# TANet 100G 研討會
# TCP-based 網路品質監控


·報告人：游子興

·davisyou@ntu.edu.tw

·02-33665008

# 大綱

- TCP-based 網路品質監控原理與方法
- Client Latency
  - 上網方式辨識
  - 頻寬壅塞對 Latency 之影響
  - 異常辨識
  - 網路設備 Inline/Bypass、 Device Loading
- Server Latency
  - 網路設備 Inline/Bypass
  - 頻寬壅塞對 Latency 之影響
  - 壅塞節點偵測
  - Client/Server 實體距離
  - 對外線路連線地區分析
  - GeoIP DB 準確率分析

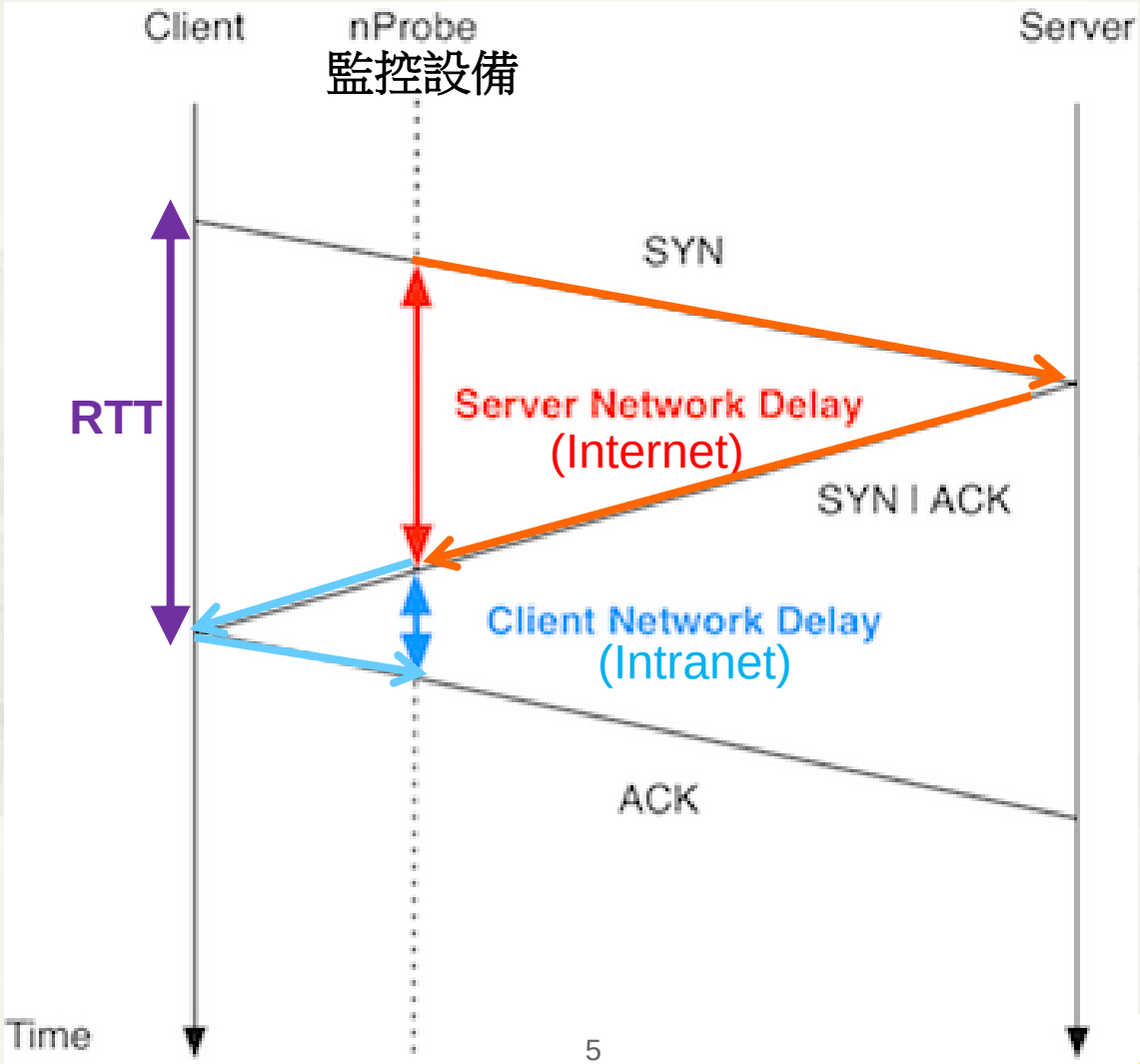
# 傳統網路品質監控

- 監控方法: ICMP Ping、TraceRoute
  - Round Trip Time(RTT)
  - Packet Lost
- 缺點與限制:
  - 需對方設備回應 ICMP Ping
  - 主動式偵測佔用頻寬資源
  - 無法大量佈建與監控:
    - 國網於所有區網中心與部分雲端佈建監控設備
  - 需專用設備與軟體才能進行 24Hr 監控與統計
  - 無法釐清問題來源為 Intranet/Internet/Application

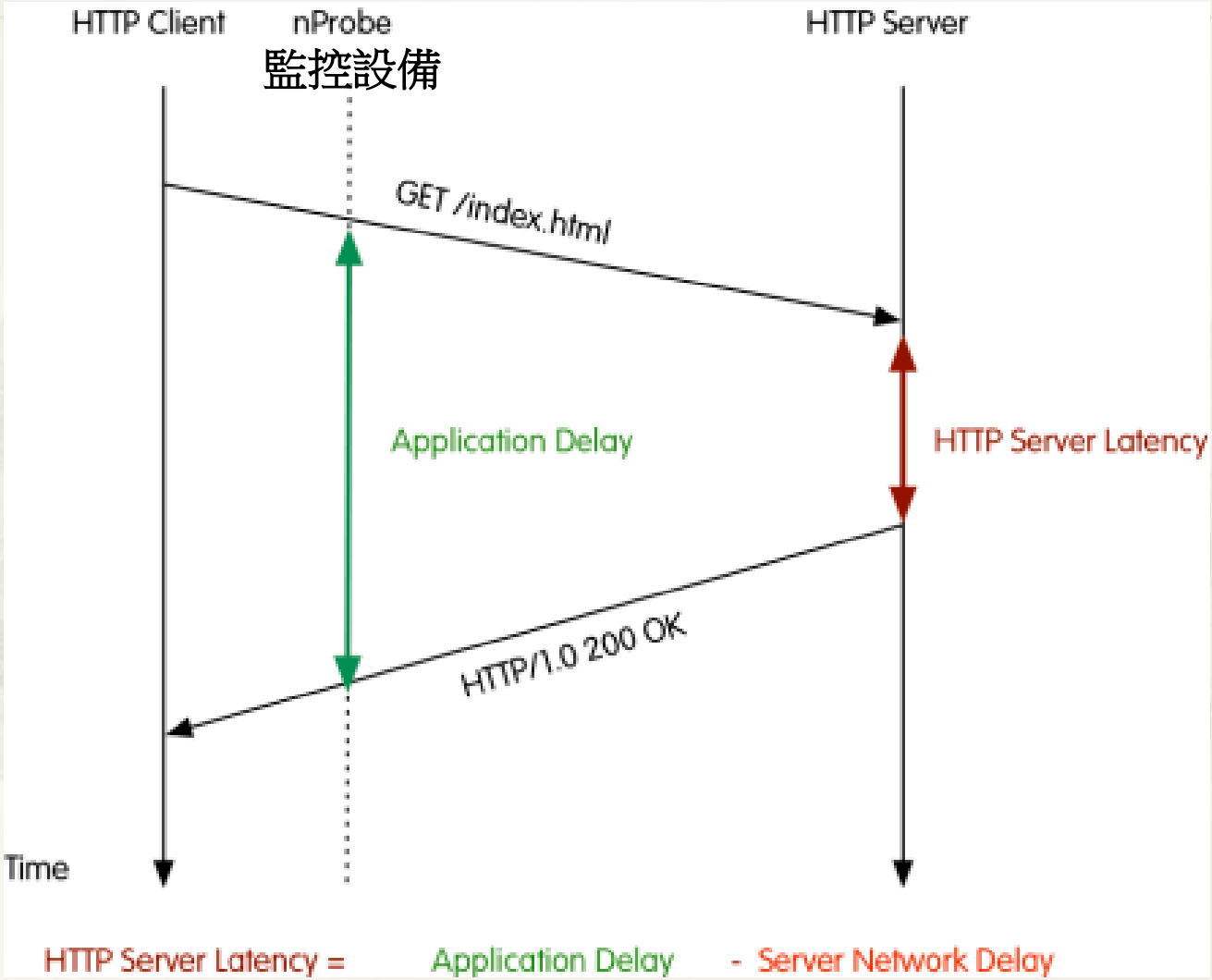
# TCP-based 網路品質監控

- 利用使用者上網行為進行量測，提供大量數據
- 數據收集方法: TCP
  - RTT:  TCP 3-way handshake
  - Packet Lost: TCP Retransmit & OutOfOrder

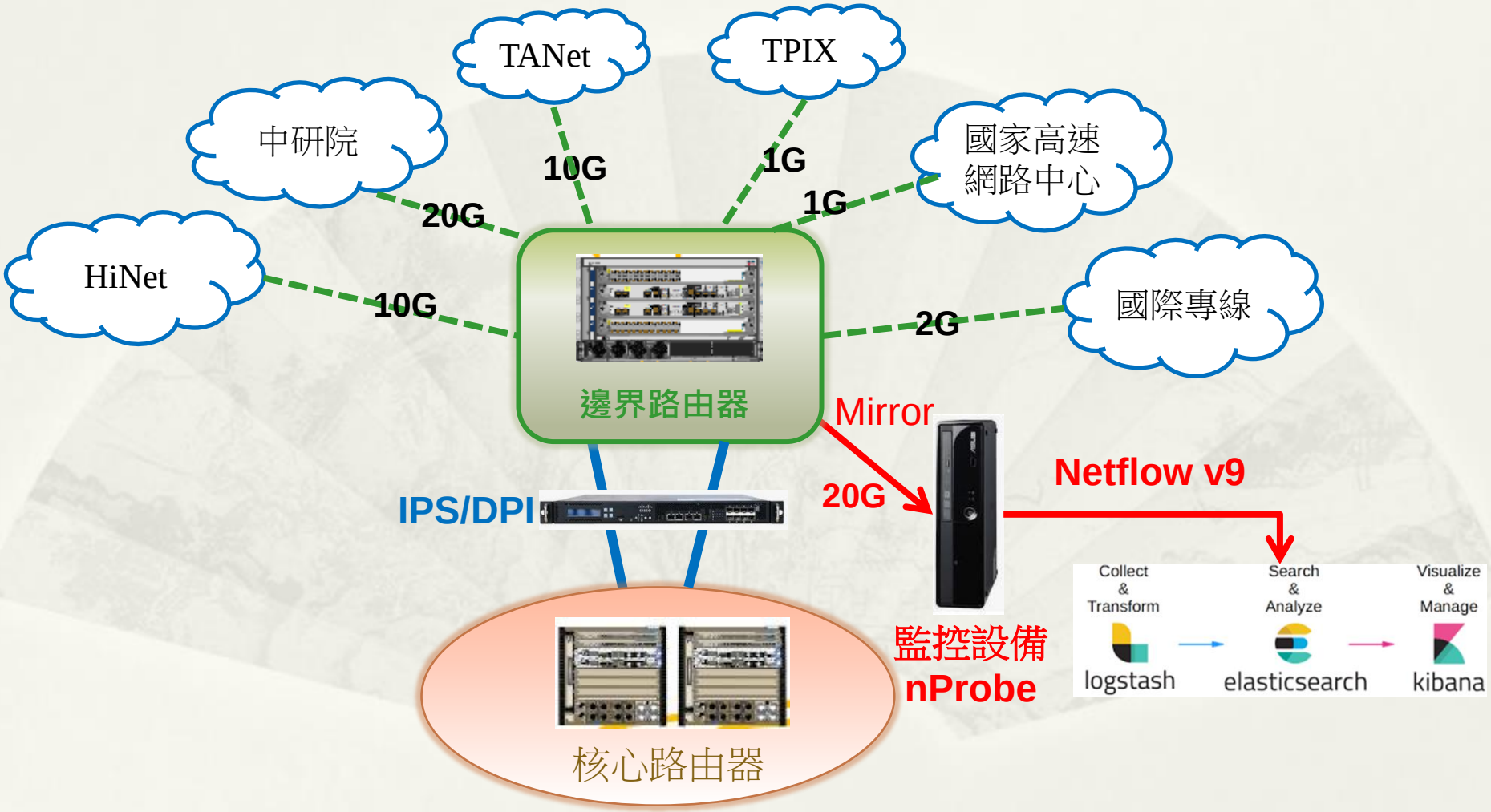
# Network Latency



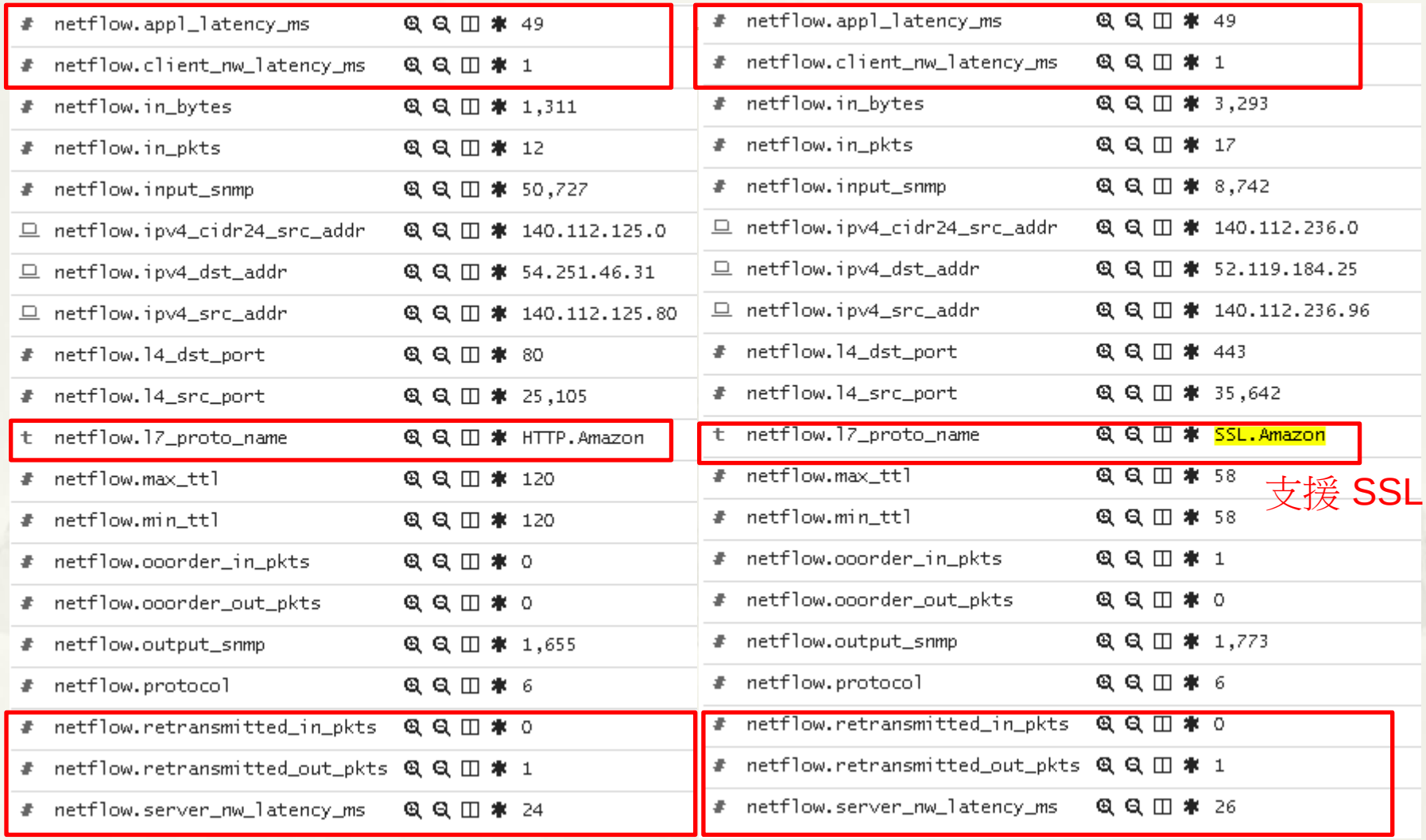
# Application Latency



# TCP-based 網路品質監控
# 臺大網路架構圖



# 範例: 校內連線 Amazon



| | | |
|---|---|---|
| # | netflow.appl_latency_ms | 49 |
| # | netflow.client_nw_latency_ms | 1 |
| # | netflow.in_bytes | 1,311 |
| # | netflow.in_pkts | 12 |
| # | netflow.input_snmp | 50,727 |
| 💻 | netflow.ipv4_cidr24_src_addr | 140.112.125.0 |
| 💻 | netflow.ipv4_dst_addr | 54.251.46.31 |
| 💻 | netflow.ipv4_src_addr | 140.112.125.80 |
| # | netflow.l4_dst_port | 80 |
| # | netflow.l4_src_port | 25,105 |
| t | netflow.l7_proto_name | HTTP.Amazon |
| # | netflow.max_ttl | 120 |
| # | netflow.min_ttl | 120 |
| # | netflow.ooorder_in_pkts | 0 |
| # | netflow.ooorder_out_pkts | 0 |
| # | netflow.output_snmp | 1,655 |
| # | netflow.protocol | 6 |
| # | netflow.retransmitted_in_pkts | 0 |
| # | netflow.retransmitted_out_pkts | 1 |
| # | netflow.server_nw_latency_ms | 24 |

| | | |
|---|---|---|
| # | netflow.appl_latency_ms | 49 |
| # | netflow.client_nw_latency_ms | 1 |
| # | netflow.in_bytes | 3,293 |
| # | netflow.in_pkts | 17 |
| # | netflow.input_snmp | 8,742 |
| 💻 | netflow.ipv4_cidr24_src_addr | 140.112.236.0 |
| 💻 | netflow.ipv4_dst_addr | 52.119.184.25 |
| 💻 | netflow.ipv4_src_addr | 140.112.236.96 |
| # | netflow.l4_dst_port | 443 |
| # | netflow.l4_src_port | 35,642 |
| t | netflow.l7_proto_name | SSL.Amazon |
| # | netflow.max_ttl | 58 |
| # | netflow.min_ttl | 58 |
| # | netflow.ooorder_in_pkts | 1 |
| # | netflow.ooorder_out_pkts | 0 |
| # | netflow.output_snmp | 1,773 |
| # | netflow.protocol | 6 |
| # | netflow.retransmitted_in_pkts | 0 |
| # | netflow.retransmitted_out_pkts | 1 |
| # | netflow.server_nw_latency_ms | 26 |

支援 SSL

# 監控設備

- 新一代 Router
  - Cisco Application Visibility and Control Solution (Cisco AVC)
    - Cisco ASR 1000 (ASR9000 不支援)
  - Use Netflow V9/V10 自訂格式
    - flow record name
      - collect connection delay network to-server sum
      - collect connection delay network to-client sum
      - collect connection delay application sum
      - collect connection client counter packets retransmitted
- Mirror/SPAN 到外部設備進行分析
  - Cisco Flow Sensor
  - nProbe (教育與研究機構免費)
  - NPM(Network Performance Manger) 設備
  - 頻寬管理器/DPI 設備: Procera

