TCP-BASED 網路品質監控

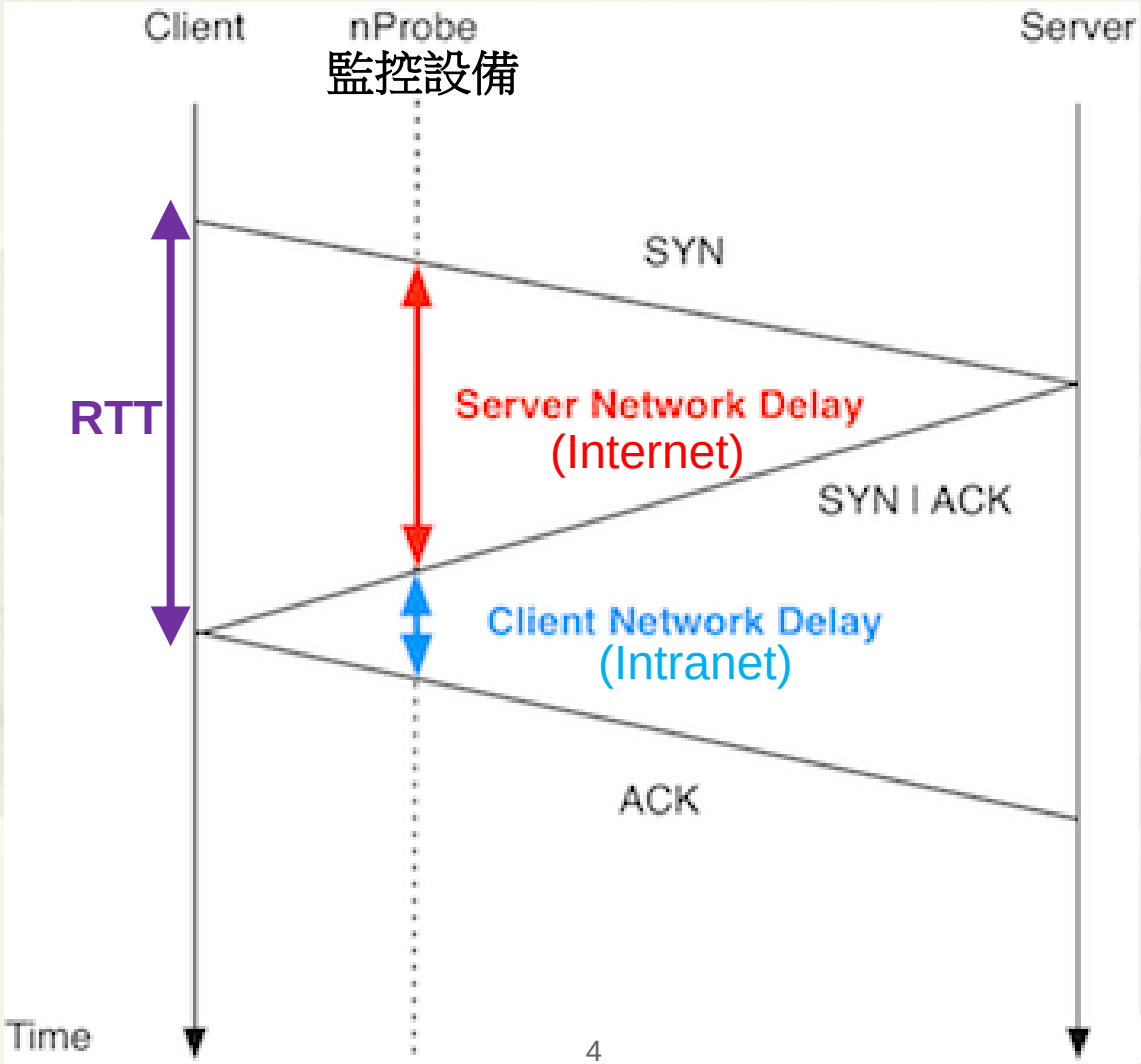
傳統網路品質監控

- 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
  - 需有專用設備與軟體才能進行 24Hr 監控與統計

