110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：莊永裕教授
- 網路組組長：謝宏昀教授
- 報告人：游子興、李墨軒

大綱

* 1.經費與人力
* 2.網路管理
* 3.資安服務
* 4.特色服務
* 5.成效精進
* 6.基礎維運
* 7.對連線學校服務的支持度
* 8.未來營運計畫

1.1 區網經費

年度	教育部核定	實支總額	人事費繳回	達成率	扣除繳回達成率
107	1,720,000	1,577,987	51,040	91.74%	95%
108	1,720,000	1,714,788	5,097	99.69%	99.99%
109	1,620,000	1,548,009	6,7841	96%	96%
110	1,792,000	1,530,130 (11月)	0	98% (預估)	98% (預估)

* 109年因新聘助理薪資級距與前任不同，人事費部分繳回

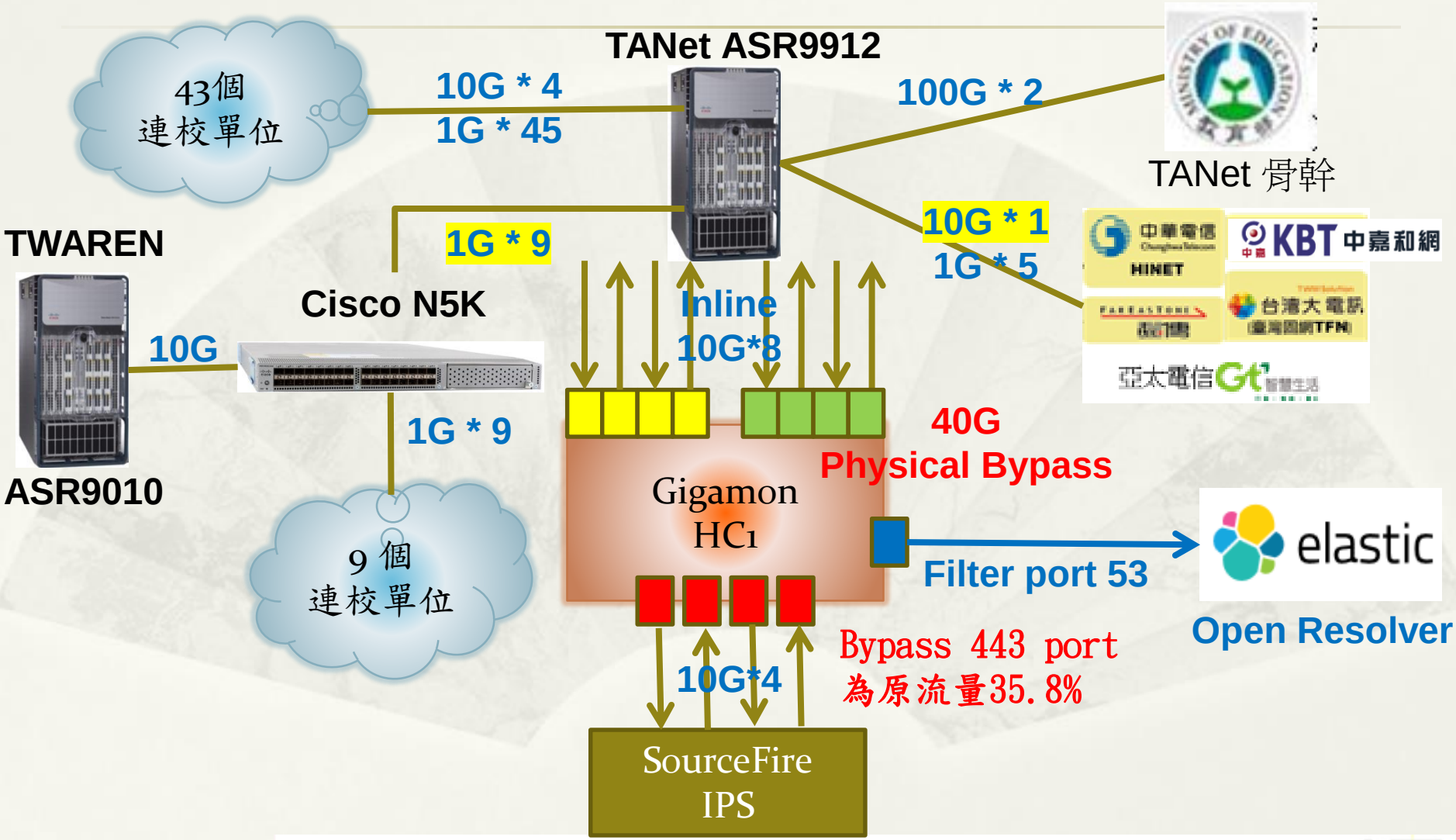
1.2 區網人力

* 計資中心主任：莊永裕教授
  * E-mail：cyy@csie.ntu.edu.tw
  * 電話：(02) 33665001
* 網路組組長：謝宏昀教授
* 網管負責人：游子興
  * E-mail：davisyou@ntu.edu.tw
  * 電話：(02) 33665008
* 資安負責人：李墨軒
  * E-mail：molee@ntu.edu.tw
  * 電話：(02) 33665012
* 編制內專職及約聘僱人員8名

2.網路管理

* 1.網路架構
* 2.網路流量
* 3.IPv6 完成率
* 4.TANet 100G 骨幹斷線說明

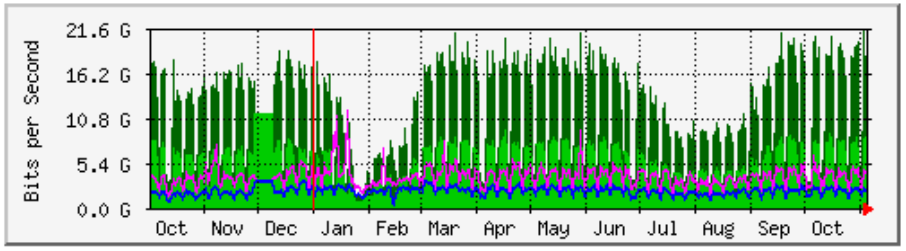
2.1 網路架構


43個
連校單位
10G * 4
1G * 45
TANet ASR9912
100G * 2
TANet 骨幹
10G * 1
1G * 5
TWAREN
1G * 9
Cisco N5K
Inline
10G*8
10G
ASR9010
1G * 9
9 個
連校單位
40G
Physical Bypass
Gigamon
HC1
Filter port 53
elastic
Open Resolver
Bypass 443 port
為原流量35.8%
10G*4
SourceFire
IPS

2.2 網路流量

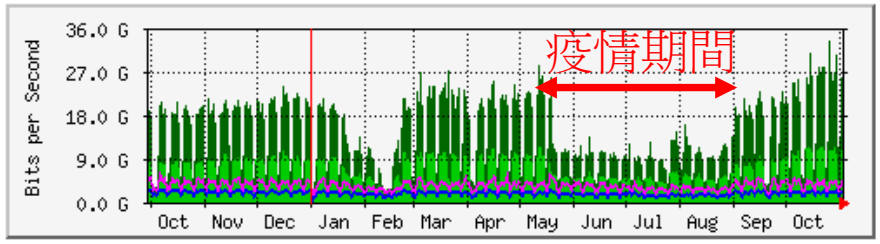
IPv4 流量

每年 圖表 (1 天 平均) 2020



	最大	平均	目前
台北主節點 => 北區區網	21.3 Gb/秒 (21.3%)	5352.9 Mb/秒 (5.4%)	8451.7 Mb/秒 (8.5%)
北區區網 => 台北主節點	11.5 Gb/秒 (11.5%)	1958.4 Mb/秒 (2.0%)	2076.6 Mb/秒 (2.1%)

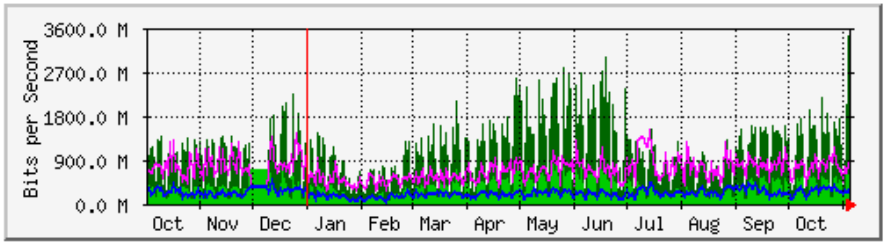
`Yearly' Graph (1 Day Average) 2021



	Max	Average	Current
台北主節點 => 北區區網	33.2 Gb/s (33.2%)	6115.1 Mb/s (6.1%)	10.8 Gb/s (10.8%)
北區區網 => 台北主節點	6075.9 Mb/s (6.1%)	1676.6 Mb/s (1.7%)	1825.1 Mb/s (1.8%)

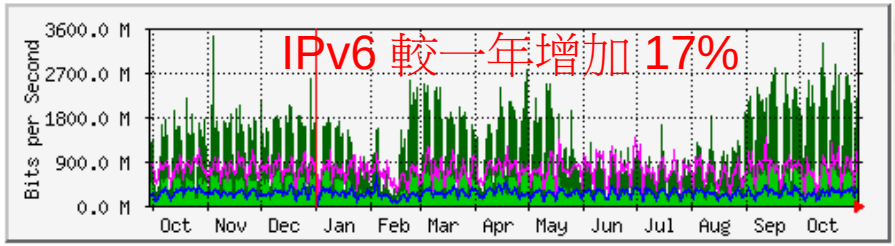
IPv6 流量

每年 圖表 (1 天 平均) 2020



	最大	平均	目前
台北主節點 => 北區區網	3431.8 Mb/秒 (3.4%)	320.0 Mb/秒 (0.3%)	566.0 Mb/秒 (0.6%)
北區區網 => 台北主節點	1476.4 Mb/秒 (1.5%)	204.3 Mb/秒 (0.2%)	301.4 Mb/秒 (0.3%)

