

111年度第一次 台北區網(臺大)網管會議

臺灣大學計資中心
游子興
davisyou@ntu.edu.tw
3366-5008

會議議程

項目	時間	主持人／報告人	報告內容
主席報告	14:00~14:05	組長：謝宏昀教授	
業務報告	14:05~14:20	游子興	區網營運業務報告
	14:20~14:30	李墨軒	資安事件相關說明
	14:30~14:50	北區 ASOC童鵬哲	資安Case Study分享
專題研討	15:00~16:20	中華資安國際	SecuTex 先進資安威脅防禦系統
	16:20~16:40	北區 ASOC童鵬哲	ASOC資安通報宣導-DNS與惡意程式
	16:40~17:00	無線漫遊中心	TANet無線漫遊建置與維運
臨時動議		出列席人員	



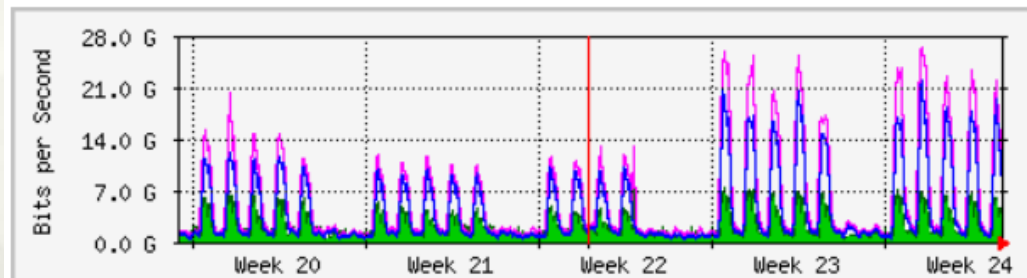
臺北市網線路 **20G 擴增至 40Gbps**

2022/06/02

臺北市網 MRTG

* 臺北市網 ipv4

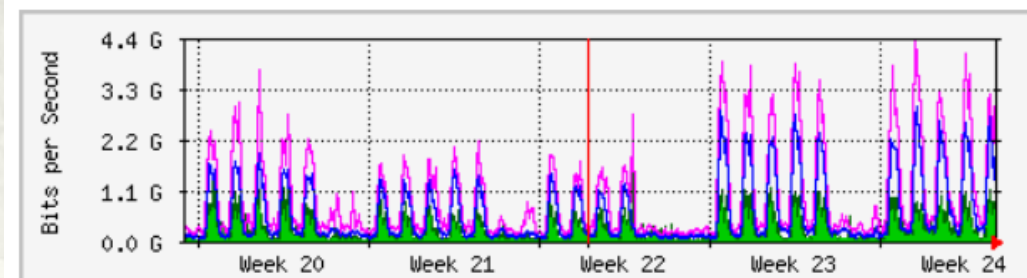
'Monthly' Graph (2 Hour Average)



	Max	Average	Current
臺北市教育網路 => 北區區網:	7522.0 Mb/s (18.8%)	1747.1 Mb/s (4.4%)	2276.1 Mb/s (5.7%)
北區區網 => 臺北市教育網路:	26.3 Gb/s (65.7%)	4010.9 Mb/s (10.0%)	5513.1 Mb/s (13.8%)

* 臺北市網 ipv6

'Monthly' Graph (2 Hour Average)

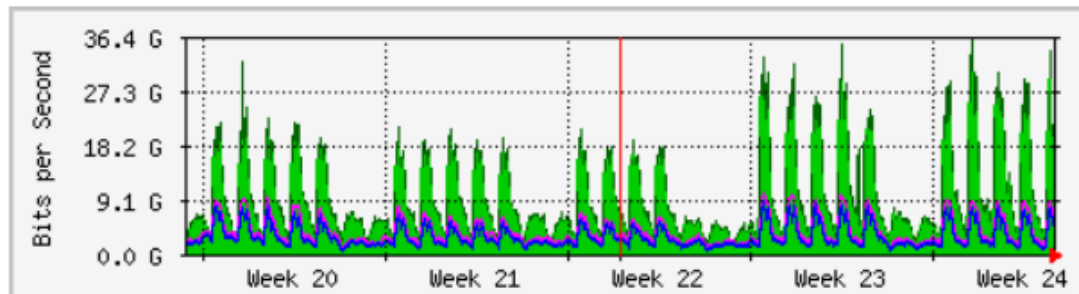


	Max	Average	Current
臺北市教育網路 => 北區區網:	1502.2 Mb/s (3.8%)	184.9 Mb/s (0.5%)	350.6 Mb/s (0.9%)
北區區網 => 臺北市教育網路:	4270.4 Mb/s (10.7%)	555.2 Mb/s (1.4%)	874.4 Mb/s (2.2%)

區網骨幹

* 區網骨幹流量

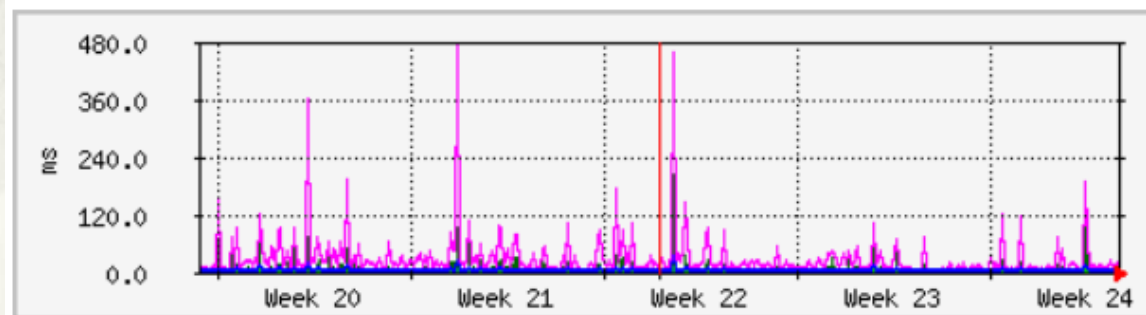
'Monthly' Graph (2 Hour Average)



	Max	Average	Current
InterNet => 北區區網	36.1 Gb/s (36.1%)	8716.5 Mb/s (8.7%)	18.9 Gb/s (18.9%)
北區區網 => InterNet	9888.8 Mb/s (9.9%)	2781.9 Mb/s (2.8%)	5577.3 Mb/s (5.6%)

