107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

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	資安事件說明
	14:30~15:10	李美雯	資安Case Study分享
專題研討	15:20~16:20	台師大:陳昱甫	國立臺灣師範大學網路電話系統建置暨使用經驗分享
	16:20~17:00	游子興	TCP-based 網路品質監控
臨時動議		出列席人員	

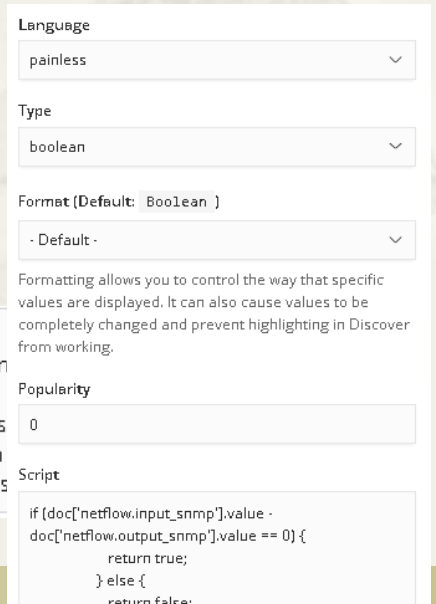
Routing Loop

偵測方法

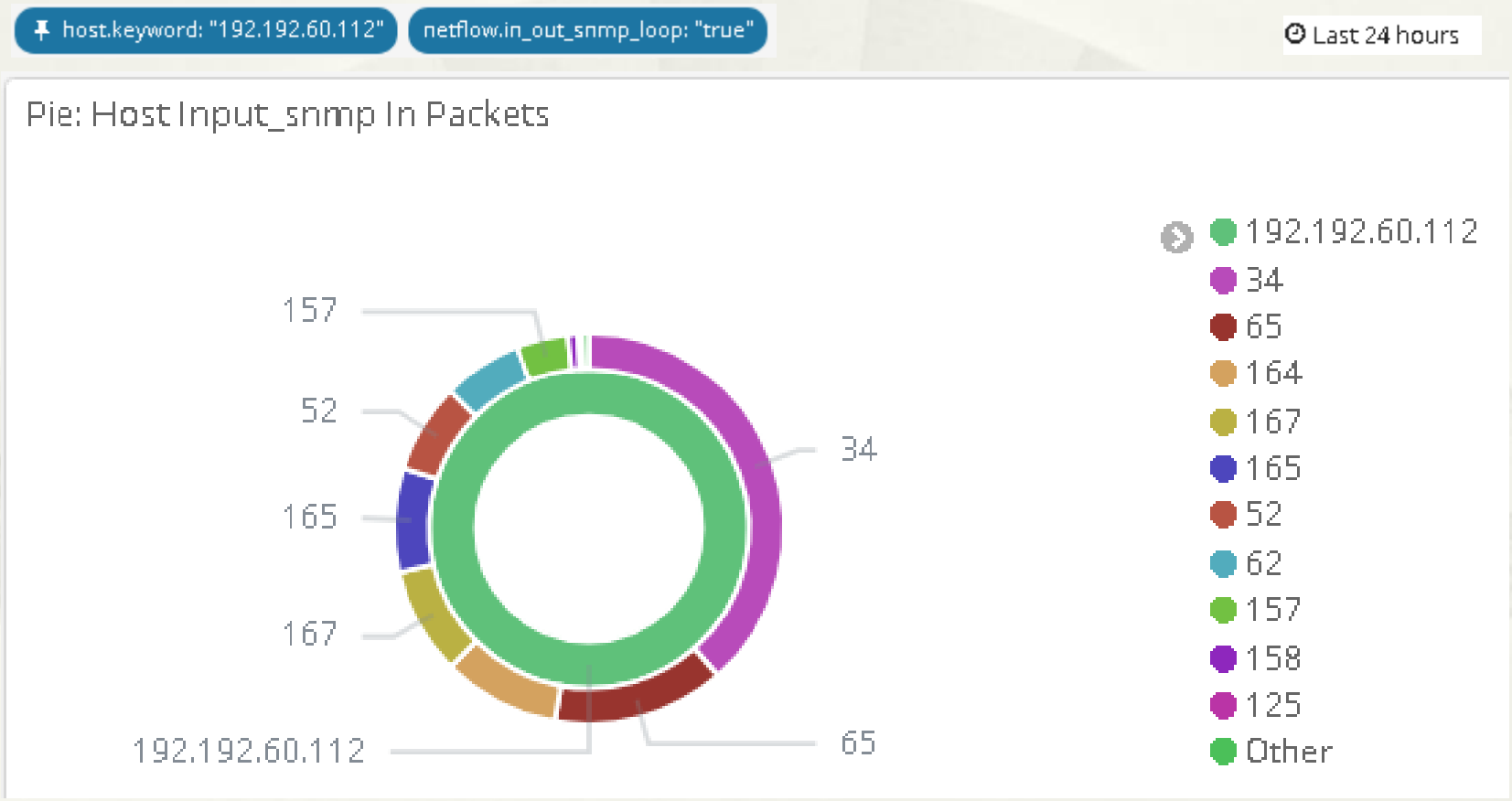
- 原理
  - input_snmp 等於 output_snmp
- 設定
  - Kibana: Script Field

```
if (doc['netflow.input_snmp'].value - doc['netflow.output_snmp'].value == 0)
{
  return true;
} else {
  return false;
}
```

netflow.in_out_snmp_loop	painless	if (doc['netflow.input_sn].value - doc['netflow.output_s p'].value == 0) { return true; } else { return fals



臺大區網路由器
Routing Loop 介面 (封包數大到小)



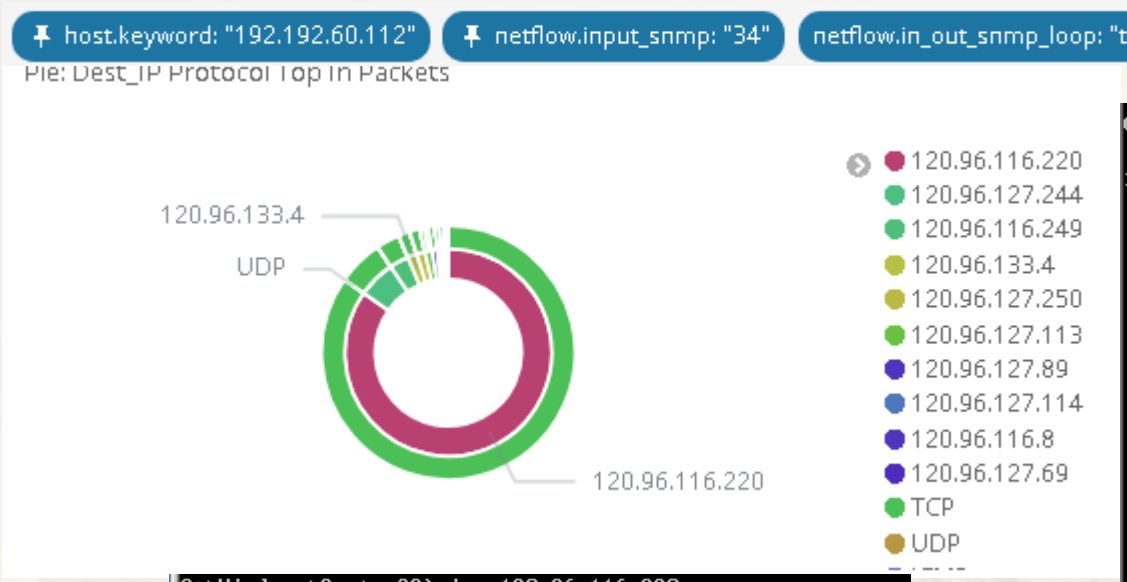
銘傳大學

擁有網段

* interface GigabitEthernet0/8/0/2
* description ## 銘傳大學_CHT-288AT-215245 ##
* ipv4 address 192.192.7.101 255.255.255.252

* #sh route next-hop 192.192.7.102
* S 120.96.80.0/20 [1/0] via 192.192.7.102, 1y19w
* S 120.96.96.0/19 [1/0] via 192.192.7.102, 1y19w
* S 120.96.128.0/20 [1/0] via 192.192.7.102, 1y19w

Routing Loop IP




```
C:\Windows\System32>ping 120.96.116.220

Ping 120.96.116.220 (使用 32 位元組的資料):
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。

120.96.116.220 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，

C:\Windows\System32>ping 120.96.127.244

Ping 120.96.127.244 (使用 32 位元組的資料):
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。
回覆自 192.192.7.102: TTL 在傳輸時到期。

120.96.127.244 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)，
```