# 影響 Latency 原因

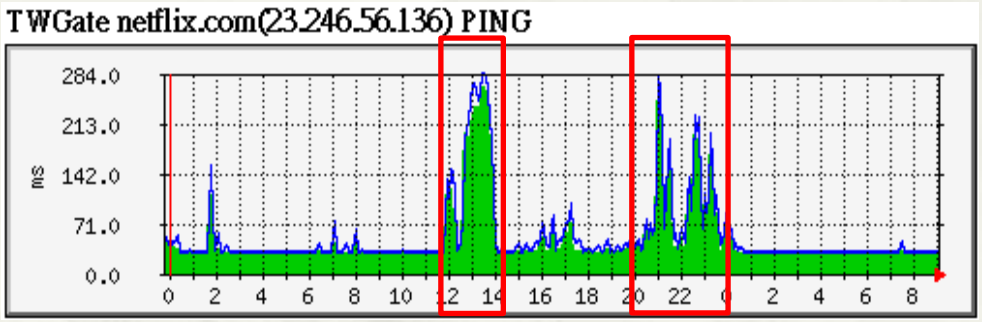
- Client 上網方式
  - 有線、WIFI、VPN、ADSL、4G (Client Latency)
- 實際距離
  - WIFI AP vs. 上網裝置 (Client Latency)
  - Client between Server (Server Latency)
- Network Congest 頻寬壅塞
  - WIFI Congest (Client Latency)
  - 骨幹 Congest (Client /Server Latency)
- 網路設備
  - Inline/Bypass (Client /Server Latency)
  - 設備 Loading (Client /Server Latency)
  - Server Loading (Application Latency)
- Server/網路設備 異常 (Server Latency)
- 封包大小(Server/Application Latency)

# Server Latency

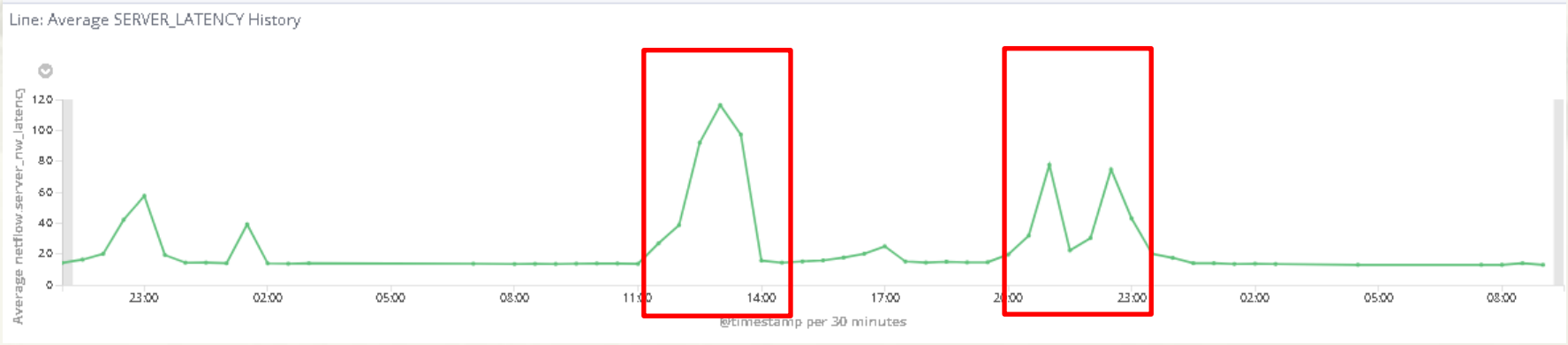
驗證

# netflix.com 23.246.56.136 ping vs. Server latency

* Ping

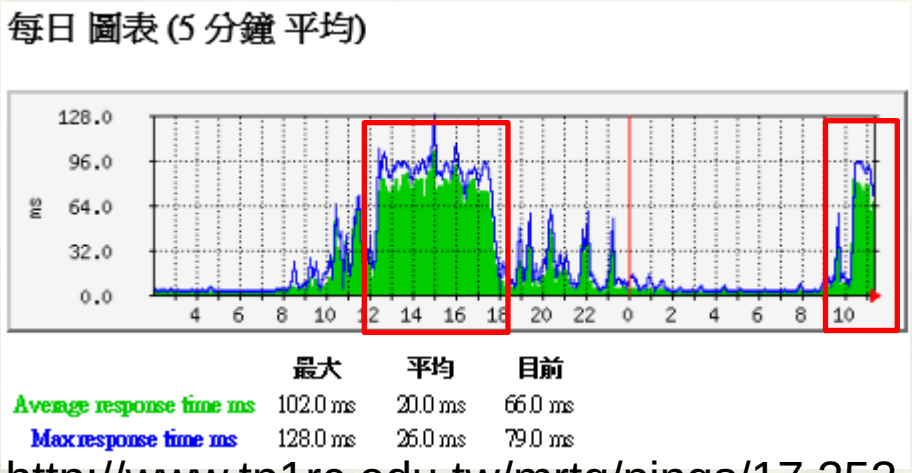



* Server Latency



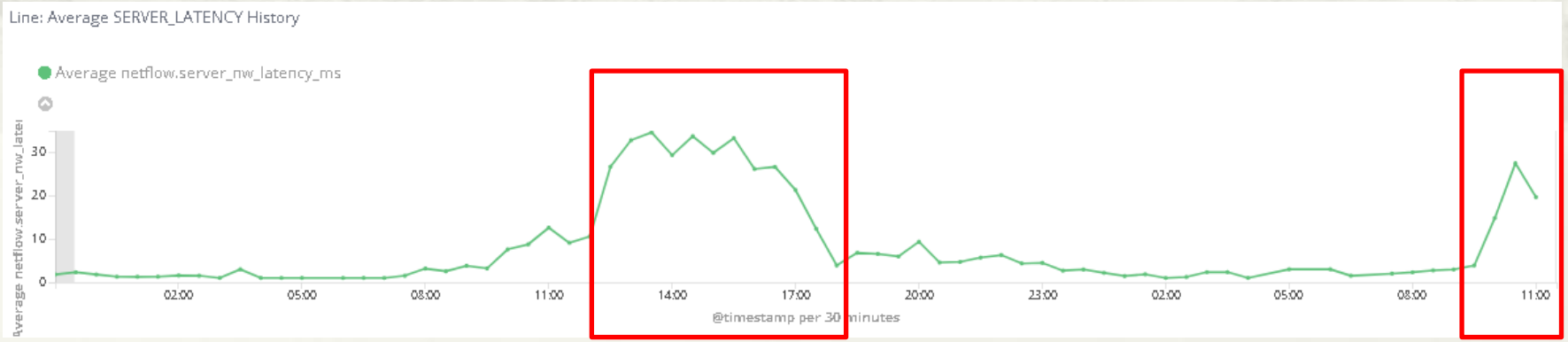
# Apple Inc. 17.253.117.202 ping vs. Server latency

* Ping




http://www.tp1rc.edu.tw/mrtg/pings/17.253.117.202.html

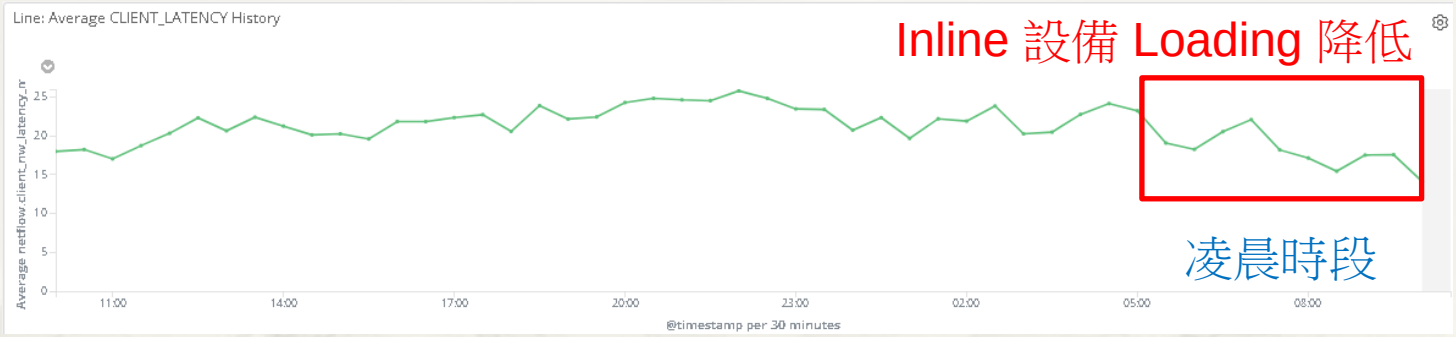
* Server Latency



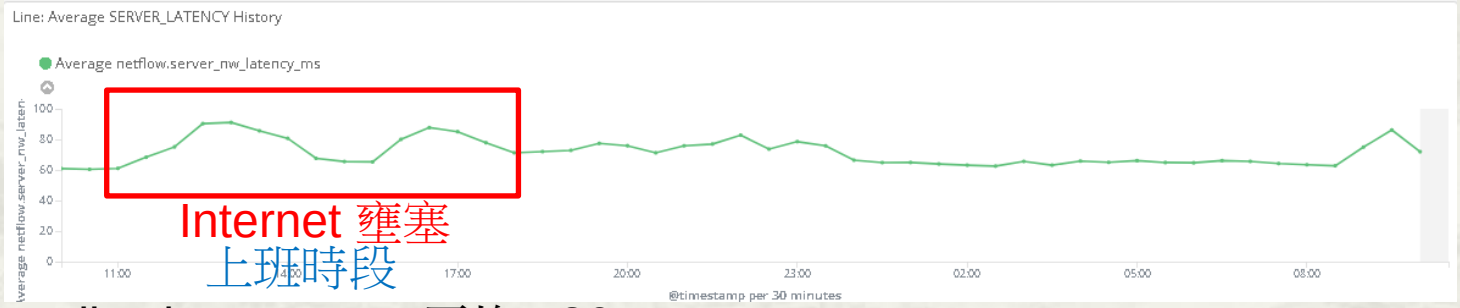
# NTU 校園網路
# Latency Overview

# NTU 校園網路 Latency 24 Hrs 統計

Client Latency 平均:22ms

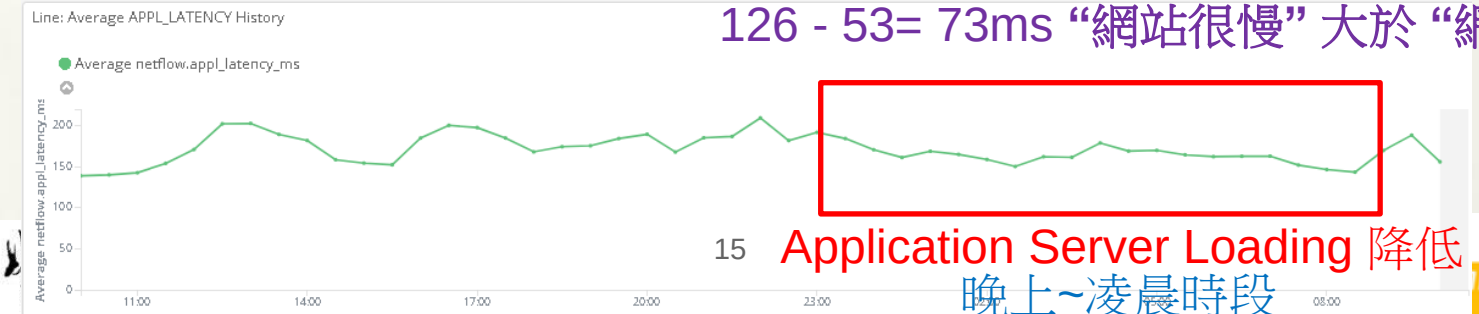



Server Latency 平均:53ms

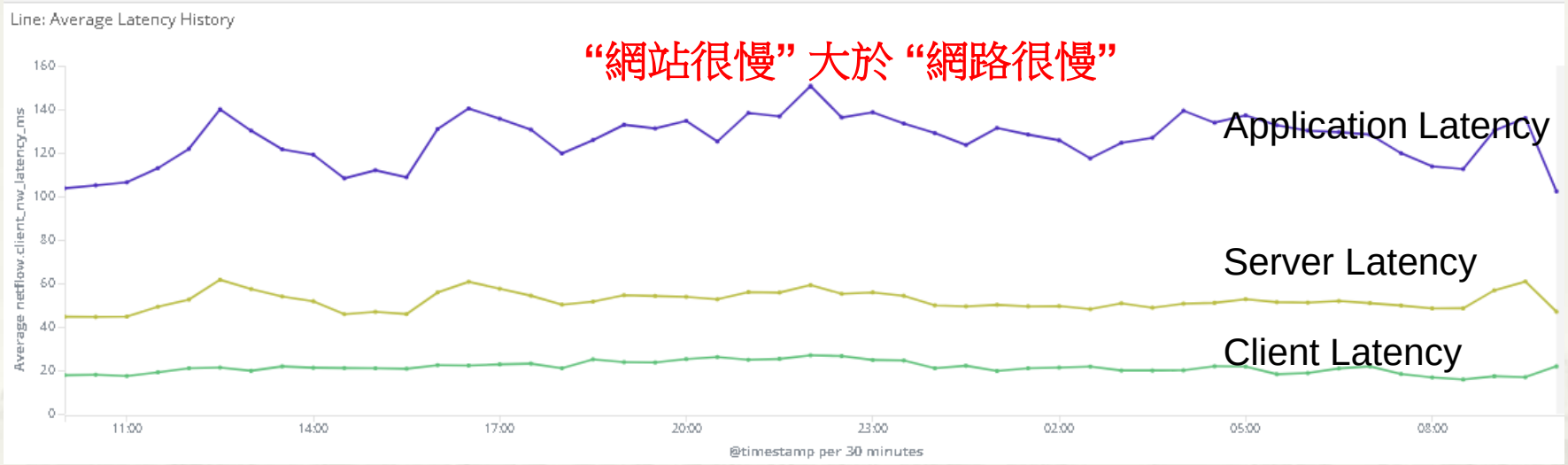



Application Latency 平均:126ms

HTTP Server Delay:
126 - 53= 73ms “網站很慢” 大於 “網路很慢”



# NTU 校園網路 Latency 24 Hrs 統計



# Client Latency

上網方式辨識

Why Avg:22ms so high?

# 上網方式 有線

* 光世代

```
C:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=1ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=1ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=1ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=1ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=1ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=248
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=248

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 1ms，最大值 = 4ms，平均 = 2ms
```

* 光世代 + VPN

```
C:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=15ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=10ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=6ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=5ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=8ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=7ms TTL=246
回覆自 168.95.1.1: 位元組=32 時間=8ms TTL=246

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 3ms，最大值 = 15ms，平均 = 5ms
```

# 上網方式 無線

* Wifi (411會議室)

```
D:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=47ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=13ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=10ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=9ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=10ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=5ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=11ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=16ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=17ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=14ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=8ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 2ms，最大值 = 47ms，平均 = 9ms
```

* 遠傳4G 無線分享

```
D:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=41ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=26ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=92ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=87ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=81ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=38ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=31ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=74ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=53ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=225ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=85ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=104ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=42ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=975ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=24ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=39ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=524ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=535ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=33ms TTL=242
回覆自 168.95.1.1: 位元組=32 時間=552ms TTL=242

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 24ms，最大值 = 975ms，平均 = 183ms
```

# 上網方式 無線

* 411 辦公室

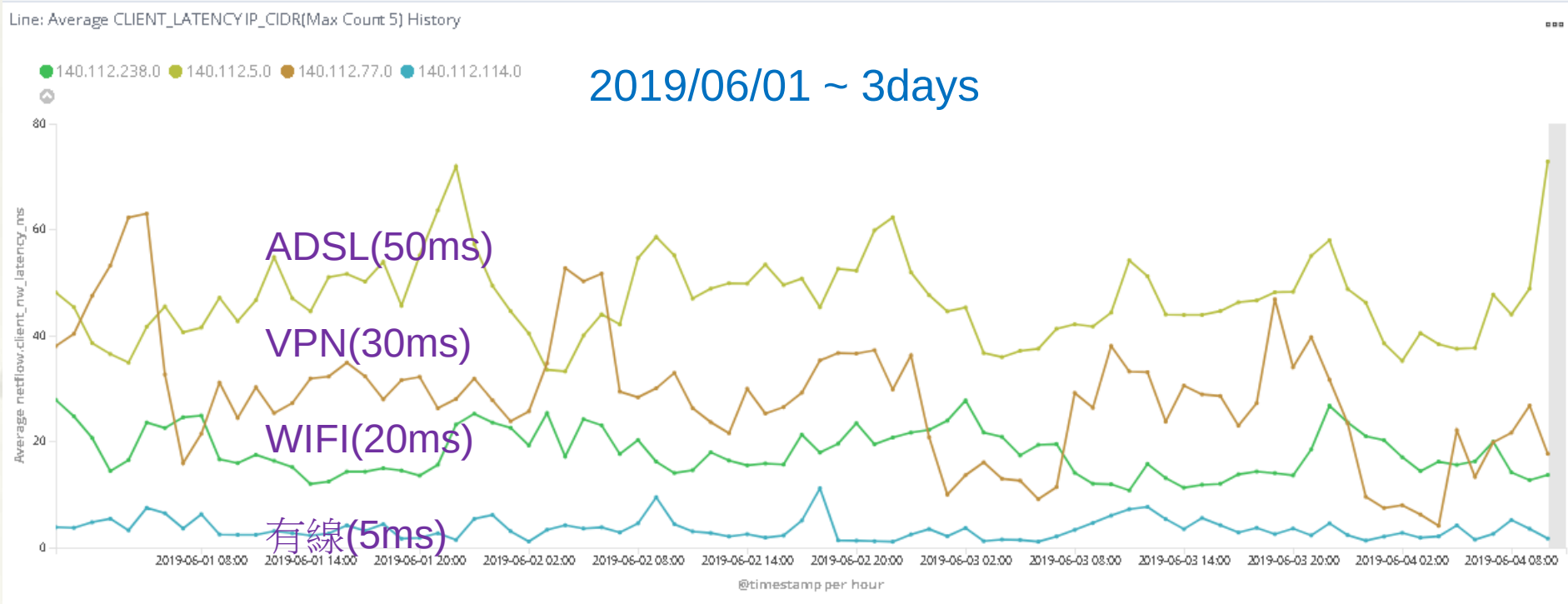
```
D:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=47ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=13ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=10ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=9ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=10ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=5ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=11ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=16ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=17ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=14ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=8ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 2ms，最大值 = 47ms，平均 = 9ms
```

* 212 會議室

```
D:\>ping 168.95.1.1 -n 20

Ping 168.95.1.1 (使用 32 位元組的資料):
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=5ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=5ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=8ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=4ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=3ms TTL=245
回覆自 168.95.1.1: 位元組=32 時間=2ms TTL=245

168.95.1.1 的 Ping 統計資料:
    封包: 已傳送 = 20，已收到 = 20，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 2ms，最大值 = 8ms，平均 = 3ms
```