* 臺北市網內部 ipv4 PING

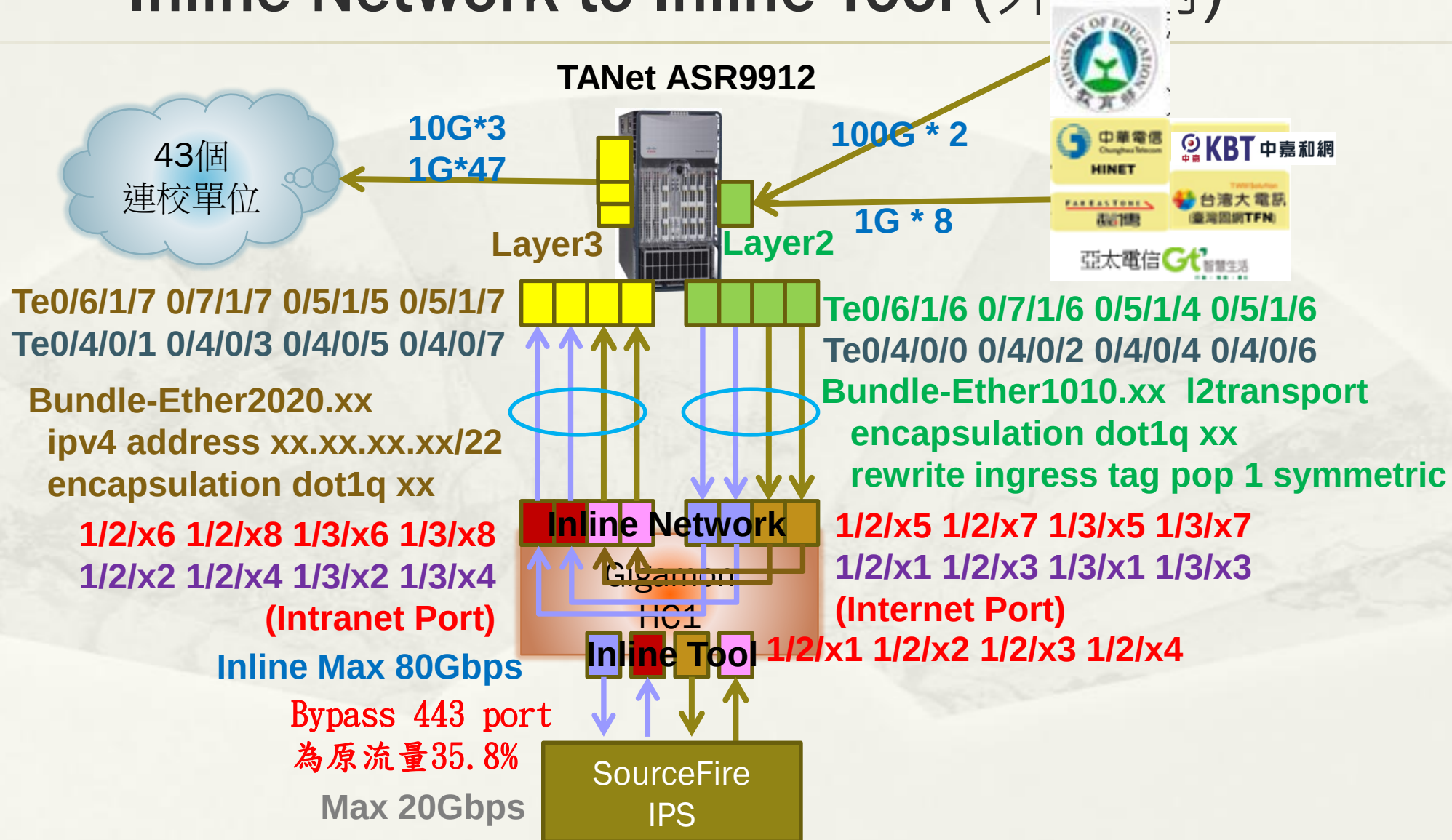
'Monthly' Graph (2 Hour Average)



	Max	Average	Current
Average response time ms	204.0 ms	2.0 ms	2.0 ms
Max response time ms	471.0 ms	3.0 ms	3.0 ms