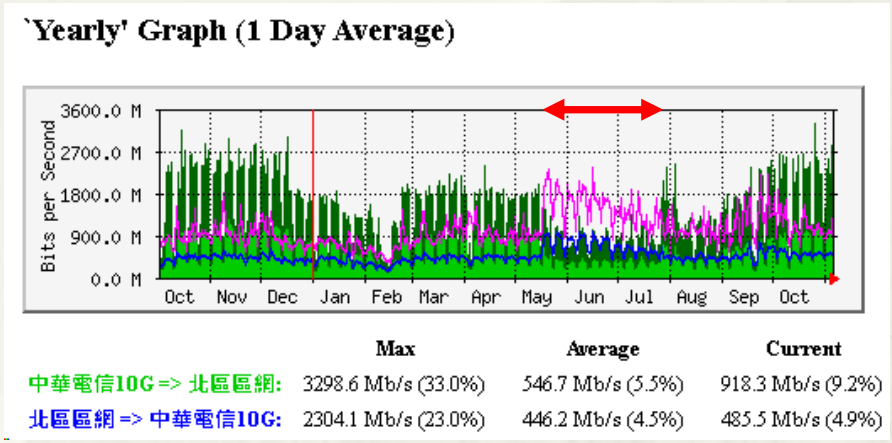
`Yearly' Graph (1 Day Average) 2021



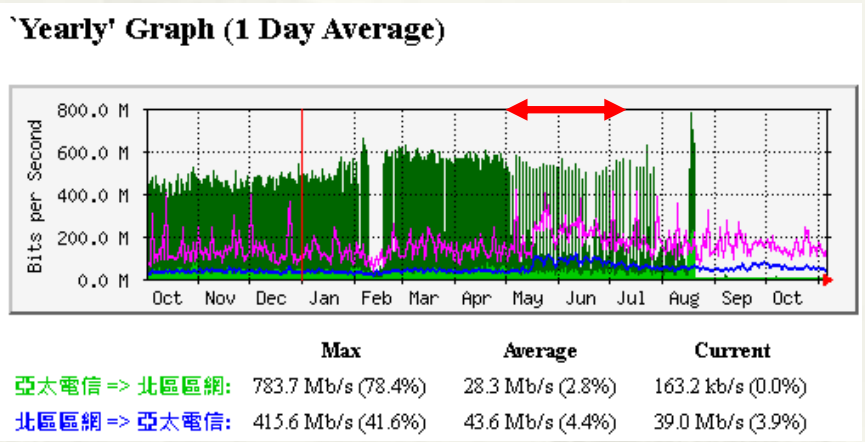
	Max	Average	Current
台北主節點 => 北區區網	3431.8 Mb/s (3.4%)	372.0 Mb/s (0.4%)	732.0 Mb/s (0.7%)
北區區網 => 台北主節點	1361.6 Mb/s (1.4%)	232.1 Mb/s (0.2%)	270.7 Mb/s (0.3%)

疫情期間 ISP Peer 網路流量

* 中華電信: Upload > Download

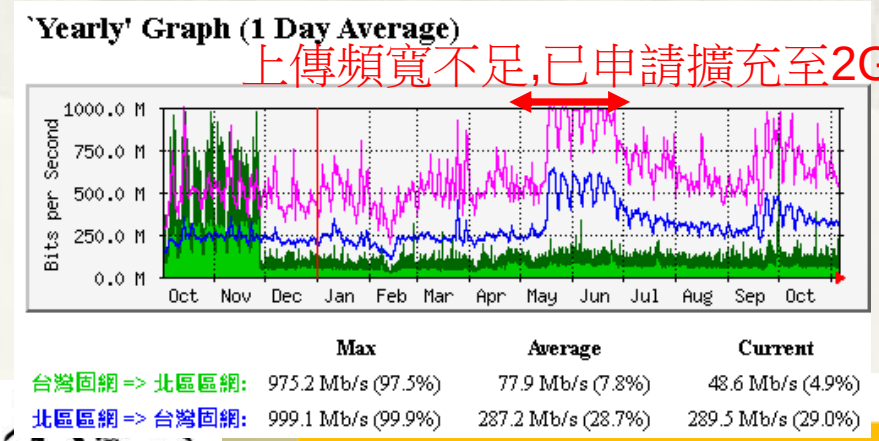


* 亞太電信: Upload > Download

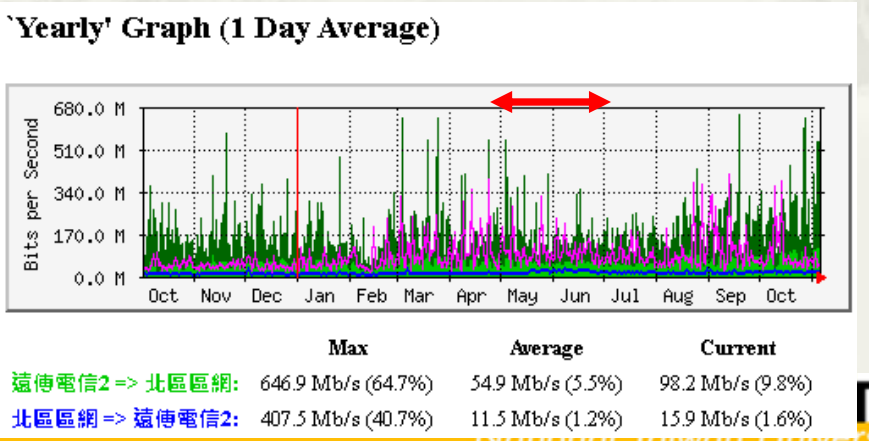


* 台灣固網: Upload > Download

上傳頻寬不足,已申請擴充至2G

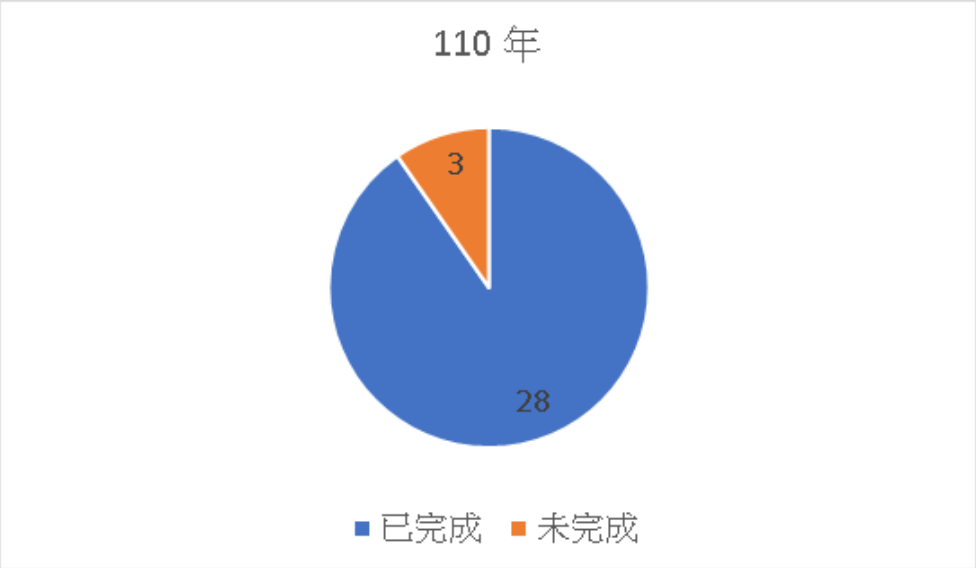


* 遠傳電信: 無明顯變化



2.3 IPv6 大專院校完成率

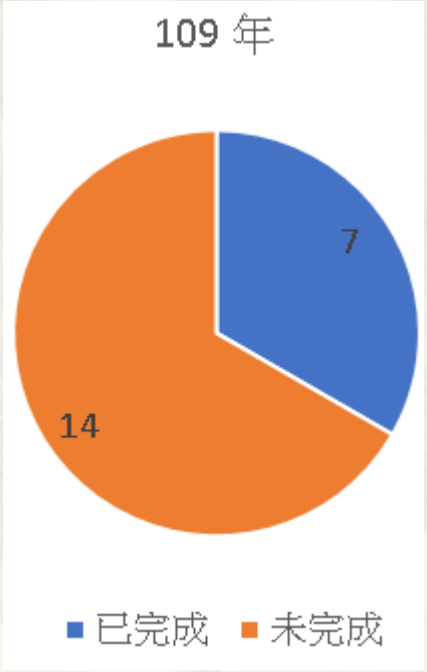
* 路由網段設定完成率
  * 大專院校: 31

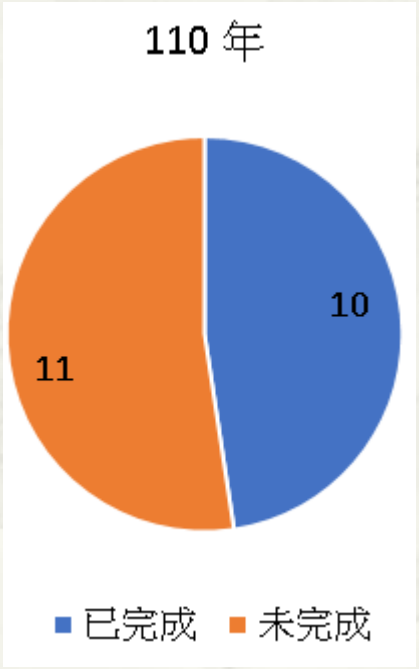


尚未完成:
台北海洋科技大學: 兩個校區，協調中
軍事情報局學校: 無 ipv6配發，申請中
臺北基督學院: 無 ipv6 配發，申請中

IPv6 高中職完成率

* 路由網段設定完成率
  * 高國中小及其他單位: 21





109年評審委員建議:

2.高中職及國小等完成比率較低，建議可規劃逐年達成。

8.轄屬高中職以 學校 IPv6達成率偏低，請後續提出具體行動方案

2.4 TANet 100G 骨幹斷線說明 2021/07/30 1小時40分

* 7/29 10:39 台大-新竹主節點100G電路沒有流量, 原預計7/30 下午前往台大查修.
  * 原因: Cisco ASR 100G-CK-C卡板 故障
  * NOC 公告 https://noc.tanet.edu.tw/index.php/operation-announcement/op-a/op-a-01/1308-7-29-10-39-100g
* 7/30 11:46 僅剩的 100G 電路 台大-台北主節點 也發生斷線
  * 原因: 亞太光纜斷線
  * NOC 公告 https://noc.tanet.edu.tw/index.php/operation-announcement/op-a/op-a-01/1307-7-30-11-46-t1-a7-a4
* 因此導致 07/30 11:46 ~ 13:25 台大區網骨幹100G 斷線共約 1小時40分
* **改善建議: 此次斷線原因，一為設備故障，另一為線路故障，因此若能在發生故障當下，將正常線路接於正常100G卡版上，則可大幅減少斷線時間。**

3.資安服務
107~110年度資安事件統計

	107	108	109	110
1、2級資安事件處理			維持高效率	
通報平均時數	1.343 小時	0.586 小時	0.04 小時	0.05 小時
應變處理平均時數	0.026 小時	0.017 小時	0.05 小時	0.86 小時
事件處理平均時數	1.369 小時	0.602 小時	0.74 小時	1.42 小時
通報完成率	99.86%	99.969%	100 %	99.89 %
事件完成率	99.92%	99.627%	100%	100%
3、4級資安事件通報	無	無	無	無
資安事件通報審核平均時數	0.519小時	0.206小時	1.12小時	0.55小時
資料更新完整校數	73.47%	81.633%	97.04%	100%

