# 106年度臺北區網Ⅰ
# 年度報告


- 單位：國立臺灣大學
- 計資中心主任：顏嗣鈞教授
- 網路組組長：謝宏昀教授
- 報告人：游子興
- Email：davisyou@ntu.edu.tw
- 電話：02-33665008

- 日期：2017/11/24

# 大綱

* 1.區網中心人力資源
* 2.網路中心運作
* 3.服務工作成效
* 4.資訊安全運作
* 5.網路應用服務特色
* 6.未來工作目標與建議

# 一、區網中心人力資源

* 計資中心主任：顏嗣鈞教授
  * E-mail：hcyen@ntu.edu.tw
  * 電話：(02) 33665001
* 網路組組長：謝宏昀教授
* 網路/資安管理負責人：游子興
  * E-mail：davisyou@mtu.edu.tw
  * 電話：(02) 33665008
* 編制內專職及約聘僱人員8名，其中區網經費及資安經費各約聘2名

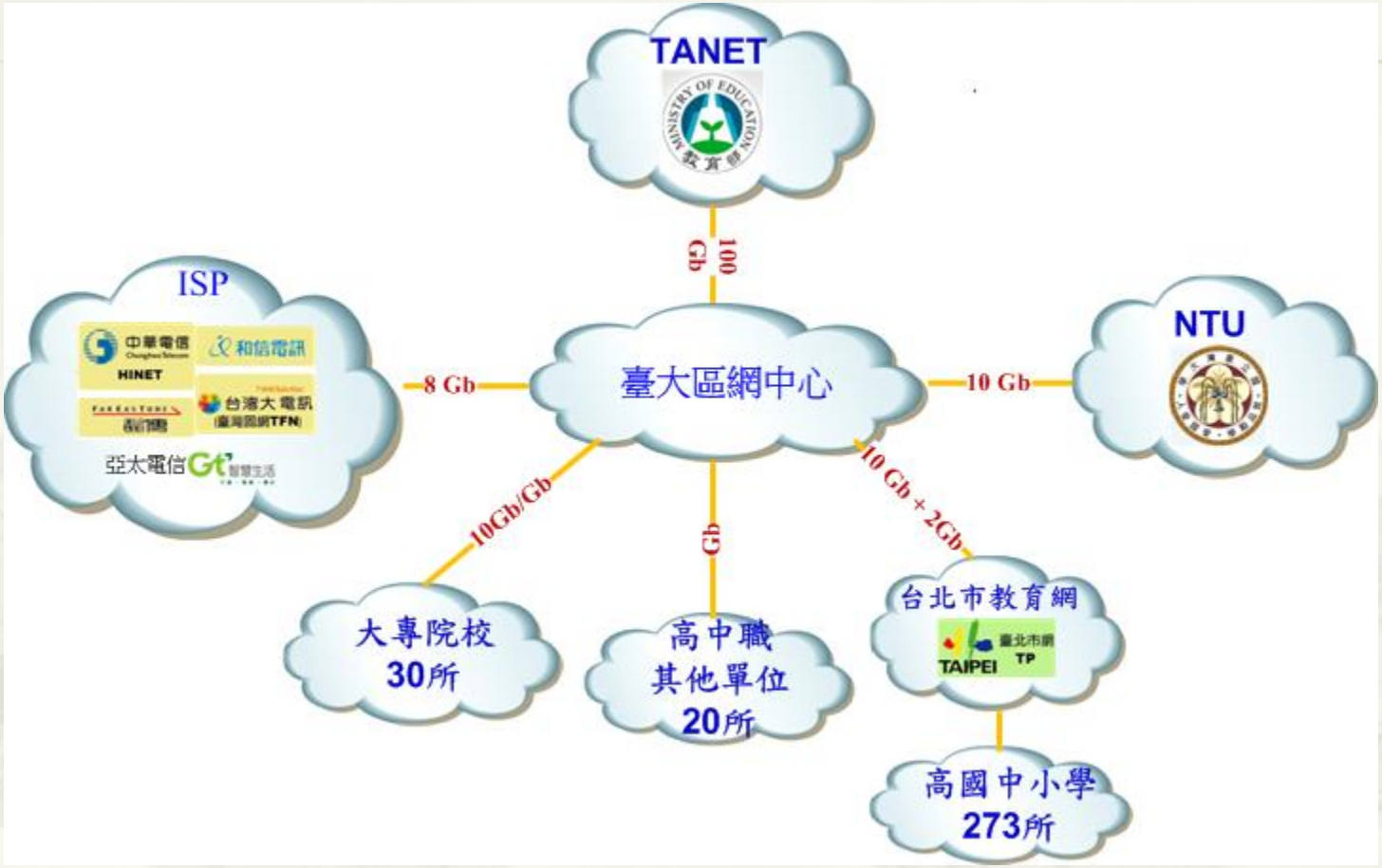
# 105年評審委員建議

| 改進意見 |
| --- |
| 1. 部分連線單位網路 ping packet loss 監控常態為 100%，建議續與連線單位溝通或變更監測方式。 |
| 2. 建議建置更多樣即時的網路監測機制給連線單位參考，讓連線單位能藉由區網中心提供之監測服務提升其維運品質。 |
| 3. 建議能有效整合校內龐大的學術資源，應能有效提升服務能量。 |
| 4. 資安事件平均審核時數達 3.43 小時，遠多於其他區網中心，是否有改善的空間? |
| 5. 資安事件量相當大，技術能力如何有效提升效能，以台大學術能量應是最有機會的單位，建議積極整合資源，並列為發展重點。 |

# 105年評審委員建議

6. 與縣市網之間應建立更有效的溝通方式。
7. 資安人力未能及時聘用，導致資安事件處理時效較久，建議爾後能盡速處理；亦或可借助與校內諸如 ISOC 等單位合作，協助解決相關問題。
8. 資安事件總量高，建議思考因應措施，協助連線單位處理。
9. 106 年重點工作僅著墨於 Traceroute 及 Netflow Based 等之推廣與改善，建議強化與連線單位之溝通協調，並協助其解決 DNS 版本老舊、IPv6 及 VoIP 等之建置，頻寬擴增等等業務。

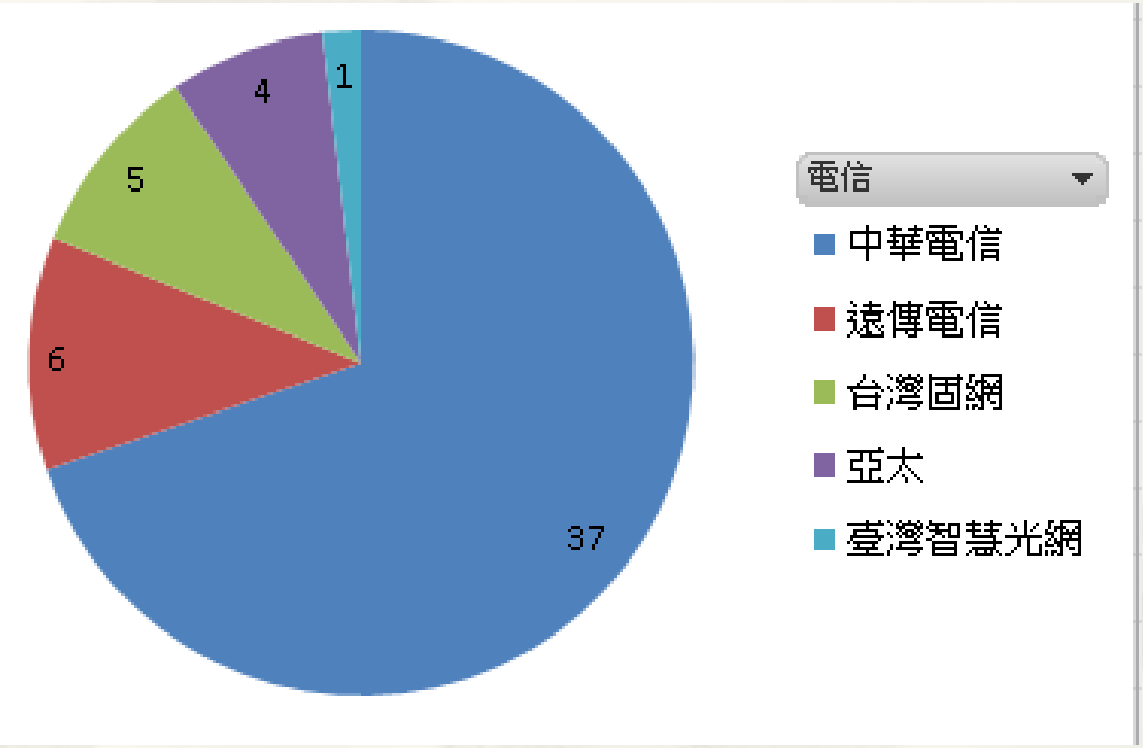
# 二、網路中心運作




* 新增連線單位: 臺灣科技大學
* 共計52個連線單位

# ISP 線路統計

| 列標籤 | 計數 - 電信 |
|---|---|
| 中華電信 | 37 |
| 遠傳電信 | 6 |
| 台灣固網 | 5 |
| 亞太 | 4 |
| 臺灣智慧光網 | 1 |
| **總計** | **53** |



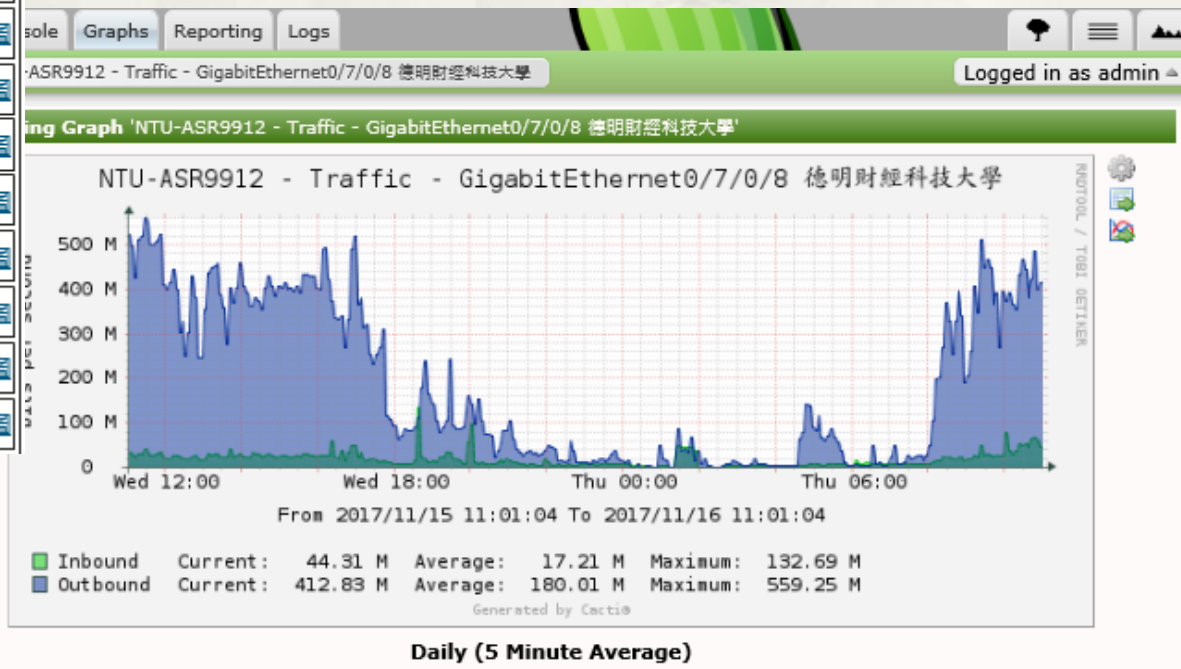
# 建置多樣即時監控機制

* 增加 Cacti 監控方式
  * 流量圖、封包量圖、介面異常統計

105年評審委員建議: 第 2 點 建置多樣即時監控機制

Cacti 流量分析

| 大專院校 | | | |
|---|---|---|---|
| 德明財經科技大學 | 流量圖 | 封包量圖 | 介面異常圖 |
| 宏國德霖科技大學 | 流量圖 | 封包量圖 | 介面異常圖 |
| 華夏科技大學 | 流量圖 | 封包量圖 | 介面異常圖 |
| 臺灣師範大學(公館校區)-2 | 流量圖 | 封包量圖 | 介面異常圖 |
| 臺灣師範大學(公館校區)-1 | 流量圖 | 封包量圖 | 介面異常圖 |
| 國防大學管理學院 | 流量圖 | 封包量圖 | 介面異常圖 |
| 臺北藝術大學 | 流量圖 | 封包量圖 | 介面異常圖 |
| 臺北商業大學 | 流量圖 | 封包量圖 | 介面異常圖 |
| 台北護理健康大學 | 流量圖 | 封包量圖 | 介面異常圖 |



# 建置事件通知警示系統

* 監控 ASR Router Log 相關事件

| Alert Name** | Severity | Method | Threshold Count | Enabled | Match Type | Search String |
|---|---|---|---|---|---|---|
| Alert-AUTHEN_SUCCESS | Warning | Individual | N/A | Yes | Contains | AUTHEN_SUCCESS |
| Alert-LINEPROTO-5-UPDOWN | Warning | Individual | N/A | Yes | Contains | LINEPROTO-5-UPDOWN |
| Alert-LINK-3-UPDOWN | Warning | Individual | N/A | Yes | Contains | LINK-3-UPDOWN |
| Alert-LOGIN_SUCCESS | Warning | Individual | N/A | Yes | Contains | LOGIN_SUCCESS |
| logged command | Warning | Individual | N/A | Yes | Contains | logged command |
| OSPF-5-ADJCHG | Warning | Individual | N/A | Yes | Contains | OSPF-5-ADJCHG |
| OSPFv3-5-ADJCHG(ipv6) | Warning | Individual | N/A | Yes | Contains | OSPFv3-5-ADJCHG |

寄件者: Cacti <Cacti@cactiusers.org>
寄件日期: 2017/11/16 (週四) 下午 09:26
收件者: 游子興
副本:
主旨: Event Alert - Alert-AUTHEN_SUCCESS