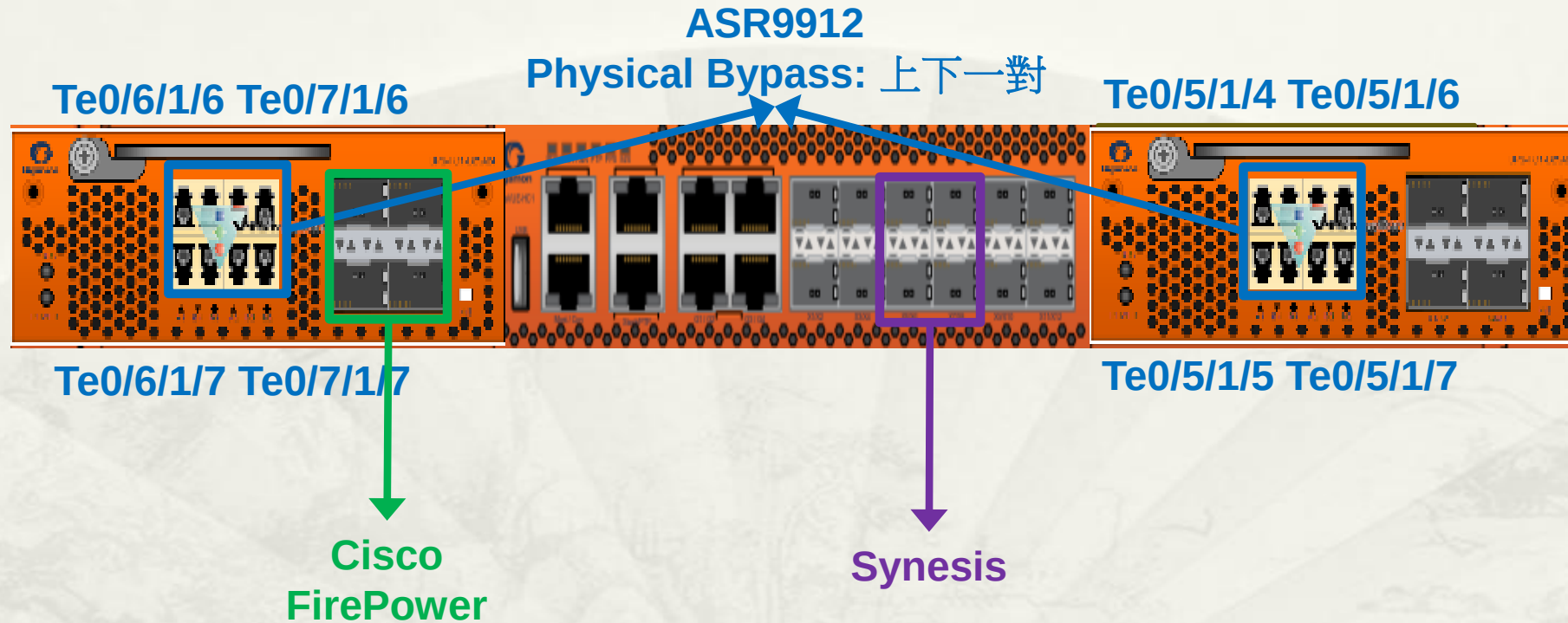
台大區網 Gigamon 分流架構 40G -> 80Gbps

Inline Network to Inline Tool (外對內)



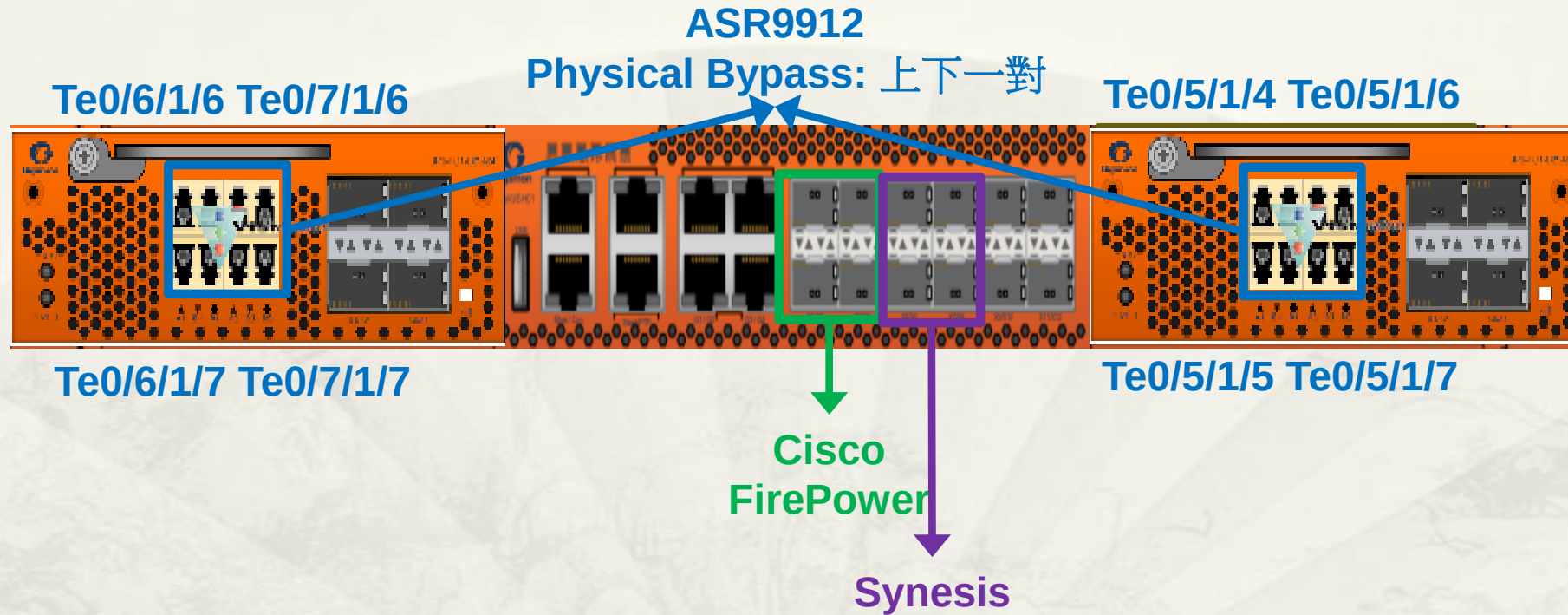
Gigamon HC1

實際接線圖 40Gbps



Gigamon HC1

實際接線圖 80Gbps





租用點對點電路是否支援 **Ether Channel** ?

Ether Channel/Port Channel/Aggregation LACP/Teaming/Bundle/Bonding

- * Protocol

- * PAgP(Port Aggregation Protocol): Cisco proprietary
- * Link Aggregation Control Protocol(LACP): IEEE 802.3ad standard
- * No protocol: 通常用於另一端是 Server. (ex.ESXi)
- * 無論何種協定，皆不支援同一 TCP/UDP Session 去回皆在同一實體介面中.(詳見 Load Balance 說明)

- * Bundle Interface

- * Access Mode(Layer2)
- * Route Mode(Layer3)

