

109年度第二次 台北區網(臺大)網管會議

臺灣大學計資中心
游子興

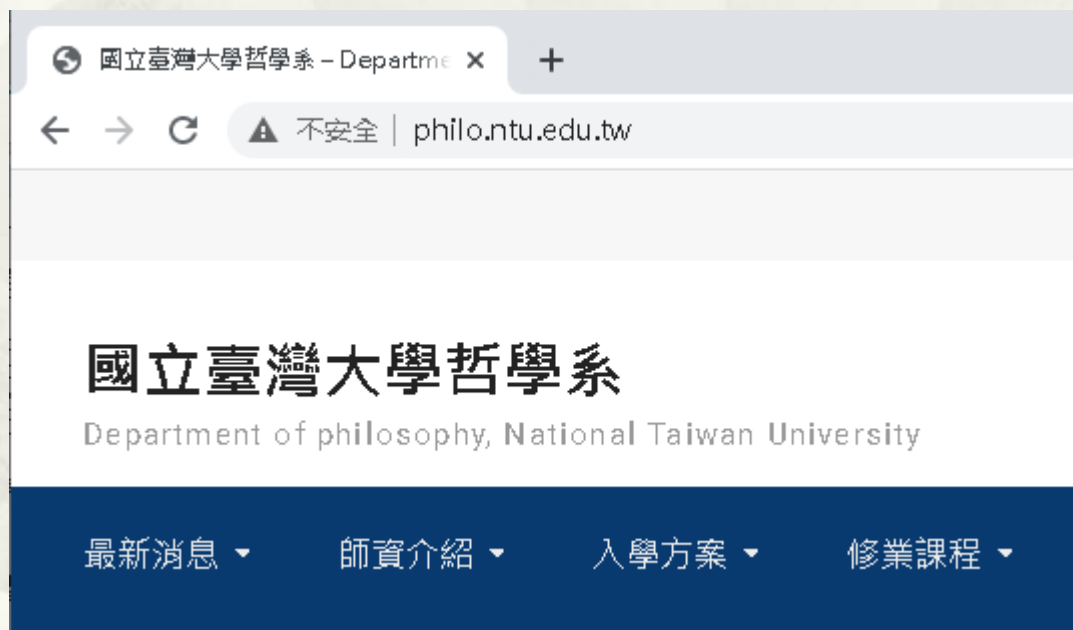
davisyou@ntu.edu.tw
3366-5008

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
	14:30~15:00	李美雯	資安Case Study分享
專題研討	15:10~16:00	國防大學_蔡文君 大考中心、北科大	教育部資通安全稽核技術與經驗分享
	16:00~16:40	游子興	TANET2020研討會創新元素與經驗分享
臨時動議		出列席人員	

https 首頁不安全

- * <https://www.philo.ntu.edu.tw/>
- * 不安全



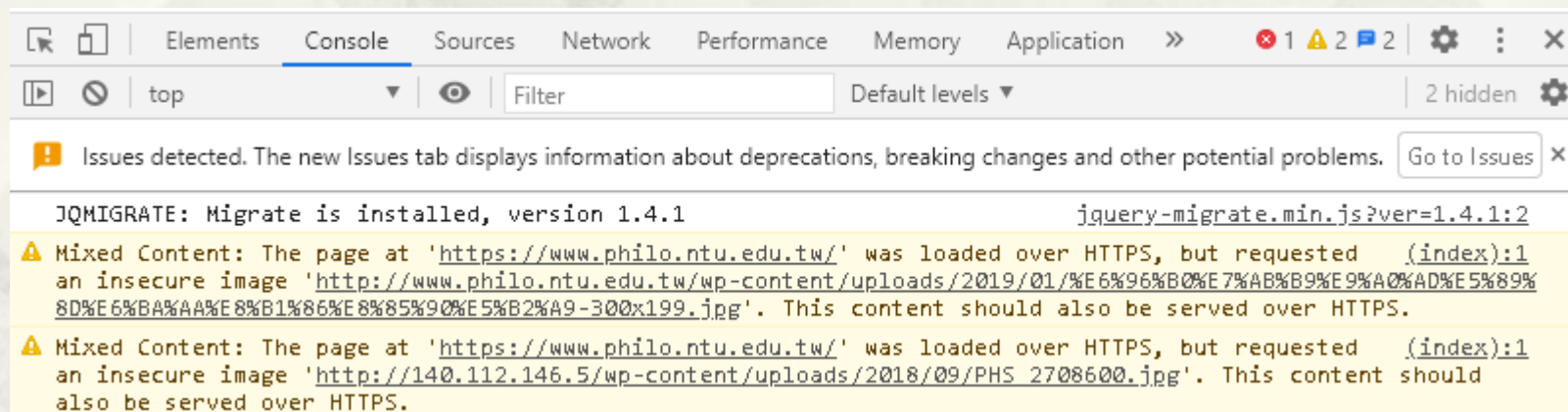
但內部頁面顯示安全

- * https://www.philo.ntu.edu.tw/?page_id=433
- * 安全



https 首頁不安全原因

- * <https://www.philo.ntu.edu.tw/>
- * 不安全原因



連線學校封包遺失

* Ping

- * From: 區網 To: 致理 peer ip
- * 無 packet lost

[illegible]

連線學校封包遺失

* Ping

- * From: 區網 To: 致理校內 IP
- * packet lost 很多

[illegible]

