113年度臺南區網
執行成效報告

國立成功大學

計算機與網路中心

朱敏清技士

大綱

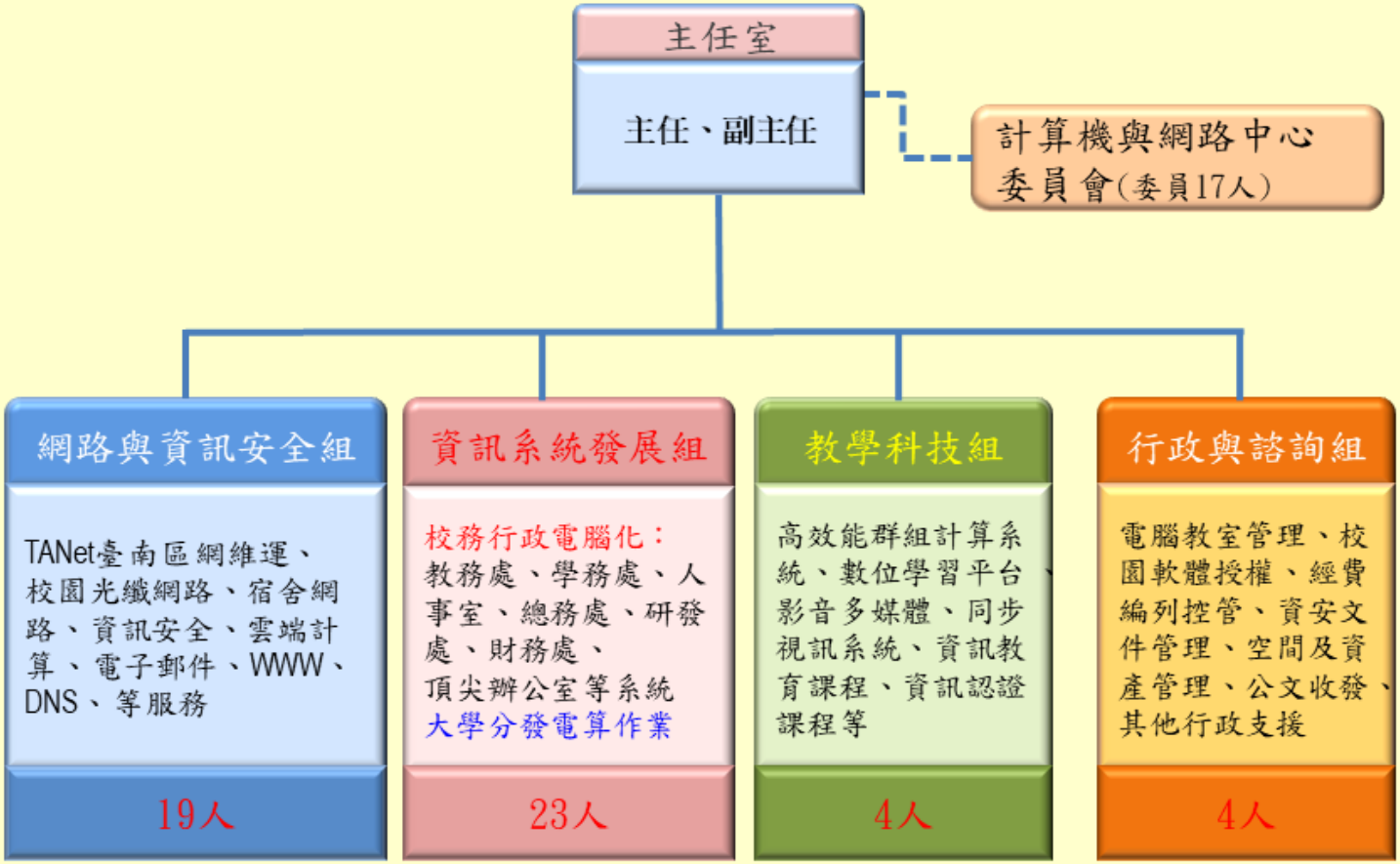
- 網路中心基本資料及經費運用
- 改進意見及改善成效
- 網路連線管理
- 資安管理
- 服務推動特色
- 工作成效及未來推動目標