109年評審委員建議:

1.資安事件通報審核平均時數及資訊完整度，尚有精進空間。

6.所屬單位資訊完整度及審核時效未臻理想，請研議後續改善方式。

3.資安服務
連線學校

* 資安事件通報
  * 轄下單位自行通報資詢
  * 提供處理協助
* 弱掃平台使用
  * 定期確認平台中未複測的中高風險網站，並通知該單位處理
  * 預計舉辦弱掃報告分析之教育訓練
* 威脅清單
  * 提供威脅清單給連線學校

北區 A-SOC 合作
DDoS 導流清洗時部份服務異常

* 被導流清洗網段
  * Line: 無法登入
  * 部份國外網站連線異常，但 Ping/TraceRoute 卻都正常:
    * Amazon, GitHub, Yahoo日本, 日本首相官網 等
* 測試結果
  * 非 DDoS 清洗設備造成: Bypass 設備依然如此
  * 於 Client or Server 設定 MTU ≦ 1492 即可正常連線

MTU	可否順利連線
1500	否
1493	否
1492	可
1000	可

北區 A-SOC 合作
DDoS 導流清洗時部份服務異常

- Alternative Solution
  - 調整本機網卡 MTU ≦ 1492
  - 於 防火牆/Router 調整 TCP Maximum Segment Size (MSS) ≦ 1452
    - 防火牆 Pfsense: MSS clamping
    - Cisco Router: (config-if)# ip tcp adjust-mss 1360
  - Client

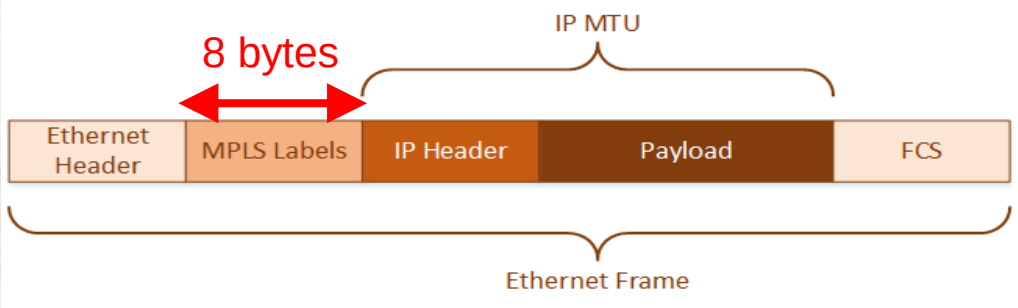
No.	Time	tcp.stream	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
1850	10.679127	10	172.16.0.17	52333	163.28.16.200	3389	TCP	66	52333 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1852	10.680699	10	163.28.16.200	3389	172.16.0.17	52333	TCP	66	3389 → 52333 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1360 WS=1 SACK_PERM=1
1853	10.680751	10	172.16.0.17	52333	163.28.16.200	3389	TCP	54	52333 → 3389 [ACK] Seq=1 Ack=1 Win=262400 Len=0

  - Server

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
771	3.196712	140.112.3.82	35276	163.28.16.200	3389	TCP	66	35276 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1360 WS=256 SACK_PERM=1
772	3.196843	163.28.16.200	3389	140.112.3.82	35276	TCP	66	3389 → 35276 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1
773	3.198009	140.112.3.82	35276	163.28.16.200	3389	TCP	60	35276 → 3389 [ACK] Seq=1 Ack=1 Win=262400 Len=0

DDoS 導流清洗時部份服務異常根因分析(推測)

* MPLS MTU
  * Adding two labels, of 4 bytes each, means that the packet with labels is **1508 bytes**.



* DDoS 導流方法為使用 MPLS 路由將異常流量經新竹主節點導入清洗機，推測為途中某節點未將 MTU 預設 1500 bytes 調整至 1508 bytes，導致部分封包中途被丟棄所致。

4.特色服務
樹莓派網路品質監控系統

* 網管面臨挑戰
  * 使用者反應網路偶有異常斷線、網速過慢等情況
  * 骨幹網路監控無法呈現使用者情況
* 樹莓派網路品質監控系統
  * 以使用者角度長期記錄網路量測數據
  * ELK Heartbeat: ICMP ping、RTT 量測、HTTP GET/POST Delay Time
  * 網頁測速: Speed Test

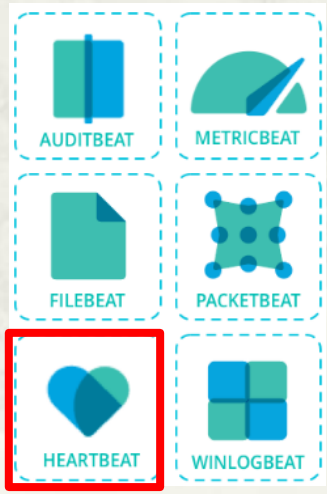
樹莓派網路品質監控系統架構圖

佈建於使用者端

佈建於計中機房

Selenium + Python

ELK Beats



SPEEDTEST

台大網頁測速

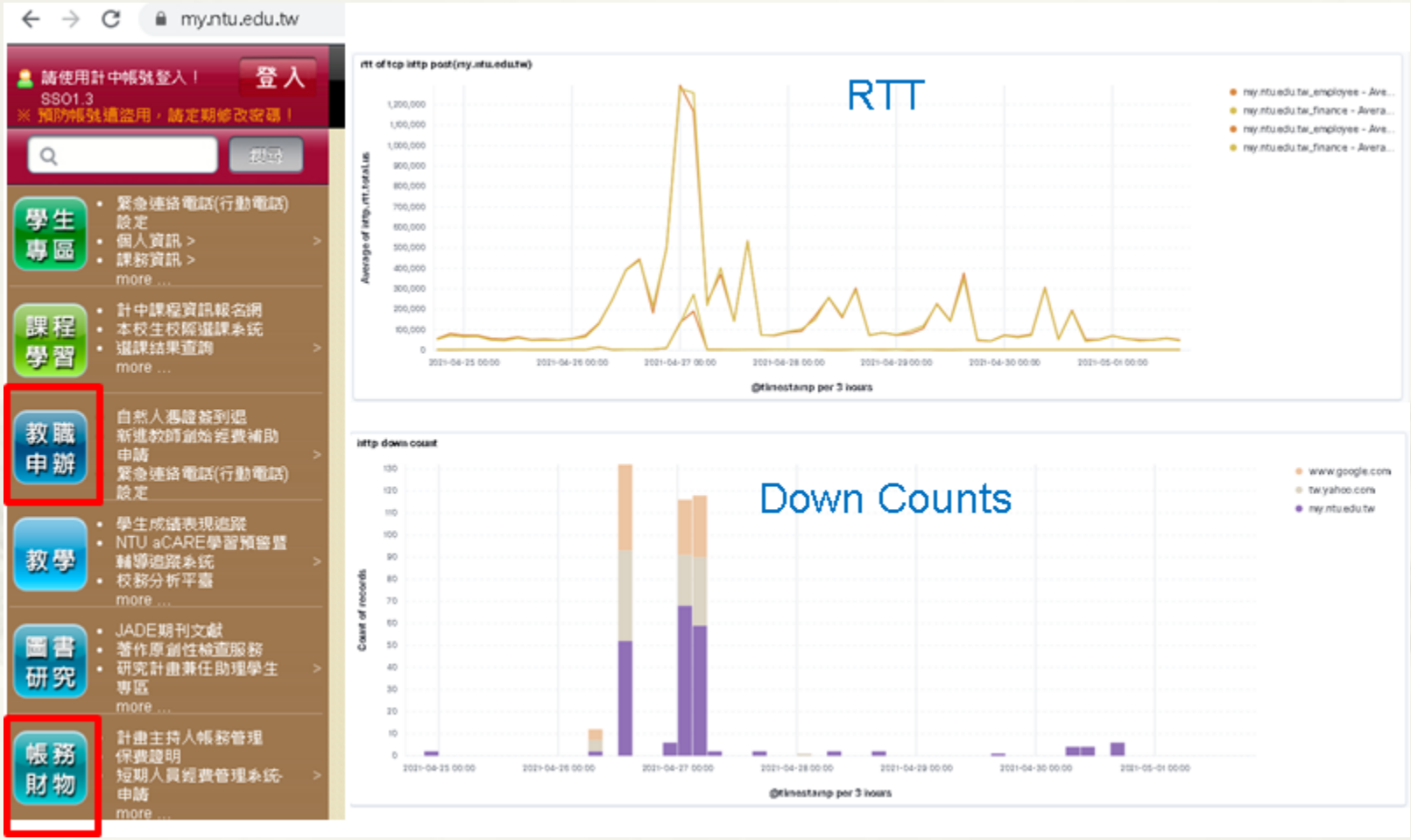
ICMP Ping

HTTP GET/POST

樹莓派網路品質監控系統

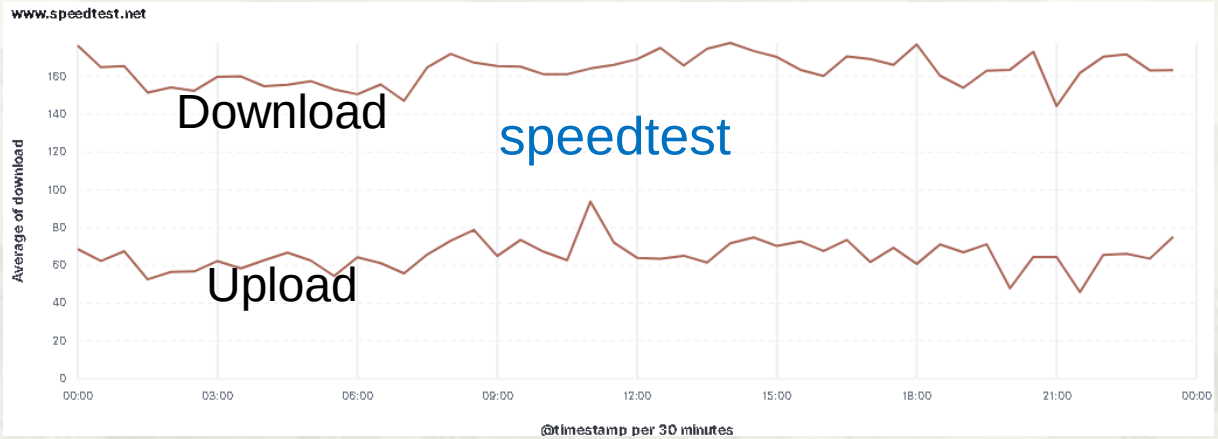
* 使用樹莓派建置優點
  * 成本低 < $2000
  * 低耗電 < 10Walt
  * 體積小佈建容易
  * 支援有線與無線網路監控

