Lab 5. STP Configuration

TA 紀政良 (clc)
Credit to cps

What is STP?

- Spanning Tree Protocol
- A layer 2 protocol
- Runs on switches and bridges
- Switches need to be enabled for STP within the same network
- Create a loop-free network
- Track all the links and blocks the redundant link

Types of STP

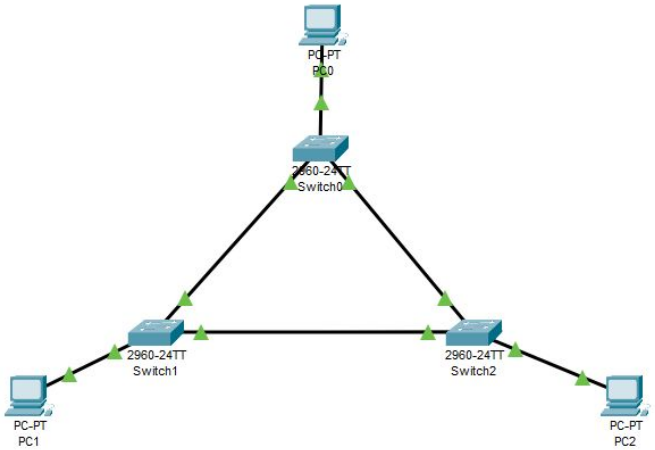
[1] Cisco IOS use PVST+ as default mode

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+ [1]	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s	Medium or high	Fast	Per Instance

```
(config)# spanning-tree mode mode
```

Need for STP

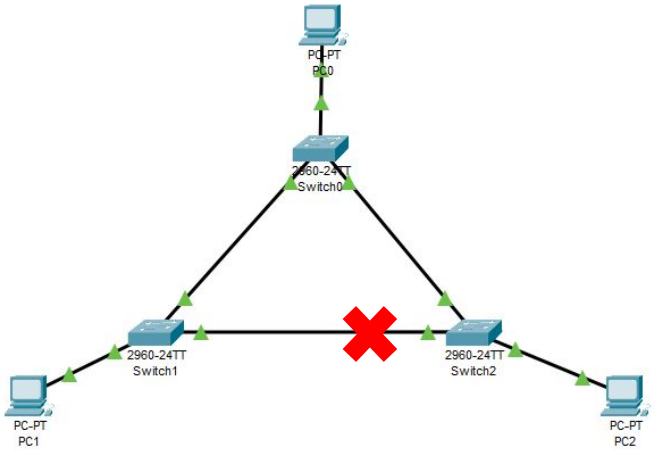
- Broadcast storm
- MAC database instability
- Multiple frame transmission



[Note] In the environment of Packet Tracer, we can use **no spanning-tree vlan 1** to see the problems above

Need for STP

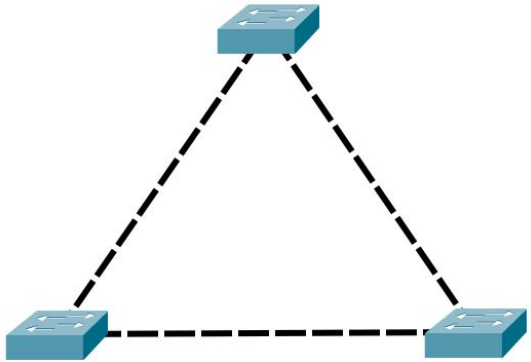
- Broadcast storm
- MAC database instability
- Multiple frame transmission



[Note] In the environment of Packet Tracer, we can use **no spanning-tree vlan 1** to see the problems above

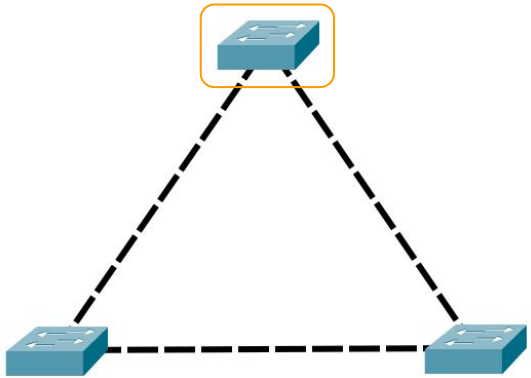
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



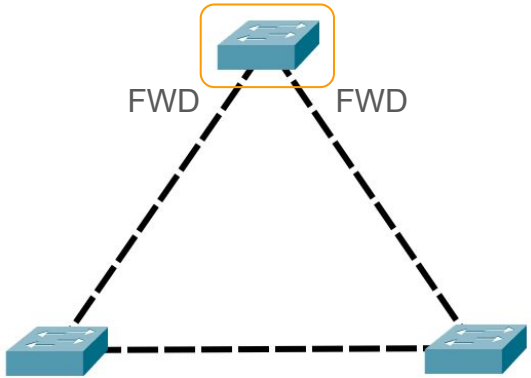
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