國立成功大學
National Cheng Kung University

網路中心基本資料及經費運用

TANet 臺南區域網路中心 Taiwan Academic Network

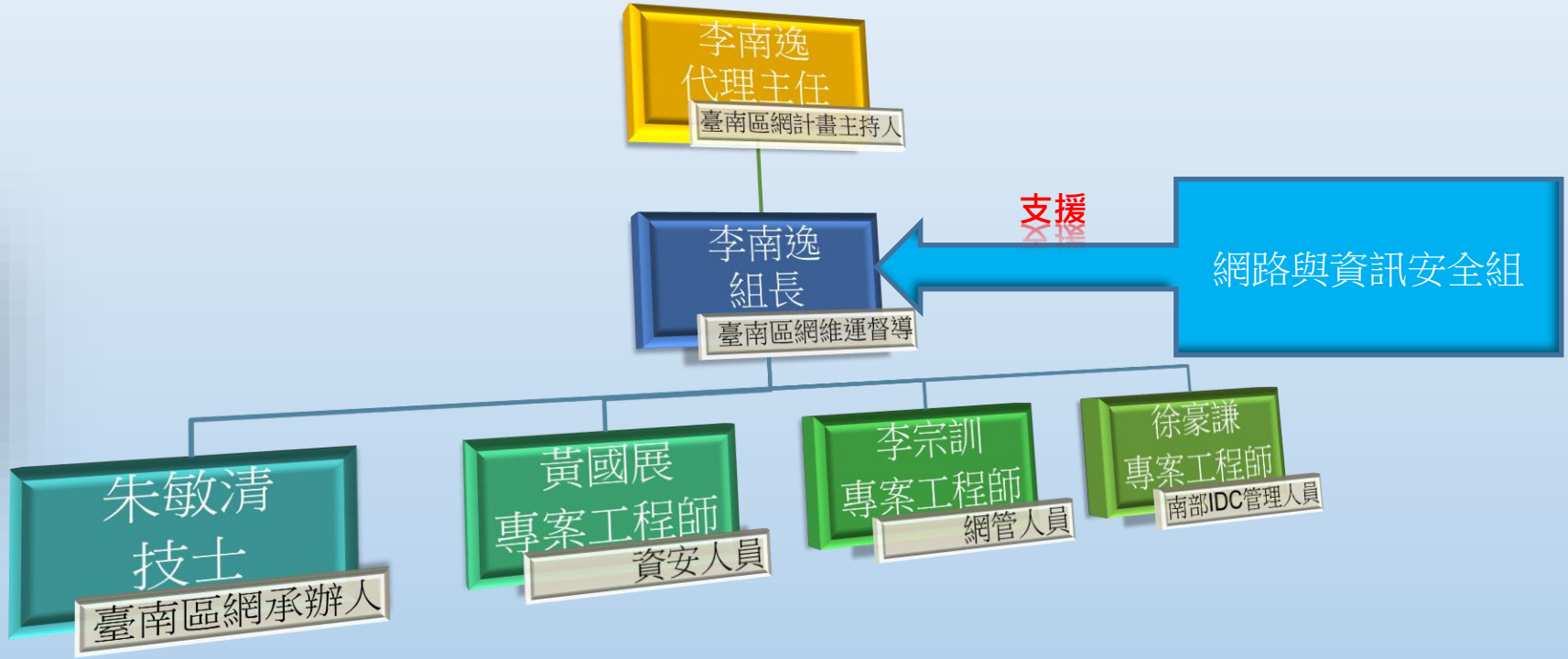
成大計網中心組織架構圖



總計51人，其中兼任主管4人、專任人員47人

統計時間：113年11月

臺南區網人員佈署架構圖



資安人力運用

1. 查看各連線單位網路流量狀況，於異常時通知所屬連線單位
2. 網站應用程式弱點監測平台及防止洩露個資掃描平台協助窗口
3. 協助各連線單位資安問題諮詢
4. 資通安全通報審核及聯絡
5. 各連線單位資通安全通報演練計畫
6. 協助區網中心辦理管理會及研討會等事宜

網管人力運用

1. 維護中心機房電力、冷氣與發電機維護，確保機房維運正常運作
2. 資訊大樓門禁及監視系統控管
3. 機房門禁、環境及監視設備控制管理，確保機房重地安全
4. 協助網路異常狀況之處理
5. 協助區網中心辦理管理會及研討會等事宜

教育雲雲端管理人力運用

1. 協助教育雲各式服務之建置
2. 雲端監控平台之管理
3. 異質管理平台之操作與管理
4. 雲端虛擬化 Server維護管理
5. 雲端儲存系統維護管理
6. 監控確認各使用服務單位連線狀況與服務品質
7. 協助雲端服務使用單位的問題排除

TANet計畫人員證照

	ISO/IEC 27001 ISMS:LA (資訊安全管理系統)	ISO/IEC 27701:2019 PIMS:LA (個人資訊管理系統)	資安職能或其他
網路管理人員	0	0	0
資安管理人員	1	0	1
雲端管理人員	0	1	2

區網年度計畫經費運用

(一)教育部區網年度計畫補助款：

- 本年度核定補助金額：335萬5千。
- 實際累計執行數(至10月底)：約289萬。
- 人事費執行率：約85.20%。
- 業務費執行率：約86.11%。
- 設備費執行率：約100%。
- 至10月底總執行率：約86.14%。