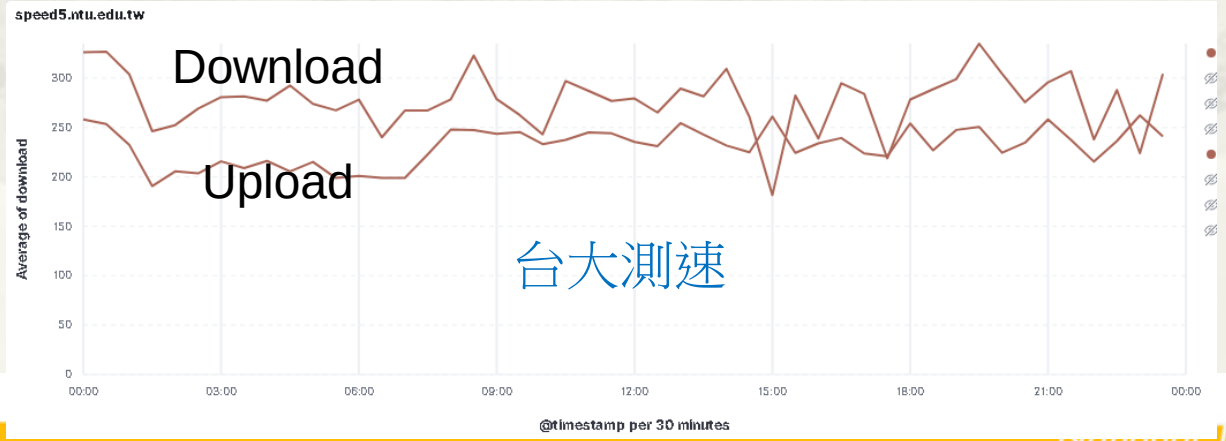
校務系統監控


my.ntu.edu.tw
請使用計中帳號登入！
登入
SSO1.3
※ 預防帳號遭盜用，請定期修改密碼！
搜尋
學生專區
緊急連絡電話(行動電話)設定
個人資訊 >
課務資訊 >
more ...
課程學習
計中課程資訊報名網
本校生校際選課系統
選課結果查詢
more ...
教職申辦
自然人憑證簽到退
新進教師創始經費補助申請
緊急連絡電話(行動電話)設定
教學
學生成績表現追蹤
NTU aCARE學習預警暨輔導追蹤系統
校務分析平臺
more ...
圖書研究
JADE期刊文獻
著作原創性檢查服務
研究計畫兼任助理學生專區
more ...
帳務財物
計畫主持人帳務管理
保費證明
短期人員經費管理系統-申請
more ...
RTT
Down Counts

網路測速

* speedtest http://www. speedtest.net
* 台大測速 http://speed5.ntu.edu.tw/





5.成效精進

109年評審委員建議與回覆

No	委員建議	回覆
1	網路中心及連線學校資安事件緊急通報處理之效率、通報率及聯絡相關資訊完整度，其完成率皆達100%，完成平均時間皆在一小時內，已有逐年 精進值得鼓勵。但資安事件通報審核平均時數：1.12小時，同時資訊完整度：97.04%，尚有精進空間。	110年資安事件通報審核平均時數已從1.12小時降低至0.55小時，資訊完整度已從97.04%提高至100%
2	IPv6之推動，已經完成28所大專院校，尚有3所未完成，同時高中職及國小等完成比率較低，建議可規劃逐年達成。	110年高中職及其他單位由原來7個增加至10個
3	滿意度調查問卷回復比率為75%，似乎偏低，可在加強。同時針對網路連線服務的順暢度，有部分勾選普通，建議可多加了解改善之。	110年滿意度調查回覆率 52連線單位，收到46份回覆，回覆率88%。另外因問卷調查回覆皆為匿名，無法確切得知該單位，唯今年問卷回覆順暢度，較去年已有改善。

109年評審委員建議與回覆

No	委員建議	回覆
4	DNS 版本更新部分，未見著墨，建議將其推動狀況列出，盡速規劃逐年完成。	110年配合教育部政策進行 DNS RPZ 導入工作，經問卷調查回覆，所有單位皆使用 Bind v9 以上，未有使用太舊版本之情況。
5	針對 110年營運僅列出大綱，建議訂定量化之 KPI 值，以利執行及檢視。	網路妥適率99%以上 區網網管會議出席率 90%以上 大專院校 ipv6 使用率100% 高國中小 ipv6 使用率60%以上 區網課程受訓實質效益分析:50%以上課程需進行前測與後測、前測與後側分數進步平均達 20%以上 資安相關文件範本: 至少完成五份以上資安相關文件

109年評審委員建議與回覆

No	委員建議	回覆
6	109年資通安全通報應變平台之所屬學校及單位的聯絡相關資訊完整度及審核時效未臻理想，請研議後續改善方式。	110年資安事件通報審核平均時數已從 1.12 小時降低至 0.55 小時，資訊完整度已從 97.04% 提高至 100%
7	區網管理會本年出席率過低，請探討原因及研議後續改善方式。	110年區網會議共有43個單位參加，出席率為 83%
8	轄屬高中職以 學校 IPv6達成率偏低，請後續提出具體行動方案。	110年大專院校 3間 高中職及其他單位由原來7個增加至10個
9	台北區網 (一)係擔負北區資安監控中心重要角色，建議未來可將營運績效及貢獻適度納入特色服務論述。	與北區 A-SOC 合作找出DDoS導流清洗時部份服務異常之原因與解決方法。 資安卓越中心計畫實習場域建置專案與北區 A-SOC 共同執行

109年評審委員建議與回覆

No	委員建議	回覆
10	教育訓練的部分可以強化在實務能力提升的指標設定與達成。	110年資安相關課程，皆預計安排前測與後測，可藉此衡量學習情況。
11	在資安防護技術提升的教育訓練可以強化上線練習的課程。	110年資安相關課程，皆預計安排前測與後測，可藉此衡量學習情況。
12	設定管理委會會議的目的，尋求共識與努力的目標。	資安力度逐年增加，人力與經費皆未增加的情況下，連線單位可共同防禦、共享資源，例如於資安檢核方法共用 GCB Template，技服 IP/DNS 黑名單於骨幹進行防禦等

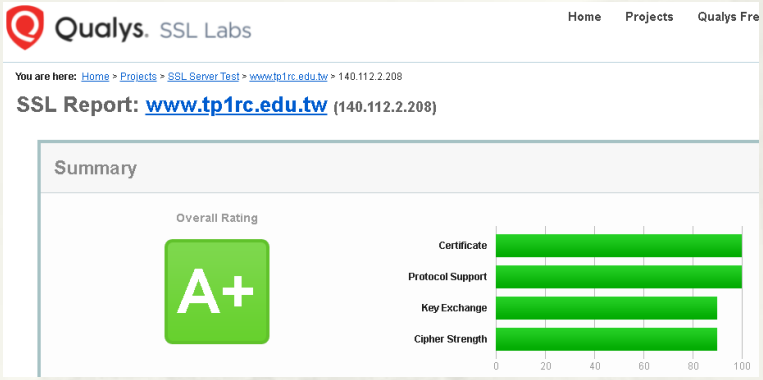
6.基礎維運

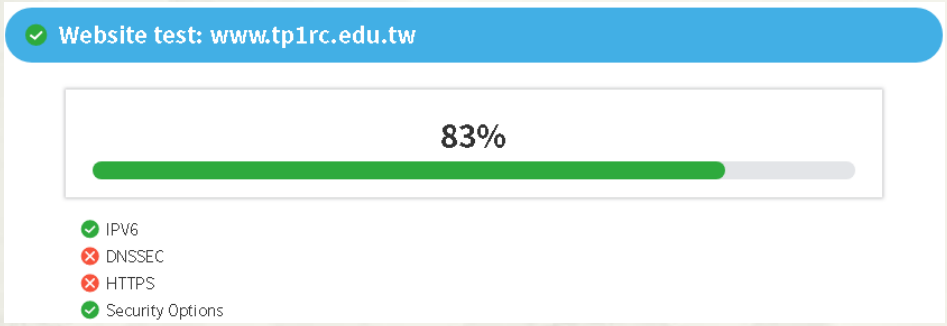
配合教育部政策
連線單位 HTTPS 檢測結果 (未通過)

檢測單位	連線單位名稱	對外網站 網域名稱(或網址)		檢測項目(通過請打V，未通過留空白)		
			certificate chains	domain name on certificate	Portocols (TLS 應 1.2 以上)	HTTP 重導向 HTTP
台北區網I	康寧大學	www.ukn.edu.tw	V	V	TLSv1.0 SSLv3	V
台北區網I	臺北市教育網路	www.doe.gov.taipei	V	V	V	No
台北區網I	真理大學	www.au.edu.tw	V	V	TLSv1.0	V
台北區網I	臺北商業大學	www.ntub.edu.tw	*.ntub.edu.tw RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1	V	TLSv1.0	V
台北區網I	臺灣師範大學(公館校區)	www.ntnu.edu.tw	V	V	TLSv1.0	V
台北區網I	國防醫學院	www.ndmctsgh.edu.tw	V	V	TLSv1.0	V
台北區網I	大學入學考試中心	www.ceec.edu.tw	*.ceec.edu.tw TWCA Secure SSL Certification Authority	V	V	X
台北區網I	台北護理健康大學	www.ntunhs.edu.tw	V	V	TLSv1.0	V
台北區網I	新北市私立東海高中	www.thhs.ntpc.edu.tw	V	V	TLSv1.0	V
台北區網I	復興實驗高中	www.fhjh.tp.edu.tw	*.fhjh.tp.edu.tw Sectigo RSA Domain Validation Secure Server CA	V	V	No
台北區網I	國北教大實小	www.ntueees.tp.edu.tw	www.ntueees.tp.edu.tw 政府伺服器數位憑證管理中心 - G1	V	V	V
台北區網I	能仁家商	www.nrvs.ntpc.edu.tw	V	V	V	No
台北區網I	清傳高商	www.ccvs.ntpc.edu.tw	V	V	SSLv3	V
台北區網I	開平餐飲	www.kpvs.tp.edu.tw	FortiWAN	FortiWAN	TLSv1.0	No
台北區網I	樹人家商	www.stgvs.ntpc.edu.tw	V	V	V	No
台北區網I	私立協和祐德高中	www.hhvs.tp.edu.tw	V	V	V	No
台北區網I	中華民國高級中等學校體	www.ctssf.org.tw	V	V	TLSv1.0	No
台北區網I	臺北基督學院	www.cct.edu.tw	www.cct.edu.tw R3	V	TLSv1.0	V
台北區網I	臺灣科技大學	www.ntust.edu.tw	*.ntust.edu.tw Sectigo RSA Domain Validation Secure Server CA	V	TLSv1.0 SSLv3	V
台北區網I	臺大醫院	www.ntuh.gov.tw	V	V	V	No