事件發生立即 email 通知
例如: 有人登入 Router

---

Hostname : 163.28.16.254
Date : 2017-11-16 21:25:16
Severity : Warning

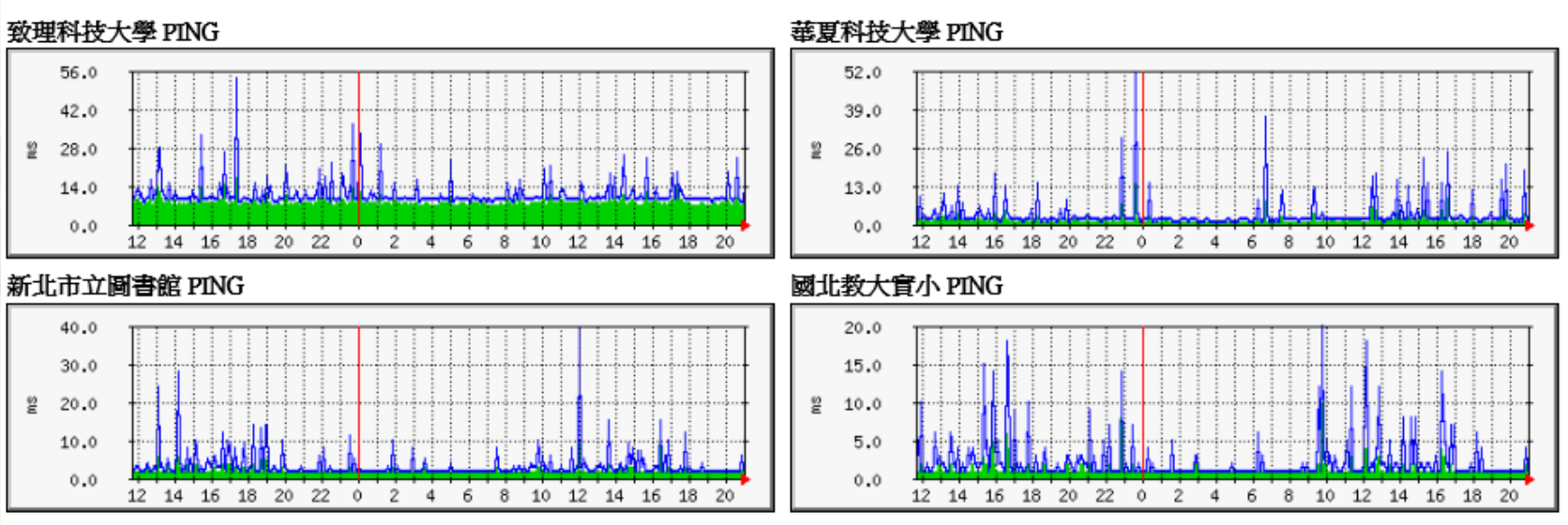
Priority : 6

Message :
RP/0/RP0/CPU0:Nov 16 21:25:16.045 : exec[65944]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'ntuadmin1' from '192.168.214.133' on 'vty4'

# 改善連線單位 Ping 統計資訊

- 今年度已完成所有大專院校 peer ip 之 Ping RTT、Packet Lost % 統計資訊
- 高中職以下受限設備與網管技術仍待完成

105年評審委員建議: 第 1 點改善連線單位 ping packet lost% ..

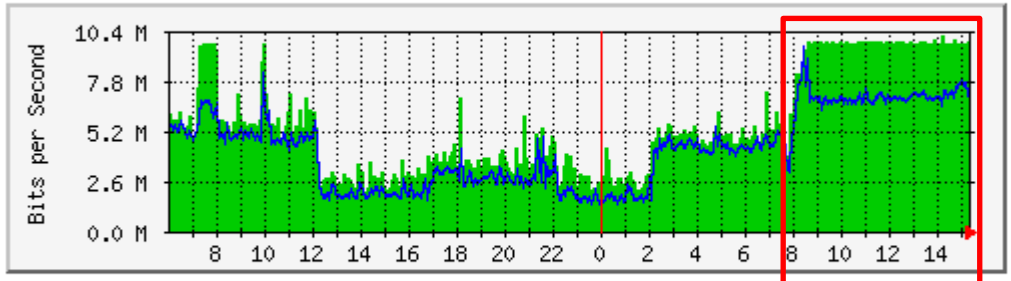


# 連線單位技術支援 案例一

* **案例一: 法鼓文理學院 流量異常**

105年評審委員建議: 第 9 點 強化連線單位溝通協調

每日 圖表 (5 分鐘 平均)




| | 最大 | 平均 | 目前 |
|---|---|---|---|
| 法鼓文理學院 => 北區區網: | 10.1 Mb/秒 (0.0%) | 5414.2 kb/秒 (0.0%) | 9798.9 kb/秒 (0.0%) |
| 北區區網 => 法鼓文理學院: | 9521.8 kb/秒 (0.0%) | 4221.4 kb/秒 (0.0%) | 6668.8 kb/秒 (0.0%) |

# 連線單位技術支援 案例一

udp.stream eq 1

| No. | tcp.stream | Time | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | | 0.000227 | 119 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 6 | | 0.000232 | 118 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 56 | | 0.004381 | 117 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 57 | | 0.004385 | 116 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 107 | | 0.008542 | 115 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 108 | | 0.008549 | 114 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 160 | | 0.012716 | 113 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 161 | | 0.012722 | 112 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 213 | | 0.016850 | 111 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 214 | | 0.016861 | 110 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 269 | | 0.021023 | 109 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 270 | | 0.021034 | 108 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 325 | | 0.025131 | 107 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 326 | | 0.025139 | 106 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 380 | | 0.029328 | 105 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 381 | | 0.029339 | 104 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 438 | | 0.033502 | 103 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |
| 439 | | 0.033513 | 102 | 218.60.112.227 | 53 | 120.97.248.154 | 59230 | DNS | 174 | Standard query response 0x99f8 A |

* 原以為是 DNS 放大攻擊
* 觀察 TTL 持續遞減 -> Routing Loop
* 因法鼓學院原有兩個校區使用不同網段:
  * 140.131.254.0/23 (金山校區)
  * 120.97.248.0/21 (城區推廣中心) -> 合併取消
* 合併後校內路由未同步修正

# 連線單位技術支援 案例二

* 臺北酷課雲使用區網雲端服務，2017/6 月反應認證連線緩慢，進行封包分析
  * SSO 收到 Client 多次 SYN 卻不回應 SYN/ACK，Client TCP Session 建立六次未成功
  * 最終原因： 市網 IPS 誤擋造成

105年評審委員建議: 第 6 點 與市網更有效溝通

ip.addr==163.28.17.2

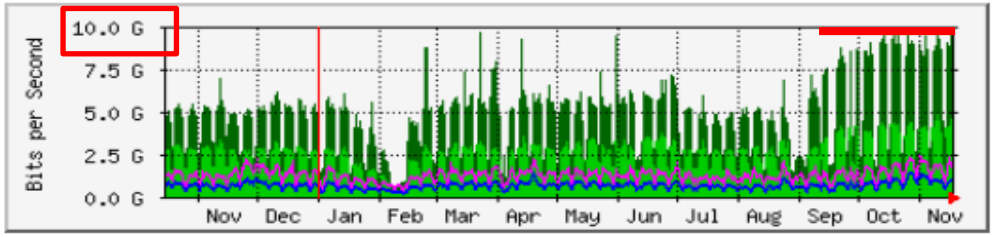
| No. | Time | Vlan | TTL | Source | Src Port | Destination | Dest Port | Src MAC | Dst MAC | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7085 | 103.258302 | | 60 | 163.28.17.2 | 11622 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7333 | 107.258298 | | 60 | 163.28.17.2 | 11622 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7507 | 114.615333 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | 12868 → 443 [SYN] Seq... |
| 7521 | 115.258194 | | 60 | 163.28.17.2 | 11622 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7531 | 115.614261 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7616 | 117.614257 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7751 | 121.614330 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 74 | [TCP Retransmission] ... |
| 7752 | 121.614365 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | TCP | 74 | 443 → 12868 [SYN, ACK... |
| 7753 | 121.615442 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 66 | 12868 → 443 [ACK] Seq... |
| 7754 | 121.616967 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TLSv1 | 242 | Client Hello |
| 7755 | 121.616995 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | TCP | 66 | 443 → 12868 [ACK] Seq... |
| 7756 | 121.627678 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | SSL | 2962 | |
| 7757 | 121.627822 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | TLSv1 | 1514 | Ignored Unknown Record |
| 7758 | 121.627873 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | TLSv1 | 886 | Ignored Unknown Record |
| 7759 | 121.630157 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 66 | 12868 → 443 [ACK] Seq... |
| 7760 | 121.630184 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 66 | 12868 → 443 [ACK] Seq... |
| 7761 | 121.630193 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 66 | 12868 → 443 [ACK] Seq... |
| 7762 | 121.631440 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TCP | 66 | 12868 → 443 [ACK] Seq... |
| 7764 | 121.634368 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TLSv1 | 141 | Client Key Exchange |
| 7765 | 121.637063 | | 60 | 163.28.17.2 | 12868 | 163.21.158.135 | 443 | aa:bb:cc:dd:ee:ff | Vmware_b4:59:29 | TLSv1 | 72 | Change Cipher Spec |
| 7766 | 121.637232 | | 64 | 163.21.158.135 | 443 | 163.28.17.2 | 12868 | Vmware_b4:59:29 | aa:bb:cc:dd:ee:ff | TCP | 66 | 443 → 12868 [ACK] Seq... |

# 三、服務工作成效

* 頻寬用量顯著增加

每年 圖表 (1 天 平均)

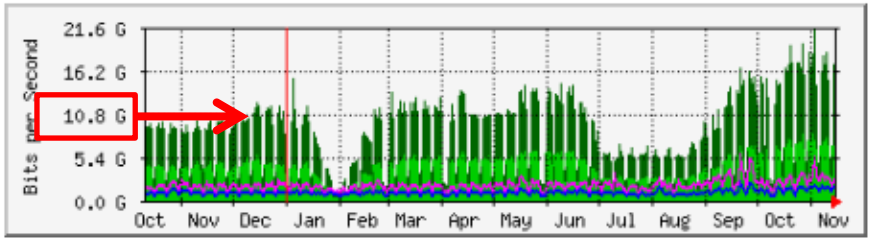
2016




| | 最大 | 平均 | 目前 |
|---|---|---|---|
| InterNet => 北區區網 | 9970.6 Mb/秒 (99.7%) | 2387.7 Mb/秒 (23.9%) | 4790.9 Mb/秒 (47.9%) |
| 北區區網 => InterNet | 2442.8 Mb/秒 (24.4%) | 625.8 Mb/秒 (6.3%) | 963.3 Mb/秒 (9.6%) |

每年 圖表 (1 天 平均)

2017

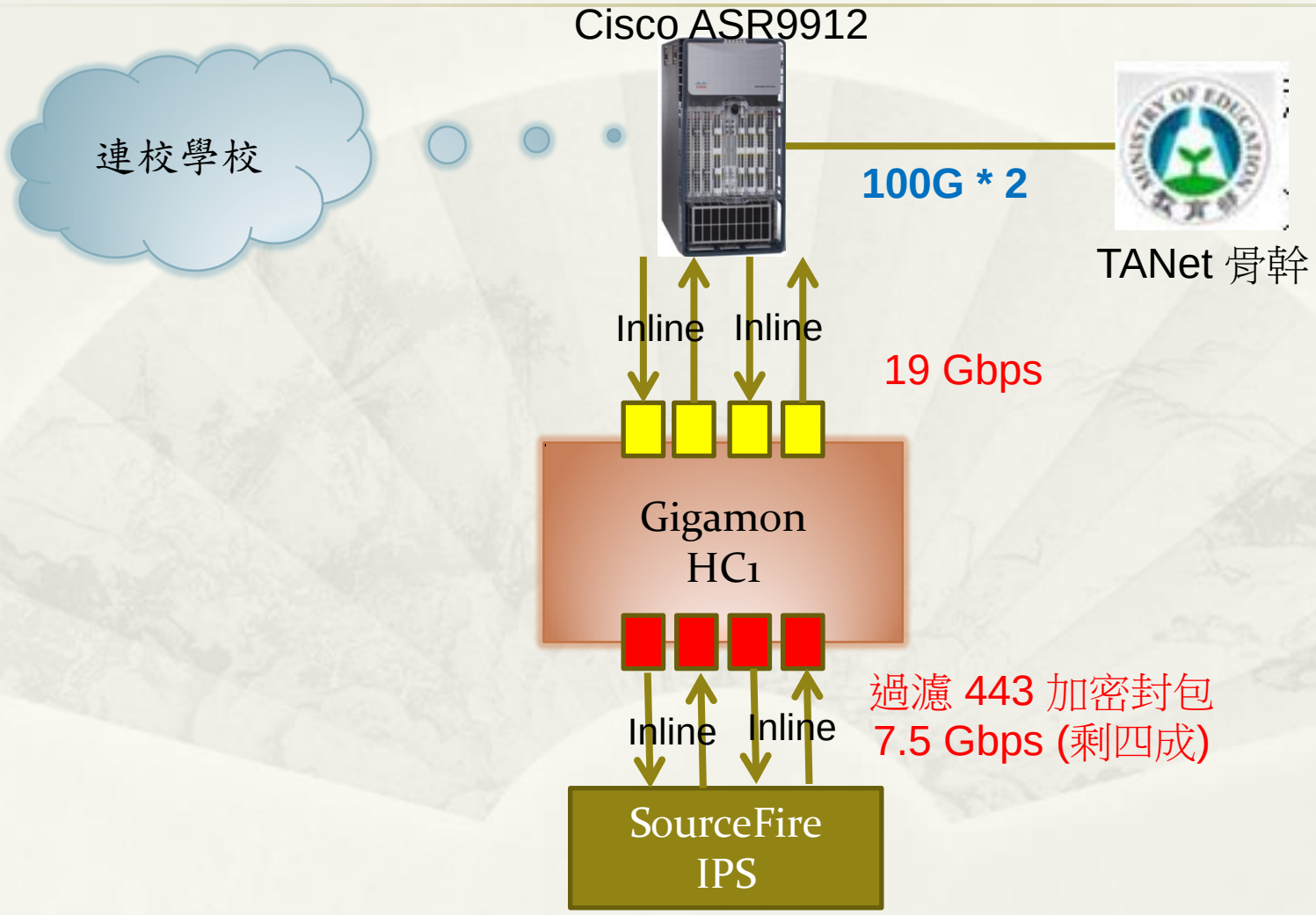



| | 最大 | 平均 | 目前 |
|---|---|---|---|
| InterNet => 北區區網 | 21.3 Gb/秒 (21.3%) | 3626.6 Mb/秒 (3.6%) | 7928.1 Mb/秒 (7.9%) |
| 北區區網 => InterNet | 5800.8 Mb/秒 (5.8%) | 946.6 Mb/秒 (0.9%) | 1579.9 Mb/秒 (1.6%) |