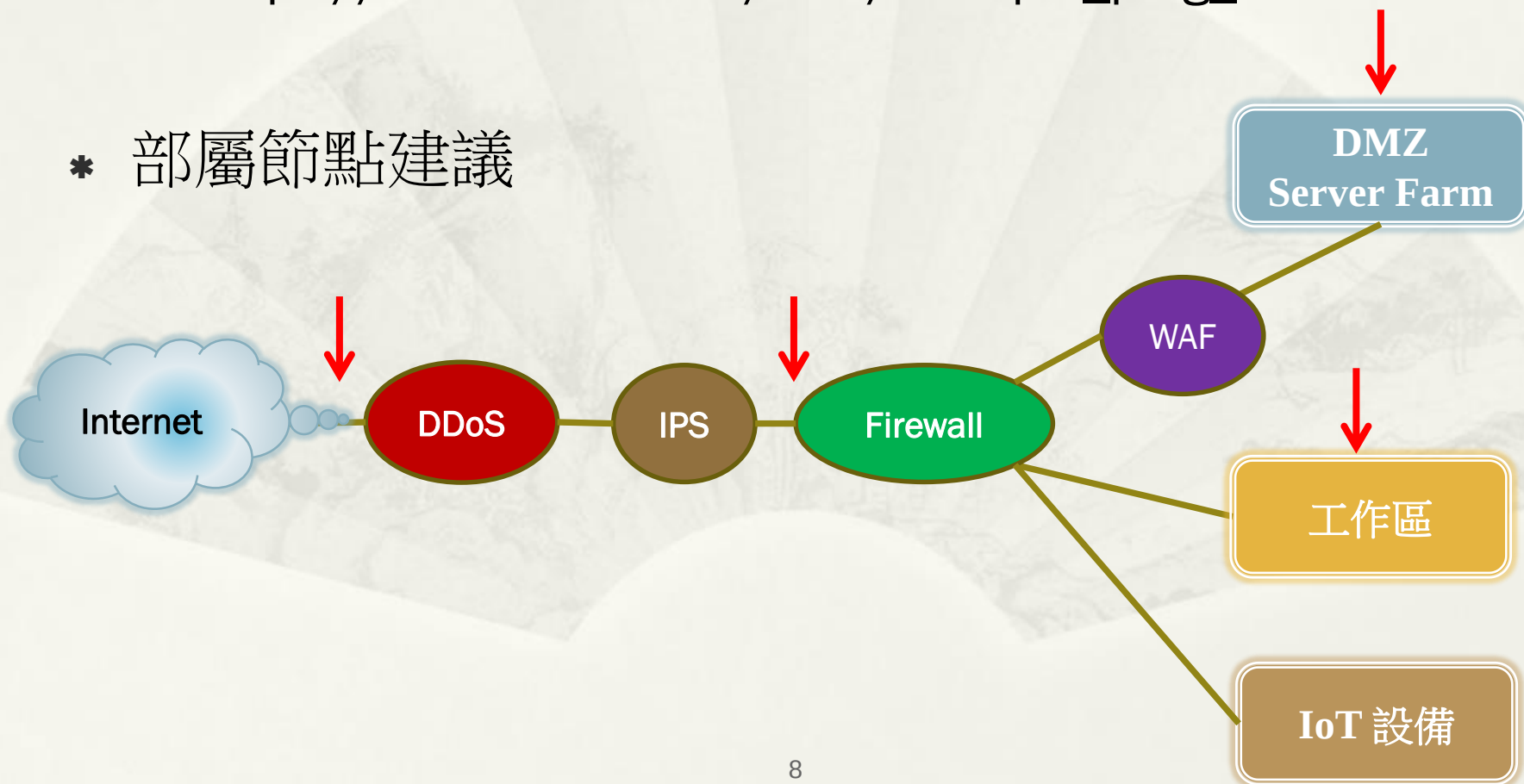
* 結論

- * 在校內網路有封包遺失

免費網路監控軟體

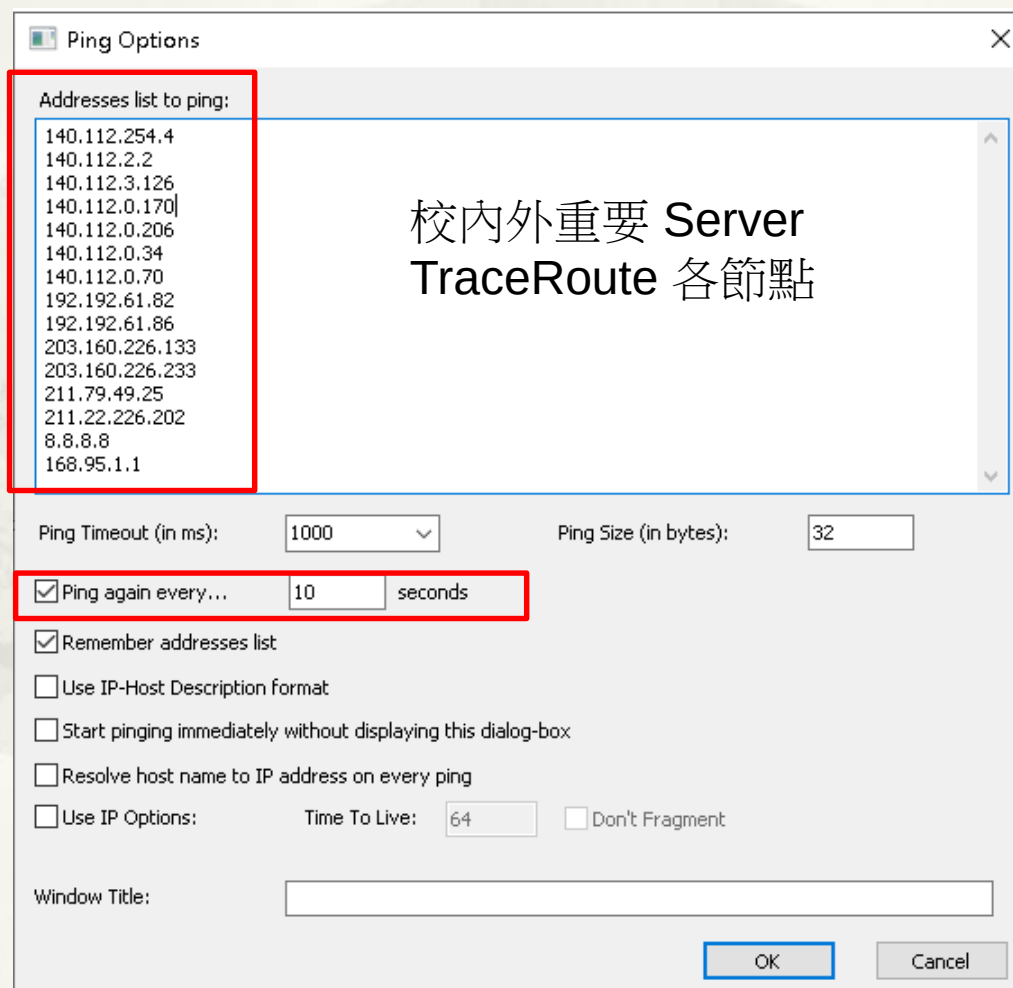
- * PingInfoView v2.10 - Ping monitor utility
 - * https://www.nirsoft.net/utils/multiple_ping_tool.html

