內部訓練 Day 1

Outline

- VLAN Overview
- VTP (VLAN Trunking Protocal)
- EtherChannel
- STP (Spanning Tree Protocal)
- Port Security
- ACL (Access Control List)

VLAN Overview

Access & Trunk

- Access Port
  - 一般主機
  - 單一VLAN
- Trunk Port
  - Switch 之間
  - Switch & Router
  - 可傳遞多個VLAN

Switch Mode

- Access
- Trunk
- Dynamic
  - Desirable
  - Auto

	Trunk	Desirable	Auto	Access
Trunk	Trunk	Trunk	Trunk	!!!Bomb!!!
Desirable	Trunk	Trunk	Trunk	Access
Auto	Trunk	Trunk	Access	Access
Access	!!!Bomb!!!	Access	Access	Access

Native VLAN

- untag
- Default native vlan 1

- (config-if)# switchport trunk native vlan NUM

Trunk

- # show int trunk
- # show vlan
- # show int switchport
- # show int fa0/1 switchport

VTP

- 共享VLAN設定，集中控管

- VTP Domain
- Mode
  - Server
  - Client
  - Transparent
- Revision

VTP

- # show vtp status

- VTP Version : 2
- Configuration Revision : 3
- Maximum VLANs supported locally : 255
- Number of existing VLANs : 8
- VTP Operating Mode : Server
- VTP Domain Name : AAA

EtherChannel

EtherChannel

- 多個Port 一起傳送資料
- 速度提高
- 容錯

- 最少 2 Port
- 最多 8 Port
- 兩種協定差不多

- Cisco::Pagp
  - Desirable
  - Auto
  - Static(on)

- IEEE::Lacp
  - active
  - Passive
  - on

EtherChannel

- 兩邊Port需要相同的
  - 速度
  - Duplex mode
  - Native VLAN
  - VLAN range
  - Trunking status
  - Type
  - 同為layer2 或 layer3

EtherChannel

- 兩邊都要設定(都先shutdown)

- (config)# int range fa0/1-4
- (config-if)# shutdown
- (config-if)# channel-protocol pagp
- (config-if)# channel-group 1 mode desirable
- (config-if)# no shutdown

EtherChannel

- interface從FastEthernet X 變為 Port-Channel X (簡寫PoX)