(二)學校補助計畫人員資訊加給：約54萬元。

國立成功大學
National Cheng Kung University

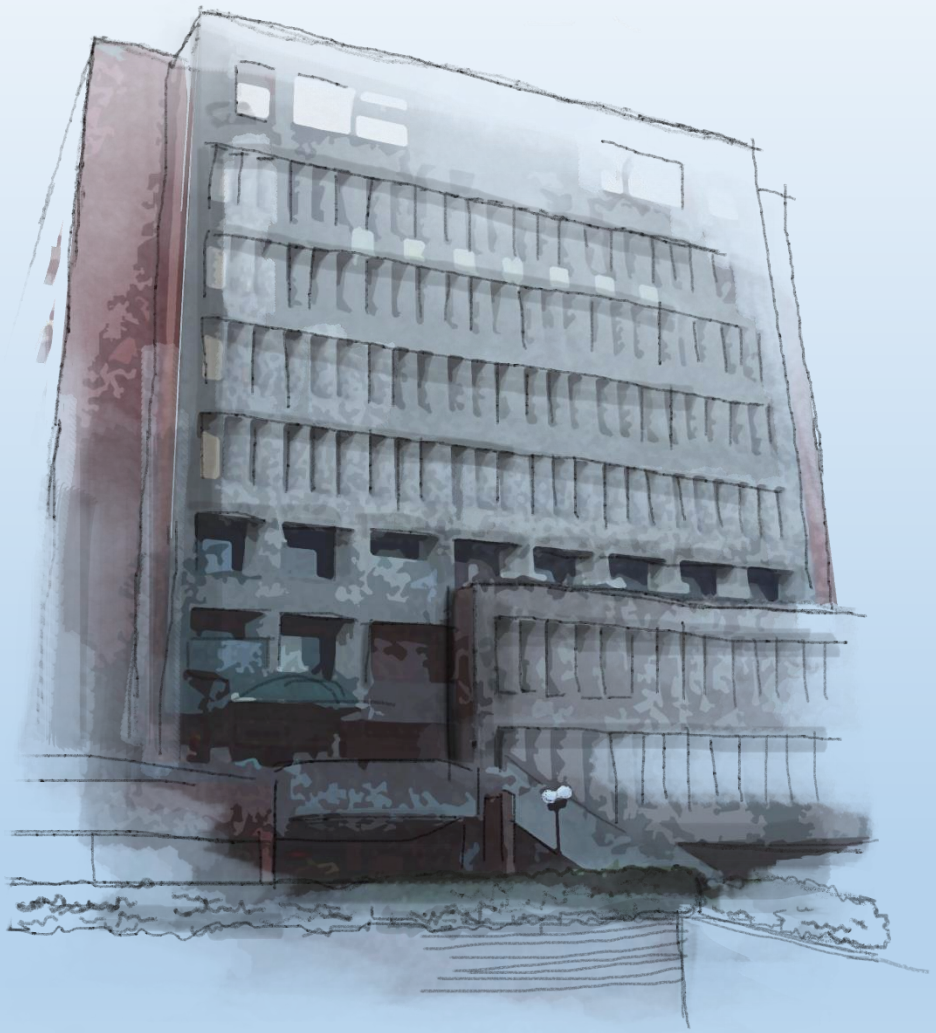
改進意見及改善成效

TANet 臺南區域網路中心 Taiwan Academic Network

項次	建議事項	具體執行狀況/說明
1	資安事件處理平均時數為4.68 小時，處理時間高於其他區網中心，事件完成率為99%，建議應加強資安通報演練及適度調整資安事件應變處理機制。	113年執行狀況，應變處理平均時數由1.88小時降至0.49小時，事件處理平均時數由4.68小時降至2.87小時，事件完成率亦為100%。
2	成大為重要區網及學術中心，建議可考慮推動零信任架構，可先推動身分鑑別，如推動多因子身分驗證，可有效提高資安防護能力。	近期建置之IP位址管理系統及網路設備監控系統開源軟體皆支援身分鑑別。其中於112年辦理教育訓練推廣IP位址管理系統，後續亦將持續推廣開源軟體工具。
3	113 年的妥善率為 90%，且計算方式為中斷4小時/總連線時數，建議再依往年運作績效研訂合理的目標值及檢視是否合宜，另對連線學校有網路障礙之回復時間為8小時亦請再構思可否縮短。	自106年完成TANet 100G建置後，迄今連線單位網路異常問題非發生於區網相關設備。 為持續了解各連線單位網路狀況，計算方式更改為中斷4小時以上單位數/總連線單位數，以留意是否有特定連線單位常有中斷過久之狀況。