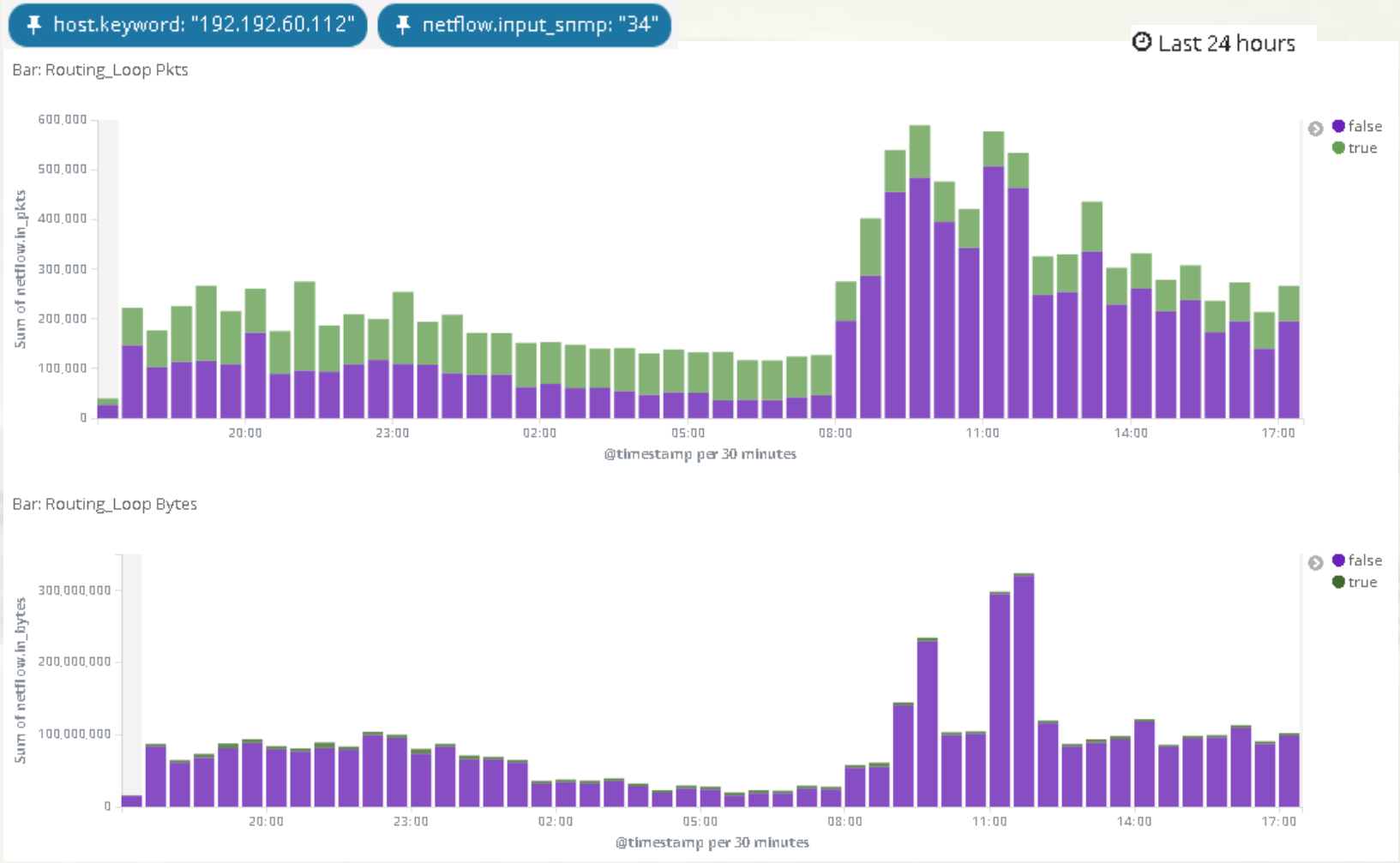
```
C:\Windows\System32>tracert -d 120.96.116.220

在上限 30 個躍點上追蹤 120.96.116.220 的路由

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  140.112.3.126
  3    <1 ms    <1 ms    <1 ms  140.112.0.170
  4     1 ms     2 ms     4 ms  140.112.0.206
  5     2 ms     3 ms     3 ms  140.112.0.70
  6     2 ms     2 ms     2 ms  192.192.7.102
  7     2 ms     2 ms     2 ms  192.192.7.101
  8     4 ms     4 ms     2 ms  192.192.7.102
  9     3 ms     2 ms     2 ms  192.192.7.101
 10     3 ms     3 ms     3 ms  192.192.7.102
 11     5 ms     6 ms     5 ms  192.192.7.101
 12     4 ms     4 ms     4 ms  192.192.7.102
 13     6 ms     4 ms     4 ms  192.192.7.101
 14     4 ms     4 ms     4 ms  192.192.7.102
 15     5 ms     4 ms     7 ms  192.192.7.101
 16     5 ms     5 ms     5 ms  192.192.7.102
 17     6 ms     7 ms     5 ms  192.192.7.101
 18     6 ms     6 ms     6 ms  192.192.7.102
 19     6 ms     6 ms     6 ms  192.192.7.101
 20     7 ms     6 ms     6 ms  192.192.7.102
 21     7 ms     6 ms     6 ms  192.192.7.101
 22     7 ms     7 ms     6 ms  192.192.7.102
 23    10 ms     8 ms     8 ms  192.192.7.101
 24     7 ms     9 ms     8 ms  192.192.7.102
 25    10 ms     8 ms     8 ms  192.192.7.101
 26     9 ms     9 ms     8 ms  192.192.7.102
 27    16 ms    11 ms     9 ms  192.192.7.101
 28     8 ms    13 ms     9 ms  192.192.7.102
 29     9 ms    10 ms    10 ms  192.192.7.101
 30    10 ms    10 ms    10 ms  192.192.7.102

追蹤完成。
```

Routing Loop IP

t	host	192.192.60.112
#	netflow.in_bits	1,056
#	netflow.in_bytes	132
◑	netflow.in_out_snmp_loop	true
#	netflow.in_pkts	3
#	netflow.input_snmp	34
💻	netflow.ipv4_dst_addr	120.96.116.209
💻	netflow.ipv4_src_addr	196.52.43.130
#	netflow.l4_dst_port	22
#	netflow.l4_src_port	65,067
#	netflow.output_snmp	34
#	netflow.protocol	6
t	netflow.protocol.keyword	TCP
#	netflow.src_tos	40
#	netflow.tcp_flags	2

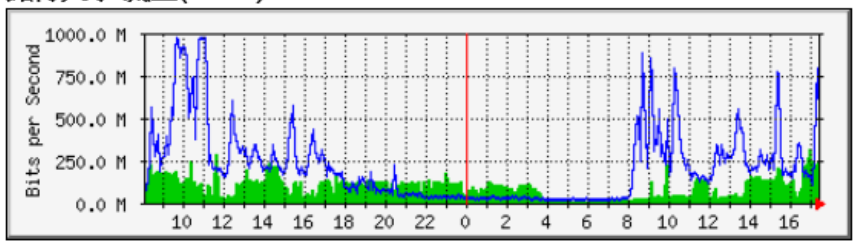
No.	Time	tcp.stream	TTL	Source	Src Port	Destination	Dest Port	Src MAC	Dst MAC	Protocol	Length	Info
2885	0.053776	70	91	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
2886	0.053776	70	90	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
2964	0.054785	70	89	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
2965	0.054785	70	88	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
3022	0.055393	70	87	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
3025	0.055393	70	86	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Out-Of-Order] 80 → 29916 [SYN, ACK
3069	0.056019	70	85	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3070	0.056019	70	84	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3136	0.056976	70	83	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3138	0.056976	70	82	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3207	0.057693	70	81	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3211	0.057694	70	80	122.226.189.53	80	120.96.116.220	29916	Cisco_2f:f7:36	Cisco_a1:0f:c4	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A
3293	0.058431	70	79	122.226.189.53	80	120.96.116.220	29916	Cisco_a1:0f:c4	Cisco_2f:f7:36	TCP	62	[TCP Retransmission] 80 → 29916 [SYN, A

Routing Loop 佔據頻寬(綠色)

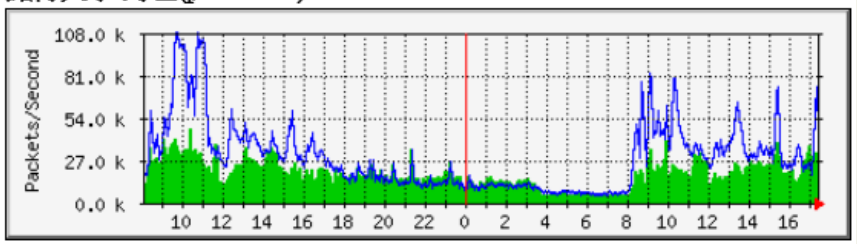


MRTG

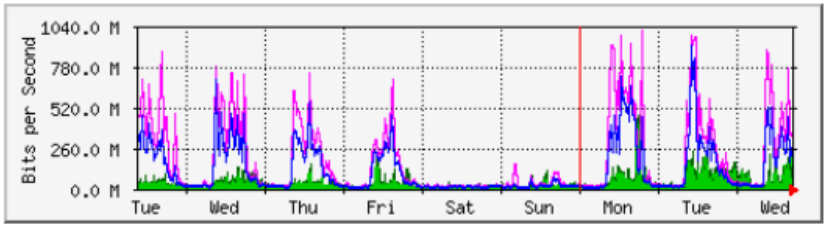
銘傳大學 流量(bit/sec)