- # show etherchannel
- # show spanning-tree

Spanning Tree

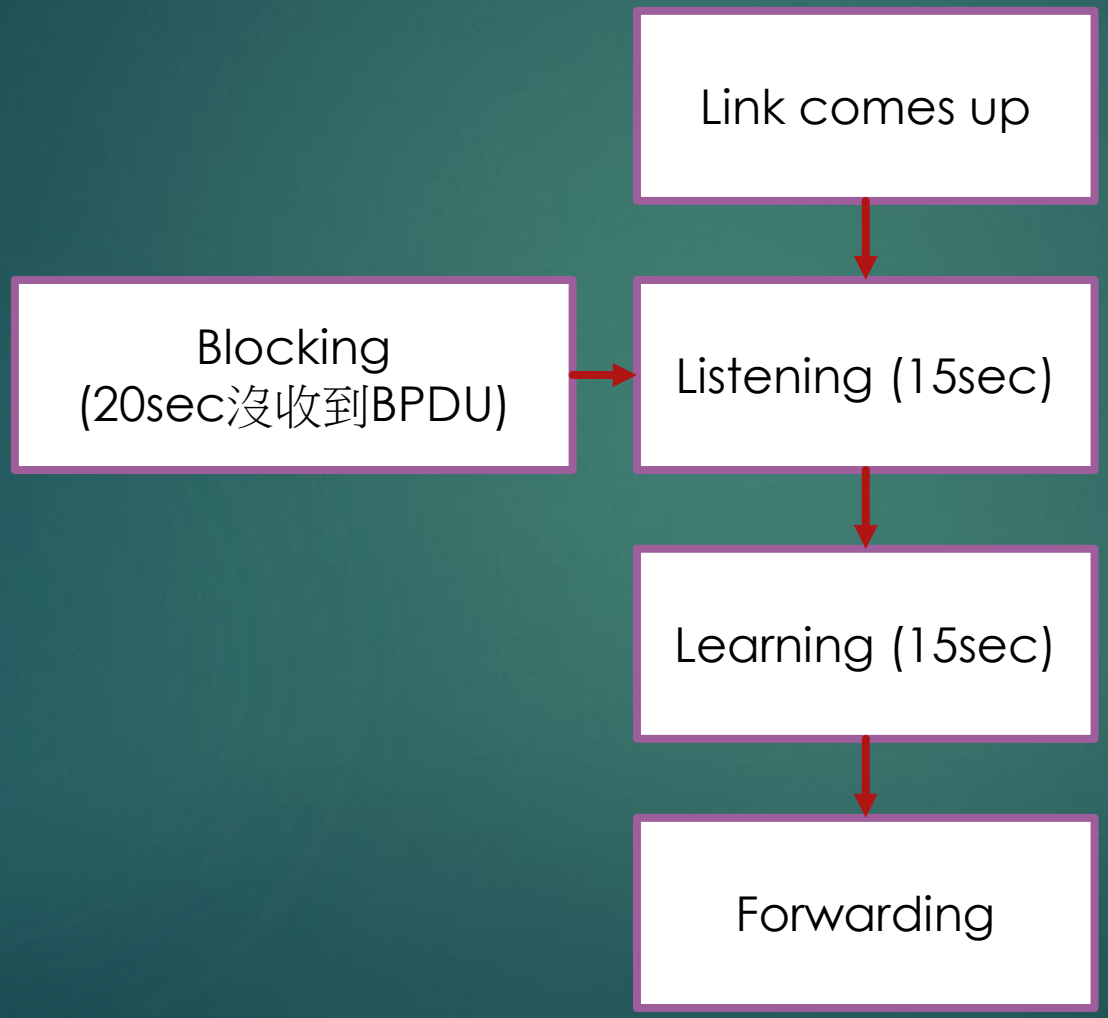
Spanning Tree Protocol

- Layer 2 防止 Loop
- Blocking Mode

Spanning Tree Protocol BPDU

- Root ID => Root 的 Bridge ID
- Bridge ID => Priority (4 bit) + VLAN ID (12 bit)
- Port ID => Priority (4 bit) + Port ID (12 bit)
- Path Cost
- Hello Time => Default 2 sec
- Max Age => Default 20 sec (10 次 * Hello Time)
  - 當超過Max Age沒收到BPDU封包，認定對方下線
- Forward Delay => Default 15 sec

Spanning Tree Protocol State



Spanning Tree Protocol State

- Blocking
  - 只會收BPDU封包，其他封包會丟棄。
  - 選擇Root Bridge ，Root Port，Designated Port
- Listening (15sec)
  - Root Bridge 發送BPDU ， 其餘不送
  - 等待是否有其他BPDU封包
- Learning (15sec)
  - 學習MAC Address
- Forwarding
  - 轉發一般封包(正常運作的Port)

Root Bridge 選擇(1)

- Path Cost

IEEE	Path Cost
10 G	2
1 G	4
100 M	19
10 M	100

Root Bridge 選擇(2)