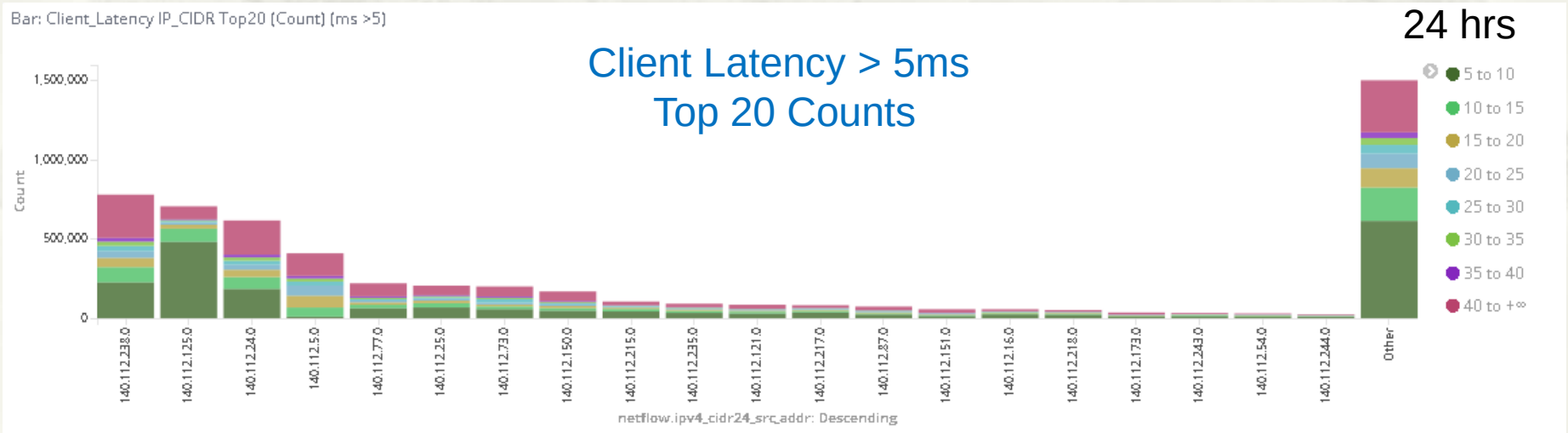
# 辨識不同網段用途
# Client 上網方式

- ADSL: 140.112.5.0/25
- WIFI: 140.112.238.0/24
- VPN: 140.112.77.0/24
- 有線: 140.112.114.0/24



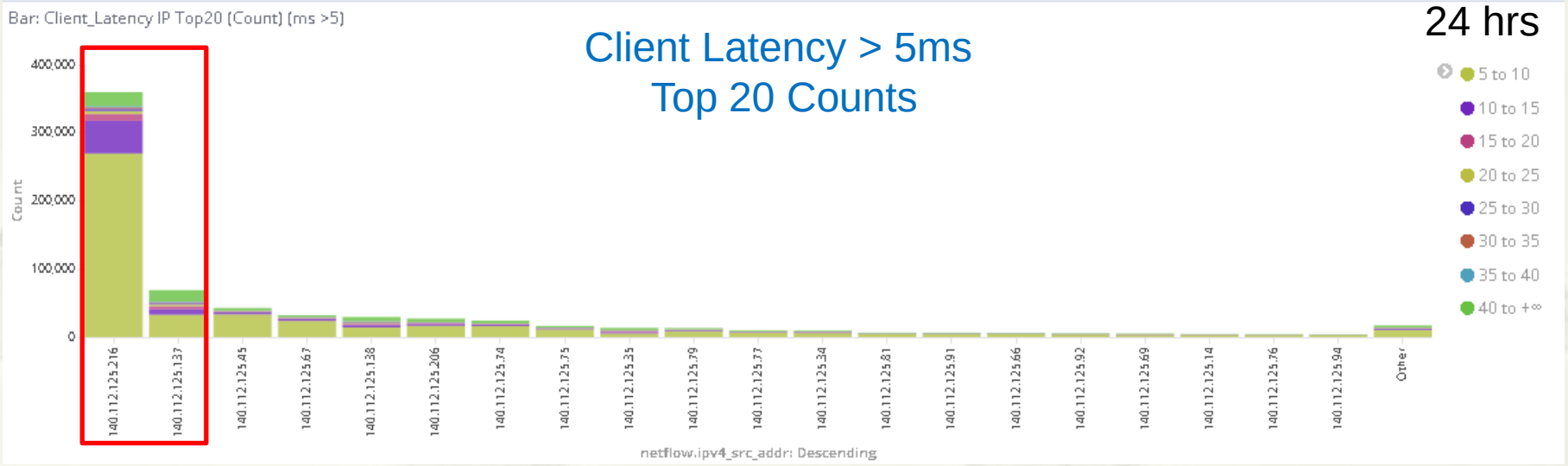
# 辨識不同網段(/24)用途
# Client Latency Top 網段

- 140.112.238.0 Wireless
- 140.112.125.0 醫學院
- 140.112.24.0 Wireless
- 140.112.5.0 ADSL、SIP
- 140.112.77.0 SSLVPN
- 140.112.25.0 Wireless ADSL
- 140.112.73.0 SSLVPN
- 140.112.150.0 SSLVPN
- 140.112.215.0 水源BOT宿舍
- 140.112.235.0 水源BOT宿舍
- 140.112.121.0 醫學院

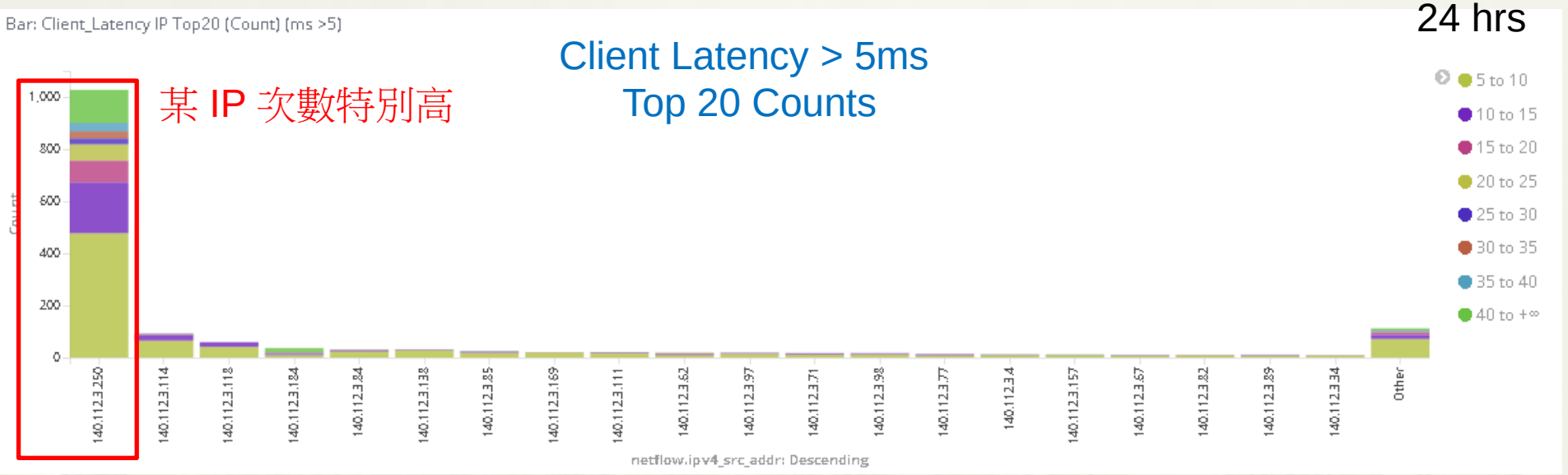


# 辨識網段內連網設備
# 140.112.125.0/24 醫學院

* 140.112.125.216 雲林分院上網 NAT 設備
* 140.112.125.137 臺大醫院東址無線 AP



# 辨識網段內連網設備
# 140.112.3.0/24 計中工作區




* 140.112.3.250 Aruba AP

```
Server6509#sh ip arp 140.112.3.250
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  140.112.3.250           0   000b.8662.e3b0  ARPA   Vlan302
```

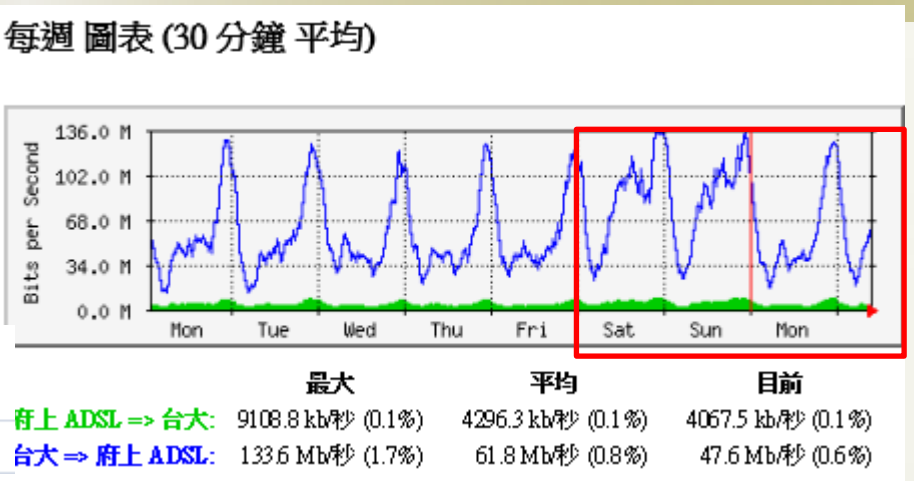
| | |
|---|---|
| **Company** | Aruba, a Hewlett Packard Enterprise Company |
| **OUI** | 00-0B-86 |

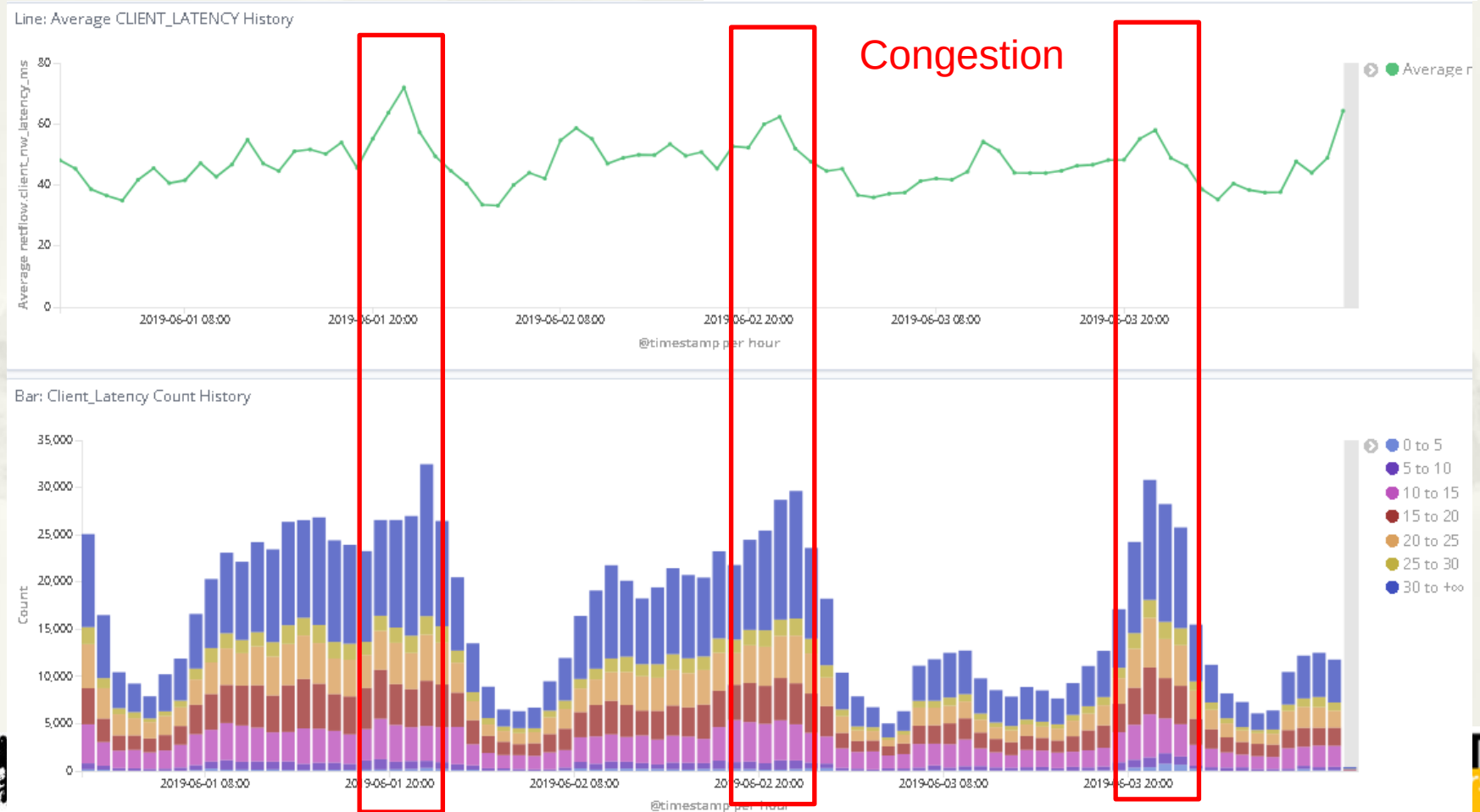
# Client Latency

## 頻寬壅塞對 Latency 之影響

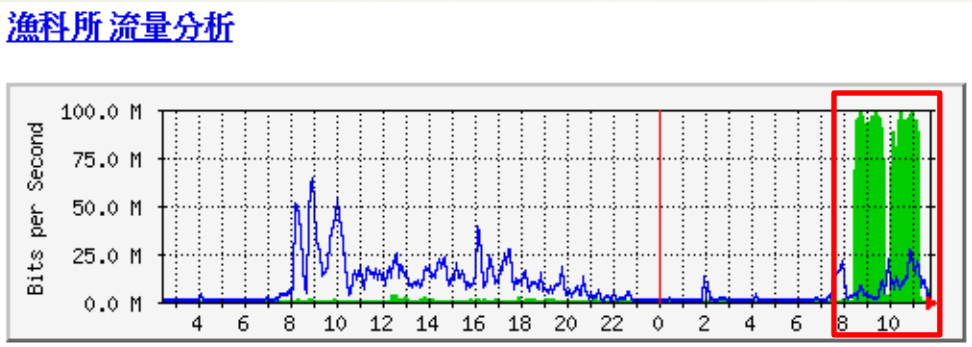
# ADSL Congestion

| 50th percentile of netflow.client_nw_latency_ms | Average netflow.client_nw_latency_ms |
|---|---|
| 23 | 49.211 |