- * 部屬節點建議



PingInfoView

* 監控 IP



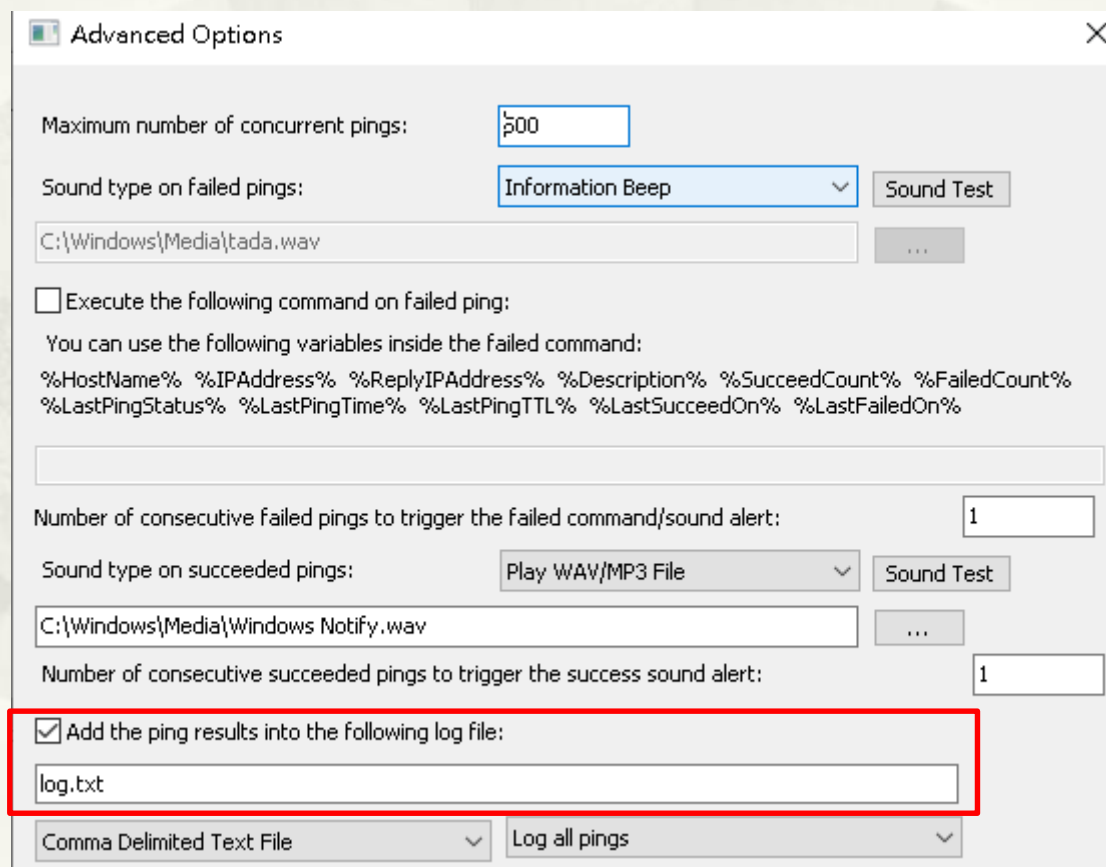
PingInfoView

IP Address	Last Failed On	Max Consecutive Failed Time	Average Ping Time	% Failed	Failed Co...	Consecu
140.112.254.4			0	0%	0	
140.112.2.2			1	0%	0	
140.112.3.126			1	0%	0	
140.112.0.170			2	0%	0	
140.112.0.206	2020/12/29 上午 04:59:32	2020/12/29 上午 04:59:32	2	0.11%	6	6
140.112.0.34	2020/12/29 上午 04:59:32	2020/12/29 上午 04:59:32	3	0.11%	6	6
140.112.0.70	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	3	0.09%	5	5
192.192.61.82	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	3	0.09%	5	5
192.192.61.86	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	4	0.07%	4	4
203.160.226.133	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	5	0.09%	5	5
203.160.226.233	2020/12/29 上午 04:59:32	2020/12/29 上午 04:59:32	5	0.13%	7	6
211.79.49.25	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	26	0.09%	5	5
211.22.226.202	2020/12/29 上午 04:59:21	2020/12/29 上午 04:59:21	5	0.11%	6	5
8.8.8.8	2020/12/29 上午 04:59:32	2020/12/29 上午 04:59:32	2	0.11%	6	6
168.95.1.1	2020/12/29 上午 04:59:32	2020/12/29 上午 04:59:32	2	0.11%	6	6

Sent On	Reply IP Address	Ping Time	Ping TTL	Ping Status	Pings Count
2020/12/29 上午 05:00:02	140.112.0.206	1	252	Succeeded	1
2020/12/29 上午 04:59:52	140.112.0.206	1	252	Succeeded	1
2020/12/29 上午 04:59:42	140.112.0.206	1	252	Succeeded	1
2020/12/29 上午 04:59:31				Request Timeout	1
2020/12/29 上午 04:59:20				Request Timeout	1
2020/12/29 上午 04:59:09				Request Timeout	1
2020/12/29 上午 04:58:58				Request Timeout	1
2020/12/29 上午 04:58:47				Request Timeout	1
2020/12/29 上午 04:58:36				Request Timeout	1
2020/12/29 上午 04:58:26	140.112.0.206	9	252	Succeeded	1
2020/12/29 上午 04:58:15	140.112.0.206	7	252	Succeeded	1
2020/12/29 上午 04:58:04	140.112.0.206	0	252	Succeeded	1

PingInfoView

* Add to log file



Advanced Options

Maximum number of concurrent pings: 500

Sound type on failed pings: Information Beep Sound Test

C:\Windows\Media\tada.wav ...

