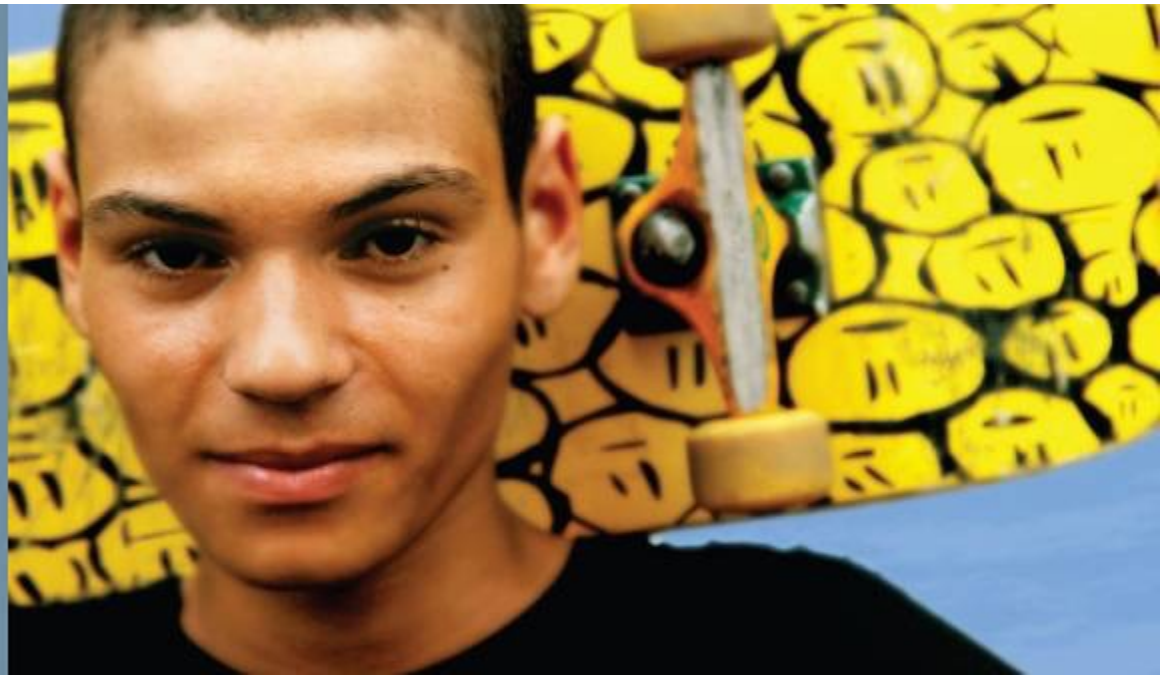


Controller-Based WLAN



- In a controller-based solution, management, control, deployment, and security functions are moved to a central point: the wireless controller.
- To implement a wireless network, APs and switches need to be configured. APs can be configured directly (autonomous APs) or through a controller (lightweight APs).
- Either way, configuring APs is a domain of the WLAN specialist. On the switch side, just configure VLANs and trunks on switches to support WLAN.

Private VLANs



Private VLANs

- Introduction to private VLANs
- Describe the private VLAN feature
- Describe the private VLAN port types
- Configure private VLANs
- Verify private VLAN configuration
- Describe private VLANs across multiple switches
- Describe the protected port feature

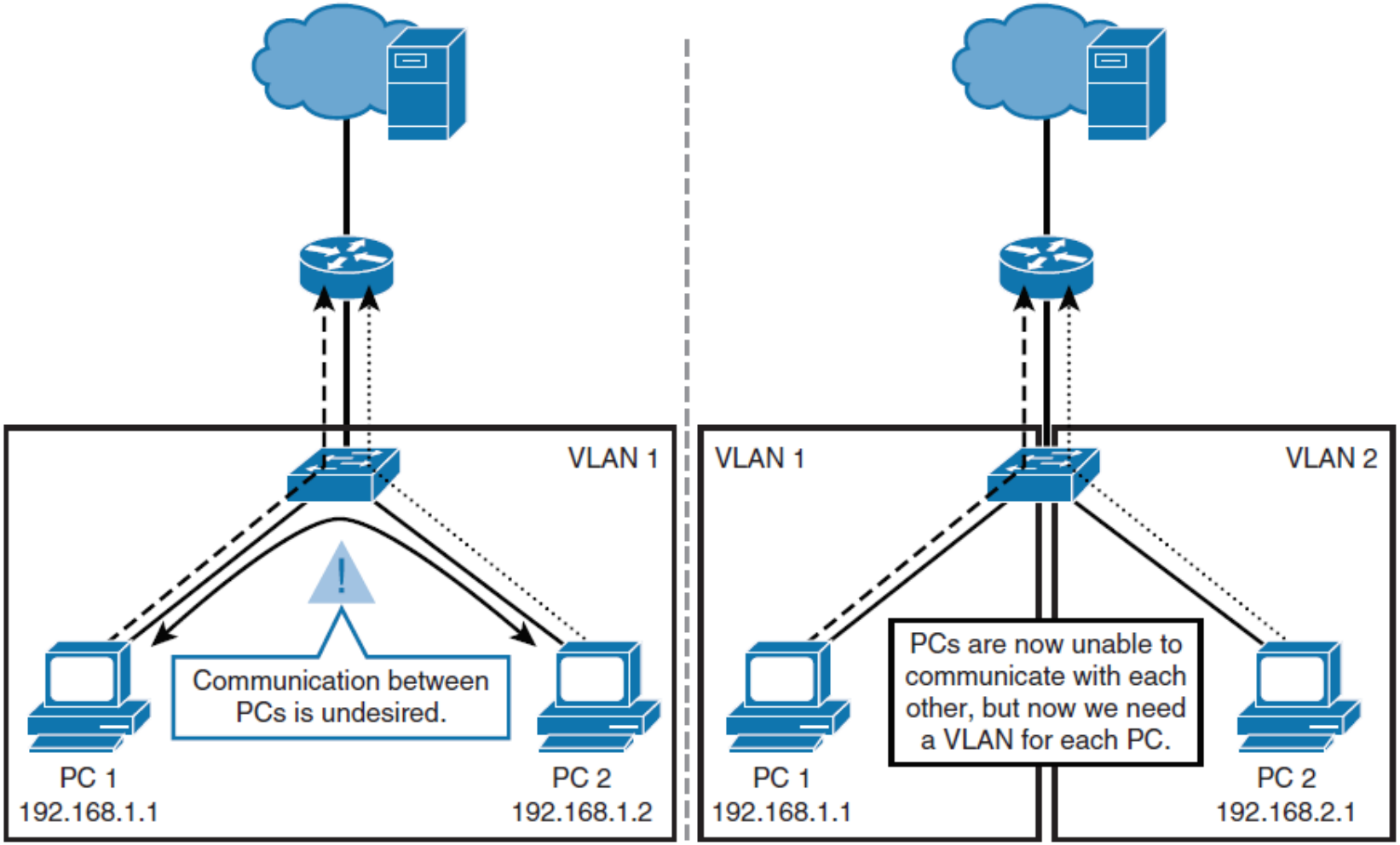
Introduction to PVLANs

- PVLANs restrict end-user devices such as PCs and mobile devices from communicating with each other, but still allow communication to router ports and network services.
- The end-user devices will behave as normal but cannot communicate to other devices in the same Layer 2 domain.
- This mechanism provides a level of security.
- Assigning every single end device its own VLAN would accomplish the same security method as PVLANs; however, switches have a limit on the number of VLANs supported, and a large number of VLANs creates scalability issues.

Introduction to PVLANs

- PVLANs are essentially VLANs inside a VLAN.
- A Layer 3 device is needed to route packets between different PVLANs.
- When a VLAN is partitioned into PVLANs, devices in different PVLANs still belong to the same IP subnet but are unable to communicate with each other on Layer 2.
- PVLANs are an elegant solution when you need to keep multiple devices in the same IP subnet yet provide port isolation on Layer 2.