- 大家選一個
- Lowest Bridge ID
- Bridge ID = Bridge Priority + MAC Address

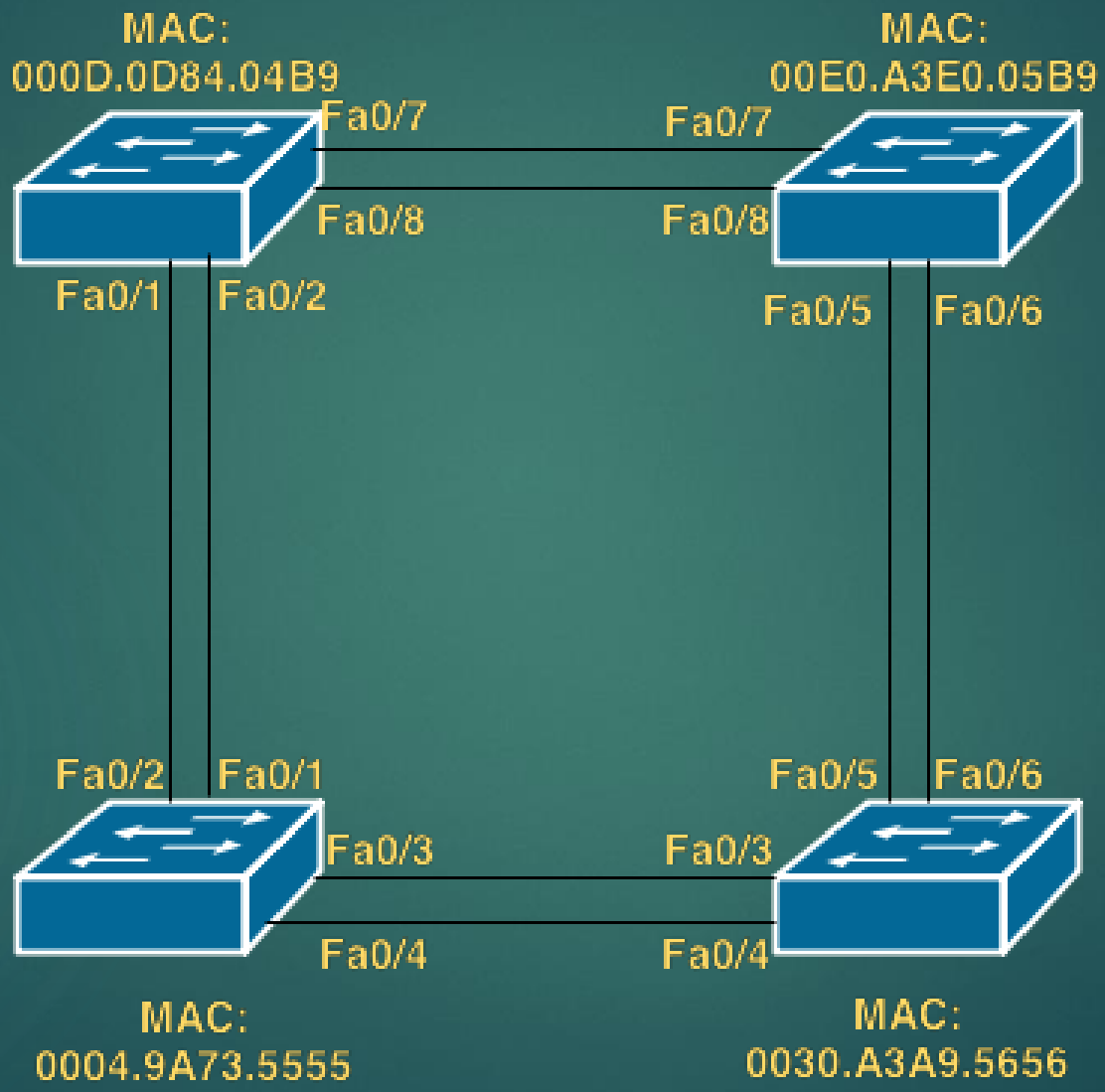
Root Port 選擇

- 每個 Switch 選出一個
- 到 Root Bridge 的 Path Cost 加總較小者
- Cost 一樣，相鄰的 Bridge ID 較小者
- Bridge ID 一樣，自己的 Port ID (Port Num.) 較小者