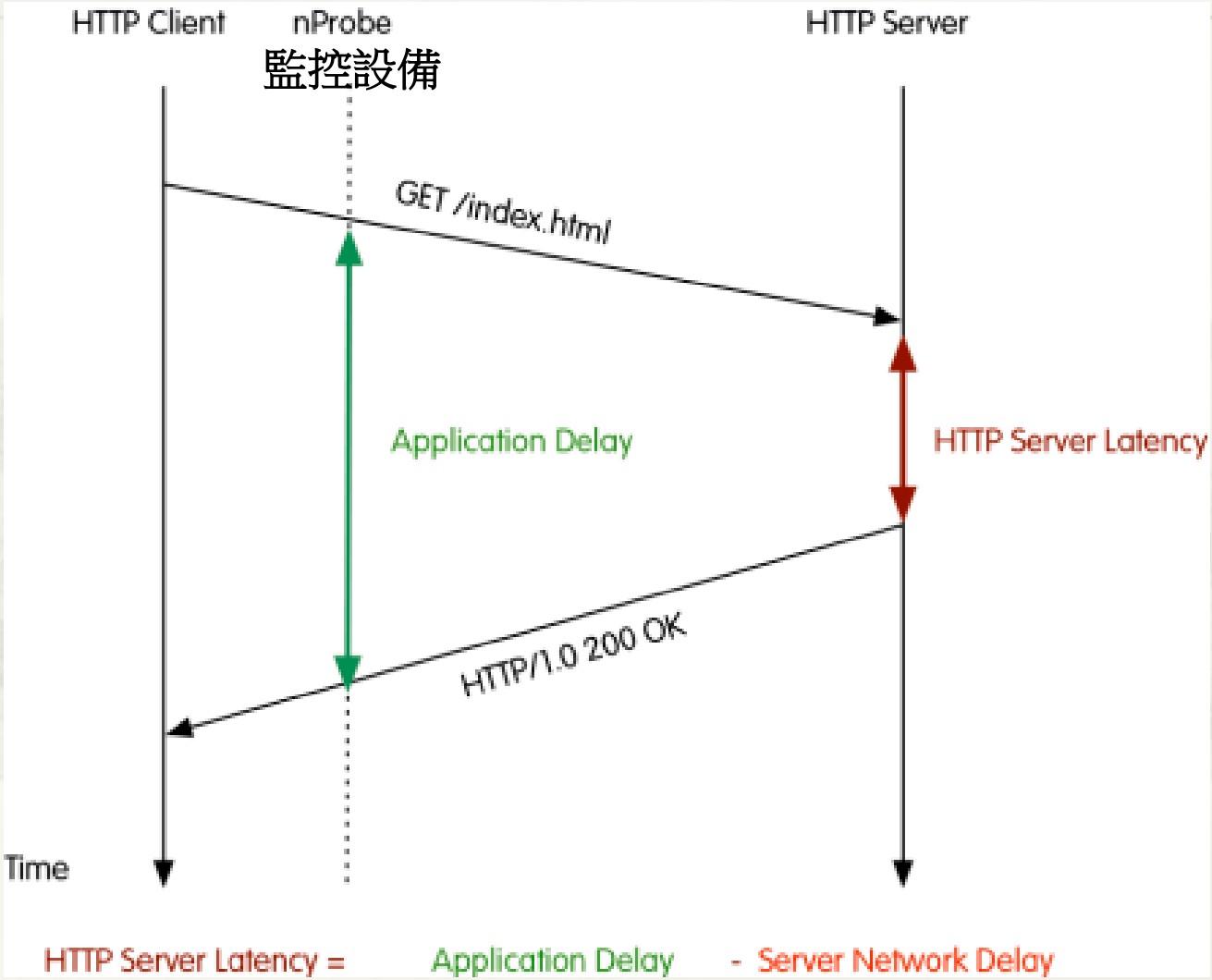
TCP-based 網路品質監控

- 監控方法: TCP
  - RTT: TCP 3-way handshake
  - Packet Lost: TCP Retrasmit & OutOfOrder