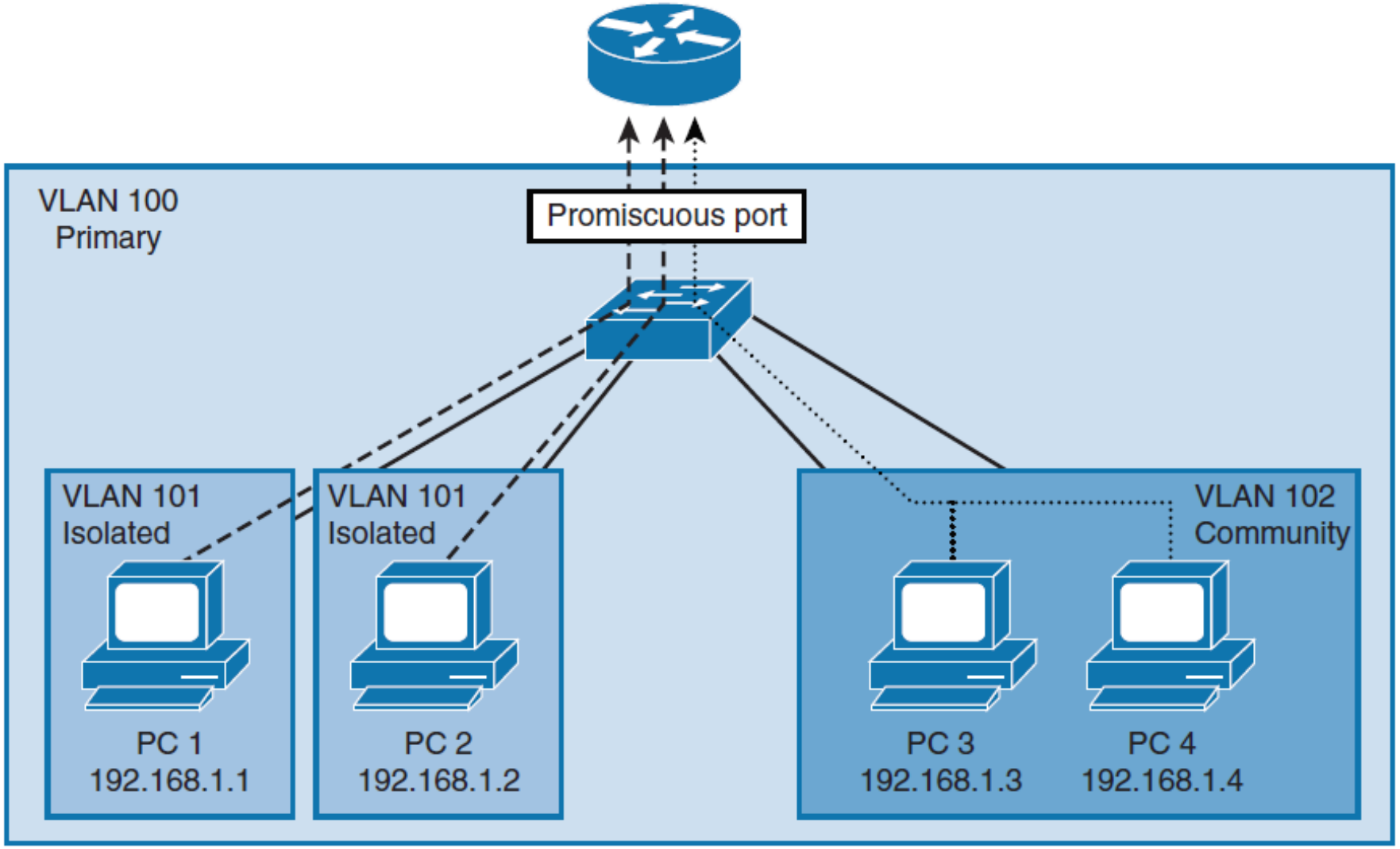
Introduction to PVLANs



PVLAN Port Types

- A PVLAN domain has one primary VLAN.
- Each port in a private VLAN domain is a member of the primary VLAN; the primary VLAN is the entire private VLAN domain.
- Secondary VLANs are subdomains that provide isolation between ports within the same private VLAN domain.
- There are two types of secondary VLANs: isolated VLANs and community VLANs.
  - Isolated VLANs contain isolated ports, which cannot communicate between each other in the isolated VLAN.
  - Community VLANs contain community ports that can communicate between each other in the community VLAN.

PVLAN Port Types



PVLAN Port Types

- **Promiscuous**
  - A promiscuous port belongs to the primary VLAN and can communicate with all mapped ports in the primary VLAN, including community and isolated ports.
  - There can be multiple promiscuous ports in a primary VLAN.
- **Isolated**
  - An isolated port is a host port that belongs to an isolated secondary VLAN.
  - An isolated port has complete isolation from other ports, except with associated promiscuous ports.
  - You can have more than one isolated port in a specified isolated VLAN.
- **Community**
  - A community port is a host port that belongs to a community secondary VLAN.
  - Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
  - They are isolated from all ports in other community VLANs and all isolated ports.

PVLAN Configuration

- VTP must be set to transparent or off (v1, v2 and v3 supp).
- Configure the primary VLAN.
- Configure the secondary VLANs and apply the configuration of these PVLANs as isolated or community.
- Associate the primary VLAN with the secondary VLANs

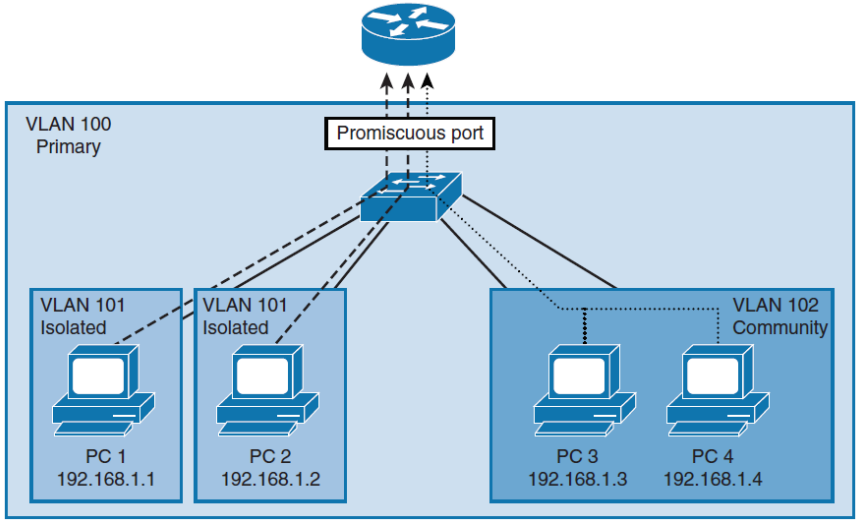
```
SW(config)# vlan 100
SW(config-vlan)# private-vlan primary
SW(config)# vlan 101
SW(config-vlan)# private-vlan isolated
SW(config)# vlan 102
SW(config-vlan) private-vlan community
SW(config) vlan 100
SW(config-vlan) private-vlan association 101, 102
```

Assign Ports

- **Promiscuous Ports**
- SW(config)# **interface** *interface-slot/number*
- SW(config-if)# **switchport mode private-vlan promiscuous**
- SW(config-if)# **switchport private-vlan mapping** *primary-vlan-id* **add** *secondary-vlanid* {, *secondary-vlan-id* }

- **Community or Isolated Ports**
- SW(config)# **interface range** *interface-range*
- SW(config-if-range)# **switchport mode private-vlan host**
- SW(config-if-range)# **switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*

Assign Ports




```
SW(config)# interface GigabitEthernet 0/1
SW(config-if)# switchport description Interface-to-Router
SW(config-if)# switchport mode private-vlan promiscuous
SW(config-if)# switchport private-vlan mapping 100 add 101, 102
SW(config-if)# interface range GigabitEthernet 0/2-3
SW(config-if-range)# switchport description End-User-Ports-In-Isolated-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 101
SW(config-if)# interface range GigabitEthernet 0/4-5
SW(config-if-range)# switchport description End-User-Ports-In-Community-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 102
```

Using the Protected Port Feature

- The PVLAN feature is not available on all switches.
- Protected port, also known as the PVLAN edge, is a feature that (unlike PVLANs) has only local significance to the switch.
- Protected ports do not forward any traffic to protected ports on the same switch.