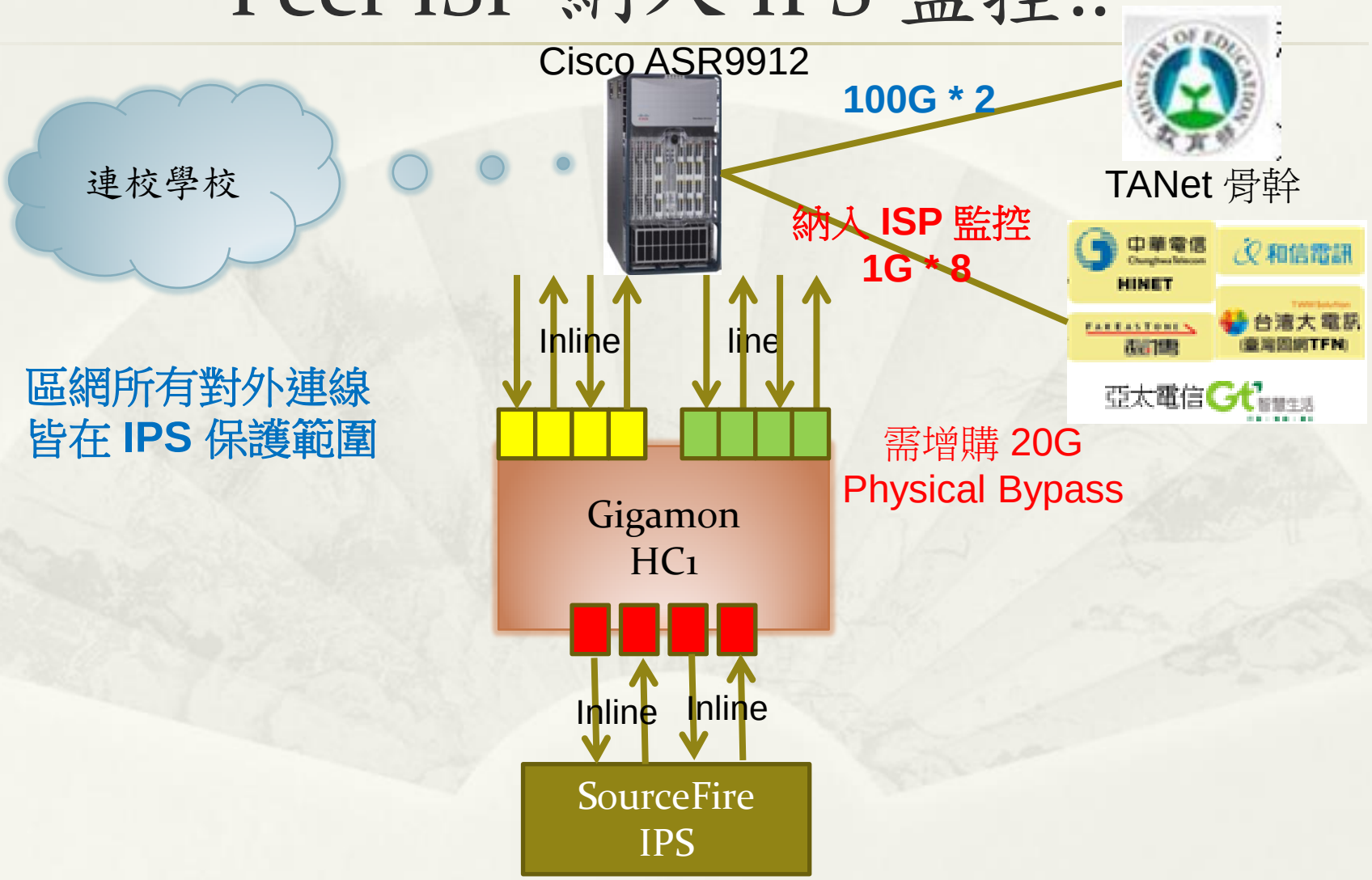
* 10Gb頻寬連線單位
  * 臺北市網、臺大、北科大、臺科大
* 現有資安設備 Capability 不足
  * IPS Capability: Max 15 Gbps

| | 2016 | 2017 | 增加% |
|---|---|---|---|
| 最大 | 9.9G | 21.3G | 110% |
| 平均 | 2.3G | 3.6G | 56% |

# 建置頻寬分流器
# 解決 IPS Capability 不足



# 下年度預計進行 Peer ISP 納入 IPS 監控..



# 四、資訊安全運作

* 通過教育版資訊安全管理制度(ISMS)認證
  * 為建立完善之資訊安全管理制度，降低組織內的重要資產與資訊之風險，台北區網中心於97年開始導入教育版ISMS制度
  * 98年至106年每年皆通過教育版ISMS 第三方認證
* 107年度開始全計資中心導入 ISO27001-2013

# 資安事件統計

| | 105 | 106 |
|---|---|---|
| 1、2級資安事件處理 | | |
| 通報平均時數 | 1.97小時 | 2.70小時 |
| 應變處理平均時數 | 0.22小時 | 0.05小時 |
| 事件處理平均時數 | 2.19小時 | 2.76小時 |
| 通報完成率 | 99.37% | 98.90% |
| 事件完成率 | 99.83% | 99.91% |
| 3、4級資安事件通報 | 無 | 無 |
| 資安事件通報審核平均時數 | 3.43小時 | 0.60小時 |
| 全年事件量統計 | 6930 | 4264 |

105年評審委員建議:

第 4 點 改善資安審核時數

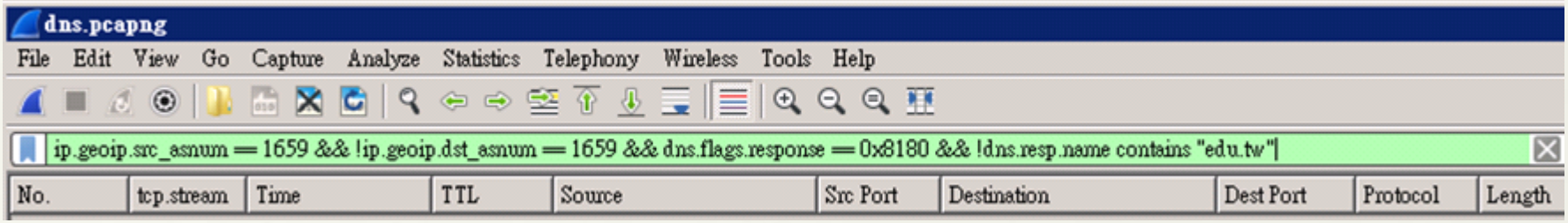
第 5 點 資安事件量龐大

# 偵測 DNS 放大攻擊之幫兇

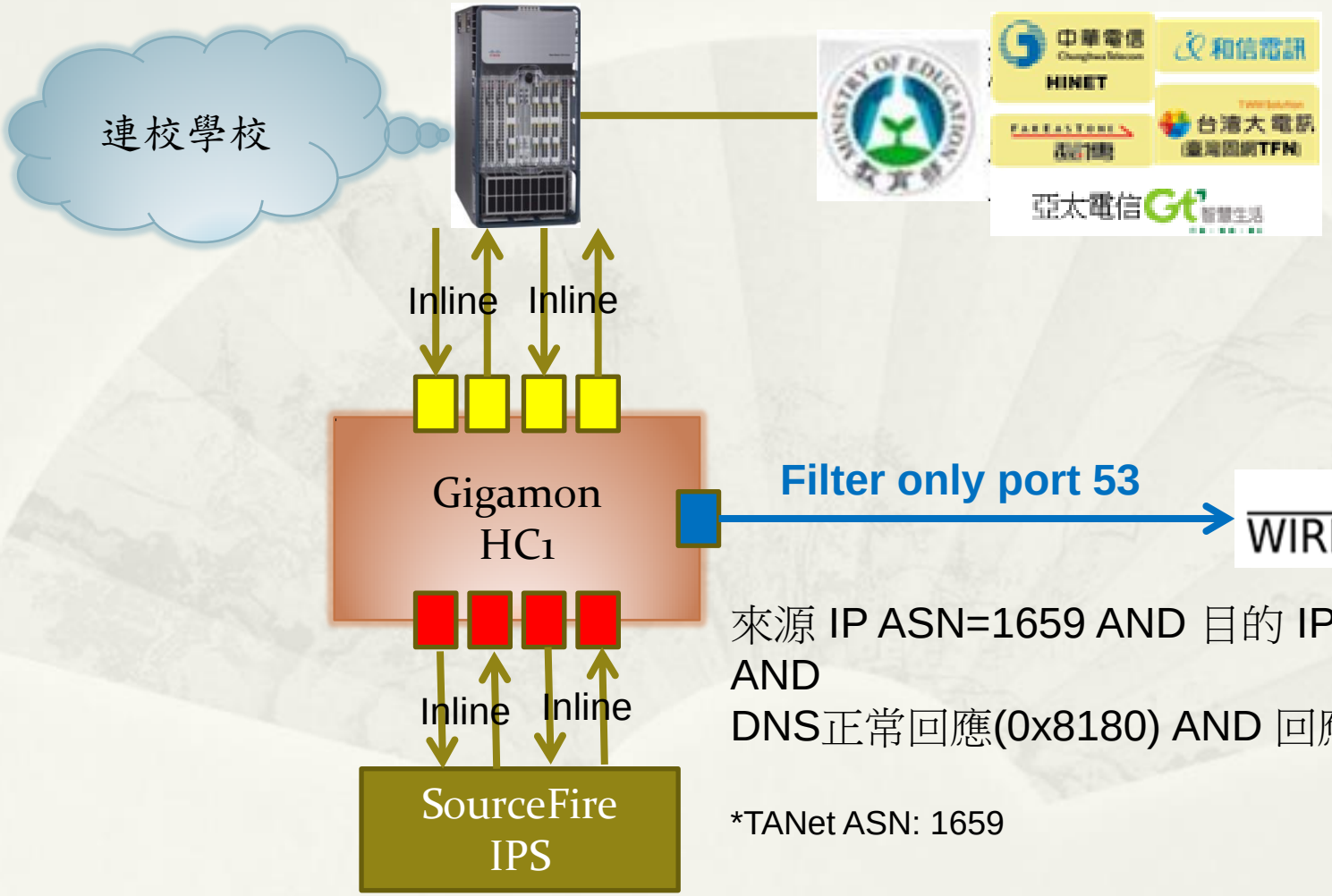
* 不正確之 DNS 設置變成 Open Resolver DNS，成為 DNS 放大攻擊之幫兇 105年評審委員建議: 第 9 點 協助解決 DNS老舊…
* 屬於正常連線封包，IPS 無法用特徵碼偵測
* 偵測連線單位是否有允許回覆來自 Internet IP 詢問非 .edu.tw 結尾之 DNS Query 連線記錄

Wireshark Display Filter:

ip.geoip.src_asnum == 1659 && !ip.geoip.dst_asnum == 1659 && dns.flags.response == 0x8180 && !dns.resp.name contains "edu.tw"