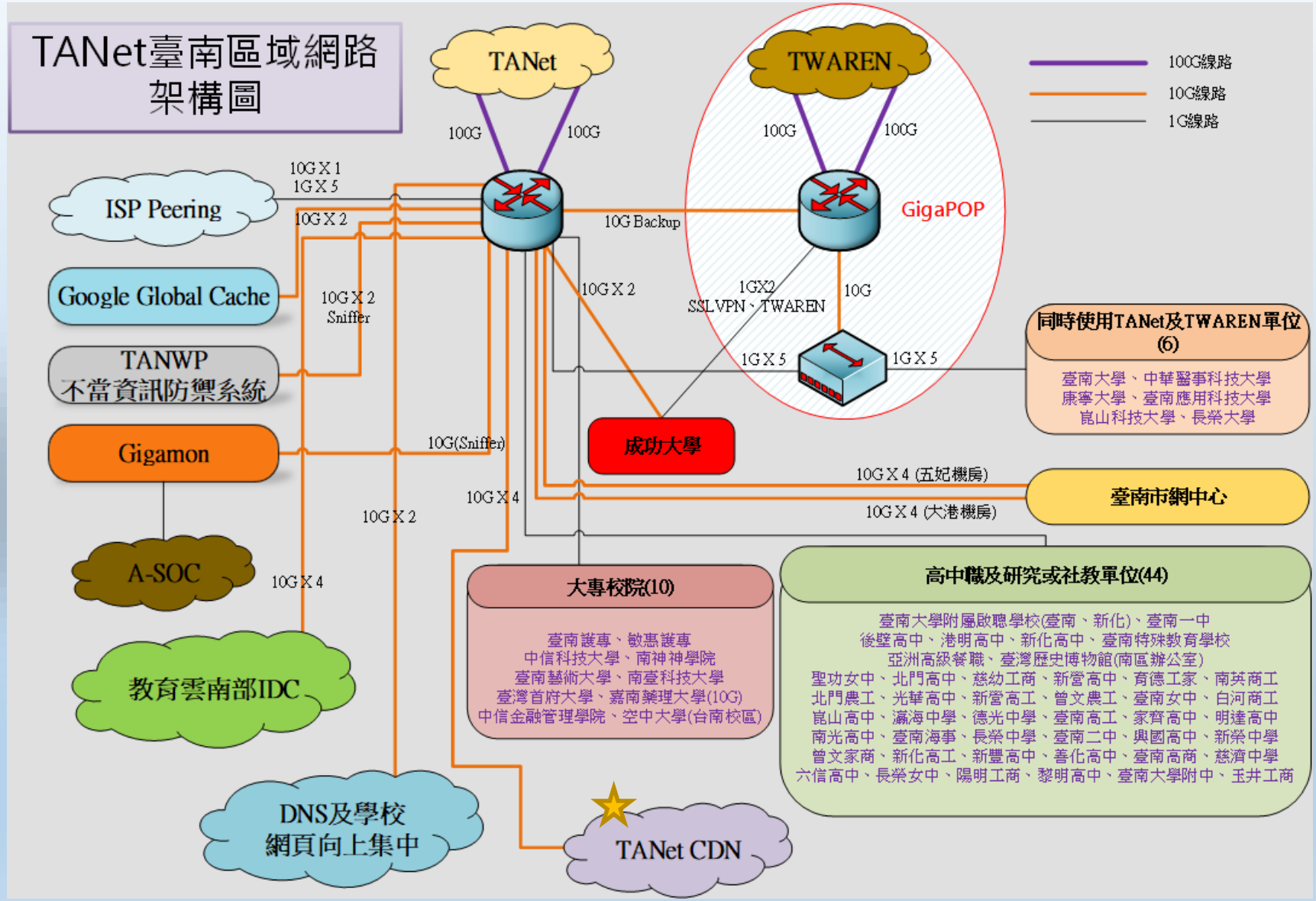
國立成功大學
National Cheng Kung University

網路連線管理

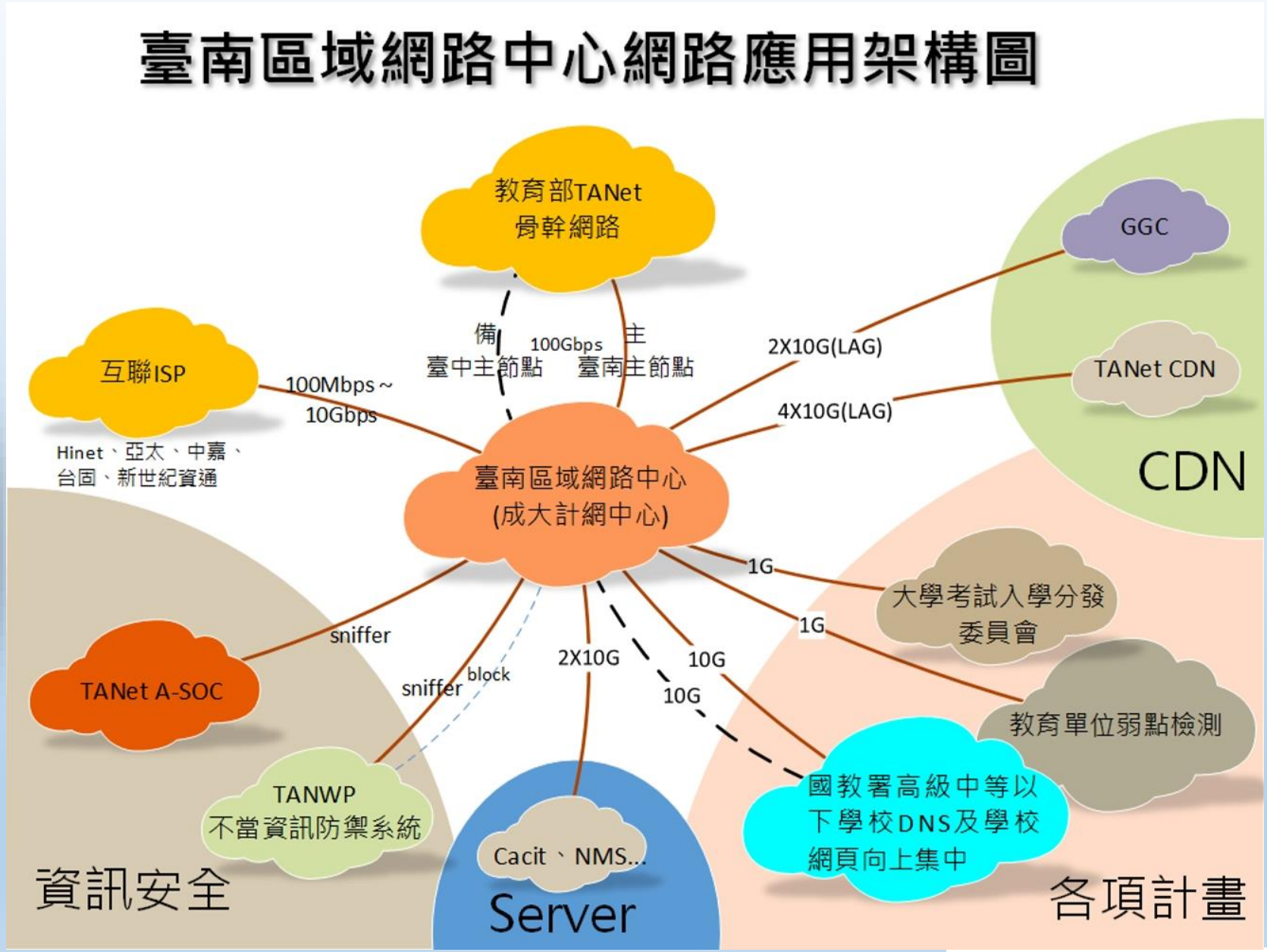


TANet 臺南區域網路中心 Taiwan Academic Network

TANet臺南區域網路架構圖



臺南區域網路中心網路應用架構圖



連線單位概況

(一)區網連線單位：共62個單位

項目	縣(市)教育網中心	大專校院	高中職校	國中小學	非學校之連線單位(不含ISP)	總計
連線學校(單位)數	1	17	43	0	1	連線單位總數： 62
連線單位比例	1.6%	27.4%	69.4%	0%	1.6%	註：單位數 / 總數