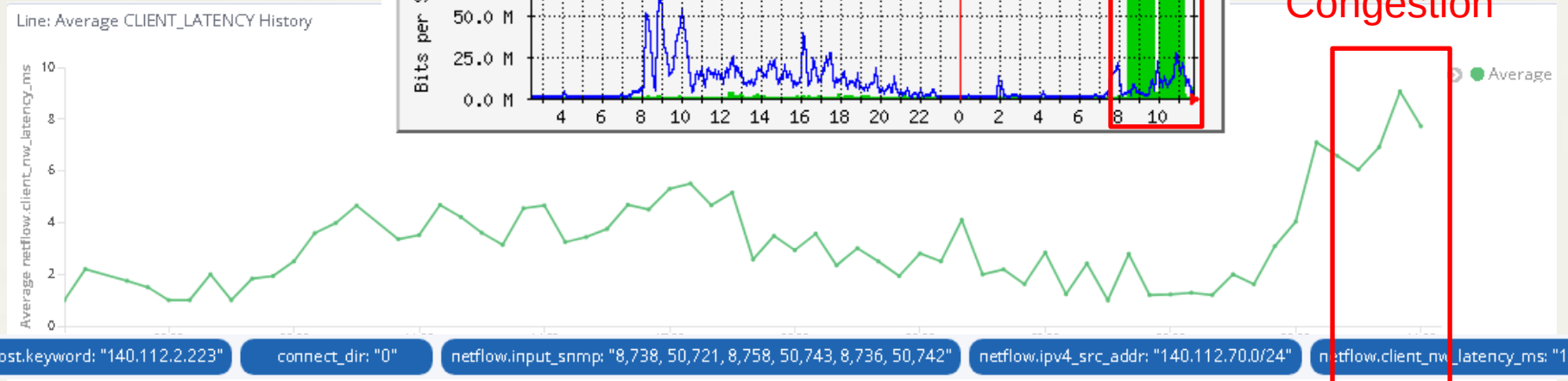


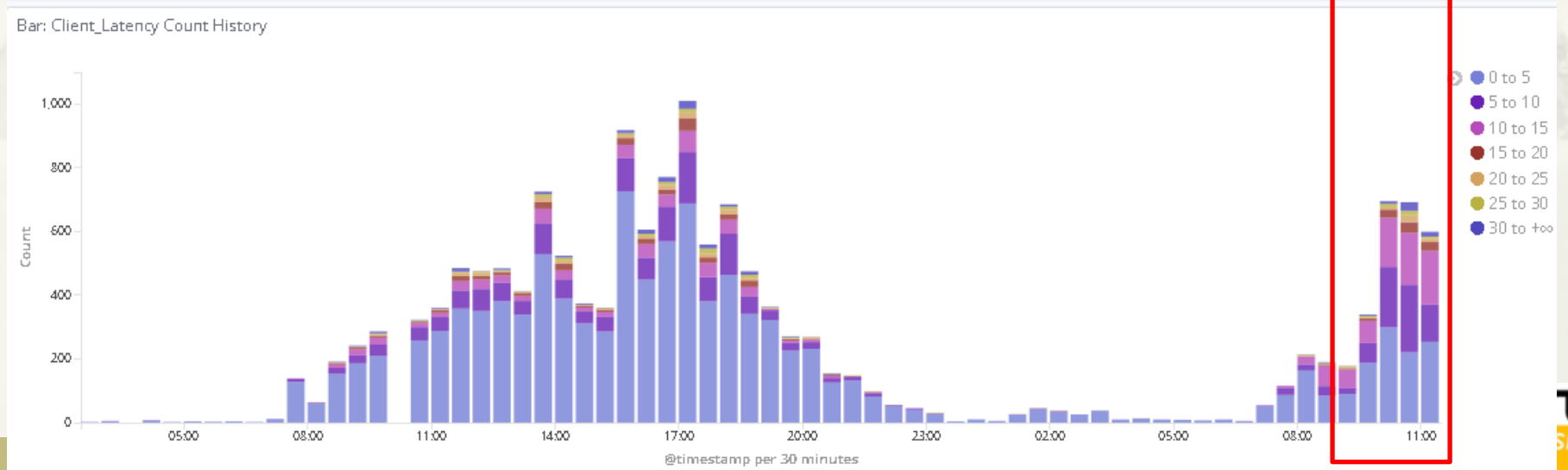



# 有線網路 Congestion




Congestion

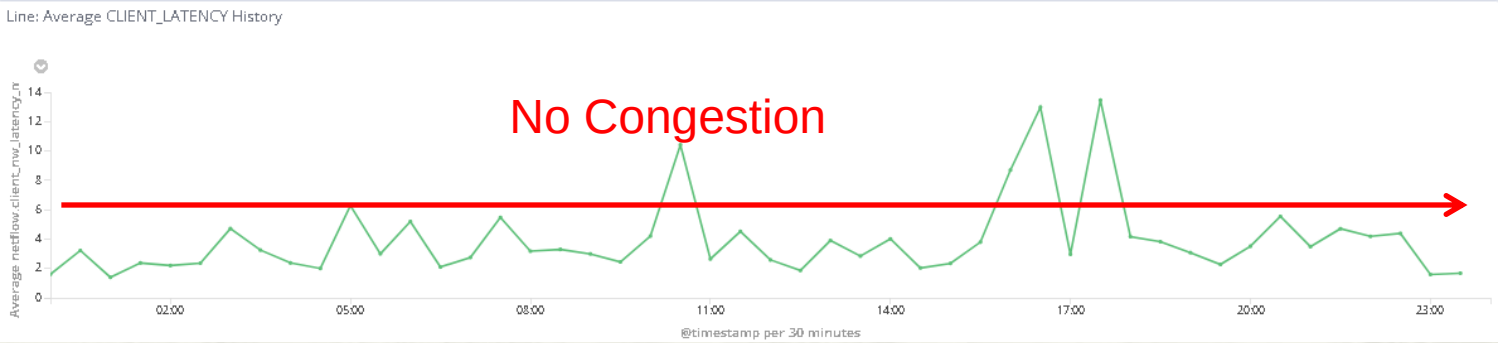


# 有線網段 vs. 無線網段 Congestion

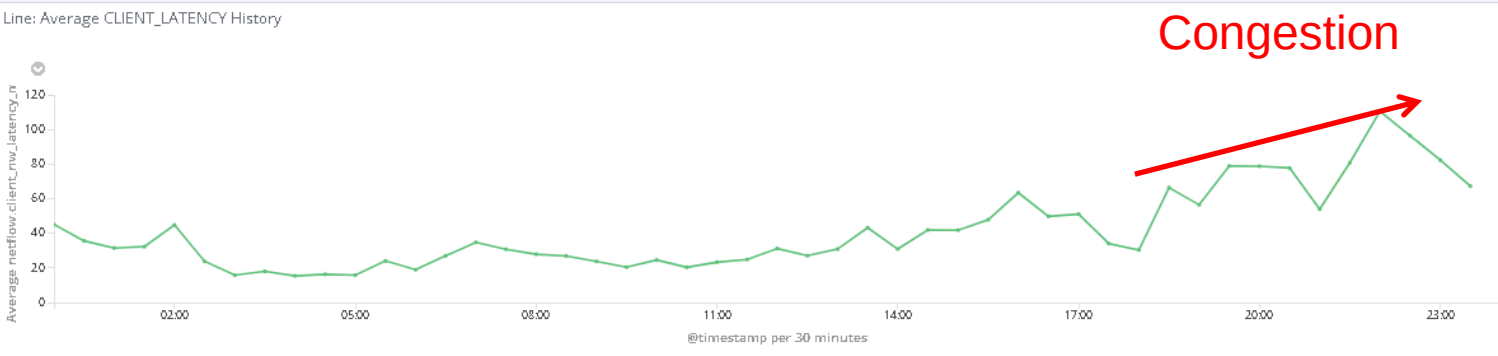
* 140.112.113.0/24 圖書館工作區

| 50th percentile of netflow.client_nw_latency_ms | Average netflow.client_nw_latency_ms | Lower Standard Deviation of netflow.client_nw_latency_ms | Upper Standard Deviation of netflow.client_nw_latency_ms |
|---|---|---|---|
| 1 | 4.512 | -60.8 | 69.824 |



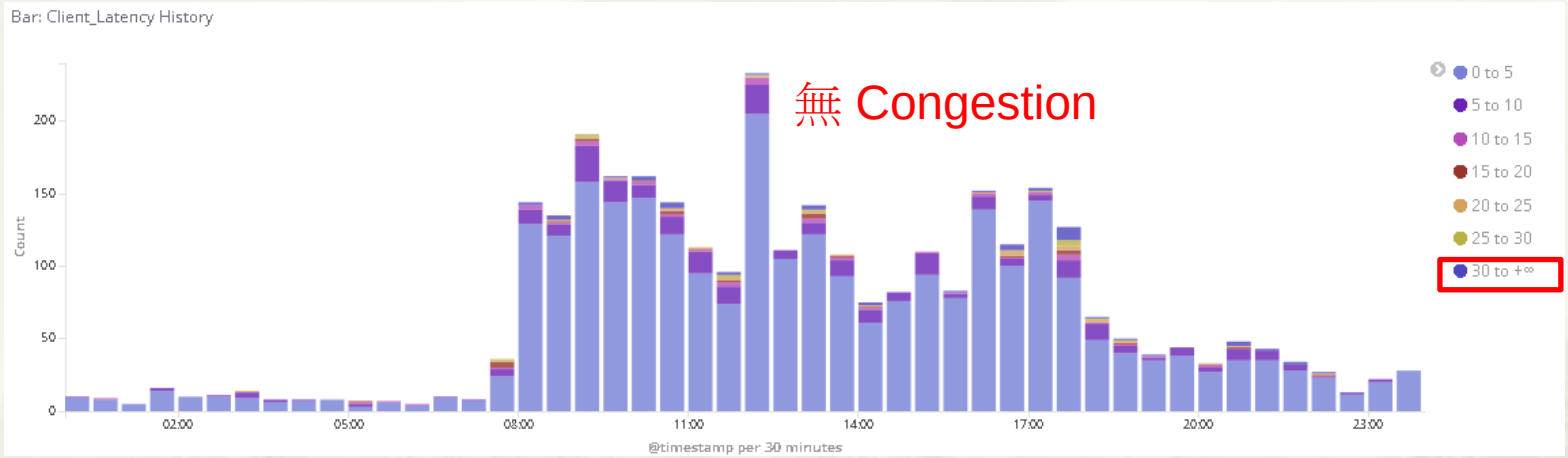

* 140.112.238.0/24 Wireless

| 50th percentile of netflow.client_nw_latency_ms | Average netflow.client_nw_latency_ms | Lower Standard Deviation of netflow.client_nw_latency_ms | Upper Standard Deviation of netflow.client_nw_latency_ms |
|---|---|---|---|
| 2 | 46.939 | -570.453 | 664.33 |

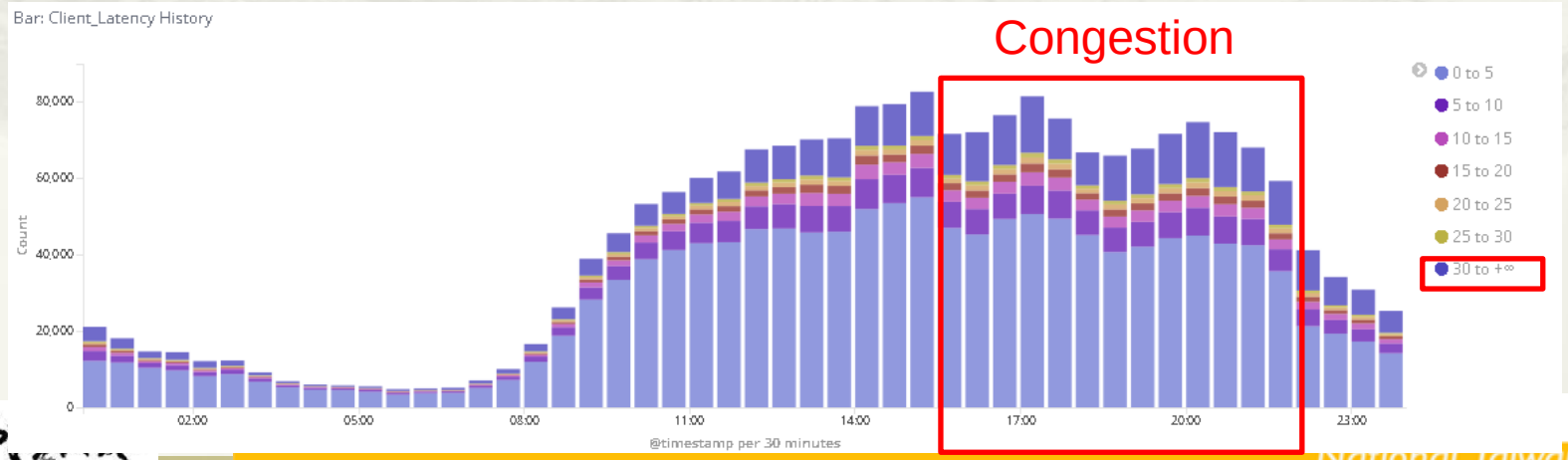


# 有線網段 vs. 無線網段 Congestion

* 140.112.113.0/24 圖書館工作區



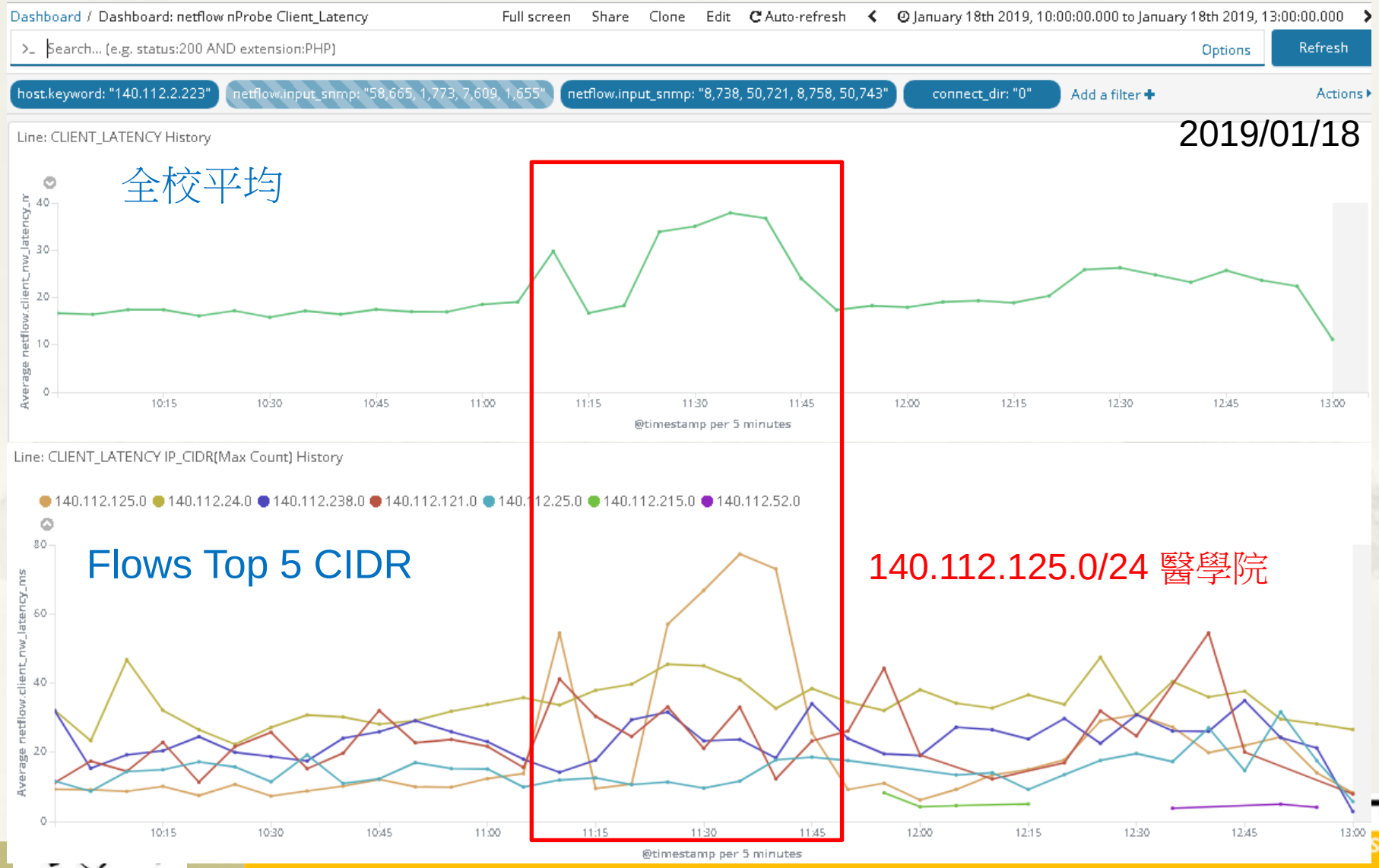

* 140.112.238.0/24 Wireless



# Client Latency
# 異常辨識

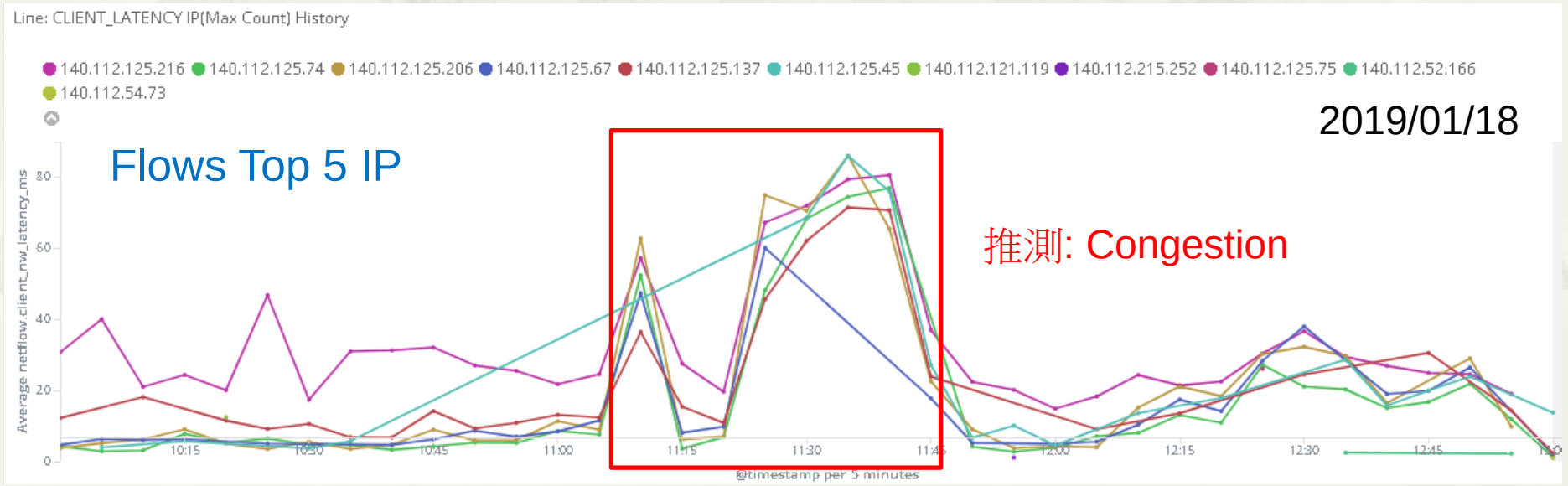
部分網段異常
導致 Latency 變高

# 部分網段異常
# 導致 Latency 變高



# 部分網段異常
# 140.112.125.0/24 醫學院

* 140.112.125.216 雲林分院上網 NAT 設備(國網電路)
* 140.112.125.206 兒童醫院上網 NAT 設備
* 140.112.125.137 臺大醫院東址無線 AP