- `SW(config)# interface interface-slot/number`
- `SW(config-if)# switchport protected`

VLAN Trunking Protocol

VLAN Trunking Protocol

- VTP overview
- VTP modes
- VTP versions
- VTP pruning
- VTP authentication
- VTP advertisements
- VTP configuration and verifications
- VTP configuration overwriting
- VTP best practices

VTP Overview

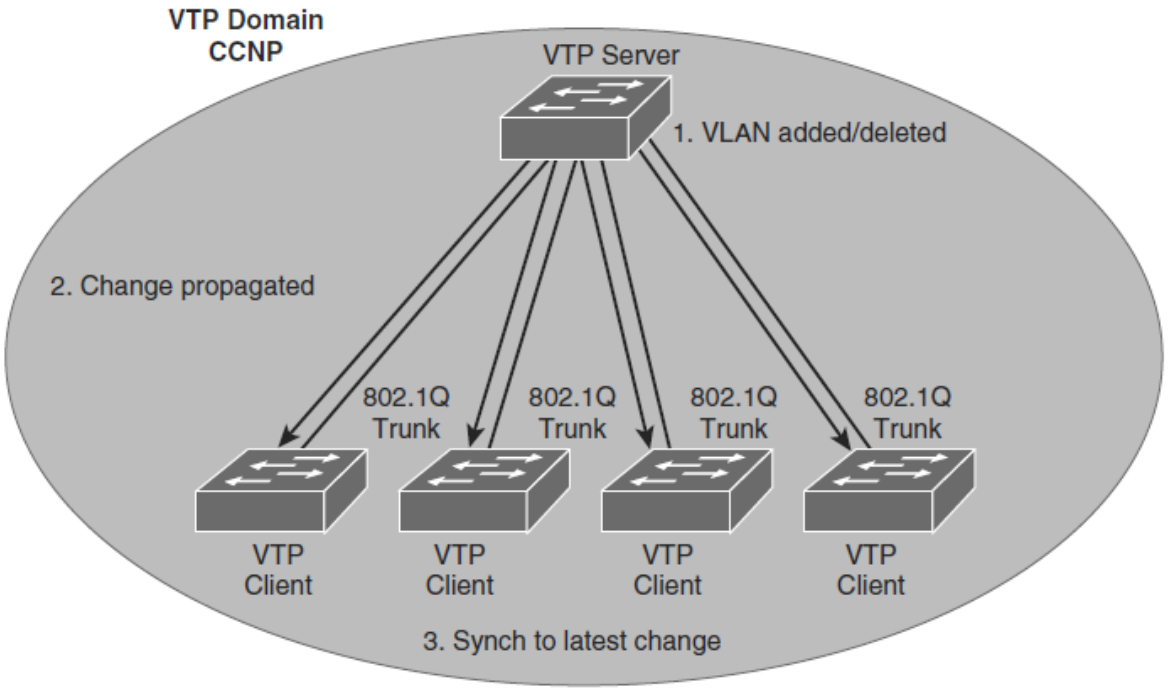
- VTP is a Layer 2 protocol that maintains VLAN configuration consistency by managing the additions, deletions, and name changes of VLANs across network
- Switches transmit VTP messages only on 802.1Q or ISL trunks.
- Cisco switches transmit VTP summary advertisements over the management VLAN (VLAN 1 by default) using a **Layer 2 multicast** frame every 5 minutes (DM: 01-00-0C-CC-CC-CC).
- **VTP domain** is one switch or several interconnected switches sharing the same VTP environment, but switch can be only in one VTP domain at any time.
- By default, a Cisco Catalyst switch is in the no-management-domain state or <null> until it receives an advertisement for a domain over a trunk link or until you configure a management domain.
- Configurations that are made on a single VTP server are propagated across trunk links to all of the connected switches in the network.
- Configurations will be exchanged if VTP domain and VTP passwords match.
- VTP is a Cisco proprietary protocol.

VTP Propagation

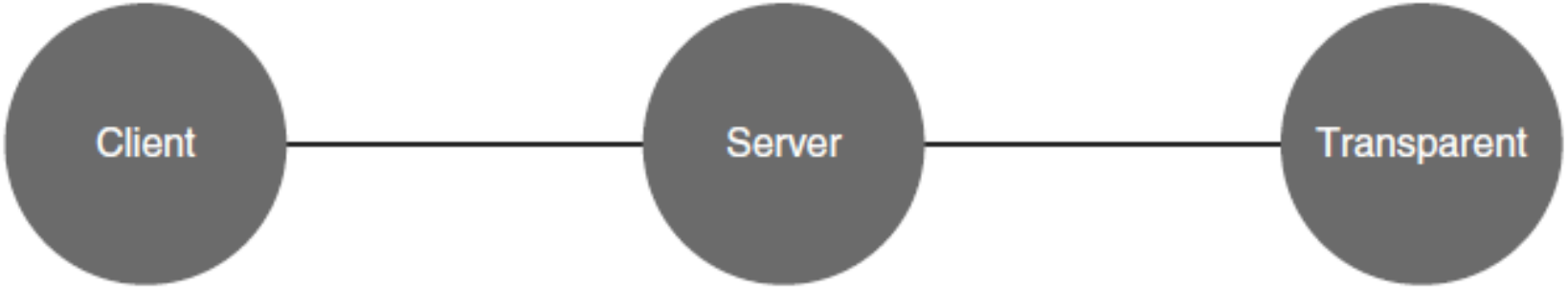
Step 1. An administrator adds a new VLAN definition.

Step 2. VTP propagates the VLAN information to all switches in the VTP domain.

Step 3. Each switch synchronizes its configuration to incorporate the new VLAN data.



VTP Modes



- Cannot create, modify, or delete VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations

- Creates, modifies, and deletes VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations

- Creates, modifies, and deletes local VLANs only
- Forwards advertisements
- Does not synchronize VLAN configurations

VTP Operation

- By default, Cisco IOS VTP servers and clients save VLANs to the vlan.dat file in flash memory, causing them to retain the VLAN table and revision number.
- The **erase startup-config** command does not affect the vlan.dat file on switches in VTP client and server modes.
- Switches that are in VTP transparent mode display the VLAN and VTP configurations in the **show running-config** command output because this information is stored in the configuration text file.
- If you perform **erase startup-config** on a VTP transparent switch you will delete its VLANs.

VTP Versions

- Cisco Catalyst switches support three different versions of VTP: 1, 2, and 3.
- It is importante to decide which version to use because they are not interoperable.
- Cisco recommends running only one VTP version for network stability.
- The default VTP version that is enabled on a Cisco switch is Version 1.
- If you do need to change the version of VTP in the domain, the only thing that you need to do is to enable it on the VTP server; the change will propagate throughout the network.

