

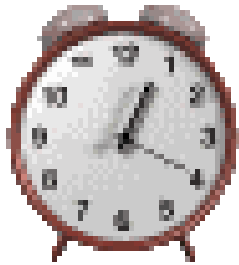
MODULE: XÂY DỰNG HẠ TẦNG MẠNG



- ✚ Bài 1: GIỚI THIỆU ROUTING VÀ PACKET FORWARDING
- ✚ Bài 2: LAYER 2 SWITCHING VÀ VIRTUAL LAN
- ✚ Bài 3: DISTANCE VECTOR ROUTING PROTOCOL
- ✚ Bài 4: LINK-STATE ROUTING PROTOCOL
- ✚ Bài 5: QUẢN LÝ TRAFFIC VỚI ACCESS LIST
- ✚ Bài 6: CẤU HÌNH TÍNH NĂNG NÂNG CAO CỦA CISCO IOS
- ✚ Bài 7: TRIỂN KHAI HIGH AVAILABILITY CHO HẠ TẦNG MẠNG
- ✚ ÔN TẬP
- ✚ BÁO CÁO ĐỒ ÁN CUỐI MÔN
- ✚ THI CUỐI MÔN



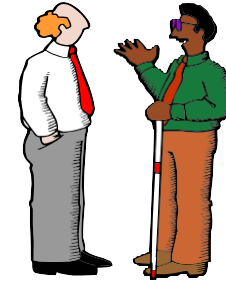
QUY ĐỊNH HỌC TẬP



Đúng giờ



Tắt chuông điện thoại



Lắng nghe



**Hỏi lại những gì
chưa hiểu**



**Đóng góp ý kiến
và chia sẻ kinh
nghiệm**



**Không hút thuốc
trong lớp học**

Cấu trúc hoạt động của bộ chuyển mạch (Switch layer 2)

- ✚ Chức năng của Switch Layer 2
- ✚ VLAN
- ✚ VLAN Trunking Protocol
- ✚ Spanning Tree Protocol (STP)
- ✚ Ôn tập

MỤC TIÊU BÀI HỌC

- ✚ Trình bày được chức năng của Switch Layer 2.
- ✚ Trình bày được khái niệm, đặc điểm và lợi ích của Virtual LAN.
- ✚ Giải thích được đặc điểm và lợi ích của VLAN Trunking Protocol.
- ✚ Giải thích được đặc điểm và cách hoạt động của Spanning Tree Protocol.
- ✚ Cấu hình được Spanning Tree Protocol.
- ✚ Xây dựng được VLAN cho doanh nghiệp.
- ✚ Cấu hình được VLAN Trunking Protocol.



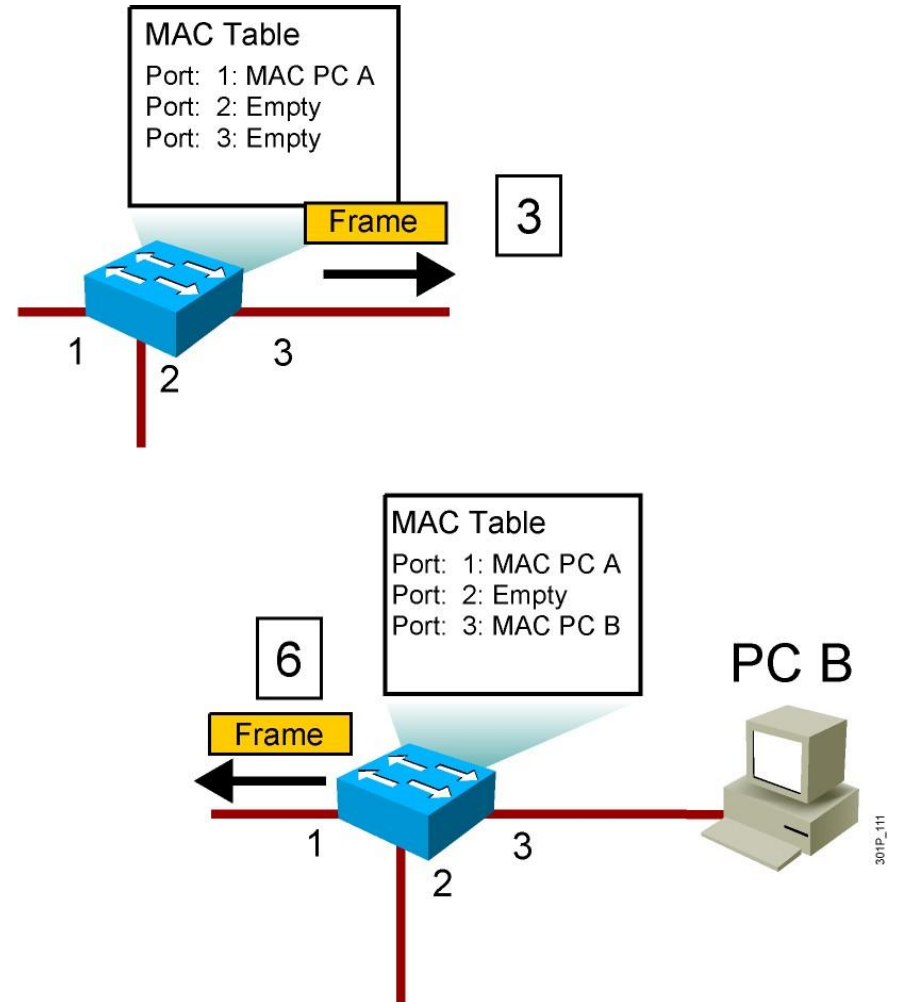
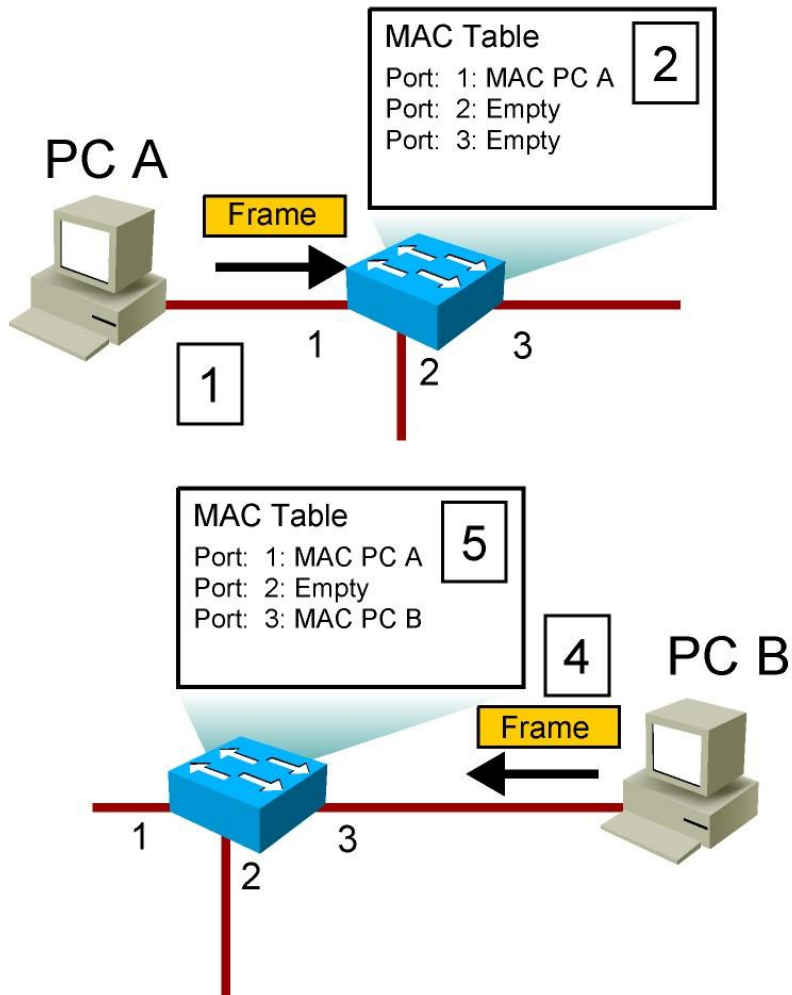
Chức năng của Switch Layer 2

Chức năng, hoạt động và ưu thế của Cisco Switch so với các Switch thường

Address learning

- ⊕ Chuyển các gói tin dựa trên bảng địa chỉ MAC (Content-Addressable Memory table).
- ⊕ Xác định vị trí của máy trạm dựa vào địa chỉ MAC nguồn.
- ⊕ Gửi gói tin ra tất cả các port khi địa chỉ MAC đích là Broadcast, multicast, hoặc không xác định trong bảng MAC.

Address learning

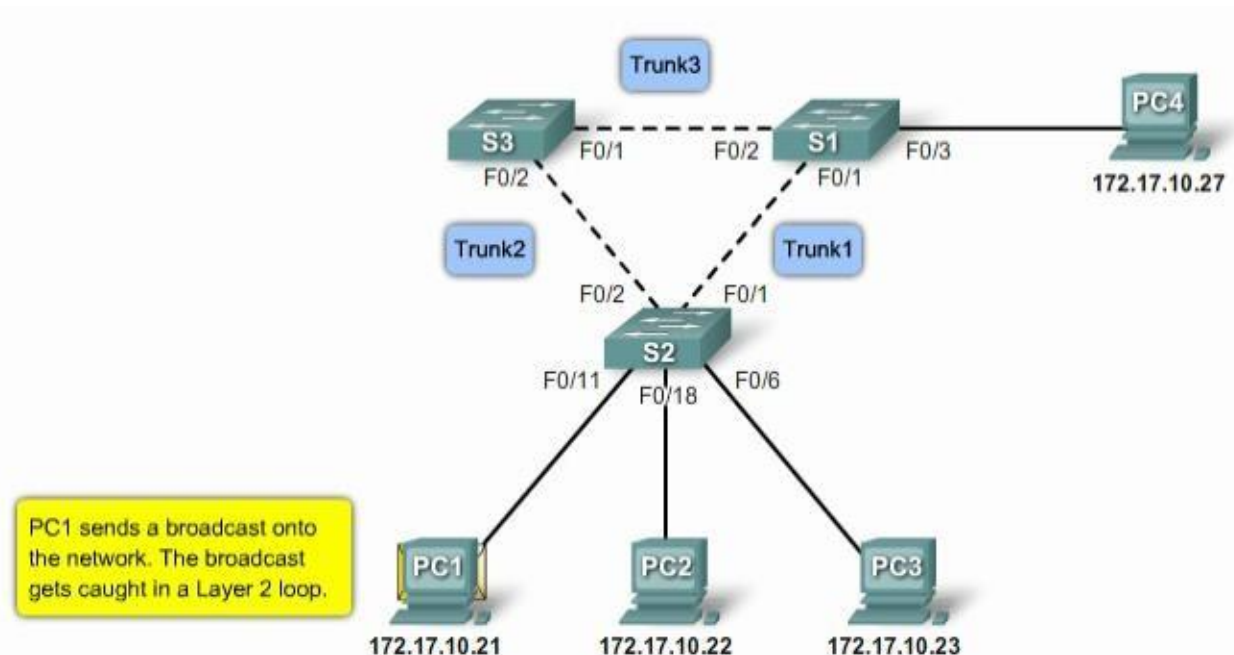


Forward/Filter

- ⊕ Khi 1 khung dữ liệu nhận vào trên 1 interface, Switch thấy được địa chỉ MAC đích và tìm kiếm trong MAC database.
- ⊕ Khung dữ liệu chỉ được chuyển ra ngoài tới 1 cổng đích chỉ định.

Loop Avoidance

- ✦ Nếu có nhiều các kết nối giữa các thiết bị chuyển mạch được tạo ra với mục đích dự phòng, vòng lặp có thể xảy ra trong hệ thống mạng.
- ✦ Spanning Tree Protocol (STP) được sử dụng để ngăn chặn hiện tượng vòng lặp.