Network Latency



Application Latency



監控設備

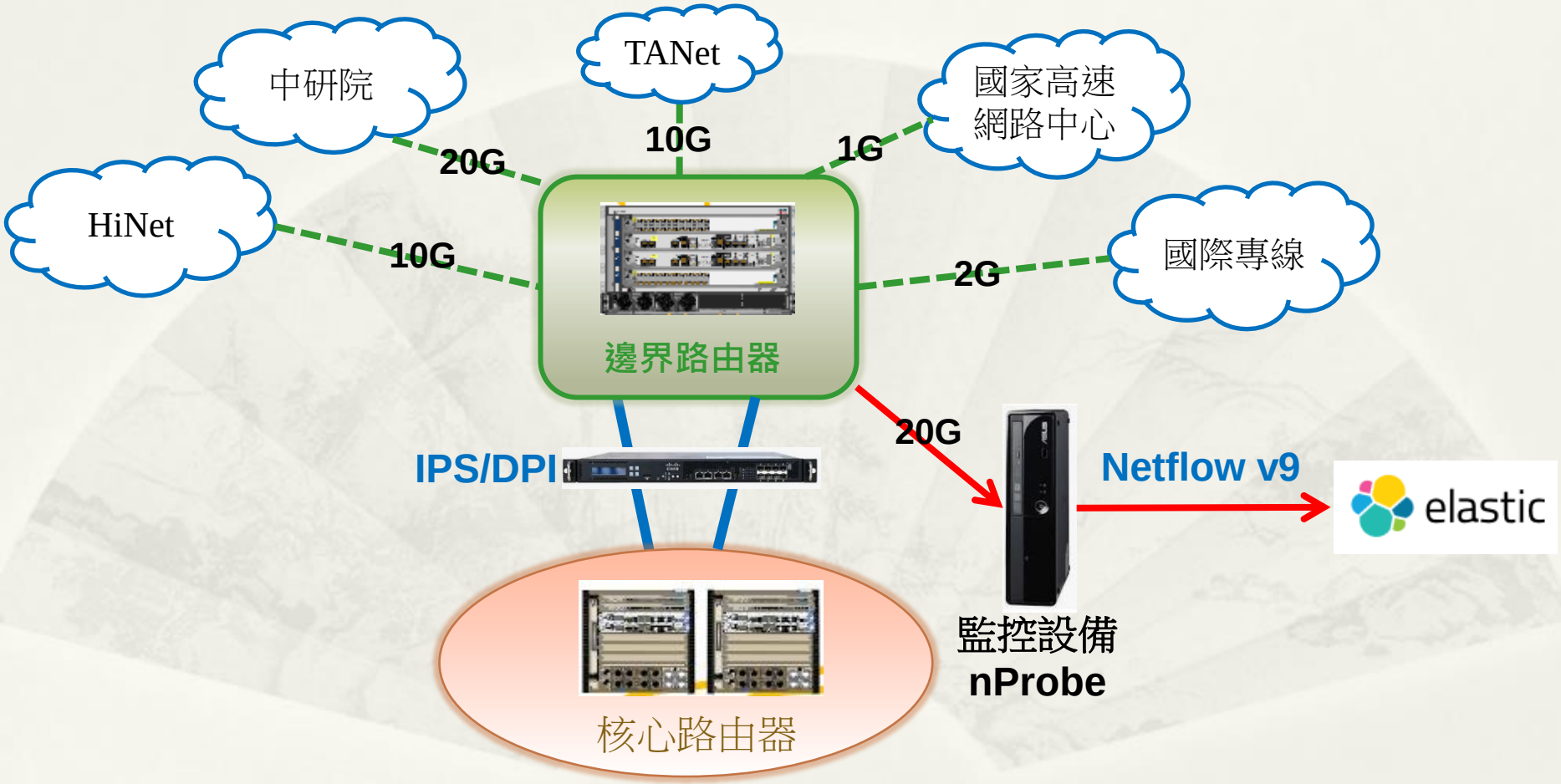
- 新一代 Router
  - Cisco Application Visibility and Control Solution (Cisco AVC)
    - Cisco ASR 1000
  - Use Netflow V9/V10 自訂格式
    - flow record name

      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)
- Inline 設備: Proprietary Report
  - 頻寬管理器/DPI 設備: Procera

TCP-based 網路品質監控

* 優點
  * 被動式偵測(封包 Listening)，不佔用頻寬資源
  * 可快速釐清 Intranet or Internet 緩慢或異常
  * 不需佈建監控設備，節省電力與資源
  * 準確性更高: 網路現成大量連線記錄提供量測結果
  * 可追溯過去之歷史統計記錄

TCP-based 網路品質監控
臺大網路架構圖



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

校外連線校內 PTT

#	netflow.appl_latency_ms	1
#	netflow.client_nw_latency_ms	16
#	netflow.in_bits	31,440
#	netflow.in_bytes	3,930
#	netflow.in_pkts	73
#	netflow.input_snmp	7,609
💻	netflow.ipv4_cidr24_dst_addr	140.112.172.0
💻	netflow.ipv4_dst_addr	140.112.172.3
💻	netflow.ipv4_src_addr	39.12.94.29
#	netflow.l4_dst_port	23
#	netflow.l4_src_port	51,651
t	netflow.l7_proto_name	Telnet
#	netflow.max_ttl	54
#	netflow.min_ttl	54
#	netflow.ooorder_in_pkts	0
#	netflow.ooorder_out_pkts	0
#	netflow.output_snmp	50,721
#	netflow.protocol	6
t	netflow.protocol.keyword	TCP
#	netflow.retransmitted_in_pkts	2
#	netflow.retransmitted_out_pkts	2
#	netflow.server_nw_latency_ms	1