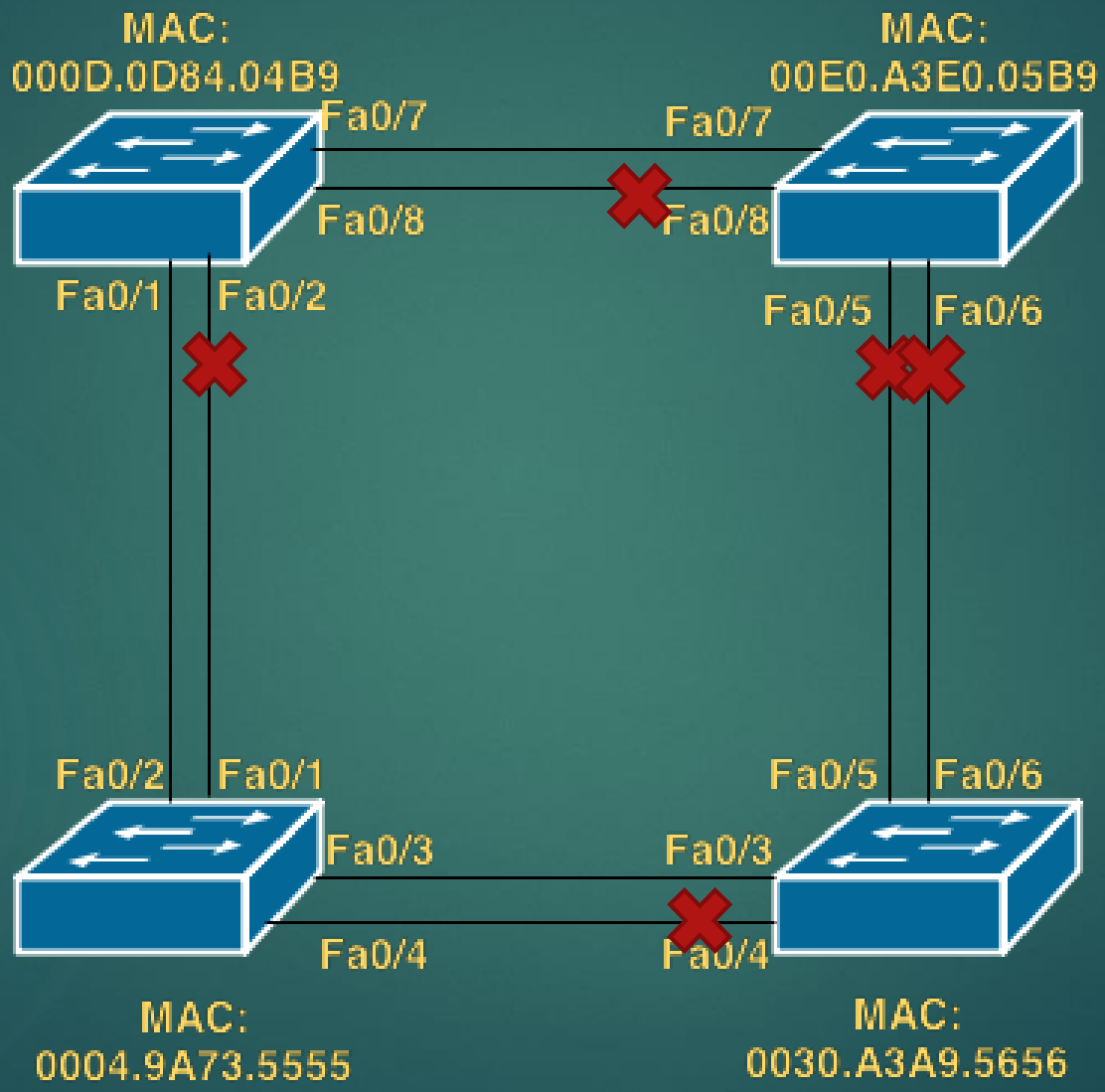
Designated Port 選擇

- 一個 Segment 選一個
- 與 Root Port 選擇方式相同

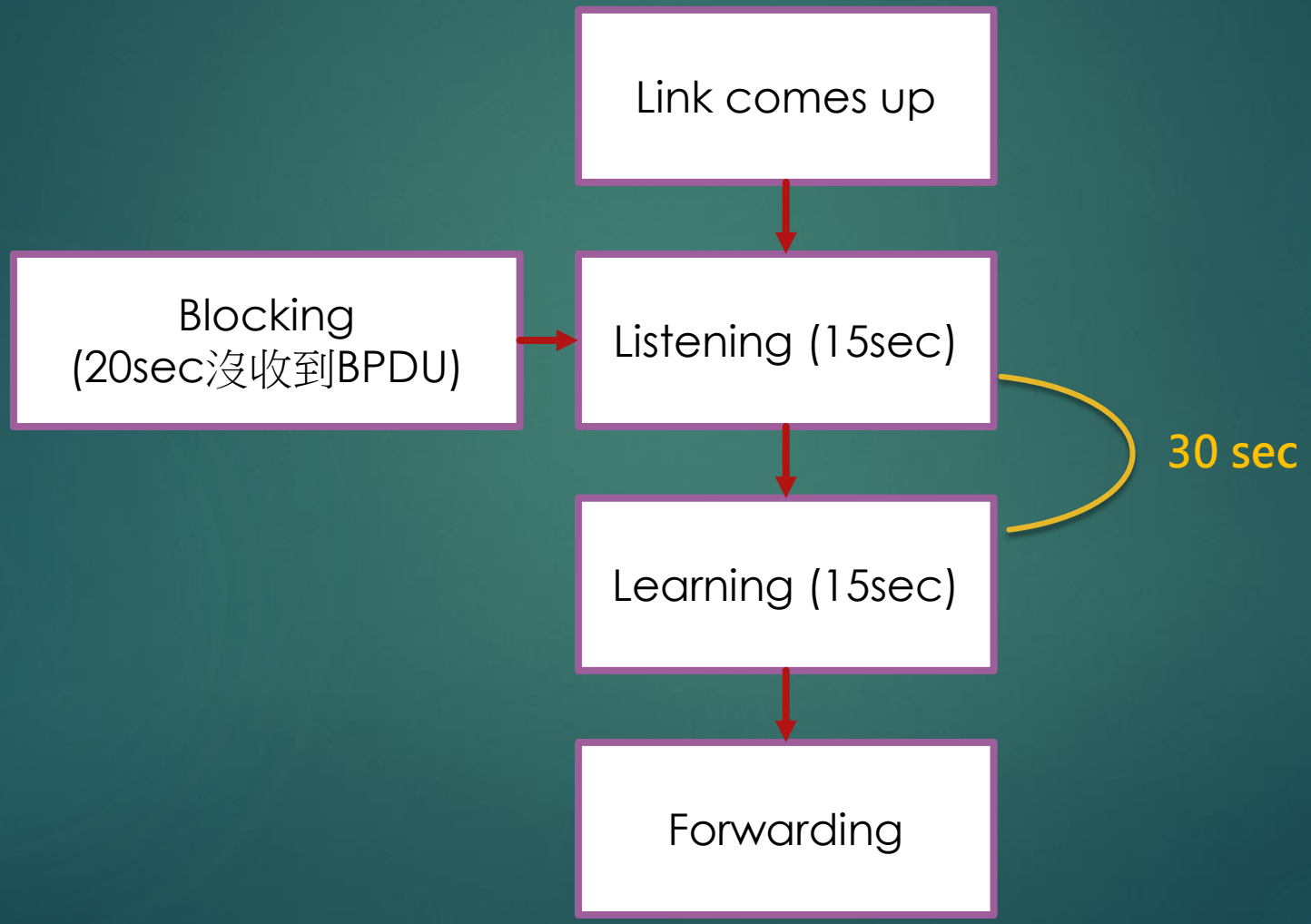
Example


MAC:
000D.0D84.04B9
Fa0/7
Fa0/8
Fa0/1
Fa0/2
MAC:
00E0.A3E0.05B9
Fa0/7
Fa0/8
Fa0/5
Fa0/6
Fa0/2
Fa0/1
Fa0/3
Fa0/4
MAC:
0004.9A73.5555
Fa0/5
Fa0/6
Fa0/3
Fa0/4
MAC:
0030.A3A9.5656