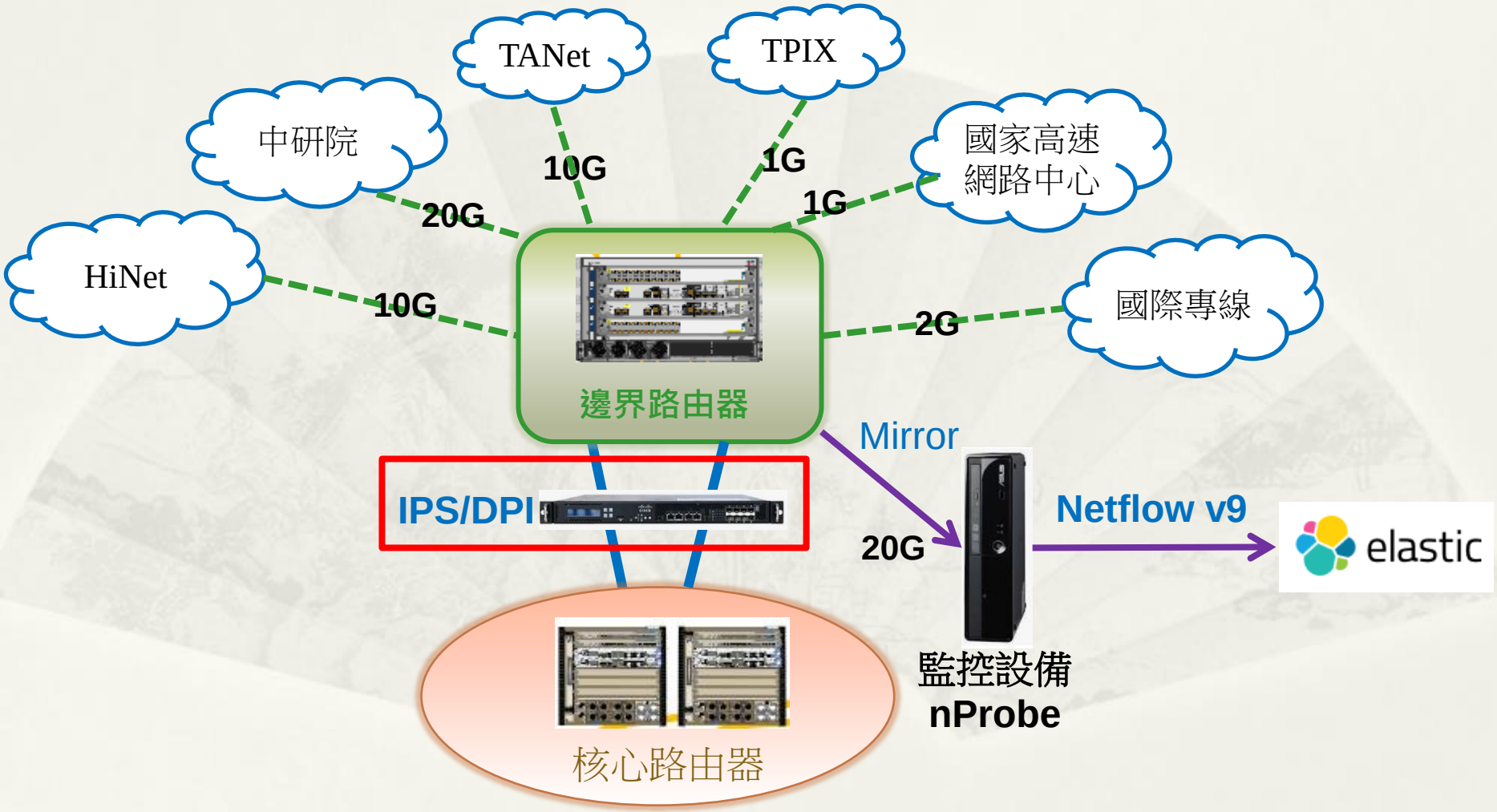


# Client Latency
# 網路設備

Inline/Bypass

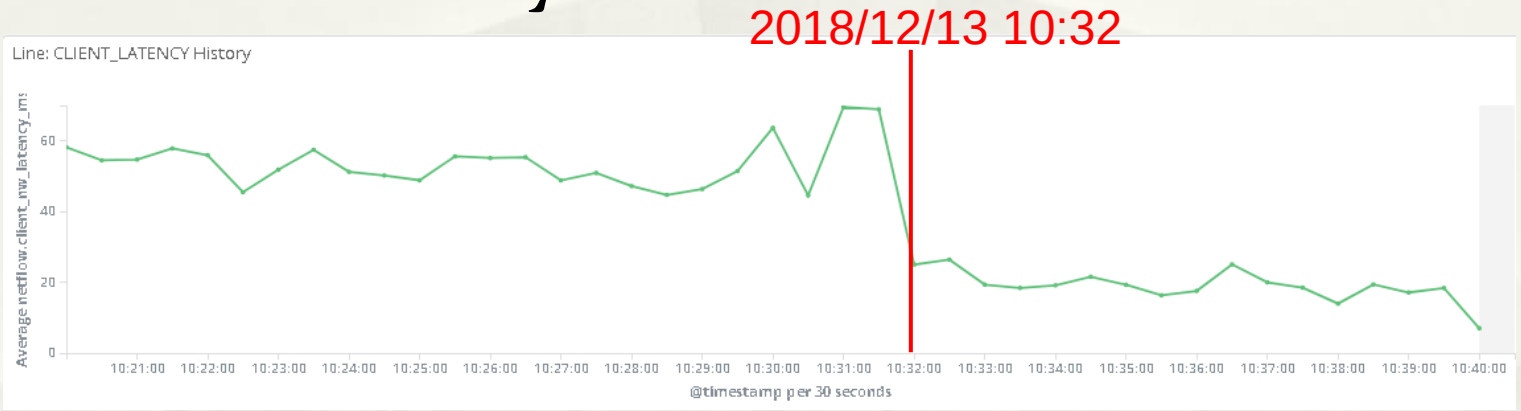
Device Loading

# TCP-based 網路品質監控
# 臺大網路架構圖

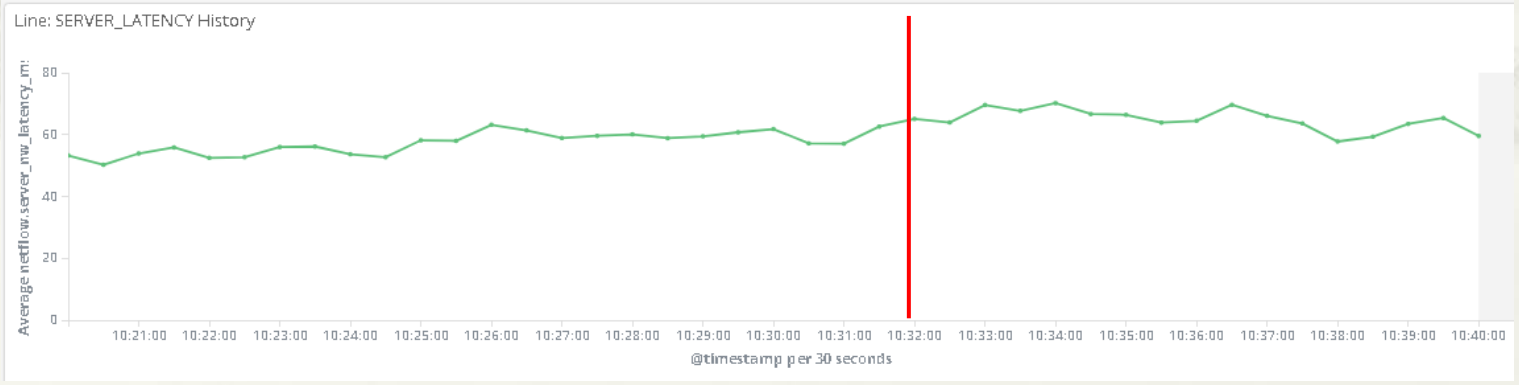


# IPS Inline/Bypass vs. Latency

* Client Latency



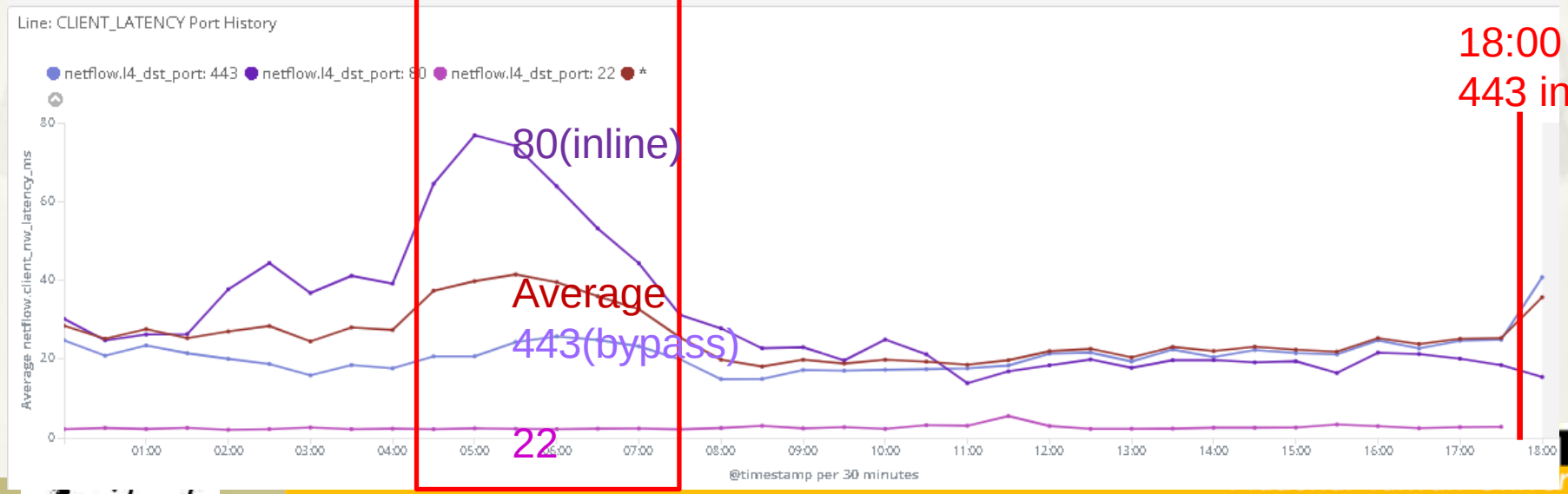

* Server Latency (無影響)