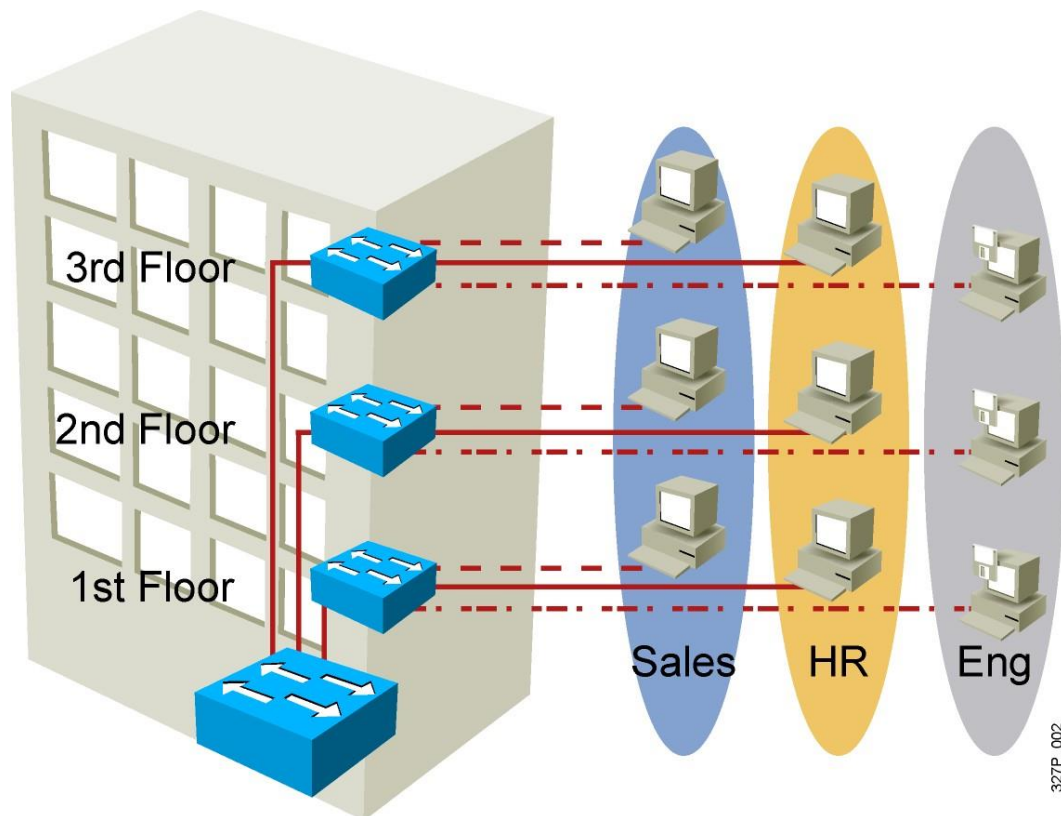


Mạng LAN ảo là cơ chế dùng để phân chia Broadcast Domain

✚ Khái niệm VLAN

✚ Giới thiệu VLAN

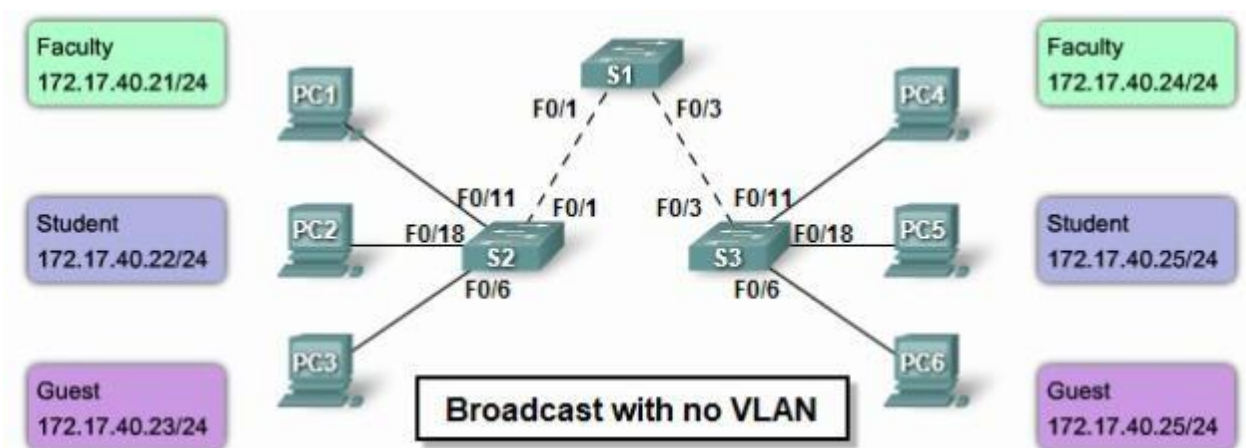
- ✚ Dễ phân chia
- ✚ Linh động
- ✚ Bảo mật



Khái niệm VLAN

Broadcast Control

- ✦ Những ứng dụng chiếm nhiều băng thông thường là các ứng dụng đa phương tiện thường sử dụng Broadcast và Multicast.
- ✦ Hệ thống mạng kiểu mới được tạo ra nhằm hạn chế tình trạng thiết bị bị lỗi, phân khúc hệ thống và nâng cao độ bảo mật.



Khái niệm VLAN

VLAN types

Static VLAN

- VLAN tĩnh là cách phổ biến nhất để tạo VLAN, và cũng là cách bảo mật nhất.
- Các port của VLAN luôn luôn được duy trì đến khi người quản trị thay đổi.

Khái niệm VLAN

VLAN types

Dynamic VLAN

- Thiết lập VLAN dựa trên MAC address, protocol, application.
- MAC address của máy nào đó đã được nhập vào 1 ứng dụng quản lý tập trung VLAN.
- Nếu 1 node mạng được gắn vào 1 cổng không được chỉ định trên switch, VLAN có thể dò tìm địa chỉ phần cứng và ấn định cấu hình các cổng chuyển đổi vào đúng VLAN.

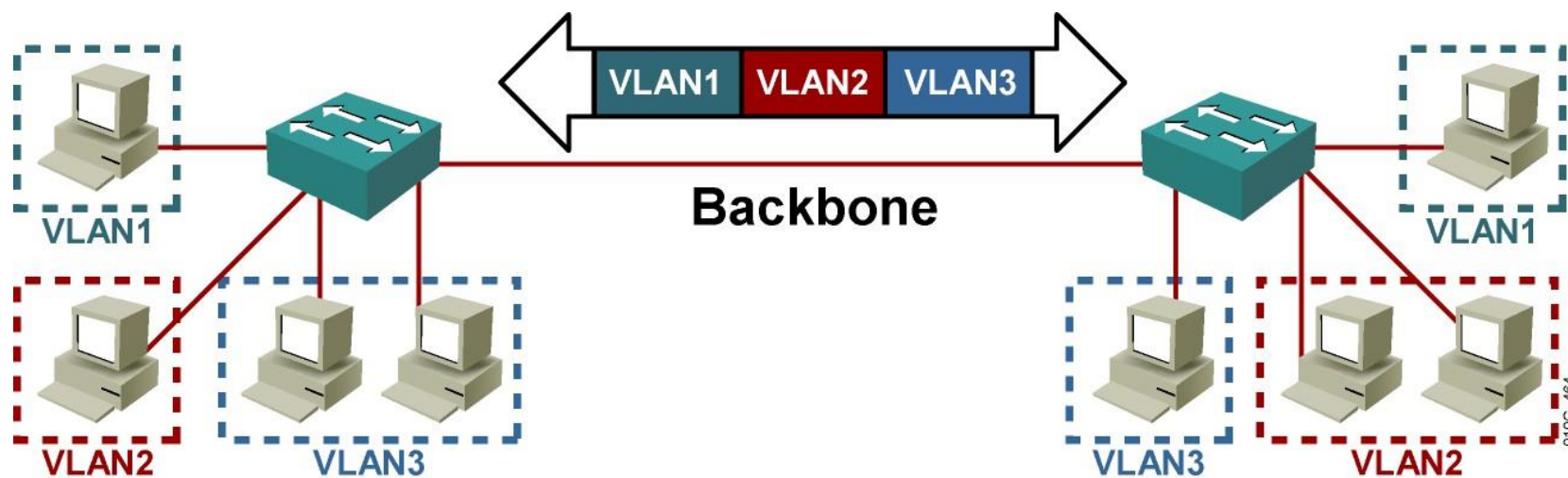
Khái niệm VLAN

Lợi ích của VLAN

-  Bảo mật.
-  Giảm chi phí.
-  Hiệu suất cao.
-  Giảm thiểu tình trạng “Broadcast storm”.
-  Nâng cao hiệu suất làm việc của IT.