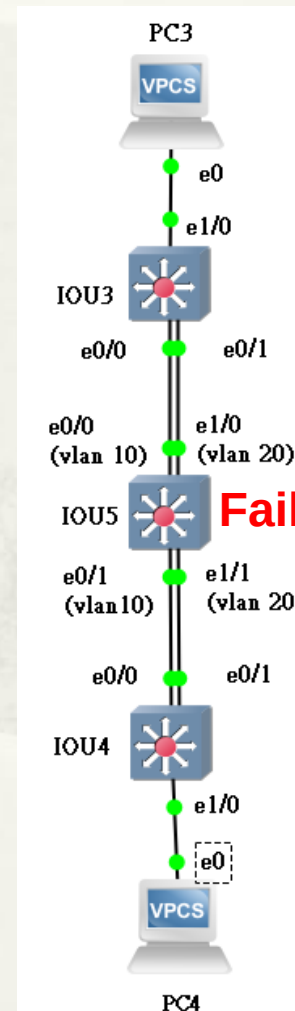
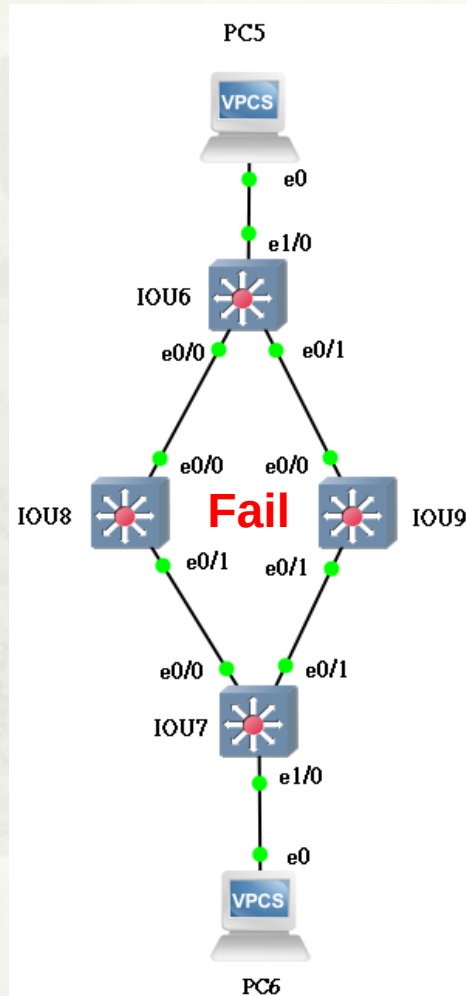
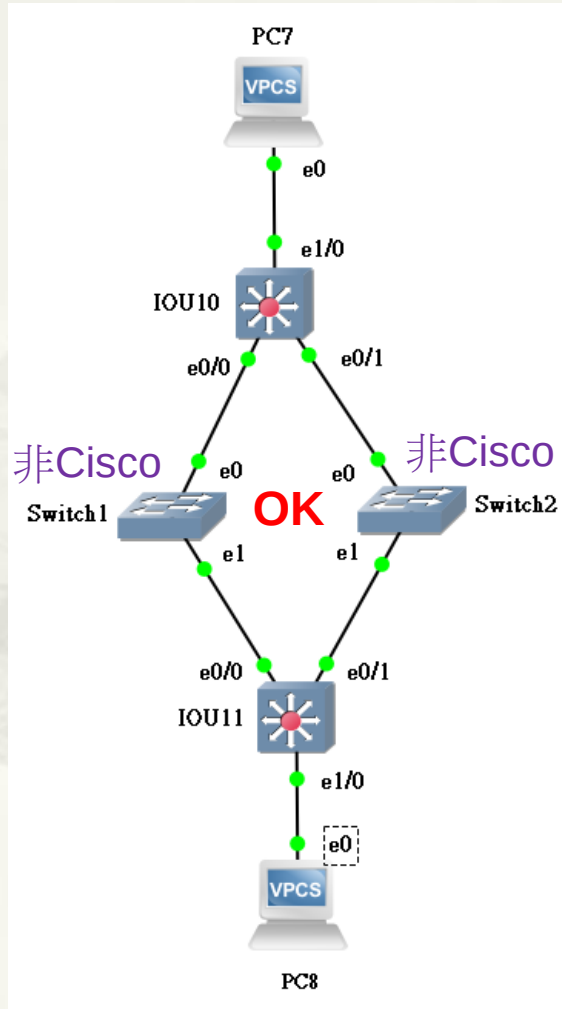
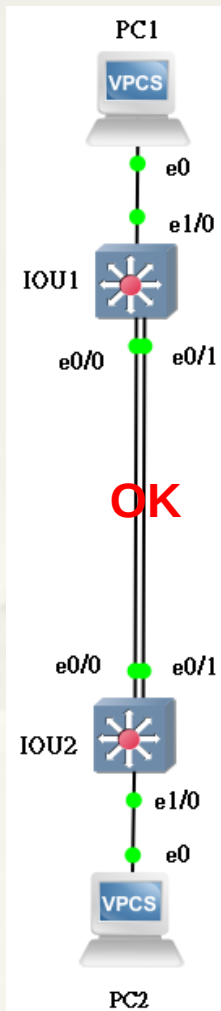
- * 限制條件

- * 線路直連 or Dark Fiber
- * Same Speed, Duplex, Trunk Mode, Vlan

channel-group mode

- * LACP
 - * active
 - * Enable LACP unconditionally
 - * 僅設定於一條 Link 時, 無法 up.
 - * passive
 - * Enable LACP only if a LACP device is detected
- * PAgP: 兩端必須皆是 Cisco 設備
 - * auto
 - * Enable PAgP only if a PAgP device is detected
 - * desirable
 - * Enable PAgP unconditionally
- * No protocol
 - * on
 - * Static. 兩端不交換資訊 (無任何 protocol)
 - * 僅設定於一條 Link 時, 可以 up.

租用點對點電路是否支援 Ether Channel ?



* LACP, PAgP

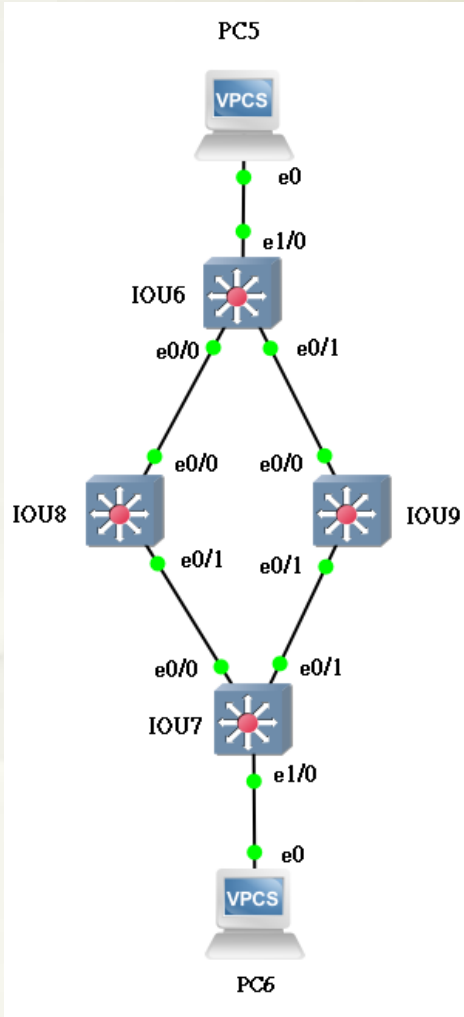
- * Layer2 protocol
- * 運作於設備與設備之間
- * Cisco 設備收到協定封包後，會以為是要跟它建立 Ether Channel，因此不允許封包穿越
- * 非 Cisco 設備(無網管功能)因為不認得此封包，因此協定封包可順利穿越