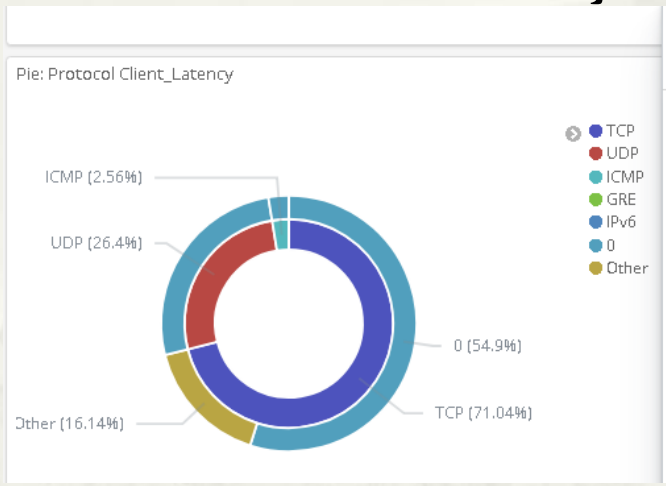
校內DNS 向其他 DNS 查詢

#	netflow.appl_latency_ms	158
#	netflow.client_nw_latency_ms	0
#	netflow.in_bits	576
#	netflow.in_bytes	72
#	netflow.in_pkts	1
#	netflow.input_snmp	50,727
💻	netflow.ipv4_cidr24_src_addr	140.112.254.0
💻	netflow.ipv4_dst_addr	199.7.91.13
💻	netflow.ipv4_src_addr	140.112.254.66
#	netflow.l4_dst_port	53
#	netflow.l4_src_port	58,349
t	netflow.l7_proto_name	DNS
#	netflow.max_ttl	0
#	netflow.min_ttl	0
#	netflow.ooorder_in_pkts	0
#	netflow.ooorder_out_pkts	0
#	netflow.output_snmp	1,655
#	netflow.protocol	17
t	netflow.protocol.keyword	UDP
#	netflow.retransmitted_in_pkts	0
#	netflow.retransmitted_out_pkts	0
#	netflow.server_nw_latency_ms	0

#	netflow.appl_latency_ms	129
#	netflow.client_nw_latency_ms	1
#	netflow.in_bits	2,696
#	netflow.in_bytes	337
#	netflow.in_pkts	5
#	netflow.input_snmp	8,738
💻	netflow.ipv4_cidr24_src_addr	140.112.254.0
💻	netflow.ipv4_dst_addr	192.33.14.30
💻	netflow.ipv4_src_addr	140.112.254.65
#	netflow.l4_dst_port	53
#	netflow.l4_src_port	45,191
t	netflow.l7_proto_name	DNS
#	netflow.max_ttl	60
#	netflow.min_ttl	60
#	netflow.ooorder_in_pkts	0
#	netflow.ooorder_out_pkts	0
#	netflow.output_snmp	58,665
#	netflow.protocol	6
t	netflow.protocol.keyword	TCP
#	netflow.retransmitted_in_pkts	0
#	netflow.retransmitted_out_pkts	0
#	netflow.server_nw_latency_ms	64

UDP 無 3-way handshake

* Client & Server Latency 皆為 0



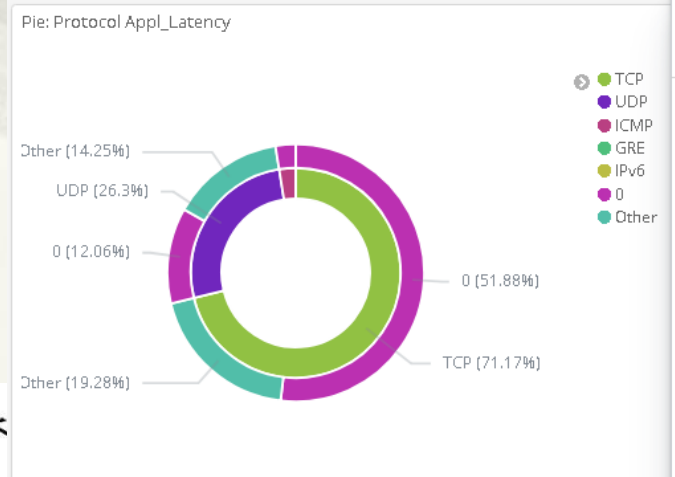
Pie: Protocol Client_Latency

View: Data

Download CSV

netflow.protocol.keywo...	Count	netflow.client_nw_laten...	Count
TCP	15,422,280	0	11,918,066
TCP	15,422,280	Other	3,503,951
UDP	5,730,242	0	5,730,242
ICMP	556,621	0	556,587
ICMP	556,621	Other	34
GRE	103	0	103
IPv6	86	0	86

