

107年度第一次 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：謝宏昫教授	
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	台師大雲端建置與各校區網路架構分享 (1)台師大雲端機房建置與備援機制：使用 Cisco OTV 技術分享 (2)台師大不同校區(校本部、林口、公館)之網路架構與備援機制
	16:20~17:00	游子興	SSL憑證安裝與申請
臨時動議		出列席人員	

大綱

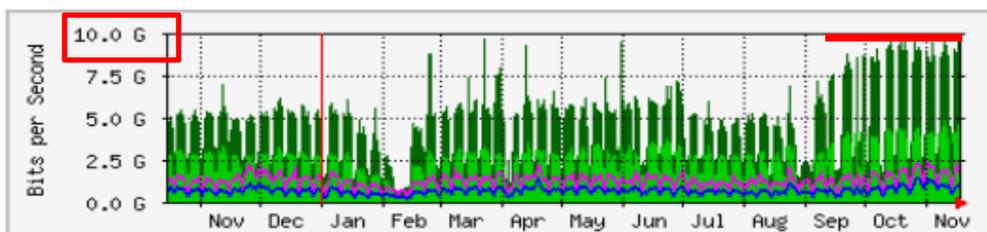
- * 頻寬分流器擴充案
- * Layer7 流量分析
- * IPv6 推廣
- * DNS 版本升級與隱藏

TANet 頻寬用量

* 頻寬用量顯著增加

每年圖表(1天平均)