銘傳大學 封包(packet/sec)

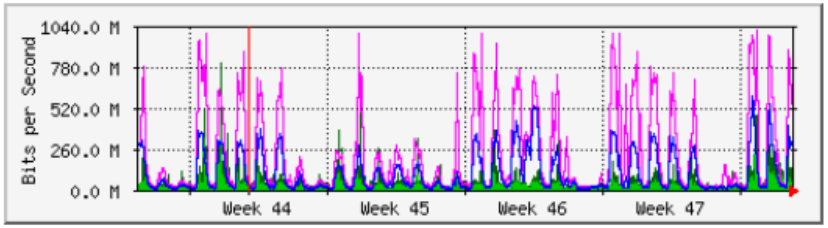


每週 圖表 (30 分鐘 平均)



	最大	平均	目前
銘傳大學 => 北區區網:	470.4 Mb/秒 (0.5%)	38.5 Mb/秒 (0.0%)	212.6 Mb/秒 (0.2%)
北區區網 => 銘傳大學:	1002.7 Mb/秒 (1.0%)	117.5 Mb/秒 (0.1%)	165.7 Mb/秒 (0.2%)

每月 圖表 (2 小時 平均)



	最大	平均	目前
銘傳大學 => 北區區網:	801.8 Mb/秒 (0.8%)	34.5 Mb/秒 (0.0%)	139.3 Mb/秒 (0.1%)
北區區網 => 銘傳大學:	1002.7 Mb/秒 (1.0%)	98.4 Mb/秒 (0.1%)	269.1 Mb/秒 (0.3%)

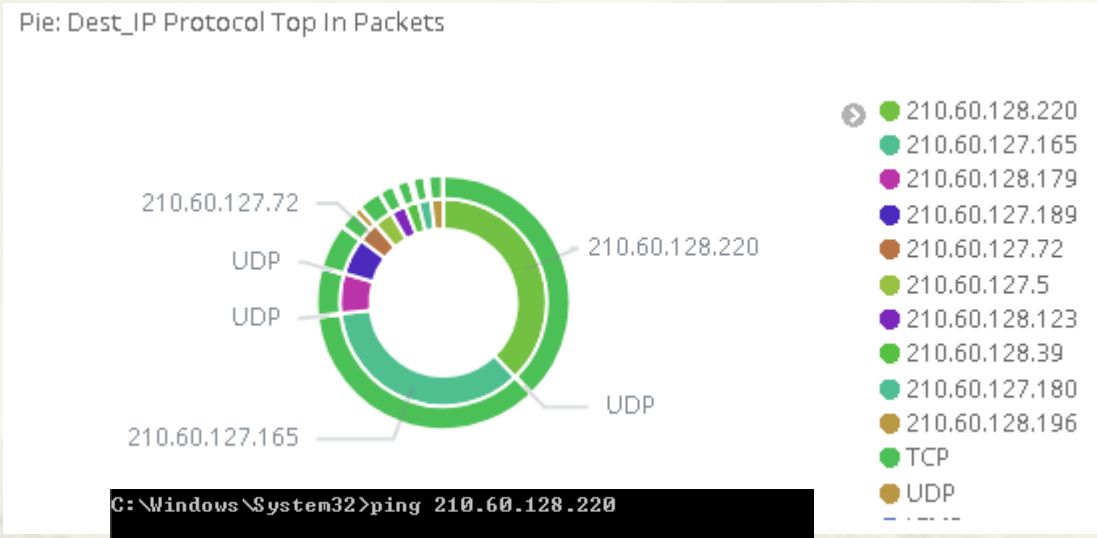
樹人家商

擁有網段

- interface GigabitEthernet0/8/1/13
- description ## 樹人家商_CHT-268YD000017 ##
- ipv4 address 192.192.7.165 255.255.255.252
-
- #sh route next-hop 192.192.7.166
- S 203.71.206.0/24 [1/0] via 192.192.7.166, 1y19w
- S 210.60.127.0/24 [1/0] via 192.192.7.166, 1y19w
- S 210.60.128.0/24 [1/0] via 192.192.7.166, 1y19w

Routing Loop IP

host.keyword: "192.192.60.112" | netflow.input_snmp: "65" | netflow.in_out_snmp_loop: "true" | Last 24 hours



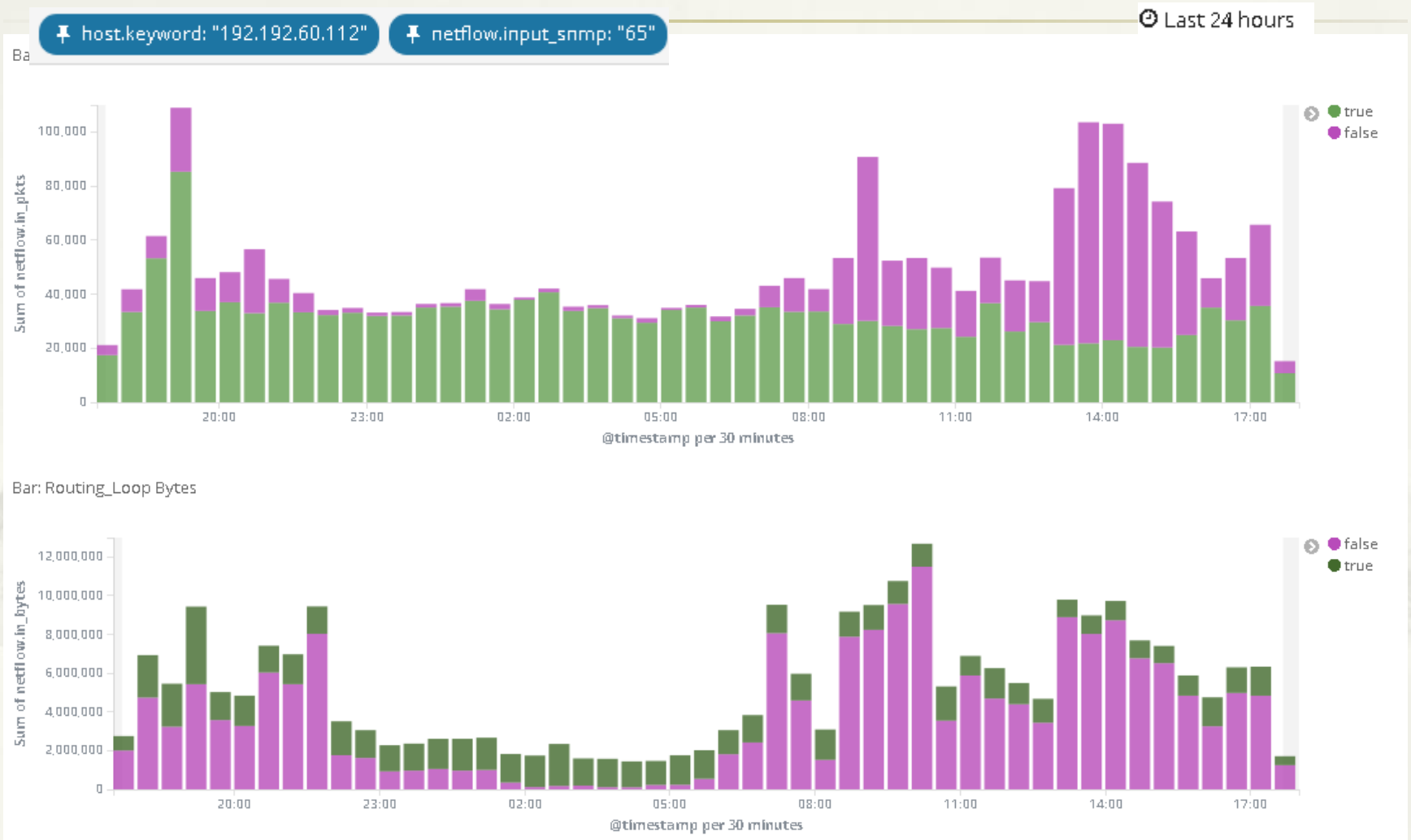

```
C:\Windows\System32>ping 210.60.128.220

Ping 210.60.128.220 (使用 32 位元組的資料):
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。

210.60.128.220 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)

C:\Windows\System32>ping 210.60.127.165

Ping 210.60.127.165 (使用 32 位元組的資料):
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。
回覆自 192.192.7.166: TTL 在傳輸時到期。

210.60.127.165 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4，已遺失 = 0 (0% 遺失)
```

```
C:\Windows\System32>tracert -d 210.60.128.220

在上限 30 個躍點上追蹤 210.60.128.220 的路由

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  140.112.3.126
  3    <1 ms    <1 ms    <1 ms  140.112.0.210
  4     1 ms     1 ms     1 ms  140.112.0.206
  5     3 ms     1 ms     1 ms  140.112.0.70
  6     3 ms     2 ms     2 ms  192.192.7.166
  7     3 ms     2 ms     2 ms  192.192.7.165
  8     3 ms     3 ms     3 ms  192.192.7.166
  9     4 ms     5 ms     4 ms  192.192.7.165
 10    10 ms    11 ms    10 ms  192.192.7.166
 11     4 ms     5 ms     4 ms  192.192.7.165
 12     6 ms     5 ms    12 ms  192.192.7.166
 13     6 ms     6 ms     6 ms  192.192.7.165
 14     7 ms     7 ms     7 ms  192.192.7.166
 15     7 ms     8 ms     7 ms  192.192.7.165
 16     8 ms    11 ms     9 ms  192.192.7.166
 17     8 ms     8 ms     8 ms  192.192.7.165
 18     9 ms     9 ms    11 ms  192.192.7.166
 19     9 ms    11 ms     9 ms  192.192.7.165
 20    17 ms    10 ms    10 ms  192.192.7.166
 21    11 ms    11 ms    10 ms  192.192.7.165
 22    11 ms    19 ms    11 ms  192.192.7.166
 23    13 ms    12 ms    12 ms  192.192.7.165
 24    22 ms    20 ms    12 ms  192.192.7.166
 25    14 ms    14 ms    13 ms  192.192.7.165
 26    13 ms    14 ms    13 ms  192.192.7.166
 27    14 ms    14 ms    13 ms  192.192.7.165
 28    14 ms    15 ms    14 ms  192.192.7.166
 29    15 ms    14 ms    14 ms  192.192.7.165
 30    16 ms    15 ms    17 ms  192.192.7.166

追蹤完成。
```