* 但有 Application Latency



Pie: Protocol Appl_Latency

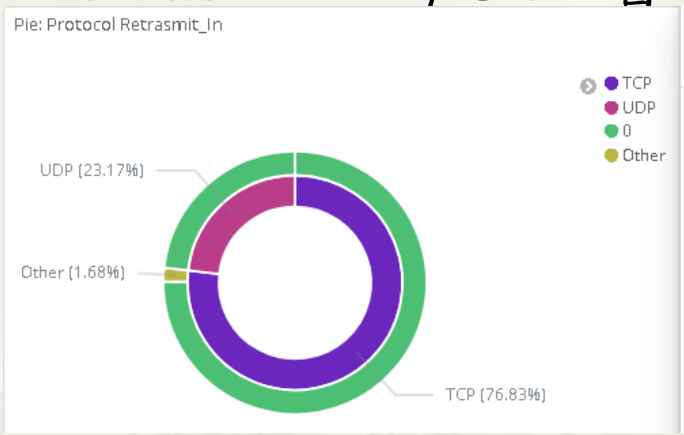
View: Data

Download CSV

netflow.protocol.keywo...	Count	netflow.appl_latency_m...	Count
TCP	15,557,043	0	11,340,878
TCP	15,557,043	Other	4,215,416
UDP	5,749,841	0	2,634,987
UDP	5,749,841	Other	3,114,190
ICMP	553,096	0	553,096
GRE	104	0	104
IPv6	83	0	83

UDP 無 Retrasmit & OutOfOrder

* Retrasmit In/Out 皆為 0



Pie: Protocol Retrasmit_In

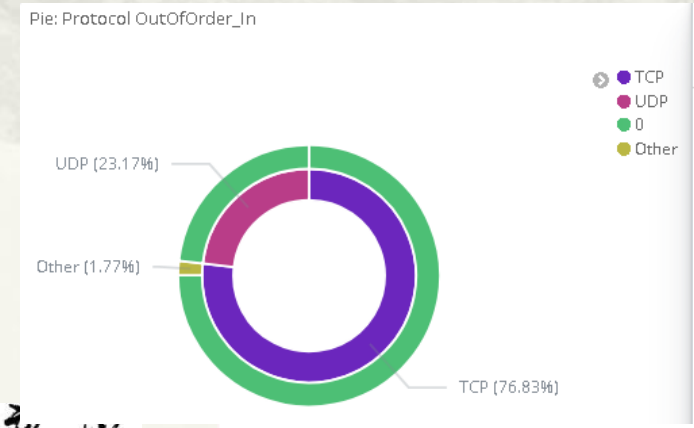
View: Data

Download CSV

netflow.protocol.keywo...	Count	netflow.retransmitted_i...	Count
TCP	66,249,037	0	64,803,086
TCP	66,249,037	Other	1,445,443
UDP	19,978,044	0	19,978,044