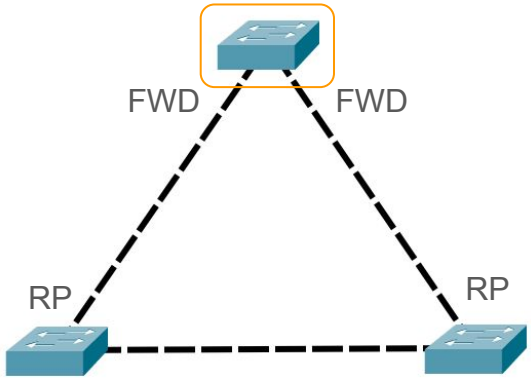
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



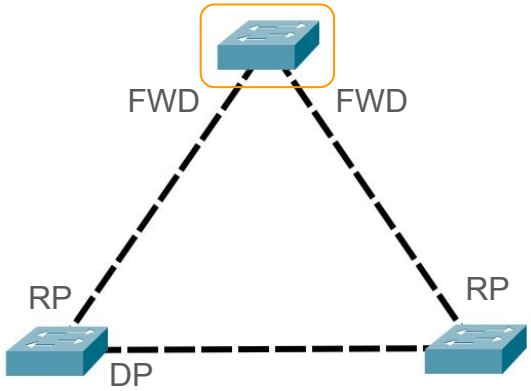
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



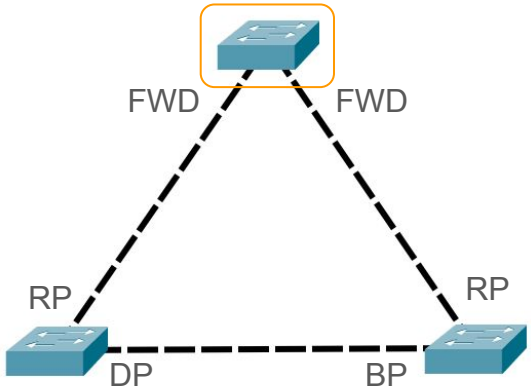
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state

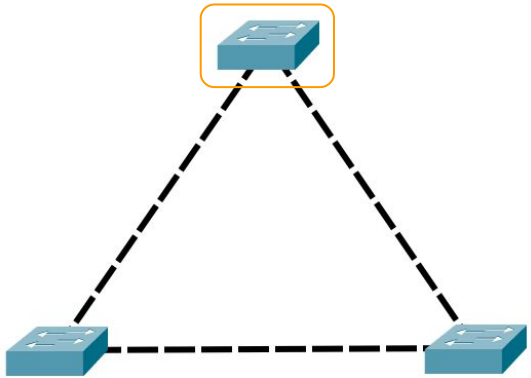


Port Roles

- Root port
  - Ports on non-root switches with the best cost path to root bridge. These ports forward data to the root bridge.
- Designated port
  - Ports on root and designated switches. All ports on the root bridge will be designated.
- Blocked port
  - All other ports to bridges or switches are in a blocked state. Access ports going to workstations or PCs are not affected.

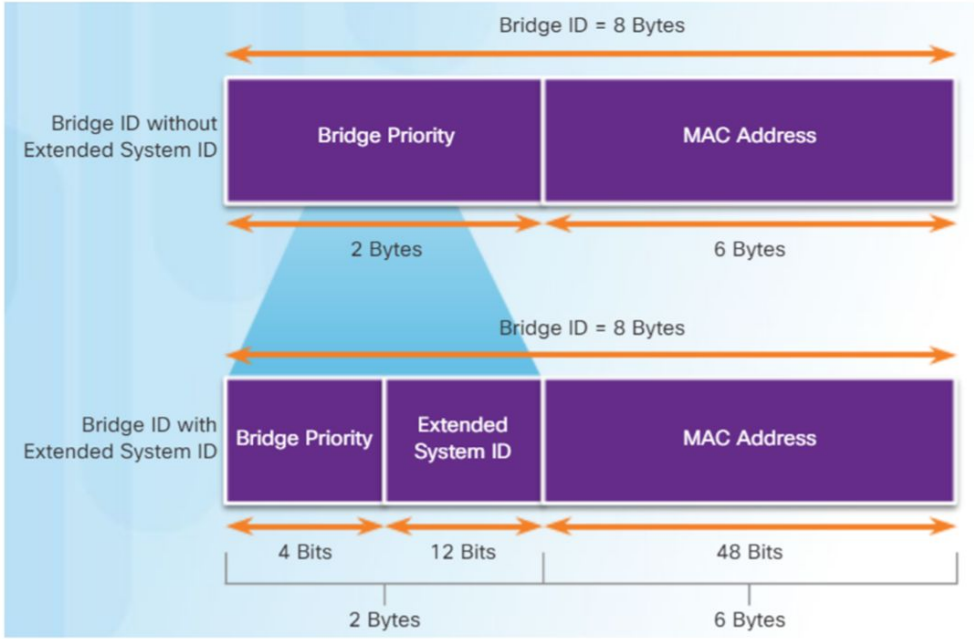
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