LACP protocol (Mode Active)

- * (config-if)# channel-group 1 mode active
- * IOU6, IOU7: # sh etherchannel summary

Group	Port-channel	Protocol	Ports	
1	Po1(SD)	LACP	Et0/0(s)	Et0/1(s)

- * IOU6, IOU7:
 - * *Jun 17 07:15:26.229: %EC-5-L3DONTBNDL2: Et0/0 suspended: LACP currently not enabled on the remote port.
 - * *Jun 17 07:15:26.862: %EC-5-L3DONTBNDL2: Et0/1 suspended: LACP currently not enabled on the remote port.
- * 彼此皆無法收到交換訊息

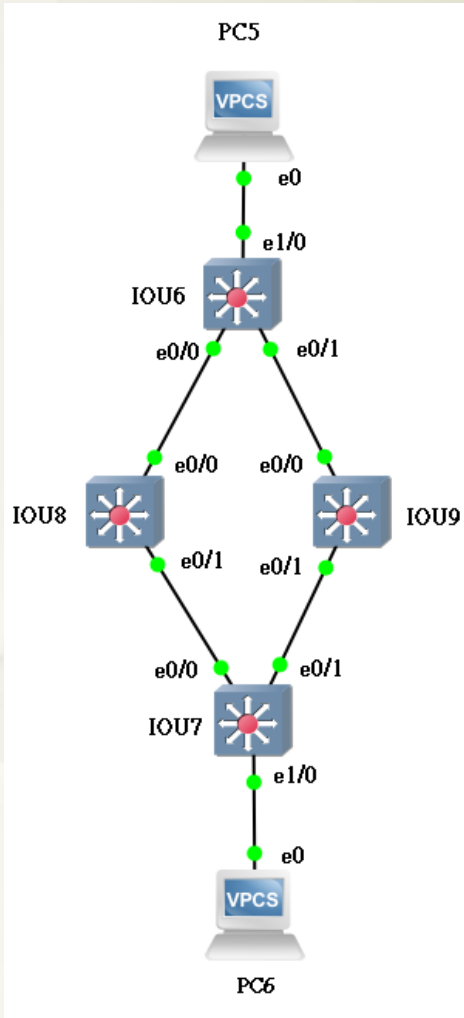


PAgP protocol (Mode Desirable)

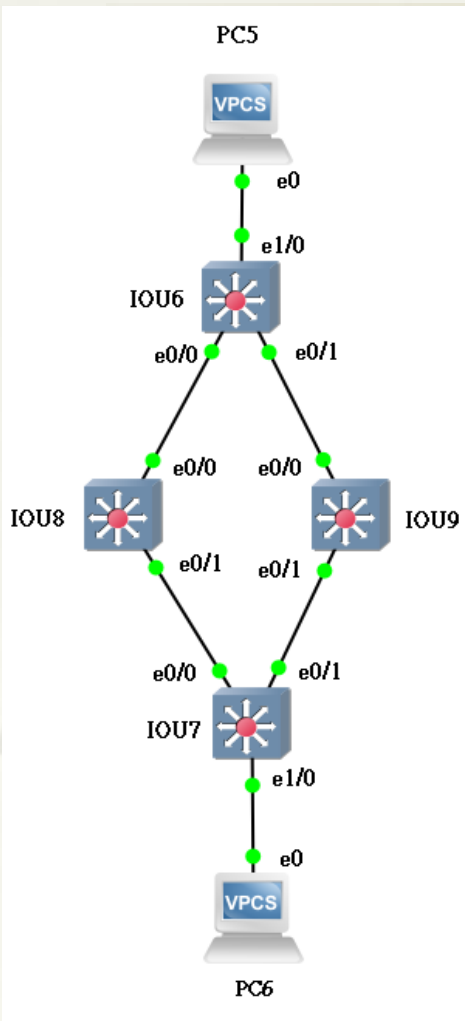
- * (config-if)# channel-group 1 mode desirable
- * IOU6, IOU7: # sh etherchannel summary

Group	Port-channel	Protocol	Ports	
1	Po1(SD)	PAgP	Et0/0(I)	Et0/1(I)

- * 彼此皆無法收到交換訊息



No protocol (Mode On)



IOU6# sh int status

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	1	auto	auto	unknown
Et0/1		connected	1	auto	auto	unknown
Et0/2		connected	1	auto	auto	unknown
Et0/3		connected	1	auto	auto	unknown
Et1/0		connected	1	auto	auto	unknown
Et1/1		connected	1	auto	auto	unknown
Et1/2		connected	1	auto	auto	unknown
Et1/3		connected	1	auto	auto	unknown
Et2/0		connected	1	auto	auto	unknown
Et2/1		connected	1	auto	auto	unknown
Et2/2		connected	1	auto	auto	unknown
Et2/3		connected	1	auto	auto	unknown
Et3/0		connected	1	auto	auto	unknown
Et3/1		connected	1	auto	auto	unknown
Et3/2		connected	1	auto	auto	unknown
Et3/3		connected	1	auto	auto	unknown
Po1		connected	1	auto	auto	auto

IOU7#sh int status

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		err-disabled	1	auto	auto	unknown
Et0/1		err-disabled	1	auto	auto	unknown
Et0/2		connected	1	auto	auto	unknown
Et0/3		connected	1	auto	auto	unknown
Et1/0		connected	1	auto	auto	unknown
Et1/1		connected	1	auto	auto	unknown
Et1/2		connected	1	auto	auto	unknown
Et1/3		connected	1	auto	auto	unknown
Et2/0		connected	1	auto	auto	unknown
Et2/1		connected	1	auto	auto	unknown
Et2/2		connected	1	auto	auto	unknown
Et2/3		connected	1	auto	auto	unknown
Et3/0		connected	1	auto	auto	unknown
Et3/1		connected	1	auto	auto	unknown
Et3/2		connected	1	auto	auto	unknown
Et3/3		connected	1	auto	auto	unknown
Po1		err-disabled	1	auto	auto	auto

- * (config-if)# channel-group 1 mode on
- * #sh etherchannel summary

Group	Port-channel	Protocol	Ports
1	Po1(SU)	-	Et0/0(P) Et0/1(P)

IOU6#

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

Group	Port-channel	Protocol	Ports
1	Po1(SD)	-	Et0/0(D) Et0/1(D)

IOU7#

- * 為何依然無法建立??