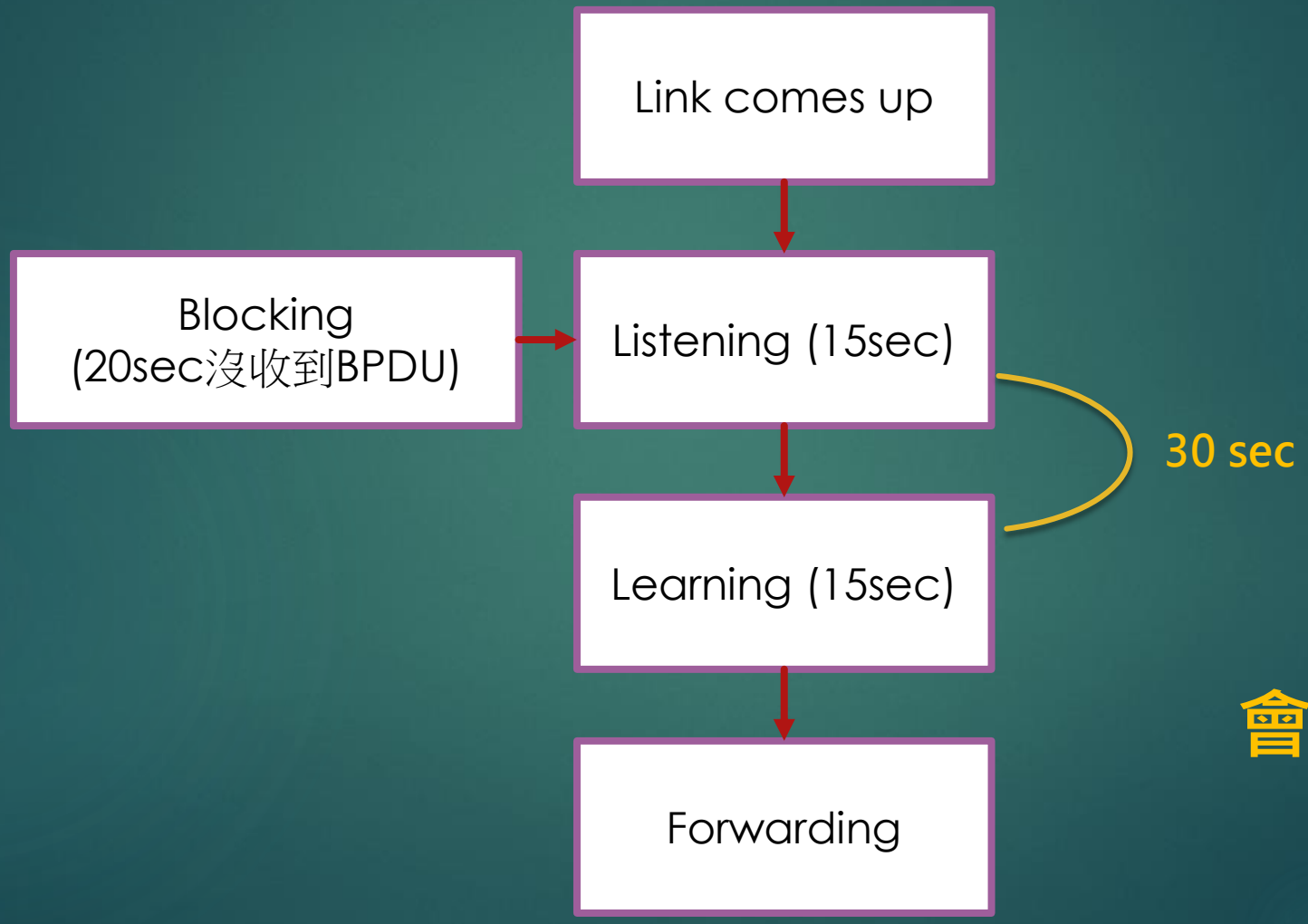
Example


MAC:
000D.0D84.04B9
Fa0/7
Fa0/8
Fa0/1
Fa0/2
MAC:
00E0.A3E0.05B9
Fa0/7
Fa0/8
Fa0/5
Fa0/6
Fa0/2
Fa0/1
Fa0/3
Fa0/4
MAC:
0004.9A73.5555
Fa0/5
Fa0/6
Fa0/3
Fa0/4
MAC:
0030.A3A9.5656

Spanning Tree Protocol State



Spanning Tree Protocol State



會不會太久啦?