# IPS Loading vs. Latency





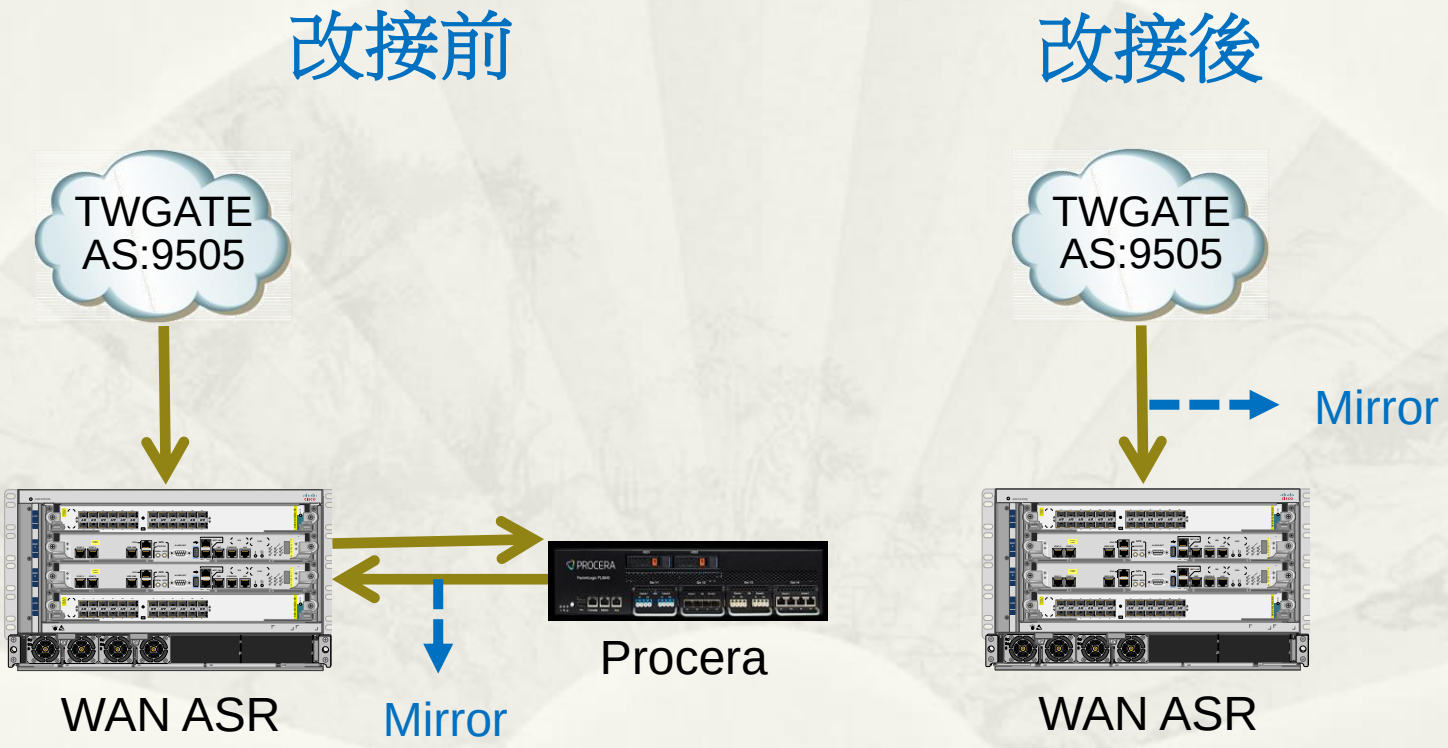


# Server Latency
# 網路設備

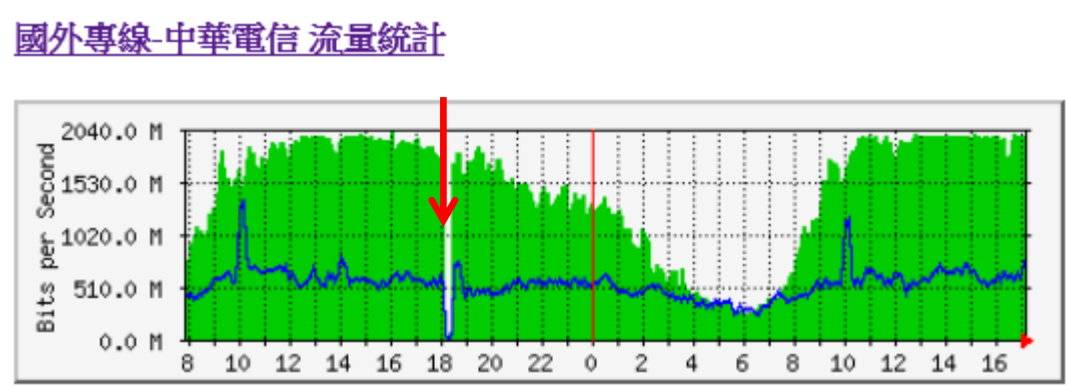
Inline/Bypass

# Procera Inline/Bypass 線路改接

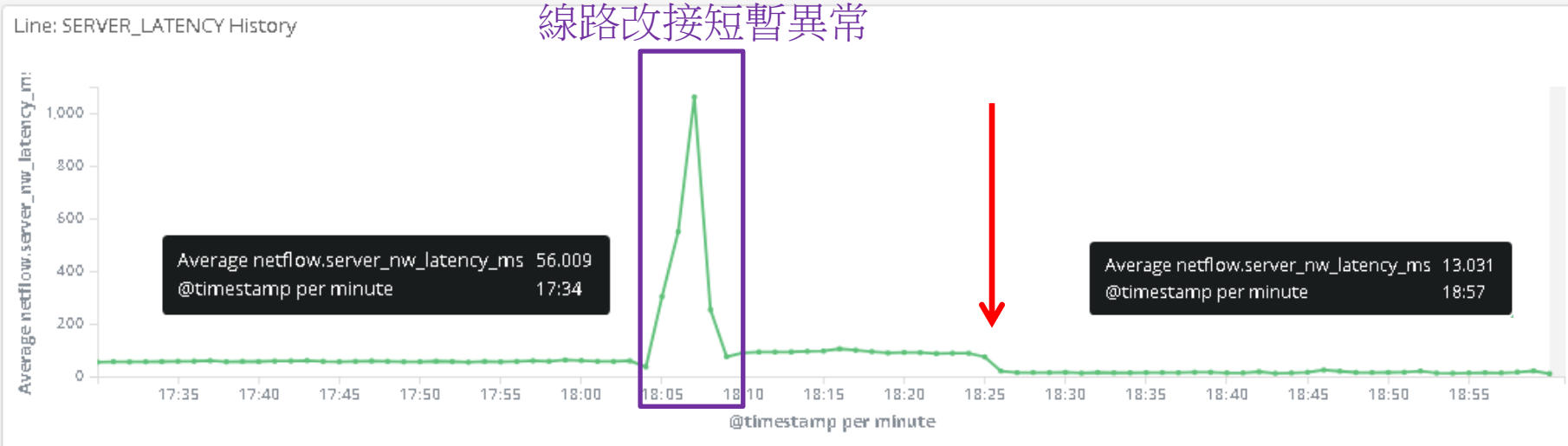
2018/12/03 18:00



# 國際頻寬 & Procera 線路改接 20181203 18:25




線路改接短暫異常

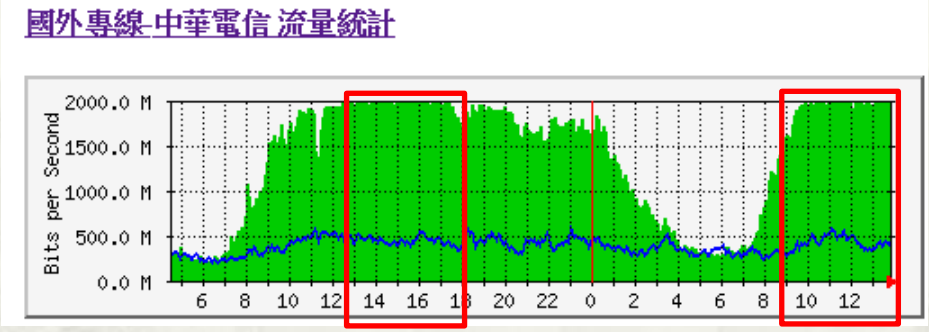


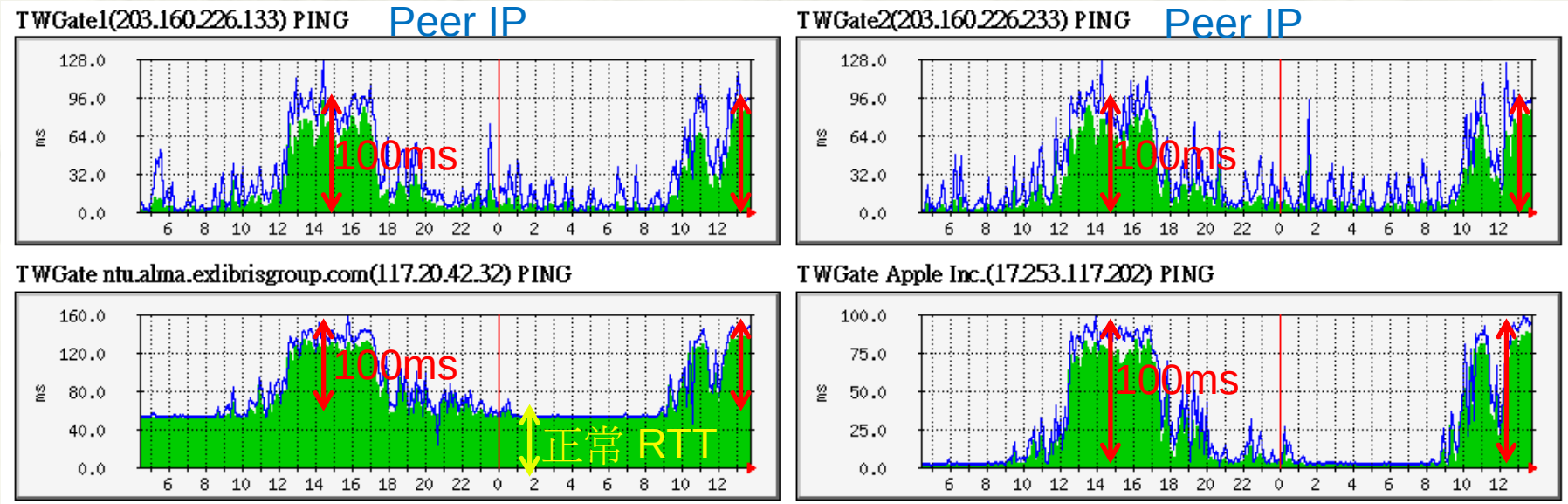
# Server Latency

## 頻寬壅塞對 Latency 之影響

# TWGate Congestion

* 頻寬壅塞時 RTT 增加約 100ms



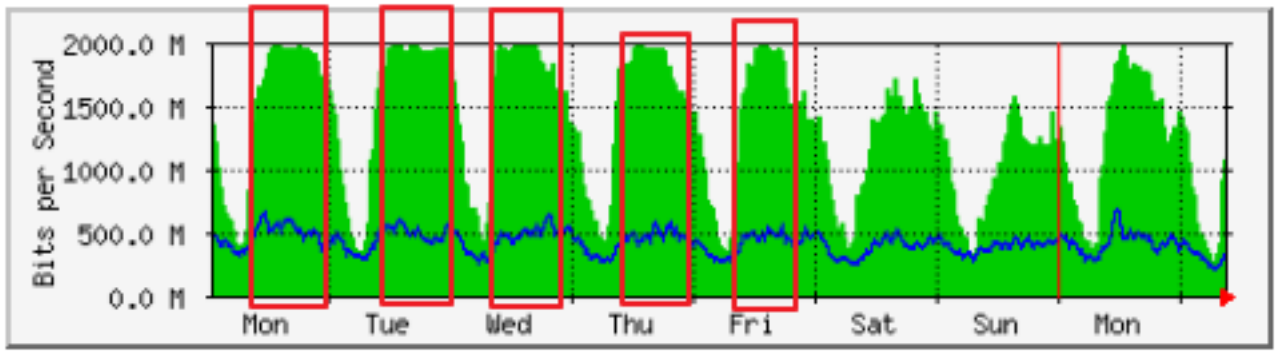




http://www.tp1rc.edu.tw/mrtg/ntu_ping.html

# 國際頻寬壅塞對 Latency 之影響

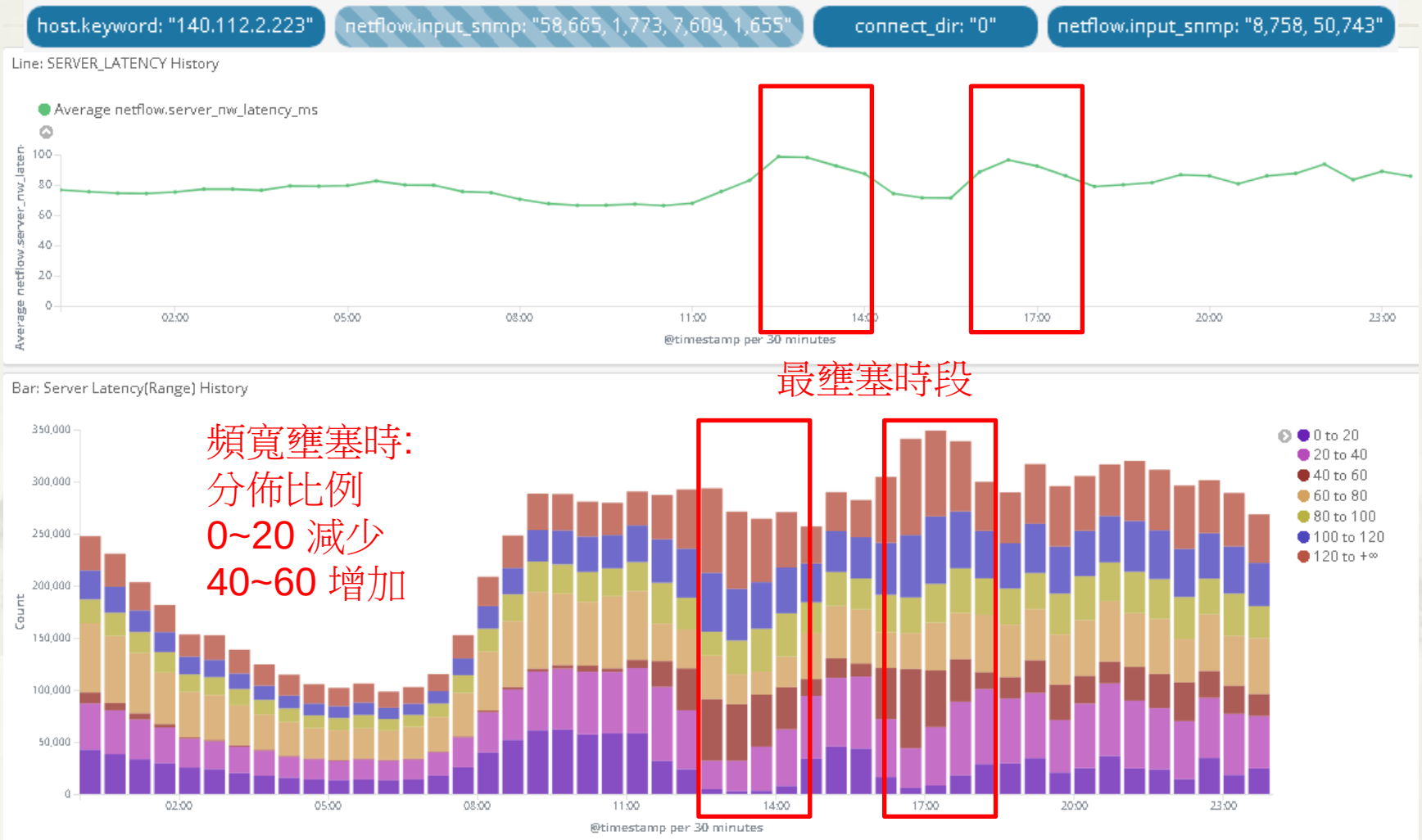
* 2019/01/07 ~ 2019/01/14

每週 圖表 (30 分鐘 平均)

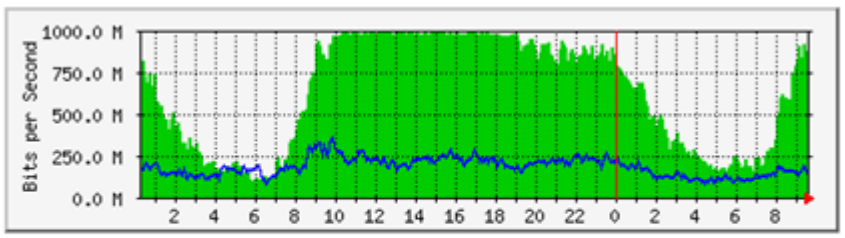



| | 最大 | 平均 | 目前 |
|---|---|---|---|
| 國外專線 => 台大: | 1973.6 Mb/秒 (12.3%) | 1301.8 Mb/秒 (8.1%) | 1076.1 Mb/秒 (6.7%) |
| 台大 => 國外專線: | 666.9 Mb/秒 (4.2%) | 411.3 Mb/秒 (2.6%) | 334.3 Mb/秒 (2.1%) |

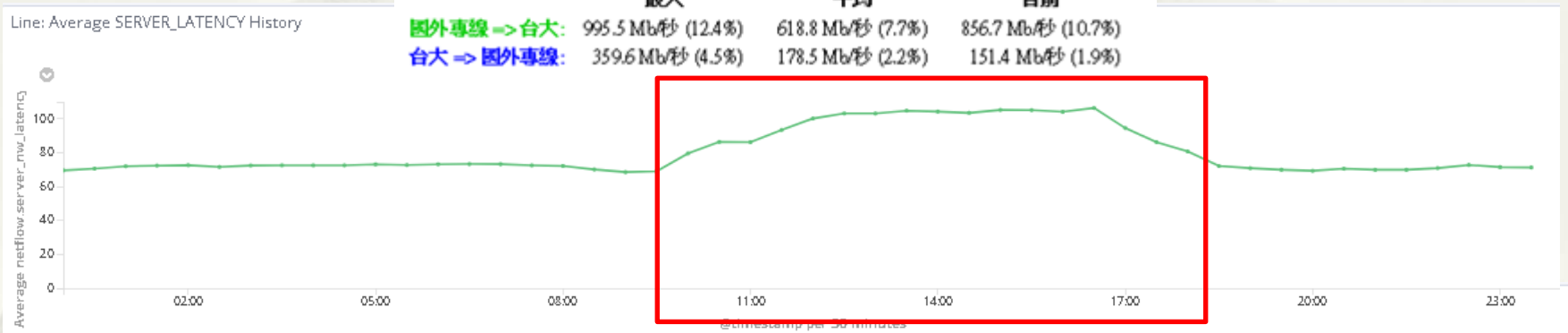
# 20190108 Server Latency

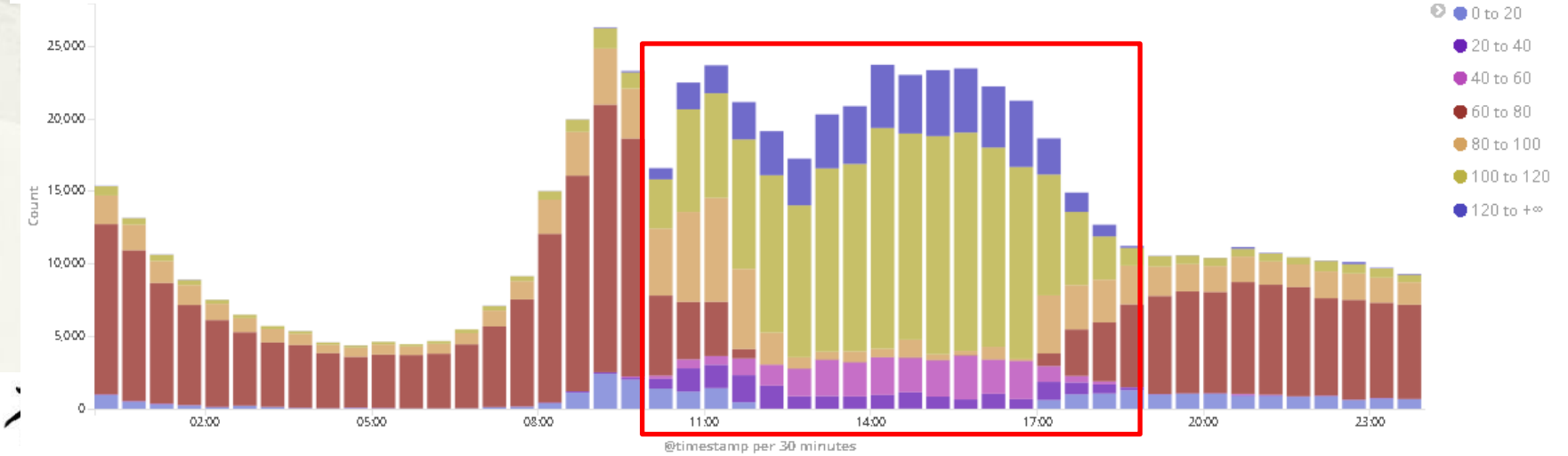


# 20190220 Server Latency
# Dst AS=Apple Inc.




| | 最大 | 平均 | 目前 |
|---|---|---|---|
| 國外專線 => 台大: | 995.5 Mb/秒 (12.4%) | 618.8 Mb/秒 (7.7%) | 856.7 Mb/秒 (10.7%) |
| 台大 => 國外專線: | 359.6 Mb/秒 (4.5%) | 178.5 Mb/秒 (2.2%) | 151.4 Mb/秒 (1.9%) |