Rows per page: 20

* OutOfOrder In/Out 皆為 0



Pie: Protocol OutOfOrder_In

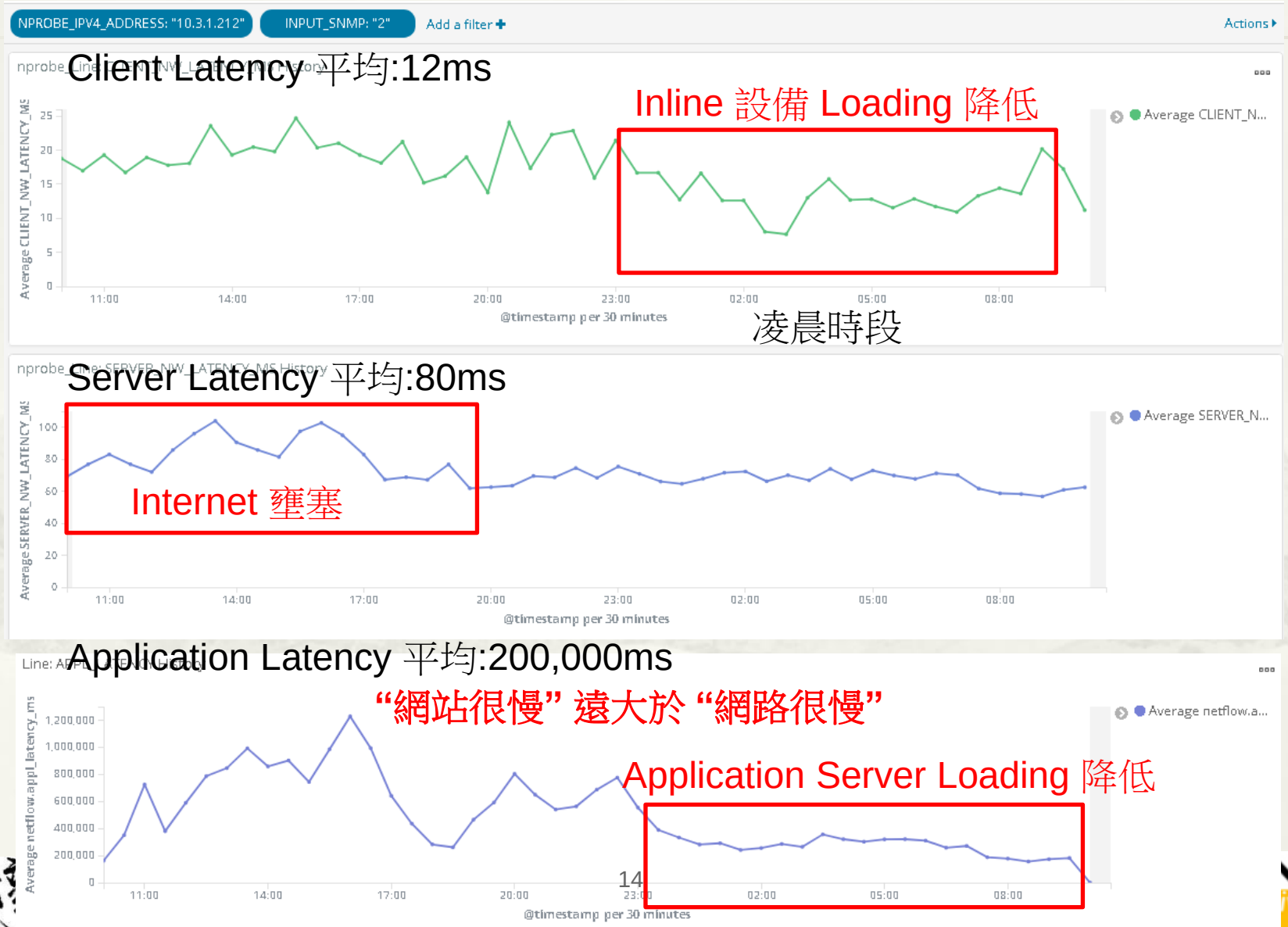
View: Data

Download CSV

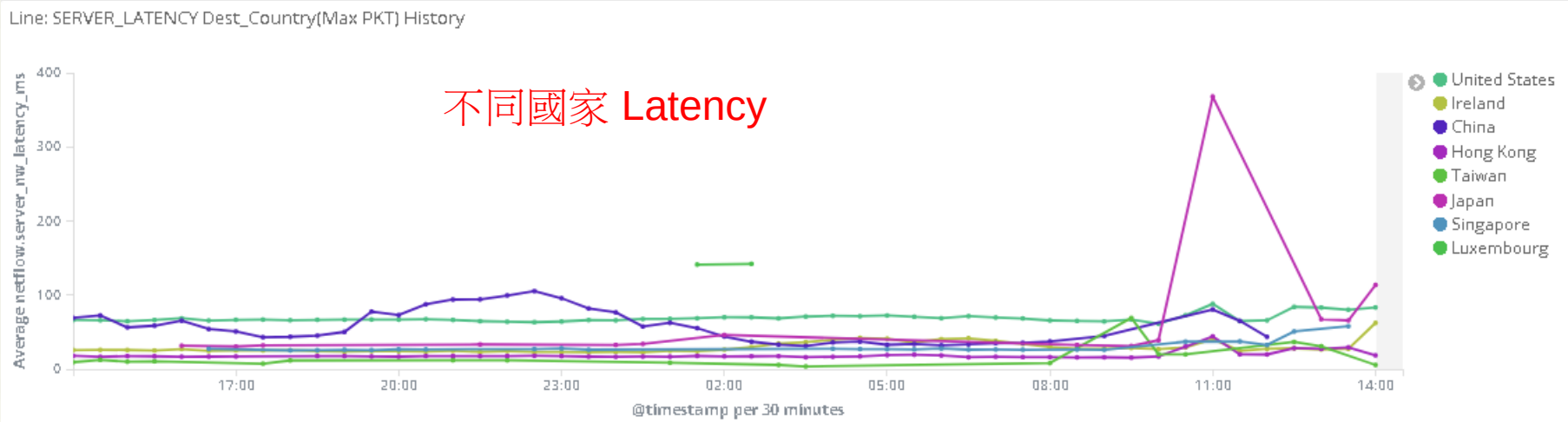
netflow.protocol.keywo...	Count	netflow.ooorder_in_pkts...	Count
TCP	66,249,037	0	64,718,376
TCP	66,249,037	Other	1,530,138
UDP	19,978,044	0	19,978,044