Trunking

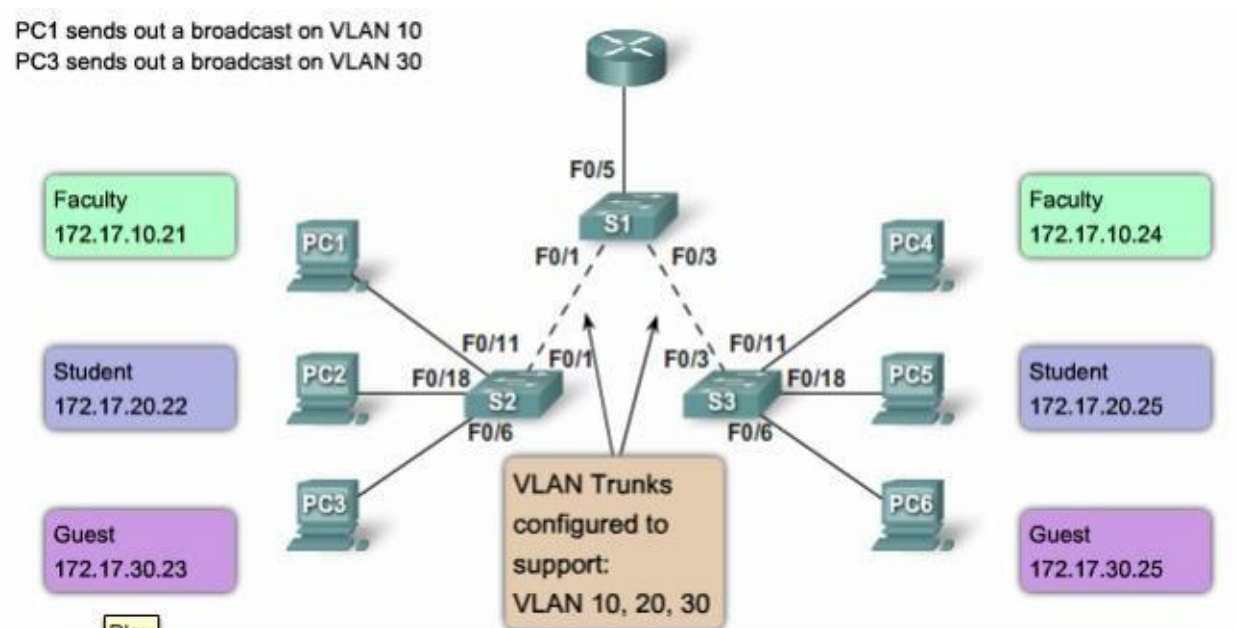
⊕ Khái niệm trunking



Trunking

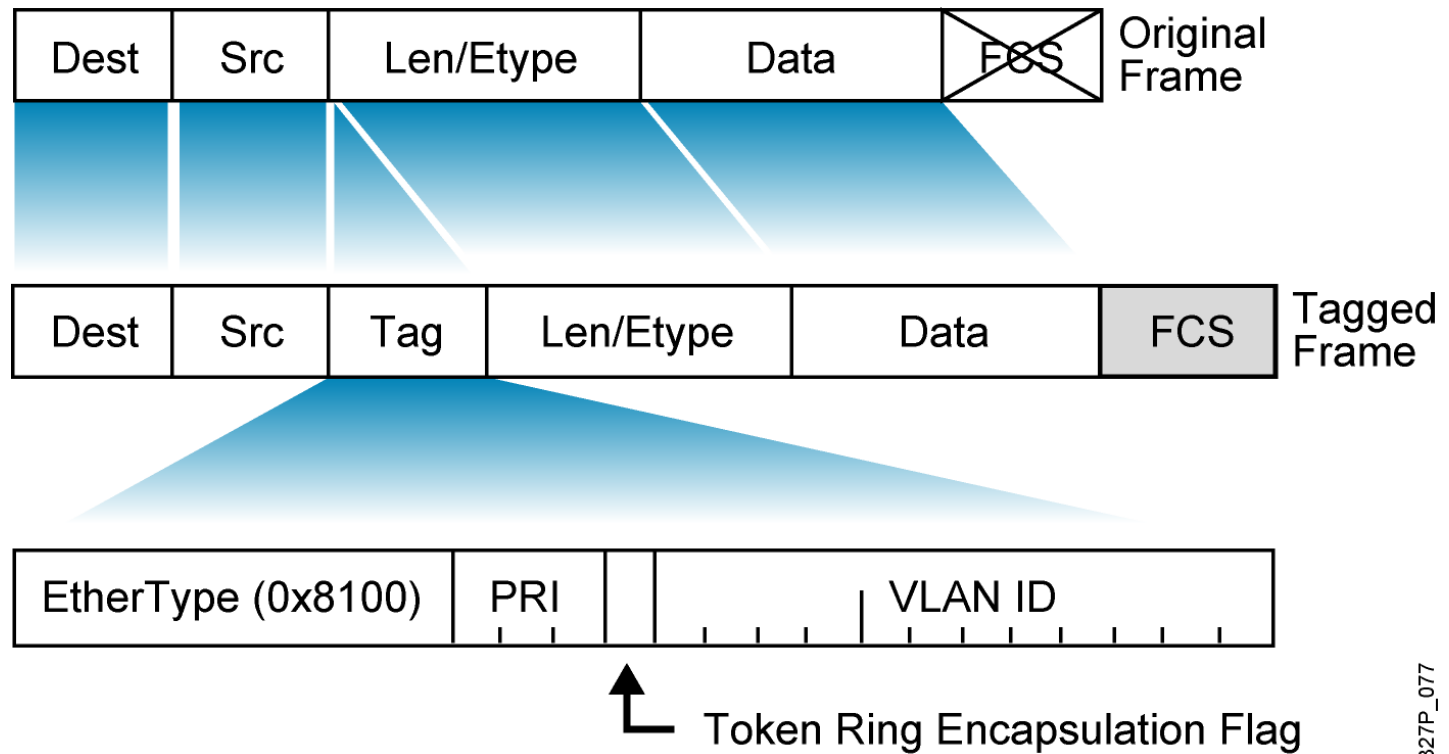
Trunking trong VLAN

-  Kết nối trunk truyền tải luồng dữ liệu của nhiều VLAN trên 1 kết nối duy nhất.
-  Cisco hỗ trợ chuẩn 802.1Q làm việc được trên Fast Ethernet và Gigabit Ethernet.



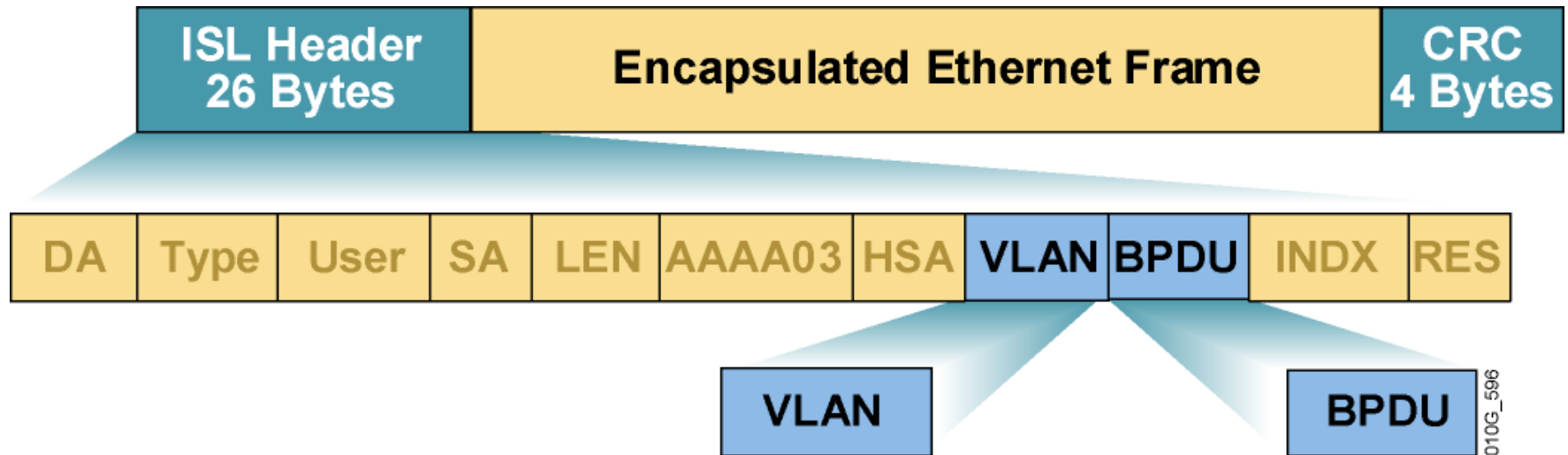
Trunking

Frame Tag: 802.1Q



Trunking

Frame Encapsulation: ISL



Trunking

Frame Tag/Encapsulation - 802.1Q/ISL

ISL	802.1Q
Proprietary	Nonproprietary
Encapsulated	Tagged
Protocol independent	Protocol dependent
Encapsulates the old frame in a new frame	Adds a field to the frame header

Cấu hình VLAN

Tạo VLAN

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

```
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#
```

Cấu hình VLAN

Gán Port vào 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

Cấu hình VLAN

 Gán Port vào VLAN

 Kiểm tra

```
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	

Cấu hình VLAN

 Gán Port vào VLAN

 Kiểm tra

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 ----
```