2016



最大

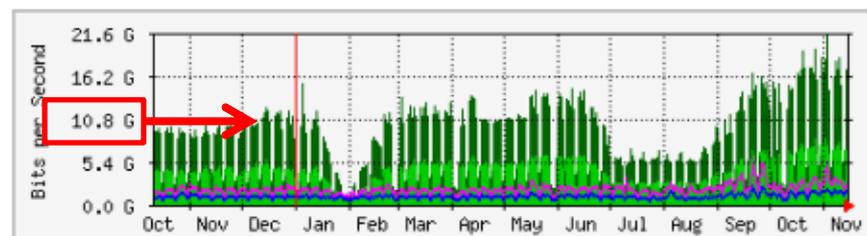
平均

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

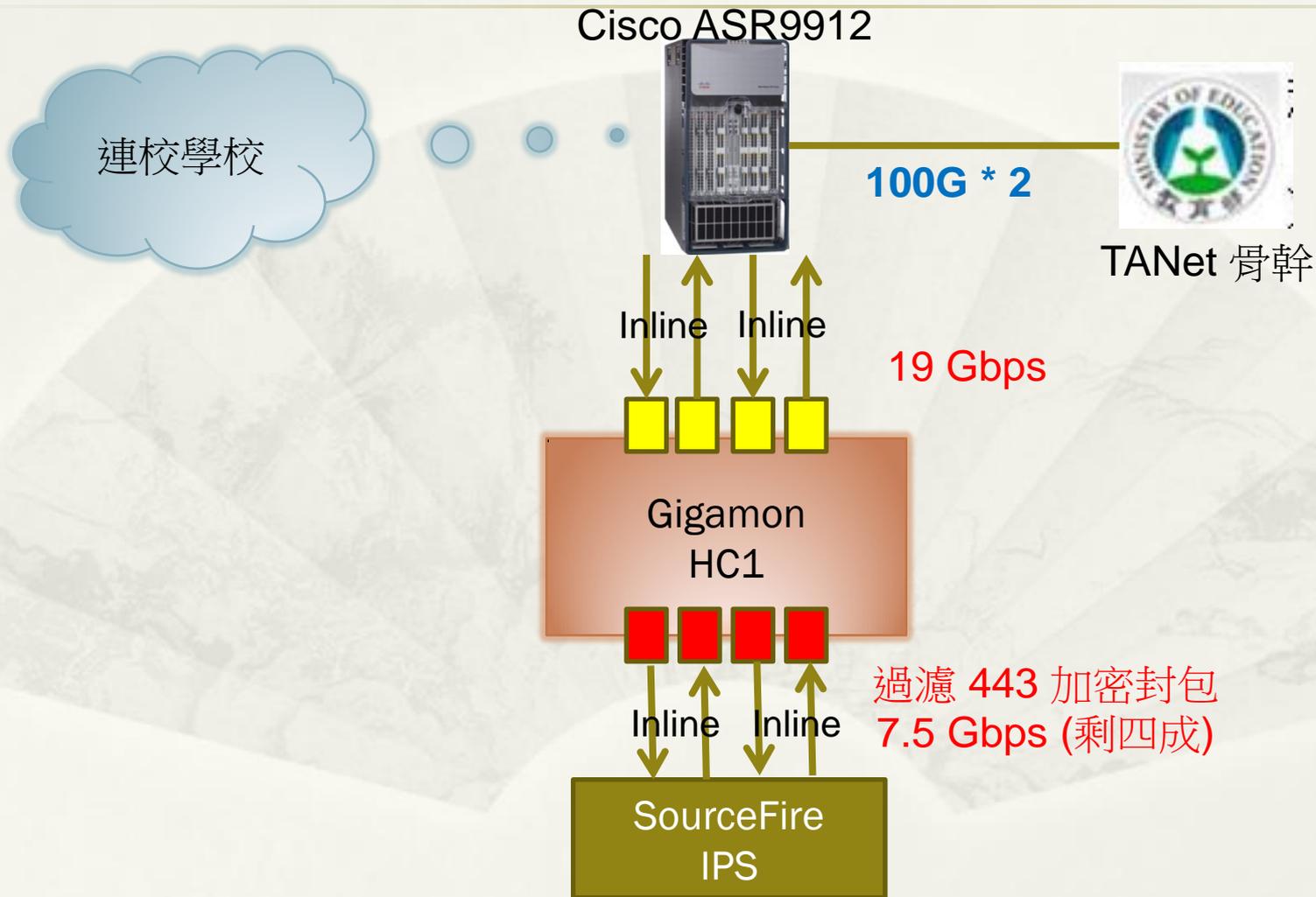
- * 臺北市網、臺大、北科大、臺科大

* 現有資安設備 Capability 不足

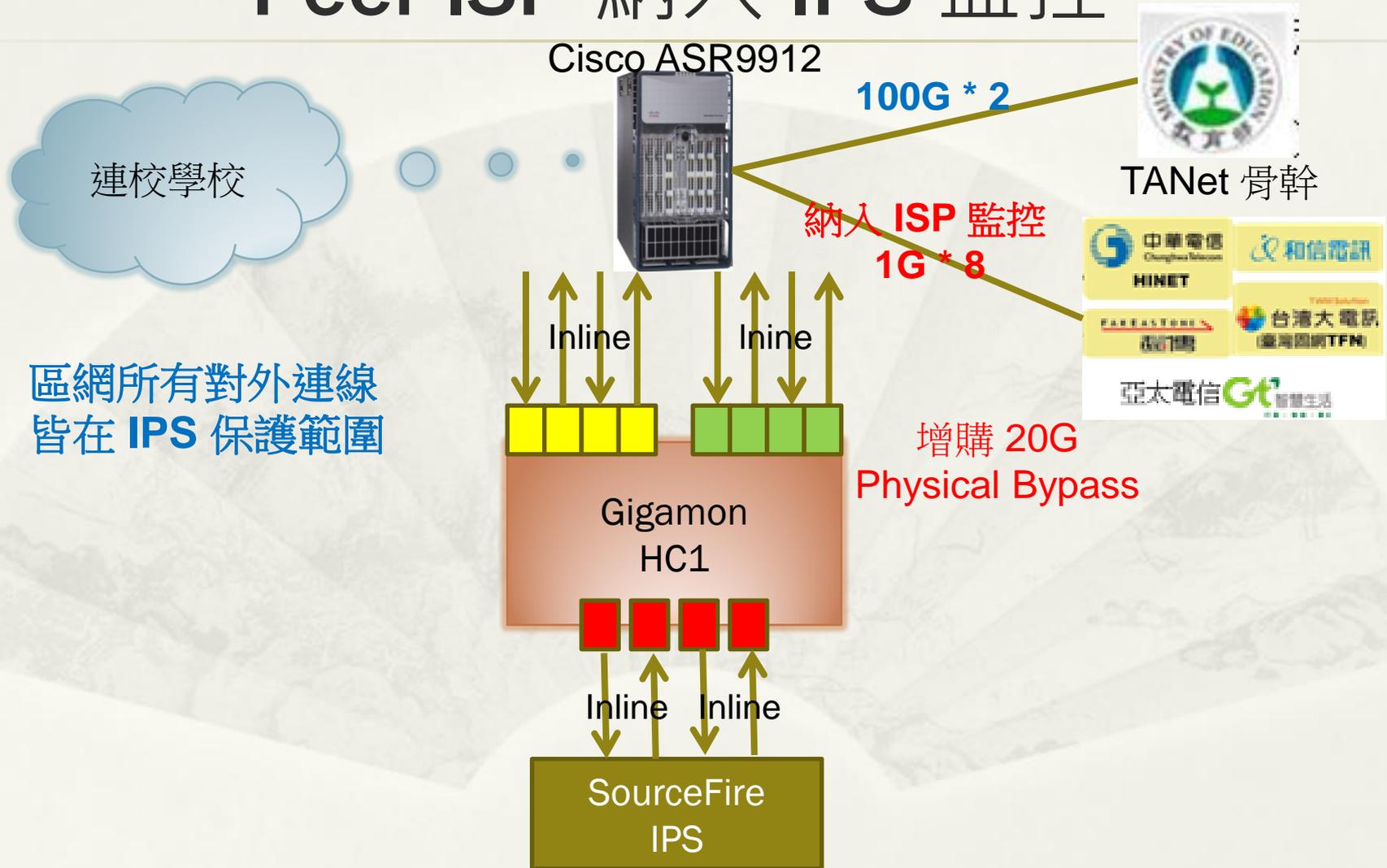
- * IPS Capability: Max 15 Gbps