Bridge Priority

- Bridge priority only allows to be in multiple of **4096**

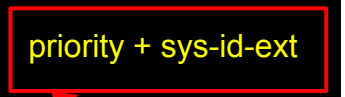


Bridge Priority

- Two ways to change bridge priority

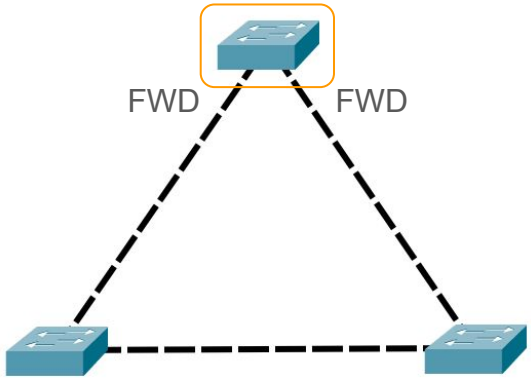
```
(config)# spanning-tree vlan vlan-id root [ primary | secondary ]
(config)# spanning-tree vlan vlan-id priority value
```

```
switch# show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID Priority       32769
          Address        0025.b4c1.b400
          This bridge is the root
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID    Priority       32769  (priority 32768 sys-id-ext 1)
          Address        0025.b4c1.b400
          Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
          Aging Time     300 sec
```



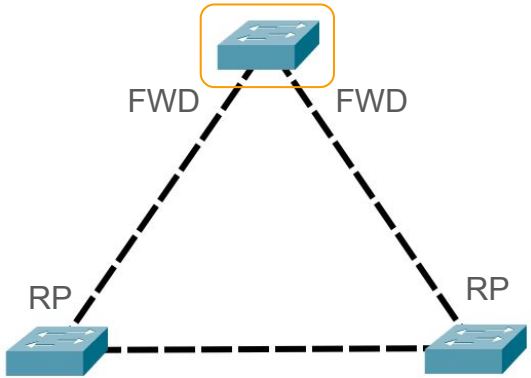
STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



STP Cost

- Configure interface cost

```
(config)# interface interface
(config-if)# spanning-tree vlan value cost value
```

- Show spanning tree cost

```
switch# show spanning-tree vlan 1
…
Interface  Role    Sts    Cost     Prio.Nbr     Type
---------  -----   -----  -----    --------     --------
Fa0/1       Root   FWD    19       128.8        P2p
Fa0/2       Desg   FWD    40       128.2        P2p
...
```

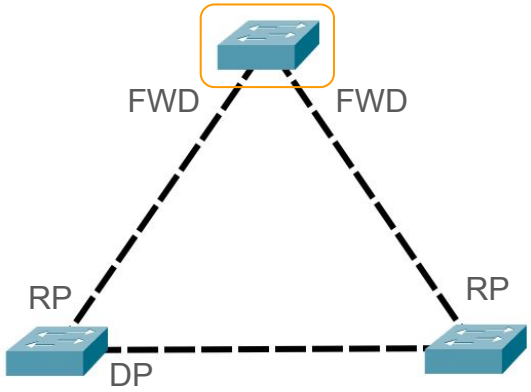
Link Speed	Cost
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

Root port selection

1. Lowest cost
2. Lowest neighbor bridge ID
3. Lowest neighbor port priority
4. Lowest neighbor physical port number

STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state

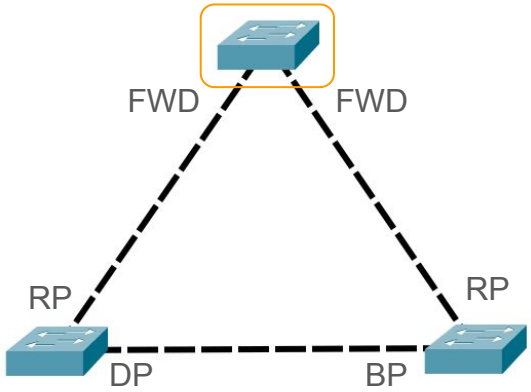


Designated port selection

1. Lowest accumulated cost to the root bridge
2. Lowest bridge ID

STP Process

- Elect a root bridge
- Place root interface to forwarding state
- Choose root port for each non-root bridge
- Choose designated port for each remaining link
- Put all other ports into blocking state