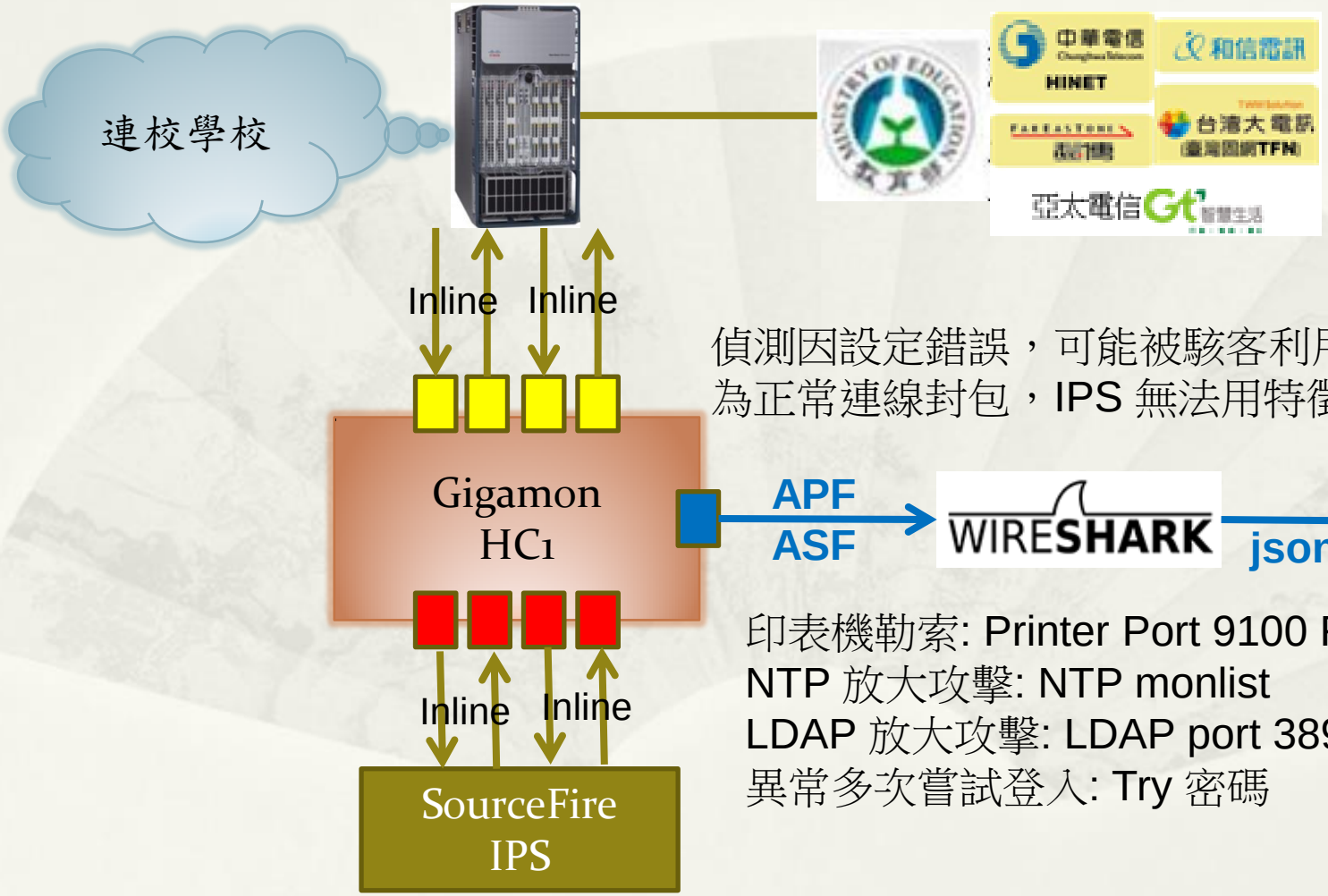
# Open Resolver DNS 偵測




來源 IP ASN=1659 AND 目的 IP ASN<>1659
AND
DNS正常回應(0x8180) AND 回應非 edu.tw 結尾

*TANet ASN: 1659

# 下年度計畫
# 偵測其他異常連線




偵測因設定錯誤，可能被駭客利用之網路服務為正常連線封包，IPS 無法用特徵碼偵測

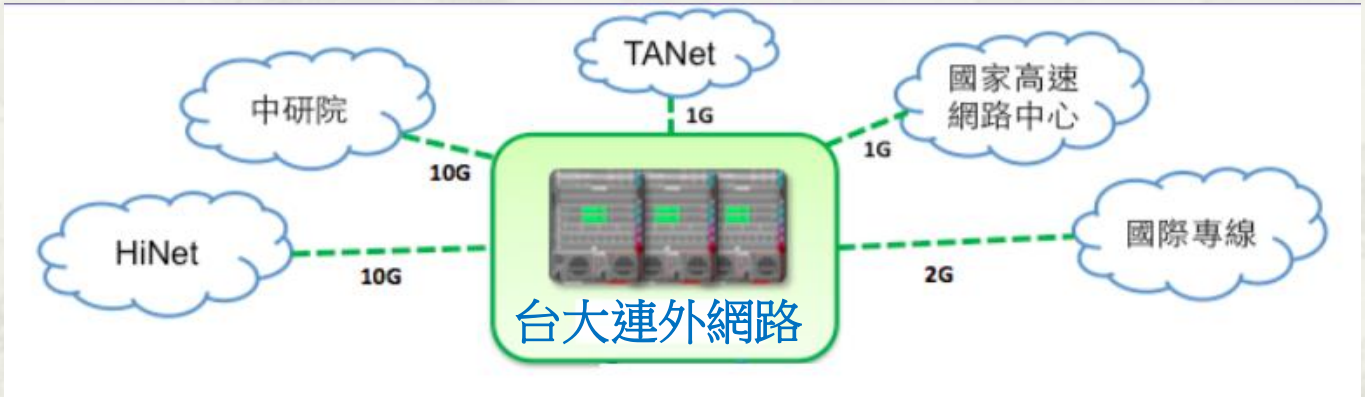
印表機勒索: Printer Port 9100 RAW
NTP 放大攻擊: NTP monlist
LDAP 放大攻擊: LDAP port 389
異常多次嘗試登入: Try 密碼

# 五、網路應用服務特色

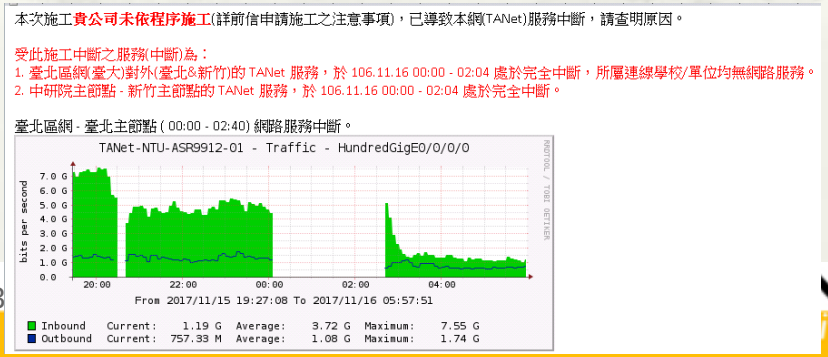
* 臺大區網網頁備援建置
* 網路行為異常偵測
* Layer 7 網路行為分析

# 臺大區網網頁備援建置

- 臺大連外網路為 Multi-Home 架構
- 建構TANet與臺大網路互為備援之區網網頁
  - TANet 斷線時仍可由臺大網路在網頁公告事項



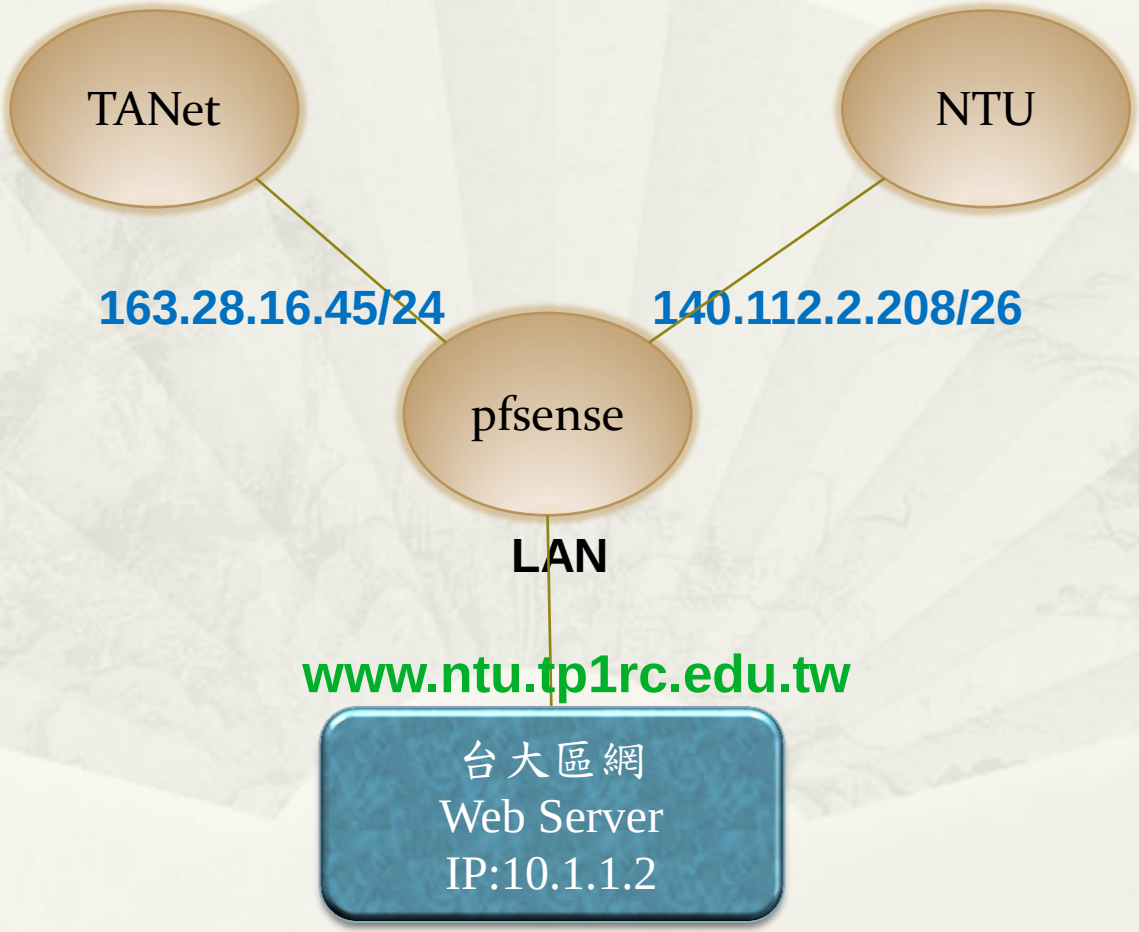

11/16 凌晨區網斷線近 3小時


本次施工**貴公司未依程序施工**(詳前信申請施工之注意事項)，已導致本網(TANet)服務中斷，請查明原因。

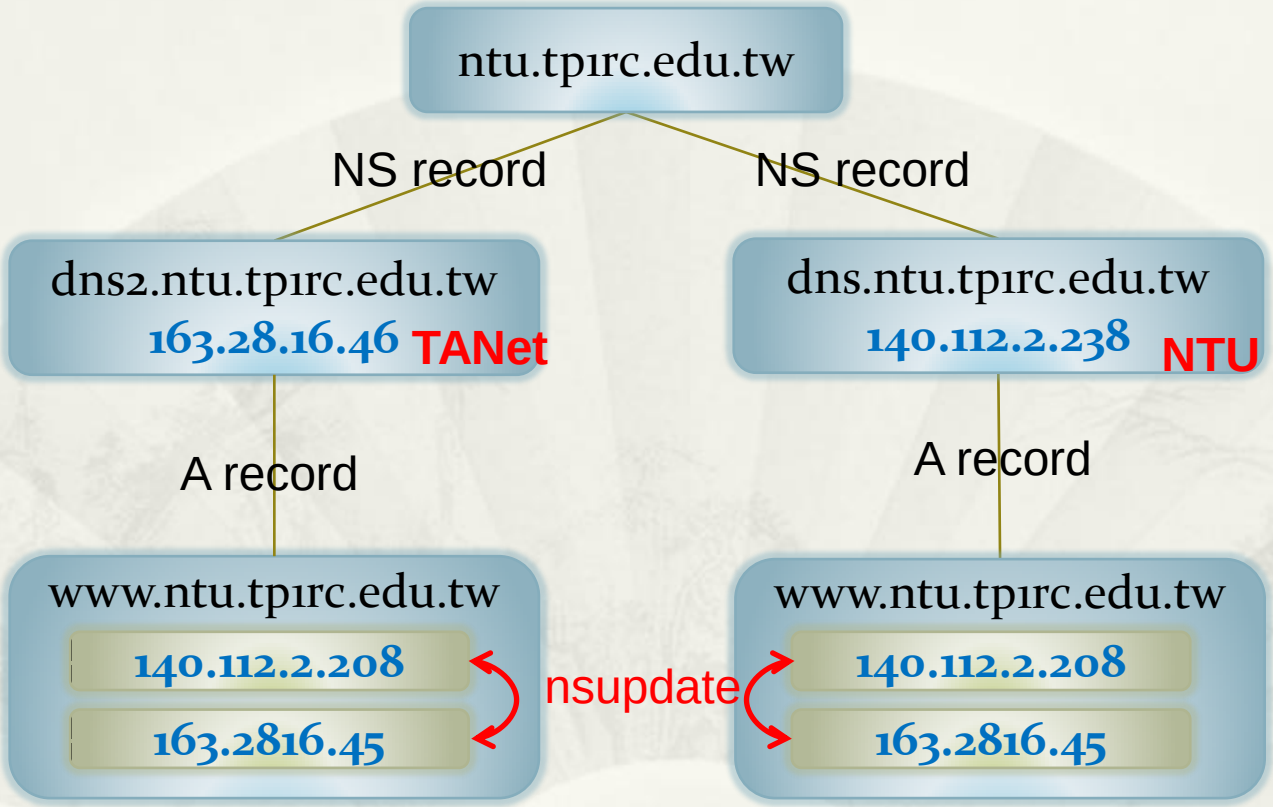
受此施工中斷之服務(中斷)為：
1. 臺北區網(臺大)對外(臺北&新竹)的 TANet 服務，於 106.11.16 00:00 - 02:04 處於完全中斷，所屬連線學校/單位均無網路服務。
2. 中研院主節點 - 新竹主節點的 TANet 服務，於 106.11.16 00:00 - 02:04 處於完全中斷。