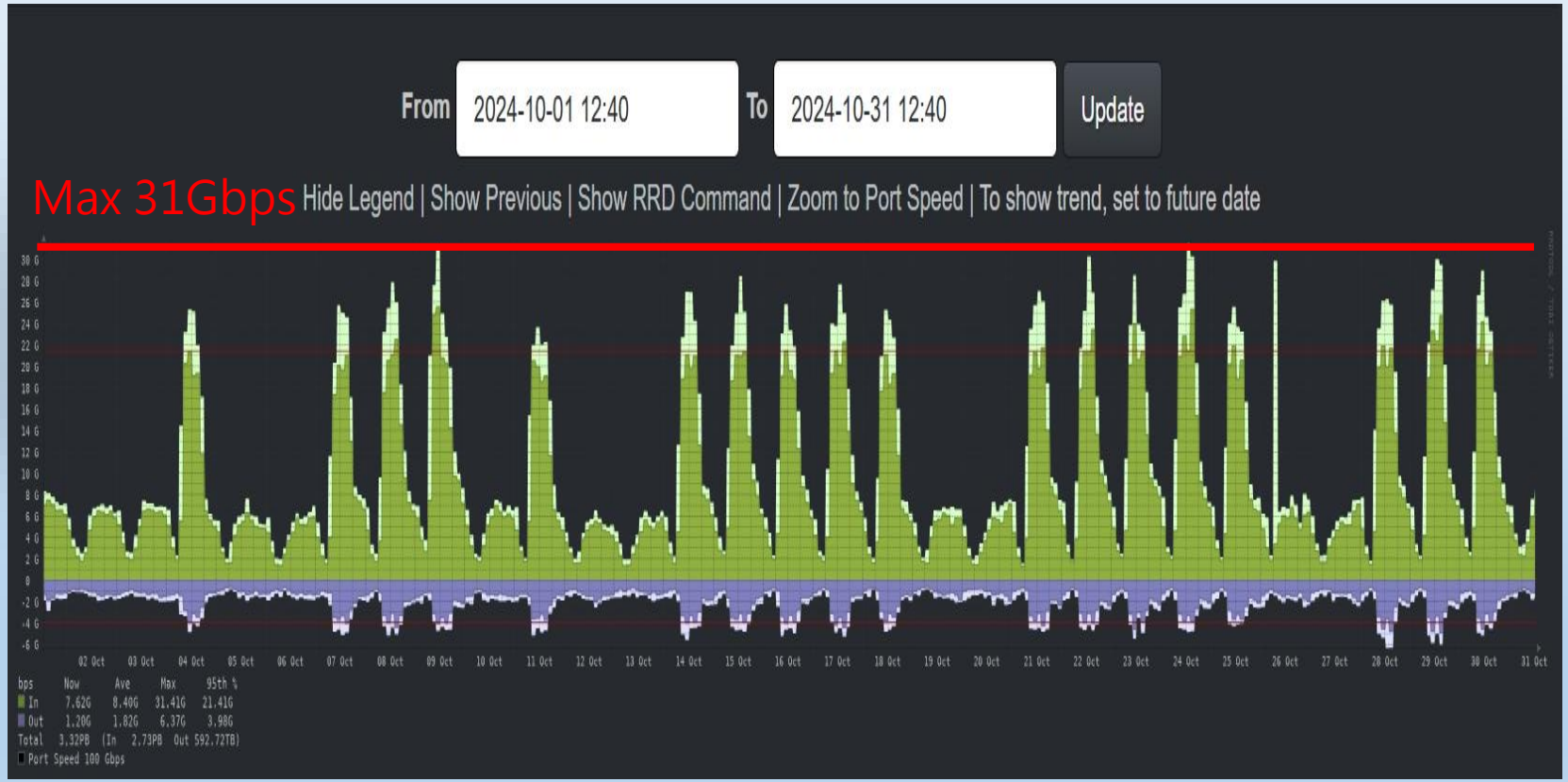
連線單位概況

(二)頻寬與電路數統計

	縣(市)教育網中心	大專校院	高中職校	非學校之連線單位(不含ISP)	總計
10M(含)以上 100M(不含)以下				1	1
100M(含)以上 500M(不含)以下		7	40		47
500M(含)以上 1G(不含)以下			3		3
1G(含)以上 10G(不含)以下		9	1		9
10G(含)以上	8	2			10
連線電路小計	8	18	44	1	71
連線電路頻寬合計	80G	31.7G	8.4G	0.01G	連線頻寬總計： 120.11G
連線頻寬比率	67%	26%	7%	數值過小	請加總電路實際租用頻寬/總計頻寬

連線單位概況

(三)實際用量：臺南主節點←→臺南區網介面



連線單位概況

(四)113年頻寬、電路異動及網路異常事件

1. 頻寬異動：
   1) 康寧大學：300Mbps至1Gbps。
   2) 國立曾文高級農工職業學校：500Mbps至1Gbps。
   3) 天主教臺南市私立德光高級中學：100Mbps至500Mbps。
   4) 私立慈幼高級工商職業學校：100Mbps至300Mbps。
   5) 私立瀛海高級中學：100Mbps至300Mbps。
   6) 私立聖功女子高級中學：100Mbps至300Mbps。
2. 電路異動：
   1) 長榮大學：更換ISP業者線路，遠傳電信→中華電信。
   2) 南榮大學：停辦退出TANet。
3. 異常事件：
   1) 2/2日，南光高中租用之ISP專線遭校外施工單位挖斷。
   2) 9/5日，臺南一中機房冷氣排水異常，滴到ISP數據機。

臺南區網網路服務中斷事件

1. 事件說明：113年6月2日成功大學進行69KV維護，全校停止供應市電，維護期間由發電機供電給機房。惟市電停止供應當下，區網骨幹設備發生重啟現象造成網路服務中斷約10分鐘。
2. 肇因：SMR電池耗損嚴重，無法支撐到發電機運作。(市電中斷至發電機啟用，間隔約20秒)

System Name	tanet-ncku-asr9912-01.moe.edu.tw
Resolved IP	192.192.
Hardware	ASR9K Series
Operating System	Cisco IOS-XR (Default)
Object ID	.1.3.6.1.4.1.9.1.1709
Device Added	1年1週21小時46分鐘19秒前
Last Discovered	1小時2分鐘29秒前
Uptime	5個月2週3天5小時45分鐘31秒

```
TANet-NCKU-ASR9912-01 uptime is 22 weeks, 3 days, 5 hours, 59 minutes
```