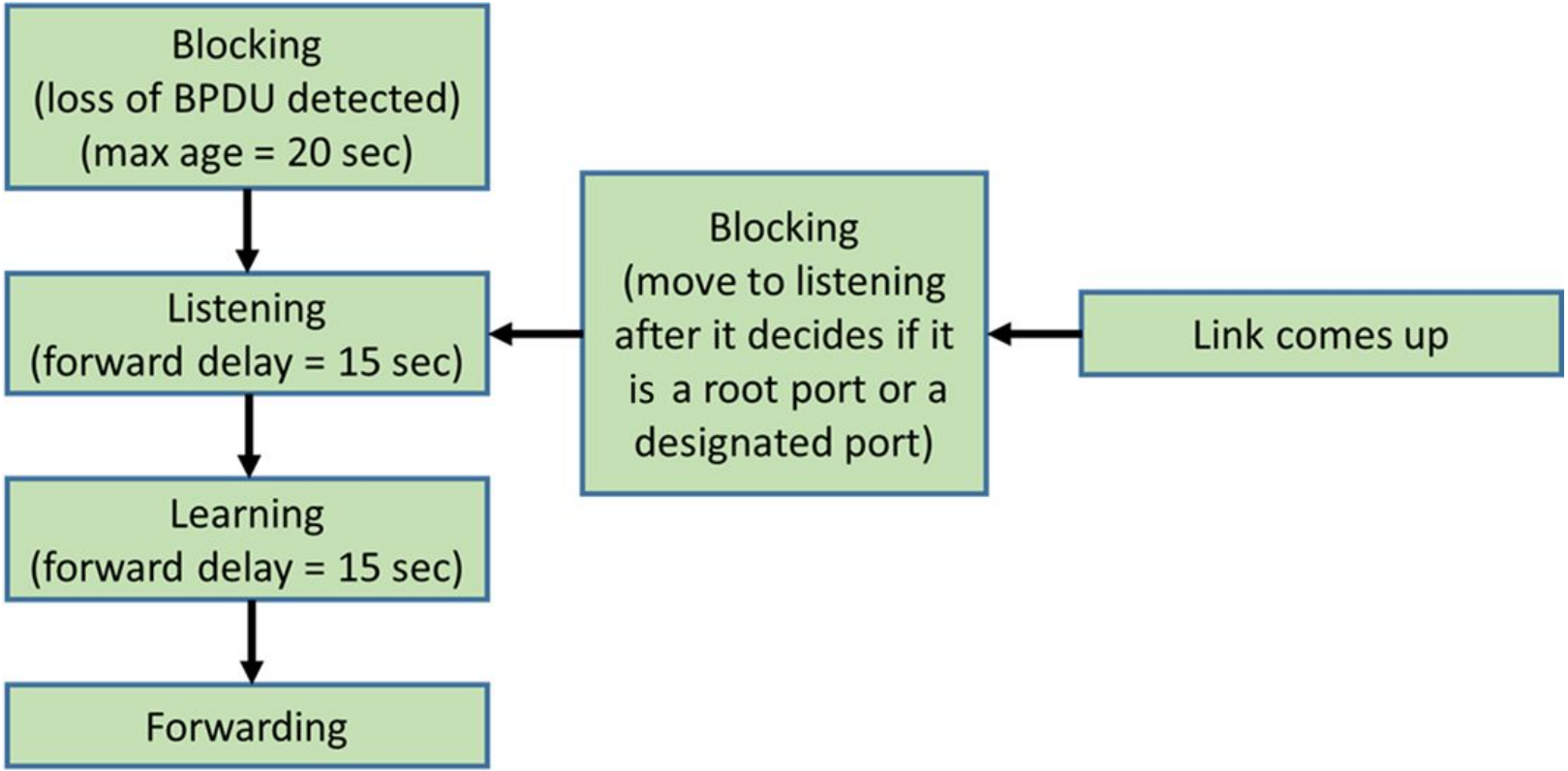
Port States

STATUS	Disabled	Blocking	Listening	Learning	Forwarding
Receive BPDU	X	O	O	O	O
Send BPDU	X	X	O	O	O
Learn MAC	X	X	X	O	O
Forwarding	X	X	X	X	O
Duration	Until no shutdown	Until topology changed	Forward Delay (default 15s)	Forward Delay (default 15s)	Until shutdown or not root/designated port