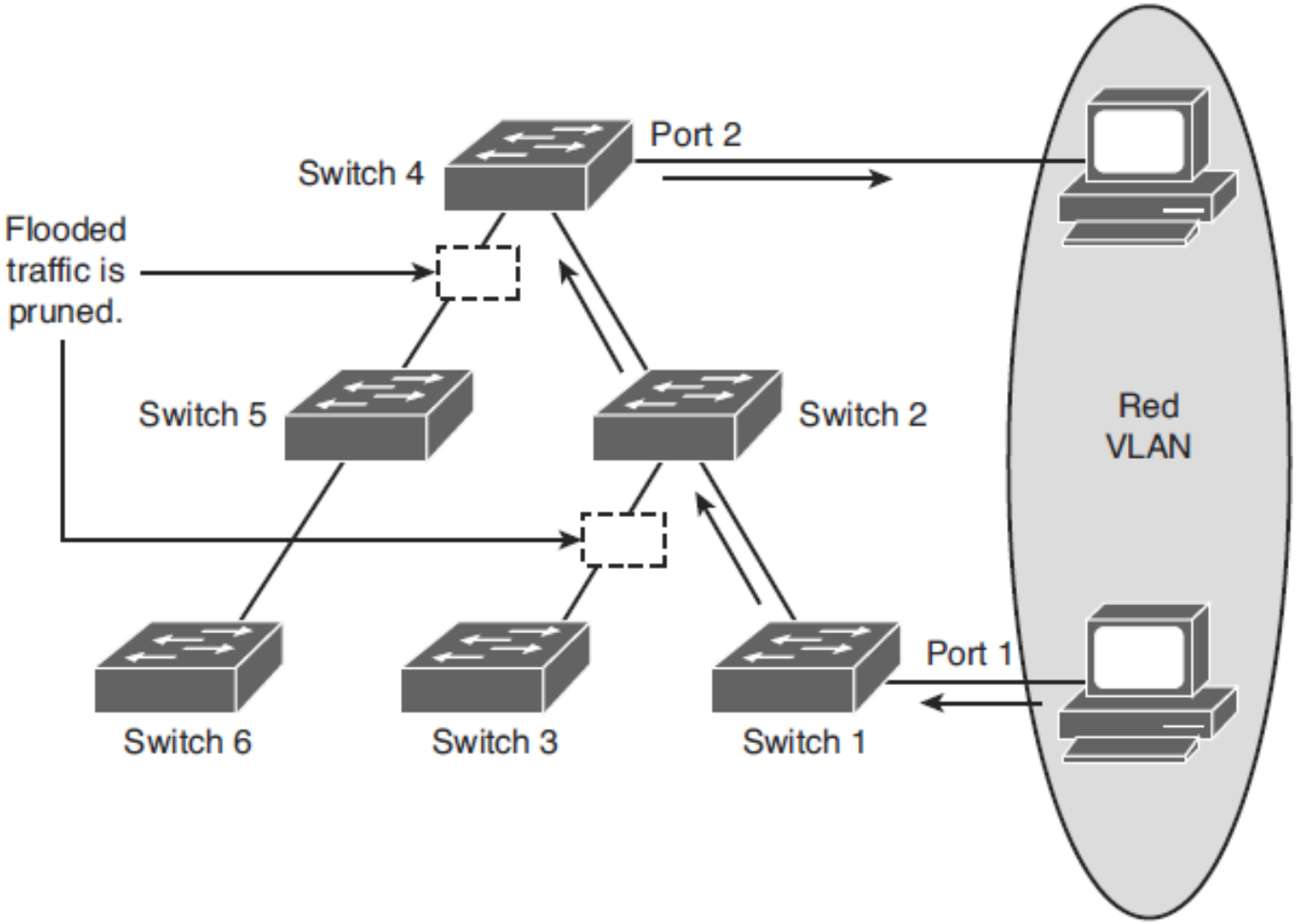
VTP Version 1 and 2

- **Version-dependent transparent mode**
  - VTP Version 1, a VTP transparent network device inspects VTP messages for the domain name and version
  - VTP Version 2 forwards VTP messages in transparent mode, without checking the version.
- **Consistency check**
  - In VTP Version 2, VLAN consistency checks, such as VLAN names and values, are performed.
- **Token ring support**
  - VTP Version 2 supports Token Ring LAN switching and VLANs.
- **Unrecognized type-length-value support**
  - VTP Version 2 switches propagate received configuration change messages out other trunk links, even if they are not able to understand the message.

VTP Version 3

- **Extended VLAN support**
  - VTP also can be used to propagate extended VLANs
- **Domain name is not automatically learned**
  - With VTPv2, a factory default switch that receives a VTP message will adapt the new VTP domain name.
- **Better security**
  - VTP domain password is secure during transmission and in the switch's database.
- **Better database propagation.**
  - Only the primary server is allowed to update other devices and only one server per VTP domain is allowed to have this role.
- **Multiple Spanning Tree (MST) support**
  - VTPv3 adds support for propagation of MST instances.

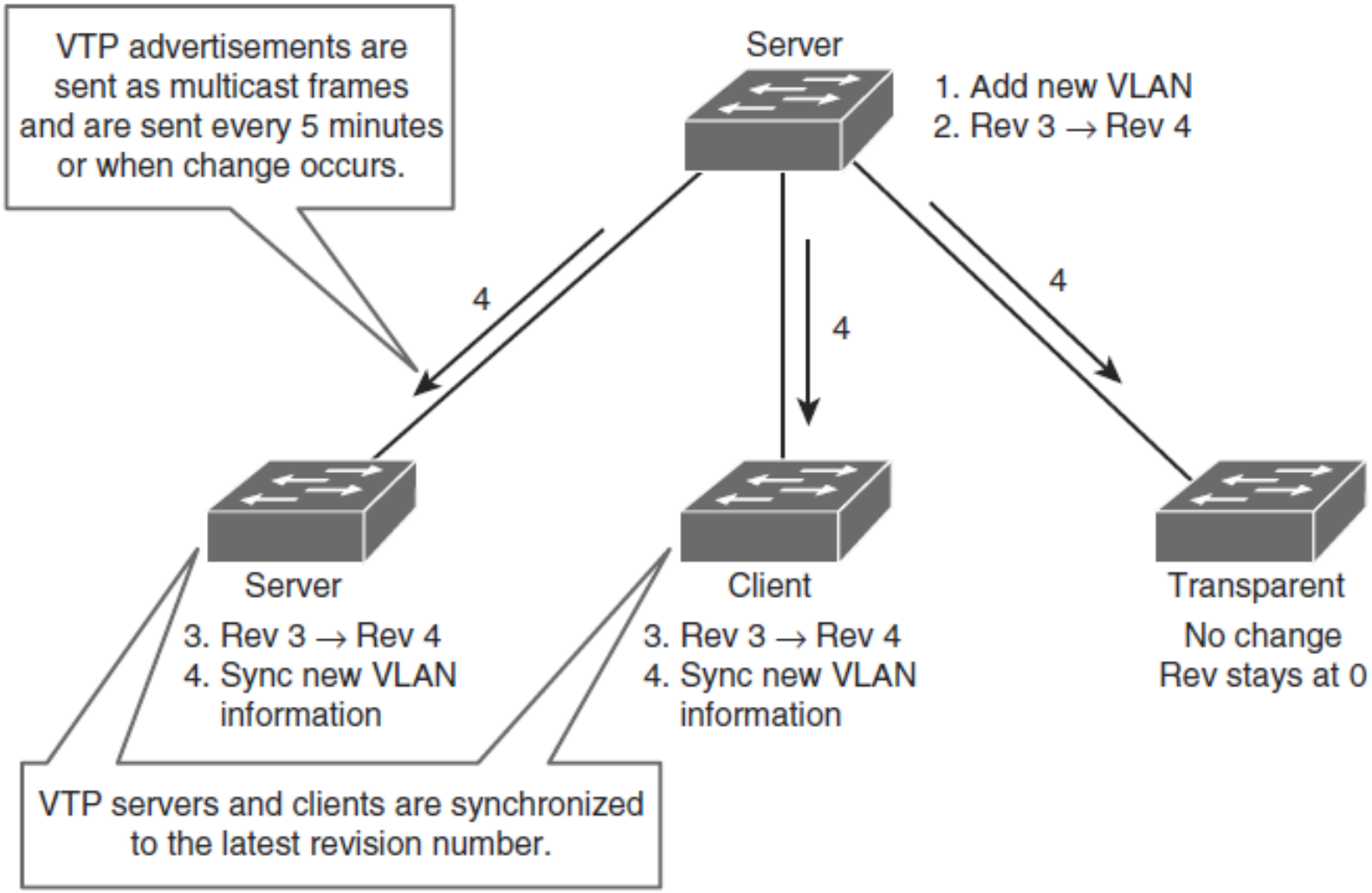
VTP Pruning



VTP Authentication

- VTP domains can be secured by using the VTP password feature.
- It is important to make sure that all the switches in the VTP domain have the same password and domain name; otherwise, a switch will not become a member of the VTP domain.
- Cisco switches use the message digest 5 (MD5) algorithm to encode passwords in 16-byte words (128b).
- These passwords propagate inside VTP summary advertisements.
- In VTP, passwords are case sensitive and can be 8 to 64 characters in length.
- The use of VTP authentication is a recommended practice.