臺南區網網路服務中斷事件

3. 改善：經教育部協助，於113年10月11日更換電池組(6V*8顆)，並進行20分鐘放電測試，測試結果為容許範圍內。

拆除舊電池組

新電池組安裝完成

IP位址管理系統-phpIPAM

支援雙因子驗證

IP位址管理系統-phpIPAM

IP位址網段切割狀況

IP位址各網段詳細資訊

VLAN	Subnet description	Subnet
	EVS弱點掃描平台	163.28. 0/28
	中山不當防禦系統_SW	163.28. 16/29
	GGC-NEW_DEVICE	163.28. 32/27
993	CDN_Edge_O2C	163.28. 96/29
993	CDN_iLo	163.28. 104/29
993	CDN_Device_OOB	163.28. 112/29
	TNRC 3750X	163.28. 128/27

單一網段資訊

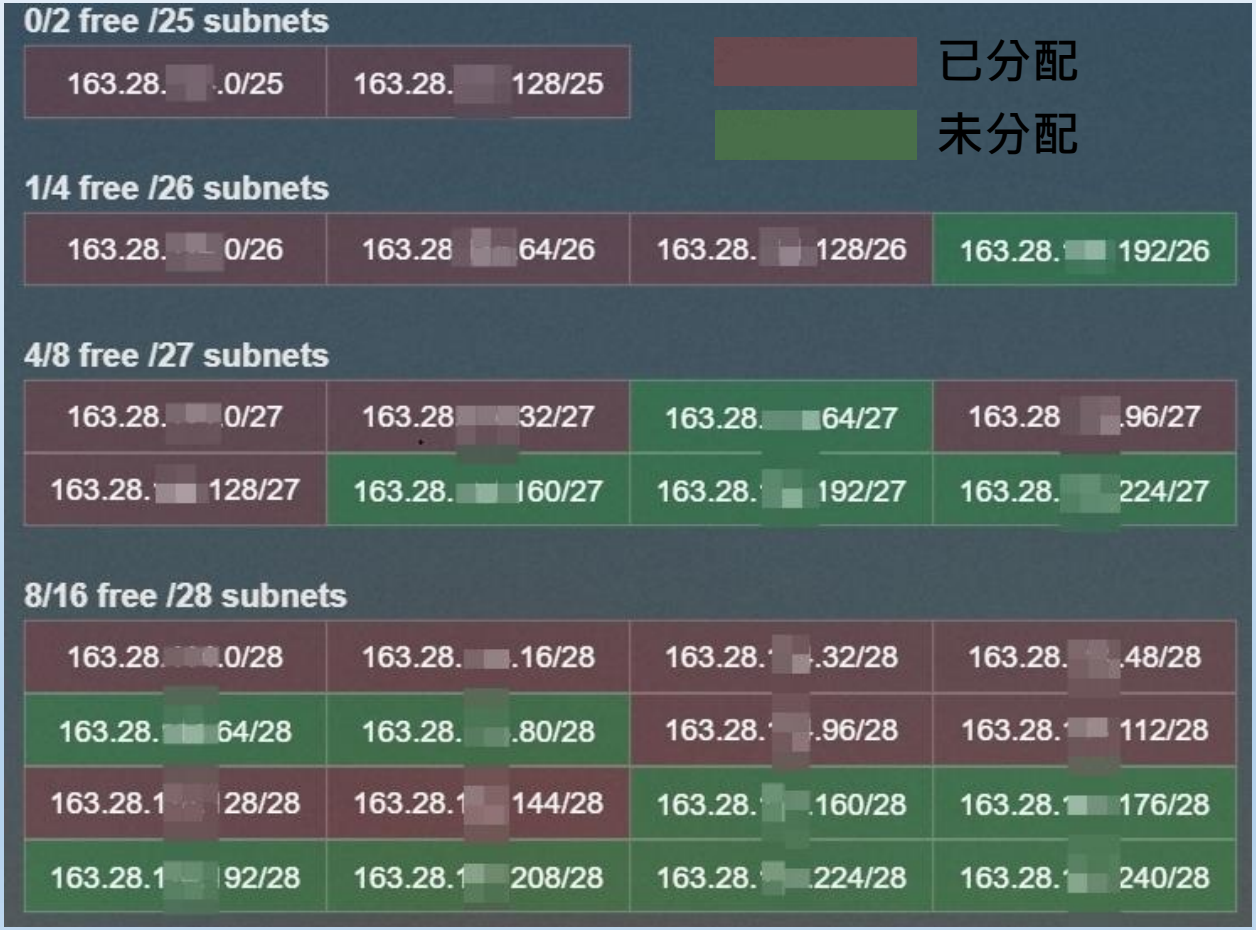
Subnet details	163.28. 104/29 (255.255.255.248)
Hierarchy	TNRC / 區網可用網段 (163.28. .0/20) / (163.28. .0/24)
Subnet description	CDN_iLo
Permission	Admin
Subnet Usage	Used: 3 | Free: 3 (50%) | Total: 6
Gateway	163.28. .110
VLAN	993 - bundle-ether 993 [TNRC CDN] default Domain
Nameservers	/
Customer	中山大學CDN團隊
Device	/
Location	/
Last edited	2024-11-05 14:22:37
Scan agent	localhost (Scanning from local machine) Last check 2024-11-05 14:15:01
Hosts check	enabled Last scan 2024-11-05 14:15:01
Discover new hosts	enabled Last scan 2024-11-05 14:15:01
Resolve DNS names	disabled
NextHop	203.72. .122
RouteProtocol	Static

IP位址資訊

IP address	Hostname	Description
163.28. .105	EDGEServer01	MGMT
163.28. .106	EDGEServer02	MGMT
163.28. .110		-- autodiscovered --

IP位址管理系統-phpIPAM

IP位址網段分配狀況表



IP位址管理系統-phpIPAM

連線單位IP位址管理

Section	Subnet	Description
TNRC	203.72. 0/30	新化高工P2P網段
TNRC	210.60. .0/23	新化高工使用網段