Routing Loop IP

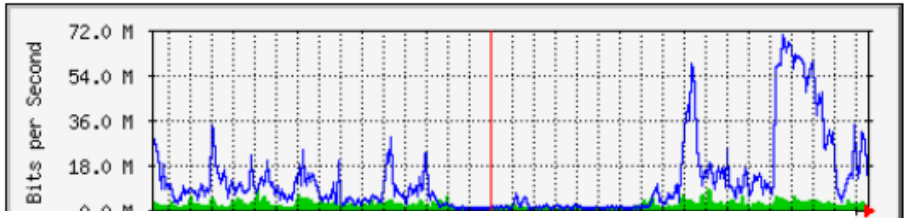
t	host	192.192.60.112
#	netflow.in_bits	320
#	netflow.in_bytes	40
◑	netflow.in_out_snmp_loop	true
#	netflow.in_pkts	1
#	netflow.input_snmp	65
💻	netflow.ipv4_dst_addr	210.60.127.193
💻	netflow.ipv4_src_addr	112.8.93.98
#	netflow.l4_dst_port	23
#	netflow.l4_src_port	49,631
#	netflow.output_snmp	65
#	netflow.protocol	6
t	netflow.protocol.keyword	TCP
#	netflow.src_tos	4
#	netflow.tcp_flags	2

Routing Loop 佔據頻寬(綠色)

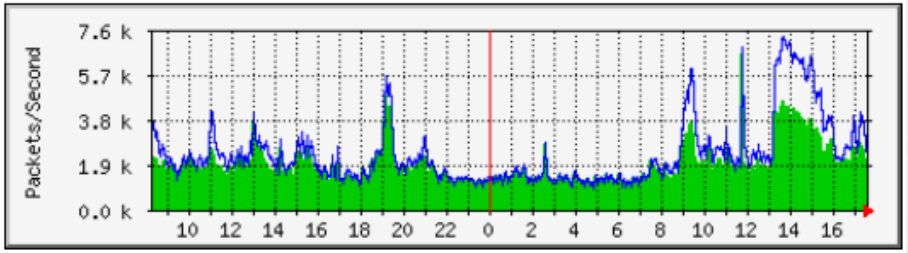


MRTG

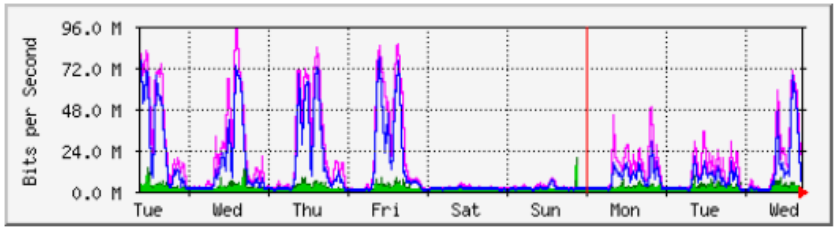
樹人家商 流量(bit/sec)



樹人家商 封包(packet/sec)

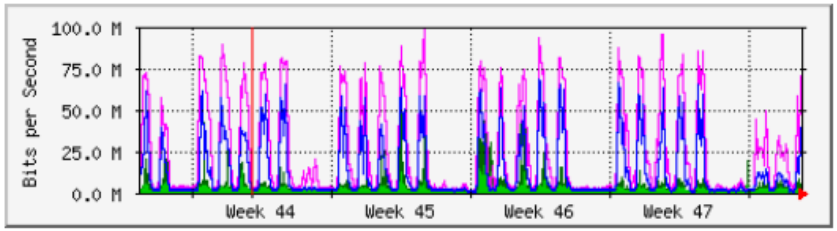


每週 圖表 (30 分鐘 平均)



	最大	平均	目前
樹人家商 => 北區區網:	19.4 Mb/秒 (0.0%)	1852.8 kb/秒 (0.0%)	2512.8 kb/秒 (0.0%)
北區區網 => 樹人家商:	94.9 Mb/秒 (0.1%)	11.0 Mb/秒 (0.0%)	17.2 Mb/秒 (0.0%)

每月 圖表 (2 小時 平均)

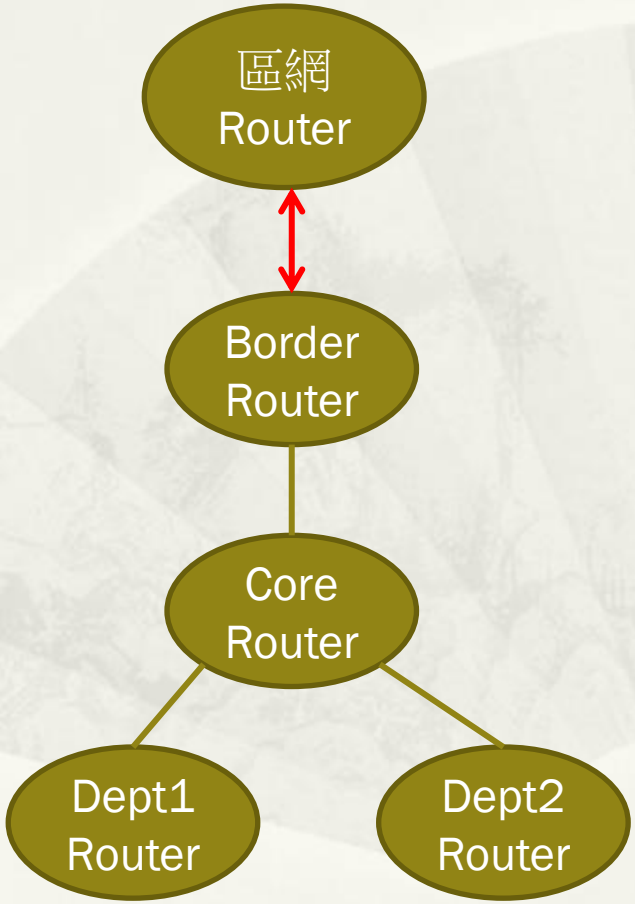


	最大	平均	目前
樹人家商 => 北區區網:	59.6 Mb/秒 (0.1%)	2422.5 kb/秒 (0.0%)	3099.4 kb/秒 (0.0%)
北區區網 => 樹人家商:	97.8 Mb/秒 (0.1%)	12.5 Mb/秒 (0.0%)	45.3 Mb/秒 (0.0%)