No protocol (Mode On)

* IOU6:

* sh spanning-tree

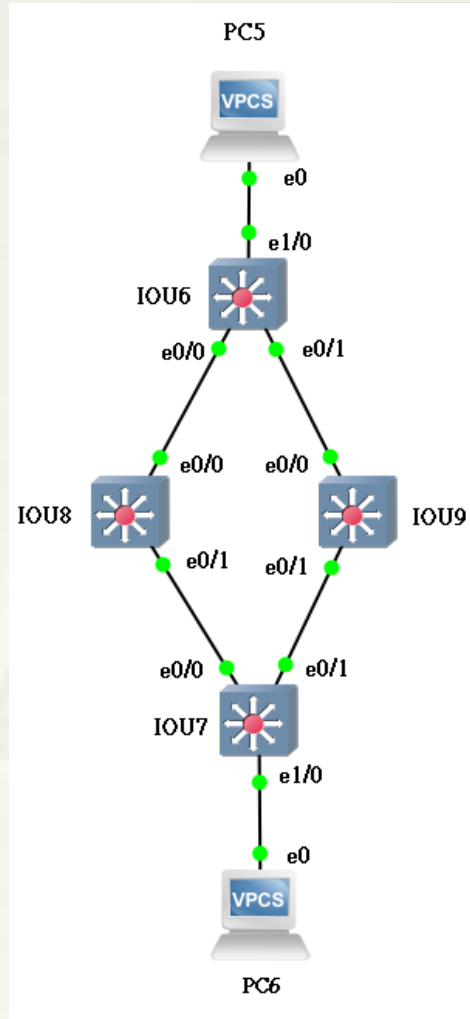
Interface	Role	Sts	Cost	Prio.Nbr	Type
Et0/2	Desg	FWD	100	128.3	Shr
Et0/3	Desg	FWD	100	128.4	Shr
Et1/0	Desg	FWD	100	128.5	Shr
Et1/1	Desg	FWD	100	128.6	Shr
Et1/2	Desg	FWD	100	128.7	Shr
Et1/3	Desg	FWD	100	128.8	Shr
Et2/0	Desg	FWD	100	128.9	Shr
Et2/1	Desg	FWD	100	128.10	Shr
Et2/2	Desg	FWD	100	128.11	Shr
Et2/3	Desg	FWD	100	128.12	Shr
Et3/0	Desg	FWD	100	128.13	Shr
Et3/1	Desg	FWD	100	128.14	Shr
Et3/2	Desg	FWD	100	128.15	Shr
Et3/3	Desg	FWD	100	128.16	Shr
Po1	Desg	<u>BLK</u>	56	128.65	<u>Shr Dispute</u>

IOU6#

* IOU7: sh log

```
*Jun 17 03:40:37.791: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Et0/0 in err-disable state
*Jun 17 03:40:37.791: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Et0/1 in err-disable state
*Jun 17 03:40:37.791: %PM-4-ERR_DISABLE: channel-misconfig (STP) error detected on Po1, putting Po1 in err-disable state
*Jun 17 03:40:38.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Jun 17 03:40:38.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*Jun 17 03:40:39.795: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
*Jun 17 03:40:39.795: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
*Jun 17 03:40:39.795: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
*Jun 17 03:40:40.801: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down
```

No protocol (Mode On) 失敗原因分析 (推測)



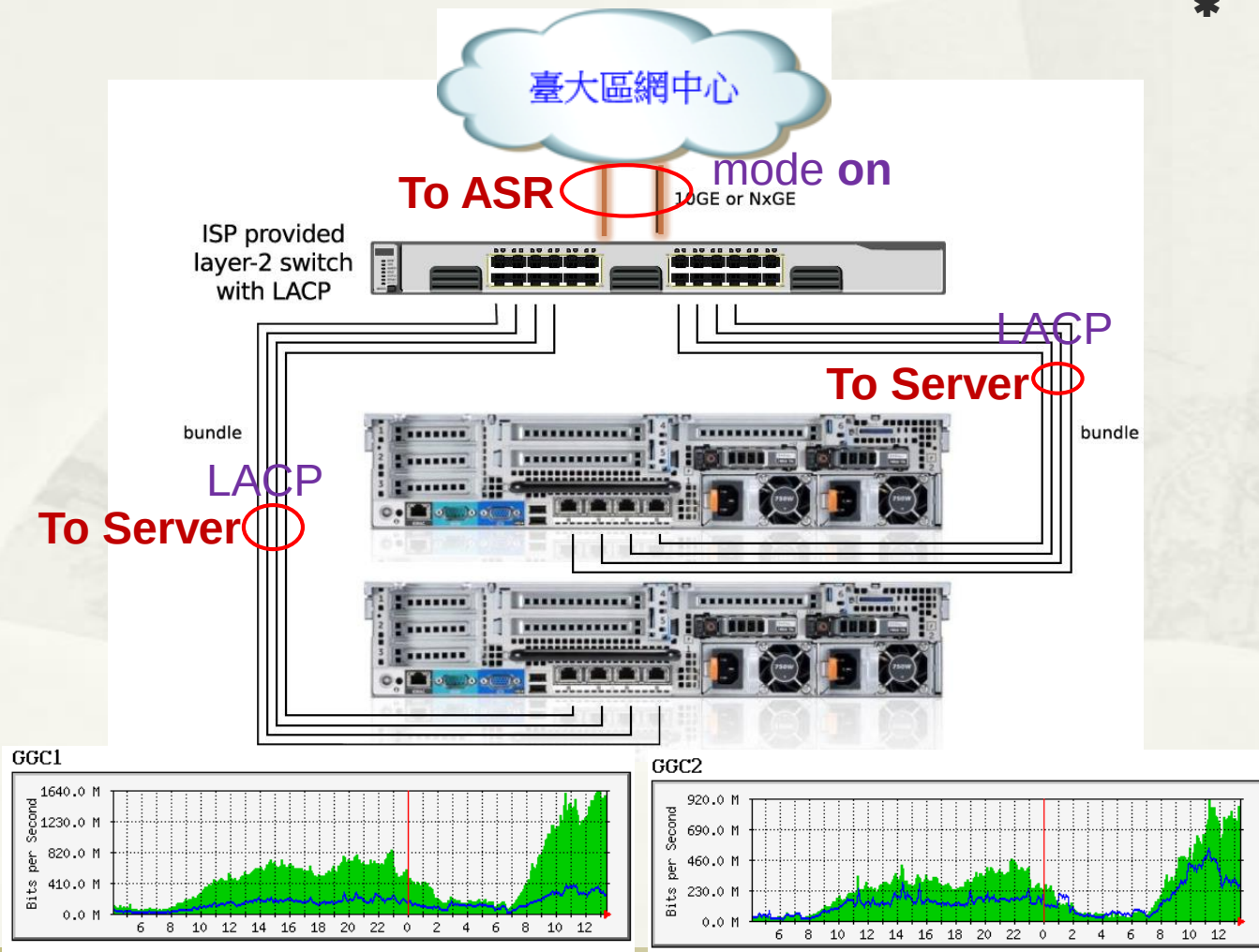
- * IOU6, IOU7: Mode On 尚未生效時
- * Spanning Tree 運作時，發現有 Loop (IOU6, IOU7, IOU8, IOU9)導致:
 - * IOU6: Po1 -> Block
 - * IOU7: Et0/0, Et0/1, Po1 -> ERR_DISABLE: channel-misconfig (STP)
- * 解決方法:
 - * IOU6/IOU7 or IOU8/IOU9 Spanning Tree 關閉
 - * no spanning-tree vlan 1
 - * IOU6, IOU7: Reload