臺北區網 - 臺北主節點 ( 00:00 - 02:40) 網路服務中斷。

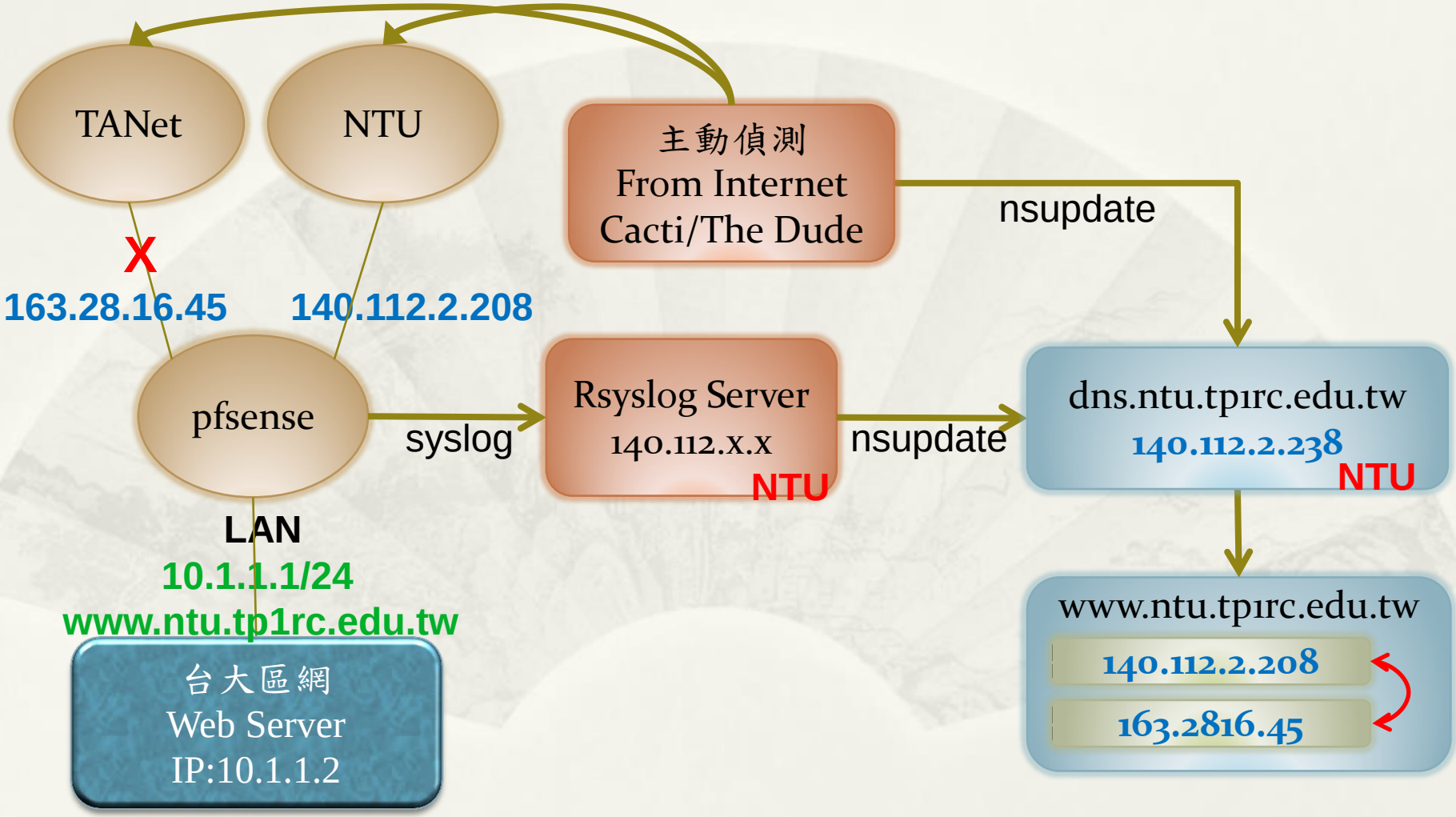
# 網頁備援運作架構


TANet
NTU
163.28.16.45/24
140.112.2.208/26
pfsense
LAN
www.ntu.tp1rc.edu.tw
台大區網
Web Server
IP:10.1.1.2

# DNS 備援設置


ntu.tp1rc.edu.tw
NS record
NS record
dns2.ntu.tp1rc.edu.tw
163.28.16.46 TANet
dns.ntu.tp1rc.edu.tw
140.112.2.238 NTU
A record
A record
www.ntu.tp1rc.edu.tw
140.112.2.208
163.2816.45
nsupdate
www.ntu.tp1rc.edu.tw
140.112.2.208
163.2816.45

# 網頁備援運作架構


TANet
NTU
主動偵測
From Internet
Cacti/The Dude
nsupdate
X
163.28.16.45
140.112.2.208
pfsense
syslog
Rsyslog Server
140.112.x.x
NTU
nsupdate
dns.ntu.tp1rc.edu.tw
140.112.2.238
NTU
LAN
10.1.1.1/24
www.ntu.tp1rc.edu.tw
www.ntu.tp1rc.edu.tw
140.112.2.208
163.2816.45
台大區網
Web Server
IP:10.1.1.2

# TANet 與臺大網路正常

Status / Gateways / Gateways

Gateways | Gateway Groups

**Gateways**

| Name | Gateway | Monitor | RTT | RTTsd | Loss | Status |
|---|---|---|---|---|---|---|
| NTUGW | 140.112.2.254 | 140.112.2.254 | 0.785ms | 0.921ms | 0.0% | Online |
| TANETGW | 163.28.16.254 | 163.28.16.254 | 0.874ms | 0.823ms | 0.0% | Online |

Status / Gateways / Gateway Groups

Gateways | Gateway Groups

**Gateway Groups**

| Group Name | Gateways | |
|---|---|---|
| | Tier 1 | Tier 2 |
| GW_GROUP | NTUGW Online | |
| | | TANETGW Online |

# TANet 網路異常

Status / Gateways / Gateways

Gateways | Gateway Groups

**Gateways**

| Name | Gateway | Monitor | RTT | RTTsd | Loss | Status |
|---|---|---|---|---|---|---|
| NTUGW | 140.112.2.254 | 140.112.2.254 | 1.027ms | 1.323ms | 0.0% | Online |
| TANETGW | 163.28.16.254 | 163.28.16.254 | 0ms | 0ms | 100% | Offline |

Status / Gateways / Gateway Groups

Gateways | Gateway Groups

**Gateway Groups**

| Group Name | Gateways | |
|---|---|---|
| | Tier 1 | Tier 2 |
| GW_GROUP | NTUGW Online | |
| | | TANETGW Offline |

# TANet 網路異常與恢復過程

Status / System Logs / System / General

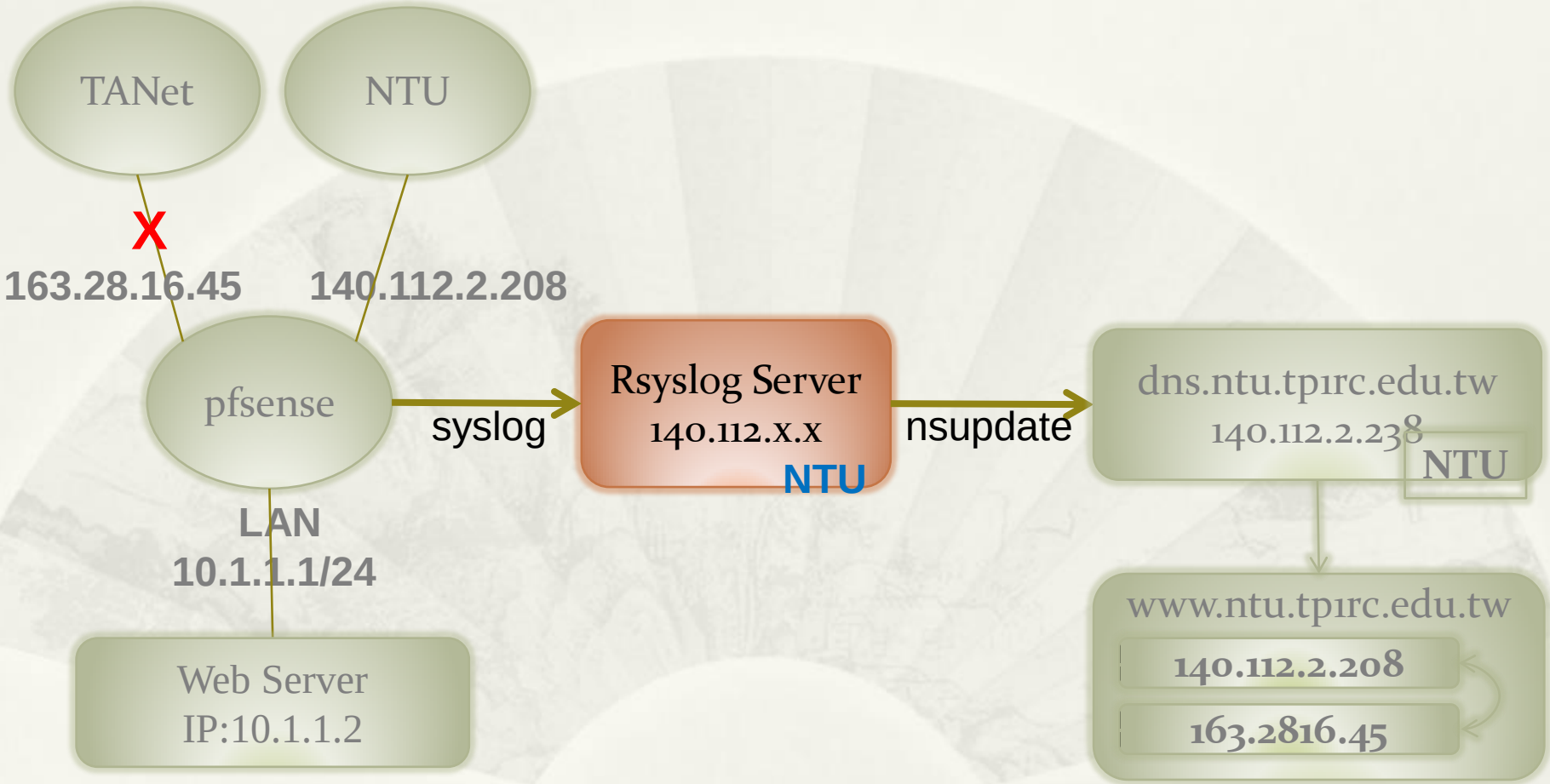
System | Firewall | DHCP | Captive Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | NTP | Settings

General | Gateways | Routing | DNS Resolver | Wireless

**Last 50 General Log Entries. (Maximum 50)**

| Time | Process | PID | Message |
|---|---|---|---|
| Nov 17 12:08:37 | rc.gateway_alarm | 33677 | >>> Gateway alarm: TANETGW (Addr:163.28.16.254 Alarm:1 RTT:819ms RTTsd:153ms Loss:22%) |
| Nov 17 12:08:37 | check_reload_status | | updating dyndns TANETGW |
| Nov 17 12:08:37 | check_reload_status | | Restarting ipsec tunnels |
| Nov 17 12:08:37 | check_reload_status | | Restarting OpenVPN tunnels/interfaces |
| Nov 17 12:08:37 | check_reload_status | | Reloading filter |
| Nov 17 12:08:38 | php-fpm | 82082 | /rc.dyndns.update: MONITOR: TANETGW is down, omitting from routing group GW_GROUP 163.28.16.254\|163.28.16.45\|TANETGW\|0.819ms\|0.155ms\|24%\|down |
| Nov 17 12:13:10 | rc.gateway_alarm | 99061 | >>> Gateway alarm: TANETGW (Addr:163.28.16.254 Alarm:0 RTT:3420ms RTTsd:14782ms Loss:5%) |
| Nov 17 12:13:10 | check_reload_status | | updating dyndns TANETGW |
| Nov 17 12:13:10 | check_reload_status | | Restarting ipsec tunnels |
| Nov 17 12:13:10 | check_reload_status | | Restarting OpenVPN tunnels/interfaces |
| Nov 17 12:13:10 | check_reload_status | | Reloading filter |
| Nov 17 12:13:11 | php-fpm | 61918 | /rc.dyndns.update: MONITOR: TANETGW is available now, adding to routing group GW_GROUP 163.28.16.254\|163.28.16.45\|TANETGW\|3.382ms\|14.656ms\|4%\|none |

# 網頁備援運作架構


TANet
NTU
X
163.28.16.45
140.112.2.208
pfsense
syslog
Rsyslog Server
140.112.x.x
NTU
nsupdate
dns.ntu.tp1rc.edu.tw
140.112.2.238
NTU
LAN
10.1.1.1/24
www.ntu.tp1rc.edu.tw
140.112.2.208
163.2816.45
Web Server
IP:10.1.1.2

# DNS 動態更新

* nsupdate -v /root/nsupdate_tp1rc.txt
* nsupdate_tp1rc.txt

```
server 140.112.2.238
update delete www.ntu.tp1rc.edu.tw A
update add www.ntu.tp1rc.edu.tw 120 A 140.112.2.208
send
```

# 網路行為異常偵測

## TANET2017論文 –與北區 ASOC共同發表

105年評審委員建議: 第 3 點 整合校內學術資源

# 傳統網路分析之瓶頸與限制
# Netflow

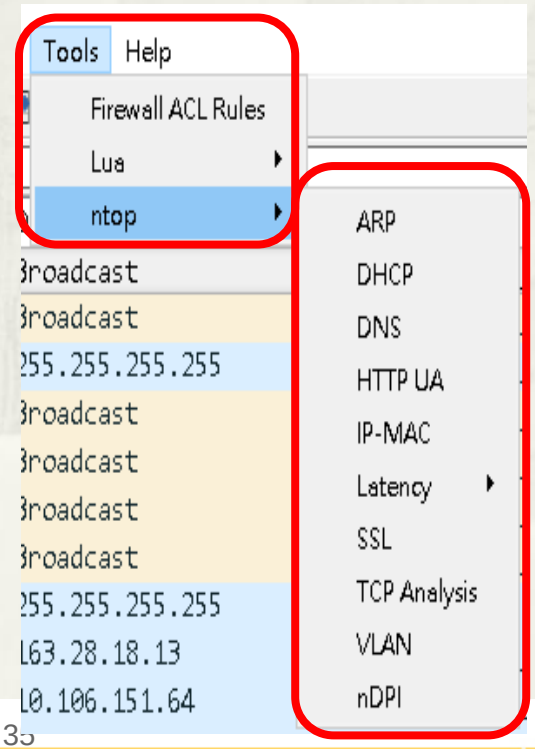
- Layer 2 mac address Level: 無法觀察
  - 無法偵測 broadcast storm, arp spoofing
- Layer 3 IP Level
  - 無法偵測同網段之網路連線行為
  - 無法即時反應網路連線資訊、僅能提供連線 Summary 結果
    - 路由器Netflow Active Time 預設 30分鐘: 一個持續檔案傳輸之連線需30分鐘後才會匯出 Summary傳輸結果資料
  - 無法觀察 TTL(Time to Live) 變化
- Layer 4 TCP Level: 有限分析
  - 無法觀察 TCP Sessions、TCP retrasmistion、Out of order、Duplicate ack ...
- Layer 7 Application Level: 無法分析