VTP Advertisements



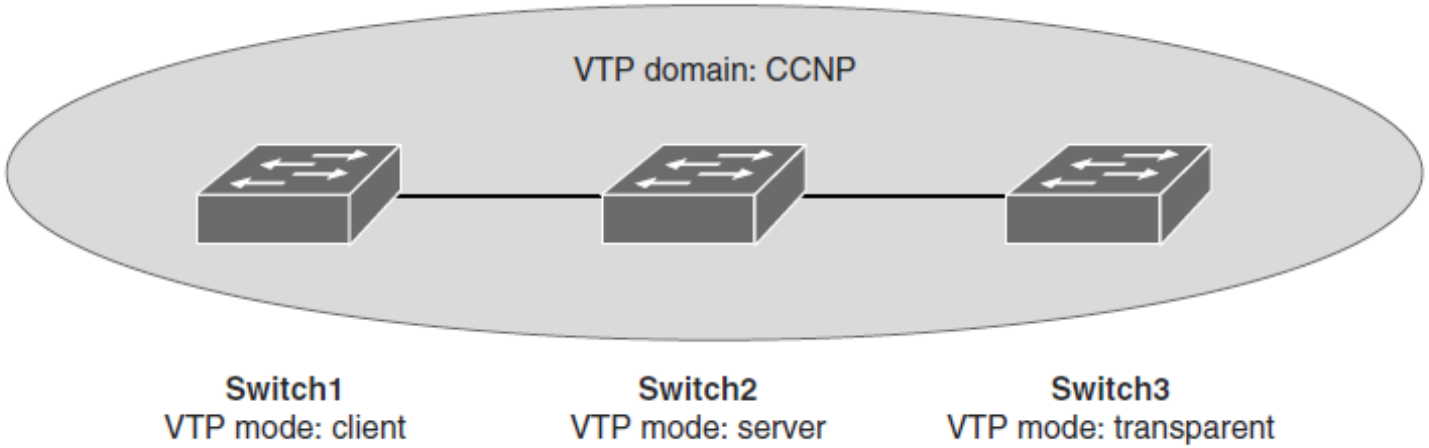
VTP Messages Types

- **Summary Advertisements**
  - By default, Catalyst switches issue summary advertisements in 5-minute increments. Summary advertisements inform adjacent Catalysts of the current **VTP domain name** and the **configuration revision** number.
  - When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name.
  - If the name differs, the switch simply ignores the packet.
  - If the name is the same, the switch then compares the configuration revision to its own revision.
  - If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an **advertisement request** is sent.

VTP Messages Types

- **Subset Advertisements**
  - When you add, delete, or change a VLAN in a Catalyst server, the Catalyst server where the changes are made increments the configuration revision and issues a summary advertisement.
  - One or several subset advertisements follow the summary advertisement.
  - A subset advertisement contains a list of VLAN information.
- **Advertisement Requests are sent when:**
  - The switch has been reset.
  - The VTP domain name has been changed.
  - The switch has received a VTP summary advertisement with a higher configuration revision than its own.
  - Upon receipt of an advertisement request, a VTP device sends a summary advertisement. One or more subset advertisements follow the summary advertisement.

Configuring and Verifying VTP



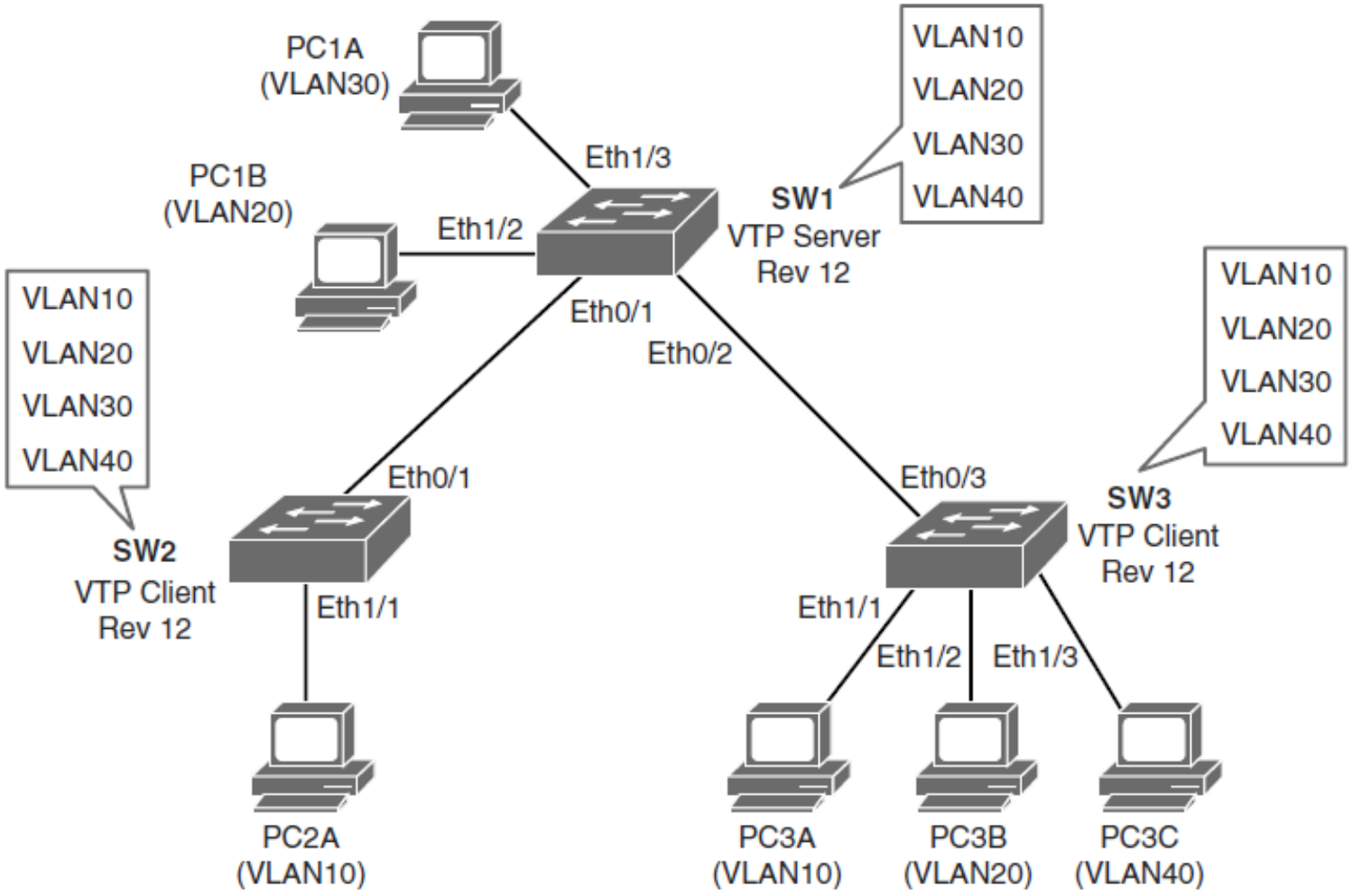
- **Step 1.** Configure VTP on all the switches, Switch 1 and Switch 3 as client mode where as Switch2 as server mode

```
Switch1(config)# vtp password Cisco
Switch1(config)#vtp mode client
Switch1(config)#vtp domain CCNP
Switch1(config)#vtp version 1
```