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

2017 建置頻寬分流器 解決 IPS Capability 不足

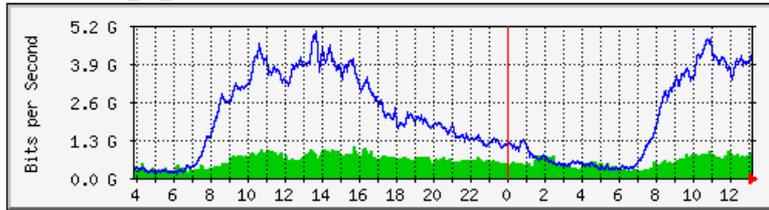


2018 頻寬分流器擴充 Peer ISP 納入 IPS 監控

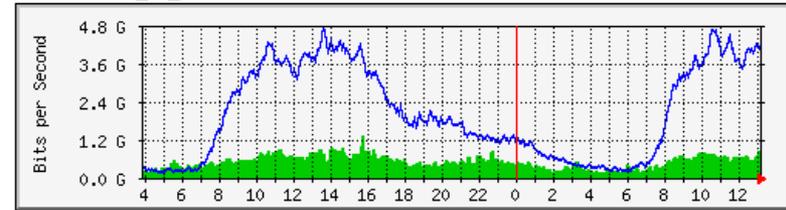


<http://tprc.tanet.edu.tw/mrtg/tpnet-all.html>

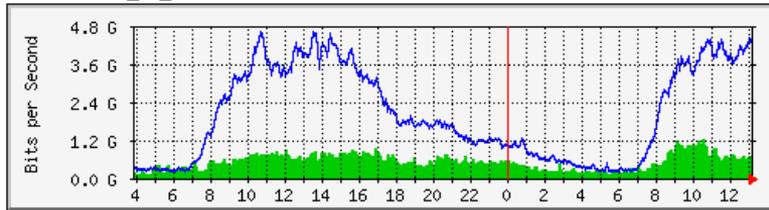
ASR-OUT1_to_IPS