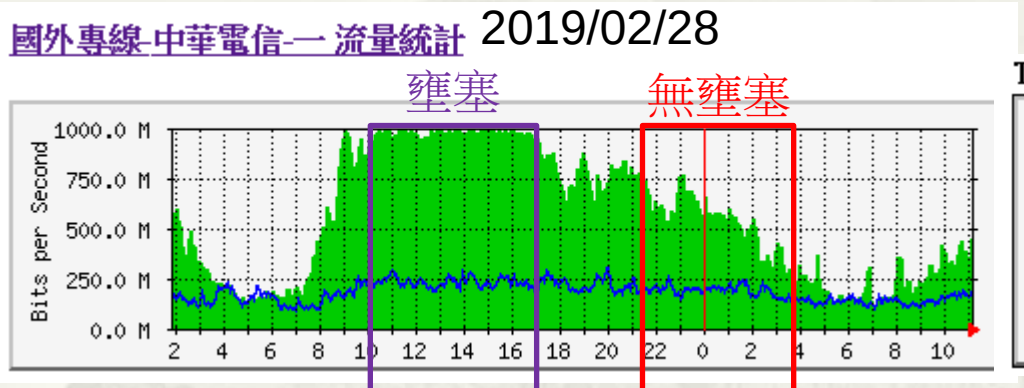


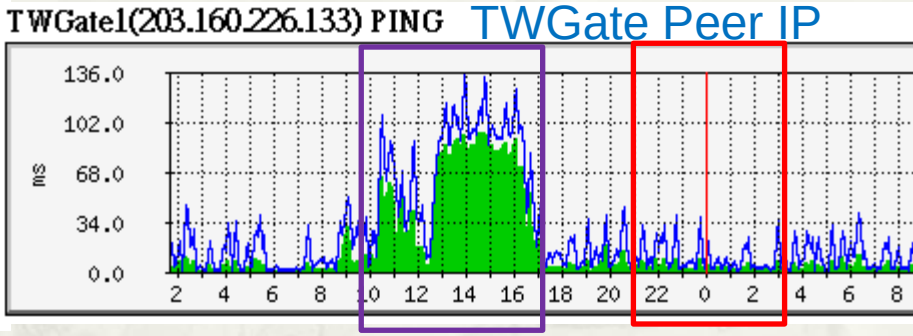



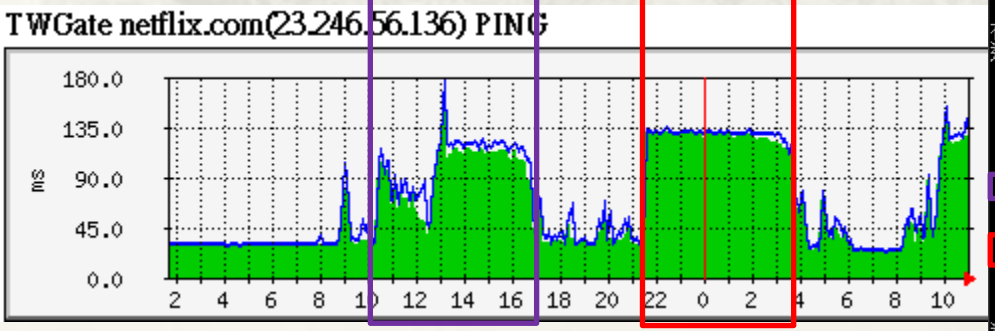
# Server Latency
# 網路壅塞節點偵測

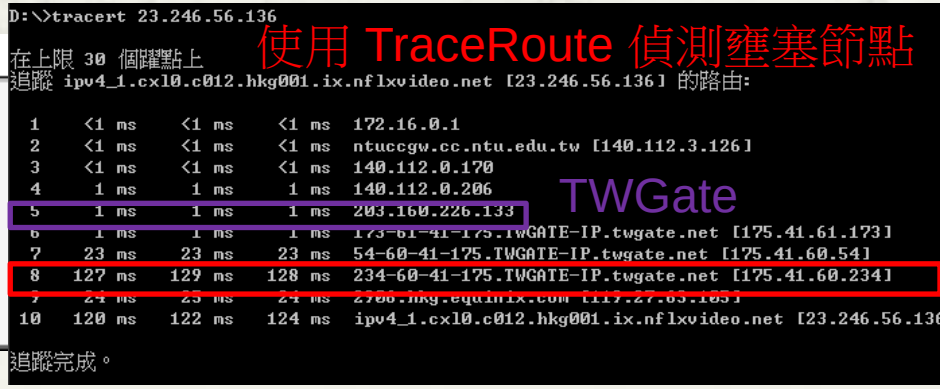
# 網路壅塞節點偵測

* 壅塞發生在其他節點:
  * 非 TWGate 壅塞造成 Netflix Latency 變高

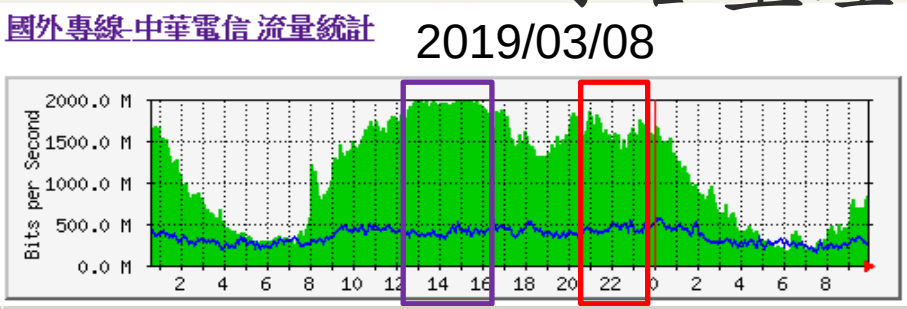


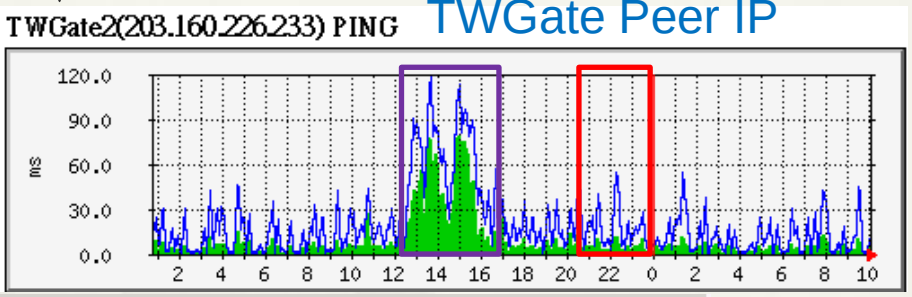



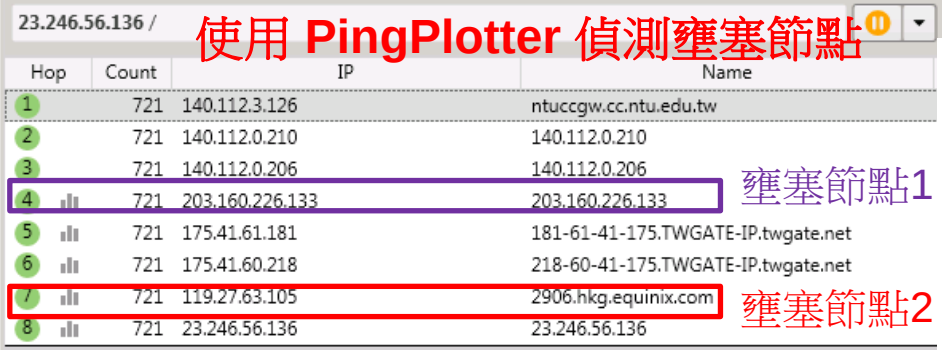



# 網路壅塞節點偵測



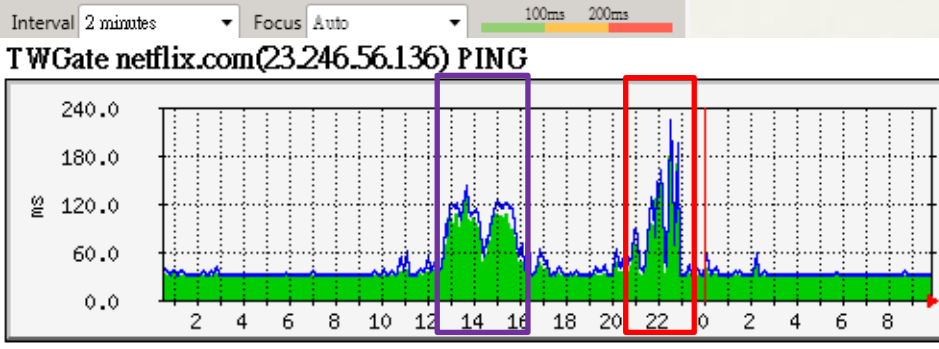



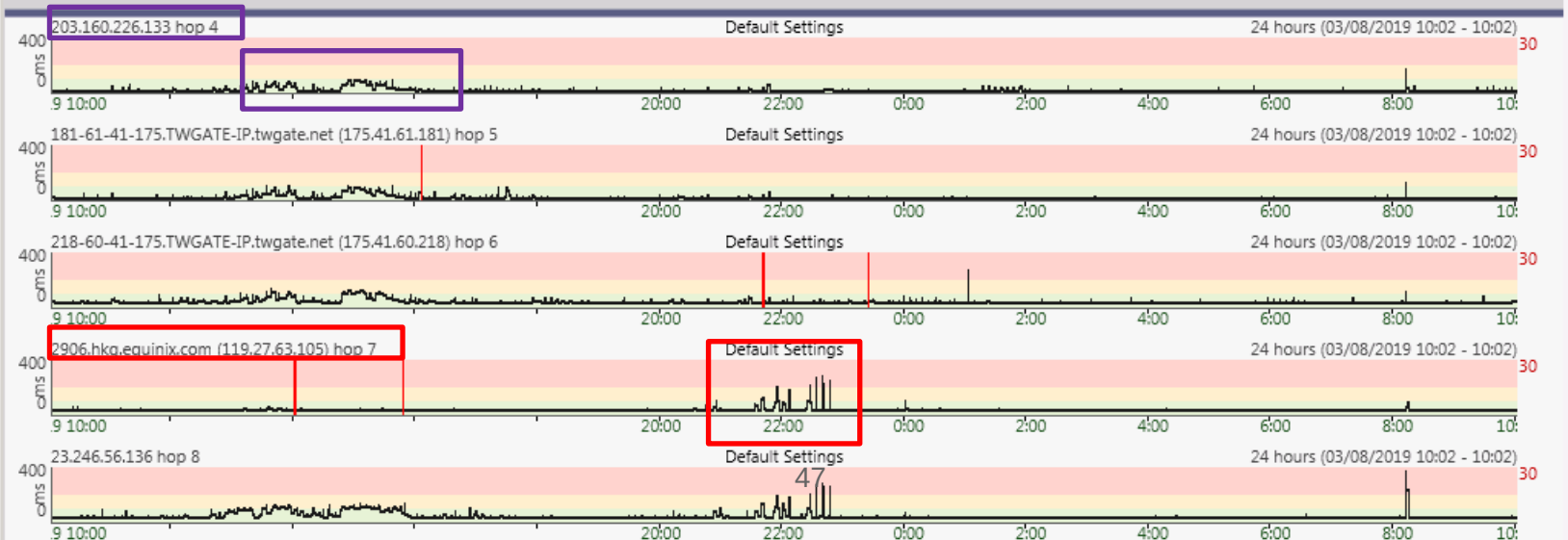

使用 **PingPlotter** 偵測壅塞節點




壅塞節點1

壅塞節點2



# Server Latency
# Client/Server 實體距離

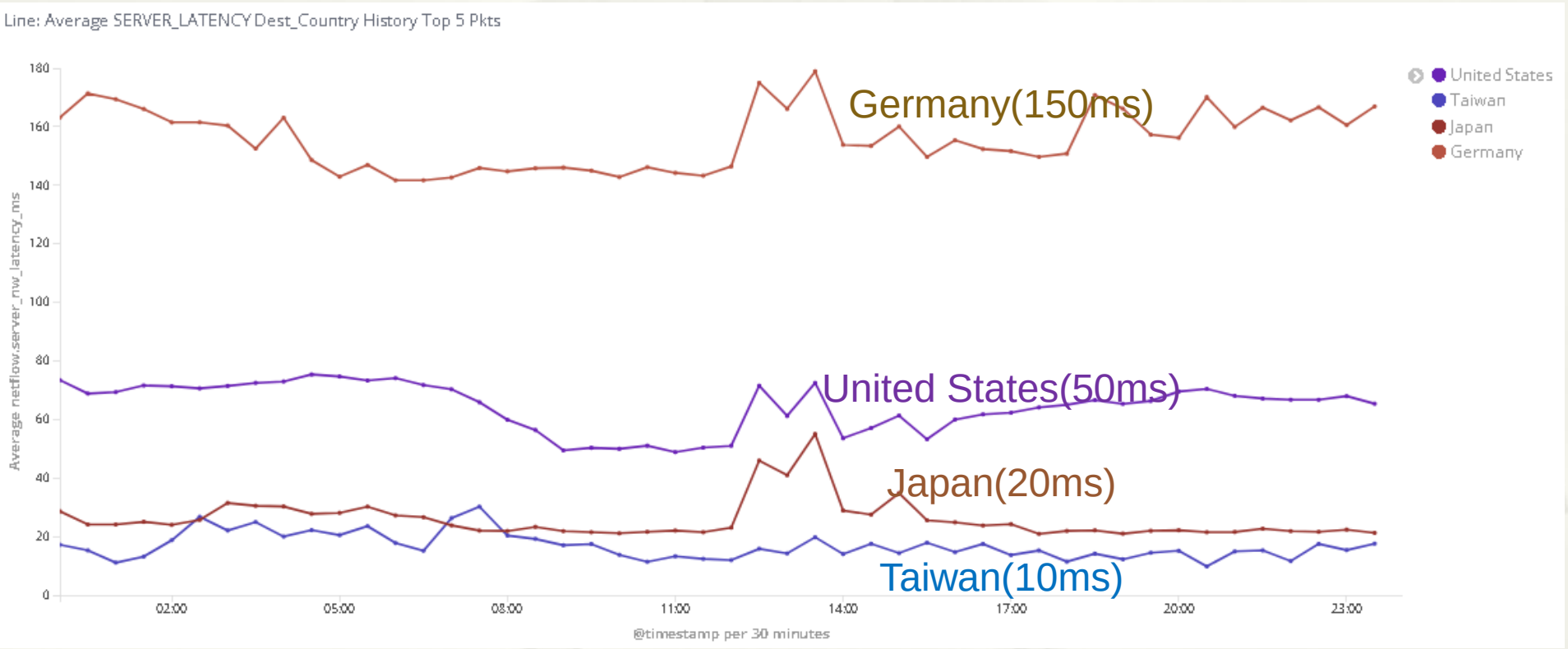
# 光速與時間

* 光速 =299, 792 Km/s


* 光速台北到洛杉磯來回需時
* 10,899 * 2/ 299, 792= 72 ms

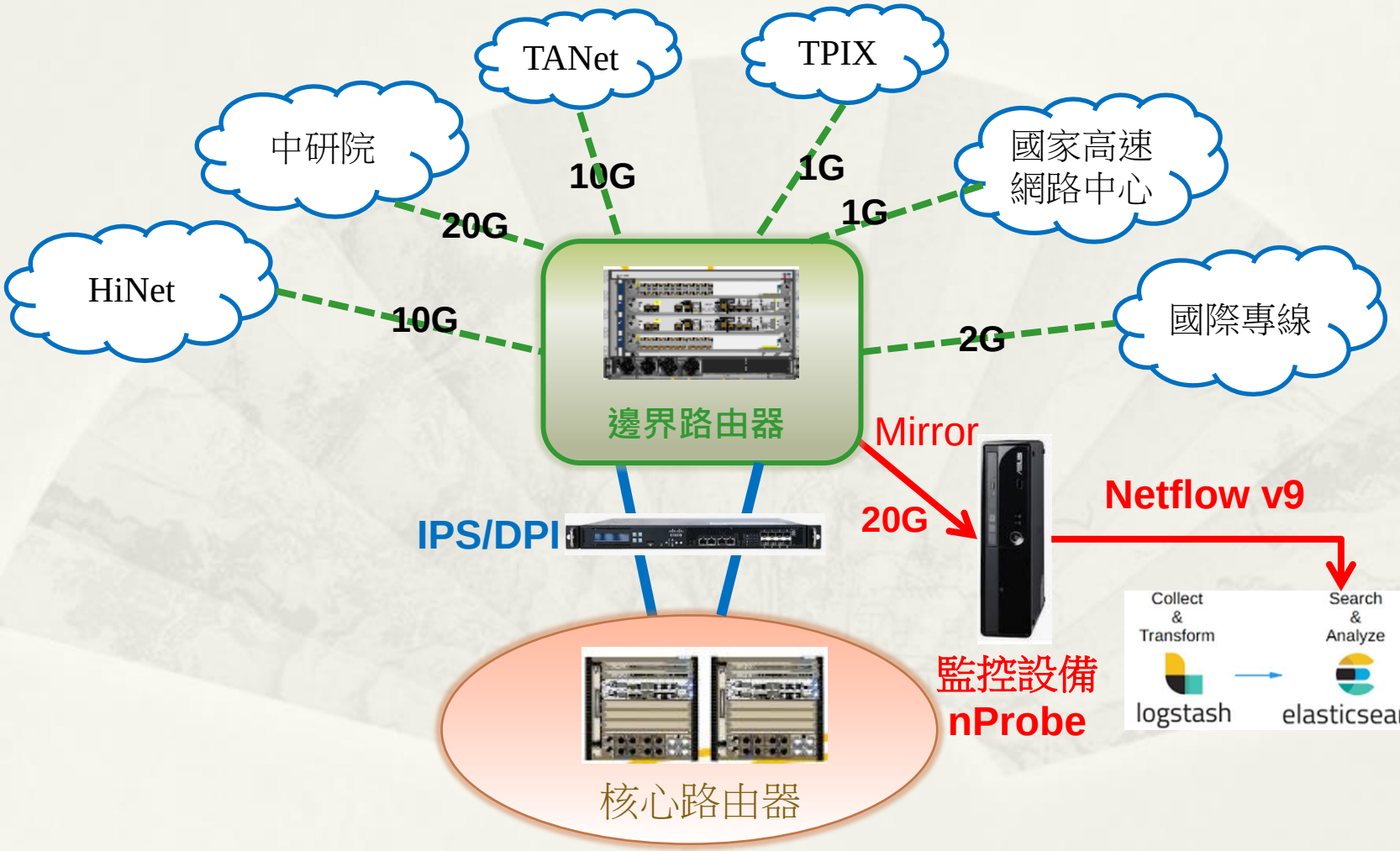
```
D:\>ping lacity.org

Ping lacity.org [54.245.230.145] (使用 32 位元組的資料):
回覆自 54.245.230.145: 位元組=32 時間=150ms TTL=42
回覆自 54.245.230.145: 位元組=32 時間=150ms TTL=42
回覆自 54.245.230.145: 位元組=32 時間=150ms TTL=42
回覆自 54.245.230.145: 位元組=32 時間=150ms TTL=42
```

# Server Latency
# 不同國家 24 Hrs



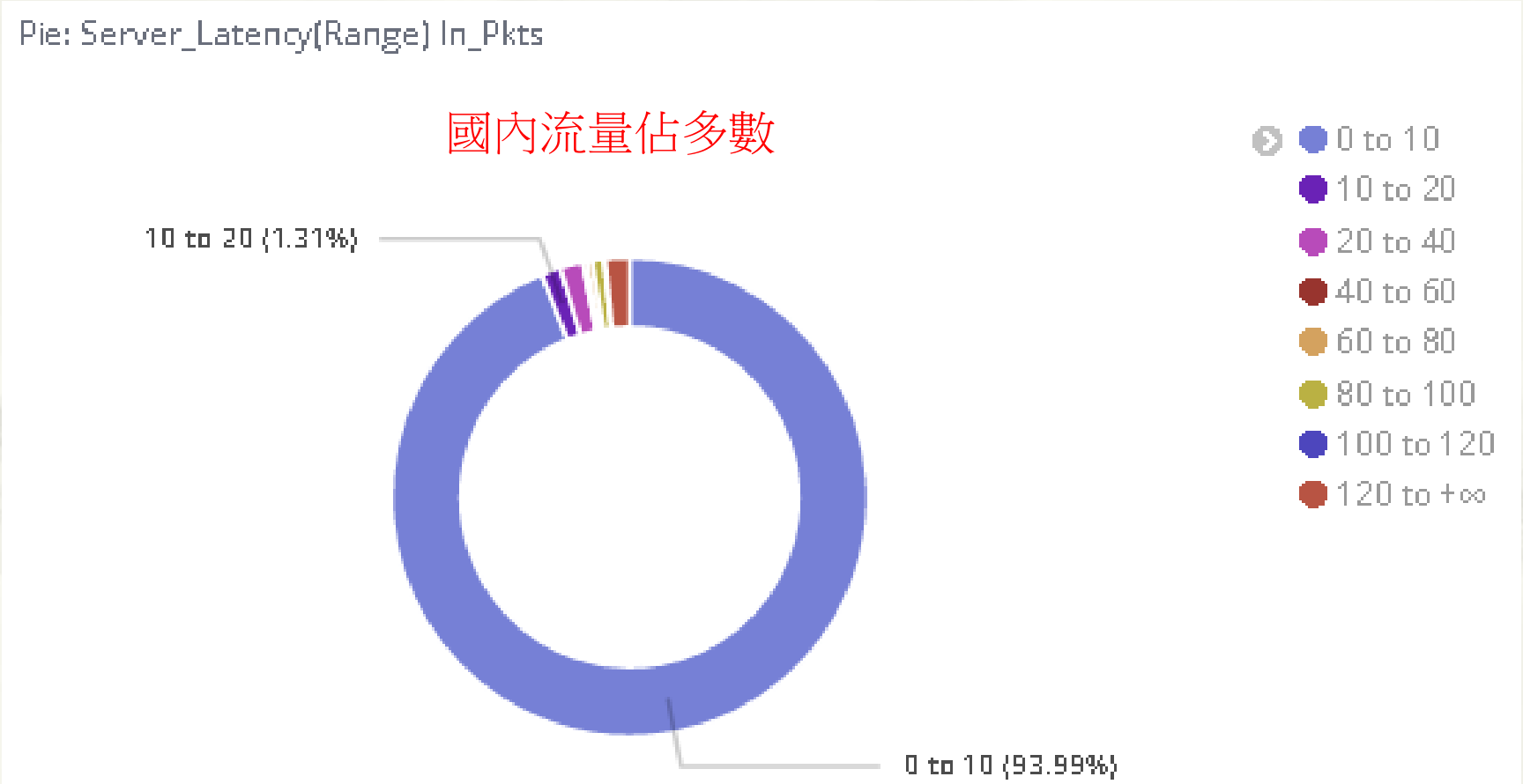
# Server Latency
# 對外線路連線地區分析

# TCP-based 網路品質監控
# 臺大網路架構圖



# TANet (24hrs)

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "50,721"

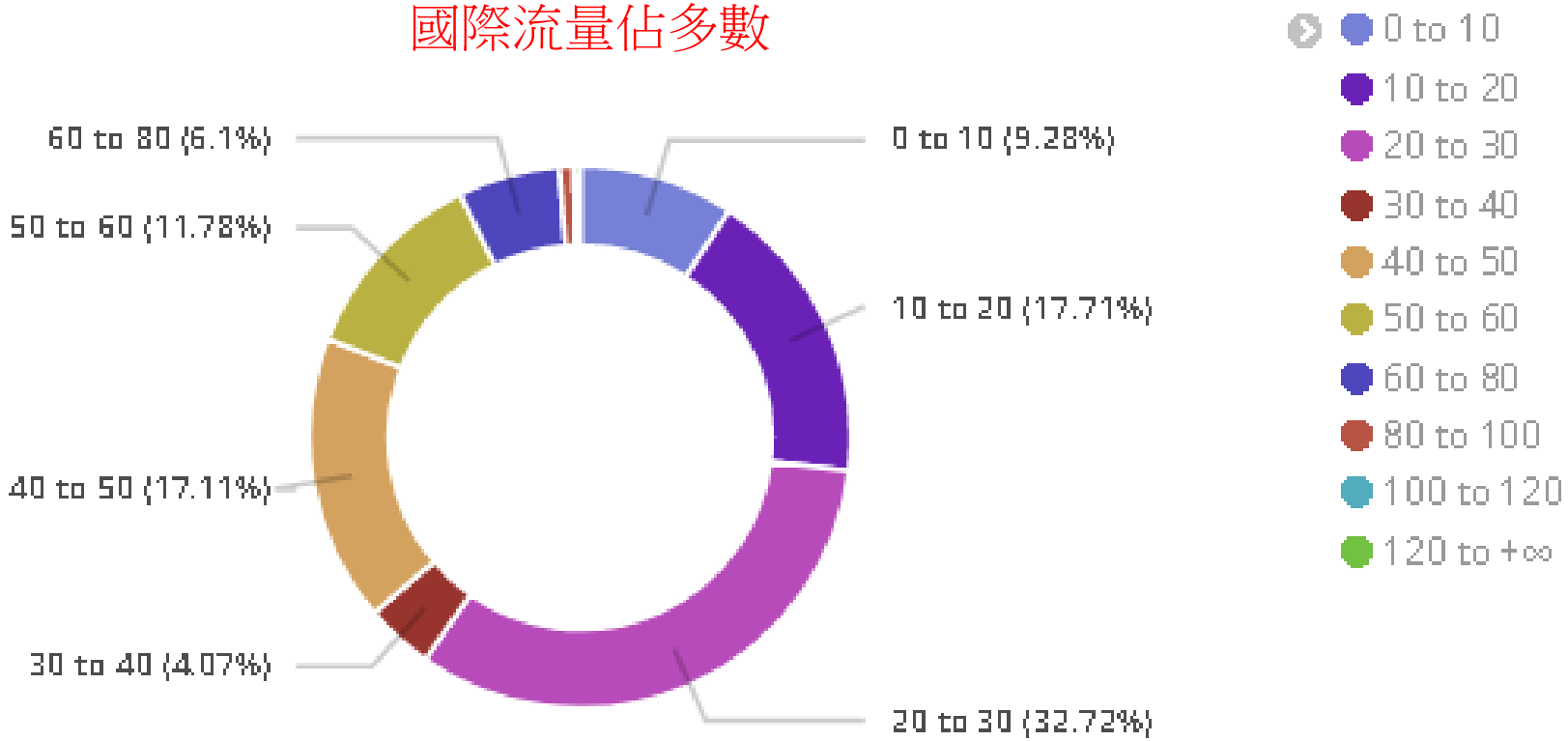


# Sinica (24hrs)

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "8,738"

Pie: Server_Latency(Range) In_Pkts

國際流量佔多數

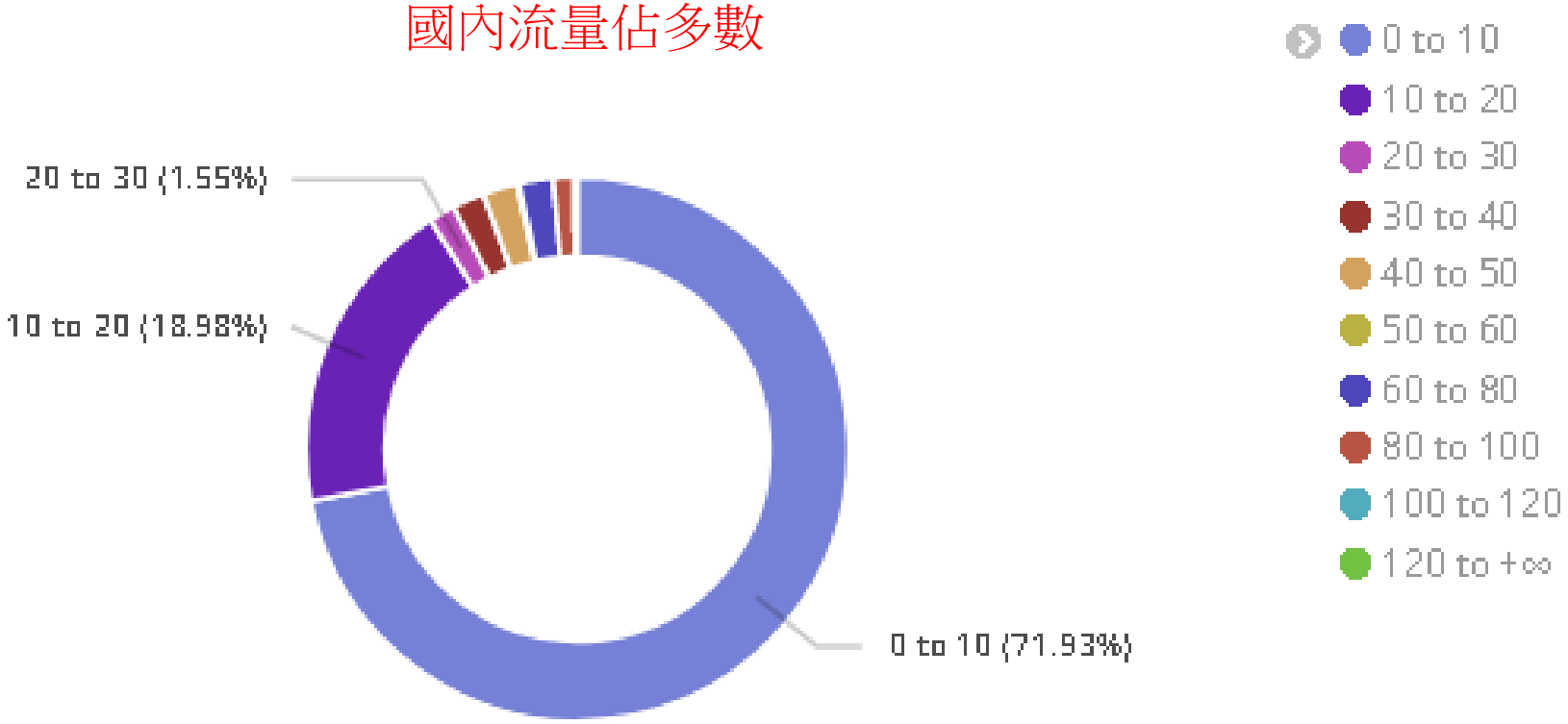


# TPIX (24hrs)

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "50,742"