Load Balance

- * 僅影響 output 方向封包，input 由對方決定
- * 與 channel-group mode(LACP/ PAgP/On) 無關
- * Hash 演算法
 - * src-ip
 - * src-mac :預設值(易造成流量不均)
 - *
 - * dst-ip
 - * dst-mac
 - * src-dst-ip :Src XOR Dst IP Addr – 建議值
 - * src-dst-mac :Src XOR Dst Mac Addr
 - * src-mixed-ip-port :來源 IP與Port 進行 hash演算法達成負載平衡
 - * dst-mixed-ip-port
 - * src-dst-mixed-ip-port

Ether Channel/Port Link Aggregation

Google Global Cache (Layer2)



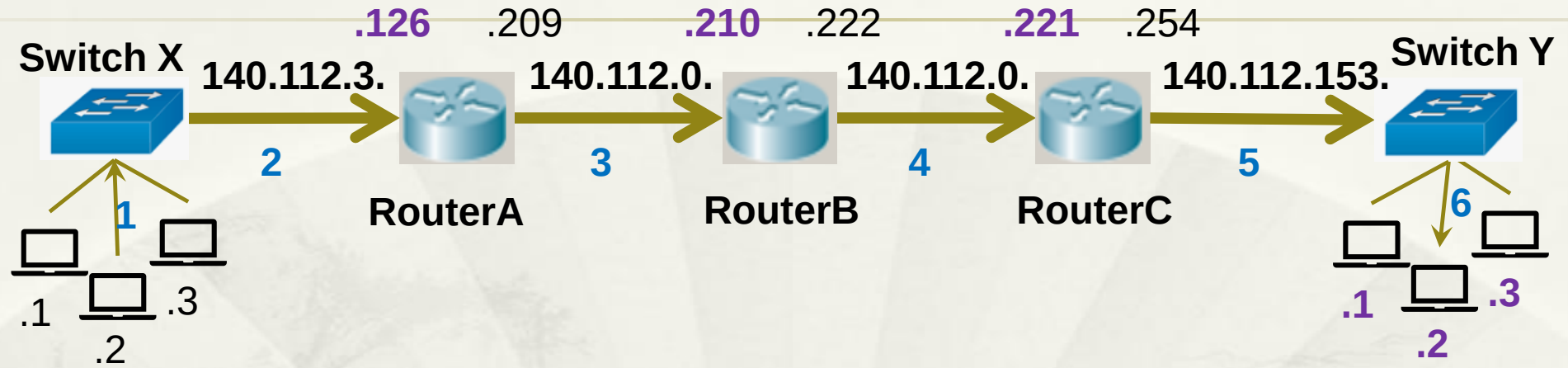
* 2960S 設定 (To ASR)

```
interface TenGigabitEthernet1/0/1  
switchport mode access  
channel-group 4 mode on
```

```
interface TenGigabitEthernet1/0/2  
switchport mode access  
channel-group 4 mode on
```

```
interface Port-channel4  
switchport mode access
```

Routing & Switching 封包變化



1 2

Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	PC x	RouterA .126	128

3

Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	RouterA .209	RouterB .210	127

4

Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	RouterB .222	RouterC .221	126

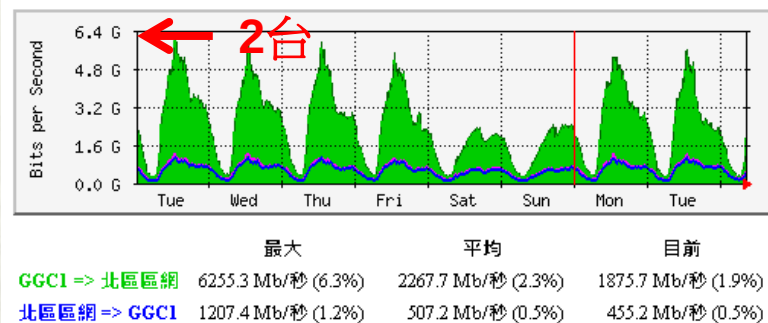
5 6

Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	RouterC .254	PC y	125

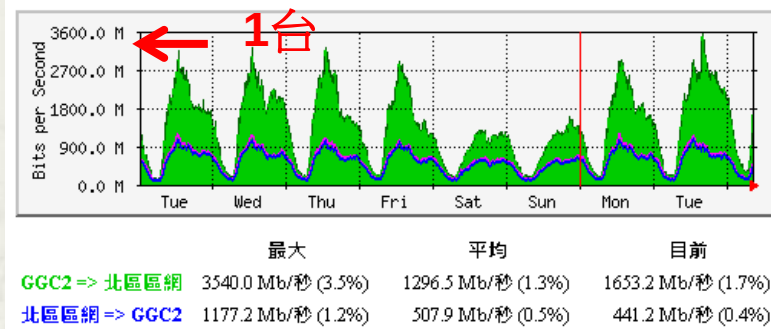
GGC C2960 To ASR(10G x 2)