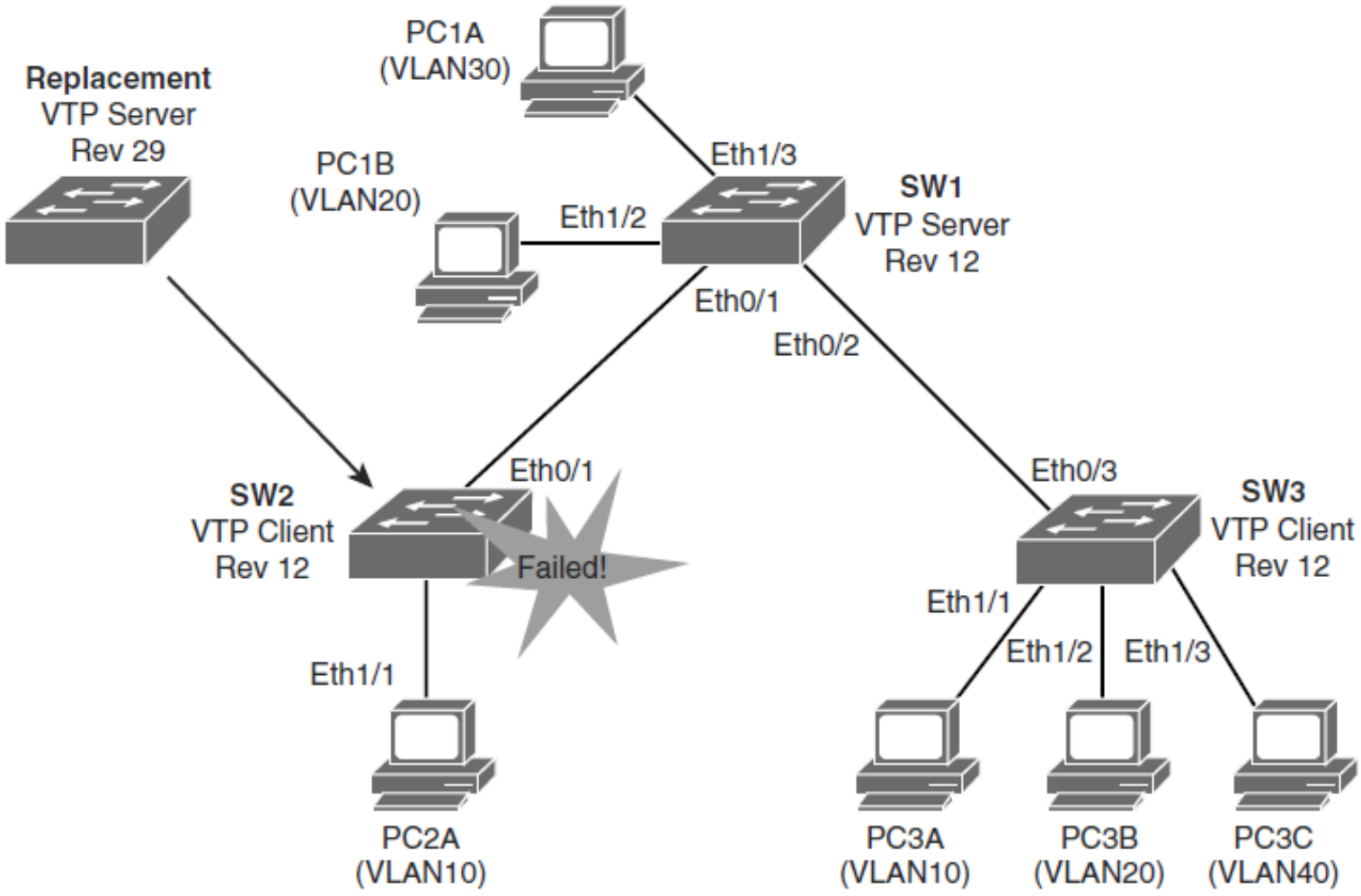
```
Switch3(config)# vtp password Cisco
Switch3(config)#vtp mode client
Switch3(config)#vtp domain CCNP
Switch3(config)#vtp version 1
```

```
Switch2(config)# vtp password Cisco
Switch2(config)#vtp mode server
Switch2(config)#vtp domain CCNP
Switch2(config)#vtp version 1
```

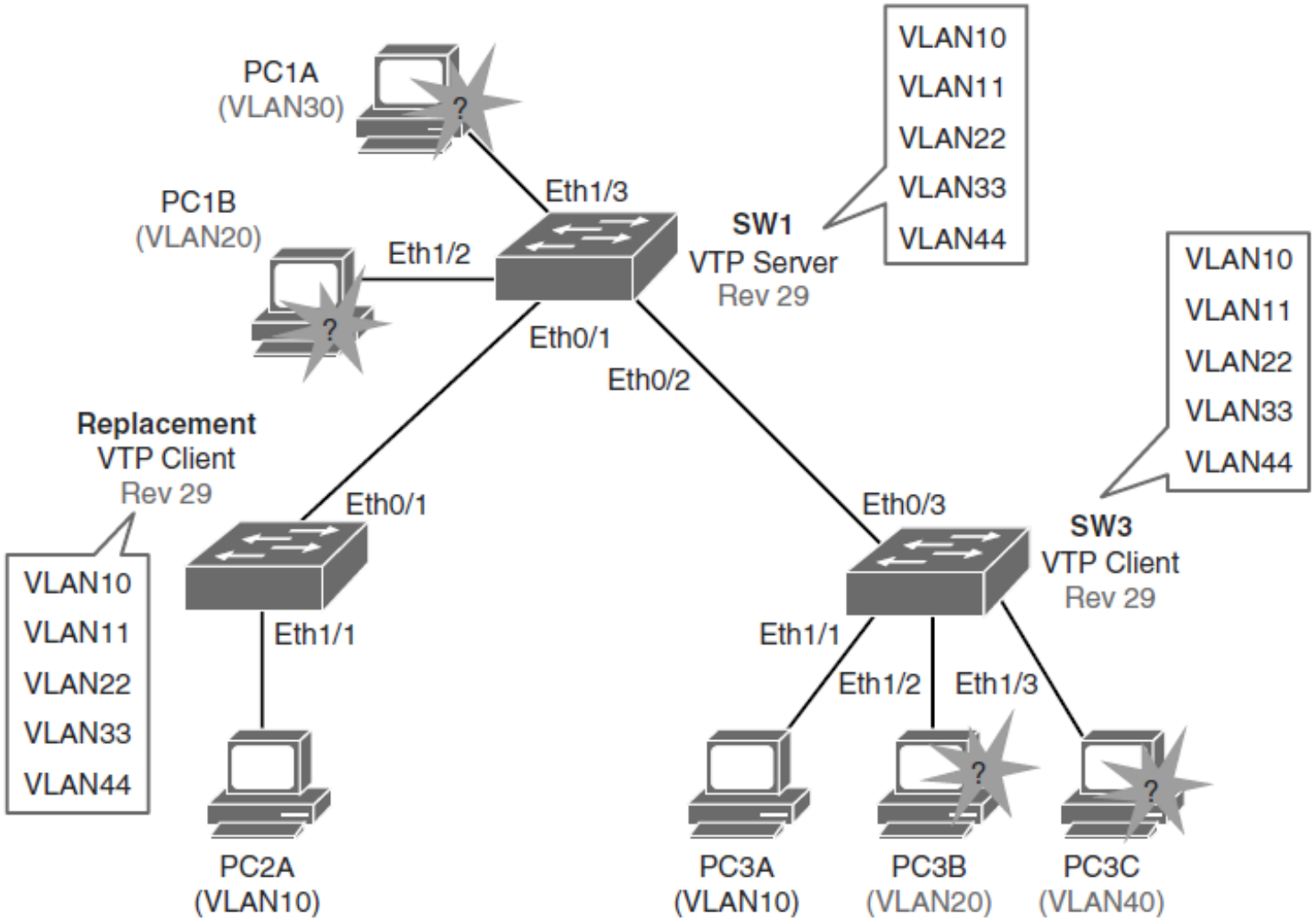
Overwriting VTP Configuration (Very Common Issue with VTP)



Overwriting VTP Configuration (Very Common Issue with VTP)



Overwriting VTP Configuration (Very Common Issue with VTP)



VTP Key Points

- Avoid, as much as possible, VLANs that span the entire network.
- The VTP revision number is stored in NVRAM and is not reset if you erase the switch configuration and reload it. To reset the VTP revision number to zero, use the following two options:
  - Change the switch's VTP domain name to a nonexistent VTP domain, and then change the domain back to the original name.
  - Change the switch's VTP mode to transparent and then back to the previous VTP mode.