Pie: Server_Latency(Range) In_Pkts

國內流量佔多數

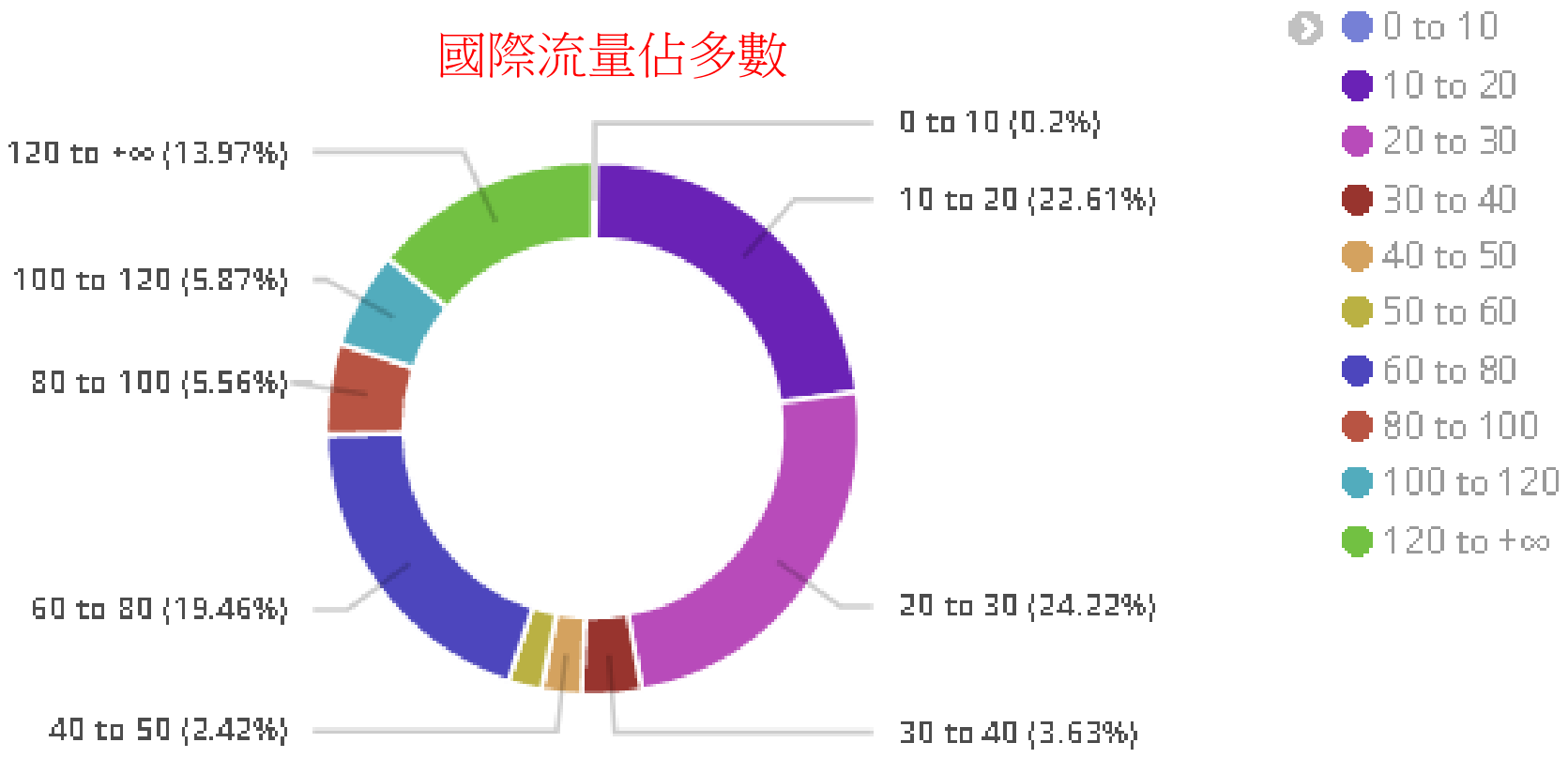


# TWGate (24hrs)

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "8,758, 50,743"

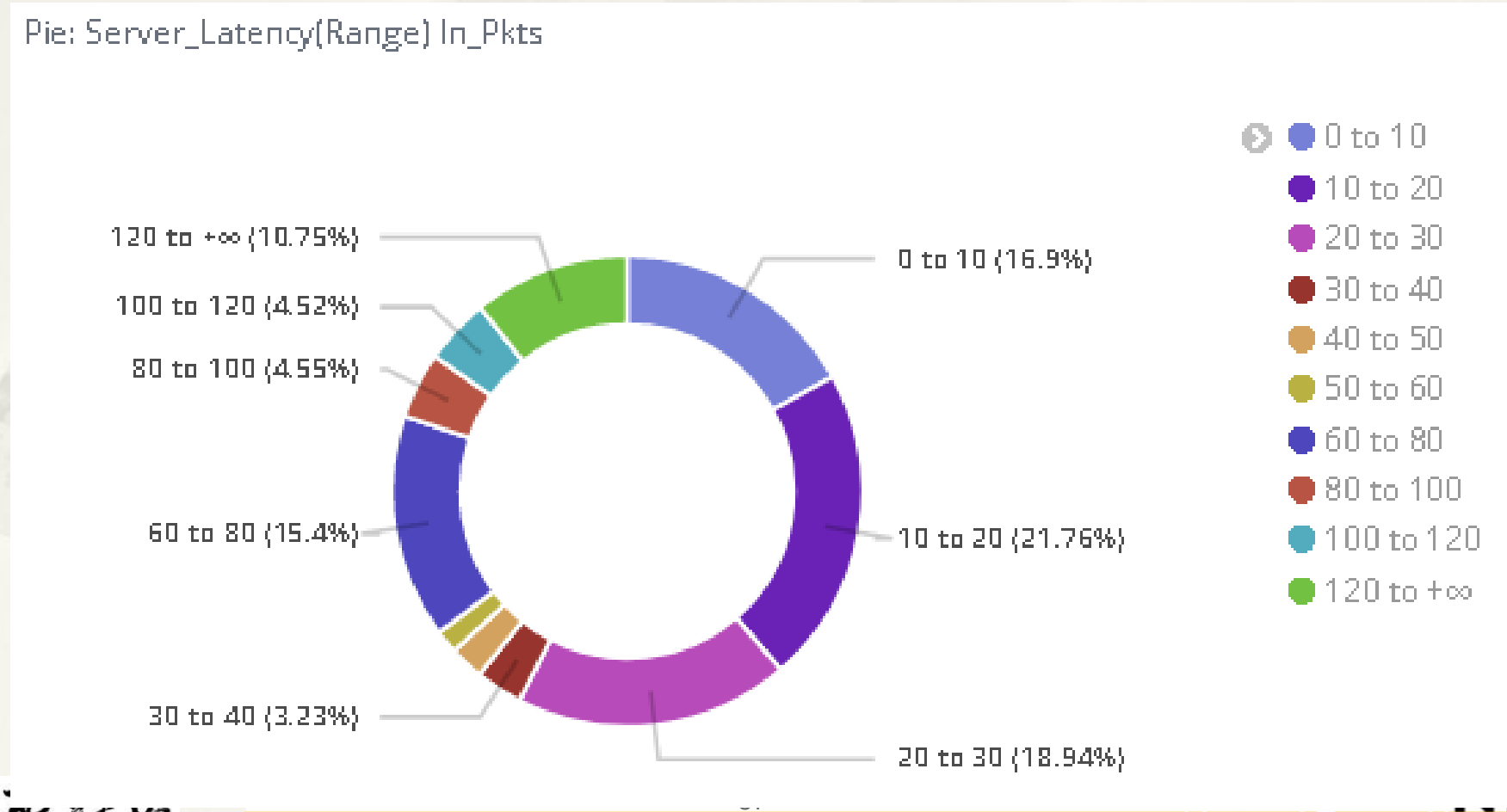
Pie: Server_Latency(Range) In_Pkts

國際流量佔多數



# TPIX + TWGate (24hrs)

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "50,742, 8,758, 50,743"



# Server Latency
# GeoIP DB 準確率分析

# 驗證方法

- 某 ASN 大部分 IP，GeoIP DB 不正確
  - 同一國家，某 ASN 平均值與其他差異太大
- 某 ASN 部分 IP ，GeoIP DB 不正確
  - Country + ASN，Latency Deviation 過大
  - Country + ASN，Latency 分佈比例異常

# 同一國家
# 某 ASN 平均值與其他差異太大

* Group By AS Order By 封包數 Where Country= US.

host.keyword: "140.112.2.223" | connect_dir: "0" | netflow.server_nw_latency_ms: "1 to 20,000" | netflow.input_snmp: "8,758, 50,743, 8,736, 8,738, 50,721, 50,742" | geoip_dst.country_name.keyword: "United States" | Add a filter +

某 ASN 大部分 IP，GeoIP DB 不正確

| Country | AS | ASN | in_pkts | Server latency(ms) |
|---|---|---|---|---|
| United States | Akamai International B.V. | 20,940 | 2,413,477 | 56.46 |
| United States | Akamai International B.V. | 33,905 | 9,351 | 43.818 |
| United States | Apple Inc. | 714 | 903,094 | 33.215 |
| United States | Apple Inc. | 6,185 | 3,251 | 120.929 |
| United States | Facebook, Inc. | 32,934 | 857,279 | 42.89 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 15,133 | 588,917 | 79.177 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 701 | 26,781 | 26.026 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 11,486 | 181 | 140.75 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 14,153 | 133 | 53.333 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 23,148 | 15 | 144.667 |
| United States | Akamai Technologies, Inc. | 35,994 | 244,152 | 11.277 |
| United States | Akamai Technologies, Inc. | 16,625 | 219,535 | 16.546 |
| United States | Google Inc. | 15,169 | 433,488 | 22.985 |
| United States | Google Inc. | 36,040 | 50 | 73 |
| United States | Amazon.com, Inc. | 16,509 | 234,941 | 122.836 |
| United States | Amazon.com, Inc. | 14,618 | 154,945 | 143.102 |
| United States | Microsoft Corporation | 8,068 | 379,896 | 5.393 |
| United States | Microsoft Corporation | 8,075 | 2,164 | 5.509 |
| United States | Unwired | 32,354 | 198,535 | 107.864 |

# Country + ASN Latency Deviation 過大

* 某 ASN 部分 IP ，GeoIP DB 不正確

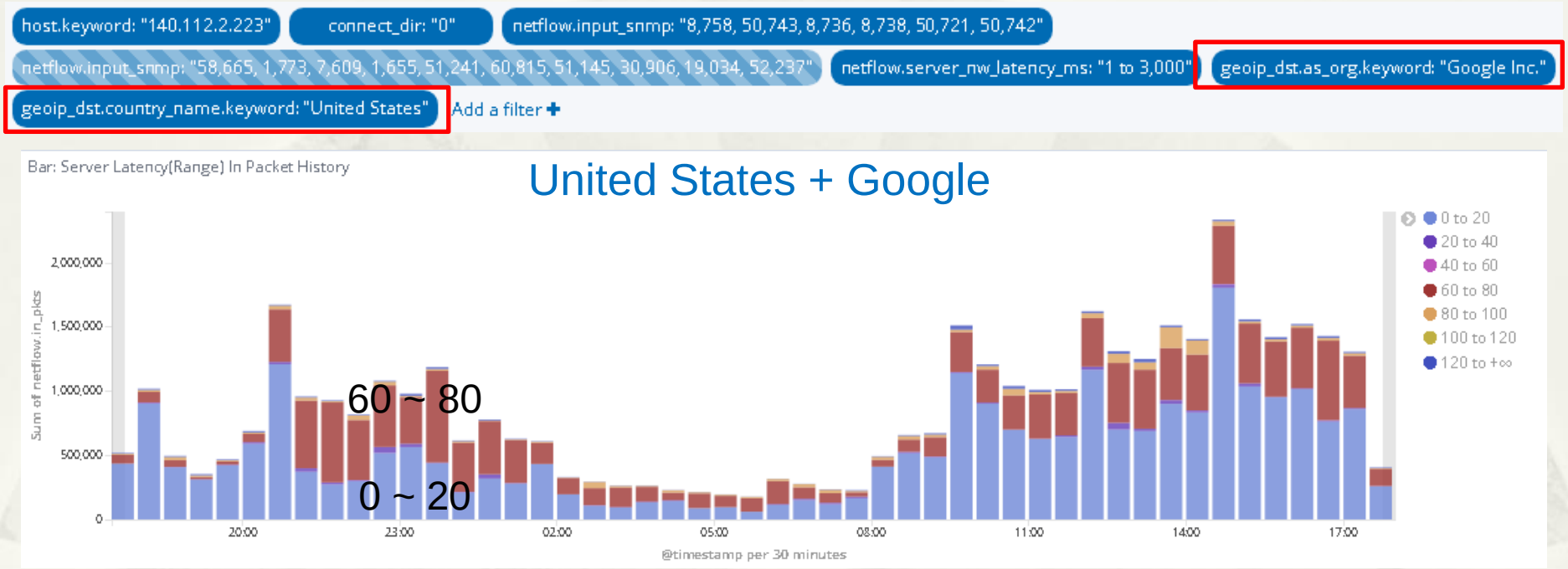
| geoip_dst.country_name.key | geoip_dst.as_org.keyword: Descending | geoip_dst.asn: Des | Count | 50th percentile | Average r | Lower Standard | Upper Standard | stdev |
|---|---|---|---|---|---|---|---|---|
| United States | Amazon.com, Inc. | 14,618 | 801,291 | 106 | 114.172 | -55.806 | 284.149 | 84.9885 |
| United States | Amazon.com, Inc. | 16,509 | 469,071 | 81 | 88.897 | -16.822 | 194.616 | 52.8595 |
| United States | Apple Inc. | 714 | 947,204 | 73 | 73.026 | 8.628 | 137.423 | 32.1985 |
| United States | Apple Inc. | 6,185 | 2,394 | 69.591 | 73.929 | -9.83 | 157.689 | 41.88 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 15,133 | 604,766 | 72 | 67.54 | 7.266 | 127.814 | 30.137 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 701 | 13,399 | 99 | 85.124 | -203.439 | 373.688 | 144.282 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 23,148 | 435 | 103.6 | 114.995 | -30.785 | 260.776 | 72.8905 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 14,153 | 196 | 18 | 25.265 | -18.167 | 68.698 | 21.7165 |
| United States | MCI Communications Services, Inc. d/b/a Verizon Business | 11,486 | 169 | 107 | 111.148 | 84.986 | 137.31 | 13.081 |
| United States | Akamai Technologies, Inc. | 16,625 | 138,965 | 10.963 | 19.136 | -48.116 | 86.388 | 33.626 |
| United States | Akamai Technologies, Inc. | 35,994 | 111,937 | 9 | 16.504 | -46.639 | 79.647 | 31.5715 |
| United States | Akamai Technologies, Inc. | 18,717 | 2 | 103.5 | 103.5 | 98.5 | 108.5 | 2.5 |
| United States | Akamai Technologies, Inc. | 18,680 | 1 | 87 | 87 | 87 | 87 | 0 |
| United States | Dropbox, Inc. | 19,679 | 184,070 | 72 | 85.156 | 21.924 | 148.387 | 31.6155 |
| United States | Digital Ocean, Inc. | 14,061 | 100,287 | 72.075 | 89.589 | -219.653 | 398.83 | 154.6205 |
| United States | Level 3 Communications, Inc. | 3,356 | 87,642 | 87.753 | 99.619 | -20.906 | 220.145 | 60.263 |
| United States | Level 3 Communications, Inc. | 3,549 | 6,797 | 78 | 143.126 | -1,020.60 | 1,306.85 | 581.8635 |
| United States | Level 3 Communications, Inc. | 10.753 | 14 | 99 | 104.357 | 77.465 | 131.25 | 13.4465 |

# Country + ASN
# Latency 分佈比例異常

| geoip_dst.country_name.ke | geoip_dst.as_org.keyword: Des | geoip_dst.asn: D | netflow.server_r | Count |
|---|---|---|---|---|
| United States | Amazon.com, Inc. | 14,618 | 0 to 20 | 16 |
| United States | Amazon.com, Inc. | 14,618 | 20 to 40 | 13 |
| United States | Amazon.com, Inc. | 14,618 | 40 to 60 | 21 |
| United States | Amazon.com, Inc. | 14,618 | 60 to 80 | 77 |
| United States | Amazon.com, Inc. | 14,618 | 80 to 100 | 67,390 |
| United States | Amazon.com, Inc. | 14,618 | 100 to +∞ | 733,774 |
| United States | Amazon.com, Inc. | 16,509 | 0 to 20 | 1,101 |
| United States | Amazon.com, Inc. | 16,509 | 20 to 40 | 1,498 |
| United States | Amazon.com, Inc. | 16,509 | 40 to 60 | 1,019 |
| United States | Amazon.com, Inc. | 16,509 | 60 to 80 | 210,158 |
| United States | Amazon.com, Inc. | 16,509 | 80 to 100 | 129,482 |
| United States | Amazon.com, Inc. | 16,509 | 100 to +∞ | 125,813 |
| United States | Apple Inc. | 714 | 0 to 20 | 93,332 |
| United States | Apple Inc. | 714 | 20 to 40 | 39,292 |
| United States | Apple Inc. | 714 | 40 to 60 | 11,758 |
| United States | Apple Inc. | 714 | 60 to 80 | 450,012 |
| United States | Apple Inc. | 714 | 80 to 100 | 192,828 |
| United States | Apple Inc. | 714 | 100 to +∞ | 159,982 |

部分 IP ，應不在 US

# Country + ASN
# Latency 分佈比例異常



# TCP-based 網路品質監控

* 優點
  * 利用使用者上網行為進行量測，提供大量數據
  * 被動式偵測(封包 Listening)，不佔用頻寬資源
  * 可快速釐清 Intranet or Internet 異常
  * 不需佈建監控設備，節省電力與資源
  * 可追溯過去之歷史統計記錄

# 簡報完畢
# 謝謝