- * ASR to GGC(藍線): 因 ASR 已設定 src-dst-ip，因此流量平均
- * GGC to ASR(綠線)
 - * 修改前 by src-mac: GGC Server 共 3台

每週 圖表 (30 分鐘 平均)

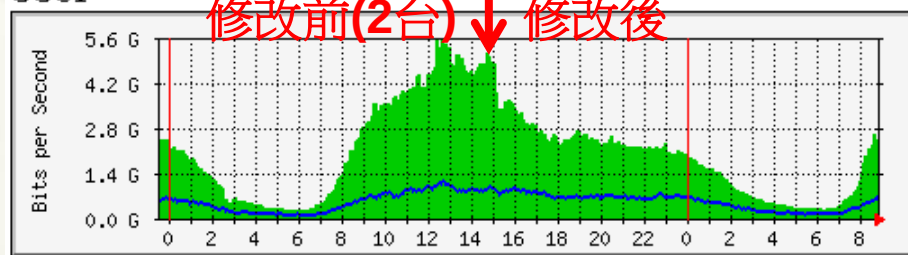


每週 圖表 (30 分鐘 平均)

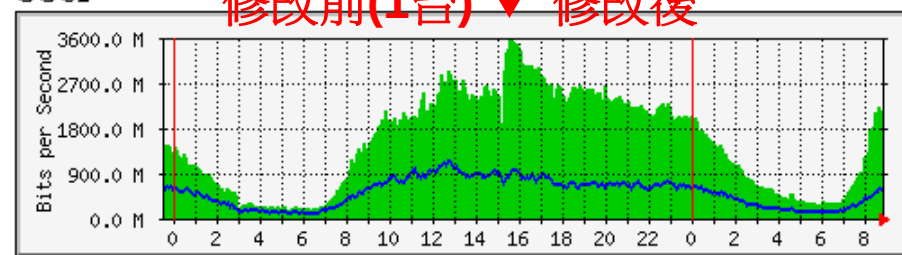


- * 修改後 by src-dst-ip

GGC1

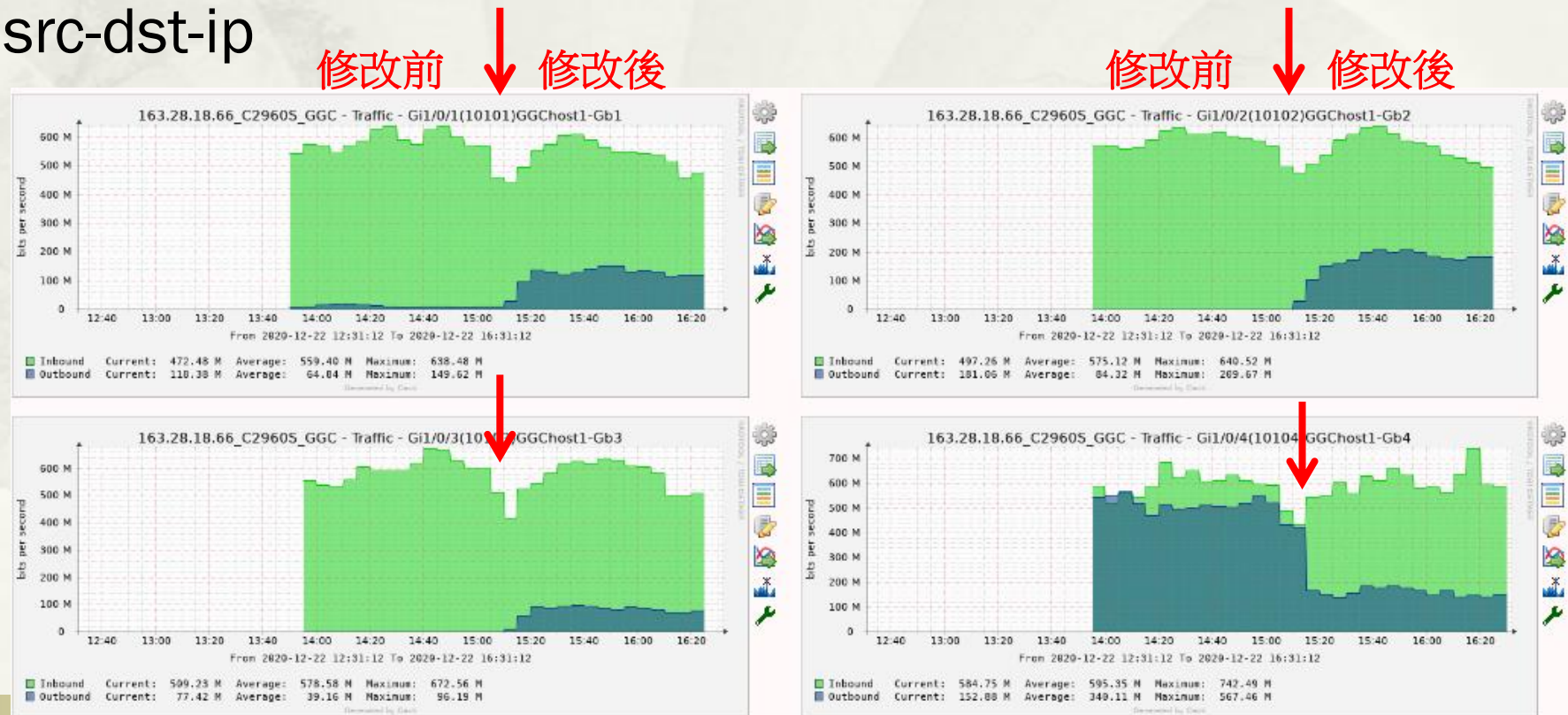


GGC2



C2960 To GGC Server 1(1G x4)

- * GGC Server to ASR(綠線): GGC Server 由 Google 設定，流量平均
- * ASR to GGC Server(藍線)
 - * 修改前 by src-mac: Only 1 MAC Addr (ASR peer IP)
 - * 修改後 by src-dst-ip



Load Balance

去回不同路

- * TCP/UDP Session 去回走同一個 Interface，需設定演算法
- * 上層 switch
 - * port-channel load-balance **src-ip**
- * 下層 switch
 - * port-channel load-balance **dst-ip**

歡迎加入區網 **Line** 群組





簡報完畢
謝謝