# 傳統網路分析之瓶頸與限制 Wireshark

- 見樹不見林:
  - 可詳細觀察每個封包所有欄位資訊，但缺乏整體統計與分析。
- 針對高速網路 10Gbps,100Gbps 側錄有困難
- 無法針對 Layer7 應用層分析與過濾
  - “filter all Skype” traffic is not possible

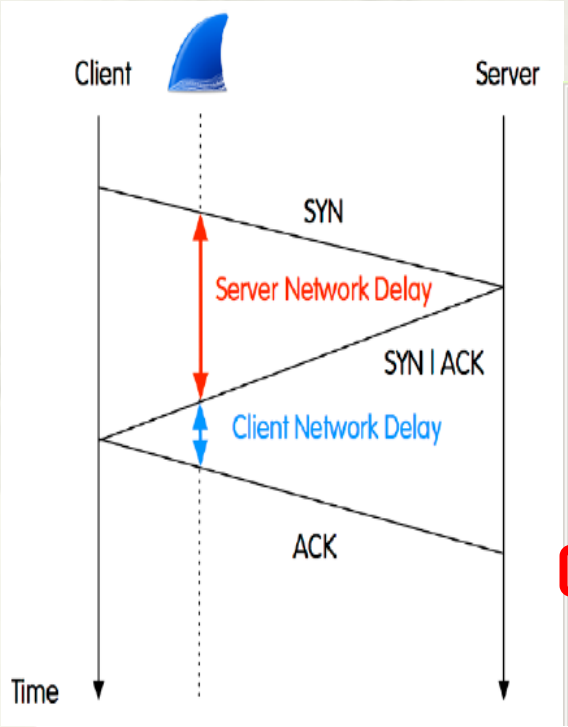
# Network Overview based on packet level
## Wireshark + ntop plugin

* ntop plugin (sharkfest 2017)
  * Lua script for wireshark (Open Source)
  * https://github.com/ntop/nDPI/tree/dev/wireshark

# 分析案例一
# 網路很慢 vs. 網站很慢

* 使用者抱怨反應
  * 網路很慢 vs. 網站很慢
  * Network Delay vs. Application Delay

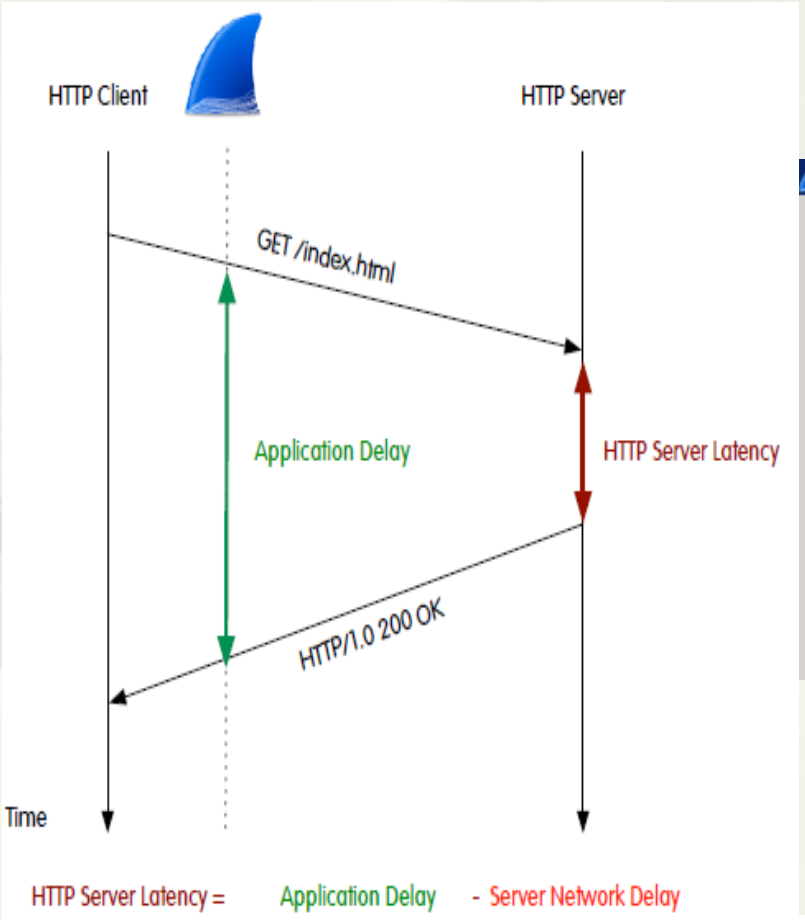



Wireshark · Network Latency

| Client | Min/Max RTT |
|---|---|
| 172.16.0.2 | 0.038 / 0.117 msec |
| **Server** | **Min RTT** |
| 54.194.226.6 | 296.570 / 296.570 msec |
| 72.251.245.181 | 286.275 / 286.275 msec |
| 37.139.11.123 | 281.332 / 281.332 msec |
| 34.224.135.40 | 197.057 / 197.057 msec |
| 34.239.56.165 | 196.941 / 196.941 msec |
| 205.180.86.172 | 142.621 / 142.621 msec |
| 64.38.119.27 | 141.538 / 141.538 msec |
| 103.243.221.109 | 108.627 / 108.627 msec |
| 106.10.193.33 | 82.442 / 82.442 msec |
| 103.67.200.188 | 74.881 / 74.881 msec |
| 50.116.239.135 | 57.246 / 57.246 msec |

# 分析案例一
# 網路很慢 vs. 網站很慢

* Application Delay

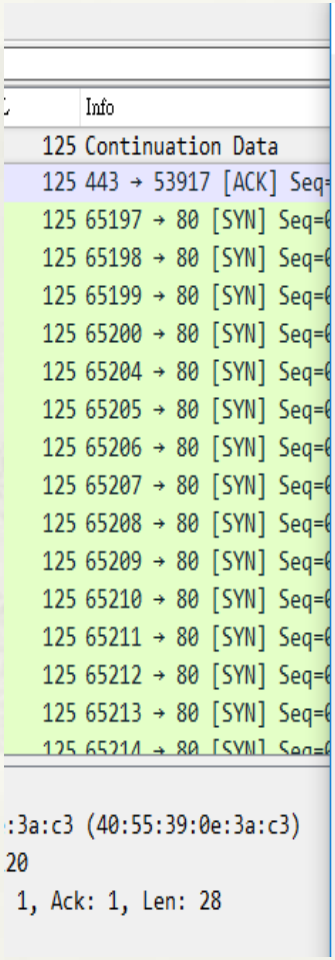


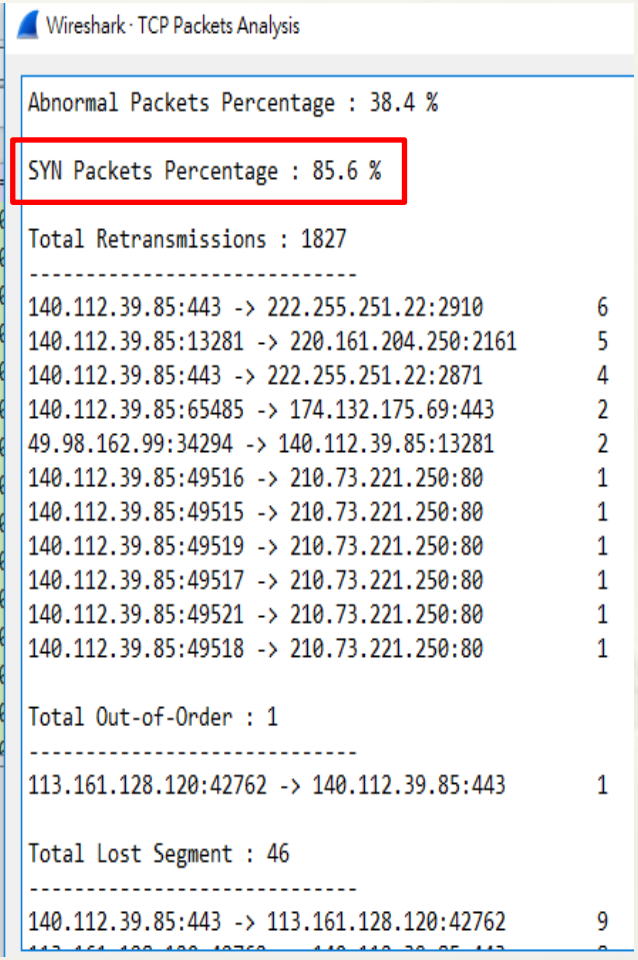

Wireshark · Application Latency

| Server | Min Application RTT |
|---|---|
| 103.243.221.109 | 1429.770 / 1429.770 msec |
| 204.11.109.68 | 432.199 / 432.199 msec |
| 63.251.252.12 | 222.961 / 222.961 msec |
| 204.2.197.204 | 220.601 / 220.601 msec |
| 34.224.135.40 | 202.335 / 202.335 msec |
| 54.172.137.57 | 202.254 / 202.254 msec |
| 69.20.20.10 | 177.324 / 177.324 msec |
| 64.38.119.27 | 145.299 / 145.299 msec |
| 52.9.175.175 | 132.866 / 132.866 msec |
| 38.106.10.133 | 131.861 / 131.861 msec |
| 103.67.200.188 | 85.984 / 85.984 msec |

# 分析案例二
# SYN Flood

- 統計 TCP flag 比例偵測異常行為。
- 自行新增 Lua script 程式碼

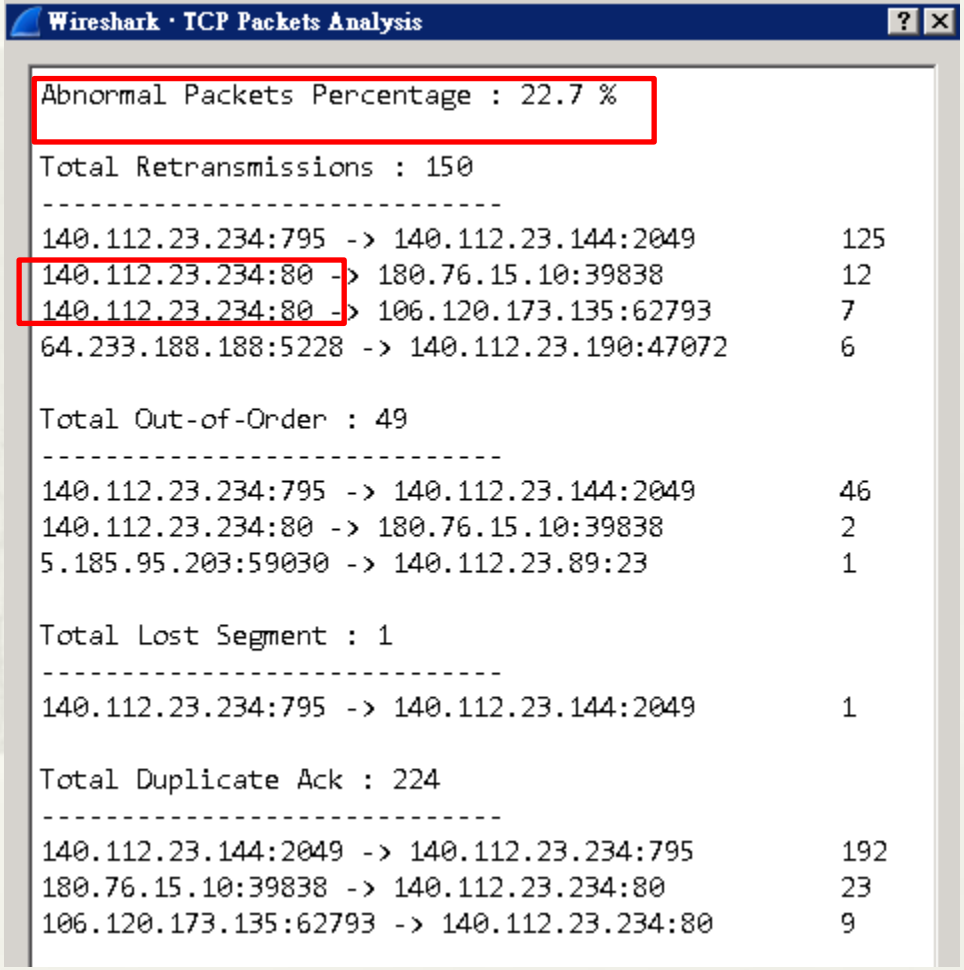


# 分析案例三
# 實體網路線異常

* 臺大校內某系所網頁首頁 Web Server
* 新增統計 TCP 封包異常比例，Lua script 程式碼

```
label = label .. "Abnormal Packets Percentage : " .. formatPctg((num_tcp_retrans + num_tcp_ooo + num_tcp_lost_segment + num_tcp_duplicate_ack) / last_processed_packet_number * 100) .. "\n"
```



# 分析案例四
# IPS 誤擋

* 連線臺大首頁 www.ntu.edu.tw 封包遭 IPS 誤擋
* 新增統計 TCP 封包異常比例，Lua script 程式碼(同前頁)

Wireshark · TCP Packets Analysis

```
Abnormal Packets Percentage : 24.1 %

Total Retransmissions : 1395
-----------------------------
140.112.8.116:80 -> 140.112.114.183:56217          358
140.112.8.116:80 -> 140.112.114.183:56214          329
140.112.8.116:80 -> 140.112.114.183:56211          224
140.112.8.116:80 -> 140.112.114.183:56213          184
140.112.8.116:80 -> 140.112.114.183:56215          130
140.112.8.116:80 -> 140.112.114.183:56210          125
140.112.8.116:80 -> 140.112.114.183:56207          23
140.112.8.116:80 -> 140.112.114.183:56218          19
108.177.97.157:443 -> 140.112.114.183:56201        3

Total Out-of-Order : 35
-----------------------------
140.112.8.116:80 -> 140.112.114.183:56213          17
140.112.8.116:80 -> 140.112.114.183:56218          16
140.112.8.116:80 -> 140.112.114.183:56211          1
140.112.8.116:80 -> 140.112.114.183:56215          1

Total Lost Segment : 68
-----------------------------
140.112.8.116:80 -> 140.112.114.183:56218          22
140.112.8.116:80 -> 140.112.114.183:56217          11
140.112.8.116:80 -> 140.112.114.183:56213          10
140.112.8.116:80 -> 140.112.114.183:56214          8
140.112.8.116:80 -> 140.112.114.183:56211          4
140.112.8.116:80 -> 140.112.114.183:56215          4
```