☐ Execute the following command on failed ping:

You can use the following variables inside the failed command:

%HostName% %IPAddress% %ReplyIPAddress% %Description% %SucceedCount% %FailedCount%
%LastPingStatus% %LastPingTime% %LastPingTTL% %LastSucceedOn% %LastFailedOn%

Number of consecutive failed pings to trigger the failed command/sound alert: 1

Sound type on succeeded pings: Play WAV/MP3 File Sound Test

C:\Windows\Media\Windows Notify.wav ...

Number of consecutive succeeded pings to trigger the success sound alert: 1

☒ Add the ping results into the following log file:

log.txt

Comma Delimited Text File Log all pings

PingInfoView

log.txt x	
1	2020/12/28 下午 05:59:12,140.112.2.2,140.112.2.2,,140.112.2.2,1,59,Succeeded,1
2	2020/12/28 下午 05:59:12,140.112.254.4,140.112.254.4,,140.112.254.4,1,59,Succeeded,1
3	2020/12/28 下午 05:59:12,140.112.0.206,140.112.0.206,,140.112.0.206,0,254,Succeeded,1
4	2020/12/28 下午 05:59:12,140.112.0.34,140.112.0.34,,140.112.0.34,0,62,Succeeded,1
5	2020/12/28 下午 05:59:12,140.112.0.170,140.112.0.170,,140.112.0.170,0,253,Succeeded,1
6	2020/12/28 下午 05:59:12,140.112.0.70,140.112.0.70,,140.112.0.70,0,253,Succeeded,1
7	2020/12/28 下午 05:59:12,203.160.226.133,203.160.226.133,,203.160.226.133,0,62,Succeeded,1
8	2020/12/28 下午 05:59:12,203.160.226.233,203.160.226.233,,203.160.226.233,0,62,Succeeded,1
9	2020/12/28 下午 05:59:12,192.192.61.82,192.192.61.82,,192.192.61.82,1,252,Succeeded,1
10	2020/12/28 下午 05:59:12,140.112.3.126,140.112.3.126,,140.112.3.126,2,252,Succeeded,1
11	2020/12/28 下午 05:59:12,211.22.226.202,211.22.226.202,,211.22.226.202,0,62,Succeeded,1
12	2020/12/28 下午 05:59:12,8.8.8.8,8.8.8.8,,8.8.8.8,0,120,Succeeded,1
13	2020/12/28 下午 05:59:12,168.95.1.1,168.95.1.1,,168.95.1.1,0,247,Succeeded,1
14	2020/12/28 下午 05:59:12,192.192.61.86,192.192.61.86,,192.192.61.86,2,251,Succeeded,1
15	2020/12/28 下午 05:59:12,211.79.49.25,211.79.49.25,,211.79.49.25,9,253,Succeeded,1
16	2020/12/28 下午 05:59:22,140.112.0.70,140.112.0.70,,140.112.0.70,0,253,Succeeded,1
17	2020/12/28 下午 05:59:22,140.112.2.2,140.112.2.2,,140.112.2.2,1,59,Succeeded,1
18	2020/12/28 下午 05:59:22,140.112.0.206,140.112.0.206,,140.112.0.206,0,254,Succeeded,1
19	2020/12/28 下午 05:59:22,203.160.226.233,203.160.226.233,,203.160.226.233,0,62,Succeeded,1
20	2020/12/28 下午 05:59:22,140.112.0.170,140.112.0.170,,140.112.0.170,0,253,Succeeded,1
21	2020/12/28 下午 05:59:22,203.160.226.133,203.160.226.133,,203.160.226.133,0,62,Succeeded,1
22	2020/12/28 下午 05:59:22,140.112.3.126,140.112.3.126,,140.112.3.126,1,252,Succeeded,1
23	2020/12/28 下午 05:59:22,211.22.226.202,211.22.226.202,,211.22.226.202,0,62,Succeeded,1
24	2020/12/28 下午 05:59:22,192.192.61.82,192.192.61.82,,192.192.61.82,1,252,Succeeded,1
25	2020/12/28 下午 05:59:22,140.112.254.4,140.112.254.4,,140.112.254.4,1,59,Succeeded,1



ACTIVE + ACTIVE LAYER2

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

* Protocol

- * PAgP(Port Aggregation Protocol): Cisco proprietary
- * Link Aggregation Control Protocol(LACP): IEEE 802.3ad standard
- * No protocol

* Bundle Interface

- * Access Mode
- * Route Mode

* 限制條件

- * 線路直連 or Dark Fiber
- * 各線路頻寬大小相同

channel-group x mode

- * 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
- * auto
 - * Enable PAgP only if a PAgP device is detected
 - * 兩端必須皆是 Cisco 設備
- * desirable
 - * Enable PAgP unconditionally
 - * 兩端必須皆是 Cisco 設備
- * on
 - * Static. 兩端不交換資訊 (無任何 protocol)
 - * 通常用於另一端是 Server.
 - * 僅設定於一條 Link 時, 可以 up.

Ether Channel/Port Link Aggregation

* 2960S 設定

```
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
```


Load Balance

Hash 演算法

- * 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
- *
- * src-dst-ip Src XOR Dst IP Addr -- 建議設此
- * src-dst-mac Src XOR Dst Mac Addr
- *
- * dst-ip
- * dst-mac
- *
- * src-ip
- * src-mac 預設值.(易造成流量不均)

Load Balance

- * 僅影響 output 方向封包，input 由對方決定
- * Catalyst
 - * port-channel load-balance src-dst-ip
- * ASR
 - * l2vpn
 - * load-balancing flow src-dst-ip