Cấu hình VLAN

Cấu hình Trunking

SwitchX(config-if) #

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

SwitchX(config-if) #

```
switchport mode trunk
```

Cấu hình VLAN

Kiểm tra một kết nối 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
```

VTP là cơ chế quy hoạch VLAN cho toàn hệ thống Switch trong cùng một Domain, giảm tối đa thời gian cho việc cấu hình VLAN

VTP

⊕ Khái niệm

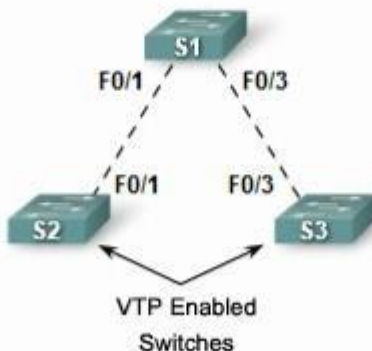
- ⊕ Mục tiêu cơ bản của VLAN Trunking Protocol (VTP) là để quản lý tất cả các cấu hình VLAN trên một mạng chuyển mạch, duy trì tính nhất quán trong cả mạng lưới.
- ⊕ VTP cho phép một quản trị viên có thể thêm, xóa, và đổi tên VLAN mà sau đó được truyền đến tất cả các switch khác trong VTP domain.

VTP

⊕ Đặc điểm VTP Protocol:

- ⊕ Cấu hình VLAN nhất quán trong tất cả các thiết bị chuyển mạch trong mạng tham gia vào VTP Domain.
- ⊕ Thiết lập VLAN Trunking trên nhiều loại mạng như: ATM LANE, FDDI.
- ⊕ Theo dõi và giám sát chính xác các VLAN.
- ⊕ Báo cáo của VLAN được gửi đến tất cả các switch trong VTP Domain.
- ⊕ Giảm thời gian cấu hình cho người quản trị.

VTP



⊕ Revision Number:

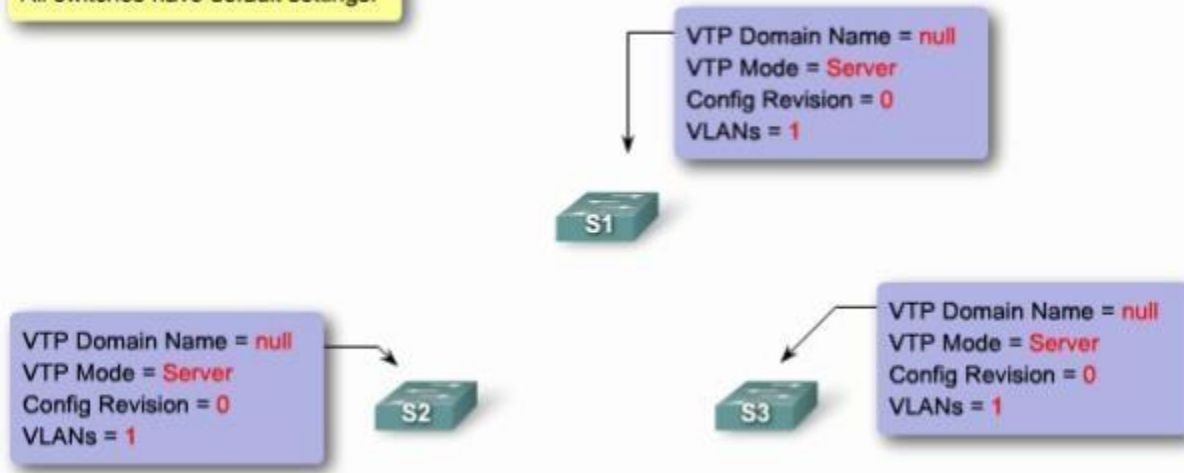
- ⊕ Là số phiên bản của một VTP Domain.
- ⊕ Số Revision sẽ tự động tăng lên một với mỗi sự thay đổi VLAN (thêm, xoá, sửa) trên Server.
- ⊕ Nếu trong cùng Domain có trên 1 Server, Server nào có số Revision lớn hơn, các Switch khác sẽ học VLAN từ Server đó.

VTP

VTP Mode

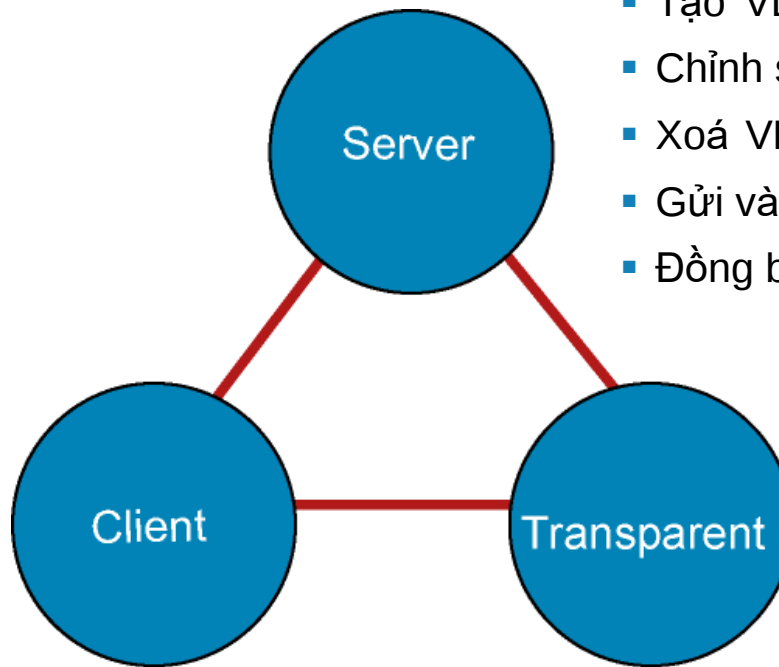
-  Server.
-  Client.
-  Transparent.

All switches have default settings.



VTP

VTP Mode



- Tạo VLAN
- Chỉnh sửa VLAN
- Xoá VLAN
- Gửi và chuyển tiếp các gói tin quảng bá
- Đồng bộ các VLAN cho Client

- Chỉ tạo local VLAN
- Chỉ chỉnh sửa local VLAN
- Chỉ xoá local VLAN
- Chuyển tiếp các gói tin quảng bá
- Không đồng bộ với Server