連線單位 HTTPS 檢測支援

* 檢測結果: 臺北區網I

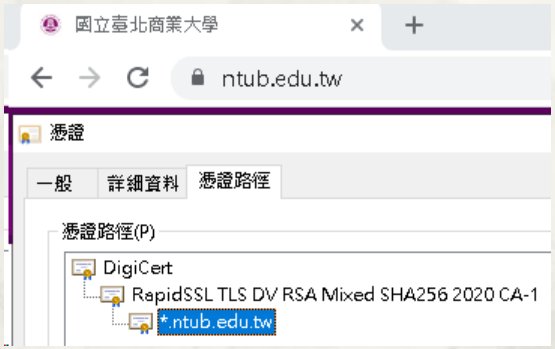




* 於區網課程及網管會議分享
  * HTTPS 免費憑證安裝 Let's Encrypt
    * Certbot: Command Line 自動化安裝工具
    * SSL For Free : 網頁申請
  * HTTPS Certificate Chain 常見問題與解決方法
  * 參考區網技術文件
    * https://www.tp1rc.edu.tw/e1.php

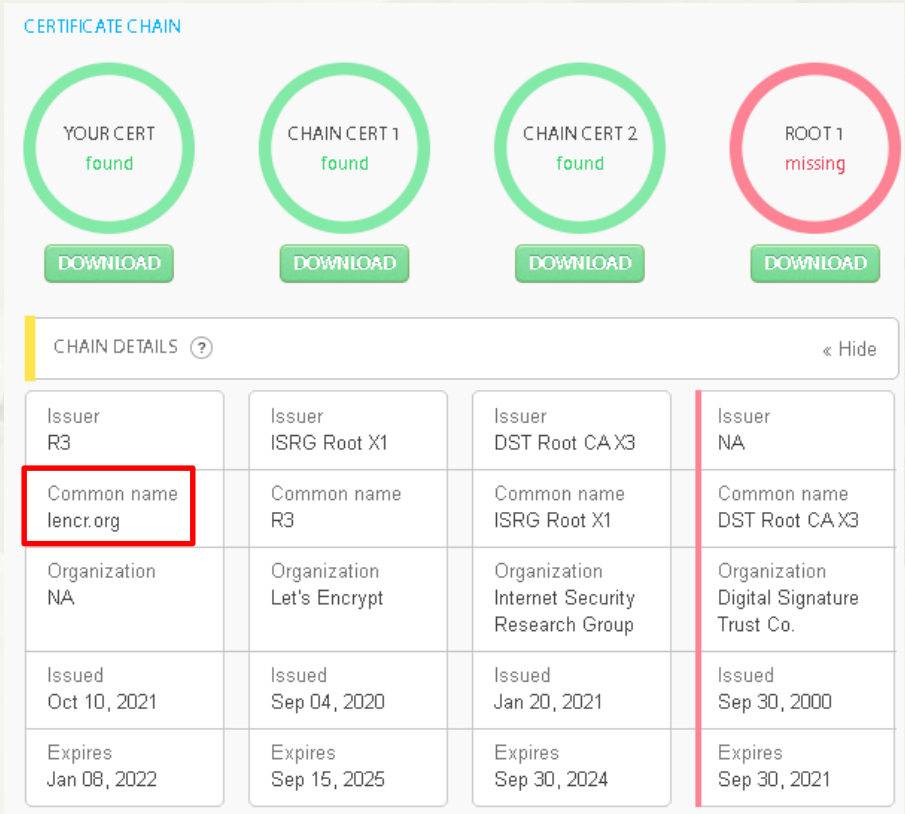
提供錯誤 Intermediate Certificate www.ntub.edu.tw