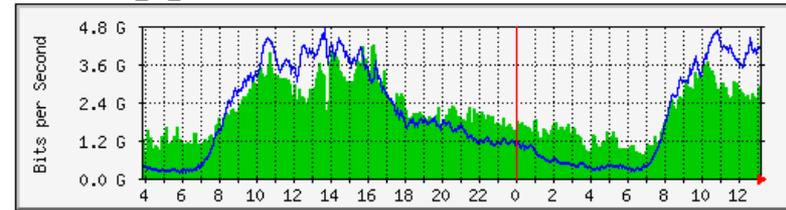
ASR-OUT2_to_IPS



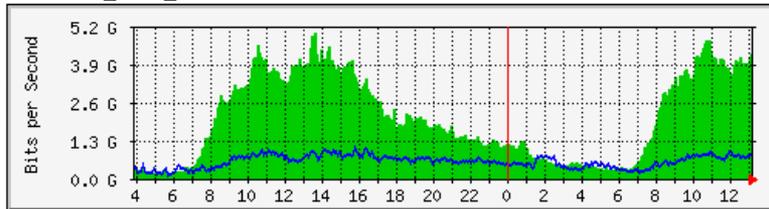
ASR-OUT3_to_IPS



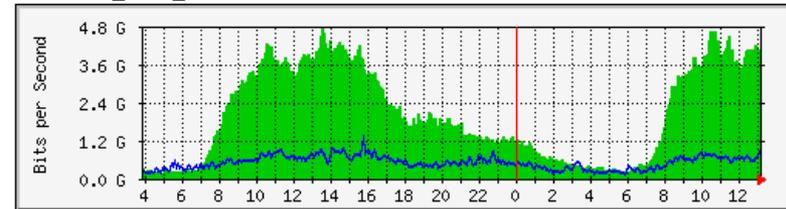
ASR-OUT4_to_IPS



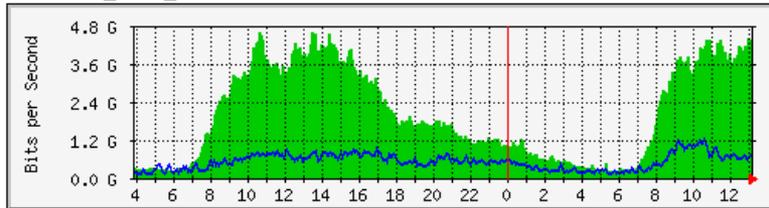
ASR-IN1_from_IPS



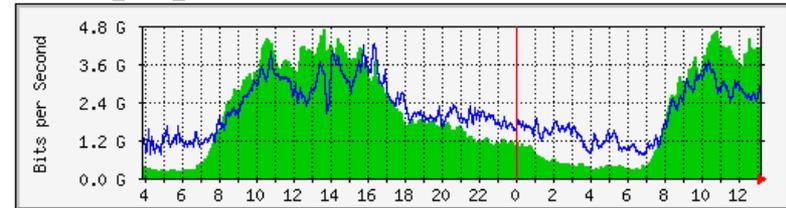
ASR-IN2_from_IPS