Load Balance

Hash 演算法

#sh etherchannel load-balance

src-mac (預設值)

```
Water-C3750G-12S#sh etherchannel load-balance
EtherChannel Load-Balancing Configuration:
    src-mac

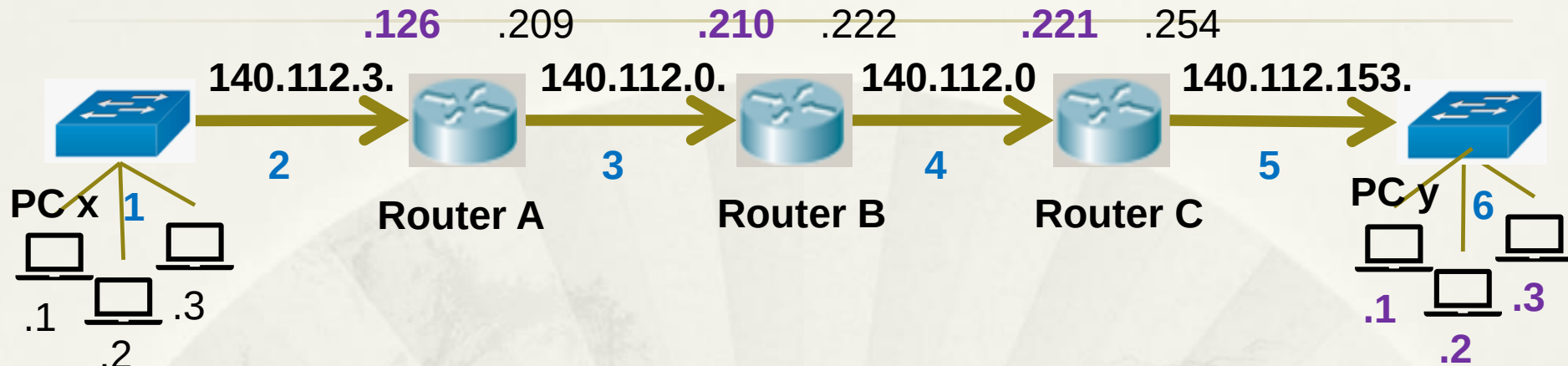
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source MAC address
IPv4: Source MAC address
IPv6: Source MAC address
```

src-dst-ip

```
Water-C3750G-12S#sh 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
```

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	Router A .126	128

3

Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	Router A .209	Router B .210	127

4

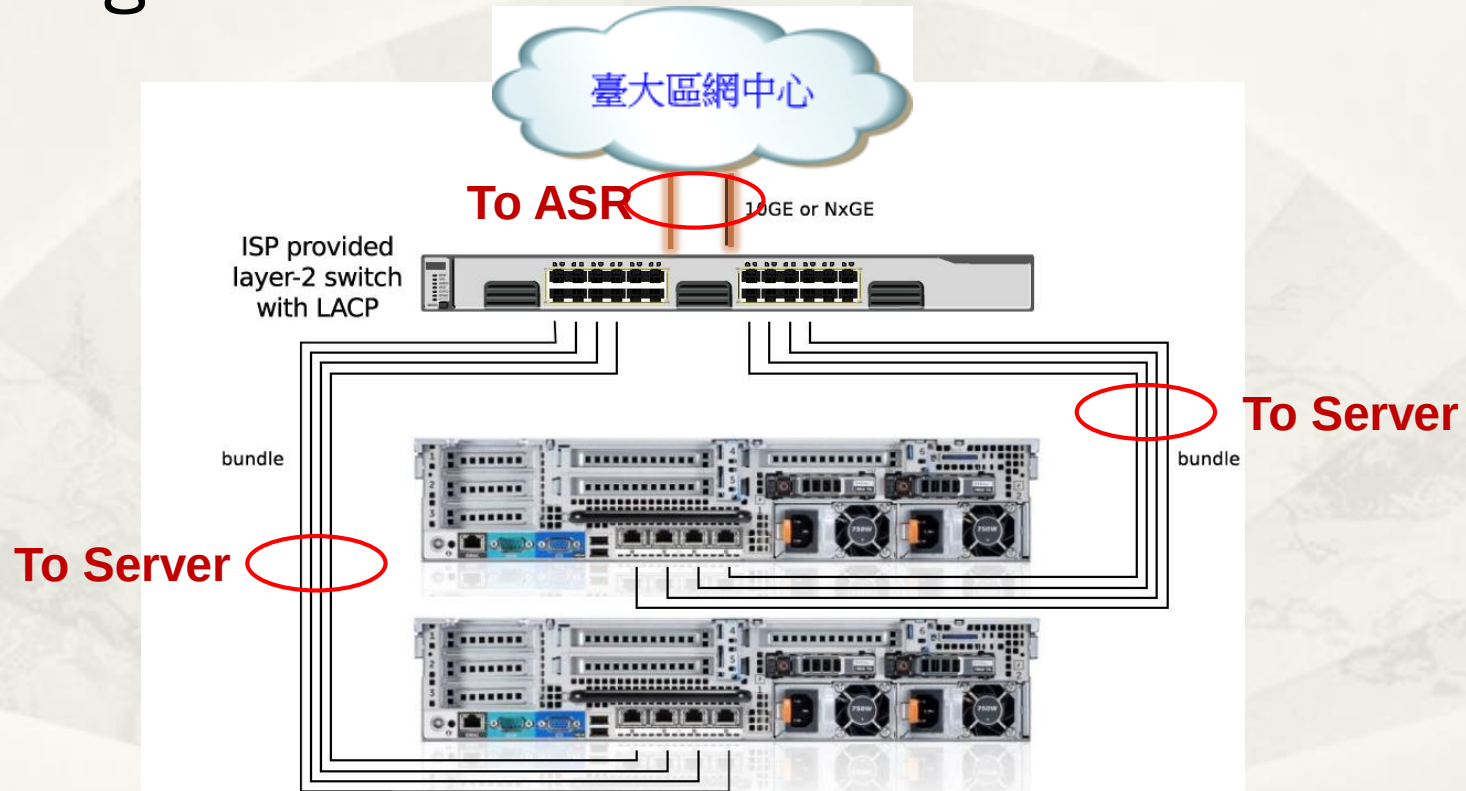
Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	Router B .222	Router C .221	126