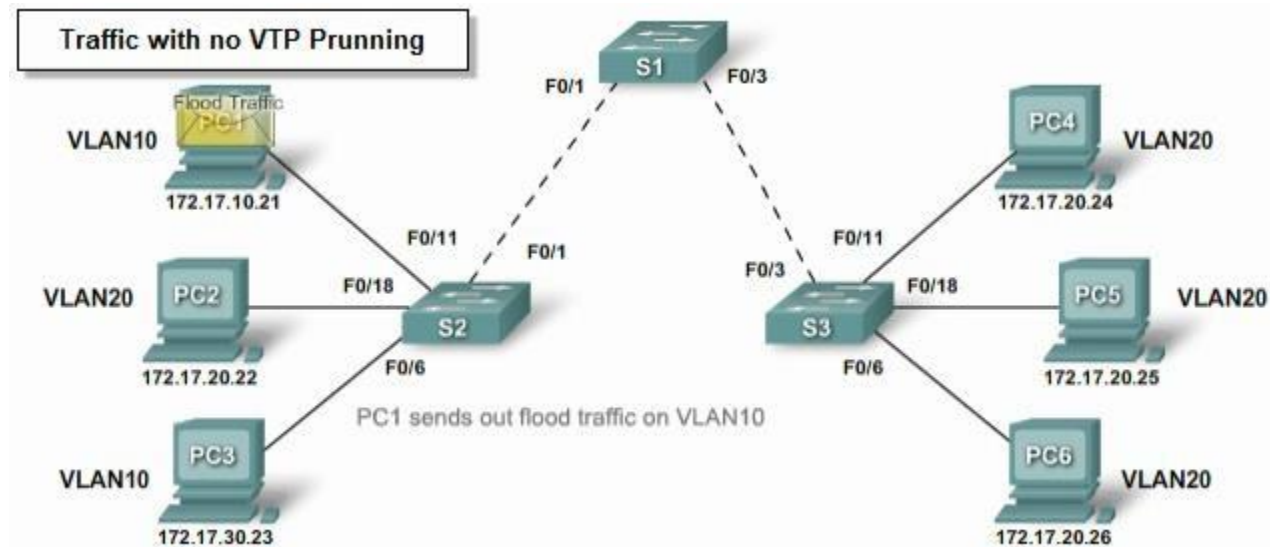
- Không thể tạo, sửa, xoá VLAN
- Gửi và chuyển tiếp các gói tin quảng bá
- Đồng bộ với Server

327P_078

VTP

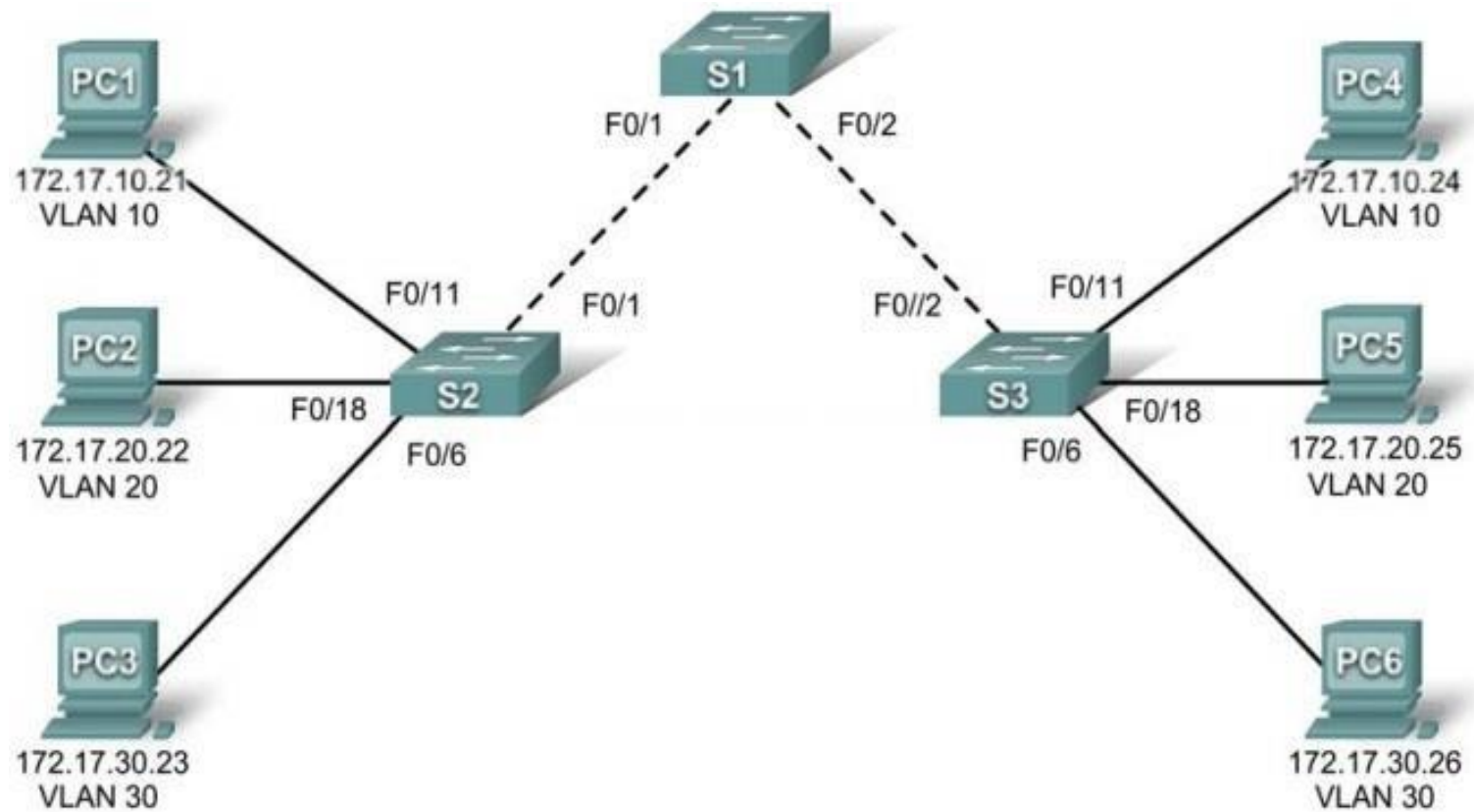
VTP Pruning

- ✦ VTP cung cấp 1 cách để bạn có thể bảo quản băng thông bằng cách cấu hình switch nhằm giảm lưu lượng broadcasts, multicasts, và unicast.
- ✦ VTP Pruning chỉ gửi các gói tin broadcast trên kết nối trunk mà thực sự phải có thông tin (có sự hiện diện đầu cuối).



VTP

Cấu hình VTP



VTP

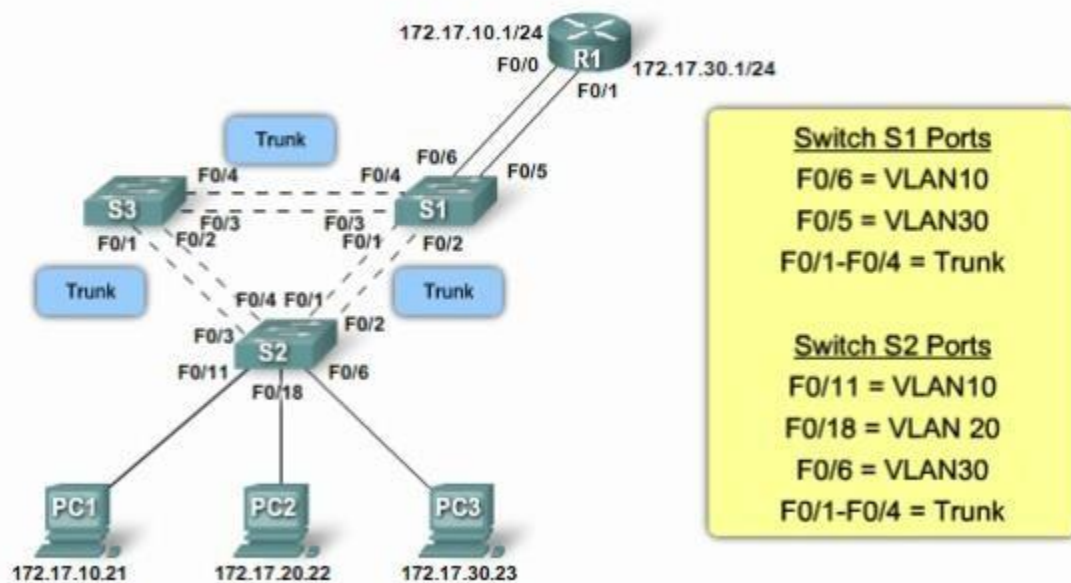
Cấu hình VTP

Step	Task	Command
Step 0	Định nghĩa VTP mode (server/client/transparent)	vtp mode <i>server client transparent</i>
Step 1	Định tên VTP domain	vtp domain <i>name</i>
Step 2	Đặt version cho VTP	vtp version <i>1 2</i>
Step 3	Đặt password cho VTP Domain	vtp password <i>password</i>
Step 4	Kiểm tra trạng thái VTP	show vtp status

Giúp cho các Host trong các VLAN khác nhau có thể liên lạc được với nhau

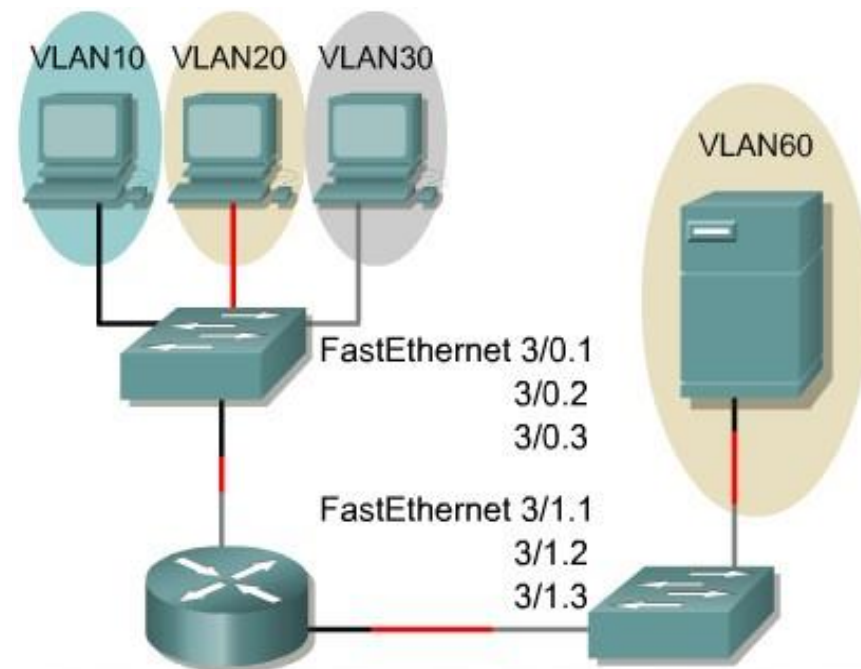
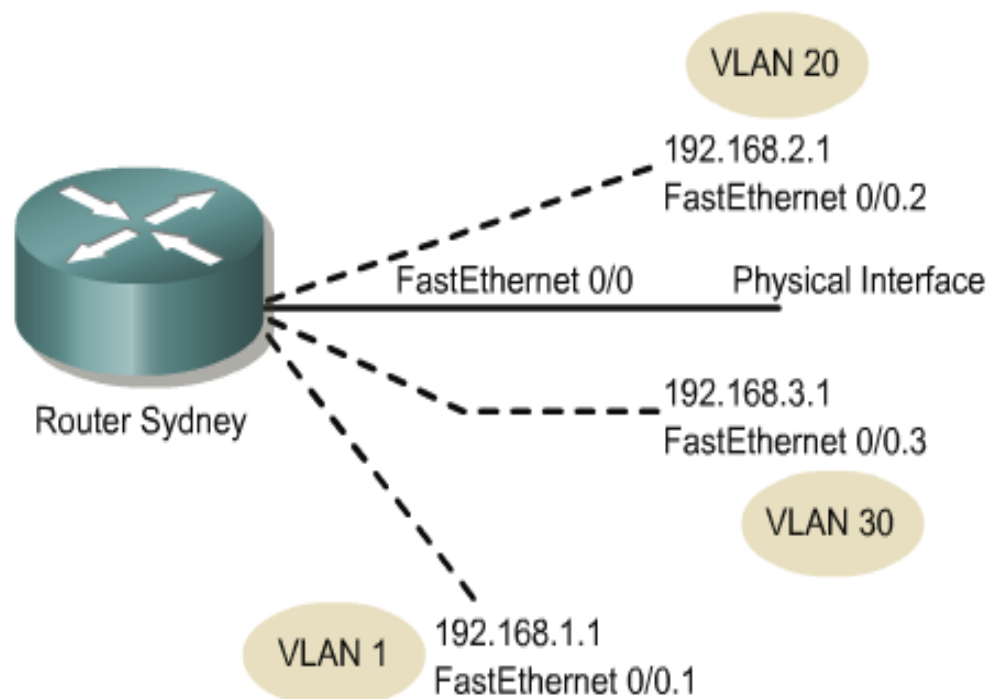
✚ Inter-VLAN Routing

⊕ Kết nối giữa các VLAN



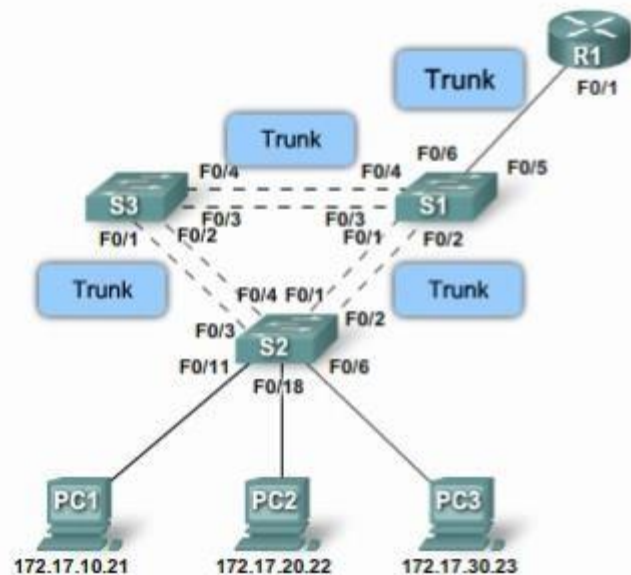
Inter-VLAN Routing

Giao tiếp vật lý và luận lý



A single ISL link can support multiple VLANs.

Inter-VLAN Routing



R1 Subinterfaces

F0/0.10: 172.17.10.1

F0/0.20: 172.17.20.1

F0/0.30: 172.17.30.1

Switch S1 Ports

F0/1-F0/4 = Trunk

F0/5 = Trunk

Switch S2 Ports

F0/11 = VLAN10

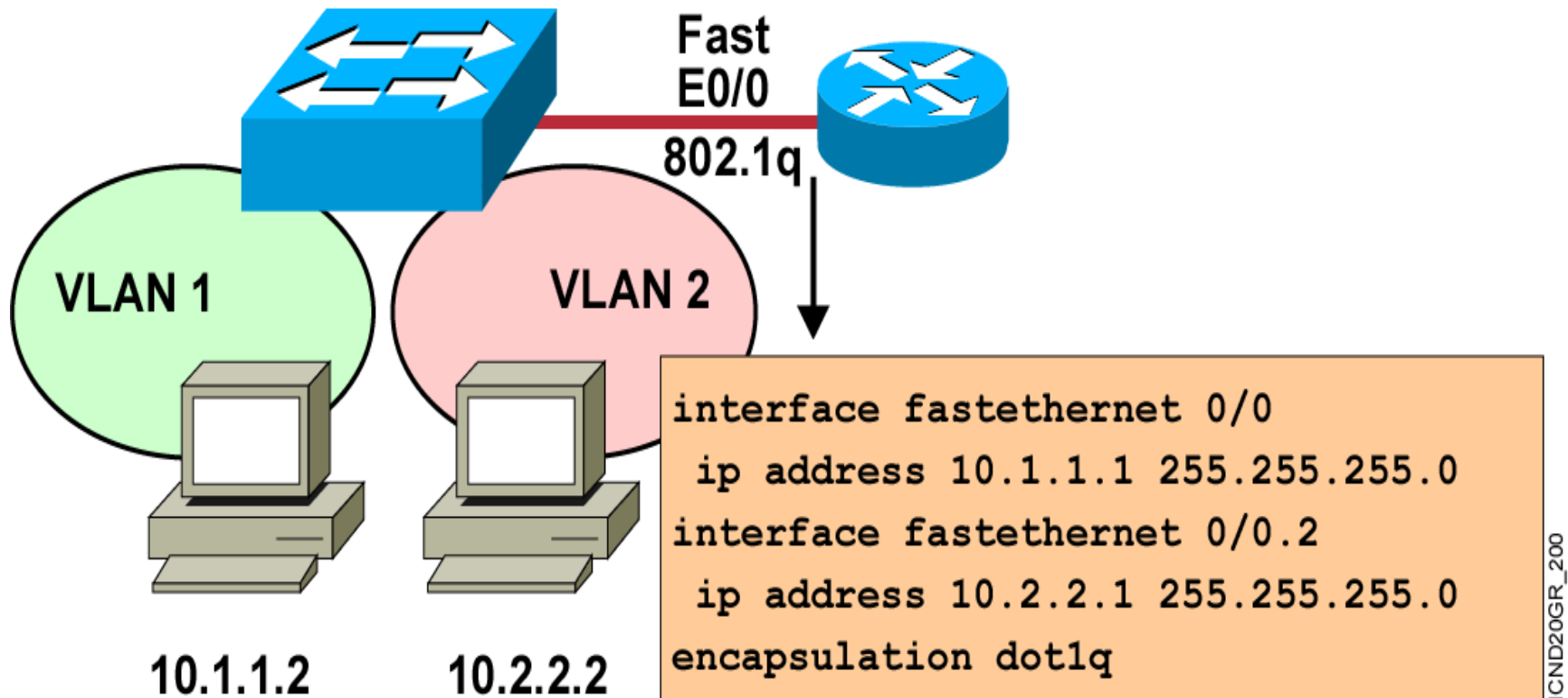
F0/18 = VLAN20

F0/6 = VLAN30

F0/1-F0/4 = Trunk

Inter-VLAN Routing

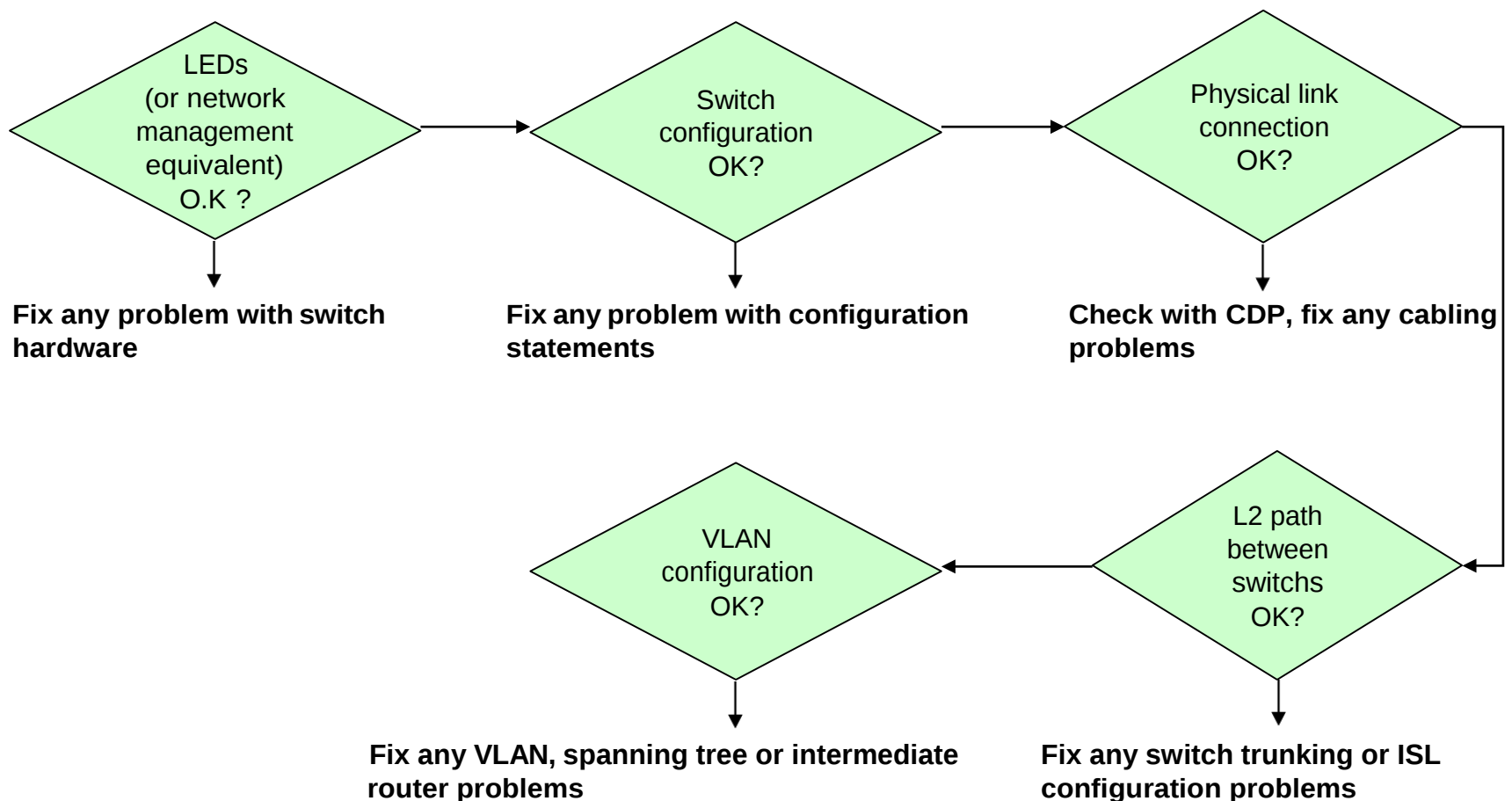
Cấu hình Inter-VLAN routing





Khắc phục lỗi VLAN

⊕ Tiến trình khắc phục lỗi VLAN



Khắc phục lỗi VLAN

Ngăn chặn Broadcast storm

-  Thiết lập các giá trị ngưỡng quá cao hoặc quá thấp để loại bỏ sự dư thừa tín hiệu broadcast, multicast, or unicast.