ASR-IN3_from_IPS



ASR-IN4_from_IPS



臺大區網

網路品質管理 -> Layer7 流量分析

* <http://www.ntu.tp1rc.edu.tw/layer7.html>

Tag: Application_Name Bytes

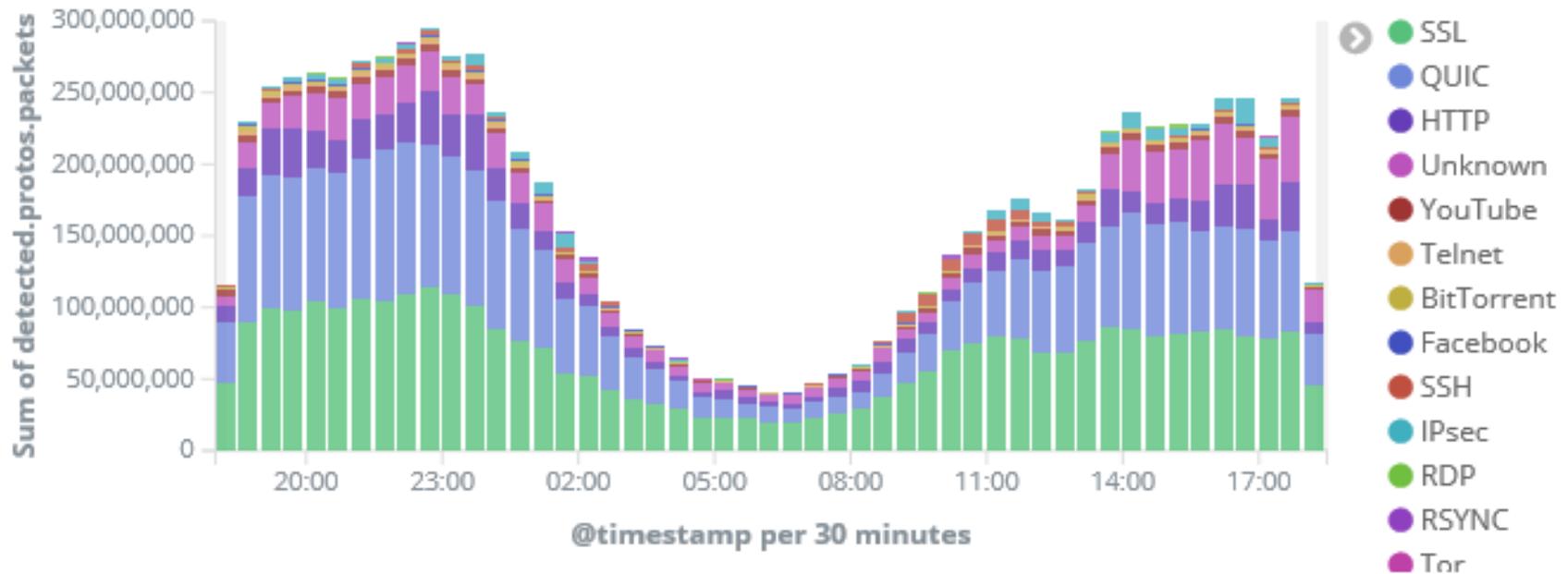


臺大區網

網路品質管理 -> Layer7 流量分析

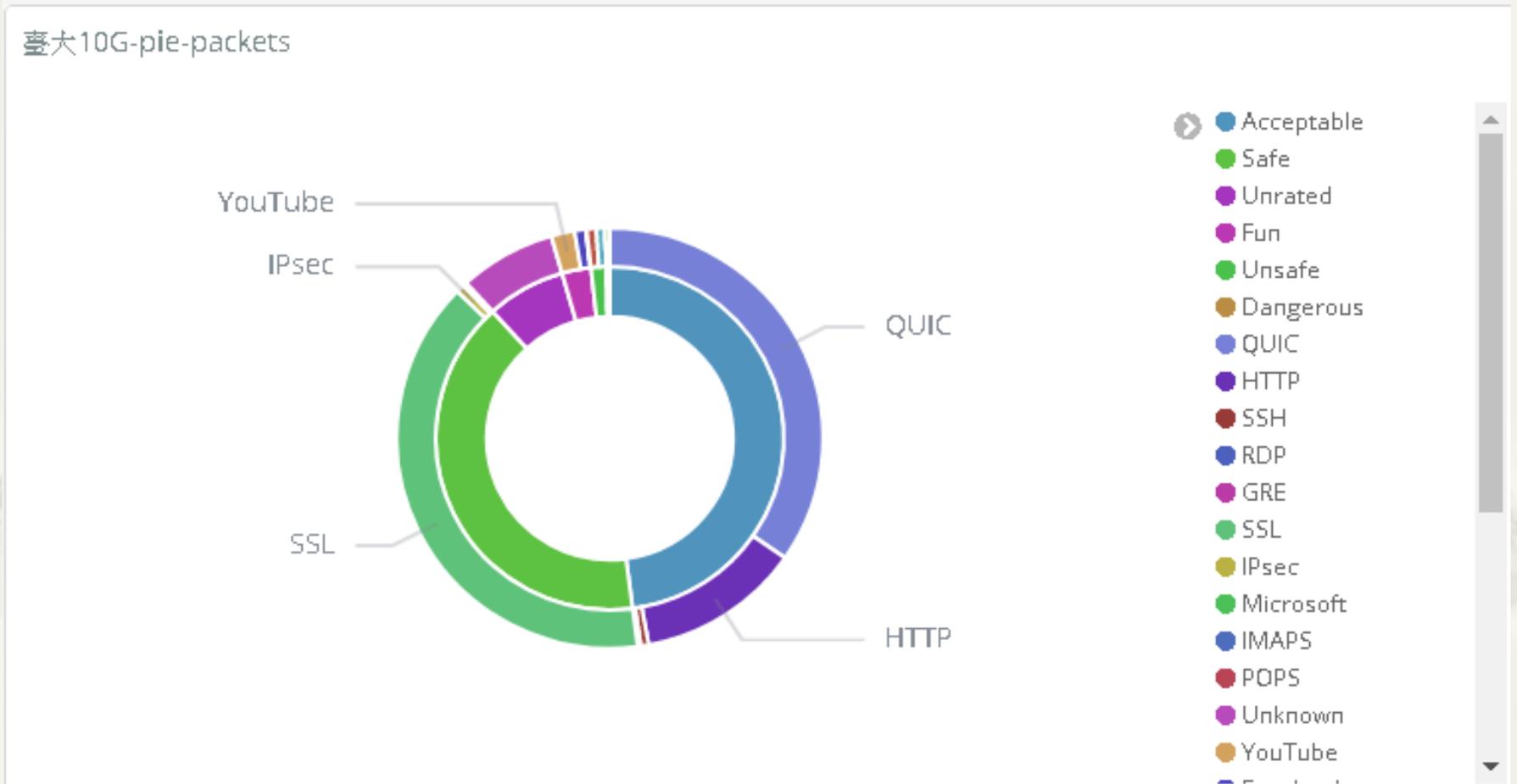
* <http://www.ntu.tp1rc.edu.tw/layer7.html>