5 6

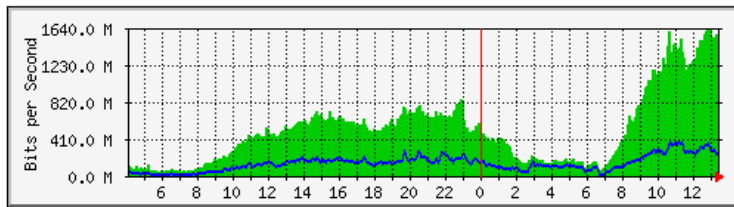
Src IP	Dest IP	Src Mac	Dest Mac	Time to Live
PC x	PC y	Router C .254	PC y	125

Ether Channel/Port Link Aggregation

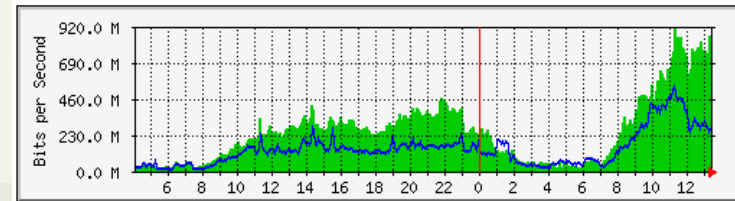
* Google Global Cache



GGC1

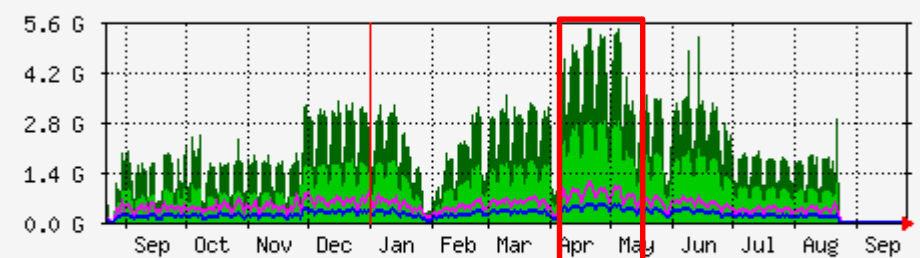


GGC2



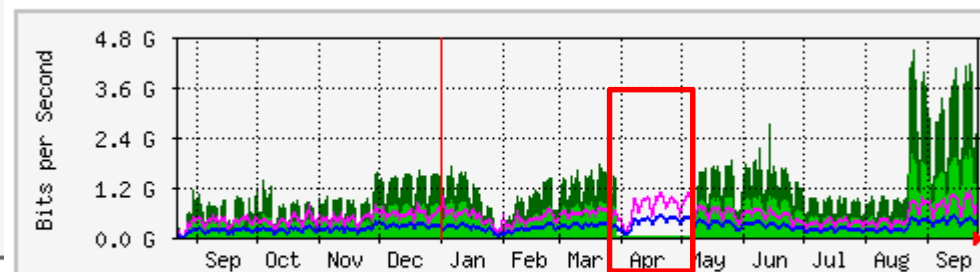
GGC LACP To ASR

手圖表 (1 天平均)



	最大	平均	目前
1 ⇒ 北區區網	5402.2 Mb/秒 (5.4%)	1144.1 Mb/秒 (1.1%)	0.0 b/秒 (0.0%)
區網 ⇒ GGC1	1074.1 Mb/秒 (1.1%)	222.4 Mb/秒 (0.2%)	0.0 b/秒 (0.0%)

每年圖表 (1 天平均)

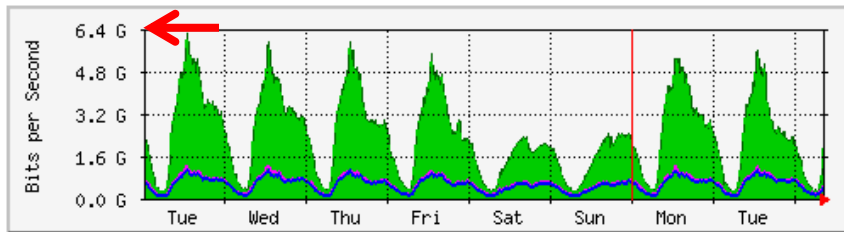


	最大	平均	目前
GGC2 ⇒ 北區區網	4502.1 Mb/秒 (4.5%)	543.6 Mb/秒 (0.5%)	2150.8 Mb/秒 (2.2%)
北區區網 ⇒ GGC2	1092.8 Mb/秒 (1.1%)	237.4 Mb/秒 (0.2%)	447.2 Mb/秒 (0.4%)

GGC LACP To ASR (2 連線)

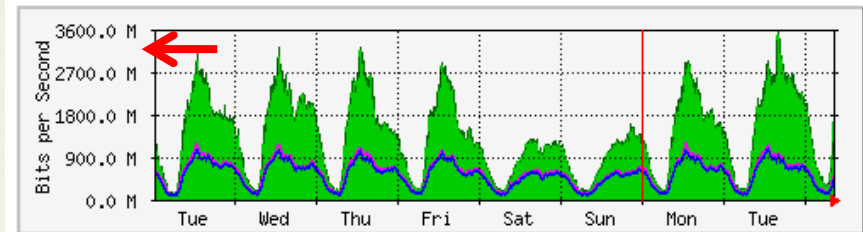
* 修改前

每週 圖表 (30 分鐘 平均)



	最大	平均	目前
GGC1 => 北區區網	6255.3 Mb/秒 (6.3%)	2267.7 Mb/秒 (2.3%)	1875.7 Mb/秒 (1.9%)
北區區網 => GGC1	1207.4 Mb/秒 (1.2%)	507.2 Mb/秒 (0.5%)	455.2 Mb/秒 (0.5%)

每週 圖表 (30 分鐘 平均)