Best Practices for VTP Implementation

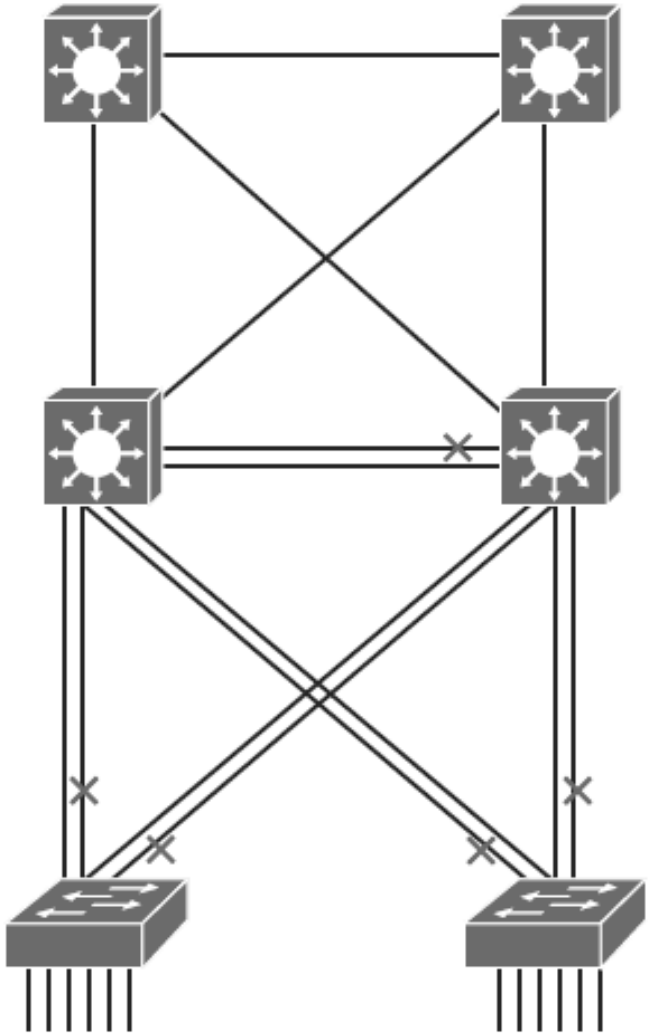
- VTP is often used in a new network to facilitate the implementation of VLANs.
- However, as the network grows larger, this benefit can turn into a liability.
- If a VLAN is deleted by accident on one server, it is deleted throughout the network.
- If a switch that already has a VLAN database defined is inserted into the network, it can hijack the VLAN database by deleting added VLANs.
- Because of this, it is the recommended practice to configure all switches to transparent VTP mode and manually add VLANs as needed, especially in a larger campus network.
- VTP configuration is usually good for small environments.

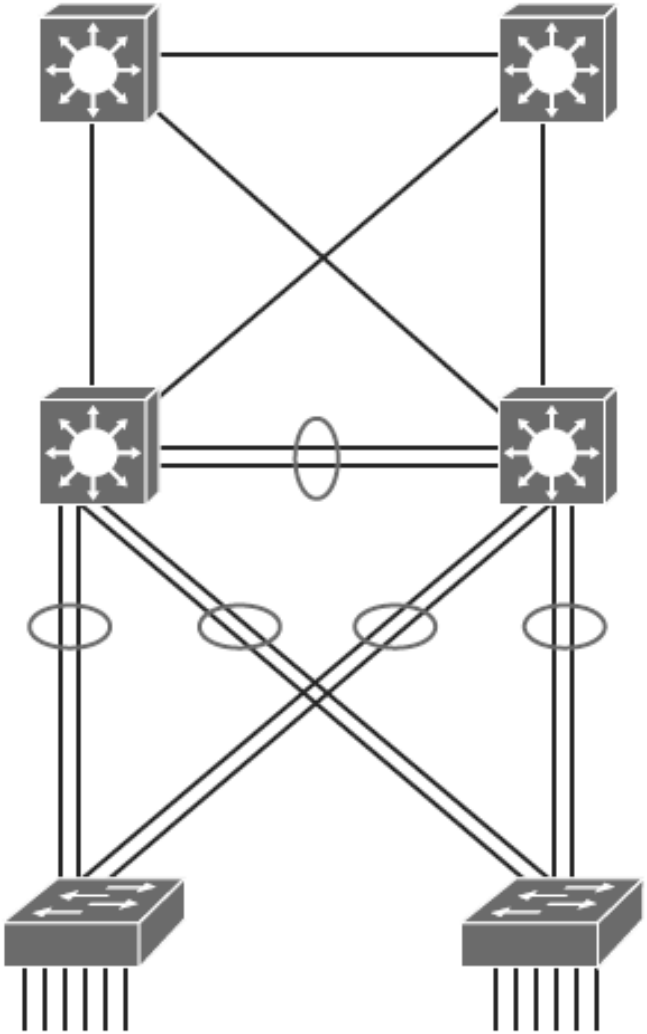
Implementing EtherChannel in a Switched Network

Implementing EtherChannel in a Switched Network

- The need for EtherChannel technology
- Port aggregation negotiation protocols
- Configuration steps for bundling interfaces into a Layer 2 EtherChannel
- Configuring EtherChannel
- Changing EtherChannel load-balancing behavior
- How EtherChannel load-balancing works
- The role of EtherChannel Guard

The Need for EtherChannel





EtherChannel Overview

- EtherChannel is a technology that was originally developed by Cisco as a LAN switch-to-switch technique of grouping several Fast or Gigabit Ethernet ports into one logical channel.
- This technology has many benefits:
  - It relies on the existing switch ports. There is no need to upgrade the switch-to-switch link to a faster and more expensive connection.
  - Most of the configuration tasks can be done on the EtherChannel interface instead of on each individual port, thus ensuring configuration consistency throughout the switch-to-switch links.
  - Load balancing is possible between the links that are part of the same EtherChannel. Depending on the hardware platform, you can implement one or several methods, such as source-MAC to destination-MAC or source-IP to destination-IP load balancing across the physical links.

EtherChannel Mode Interactions

- EtherChannel can be established using one of the following three mechanisms:
  - **LACP:** IEEE's negotiation protocol
  - **PAgP:** Cisco's negotiation protocol
  - **Static persistence:** No negotiation protocol

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Static Persistance

	On
On	Yes

LACP

- Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows several physical ports to be bundled together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.
- It ensures that when EtherChannel is created, all ports have the same type of configuration speed, duplex setting, and VLAN information. Any port modification after the creation of the channel will also change all the other channel ports.
- The switch with the lowest system priority is allowed to make decisions about what ports actively participate in EtherChannel.

LACP

- Ports become active according to their port priority.
- A lower number means higher priority.
- Commonly up to 16 links can be assigned to an EtherChannel, but only 8 can be active at a time.
- Nonactive links are placed into a standby state and are enabled if one of the active links goes down.
- The maximum number of active links in an EtherChannel varies between switches.

LACP Modes of Operation

These are the LACP modes of operation:

- **Active:** Enable LACP
- **Passive:** Enable LACP only if an LACP device is detected

The following are some additional parameters that you can use when configuring LACP:

- **System priority**
  - Each switch running LACP must have a system priority. The system priority can be specified automatically or through the CLI. The switch uses the MAC address and the system priority to form the system ID.
- **Port priority**
  - Each port in the switch must have a port priority. The port priority can be specified automatically or through the CLI.
- **Administrative key**
  - Each port in the switch must have an administrative key value, which can be specified automatically or through the CLI. The administrative key defines the capability of a port to aggregate with other ports, determined by these factors: the port's physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium.

PAgP

- Port Aggregation Protocol (PAgP) provides the same negotiation benefits as LACP.
- PAgP is a Cisco proprietary protocol, and it will work only on Cisco devices.
- PAgP packets are exchanged between switches over EtherChannel-capable ports.
- Neighbors are identified and capabilities are learned and compared with local switch capabilities.
- Ports that have the same capabilities are bundled together into an EtherChannel.
- PAgP forms an EtherChannel only on ports that are configured for identical VLANs or trunking.
- PAgP will automatically modify parameters of the EtherChannel if one of the ports in the bundle is modified.
- PAgP and LACP are not compatible.