臺大10G-bar-packets



臺大區網

網路品質管理 -> Layer7 流量分析



教育部 IPv6 分配表

* <http://domain.edu.tw/dns/colleges.htm>

臺北臺大區網 2001:288:1000::/36 (2001:288:1000--1FFF) 縣市

臺北臺大區網連線單位 2001:288:1000::/39 (2001:288:1000--11FF)

臺北臺大區網 2001:288:1000::/48

國立臺灣大學 2001:288:1001::/48

國立臺灣師範大學 2001:288:1002::/48

國立臺北藝術大學 2001:288:1003::/48

國立臺灣藝術大學 2001:288:1004::/48

國立臺北護理學院 2001:288:1005::/48

國立臺北商業技術學院 2001:288:1006::/48

銘傳大學 2001:288:1007::/48

實踐大學 2001:288:1008::/48

真理大學 2001:288:1009::/48

大同大學 2001:288:100A::/48

臺北醫學大學 2001:288:100B::/48

龍華科技大學 2001:288:100C::/48

明志科技大學 2001:288:100D::/48

德明財經科技大學 2001:288:100E::/48

致理技術學院 2001:288:100F::/48

亞東技術學院 2001:288:1010::/48

德霖技術學院 2001:288:1011::/48

黎明技術學院 2001:288:1012::/48

華夏技術學院 2001:288:1013::/48

連線單位已經設定 IPv6 路由

* 23 個連線單位已經設定 IPv6 路由

- * 臺灣大學
- * 臺灣師範大學
- * 銘傳大學
- * 實踐大學
- * 真理大學
- * 大同大學
- * 龍華科技大學
- * 致理科技大學
- * 宏國德霖科技大學
- * 空中大學
- * 國防大學
- * 臺北市立大學
- * 國防醫學院
- * 臺北科技大學
- * 臺灣科技大學
- * 亞東技術學院
- * 康寧大學
- * 樹人家商
- * 南山高中
- * 開平餐飲
- * 市立教大實小
- * 臺北市網
- * 新北市圖書館

IPv6 設定方式-區網端

* IPv6 區網端設定

* 介面設定

```
interface xxx
```

```
ipv6 address 2001:288:1000:0:2::501/124
```

```
ipv6 enable
```

* 靜態路由設定

```
ipv6 route 2001:288:102D::/48
```

```
2001:288:1000:0:2::502
```

IPv6 設定方式-連線單位

- * IPv6 連線單位設定

- * 介面設定

- interface xxx

- ipv6 address 2001:288:1000:0:2::502/124

- ipv6 enable

- * 靜態路由設定(default route)