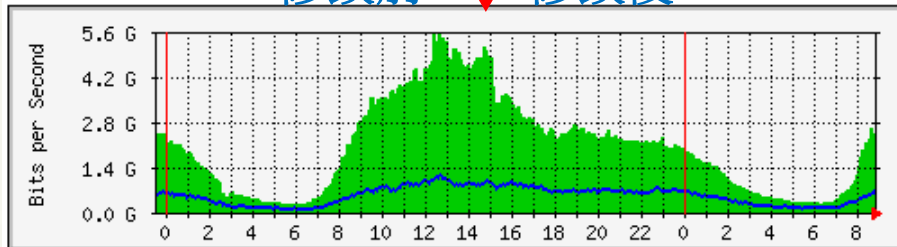


	最大	平均	目前
GGC2 => 北區區網	3540.0 Mb/秒 (3.5%)	1296.5 Mb/秒 (1.3%)	1653.2 Mb/秒 (1.7%)
北區區網 => GGC2	1177.2 Mb/秒 (1.2%)	507.9 Mb/秒 (0.5%)	441.2 Mb/秒 (0.4%)

* 修改前後差異

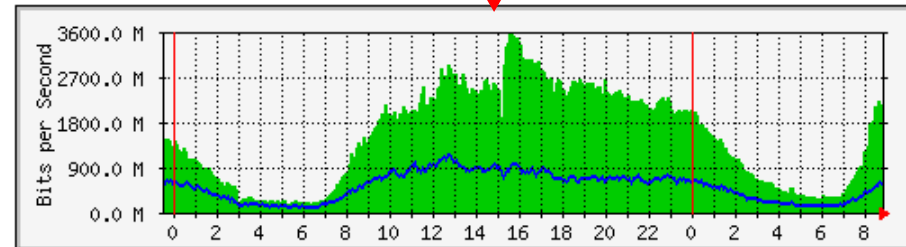
GGC1

修改前 ↓ 修改後



GGC2

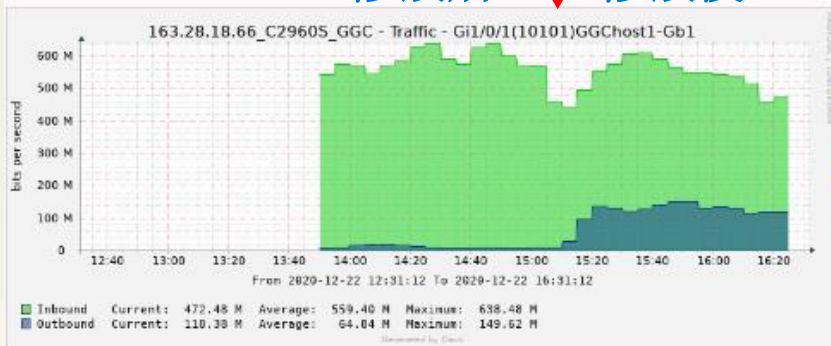
修改前 ↓ 修改後



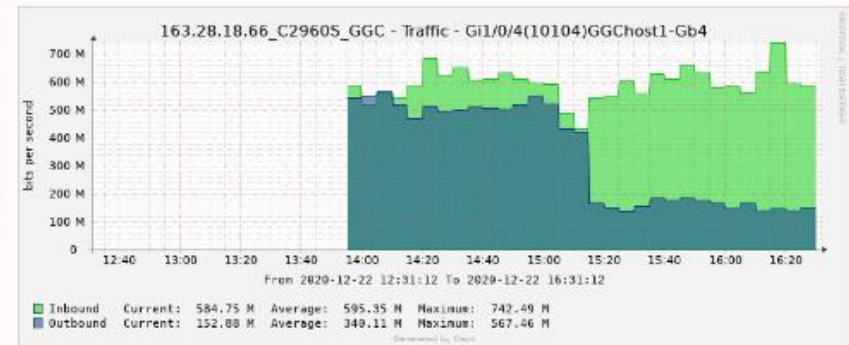
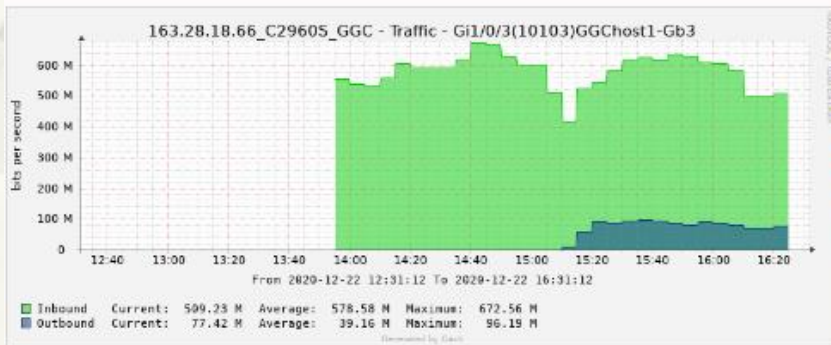
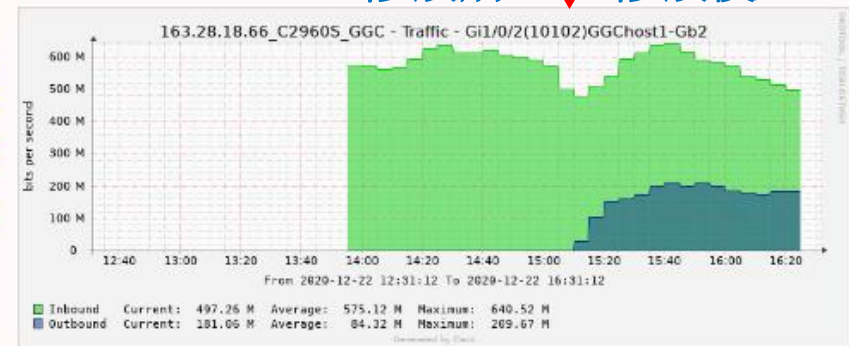
GGC LACP

To Dell Server 1 ASR (4 連線)