* https://www.digicert.com/help/
* Chrome 會自行修正

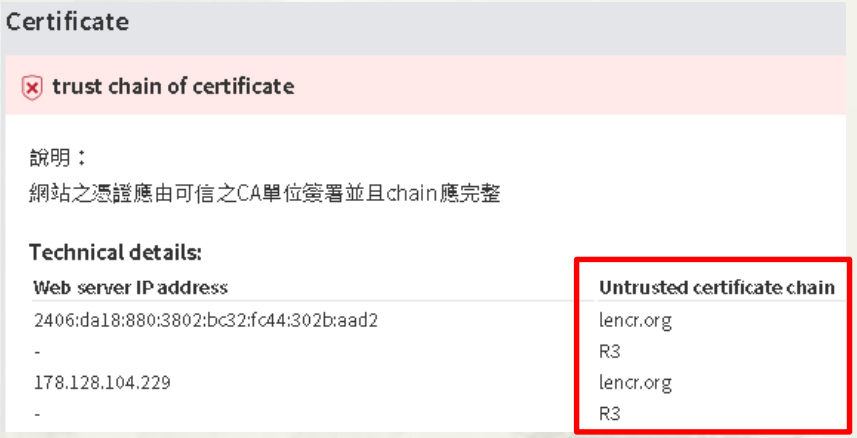


Root Certificate Cross-signed With Expired CA letsencrypt.org

* https://www.sslchecker.com/sslchecker

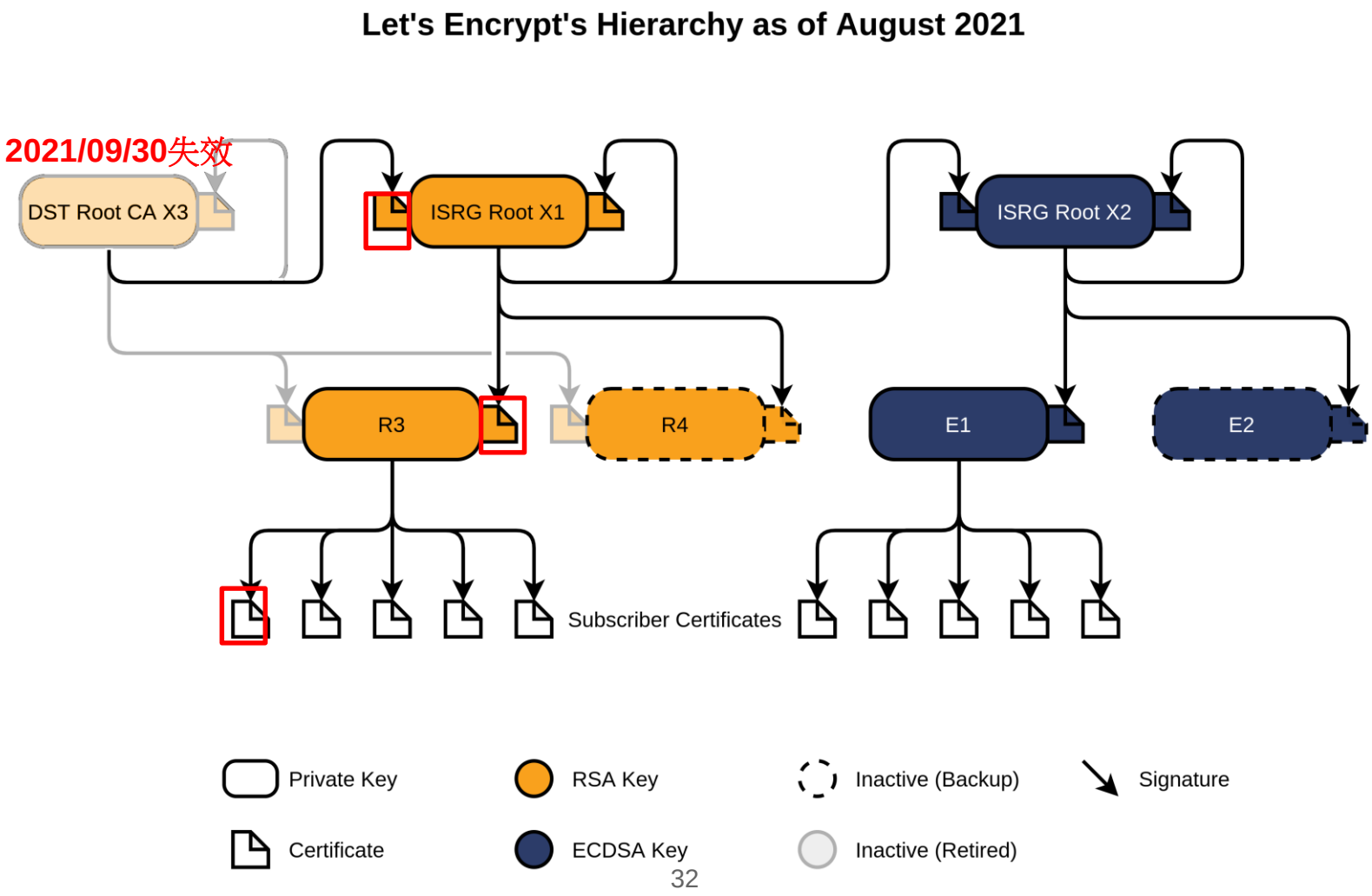


* https://check.twnic.tw/

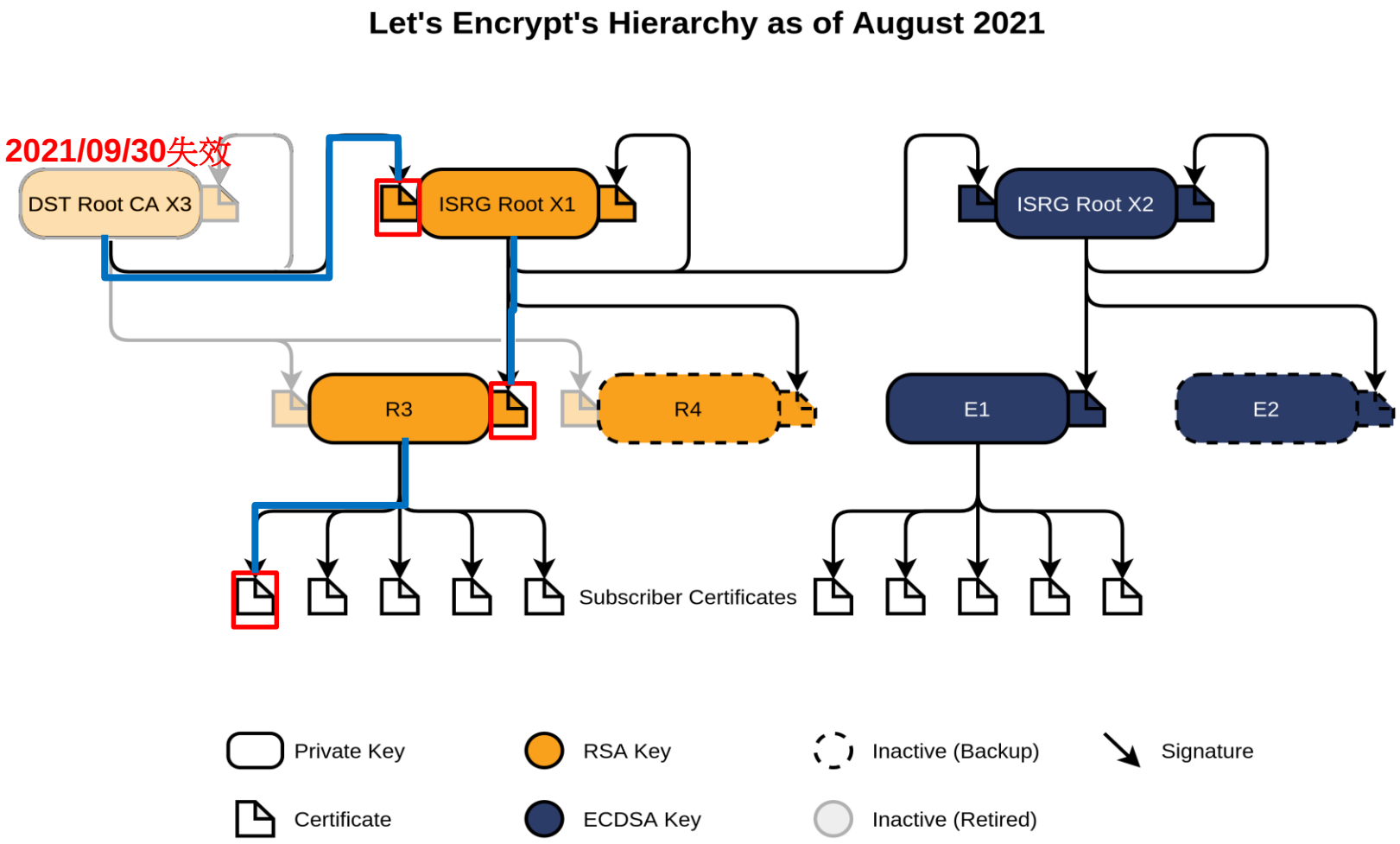


* 所有使用 Let's Encrypt 憑證之網站皆有相同問題
* TANet NOC
  * https://noc.tanet.edu.tw/
* 政大區網
  * https://tp2rc.tanet.edu.tw/
* 交大區網
  * www.hcrc.edu.tw

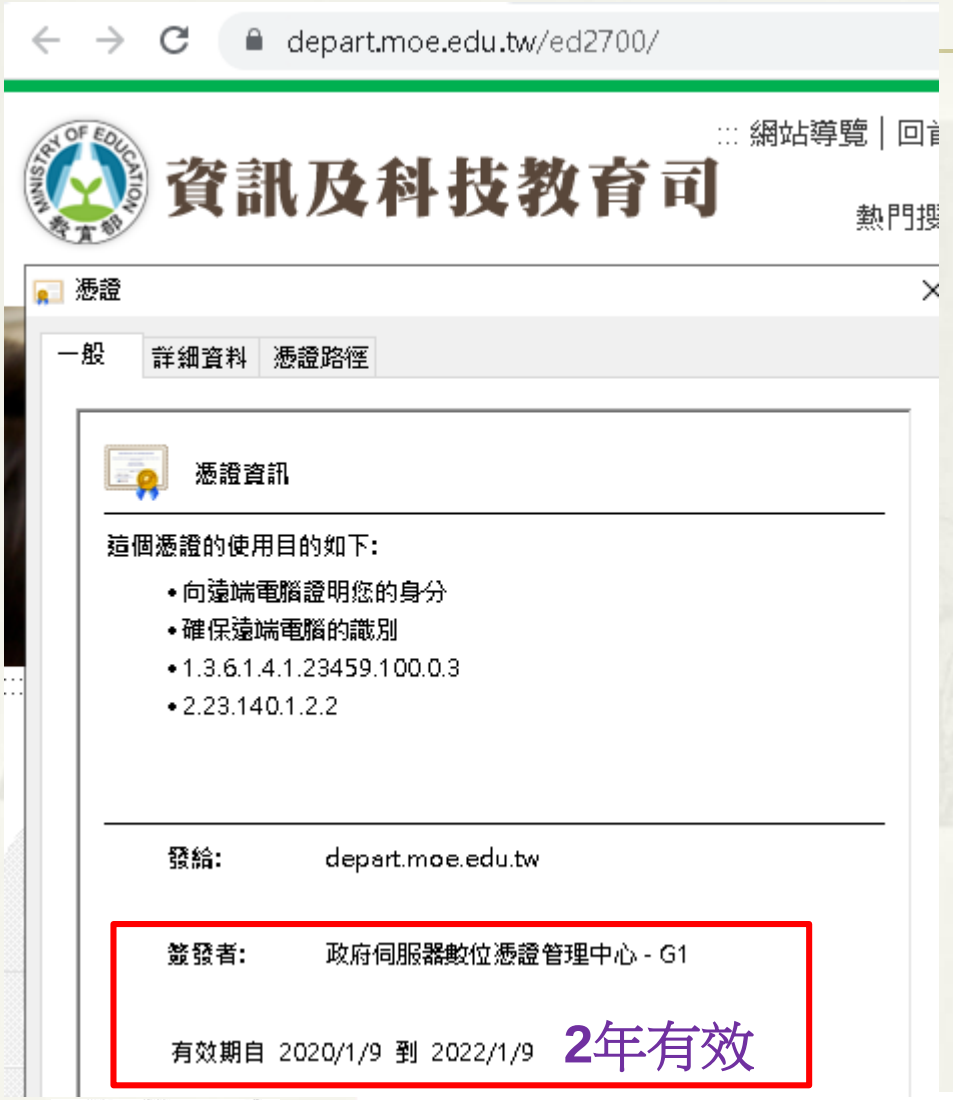
Let's Encrypt Trust Chain



Let's Encrypt Trust Chain



政府數位憑證 vs. 免費憑證



ntu.edu.tw 有效憑證統計

- https://crt.sh/?dNSName=ntu.edu.tw&exclude=expired&match=LIKE&deduplicate=Y
- Criteria
  - Type: Domain Name
  - Match: LIKE Search: 'ntu.edu.tw'
  - Exclude expired certificates
- 搜尋結果: 節錄部分

Criteria	Type: Domain Name Match: ILIKE Search: 'ntu.edu.tw' Exclude expired certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5062274139	2021-08-18	2021-08-18	2021-11-16	mail.nems.ntu.edu.tw	mail.nems.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5062272221	2021-08-18	2021-08-18	2021-11-16	mail.nems.ntu.edu.tw	mail.nems.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5064096093	2021-08-18	2021-08-18	2021-11-16	rec.ord.ntu.edu.tw	rec.ord.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5064095977	2021-08-18	2021-08-18	2021-11-16	rec.ord.ntu.edu.tw	rec.ord.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5099018356	2021-08-24	2021-08-24	2021-11-22	bach.ee.ntu.edu.tw	bach.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5099017018	2021-08-24	2021-08-24	2021-11-22	bach.ee.ntu.edu.tw	bach.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108973743	2021-08-26	2021-08-26	2021-11-24	nhi2.cph.ntu.edu.tw	nhi2.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108974572	2021-08-26	2021-08-26	2021-11-24	nhi2.cph.ntu.edu.tw	nhi2.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108872153	2021-08-26	2021-08-26	2021-11-24	nhi.cph.ntu.edu.tw	nhi.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108872028	2021-08-26	2021-08-26	2021-11-24	nhi.cph.ntu.edu.tw	nhi.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108947902	2021-08-26	2021-08-26	2021-11-24	phst.cph.ntu.edu.tw	phst.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5108947357	2021-08-26	2021-08-26	2021-11-24	phst.cph.ntu.edu.tw	phst.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5150559026	2021-09-02	2021-09-02	2021-12-01	gsat.ntu.edu.tw	gsat.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5150558834	2021-09-02	2021-09-02	2021-12-01	gsat.ntu.edu.tw	gsat.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5167528652	2021-09-05	2021-09-05	2021-12-04	schumann.ee.ntu.edu.tw	schumann.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5167528854	2021-09-05	2021-09-05	2021-12-04	schumann.ee.ntu.edu.tw	schumann.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172388297	2021-09-06	2021-09-06	2021-12-05	brahms.ee.ntu.edu.tw	brahms.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172387100	2021-09-06	2021-09-06	2021-12-05	brahms.ee.ntu.edu.tw	brahms.ee.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
5172837705	2021-09-06	2021-09-06	2021-12-05	chps.cph.ntu.edu.tw	chps.cph.ntu.edu.tw	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

ntu.edu.tw 有效憑證統計

Issuer Name	計數	%
C=US, O=Let's Encrypt, CN=R3（免費）	507	68
C=TW, O=TAIWAN-CA, OU=Secure SSL Sub-CA, CN=TWCA Secure SSL Certification Authority	114	15
C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"	44	6
C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA（免費）	26	3
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA	19	3
C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA	13	2
C=TW, O="Chunghwa Telecom Co., Ltd.", OU=Public Certification Authority - G2	7	1
C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2	7	1
C=US, O=Google Trust Services LLC, CN=GTS CA 1D4	4	1
C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3	3	0
C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2	3	0
C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R3 DV TLS CA 2020	1	0
C=TW, O=TAIWAN-CA, OU=Global EVSSL Sub-CA, CN=TWCA Global EVSSL Certification Authority	1	0
C=US, O=DigiCert Inc, CN=GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1	1	0
C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust EV RSA CA 2018	1	0
總計	751	

ntu.edu.tw 有效憑證統計

* 統計結果

類別	總數	百分比 %
免費	533	71
付費	218	29

* 付費憑證報價: https://www.twca.com.tw/sslService

* .ntu.edu.tw 一年付費憑證費用

218 * 3780 = $824,040

(若使用"政府數位憑證"每年可省)