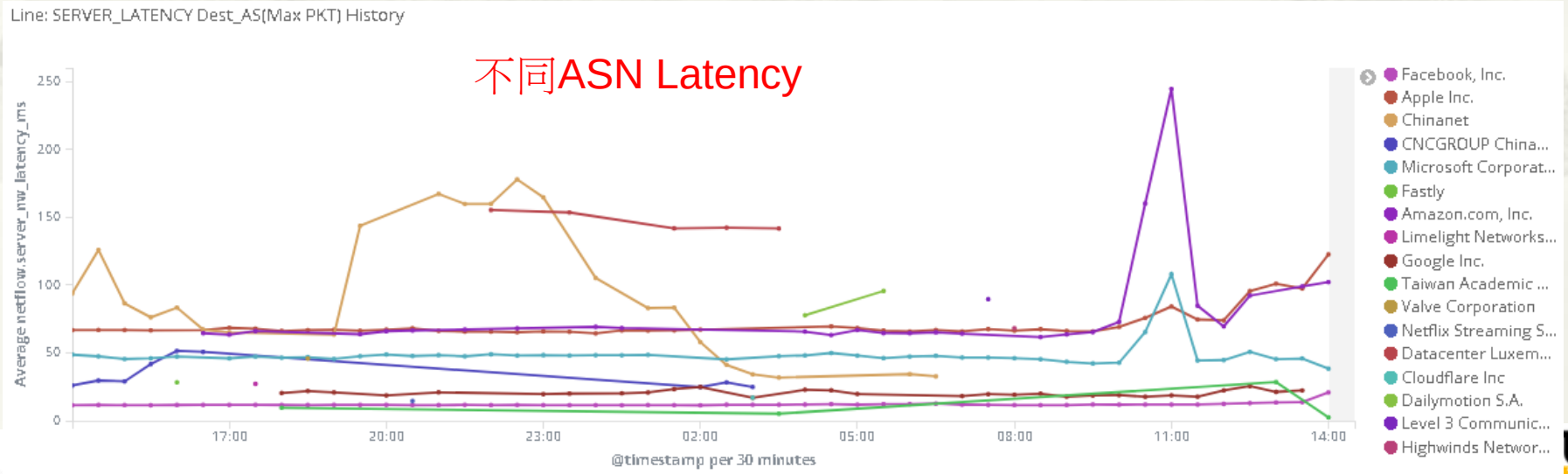
Rows per page: 20

Latency 24 Hrs 統計

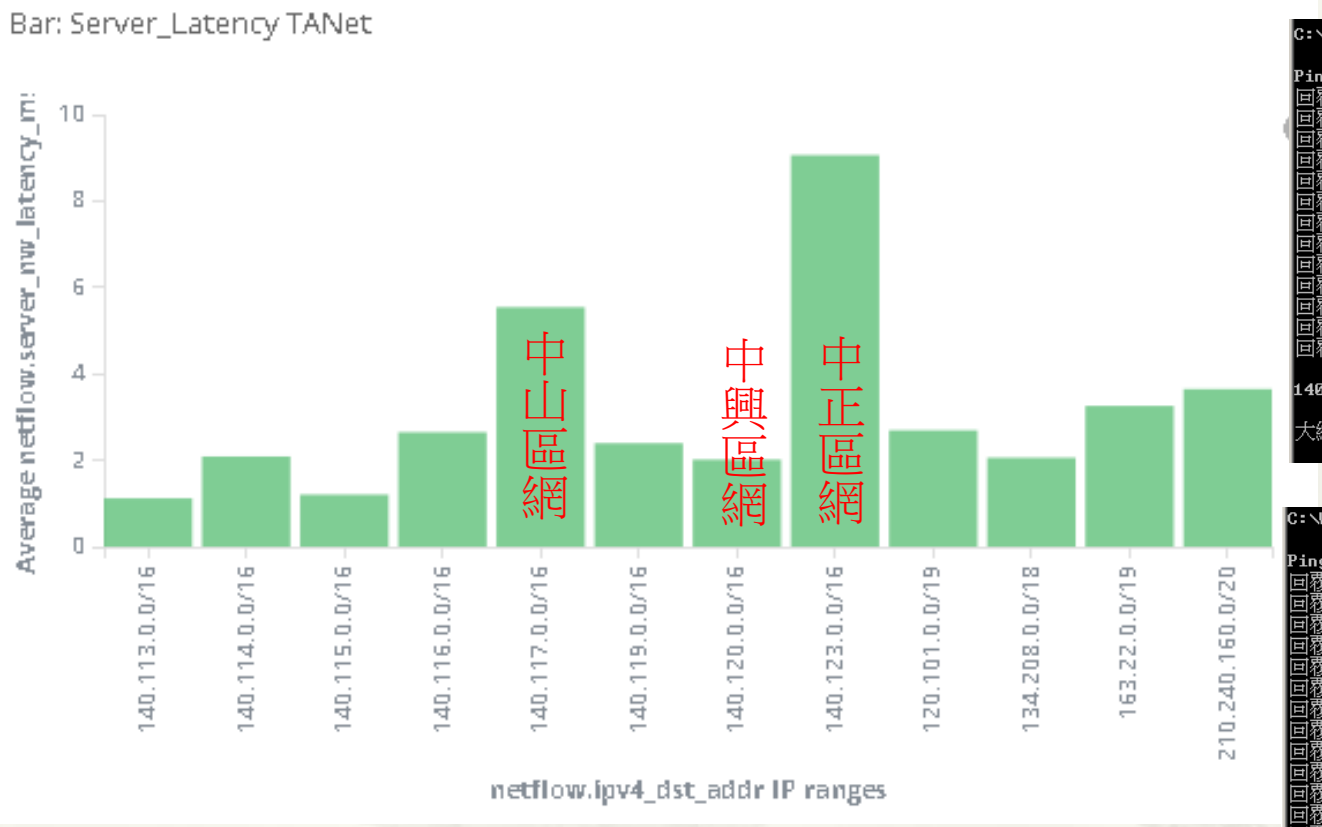


Latency 24 Hrs 統計
國家/ASN





Latency 24 Hrs 統計
各區網中心




```
C:\Windows\System32>ping www.ccu.edu.tw -t

Ping hero1.ccu.edu.tw [140.123.5.5] (使用 32 位元組的資料):
回覆自 140.123.5.5: 位元組=32 時間=33ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=9ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=8ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=8ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=32ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=7ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=8ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=42ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=11ms TTL=54
回覆自 140.123.5.5: 位元組=32 時間=29ms TTL=54

140.123.5.5 的 Ping 統計資料:
    封包: 已傳送 = 13，已收到 = 13，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 7ms，最大值 = 42ms，平均 = 16ms