Topology Change

- Send TCN (topology change notification) on its root port
- Upstream bridge responds an TCA (topology change acknowledgement)
- Root bridge send BPDU with TC bit set
- Lower their MAC table address aging time (from 300s to 15s)

Port States


Blocking
(loss of BPDU detected)
(max age = 20 sec)
Listening
(forward delay = 15 sec)
Learning
(forward delay = 15 sec)
Forwarding
Blocking
(move to listening
after it decides if it
is a root port or a
designated port)
Link comes up

STP Convergence

- 50 seconds for going through all state

STP Timer

- Hello Timer (default 2 sec)
  - The frequency of sending BPDU
- Max Age Timer (default 20 sec)
  - The maximum length of time a switch saves BPDU information
- Forward Delay Timer (default 15 sec)
  - The time spent on the listening and learning states

STP Timer

- The diameter is the maximum number of switches that data must cross to connect any two switches
- Diameter configuration (deprecated on Packet Tracer)

```
(config)# spanning-tree vlan vlan-id root primary diameter size
```

Diameter	2	3	4	5	6	7
Hello Time	2	2	2	2	2	2
Max Age	10	12	14	16	18	20
Forward Delay	7	9	10	12	13	15

STP Enhancements

- PortFast
- BPDU Guard
- BPDU Filter
- Root Guard

PortFast

- Allow a port to enter from blocking to forwarding state immediately, bypassing the listening and learning states
- You will see warning as below after configuring PortFast

```
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc… to this
interface when portfast is enabled, can cause temporary bridging loops.
   Use with CAUTION
```

- Need to wait for convergence to communicate with a port on which the PortFast feature is disabled (normally a port connected to another switch).
- Never enable PortFast on a Trunk port!

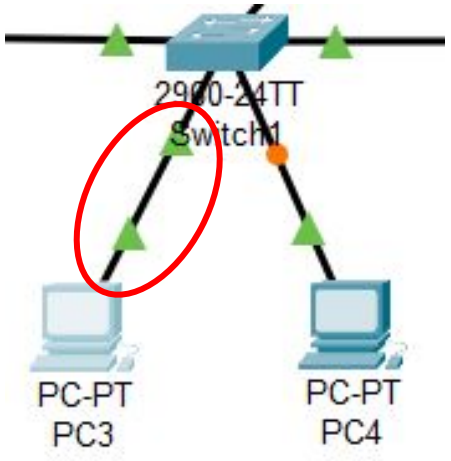
PortFast Configuration

- Configure PortFast on a switch port

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

- Enable PortFast on all nontrunking interfaces

```
(config)# spanning-tree portfast default
```



with Portfast without Portfast

BPDU Guard

- If BPDU guard is enabled, it puts the port in an **err-disabled** state when receiving a BPDU
  - This will effectively shut down the port
- The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back into service
  - **shutdown** the interface and **no shutdown** it back to recover
- Turn on BPDU Guard

```
(config)# interface interface
(config-if)# spanning-tree bpduguard enable
```

BPDU Filter

- Similar to BPDU Guard, but just “filter” it
- Two different configuration styles, with different behaviors
  - Configure it globally
  - Configure it on the specified port

BPDU Filter

- When configured globally
  - Affect all operational PortFast ports
  - If BPDUs are seen on the port
    1. The port loses its PortFast status
    2. BPDU filtering is disabled
    3. STP sends and receives BPDUs as any other STP port
  - Upon startup, the port transmits ten BPDUs. If this port receives any BPDUs during that time, PortFast and BPDU filtering are disabled
- When configured on an individual port
  - Ignore all BPDUs received
  - Send no BPDUs

BPDU Filter Configuration

- Enable BPDU filtering globally (deprecated on Packet Tracer)

```
(config)# spanning-tree portfast bpdufilter default
```

- Enable BPDU filtering on a specific switch port (deprecated on Packet Tracer)

```
(config)# interface interface
(config-if)# spanning-tree bpdufilter enable
```

- To verify the configuration

```
# show spanning-tree summary totals
# show spanning-tree interface interface detail
```

Root Guard

- Root guard is configured on a per-port basis
- If there is a superior BPDU received on the port, root guard does not take the BPDU into account and so puts the port into **root inconsistent state**
- Root guard configuration