```
Switch# configure terminal
```

```
Switch(config)# interface gigabitethernet0/1
```

```
Switch(config-if)# storm-control broadcast level 20
```

Giảm tối thiểu quá trình STP diễn ra trên thiết bị

- Portfast.
- Uplinkfast.
- Backbonefast.

Khắc phục lỗi VLAN

- ⊕ Lệnh dùng khắc phục sự cố
 - ⊕ Show VLAN
 - ⊕ Show spanning-tree
 - ⊕ Show vlan
 - ⊕ Debug vlan packet

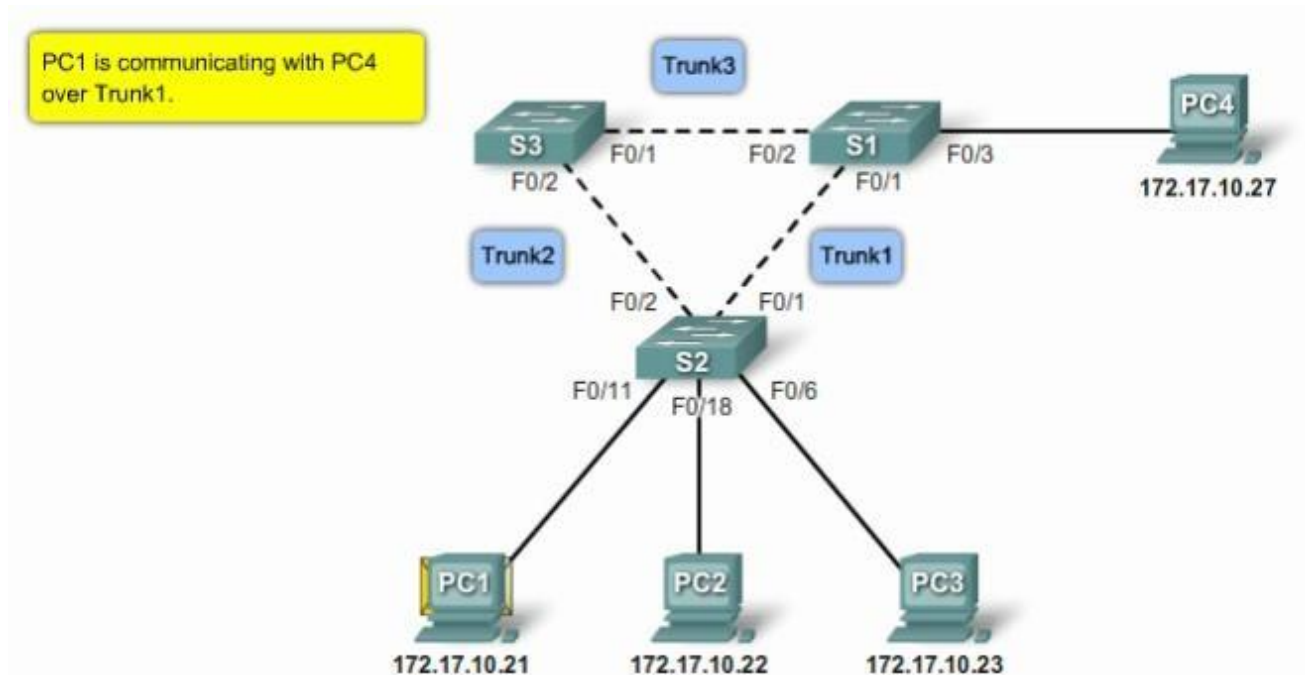
Khắc phục lỗi VLAN

Các trường hợp lỗi thông dụng

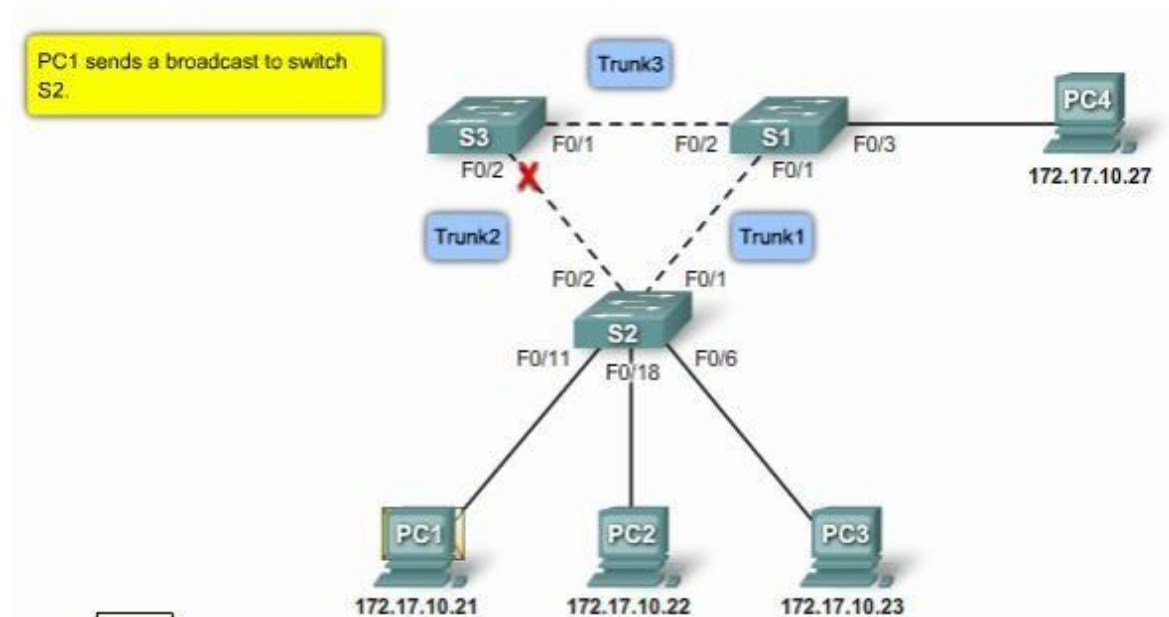
-  Kết nối trunk không được thiết lập giữa các Switch hoặc Switch với Router.
-  VTP không được cấu hình đúng.
-  Rút gói tin và vòng lặp.

Khái niệm các thành phần, hoạt động, thuật toán chống Loop của Spanning Tree

Redundant Topology



Redundance Topology và STP



Các thuật ngữ

BPDU

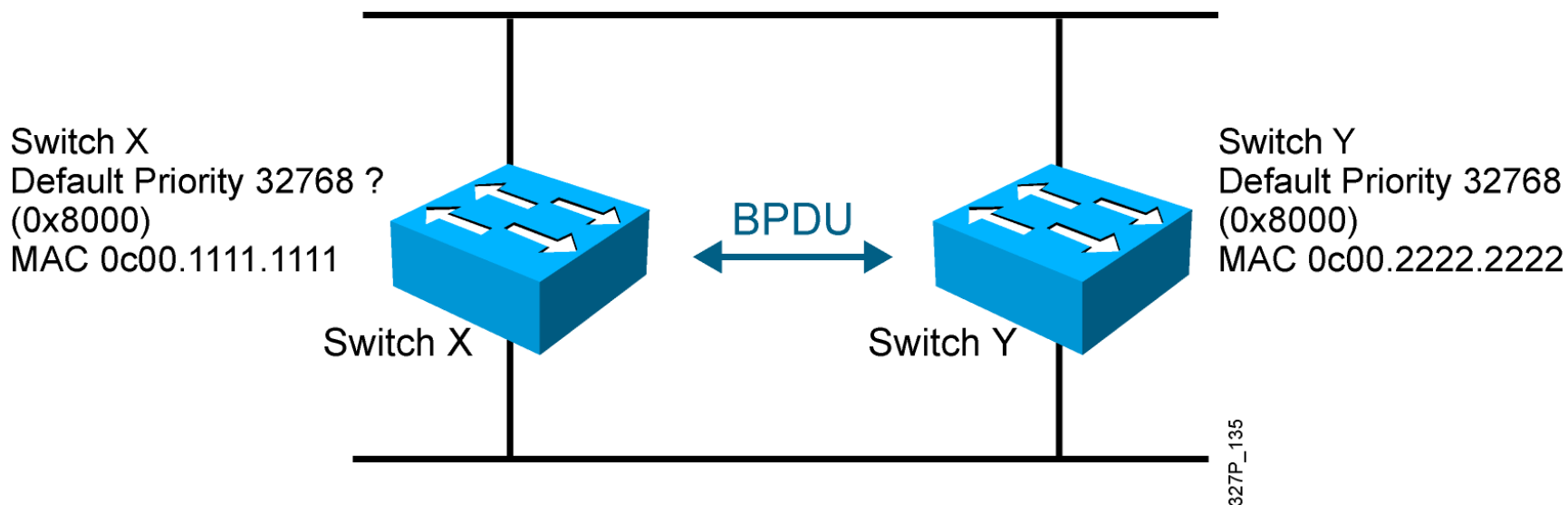
-  Sau khi Switch khởi động, nó sẽ gửi ra gói BPDU chứa Switch Bridge ID và Root ID.
-  BPDU mang thông tin thiết lập STP của Switch.
-  ID phù hợp với Bridge ID cho tất cả các thiết bị chuyển mạch.
-  BPDU được gửi đi mỗi 2 giây.

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hellotime
2	Forward delay

Các thuật ngữ

STP/Root Bridge

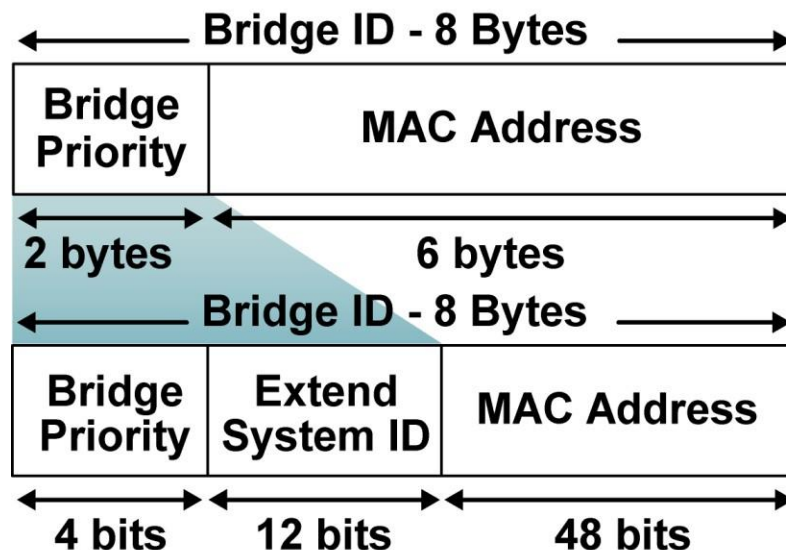
-  Root bridge như 1 điểm tham chiếu cho tất cả các tính toán Spanning-tree để tạo đường đi dự phòng ngăn chặn.
-  SW nào có Bridge ID nhỏ nhất sẽ được chọn làm Root Bridge.



Các thuật ngữ

Bridge ID

-  Được xác định bằng cách kết hợp độ ưu tiên Bridge và Mac address.
-  Bridge với số Bridge ID thấp nhất sẽ được chọn làm Root Bridge trên hệ thống mạng.

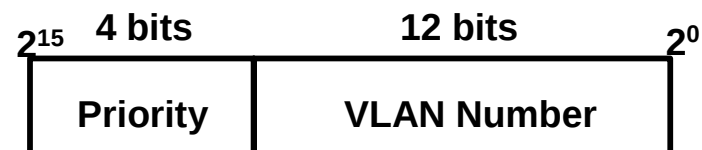


Các thuật ngữ

Bridge ID

 Ví dụ về Extended ID cho VLAN 12: Nếu trường Priority là default (8 – Hex), ta đổi 8 từ Hexa sang Decimal.

**Bridge Priority = 32768
+ 12 = 32780.**



Priority Values (Hex)

0
1
2
.
.
8 (default)
.
.
F

Priority Values (Dec)

0
4096
8192
.
.
32768
.
.
61440

Các thuật ngữ

Path cost

-  Đánh số cho bảng thông các kết nối.
-  Dùng trong thuật toán xây dựng STP.

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Các thuật ngữ

Root port

-  Root port là đường kết nối trực tiếp tới Root bridge, hoặc đường kết nối ngắn nhất tới Root bridge.
-  Nếu có nhiều kết nối tới Root bridge, giá trị port (Port cost) được xác định bằng cách kiểm tra bảng thông của mỗi đường kết nối.
-  Giá trị port thấp nhất sẽ được chọn làm Root port.
-  Nếu có nhiều kết nối có cùng giá trị, bridge với giá trị quảng bá bridge ID thấp nhất được chọn.

Các thuật ngữ

⊕ Nonroot Bridge:

- ⊕ Đây là tất cả các Bridge mà không phải là Root Bridge.
- ⊕ Nonroot Bridge trao đổi BPDU với tất cả Bridge và cập nhật dữ liệu mô hình STP trên các thiết bị chuyển mạch.