Subnet details	210.60. .0/23 (255.255.254.0)
Hierarchy	TNRC / 新化高工使用網段 (210.60. .0/23)
Subnet description	新化高工使用網段
Permission	Admin
Subnet Usage	Used: 0 | Free: 510 (100%) | Total: 510
VLAN	/
Nameservers	/
Customer	/
Device	/
Location	/
Last edited	Never
Hosts check	disabled
Discover new hosts	disabled
Resolve DNS names	disabled
NextHop	203.72. .2
RouteProtocol	Static

IP address	Hostname	Description
203.72. .1	GigabitEthernet0/4/0/13	新化高工
203.72. .2		-- autodiscovered --

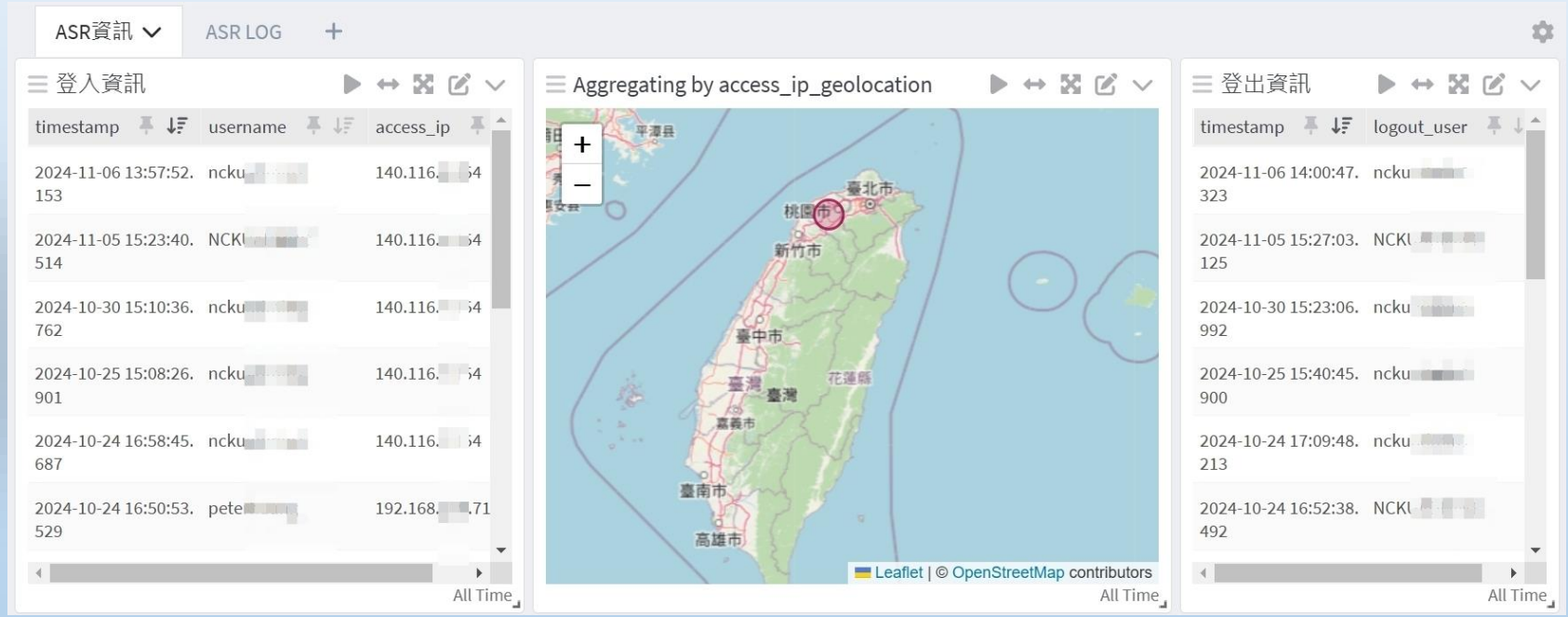
Log分析系統-Graylog

主機Log資訊訊息過多，難以查閱

```
RP/0/RP0/CPU0:Oct 24 15:57:09.419 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 147.203.255.20 1 packet
RP/0/RP0/CPU0:Oct 24 15:57:09.419 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 209.141.51.66 4 packets
RP/0/RP0/CPU0:Oct 24 15:58:55.351 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 23.251.102.205 1 packet
RP/0/RP0/CPU0:Oct 24 15:59:09.433 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 45.90.97.242 1 packet
RP/0/RP0/CPU0:Oct 24 15:59:52.350 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 147.185.132.16 1 packet
RP/0/RP0/CPU0:Oct 24 15:59:52.780 : SSHD_[65583]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'nck[redacted]' from '140.116.[redacted].154' on 'vty0'(cipher 'aes256-ctr', mac 'hmac-sha2-256')
RP/0/RP0/CPU0:Oct 24 16:00:43.405 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 128.14.188.98 1 packet
RP/0/RP0/CPU0:Oct 24 16:00:46.181 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 159.223.46.195 1 packet
RP/0/RP0/CPU0:Oct 24 16:00:48.666 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 47.74.60.48 1 packet
RP/0/RP0/CPU0:Oct 24 16:01:20.451 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 64.62.197.114 1 packet
RP/0/RP0/CPU0:Oct 24 16:01:23.869 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 65.49.20.75 1 packet
RP/0/RP0/CPU0:Oct 24 16:01:27.942 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 65.49.20.97 1 packet
RP/0/RP0/CPU0:Oct 24 16:01:37.251 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 65.49.1.61 1 packet
RP/0/RP0/CPU0:Oct 24 16:01:45.017 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 65.49.20.104 1 packet
RP/0/RP0/CPU0:Oct 24 16:02:05.143 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 167.94.138.159 1 packet
RP/0/RP0/CPU0:Oct 24 16:02:07.880 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 184.105.247.244 1 packet