Routing Loop 分析

* 偵測方法:
  * Ping: Both
  * Tracert: Both
  * Netflow: 僅能在各自 Router 上偵測

Routing Loop
WAN <-> Border

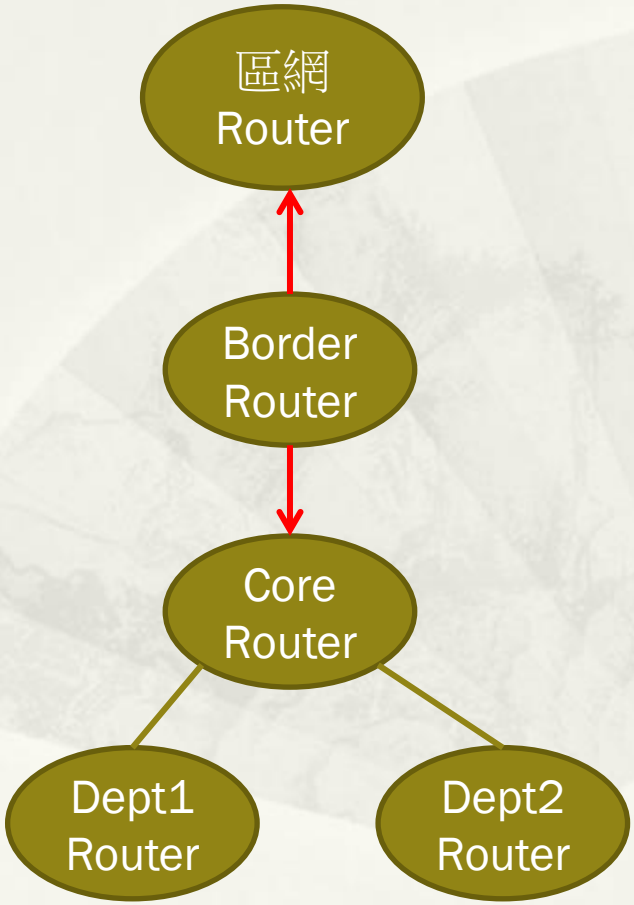



```
C:\Windows\System32>tracert -d 120.96.116.220

在上限 30 個躍點上追蹤 120.96.116.220 的路由

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  140.112.3.126
  3    <1 ms    <1 ms    <1 ms  140.112.0.170
  4     1 ms     2 ms     4 ms  140.112.0.206
  5     2 ms     3 ms     3 ms  140.112.0.70
  6     2 ms     2 ms     2 ms  192.192.7.102
  7     2 ms     2 ms     2 ms  192.192.7.101
  8     4 ms     4 ms     2 ms  192.192.7.102
  9     3 ms     2 ms     2 ms  192.192.7.101
 10     3 ms     3 ms     3 ms  192.192.7.102
 11     5 ms     6 ms     5 ms  192.192.7.101
 12     4 ms     4 ms     4 ms  192.192.7.102
 13     6 ms     4 ms     4 ms  192.192.7.101
 14     4 ms     4 ms     4 ms  192.192.7.102
 15     5 ms     4 ms     7 ms  192.192.7.101
 16     5 ms     5 ms     5 ms  192.192.7.102
 17     6 ms     7 ms     5 ms  192.192.7.101
 18     6 ms     6 ms     6 ms  192.192.7.102
 19     6 ms     6 ms     6 ms  192.192.7.101
 20     7 ms     6 ms     6 ms  192.192.7.102
 21     7 ms     6 ms     6 ms  192.192.7.101
 22     7 ms     7 ms     6 ms  192.192.7.102
 23    10 ms     8 ms     8 ms  192.192.7.101
 24     7 ms     9 ms     8 ms  192.192.7.102
 25    10 ms     8 ms     8 ms  192.192.7.101
 26     9 ms     9 ms     8 ms  192.192.7.102
 27    16 ms    11 ms     9 ms  192.192.7.101
 28     8 ms    13 ms     9 ms  192.192.7.102
 29     9 ms    10 ms    10 ms  192.192.7.101
 30    10 ms    10 ms    10 ms  192.192.7.102

追蹤完成。
```

0.70 區網
7.102 Border
7.101 區網

19

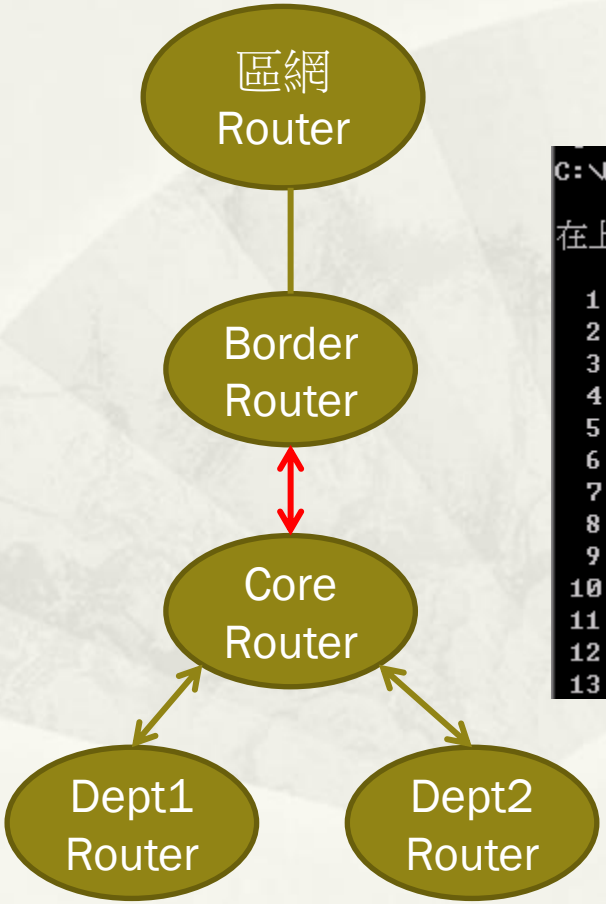
Routing Loop
WAN ← Border →Core




```
C:\Windows\System32>tracert -d 120.97.89.182

在上限 30 個躍點上追蹤 120.97.89.182 的路由

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2    <1 ms    <1 ms    <1 ms  140.112.3.126
  3     6 ms    <1 ms    <1 ms  140.112.0.210
  4     1 ms     2 ms     1 ms  140.112.0.206
  5     1 ms     1 ms     1 ms  140.112.0.70
  6     2 ms     2 ms     2 ms  192.192.7.34
  7     2 ms     2 ms     1 ms  120.97.80.249
  8     2 ms     2 ms     2 ms  172.16.101.65
  9     4 ms     6 ms     2 ms  192.192.7.33
 10    25 ms    41 ms    24 ms  192.192.7.34
 11     3 ms     3 ms     3 ms  120.97.80.249
 12   530 ms   667 ms   682 ms  172.16.101.65
 13     4 ms     4 ms     6 ms  192.192.7.33
 14     4 ms     5 ms     6 ms  192.192.7.34
 15     9 ms     6 ms     5 ms  120.97.80.249
 16     4 ms     4 ms     4 ms  172.16.101.65
 17     6 ms     5 ms     5 ms  192.192.7.33
 18     6 ms     6 ms     5 ms  192.192.7.34
 19     7 ms     5 ms     7 ms  120.97.80.249
 20     6 ms     5 ms     5 ms  172.16.101.65
 21     6 ms     9 ms     7 ms  192.192.7.33
 22     7 ms     8 ms     6 ms  192.192.7.34
 23     7 ms     6 ms     7 ms  120.97.80.249
 24     7 ms     6 ms     7 ms  172.16.101.65
 25     8 ms     9 ms     8 ms  192.192.7.33
 26    49 ms    49 ms    67 ms  192.192.7.34
 27     7 ms     8 ms     8 ms  120.97.80.249
 28     8 ms     8 ms    13 ms  172.16.101.65
 29    13 ms    11 ms     8 ms  192.192.7.33
 30     9 ms    11 ms     9 ms  192.192.7.34

追蹤完成。
```