修改前 ↓ 修改後



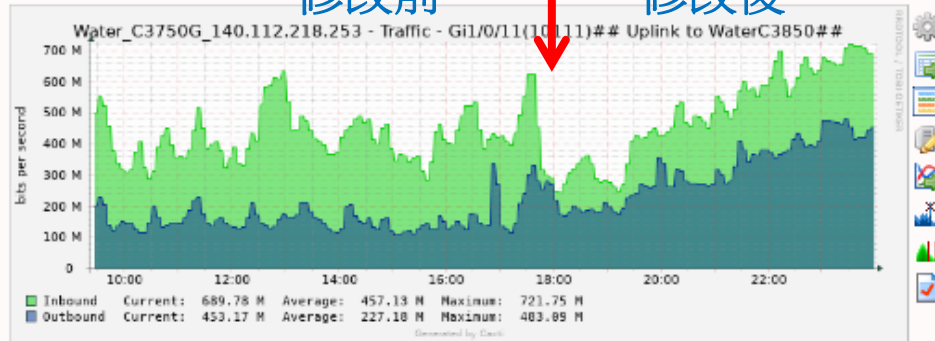
修改前 ↓ 修改後



水源校區 3750G 流量圖 To C3850

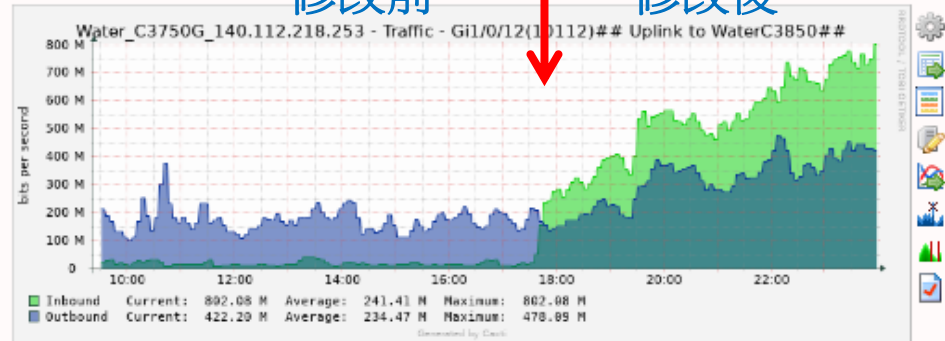
修改前

修改後



修改前

修改後



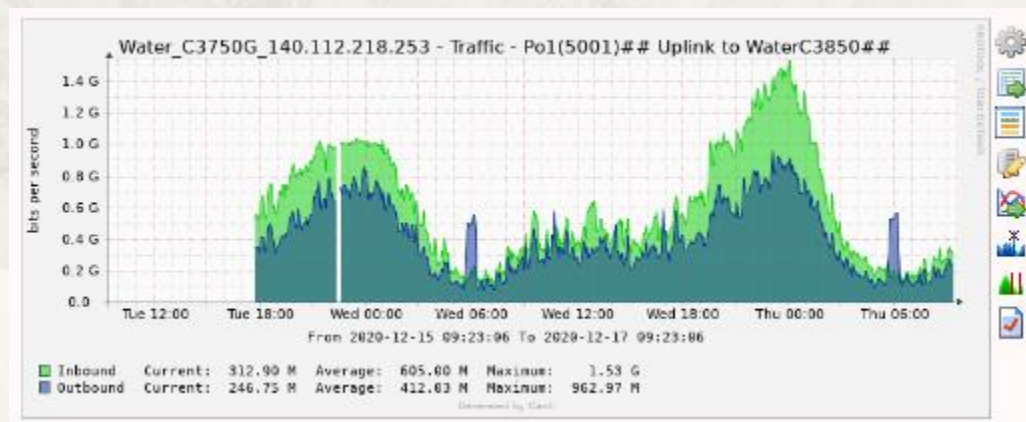
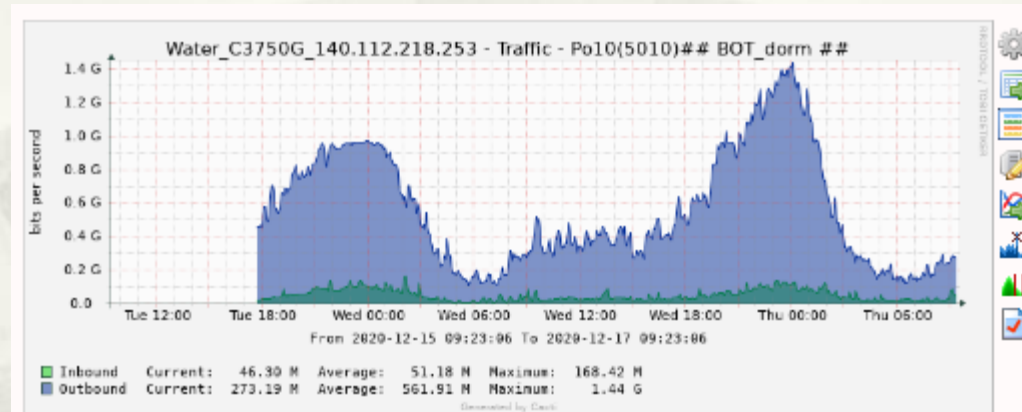
水源校區 3750G 介面流量

To BOT Dorm

```
Water-C3750G-12S#sh int g1/0/1
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is dc7b.94e4.0e01 (bia dc7b.94e4.0e01)
  Description: ## BOT_dorm ##
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 69/255, rxload 12/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 1000Mb/s, link type is auto, media type is 1000BaseLX SFP
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:14, output 00:00:19, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 533612
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 48576000 bits/sec, 11192 packets/sec
  30 second output rate 272814000 bits/sec, 29058 packets/sec
```

```
Water-C3750G-12S#sh int g1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is dc7b.94e4.0e02 (bia dc7b.94e4.0e02)
  Description: ## BOT_dorm ##
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 1000Mb/s, link type is auto, media type is 1000BaseLX SFP
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:29, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 287560
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 10270000 bits/sec, 5439 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
```

水源校區 流量圖



Load Balance

去回不同路

- * 希望固定同 session 要走同一個Interface，不要有左去右回的現象，需設定LACP演算法
- * 上層switch
 - * link-aggregation load-sharing mode source-ip
 - * port link-type trunk
 - * port trunk permit vlan all
- * 下層switch
 - * link-aggregation load-sharing mode destination-ip
 - * port link-type trunk
 - * port trunk permit vlan all



簡報完畢
謝謝