配合教育部政策
DNS RPZ 導入

* 2021/09 調查結果已有4個單位導入完成
* 後續建置之建議
  * 與 DNSSEC 衝突
    * 若 Client 啟用 DNSSEC 將無法接受 RPZ 更改後之 DNS 記錄
  * 使用 Zone Transfer 方式同步記錄
    * 非加密傳輸協定，途中可能經過竄改
    * 供應鏈攻擊，將正常網站 IP 導向惡意網站
  * 不支援Windows DNS Server
    * 經統計約有 20% 連線單位使用Windows DNS Server
  * 考慮建置 TANet 專屬 RPZ Server
    * 目前 TWNIC RPZ 僅有八筆記錄(https://rpz.twnic.tw/e.html)，防護效果有效
    * 應考慮支援：內政部警政署刑事警察局每月非法網站清單、技服黑名單、TANet 侵權黑名單

7.對連線學校服務的支持度

* 1. 110年度區網暑期課程
* 2.區網網管會議
* 3.滿意度調查

110年度區網課程(10門)

分類	日期	講題	講者	名額	報名
法規	08/18（線上）	網路教學與著作權法的關聯	劉灝宇	100	66
法規	08/20（線上）	面對資安法：如何做好第一道防線？認識法規與制度	曾品媛協理(安永企管諮詢)	100	115
法規	08/25（線上）	資安法資訊系統分級分類及防護基準說明	黃承漢	100	145
法規	08/27（線上）	因應資安稽核：風險管理及稽核受稽核準備	曾品媛協理(安永企管諮詢)	100	151
資安	10/27（實體）	2021年 惡意程式攻擊案例	劉得民老師	40	38

線上課程報名踴躍，不受實體教室座位限制

110年度區網課程(10門)

分類	日期	講題	講者	名額
網路	12/7 (實體)	HTTPS 憑證安裝與原理介紹 1.HTTPS 免費憑證安裝 Let's Encrypt Certbot 2.HTTPS 憑證簽署架構介紹	台大網路組 游子興	80
資安	12/14 (實體)	1.Shodan資料分析 2.OpenSource資安防護搭配snort偵測 3.OpenSource資安防護	1.ASOC林宜進 2.ASOC劉家維 3.台大網路組童鵬哲	80
資安	12/17 (實體)	近期常見入侵案例分享及防駭方法	中華資安 馬洪雯	80
資安	12/21 (實體)	資通安全健診	中山大學 王聖全	80
資安	12/28 (實體)	以藍隊角度探討入侵事件常見問題	詮睿科技 陳昱崇	80

受疫情影響，為了有更好的學習效果
實體課程延後至十二月辦理

110年度區網網管會議

* 109年度出席率:63%　110年度出席率:83%

項目	主持人／報告人	報 告 內 容
109年度	國防大學蔡文君 大考中心、北科大	教育部資通安全稽核技術與經驗分享
110年度	台大電機鄭皓中教授	量子電腦之緣起與現況及未來的應用
110年度	北區 ASOC童鵬哲	DDoS流量清洗現況說明
110年度	游子興	資安檢核GCB 導入案例分享
110年度	游子興	HTTPS Certificate Chain 常見問題與解決方法

109年評審委員建議:

7.區網管理會本年出席率過低，請探討原因及研議後續改善方式

連線單位滿意度調查

* 6 項選擇、2 項簡答
  * 本年度貴單位之網路連線服務，您認為順暢度為何？
  * 本年度貴單位如有網路管理或連線問題時，區網中心的協助是否有順利排除障礙？？
  * 資通安全事件的通報應變的協助處理？
  * 對區網所舉辦之教育訓練或研討(習)課程，是否能符合貴單位實務運作上的需求?
  * 貴單位對於區網中心服務人員之熱忱及親和力的滿意度？
  * 貴單位對於區網中心綜合整體服務的表現？
  * 對區域網路中心在網路維運管理的建議
  * 對區網所舉辦之教育訓練或研討(習)課程建議
* **滿意度調查回覆率**
  * **52連線單位，收到 46 份回覆**
  * **回覆率 88%**

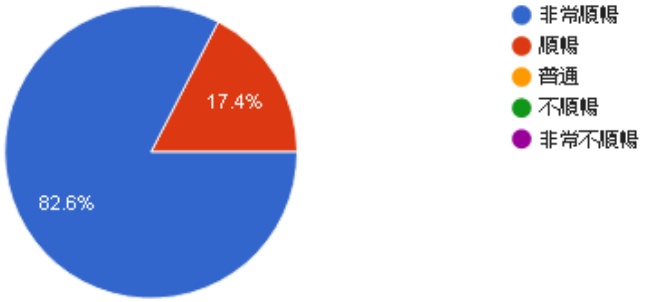
109年評審委員建議:

3.滿意度調查問卷回復比率為 75% ，似乎偏低。

滿意度調查結果 part1

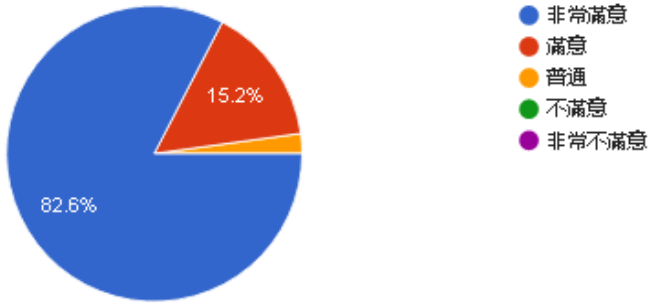
本年度　貴單位之網路連線服務，順暢與否?

46 則回應



資通安全事件的通報應變的協助處理：

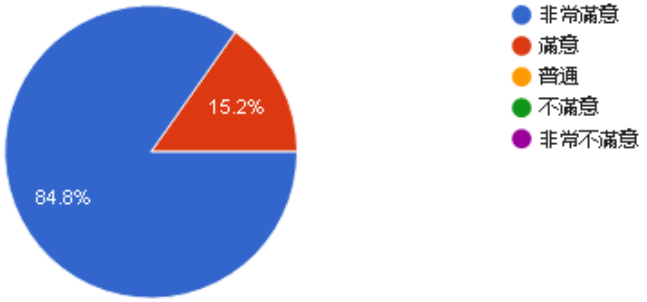
46 則回應



非常滿意佔八成以上

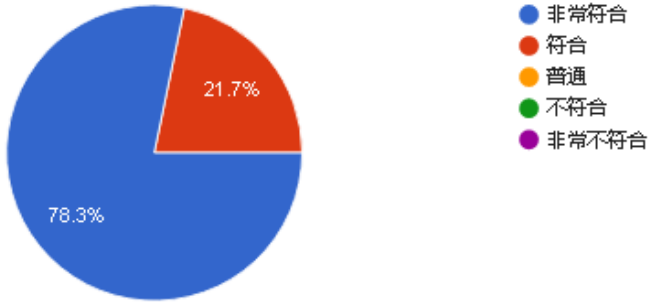
本年度　貴單位如有網路管理或連線問題時，區網中心的協助是否有順利排除障礙?

46 則回應



對區網所舉辦之教育訓練或研習課程，是否能符合　貴單位實務運作上的需求?

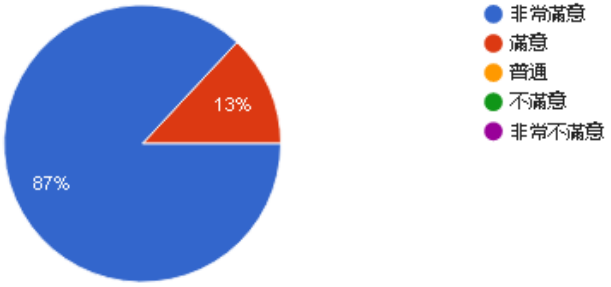
46 則回應



滿意度調查結果 part2

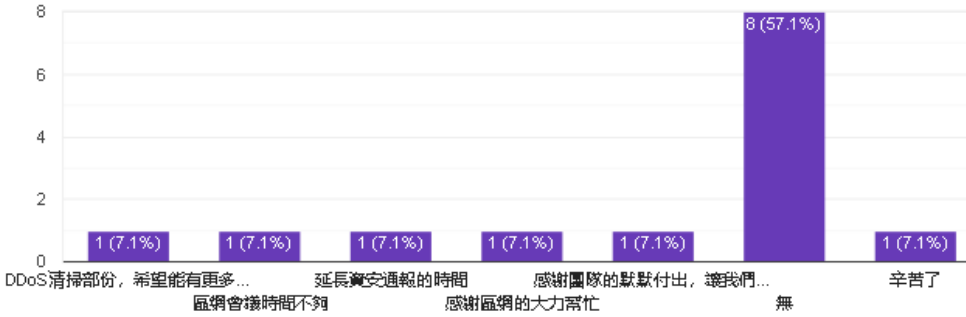
貴單位對於區網中心服務人員之熱忱及親和力的滿意度?

46 則回應



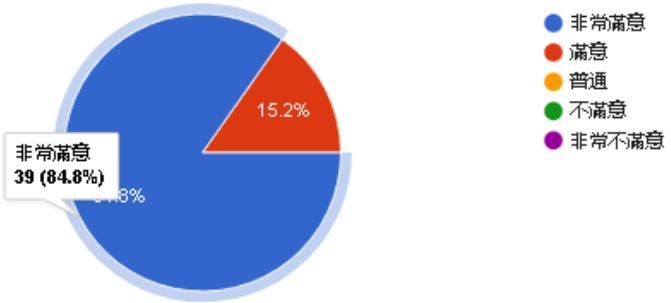
對區域網路中心在網路維運管理的建議

14 則回應



貴單位對於區網中心綜合整體服務的表現

46 則回應



對區網所舉辦之教育訓練或研習課程建議

13 則回應

無
無，辦的很好，感謝您。
滿意
受益良多
希望可以多舉辦一些技術面實務操作研習課程，非常感謝。

教育體系資安檢核 GCB

* 教育部資通安全稽核 @ 臺灣大學
  * 技術檢測: 2021/09/01~09/03
  * 實地稽核: 2021/09/27
* 於網管會議分享
  * 資安檢核 GCB 導入案例分享
    * 技服 GCB 之規則及如何找出排除項，並使用微軟提供之免費工具 LGPO、Policy Analyzer進行導入與檢核，提出三種不同的導入方法供使用者參考。
  * 資安檢核 GCB 排除項參考文件
    * 臺大計資中心導入技服 GCB 規則之排除項目，增加"風險等級"欄位以供參考。
  * 參考區網技術文件
    * https://www.tp1rc.edu.tw/e1.php

GCB 規則Review

項目	技服 GCB 規則項數
Win10	345
Windows Server 2016	590
Red Hat Enterprise Linux 8	292
IE11	154
Chrome	33
Firefox	52
Edge	12
Wireless	19
Fortigate Firewall	46
…	…
總數	1500+

GCB 規則Review

* 若完整導入技服GCB 所有項目
* → 是否仍有可能發生”突破性感染”?