# 分析案例五
# 重複嘗試登入

* 不尋常的重複嘗試登入，可能被入侵的徵兆
* 傳統偵測方式：需於應用程式 Access Log 進行分析

SSH login failed

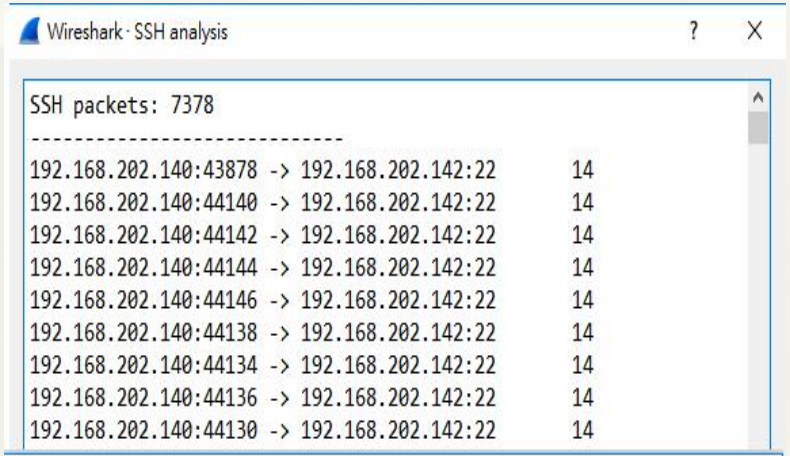
```
Last failed login: Mon Nov 20 08:59:19 CST 2017 from 223.68.134.29 on ssh:notty
There were 4770 failed login attempts since the last successful login.
Last login: Mon Oct 30 20:59:47 2017 from davisyoupc.cc.ntu.edu.tw
```

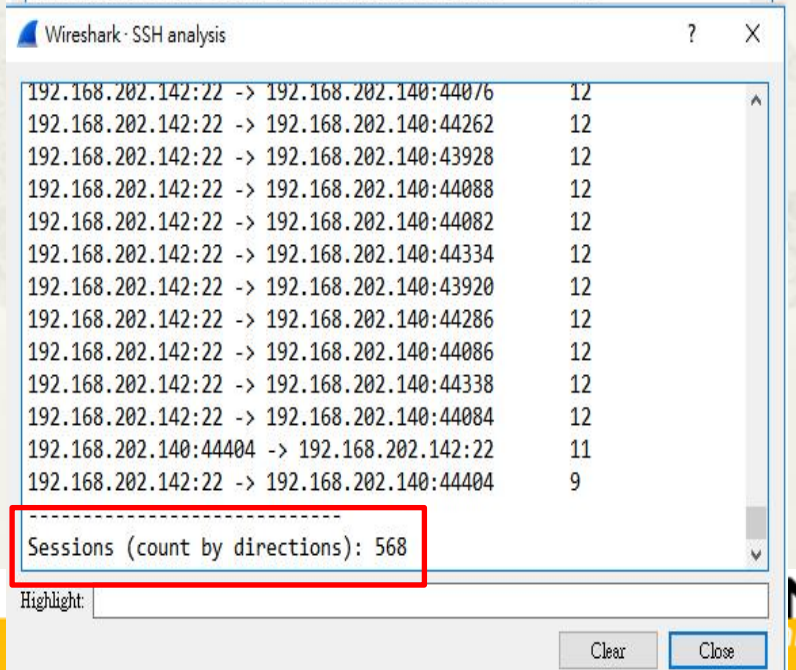
RDP login failed

| 等級 | 日期和時間 | 來源 | 事件識別碼 | 工作類別 |
|---|---|---|---|---|
| 資訊 | 2017/10/25 下午 04:06:51 | TerminalServices-RemoteConnectionMana... | 1149 | 無 |
| 資訊 | 2017/10/25 下午 04:06:51 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:51 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:45 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:42 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:38 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:34 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:31 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 04:06:25 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 03:53:32 | TerminalServices-RemoteConnectionMana... | 1149 | 無 |
| 資訊 | 2017/10/25 下午 03:53:32 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 03:53:32 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 03:05:11 | TerminalServices-RemoteConnectionMana... | 1149 | 無 |
| 資訊 | 2017/10/25 下午 03:05:10 | TerminalServices-RemoteConnectionMana... | 261 | 無 |
| 資訊 | 2017/10/25 下午 03:05:09 | TerminalServices-RemoteConnectionMana... | 261 | 無 |

# 分析案例五
# 重複嘗試登入...

* 分析連入 Server 封包，相同 Clinet IP 在短時間內不斷建立不同 tcp.stream，即可能是嘗試登入行為
* 自行新增 Lua script 程式碼



# LAYER 7 網路行為分析

# Layer 7 分析-傳統方式

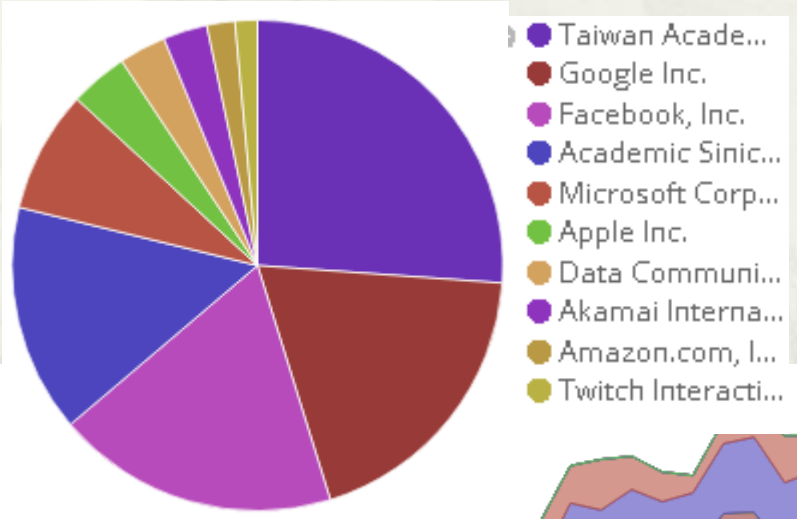
* 傳統分析方式
  * 21 ftp
  * 22 ssh
  * 23 telnet
  * 80 http
  * 443 https
  * …

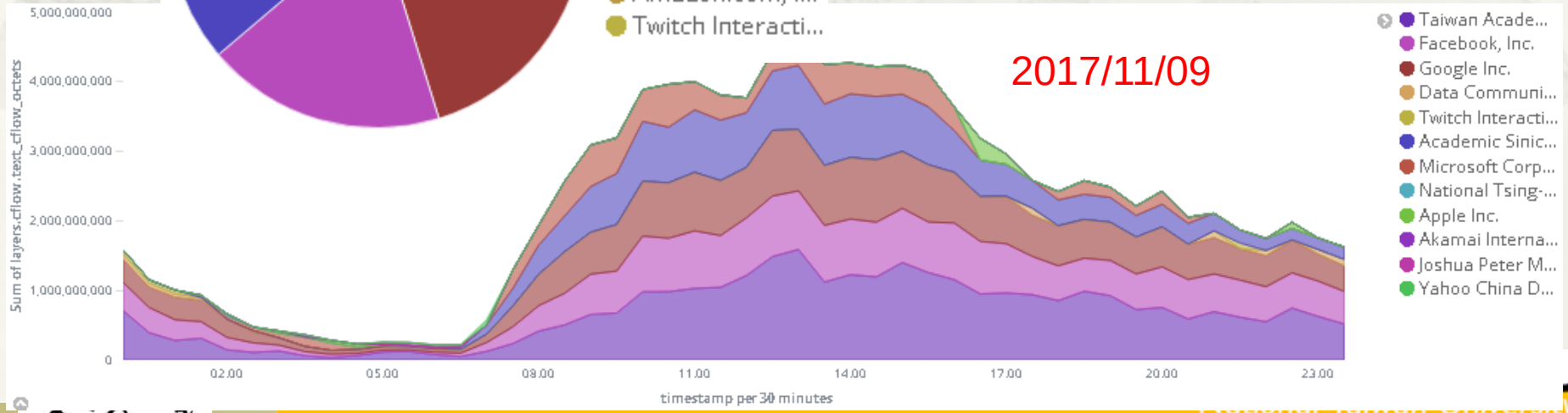
# Layer 7 分析-ASN

- 使用 Geoip 查詢 IP 所屬 Autonomous System Number(ASN)
  - 優點: 現有 IP 就可分析，可套用於現成 Netflow 分析工具
  - 缺點: 僅能大略分析網路行為，無法辨識如 P2P 等 Protocol

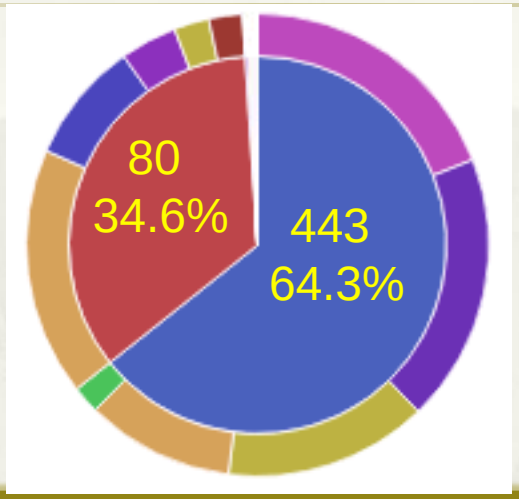
# Layer 7 分析-ASN

- 區網 TANet 100G Top 10 ASN 分析結果
- netflow + ELK Stack



# Layer 7 分析-ASN




| port | Source ASN | % |
|---|---|---|
| 443 | Facebook, Inc. | 26% |
| 443 | Google Inc. | 25% |
| 443 | Academic Sinica Network | 19% |
| 443 | Taiwan Academic Network (TANet) Information Center | 14% |
| 443 | Data Communication Business Group | 3% |
| 80 | Taiwan Academic Network (TANet) Information Center | 50% |
| 80 | Microsoft Corporation | 25% |
| 80 | Apple Inc. | 11% |
| 80 | Academic Sinica Network | 8% |
| 80 | Akamai International B.V. | 6% |

# Layer 7 分析-DPI

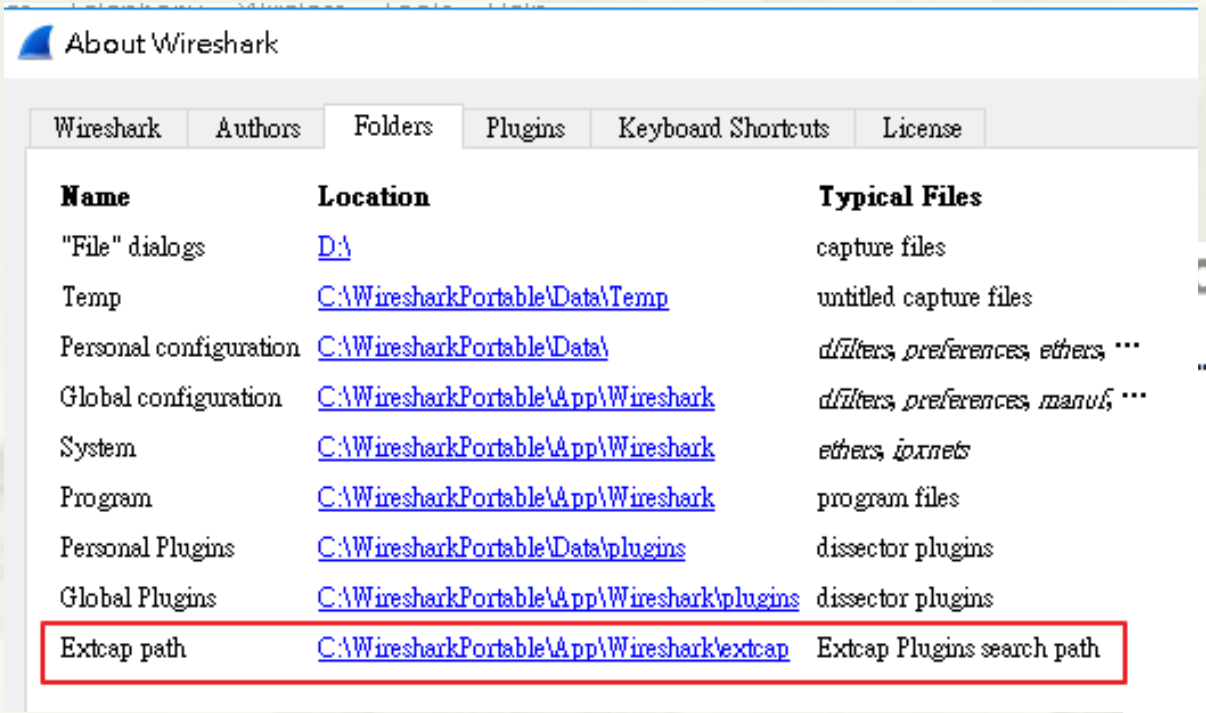
- 使用DPI(Deep Packet Inspection )分析
  - 商業硬體設備
    - Proprietary protocol pattern 非公開
    - 倚賴廠商不斷更新 pattern
  - Open Source DPI Library
    - nDPI，Support 186+ application protocols
    - https://github.com/ntop/nDPI/tree/dev/example
    - 網路社群力量大