```

中正大學

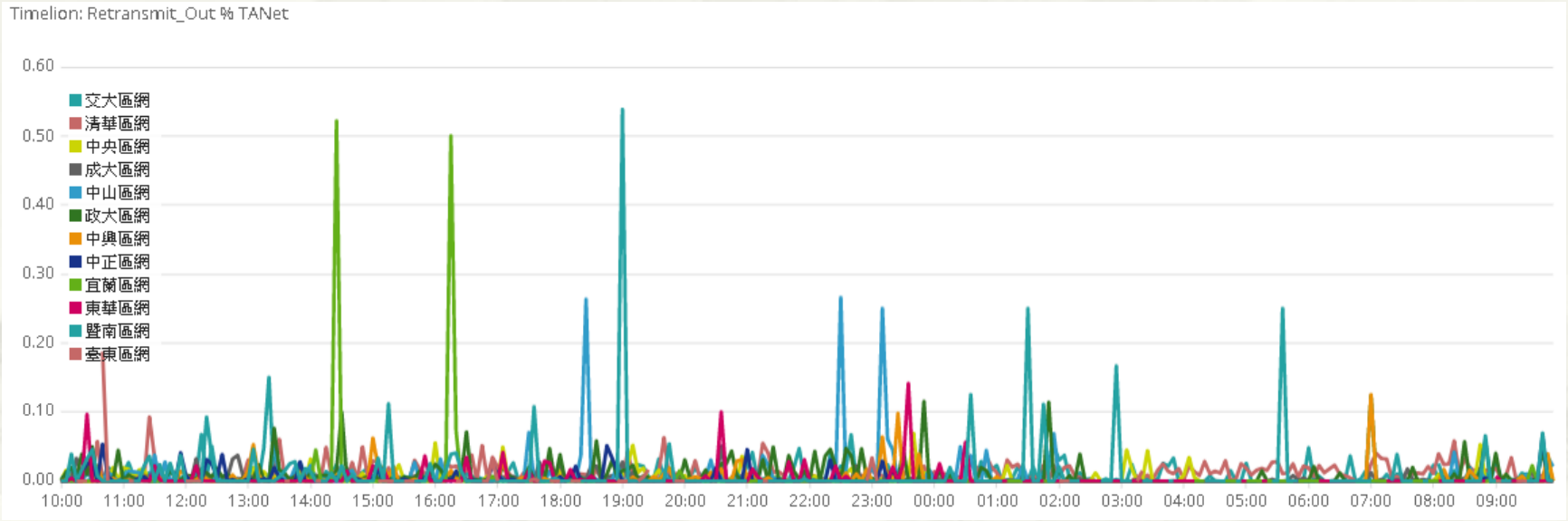
```
C:\Windows\System32>ping www.nchu.edu.tw -t

Ping www.nchu.edu.tw [140.120.1.20] (使用 32 位元組的資料):
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=4ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=4ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52
回覆自 140.120.1.20: 位元組=32 時間=5ms TTL=52

140.120.1.20 的 Ping 統計資料:
    封包: 已傳送 = 14，已收到 = 14，已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 4ms，最大值 = 5ms，平均 = 4ms
```

中興大學

封包重送 24 Hrs 統計 Retransmit

* 因國際頻寬壅塞 NTU Client 未依序收到封包，要求 Server 重送封包

Retransmit %比例 24 Hrs 統計
各區網中心



RTT、Packet Lost 分析

- 影響 RTT 高低
  - Inline 設備之有、無
  - Inline 設備之 Loading 高、低
  - 經過之 Node 節點數
  - 網路設備 Loading
- 影響 Packet Lost
  - 頻寬壅塞
  - 實體線路不良: 污損、接線不良
  - Server 異常: Loading 過高
  - Inline 設備(防火牆/IPS/頻寬管理器) Drop

簡報完畢
謝謝