* 100% 有效的CCB設定其實只需要一個
* → “停用”網路卡

GCB 規則Review

* 完全不接種(套用GCB規則0%)→ 感染率 60%
* 接種第一劑(套用GCB規則60%) → 感染率 30%
* 接種第二劑(套用GCB規則70%) → 感染率 20%
* ....
* 完整接種(套用GCB規則100%) → 感染率 5%

GCB 排除項

* GCB 排除項來源
  * 技服 GCB 規則 Review
    * 顯而易見、難以達成
    * 造成使用者不便且低風險等級
  * 技服 GCB 網站FAQ
  * 其他學校經驗 (智慧財產權)
  * 自行測試及使用者回饋

項目	技服 GCB 規則項數	排除項	排除比率
Win10	345	56	16%
IE11	154	34	22%
Chrome	33	15	45%
Firefox	52	3	6%
Edge	12	0	0%

技服 GCB 規則 Review
顯而易見、難以達成

* 無線網路

項次	TWGCB-ID	類別	原則設定名稱	說明	D-Link 設定路徑	EDIMAX 設定路徑	ZyXEL 設定路徑
5	TWGCB-03-001-0005		變更預設 SSID	變更預設的 SSID，並且採用不足以識別為特定組織所使用之無線網路名稱	Basic Settings > Wireless Settings > Network Name (SSID) > Rename	Wireless Setting > Basic > SSID > Rename	Network > Wireless LAN 2.4G/5G > General > Network Name(SSID) > Rename
6	TWGCB-03-001-0006		關閉 SSID 廣播	▪ 關閉 SSID 的廣播模式，並要求使用者自行記錄連線的 SSID ▪ 這作法並不能避免有經驗的攻擊者發現 SSID，但仍應作為安全防護的一個部分	Basic Settings > Wireless Settings > SSID Visibility > Disable	Wireless Setting > Security > Broadcast SSID > Disable	Network > Wireless LAN 2.4G/5G > General > Hide SSID > Enable

技服 GCB 規則 Review
顯而易見、難以達成

* 無線網路

10	TWGCB-03-001-0010	存取控制	啟用 MAC 位置過濾	▪如果採用自動化的裝置網路登錄，應啟用 MAC 位置過濾功能 ▪這作法並不能避免有經驗的攻擊者冒用偽裝的 MAC 進行攻擊，但仍應作為安全防護的一個部分	Filters > MAC Bypass > 設定 MAC 名單	Wireless Setting > Securiy > Additional Authentication > MAC Filter > 設定 MAC 名單	Security > Firewall > MAC Filtering Rule > Enable MAC Filtering > 設定 MAC 名單
11	TWGCB-03-001-0011		關閉 DHCP 協定	關閉 DHCP 協定，並指定固定靜態 IP 位置給每個終端使用者	DHCP Server > Static Pool Settings	Wireless Setting > Basic > IP Address Assignment > Static IP	Network > DHCP Server > General > Disable

技服 GCB 規則 Review
造成使用者不便且低風險等級

* Windows10

編號	原則設定名稱	GCB建議值	風險等級
TWGCB-01-005-0284	關閉市集應用程式	啟用	低
TWGCB-01-005-0285	停用Windows市集中的所有應用程式	停用	低

* Chrome

編號	原則設定名稱	GCB建議值	風險等級
TWGCB-02-003-0018	無痕模式適用性	啟用，"無痕模式已停用"	低
TWGCB-02-003-0014	啟用自動填入		低
TWGCB-02-003-0032	啟用地址的自動填入功能		低

應建立更接地氣的 GCB 規範

- 建議技服GCB規則可增加"風險等級:高/中/低"欄位可供參考
- 應區分不同工作角色(行政人員、程式設計師、網管人員等)，訂立多套 GCB 規則範本
  - 若所有電腦不區分工作角色都套用相同規則，導致排除項非常多，可能造成資安破口。
- 取其 GCB 精神，而非規則細項
  - 可先從計中管理設備做起
    - Cisco Config Template: 套用統一設定檔範本(Login, NTP, SSH, SNMP, ACL等)

Cisco Config Template 範例

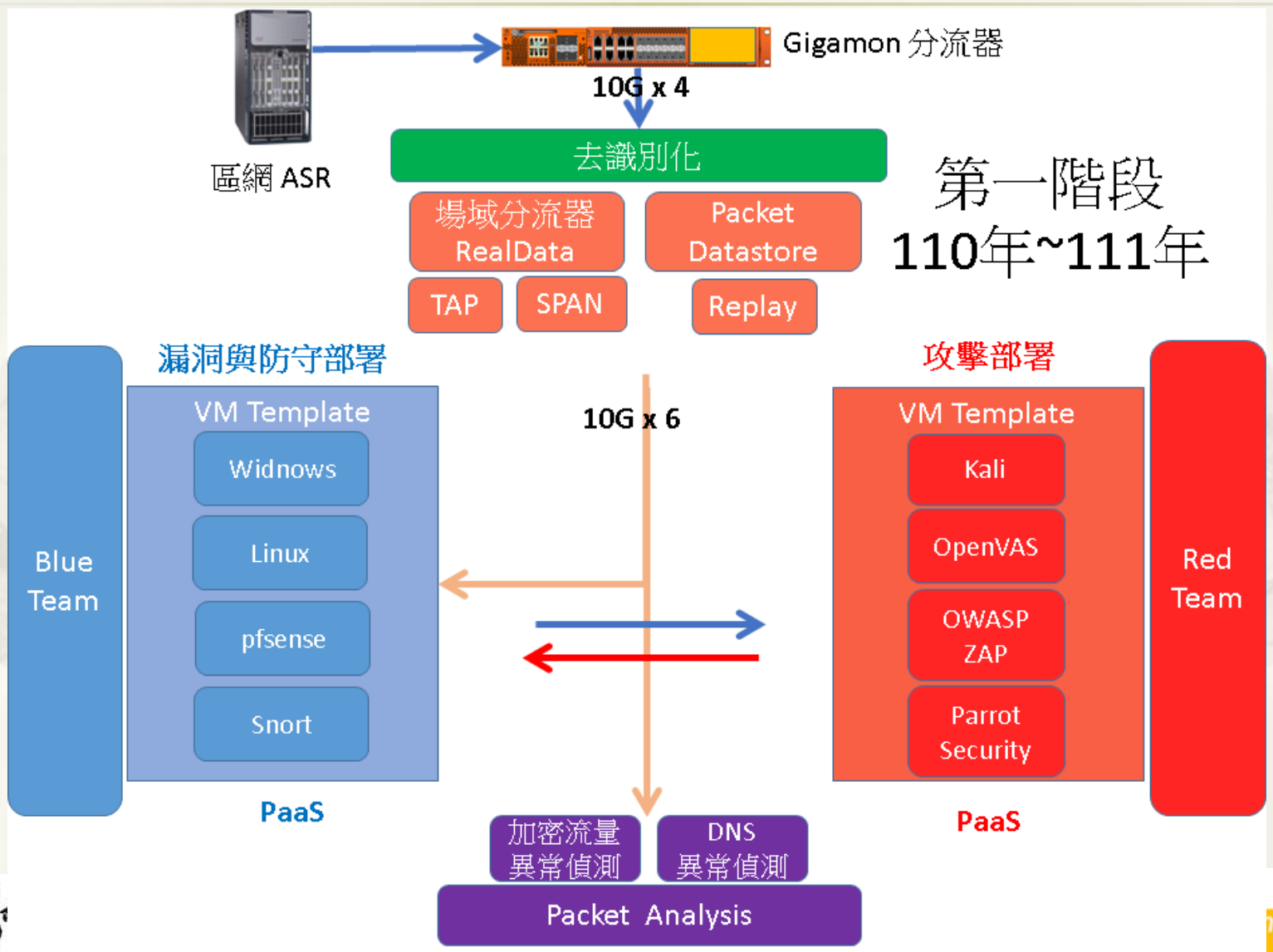
```
權限相關
  (config)# enable secret 12345
  (config)# username davis secret 12345
  password 加密
  (config)# service password-encryption

Line VTY
  ip access-list standard telnet-acl
    permit 140.112.0.0 0.0.255.255
    permit 120.96.0.0 0.0.31.255 or 120.96.0.0/19
    permit 120.96.240.0 0.0.7.255 or 120.96.240.0/21
    permit 120.96.248.0 0.0.3.255 or 120.96.248.0/22

  (config)# line vty 0 15
  (config-line)# login local
  (config-line)# access-class telnet-acl in

關閉 HTTP & HTTPS
  (config)# no ip http server
  (config)# no ip http secure-server

Logging
  (config)#no logging console
  (config)#logging buffered 96000
  (config)#service timestamps log datetime localtime show-timezone

時間相關
  (config)#clock timezone ROC 8
           clock timezone TW 8

          #clock set 10:30:00 15 Apr 2013
```

8. 未來營運計畫

8.1 未來營運目標

* 網路妥適率: 99.9%以上
* 區網網管會議出席率: 90%以上
* 大專院校 ipv6 使用率: 100%
* 高國中小 ipv6 使用率: 60%以上
* 區網課程受訓實質效益分析
  * 50%以上課程需進行前測與後測
  * 前測與後側分數進步平均達 20%以上
* 技術文件分享: 完成 3份以上網路資安文件撰寫
* HTTPS 網站自動檢核程式
  * check.twnic.tw (Selenium)
* Google 表單結合發信回覆等功能

資安卓越中心計畫
實習場域建置



實習場域建置
Packet Datastore

- IPS 資安事件封包蒐集
  - 區網資安事件: 每日約 1000+ 事件
  - 依據事件類別決定錄封包條件
    - 攻擊事件: by Src IP 攻擊來源
    - 挖礦事件: 礦場IP、挖礦IP
- 區網特色資料集
  - Layer2 異常: Loop, Arp spoofing
  - Layer3 異常: Routing Loop, Unicast Flooding, Port scan
  - Web 攻擊: SQL Injection, 暴力破解
  - 放大攻擊: DNS, NTP, LDAP
- Replay 模擬各式網路情境，並可用於攻防情境或 Packet Analysis

8.2 其他建議

- TANet 黑名單、技服黑名單
  - 應開放給所有連線單位
  - 為了讓防火牆或自動開發程式可自動更新，建議黑名單 List 用 .txt or URL 而非用 Excel 檔案
- 建議部內成立資安檢核輔導推動小組
  - 資安力度逐年增加，要人沒有、要錢沒有
  - 面對相同的問題
  - 共同防禦、共享資源
    - 免費 GCB 導入程式、GCB 規則範本
    - TANet 專屬 RPZ Server: 包含技服 DNS 黑名單
    - 政府數位憑證

簡報完畢
謝謝