RSTP (Rapid Spanning Tree Protocol)

- IEEE 802.1w
- Max Age 改成三次 Hello time
  - 當 Root Bridge 死掉惹，會等6秒鐘才切換

MST (Multiple Spanning Tree)

- IEEE 802.1s

- 共計兩枝生成樹
- 群組設定VLAN

PVST (Per-VLAN Spanning Tree)

- Cisco Only
- 根據不同VLAN 設定不同Root Bridge
- 缺點 每個VLAN都要計算一次Root Bridge
- (config)# spanning-tree vlan 11,12 priority
- or
- (config)# spanning-tree vlan 11,12 root [primary | secondary]

PVST (Per-VLAN Spanning Tree)

- Port Roles
  - Root
  - Designate
  - Alternate
  - Backup
  - Disabled

PVRST (Per-VLAN Rapid Spanning Tree)

- 兼具 Per-VLAN Spanning Tree 與 Rapid Spanning Tree 的特性與優點

- (config)# spanning-tree mode rapid-pvst

Spanning Tree Protocol

- 對於一般pc的port可設定：
  - (config-if)# spanning-tree portfast
- 防止bpdu封包從這個port送上來
  - (config-if)# spanning-tree bpduguard
- 就算連接上來的switch BID較小，也不會成為root bridge
  - (config-if)# spanning-tree guard root

中場休息

Port Security

Port Security

- Violation
  - Protect
  - Restrict
  - Shutdown
- (config-if)# switchport port-security violation ACTION

Port Security

- 設定多組MAC Address
- (config-if)# switchport port-security maximum NUM

- 設定自動記錄MAC Address
- (config-if)# switchport port-security mac-address sticky

Access Control List

Access Control List

- Standard
  - 數字1~99、1300-1999
  - 英文字
  - 只可設定來源IP (無法指定protocol)
- Extended
  - 數字101~199、2000-2699
  - 英文字
- (config-if)# ip access-list [standard | extended] NAME

Access Control List

- (config-ext-nacl)# [NUMBER] [permit | deny]…
- (config-ext-nacl)# permit PROTOCOL …

- permit PROTOCOL SOURCE DESTINATION
- SOURCE DESTINATION 可以下列方式表示
  - A.B.C.D wildcard
  - host A.B.C.D
  - any

ACL Wildcard

- 格式 A.B.C.D
- 轉換為二進位制
- 1的位置忽略不計
- 不一定要連續的1

ACL Wildcard

- 140.123.239.0 0.0.0.255
  - 140.123.239.0~140.123.239.255
- 140.123.0.0 0.0.255.255
  - 140.123.0.0~140.123.255.255

ACL Wildcard

- 練習：
  - A. 允許10.1.1.[16 17 18 19 20]通過
  - B. 允許 10.1.1.[1 3 5 7]通過

ACL Wildcard

- 練習：
  - A. 允許10.1.1.[16 17 18 19 20]通過
    - permit 10.1.1.16 0.0.0.3
    - permit 10.1.1.20 0.0.0.0
  - B. 允許 10.1.1.[1 3 5 7]通過
    - permit 10.1.1.1 0.0.0.6

ACL Wildcard

- 允許 10.1.1.[1 3 5 7]通過
- permit 10.1.1.1 0.0.0.6

- 10.1.1.1 => 00000001
- 10.1.1.3 => 00000011
- 10.1.1.5 => 00000101
- 10.1.1.7 => 00000111
- mask => 00000110 => 0.0.0.6

Access Control List

- permit tcp 來源網段 PORT 目的網段 PORT

- permit tcp any any eq 80
  - 允許任意存取80 port (http)
- permit tcp any gt 1024 any eq 443
  - 允許來源大於1024的port存取443 port (https)

Time Base ACL

- (config)# time-range NAME
- (config-time-range)# periodic DAY TIME to TIME

- DAY 包含 daily weekdays weekend
  - Monday Tuesday…
- TIME
  - 19:00 to 22:00

Time Base ACL

- (config)# time-range DUTY
- (config-time range)#
  - periodic weekdays 19:00 to 22:00
- ip access-list extended QAQ
- permit ip any any time-range DUTY

Access Control List

- 規則查看
  - (config-ext-nacl)# do show access-list NAME
- 規則插入與刪除
  - (config-ext-nacl)# 25 permit …
  - (config-ext-nacl)# no NUM
- 重新排序
  - ip access-list resequence NAME START INCREMENT

QAQ時間

終場休息