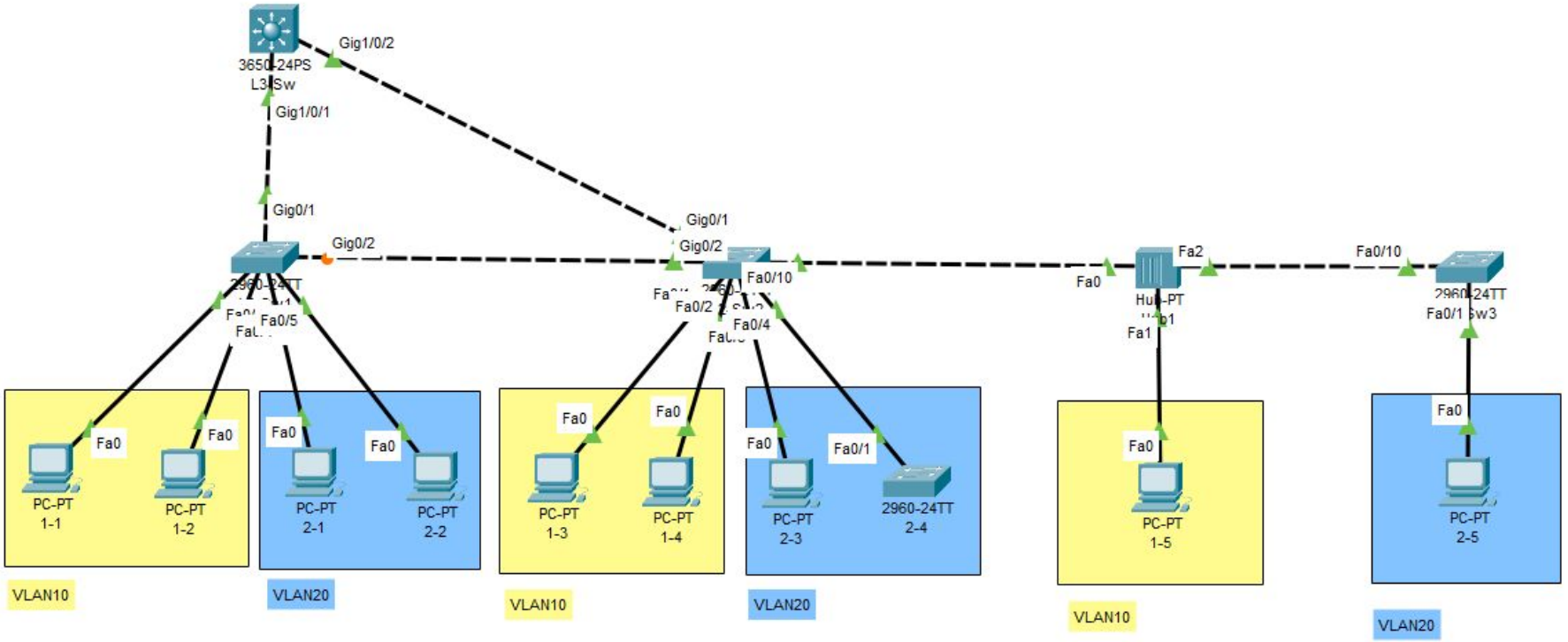
```
(config)# interface interface
(config-if)# spanning-tree guard root
```

```
switch# show spanning-tree inconsistentports
Name                 Interface             Inconsistency
-------------------- --------------------- ------------------
VLAN0001             FastEthernet0/4       Root Inconsistent

Number of inconsistent ports (segments) in the system : 1
```

Reference

- https://www.omnisecu.com/cisco-certified-network-associate-ccna/index.php
- https://www.youtube.com/watch?v=japdEY1UKe4&t=273s

VLAN STP Review



VLAN STP Review

- End devices x-y IP: 192.168.x0.y/24, GW: 192.168.x0.254

```
(config)# ip default-gateway x.x.x.x
```

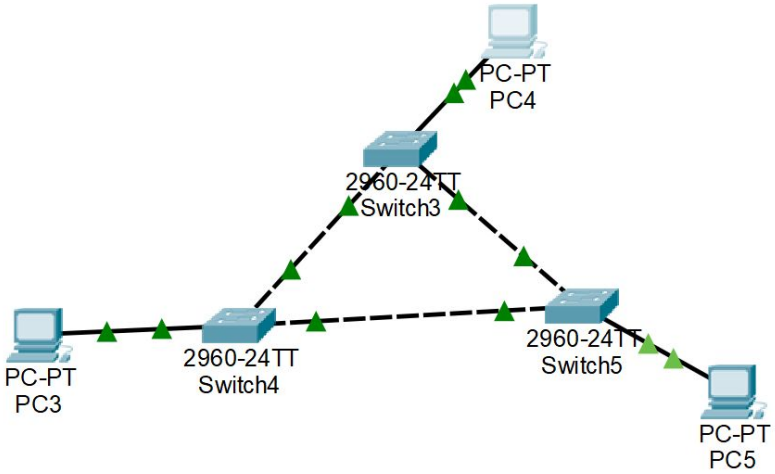
- VLAN: 如圖所示, 啟用10 或 20, 命名為 VLAN{num}
- 請設定 Sw1-3 、L3-Sw 使同 LAN 能互通
- 請設定 Gateway 在 L3-Sw 使不同 LAN 能互通
- spanning-tree mode: rapid-pvst
- 對 End devices 設定 Portfast 、BPDU guard
- 2-4 被使用者接成 Switch 了, 要怎麼更改設定使它連線可以使用, 但不會搶走 root。