- ipv6 route ::/0 2001:288:1000:0:2::501

DNS 版本顯示

學校名稱	FQDN	DNS server Ipv4	DNS server Ipv6	DNS server 版本
致理科技大學	dns.chihlee.edu.tw	140.131.77.1	2001:288:100f:1::2	BIND 9.6.-ESV-R3
	dns2.chihlee.edu.tw	140.131.77.33	2001:288:100f:1::3	BIND 9.6.-ESV-R3
	dns3.chihlee.edu.tw	211.22.7.173		停用
華夏科技大學	proxy1.hwh.edu.tw	140.131.39.205		bind 9.10.5-P3
	cc.hwh.edu.tw	140.131.39.200		bind 9.10.5-P3
	proxy2.hwh.edu.tw	140.131.39.206		bind 9.10.5-P3
	hwh.edu.tw	140.131.39.1		bind 9.10.5-P3
新北市立圖書館	dns.tphcc.gov.tw	203.64.154.1	2001:288:102c:1::2	Infoblox 7.3.13
國北教大實小	ntueees.tp.edu.tw	203.64.153.100		NTUEEES DNS
樹人家商	dns.stgvs.ntpc.edu.tw	203.71.206.1		bind 9.3.4-p1.1
龍華科技大學	dns2.lhu.edu.tw	140.131.1.20		bind 9.9.9-P8
	dns.lhu.edu.tw	140.131.1.11		bind 9.9.9-P8
	dns3.lhu.edu.tw	218.32.30.125		bind 9.9.9-P8
東海高中	dns.thhs.ntpc.edu.tw	210.71.122.1		TIME OUT
開平中學	ns.kpvs.tp.edu.tw	61.219.31.96		9.3.6-P1-RedHat-9.3.6-20.P1.e15_8.6
	ns2.kpvs.tp.edu.tw	203.72.253.2		9.8.2xc1-RedHat-9.8.2-0.37.rc1.e16_7.5
光啟高中	dns.phsh.tyc.edu.tw	210.71.74.1		Bind 9.3.6-P1-RedHat-9.3.6-20.P1.e15_8.6,
南山高中	dns1.nssh.ntpc.edu.tw	203.71.175.1		bind 9.10.3
	dns.nssh.ntpc.edu.tw	203.71.175.1	2001:288:102f:2::1	bind 9.10.3
	dns2.nssh.ntpc.edu.tw	203.71.175.51		bind 9.10.3
台北護理健康大學	dns.ntunhs.edu.tw	140.131.85.210		9.3.6-P1-RedHat-9.3.6-25.P1.e15_11.6
	dns2.ntunhs.edu.tw	140.131.85.212		9.3.6-P1-RedHat-9.3.6-25.P1.e15_11.4
中華民國學生棒球運動聯盟	ns1.ctsbf.edu.tw	140.131.124.1		9.8.2xc1-RedHat-9.8.2-0.17.rc1.e16_4.4
臺灣藝術大學	sd1.ntua.edu.tw	140.131.21.1		Microsoft DNS 6.1.7601 (1DB15CD4)
	sd2.ntua.edu.tw	140.131.21.10		Microsoft DNS 6.1.7601 (1DB15CD4)

DNS Server Version Query

- * nslookup -class=chaos -query=txt version.bind
ip_address
- * Bind dns server

```
D:\>nslookup -class=chaos -query=txt version.bind 163.28.16.46
伺服器: Unknown
Address: 163.28.16.46

version.bind      text =

                "9.9.4-RedHat-9.9.4-51.e17"
version.bind      nameserver = version.bind
```

DNS Server Version Query

* Windows dns server

```
D:\>nslookup -class=chaos -query=txt version.bind 220.134.115.14
(root) nameserver = j.root-servers.net
(root) nameserver = k.root-servers.net
(root) nameserver = l.root-servers.net
(root) nameserver = m.root-servers.net
(root) nameserver = a.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = i.root-servers.net
j.root-servers.net      internet address = 192.58.128.30
k.root-servers.net      internet address = 193.0.14.129
l.root-servers.net      internet address = 199.7.83.42
伺服器: UnKnown
Address: 220.134.115.14

version.bind      text =

                "Microsoft DNS 6.1.7601 <1DB15B4F>"
```

隱藏 DNS Server version for bind

- * 修改 bind 設定檔

~# vi /etc/named.conf

```
options {
```

```
    version "None of your business";
```

- * 重啟 bind server

~# systemctl restart named

```
D:\>nslookup -class=chaos -query=txt version.bind 163.28.16.46
伺服器: UnKnown
Address: 163.28.16.46

version.bind      text =
                  "None of your business"
version.bind      nameserver = version.bind
```

隱藏 DNS Server version for Windows

* dnscmd /config /EnableVersionQuery 0

```
D:\>nslookup -class=chaos -query=txt version.bind 220.134.115.14
(root) nameserver = k.root-servers.net
(root) nameserver = l.root-servers.net
(root) nameserver = m.root-servers.net
(root) nameserver = a.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = i.root-servers.net
(root) nameserver = j.root-servers.net
k.root-servers.net      internet address = 193.0.14.129
l.root-servers.net     internet address = 199.7.83.42
m.root-servers.net     internet address = 202.12.27.33
伺服器: Unknown
Address: 220.134.115.14

DNS request timed out.
  timeout was 2 seconds.
*** 對 Unknown 的要求逾時
```



簡報完畢
謝謝