0.70 區網
7.34 Border
80.249 Core
101.65 Dept
7.33 區網

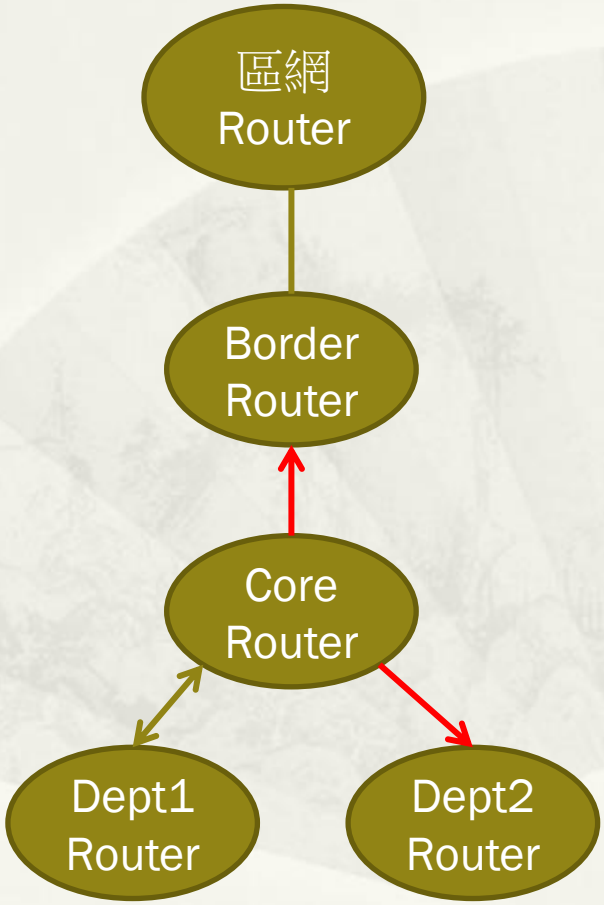
Routing Loop
Border <-> Core



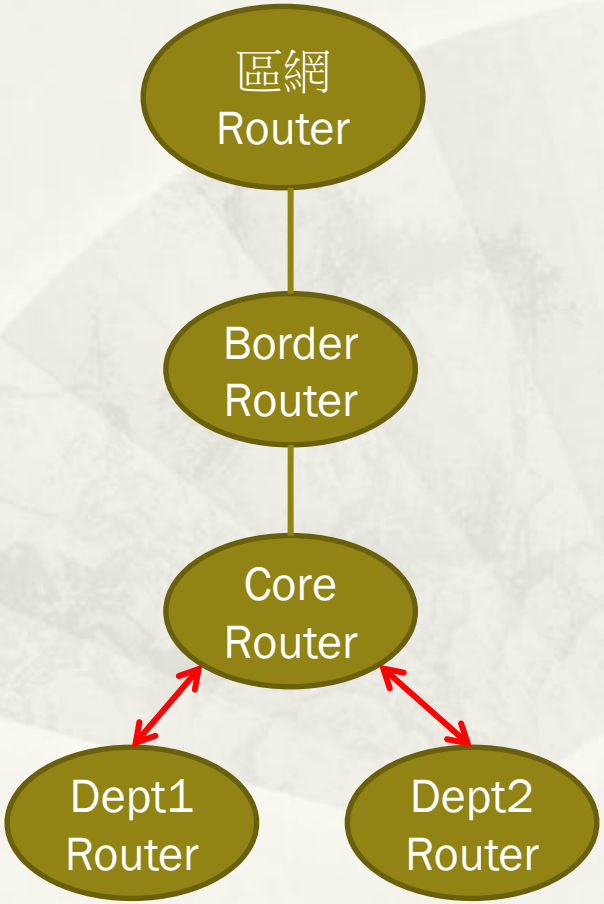

```
C:\Users\Administrator>tracert -d 120.96.4.92

在上限 30 個躍點上追蹤 120.96.4.92 的路由

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2     1 ms    <1 ms    <1 ms  163.28.17.254
  3     1 ms    <1 ms    <1 ms  140.112.0.69
  4     1 ms    <1 ms    <1 ms  140.112.0.201
  5     1 ms     1 ms     1 ms  140.112.0.206
  6     1 ms    <1 ms     1 ms  140.112.0.201
  7     1 ms     1 ms     1 ms  140.112.0.206
  8     1 ms     1 ms     1 ms  140.112.0.201
  9     2 ms     1 ms     2 ms  140.112.0.206
 10     2 ms     1 ms     2 ms  140.112.0.201
 11     2 ms     1 ms     2 ms  140.112.0.206
 12     2 ms     2 ms     2 ms  140.112.0.201
 13     2 ms     2 ms     2 ms  140.112.0.206
```

17.254 區網
0.69 Border
0.201 Core
0.206 Border

Routing Loop
Border ← Core → Dept



Routing Loop
Core <->Dept

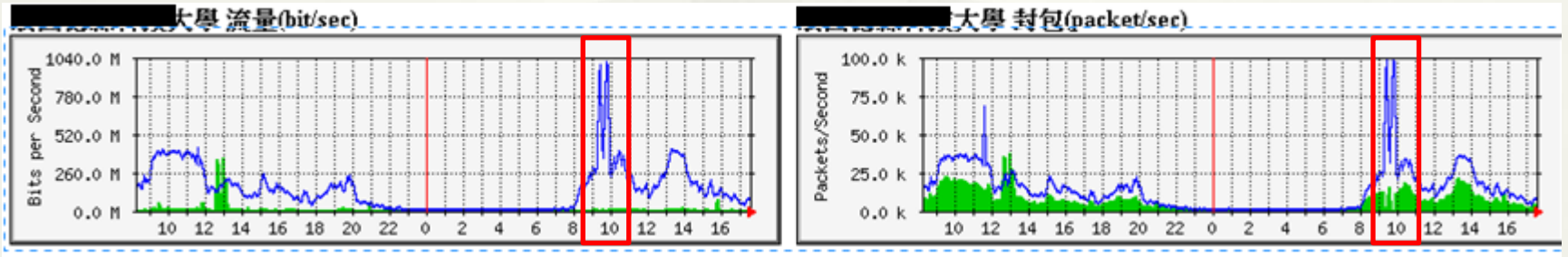


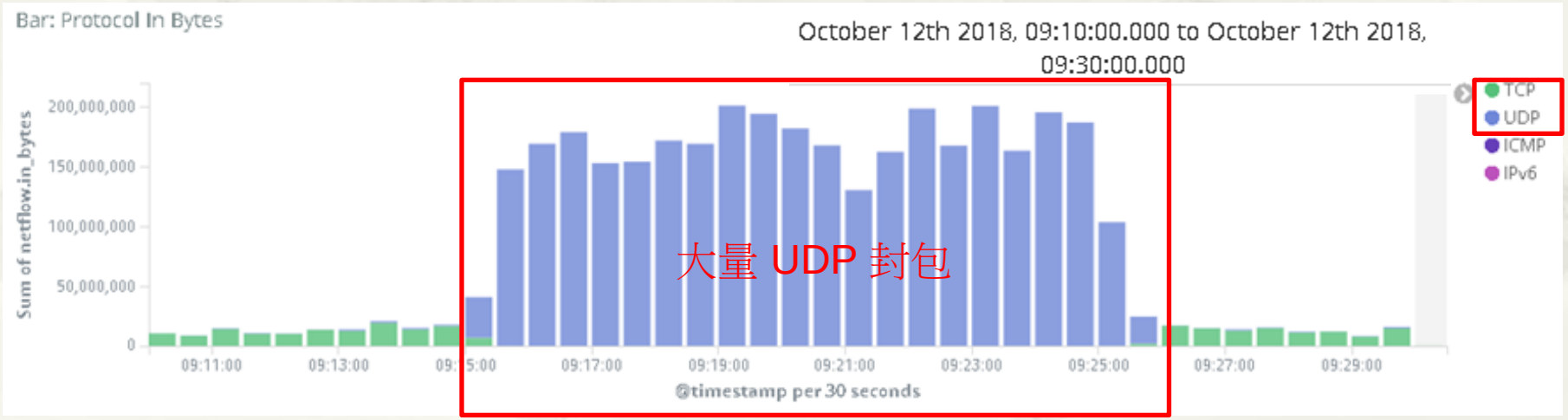
DDoS 案例分析

DDoS 案例分析

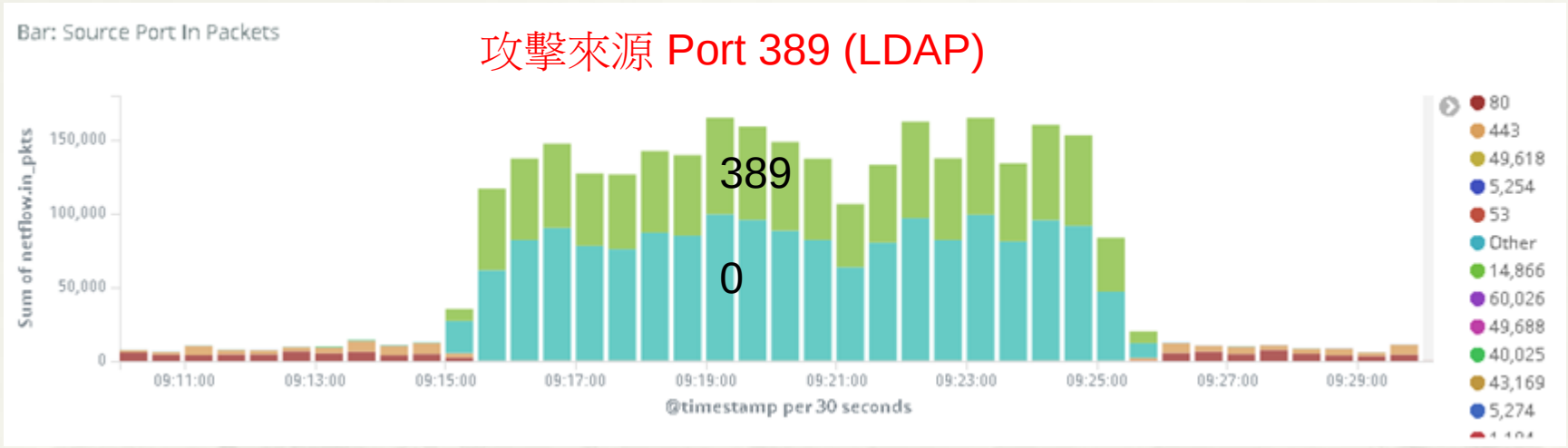
- DDoS 攻擊方法
  - 新型 LDAP 攻擊取代傳統 DNS、NTP 放大攻擊
- DDoS 攻擊來源
  - 過去使用 Internet Server(NTP, Open Resolver) 轉而利用現成雲端資源