PAgP Modes of Operation

These are the following two PAgP modes of operation:

- **Desirable:** Enable PAgP
- **Auto:** Enable PAgP only if a PAgP device is detecte

Statically Bundle Links

- Negotiation with either LACP or PAgP introduces overhead and delay in initialization.
- As an alternative, you can statically bundle links into an EtherChannel.
- This method introduces no delays but can cause problems if not properly configured on both ends.

Layer 2 EtherChannel Configuration Guidelines

Before implementing EtherChannel in a network, plan the following steps necessary to make it successful:

- The first step is to identify the ports that you will use for the EtherChannel on both switches.
- Each interface should have the appropriate protocol identified (PAgP or LACP), have a channel group number to associate all the given interfaces with a port group, and be configured whether negotiation should occur.
- After the connections are established, make sure that both sides of the EtherChannel have formed and are providing aggregated bandwidth.

Layer 2 EtherChannel Configuration Guidelines

Follow these guidelines and restrictions when configuring EtherChannel interfaces:

- **EtherChannel support**
  - All Ethernet interfaces on all modules support EtherChannel, with no requirement that interfaces be physically contiguous or on the same module.
- **Speed and duplex**
  - Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode.
- **VLAN match**
  - All interfaces in the EtherChannel bundle must be assigned to the same VLAN or be configured as a trunk.
- **Range of VLANs**
  - An EtherChannel supports the same allowed range of VLANs on all the interfaces in a trunking Layer 2 EtherChannel.

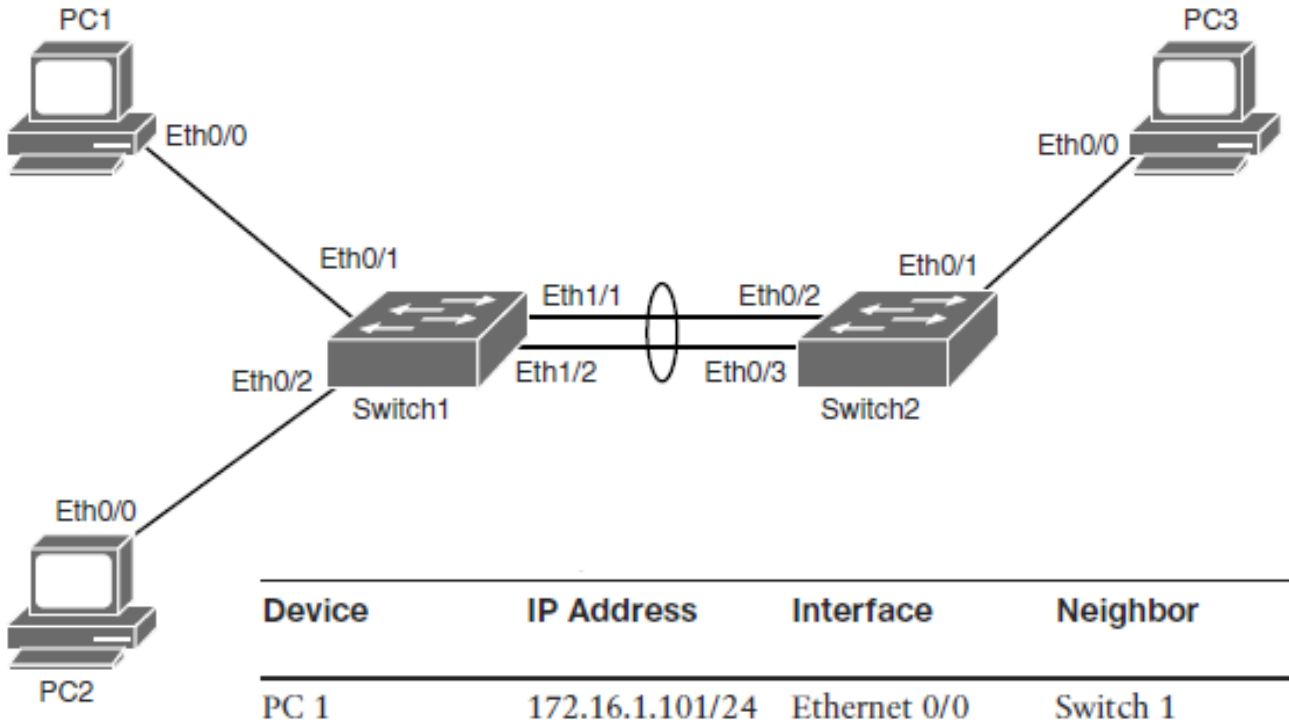
Layer 2 EtherChannel Configuration Guidelines

- **STP path cost**
  - Interfaces with different STP port path costs can form an EtherChannel as long as they are compatibly configured.
  - Setting different STP port path costs does not, by itself, make interfaces incompatible for the formation of an EtherChannel.
- **Port channel versus interface configuration**
  - After you configure an EtherChannel, any configuration that you apply to the port channel interface affects the EtherChannel.
  - Any configuration that you apply to the physical interfaces affects only the specific interface that you configured.

EtherChannel Load-Balancing Options

Hash Input Code	Hash Input Decision	Switch Model
dst-ip	Destination IP address	All models
dst-mac	Destination MAC address	All models
src-dst-ip	Source and destination IP address	All models
src-dst-mac	Source and destination MAC address	All models
src-ip	Source IP address	All models
src-mac	Source MAC address	All models
src-port	Source port number	4500, 6500
dst-port	Destination port number	4500, 6500
src-dst-port	Source and destination port number	4500, 6500

Configuring EtherChannel in a Switched Network



Device	IP Address	Interface	Neighbor	Interface on the Neighbor
PC 1	172.16.1.101/24	Ethernet 0/0	Switch 1	Ethernet 0/1
PC 2	172.16.1.102/24	Ethernet 0/0	Switch 1	Ethernet 0/2
PC 3	172.16.1.203/24	Ethernet 0/0	Switch 2	Ethernet 0/1
Switch 1	*No IP address*	Ethernet 1/1	Switch 2	Ethernet 0/2
Switch 1	*No IP address*	Ethernet 1/2	Switch 2	Ethernet 0/3

Configuring EtherChannel in a Switched Network

Step 1.

Configure the two ports that connect each switch to use channel group 1 and LACP active mode:

- `Switch1# configure terminal`
- `Switch1(config)# interface range Ethernet 1/1-2`
- `Switch1(config-if-range)# channel-group 1 mode active`
- `Creating a port-channel interface Port-channel 1`

Step 2.

Enter interface configuration mode for the newly created port channel interface and configure it for trunk mode using dot1Q:

- `Switch1(config)# interface port-channel 1`
- `Switch1(config-if)# switchport trunk encapsulation dot1q`
- `Switch1(config-if)# switchport mode trunk`

Configuring EtherChannel in a Switched Network

Step 3.

On Switch 1, enter the **show etherchannel summary** command:

```
Switch1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
1      Po1(SU)         LACP      Et1/1(P)    Et1/2(P)
```

Configuring EtherChannel in a Switched Network

Step 4.

- Enter the **show etherchannel load-balance** command to verify which information EtherChannel uses to load balance traffic:

```
Switch1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
```

Chapter 3 Summary

- Implementing VLANs and trunks in campus switched architecture
- Understanding the concept of VTP and its limitation and configurations
- Implementing and configuring EtherChannel

Chapter 3 Labs

- **CCNPv7.1 SWITCH Lab3.1 VLAN TRUNK VTP**
- **CCNPv7.1 SWITCH Lab3.2 ETHERCHANNEL**

Acknowledgment

- *Some of the images and texts are from Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: (CCNP SWITCH 300-115)* by Richard Froom and Erum Frahim (1587206641)
- Copyright © 2015 – 2016 Cisco Systems, Inc.
- Special Thanks to *Bruno Silva*