- ⊕ Cung cấp 1 biện pháp phòng vệ chống lại hiện tượng liên kết bị lỗi (Link Failures).

⊕ Forwarding Port:

- ⊕ Chuyển tiếp các gói tin.

⊕ Designated Port:

- ⊕ Designated Port được xác định khi nó không phải Root port và có giá trị Local Path cost thấp nhất.
- ⊕ Designated Port sẽ được đánh dấu như là 1 Forwarding Port.

Các thuật ngữ

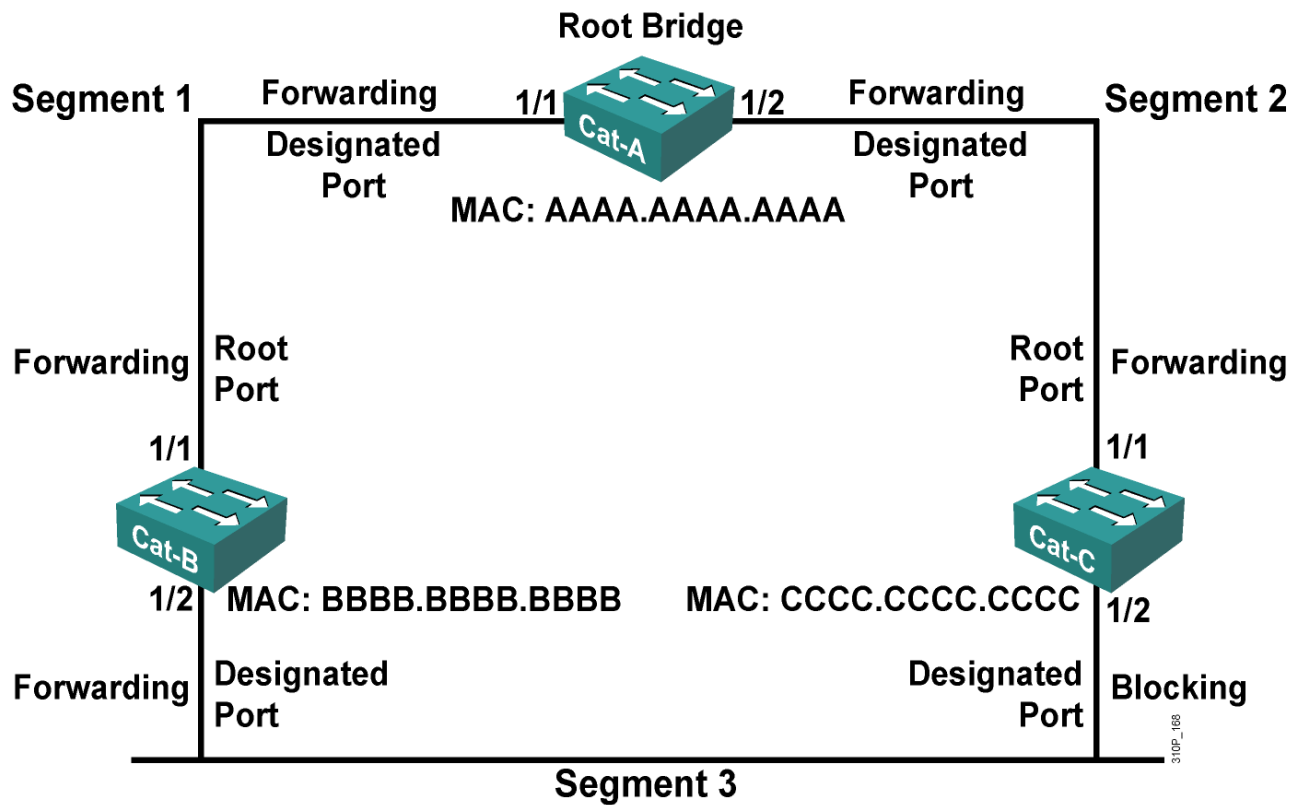
⊕ Nondesignated Port:

- ⊕ Nondesignated Port có Path Cost cao hơn Designated Port.
- ⊕ Nondesignated Port được đặt ở chế độ chặn (blocking mode).
- ⊕ Chúng không phải là Forwarding Port.

⊕ Blocked port:

- ⊕ Blocked port sẽ không chuyển tiếp khung, để ngăn chặn vòng lặp.
- ⊕ Tuy nhiên Blocked Port vẫn lắng nghe các BPDU.

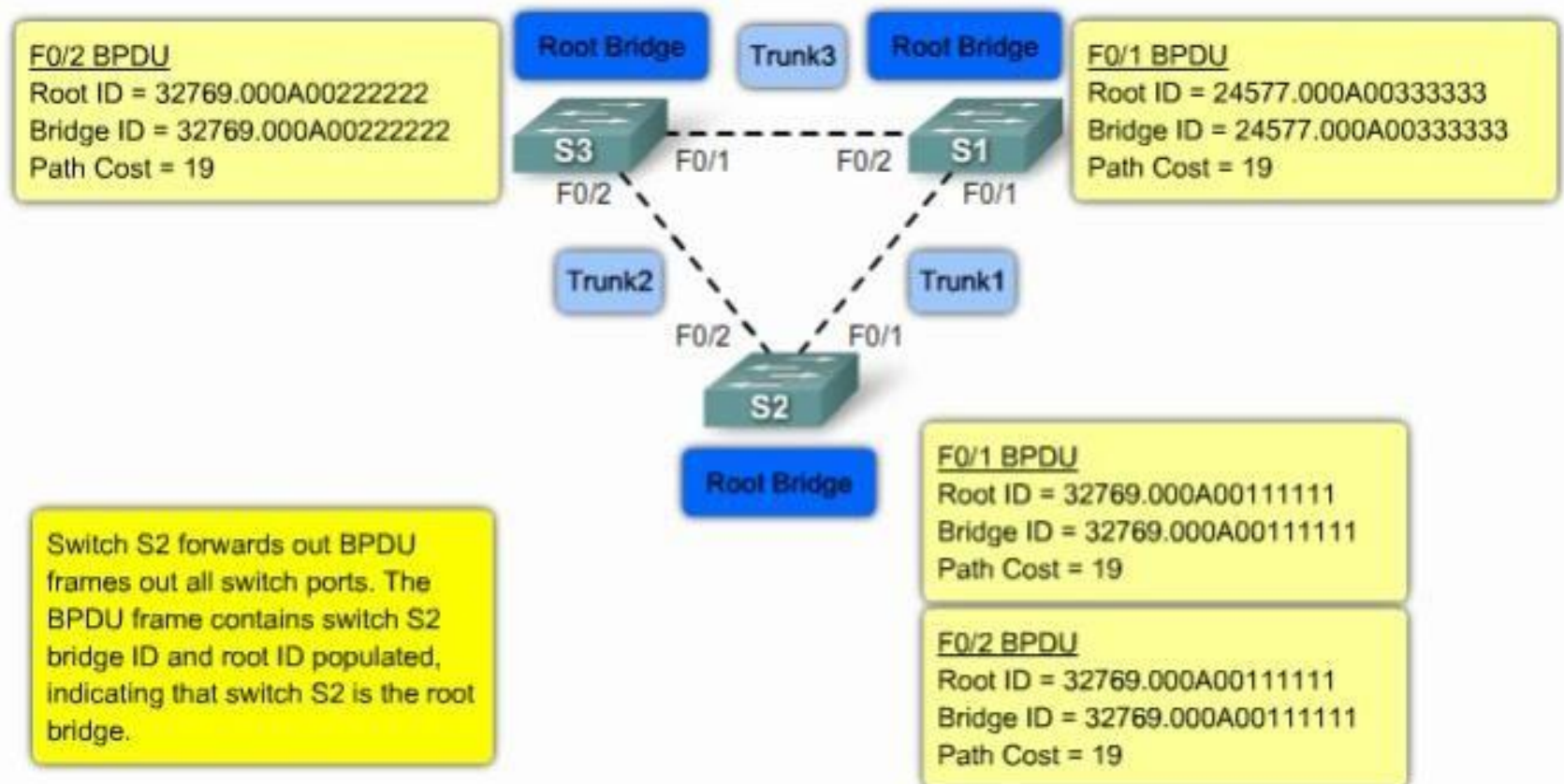
Các thuật ngữ



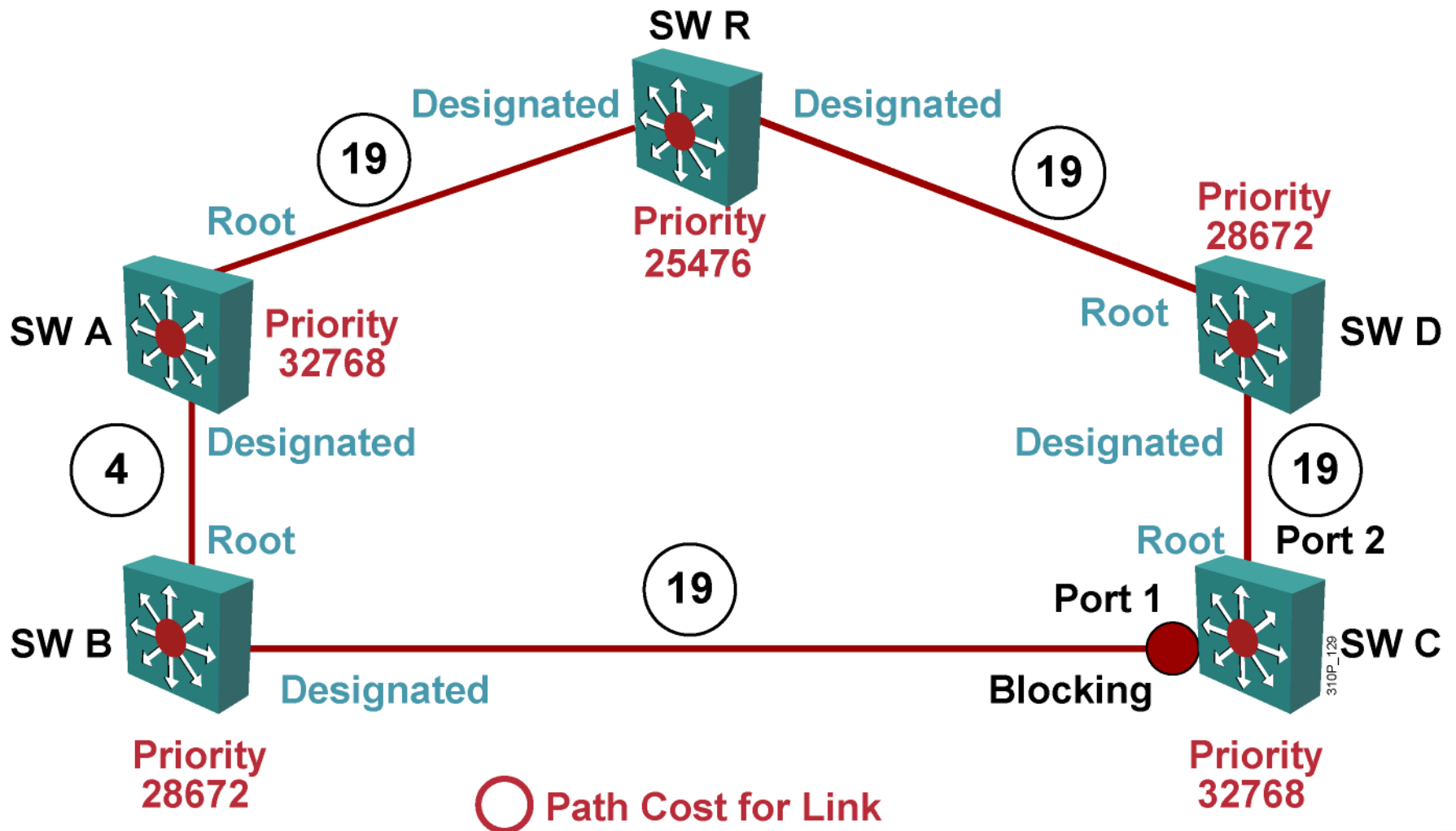
Spanning-tree Operation

- ⊕ Nhiệm vụ của STP là tìm tất cả các liên kết trong mạng và tắt bất kỳ các kết nối dư thừa, do đó nó ngăn chặn hiện tượng vòng lặp xảy ra.
- ⊕ STP thực hiện điều này bằng cách bầu chọn một Root Bridge có tác dụng như một điểm tham chiếu cho tất cả các thiết bị khác trong việc tính toán STP.

Lựa chọn STP RootBridge



STP Role Vote



Spanning-Tree Port States

Blocking:

-  Trạng thái ban đầu khi chưa tham gia vào quá trình bầu chọn STP.
-  Không chuyển khung dữ liệu.
-  Không xây dựng bảng MAC.
-  Nhận BPDU nhưng không gửi ra.

Listening:

-  Cổng nhận truyền và xử lý BPDU.
-  Không chuyển khung dữ liệu.
-  Không xây dựng bảng MAC.

Spanning-Tree Port States

⊕ Learning:

- ⊕ Lắng nghe các gói BPDU và học tất cả các đường dẫn trong mạng chuyển mạch.
- ⊕ Không chuyển khung dữ liệu.
- ⊕ Bắt đầu xây dựng bảng MAC.

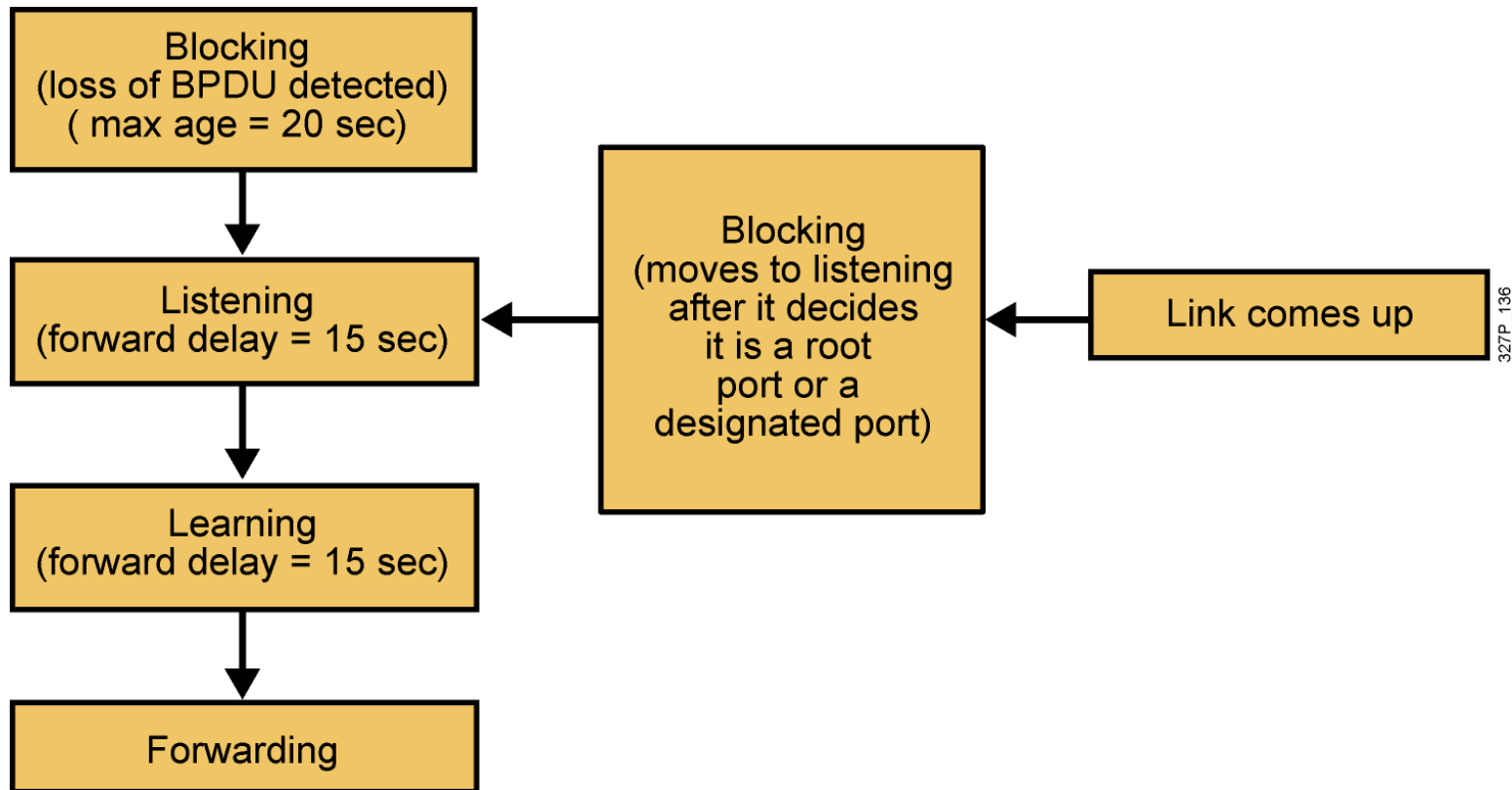
⊕ Forwarding:

- ⊕ Cổng nhận và gửi tất cả các khung dữ liệu.
- ⊕ STP luôn giám sát các gói BPDU để kịp thời ngăn Loop khi có sự cố.

⊕ Disable

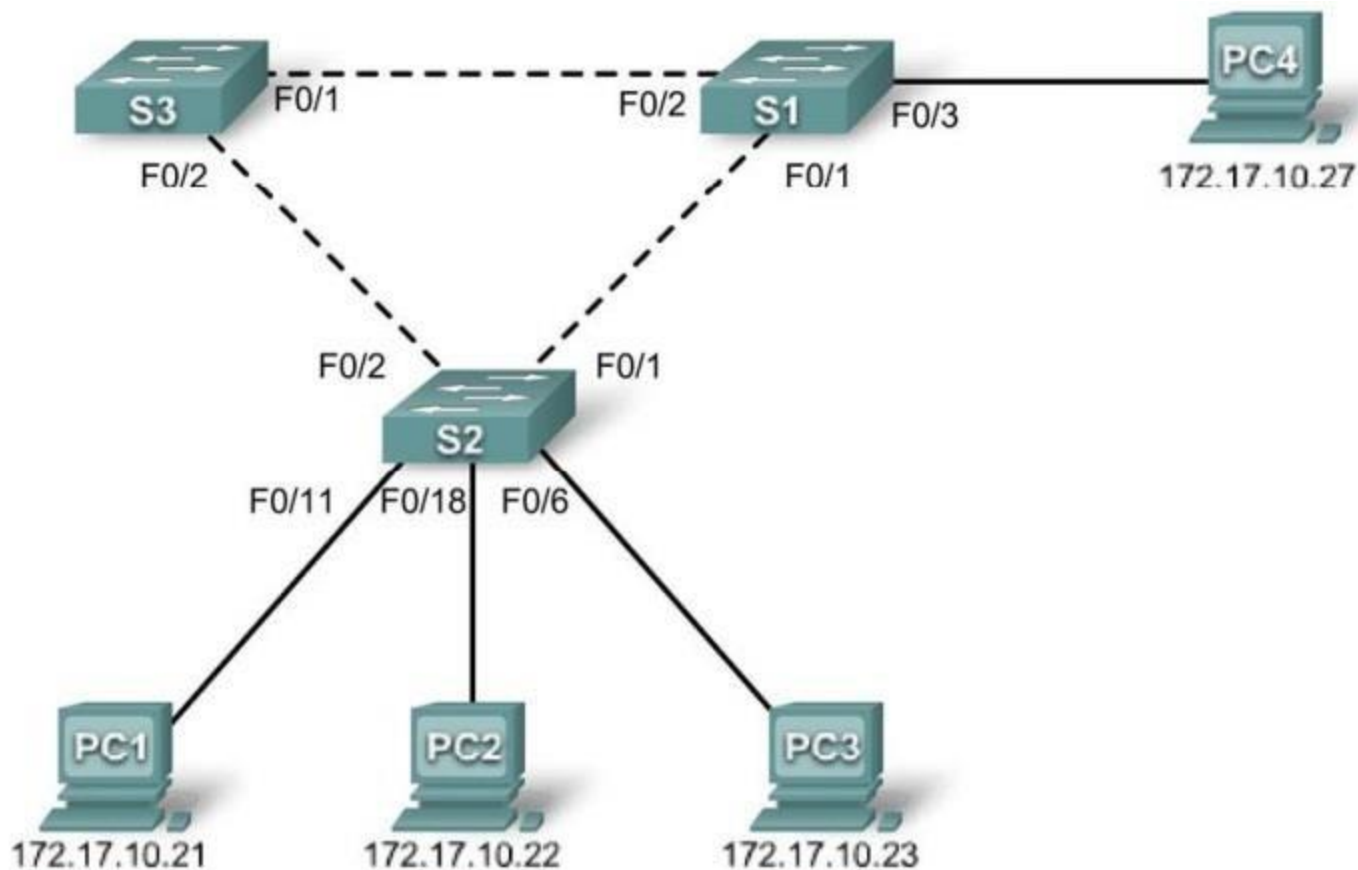
- ⊕ 1 cổng ở trạng thái Disable không tham gia vào quá trình gửi khung hoặc STP được cấu hình bởi người quản trị.

Spanning-Tree Port States



✚ Ví dụ Spanning Tree

⊕ STP Topology



✚ Ví dụ Spanning Tree

⊕ STP Topology

S2#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769
 Address 0019.068d.6980
 Cost 19
 Port 1 (FastEthernet0/1)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
 Address 001b.0c68.2080
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/11	Desg	FWD	19	128.11	P2p
Fa0/18	Desg	FWD	19	128.18	P2p

Cấu hình STP

Các bước cấu hình

-  Cấu hình cơ bản trên Switch.
-  Cấu hình các Interfaces trên các Host PC.
-  Cấu hình VLAN.
-  Cấu hình Spanning tree.
-  Tối ưu Spanning tree.

Cấu hình STP