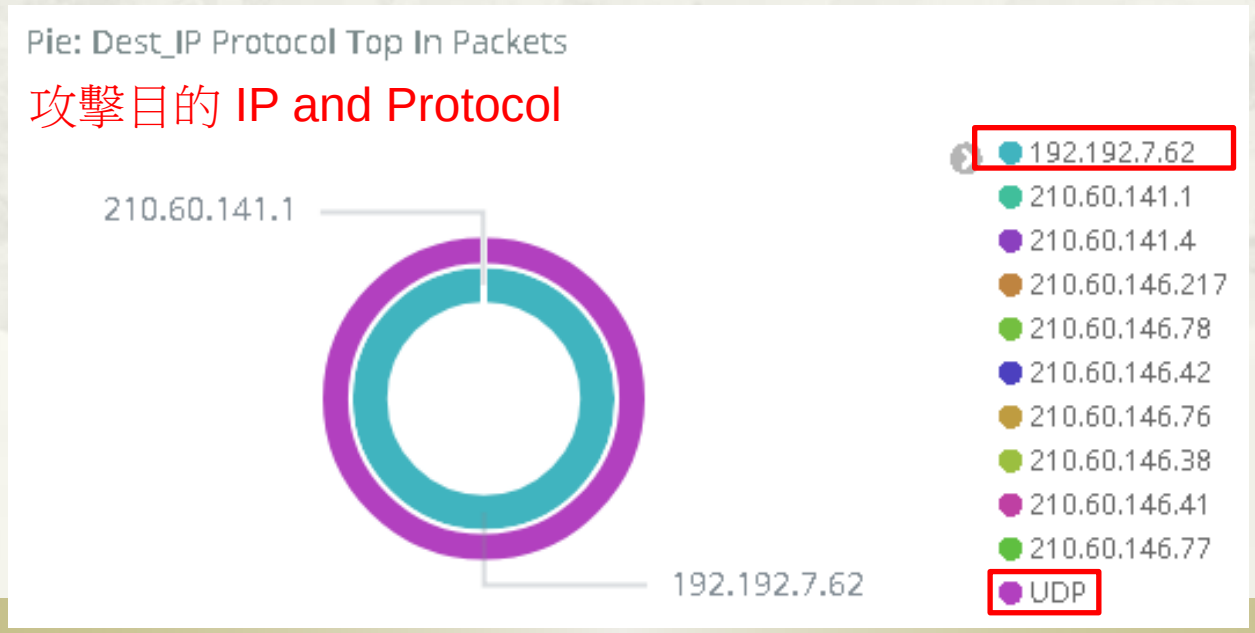
連線學校 **DDoS**
攻擊前後流量分析





攻擊來源與目的

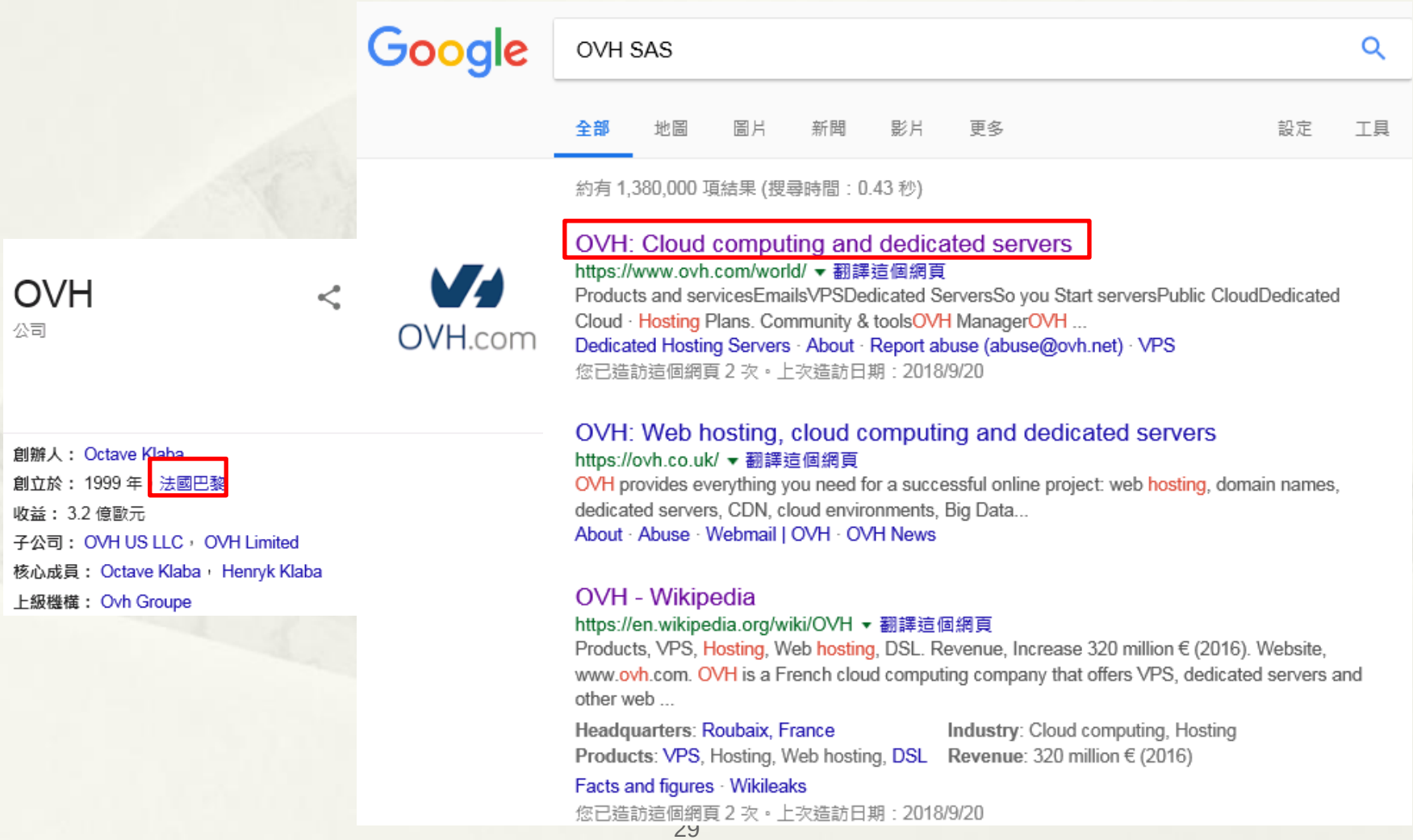

Bar: Source Port In Packets
攻擊來源 Port 389 (LDAP)
Sum of netflow.in_pkts
150,000
100,000
50,000
0
389
0
09:11:00
09:13:00
09:15:00
09:17:00
09:19:00
09:21:00
09:23:00
09:25:00
09:27:00
09:29:00
@timestamp per 30 seconds
80
443
49,618
5,254
53
Other
14,866
60,026
49,688
40,025
43,169
5,274


Pie: Dest_IP Protocol Top In Packets
攻擊目的 IP and Protocol
210.60.141.1
192.192.7.62
192.192.7.62
210.60.141.1
210.60.141.4
210.60.146.217
210.60.146.78
210.60.146.42
210.60.146.76
210.60.146.38
210.60.146.41
210.60.146.77
UDP