Outline

- 實驗目的
- 實驗環境
- 指令介紹
- **小作業 (不算分)**

STP 的重要性

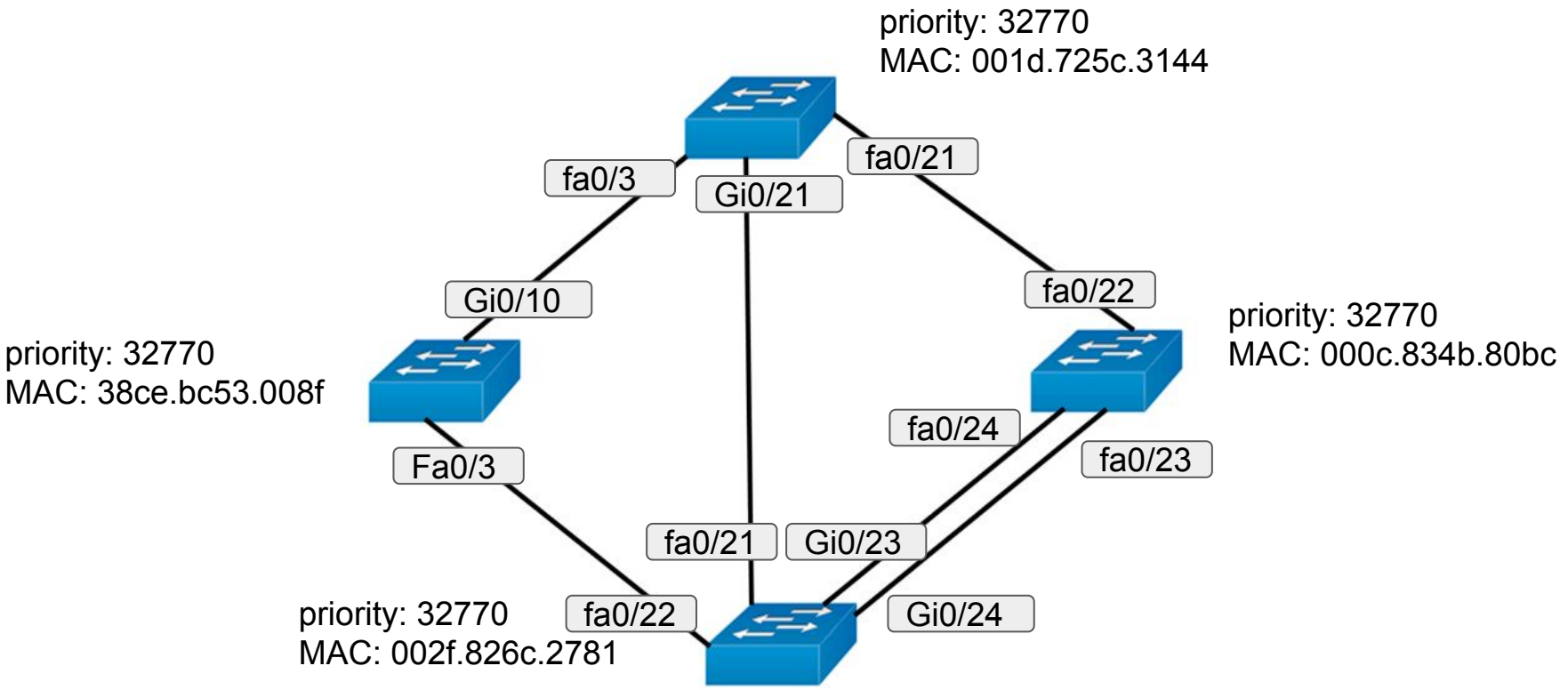
1. 在 L2 環境中，STP 的扮演著不可或缺的角色，如果缺少 STP，會造成 MAC database instability, broadcast storms, multiple frame transmission 等事情發生。請使用 packet tracer 的功能，模擬並截圖說明如果下圖的拓樸缺少 STP 會發生什麼嚴重的後果。(擇二說明即可)