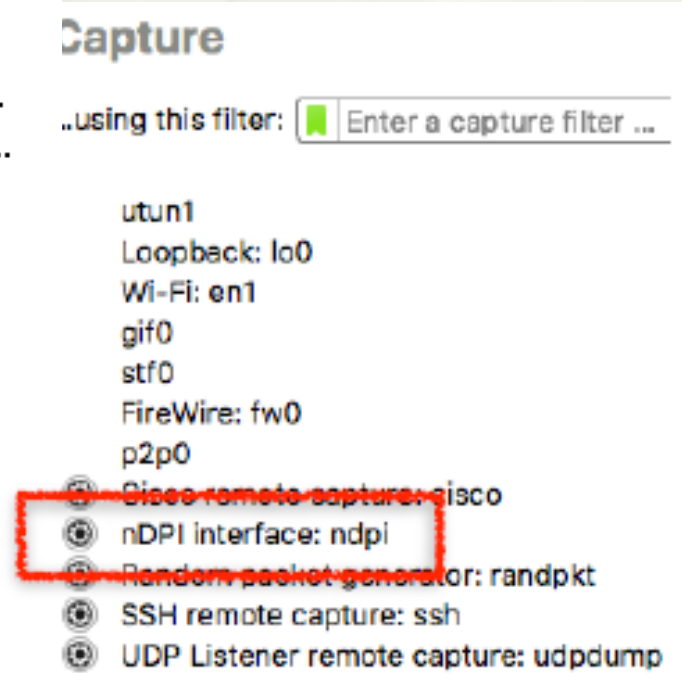
# nDPI Support 186+ Protocols

FTP POP SMTP IMAP DNS IPP HTTP MDNS NTP NETBIOS NFS SSDP BGP SNMP XDMCP SMB SYSLOG DHCP PostgreSQL MySQL TDS DirectDownloadLink I23V5 AppleJuice DirectConnect Socrates WinMX VMware PANDO Filetopia iMESH Kontiki OpenFT Kazaa/Fasttrack Gnutella eDonkey Bittorrent OFF AVI Flash OGG MPEG QuickTime RealMedia Windowsmedia MMS XBOX QQ MOVE RTSP Feidian Icecast PPLive PPStream Zattoo SHOUTCast SopCast TVAnts TVUplayer VeohTV QQLive Thunder/Webthunder Soulseek GaduGadu IRC Popo Jabber MSN Oscar Yahoo Battlefield Quake VRRP Steam Halflife2 World of Warcraft Telnet STUN IPSEC GRE ICMP IGMP EGP SCTP OSPF IP in IP RTP RDP VNC PCAnywhere SSL SSH USENET MGCP IAX TFTP AFP StealthNet Aimini SIP Truphone ICMPv6 DHCPv6 Armagetron CrossFire Dofus Fiesta Florensia Guildwars HTTP Application Activesync Kerberos LDAP MapleStory msSQL PPTP WARCRAFT3 World of Kung Fu MEEBO FaceBook Twitter DropBox Gmail Google Maps YouTube Skype Google DCE RPC NetFlow_IPFIX sFlow HTTP Connect (SSL over HTTP) HTTP Proxy Netflix Citrix CitrixOnline/GotoMeeting Apple (iMessage, FaceTime...) Webex WhatsApp Apple iCloud Viber Apple iTunes Radius WindowsUpdate TeamViewer Tuenti LotusNotes SAP GTP UPnP LLMNR RemoteScan Spotify H323 OpenVPN NOE CiscoVPN TeamSpeak Tor CiscoSkinny RTCP RSYNC Oracle Corba UbuntuONE CNN Wikipedia Whois-DAS Collectd Redis ZeroMQ Megaco QUIC WhatsApp Voice Stracraft Teredo Snapchat Simet OpenSignal 99Taxi GloboTV Deezer Instagram Microsoft cloud services Twitch KakaoTalk Voice and Chat HotspotShield VPN

# Install nDPI with Wireshark

* Wireshark Extcap plugin



# nDPI Layer 7 protocol 分析

| Src port | Destination | Dest port | Protocol | Length | info |
|---|---|---|---|---|---|
| 443 | 140.112.41.76 | 2242 | SSL.Facebook | 1492 | [TCP segment of a reassembled PDU] |
| 443 | 140.112.41.76 | 2242 | SSL.Facebook | 1492 | [TC |
| 443 | 140.112.41.76 | 2242 | SSL.Facebook | 1458 | App |
| 443 | 140.112.41.76 | 2242 | SSL.Facebook | 1492 | [TC |
| 2461 | 216.58.200.46 | 443 | SSL.Google | 135 | App |
| 2461 | 216.58.200.46 | 443 | SSL.Google | 138 | App |
| 2461 | 216.58.200.46 | 443 | SSL.Google | 124 | App |
| 443 | 140.112.41.76 | 2461 | SSL.Google | 151 | App |
| 2461 | 216.58.200.46 | 443 | SSL.Google | 120 | App |
| 443 | 140.112.41.76 | 2461 | SSL.Google | 88 | 443 |
| 443 | 140.112.41.76 | 2461 | SSL.Google | 120 | App |
| 443 | 140.112.41.76 | 2461 | SSL.Google | 88 | 443 |
| 2461 | 216.58.200.46 | 443 | TCP | 82 | 246 |
| 2393 | 111.221.29.193 | 443 | TCP | 82 | 239 |
| 2394 | 111.221.29.194 | 443 | TCP | 82 | 239 |
| 443 | 140.112.41.76 | 1808 | SSL.Dropbox | 339 | App |
| 1808 | 162.125.34.129 | 443 | SSL.Dropbox | 1091 | App |
| 443 | 140.112.41.76 | 1808 | SSL.Dropbox | 88 | 443 |
| 443 | 140.112.41.76 | 1808 | SSL.Dropbox | 437 | App |
| 1808 | 162.125.34.129 | 443 | SSL.Dropbox | 817 | App |

Wireshark · nDPI Protocol Statistics

nDPI Protocol Breakdown

| | | |
|---|---|---|
| SSL | 2.5 MB | [60.5 %] |
| QUIC.GMail | 725.97 KB | [17.2 %] |
| SSL.Facebook | 438.13 KB | [10.4 %] |
| QUIC.Google | 334.06 KB | [7.9 %] |
| Unknown | 51.76 KB | [1.2 %] |
| SSL.Google | 35.27 KB | [< 1 %] |
| QUIC | 16.23 KB | [< 1 %] |
| QUIC.YouTube | 10.63 KB | [< 1 %] |
| BitTorrent | 10.42 KB | [< 1 %] |
| SSL.Amazon | 7.78 KB | [< 1 %] |
| DNS | 7.44 KB | [< 1 %] |

Top nDPI Flows

| | | |
|---|---|---|
| 203.66.159.1 / 140.112.41.128 [SSL] | 2.26 MB | [54.7 %] |
| 172.217.24.5 / 140.112.41.128 [QUIC.GMail] | 650.83 KB | [15.4 %] |
| 31.13.87.36 / 140.112.41.128 [SSL.Facebook] | 238.69 KB | [5.6 %] |
| 31.13.87.5 / 140.112.41.128 [SSL.Facebook] | 174.31 KB | [4.1 %] |
| 202.39.235.195 / 140.112.41.128 [SSL] | 145.76 KB | [3.4 %] |
| 140.112.41.128 / 172.217.24.5 [QUIC.GMail] | 72.36 KB | [1.7 %] |
| 216.58.200.238 / 140.112.41.128 [QUIC.Google] | 49.51 KB | [1.2 %] |
| 74.125.204.189 / 140.112.41.128 [QUIC.Google] | 49.01 KB | [1.2 %] |
| 74.125.23.189 / 140.112.41.128 [QUIC.Google] | 49.01 KB | [1.2 %] |
| 172.217.24.14 / 140.112.41.128 [QUIC.Google] | 44.96 KB | [1.1 %] |
| 140.112.41.128 / 172.217.24.14 [QUIC.Google] | 38.91 KB | [< 1 %] |

# 六、未來工作目標與建議

- ISO27001-2013 全臺大計資中心導入
- 區網 Peer ISP 電路納入 IPS 偵測範圍
- 搭配 Gigamon APF、ASF 功能持續進行網路異常偵測與分析
  - 印表機勒索: Printer Port 9100
  - NTP 放大攻擊:NTP monlist
  - LDAP 放大攻擊: LDAP Port 389
- 網路行為異常偵測 + ELK Stack

# 105年評審委員建議與回覆

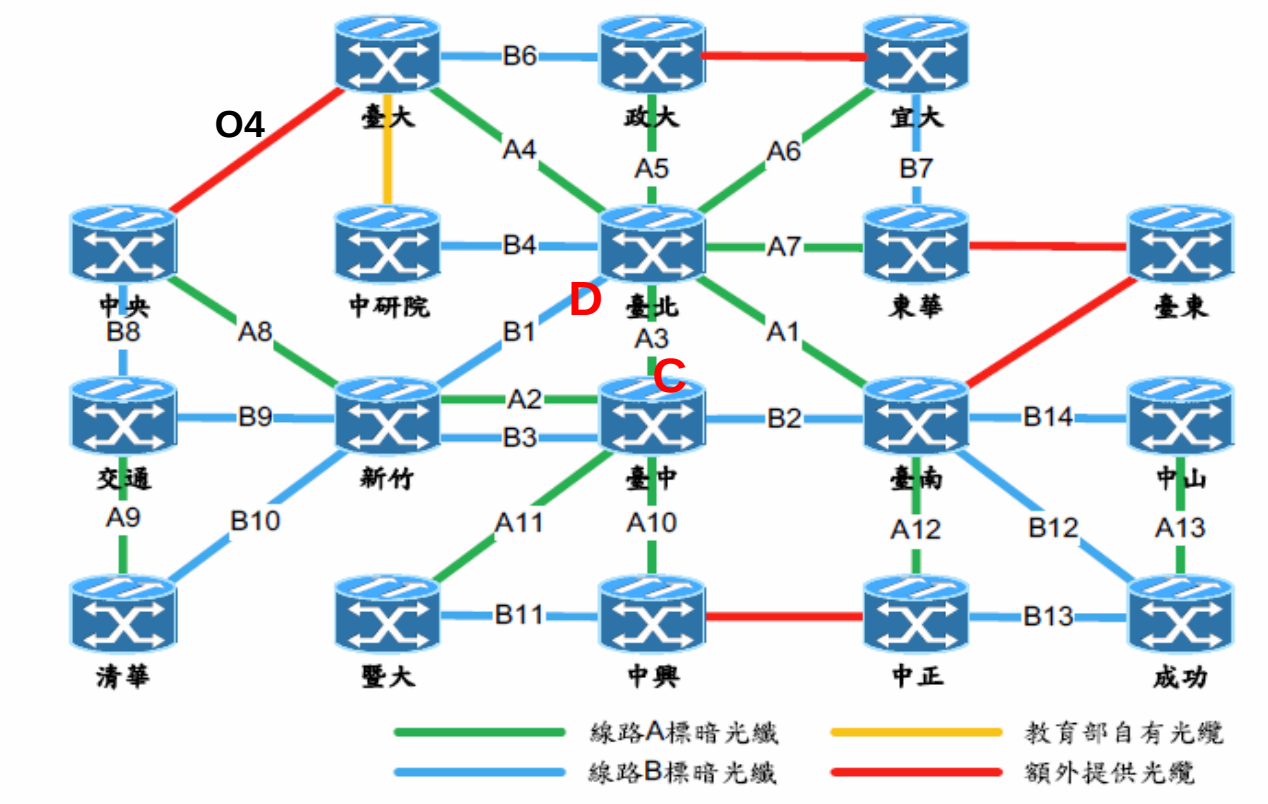
| 委員建議 | 回覆 |
| --- | --- |
| 1.改善連線單位 ping packet lost% 監控機制 | 大專院校 peer ip 使用 Ping 統計已全部完成(RTT、Packet Lost %)，高中職以下受限設備與網管技術仍待努力 |
| 2.建置多樣即時監控機制 | 增加 Cacti 流量圖、封包量圖、介面異常統計，建置事件通知警示系統監控 ASR Router Log 事件 |
| 3.整合校內學術資源，有效提升服務能量 | 在 TANET2017論文發表 –網路行為異常偵測，與北區 ASOC、電機系、電信所教授共同發表 |
| 4.改善資安審核時數 | 已改善，由 3.43小時 減少為 0.60小時 |
| 5 資安事件量龐大 | 已改善，事件量由 6930 減少為 4264 |

# 105年評審委員建議與回覆

| 委員建議 | 回覆 |
| --- | --- |
| 6.與市網更有效溝通 | 協助解決臺北酷課雲在區網雲端服務 SSO 連線問題 |
| 7.資安人力未能及時聘用 | 資安人力今年已經到位，另有聘請工讀生協助區網網頁與相關資料整理 |
| 8.資安事件總量高 | 已改善，事件量由 6930 減少為 4264 |
| 9. 強化連線單位溝通協調，協助解決 DNS老舊 | 協助解決連線單位-法鼓文理學院 Routing Loop 問題，並建置主動偵測 DNS 放大攻擊機制 |

# 基礎電路建議

* 臺大連外A4、O4 光纖應由兩家不同 ISP 承包　11/16 凌晨區網斷線近 3小時



# 其他建議

- Line 發生多次無法登入
  - 2017/4/12 、2017/5/10 、2017/10/11 、2017/11/15
  - 缺乏顯示 TANet 連外線路頻寬與限制
- 建議各節點路由器加上IP 反解，網管才能瞭解網路路徑

```
C:\Users\Administrator>tracert line.me

在上限 30 個躍點上
追蹤 line.me [203.104.138.138] 的路由:

  1    <1 ms    <1 ms    <1 ms  192.168.20.1
  2     1 ms    <1 ms    <1 ms  nep17-254.tp1rc.edu.tw [163.28.17.254]
  3     2 ms     1 ms     1 ms  192.192.61.82
  4     3 ms     3 ms     3 ms  192.192.61.185
  5     1 ms     1 ms     1 ms  192.192.61.194
  6    53 ms    53 ms    52 ms  202.169.174.154
  7     *        *        *     要求等候逾時。
  8     *        *        *     要求等候逾時。
  9  ^C
```

# 其他建議

* TANET研討會
  * 開幕式->高朋滿座、論文發表->門可羅雀
  * 應多鼓勵參與論文發表
    * 論文發表可當區網加分項目
    * TANet 維運相關論文可集中於同場次發表(比照 TWAREN 模式)
    * 出席論文發表會全勤獎(比照廠商集點章)

# 簡報完畢
# 謝謝