攻擊來源 Top ASN

* 攻擊來源: 各大雲端平台

攻擊來源 Top ASN
OVH SAS



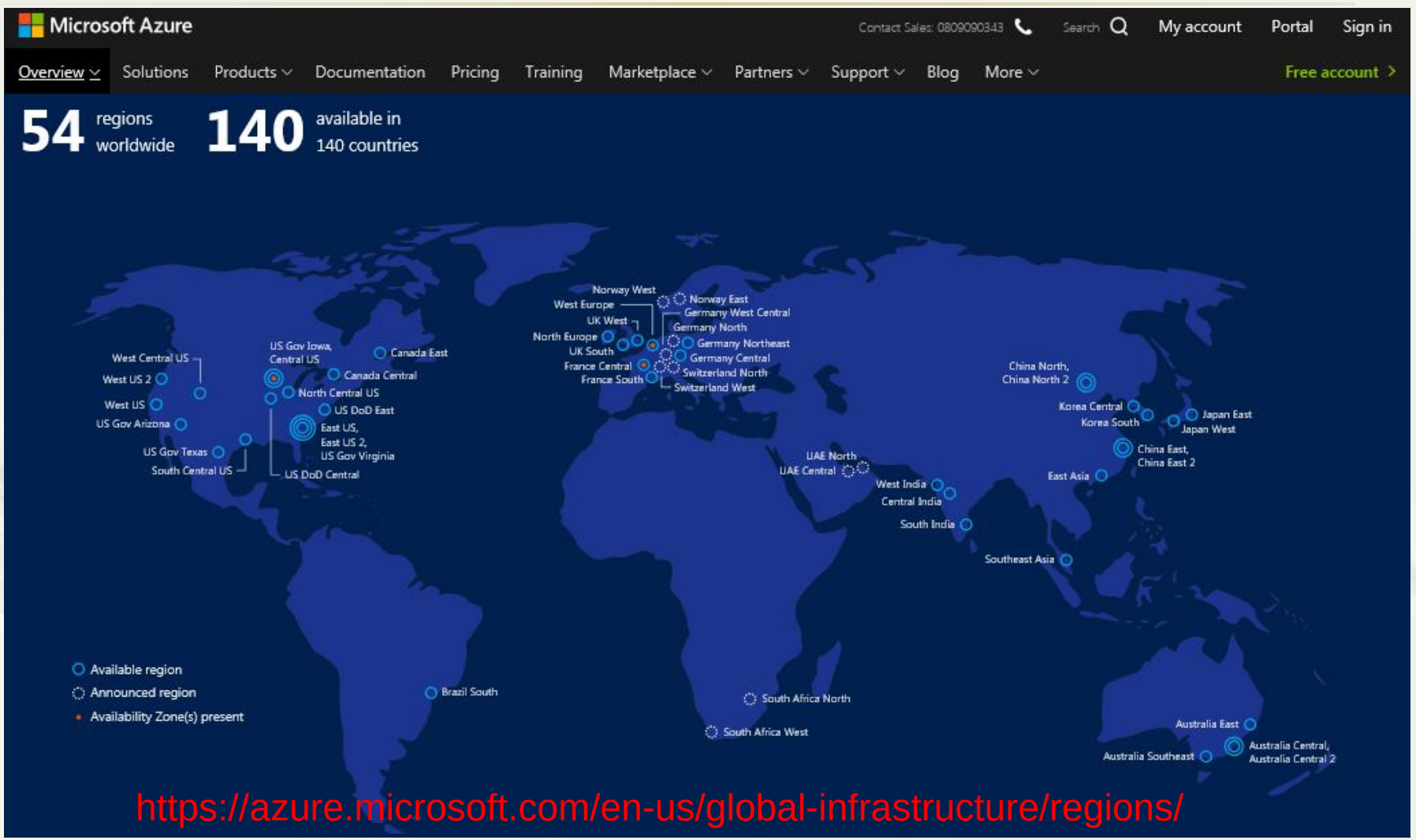
攻擊來源 Top ASN
OVH SAS

host.keyword: "192.192.60.112" | netflow.output_snmp: "159" | netflow.protocol.keyword: "UDP" | geoip_src.as_org.keyword: "OVH SAS"

攻擊來源 Top ASN
Microsoft Corporation

host.keyword: "192.192.60.112" | netflow.output_snmp: "159" | netflow.protocol.keyword: "UDP" | geoip_src.as_org.keyword: "Microsoft Corporation"

Microsoft Azure regions

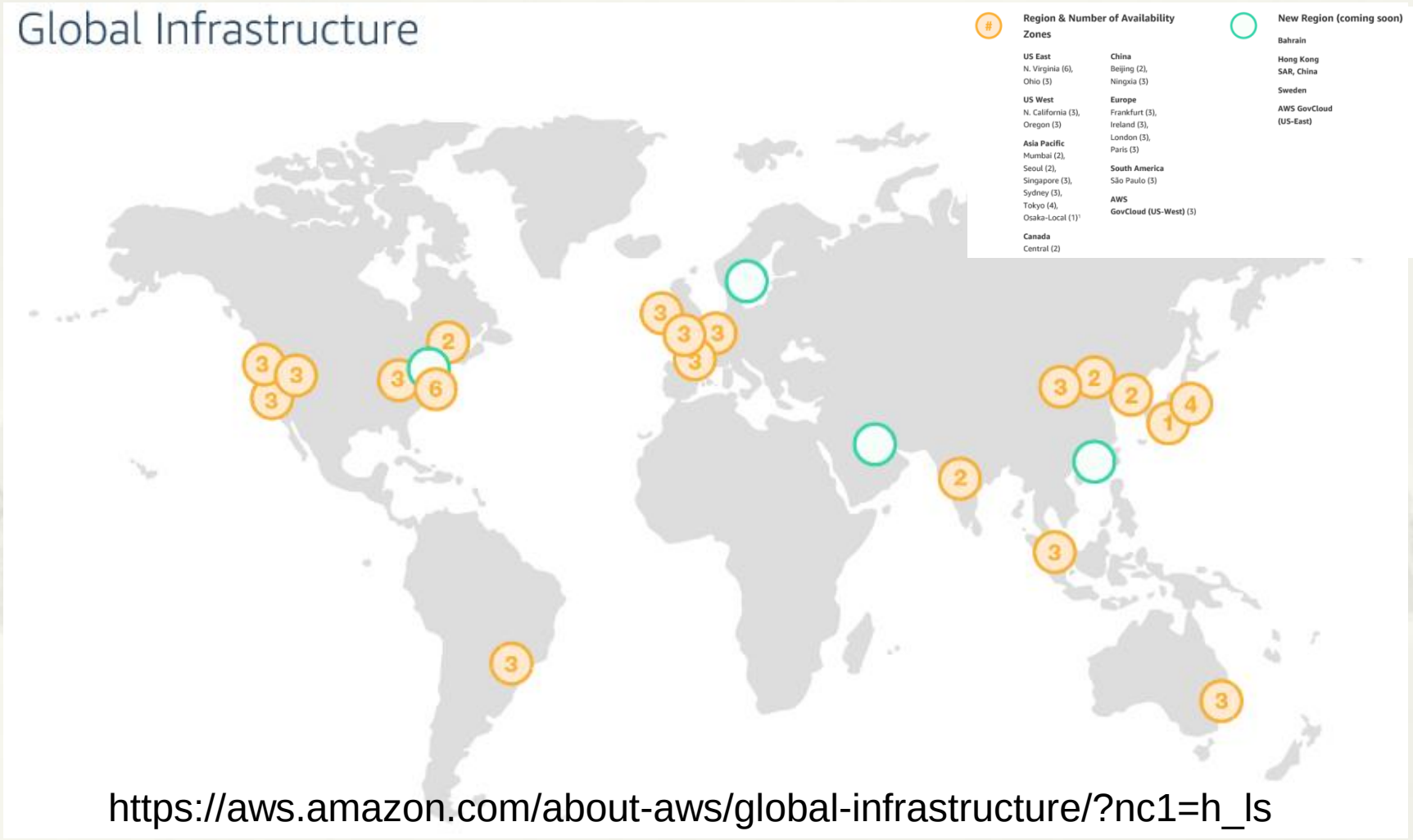


https://azure.microsoft.com/en-us/global-infrastructure/regions/

攻擊來源 Top ASN
Amazon.com, Inc.

host.keyword: "192.192.60.112" | netflow.output_snmp: "159" | netflow.protocol.keyword: "UDP" | geoip_src.as_org.keyword: "Amazon.com, Inc."

AWS Global Infrastructure



https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls

DDoS 案例分析

- LDAP 是微軟 Active Directory 認證使用之通訊協議，因雲端租用使用者可能有遠端認證需求，又未限制來源IP，而被駭客利用作為放大攻擊。
- DDoS 攻擊來源已從過去使用 Internet Server(NTP, Open Resolver) 轉而利用現成雲端資源。
- 雲端資源主機多且對外流量大。
- 雲端租用計費方式: 上傳流量不計費、僅計算下載流量
  - 雲端公司也許不會主動告知流量異常(Money $$$$$...)
  - 租用雲端使用者誤以為網站變熱門，下載流量變高


雲端業務扮演火車頭，Azure強勢成長89%

雲端業務是這幾年推升微軟營收的強力引擎，原因是越來越多企業將工作資料轉移到雲端，以此降低資料儲存、軟體成本。根據市場研究公司Canalys的預估，公用雲端服務平台Azure在全市場占比達16%，是僅次於亞馬遜AWS的全球第二大雲端服務供應商。

To Do List

- 偵測
  - 現況由人為判斷攻擊發生，未來應可由程式依據設定 Threshold 或 異常Protocol 分佈比例 (UDP vs. TCP) 來自動偵測
  - 上述所提 Threshold 或 異常分佈比例之設定值，可由歷史記錄自動學習
- 清洗
  - Open Source 清洗軟體