```
Switch(config) #spanning-tree vlan 1 root primary
```

⊕ Cấu hình một Switch trở thành Root.

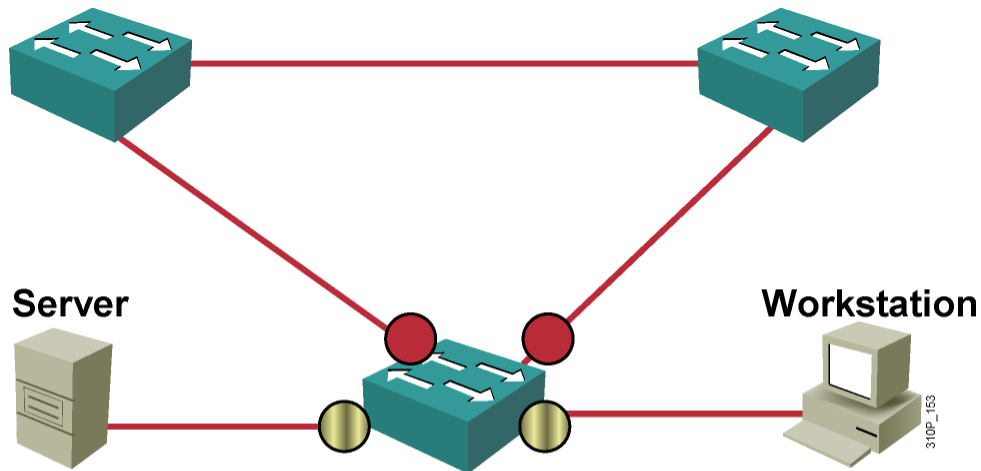
```
Switch(config) #spanning-tree vlan 1 root secondary
```

⊕ Cấu hình một Switch trở thành Secondary Root.

```
Switch(config) #spanning-tree vlan 1 priority priority
```

⊕ Cấu hình Priority cho 1 Switch (Bội số của 4096).

Cấu hình STP Portfast



On these access switch ports:

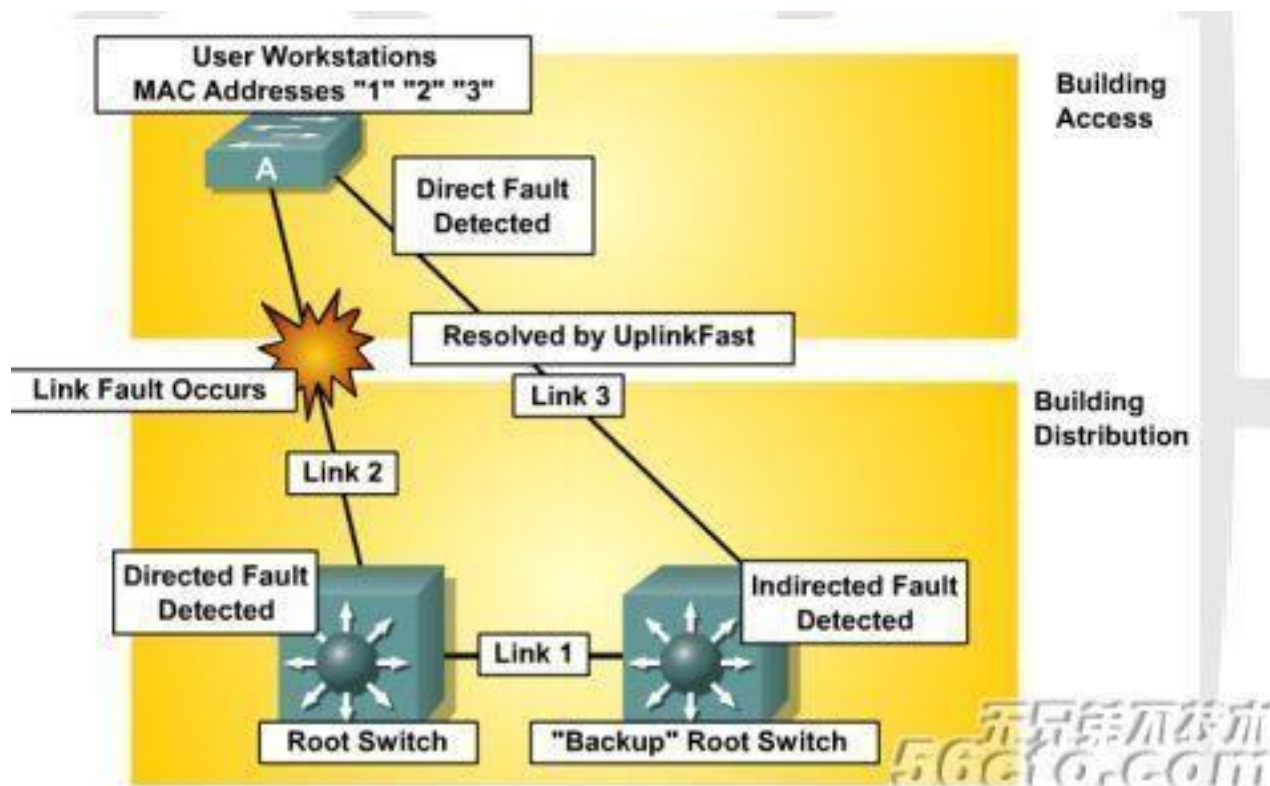
 Configure PortFast.

 Do not configure PortFast.

```
Switch(config-if)# spanning-tree portfast (interface command)
```

```
Switch(config)# spanning-tree portfast default (global command)
```

Cấu hình STP Uplinkfast, Backbonefast



```
Switch(config)# spanning-tree uplinkfast(Blocked port SW)
```

```
Switch(config)# spanning-tree backbonefast(Forwarding SW)
```

- ✚ Trình bày khái niệm VLAN, cách hoạt động của Switch có chi VLAN.
- ✚ Trình bày tác dụng của VTP.
- ✚ Trình bày cách liên lạc giữa các VLAN.
- ✚ Trình bày thuật toán chống Loop của Spanning Tree, cấu hình tùy biến Spanning Tree.

TÓM LƯỢC BÀI HỌC

- + Chức năng của Switch Layer 2
- + VLAN
- + VLAN Trunking Protocol
- + Spanning Tree Protocol



Q & A