作業要求

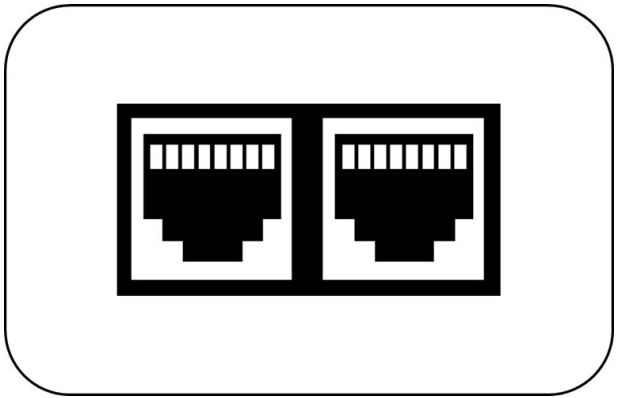
2. 下頁圖片為一簡單網路拓樸，若此拓樸使用的協定為 PVST，根據圖上提供的資訊回答下列問題
   a. 請問此拓樸最有可能是 VLAN 多少？
   b. 請找出此 Spanning 的 root，並標示出各介面的 STP role 以及那些線路不會有流量經過

作業要求


priority: 32770
MAC: 001d.725c.3144
fa0/3
Gi0/21
fa0/21
Gi0/10
fa0/22
priority: 32770
MAC: 38ce.bc53.008f
priority: 32770
MAC: 000c.834b.80bc
fa0/24
Fa0/3
fa0/23
fa0/21
Gi0/23
priority: 32770
MAC: 002f.826c.2781
fa0/22
Gi0/24

作業要求

3. 假設你是交大資工某實驗室的網管，你發現牆壁上有兩個網路孔 (以下稱為壁孔)，如下圖所示，已知兩壁孔後端連接至同一網路設備。然而，兩個壁孔並不足以提供整間實驗室使用，於是你決定自己買一台網路設備供實驗室使用。請依照課堂所學的內容，回答下頁問題

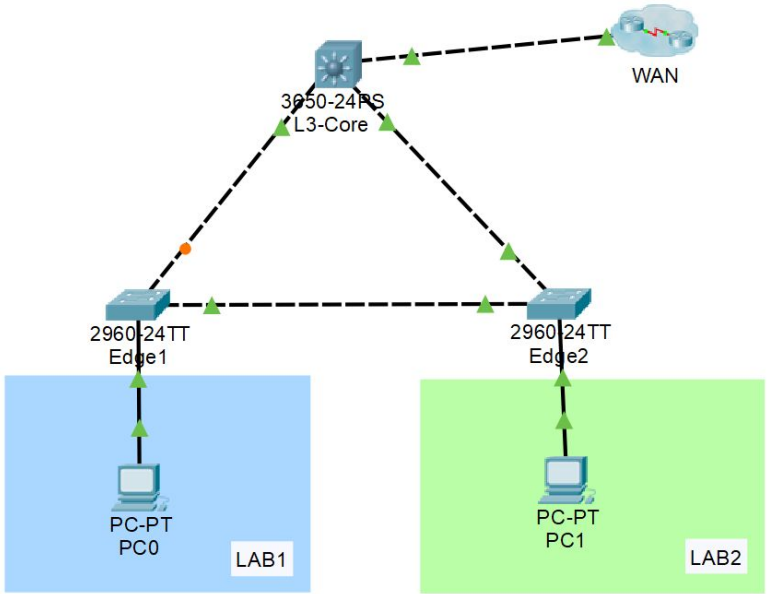


作業要求

a. 此二壁孔後端最有可能連接至何種網路設備？請回答 Switch, Router 或 L3 switch 並敘述原因
b. 相較於只連接一個壁孔，同時將兩個壁孔連接至你自己購買的網路設備，是否能有效增加你所購買之網路設備與壁孔之間的頻寬？為什麼？
c. 在你自己購買的網路設備上，除了連接壁孔的 interface 之外，是否適合在其他 interface 上設定 portfast 功能？原因為何？

作業要求

4. 身為優質的實驗室網管，你獲得了成為系計中助教的機會，除了整天吸貓貓之外你還必須管理工三網路。如果有一網路拓樸如下圖，根據你強大的網路知識，請回答下頁問題



作業要求

a. 此網路拓樸有一大缺點，故通常網管人員會極力避免做出此拓樸。請問此缺點為何？應如何避免？
b. 承(a)，若實驗室想把 PC 換成 switch，欲讓實驗室內部的交換器也能參與工三網路 STP 選舉，卻不希望讓 Spanning Tree 的根橋接器角色被實驗室搶走，應在哪台機器上做哪些設定？
c. 承(a)，若不希望實驗室內部的交換器參與工三網路 STP 選舉，卻允許實驗室內部自行安裝交換器，且當 BPDU 封包進入壁孔時該 interface 不會被關閉，應在哪些機器上做哪些設定?