RP/0/RP0/CPU0:Oct 24 16:02:09.454 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 209.141.51.66 12 packets
RP/0/RP0/CPU0:Oct 24 16:02:20.849 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 64.62.197.146 1 packet
RP/0/RP0/CPU0:Oct 24 16:03:47.808 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 159.203.26.198 1 packet
RP/0/RP0/CPU0:Oct 24 16:03:58.112 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 192.241.155.120 1 packet
RP/0/RP0/CPU0:Oct 24 16:04:09.468 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 45.90.97.242 2 packets
RP/0/RP0/CPU0:Oct 24 16:04:11.634 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 223.113.128.229 1 packet
RP/0/RP0/CPU0:Oct 24 16:05:09.475 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 147.185.132.16 1 packet
RP/0/RP0/CPU0:Oct 24 16:05:43.734 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 199.45.154.177 1 packet
RP/0/RP0/CPU0:Oct 24 16:06:41.262 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 144.126.212.130 1 packet
RP/0/RP0/CPU0:Oct 24 16:07:09.489 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 209.141.51.66 5 packets
RP/0/RP0/CPU0:Oct 24 16:07:09.489 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 65.49.20.97 1 packet
RP/0/RP0/CPU0:Oct 24 16:07:09.489 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 64.62.197.114 1 packet
RP/0/RP0/CPU0:Oct 24 16:07:25.479 : ipv4_acl_mgr[304]: %ACL-IPV4_ACL-6-IPACCESSLOGS : access-list acl_internet_denied_services (10) deny 206.168.34.173 1 packet
RP/0/RP0/CPU0:Oct 24 16:08:06.919 : SSHD_[65583]: %SECURITY-SSHD-6-INFO_USER_LOGOUT : User 'nck[redacted] from '140.116.[redacted].154' logged out on 'vty0'
RP/0/RP0/CPU0:Oct 24 16:08:43.825 : SSHD_[65583]: %SECURITY-SSHD-4-WARNING_LOGIN : The requested term-type 'xterm-256color' is not supported
RP/0/RP0/CPU0:Oct 24 16:08:43.847 : SSHD_[65583]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated user 'nck[redacted]' from '140.116.[redacted].154' on 'vty0'(cipher 'aes256-ctr', mac 'hmac-sha2-256')
```

Log分析系統-Graylog

使用者登出、入ASR 資訊



Log分析系統-Graylog

ASR configuration變更資訊

設定修改資訊

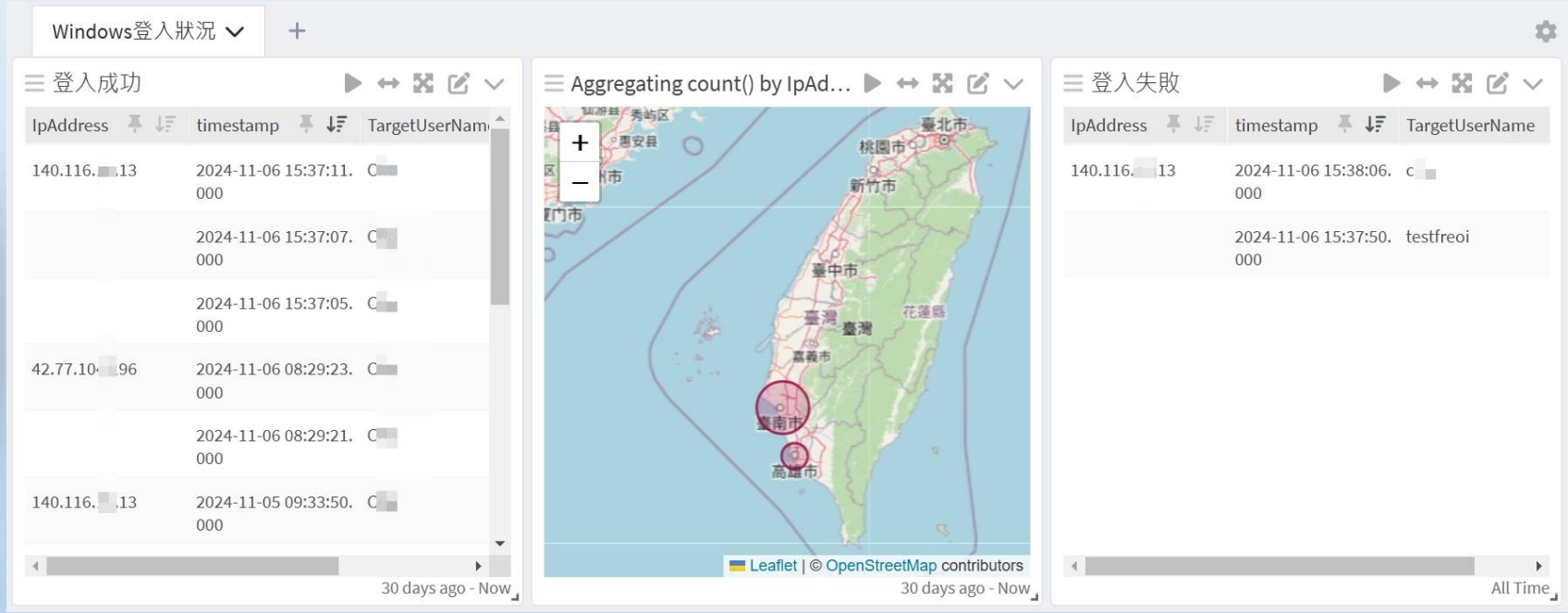
timestamp	conf_user	changlist
2024-10-24 17:01:40.437	ncku	1000000180
2024-10-24 17:00:30.041	ncku	1000000179
2024-09-26 12:25:46.647	ncku	1000000178

ASR本機commit list資訊

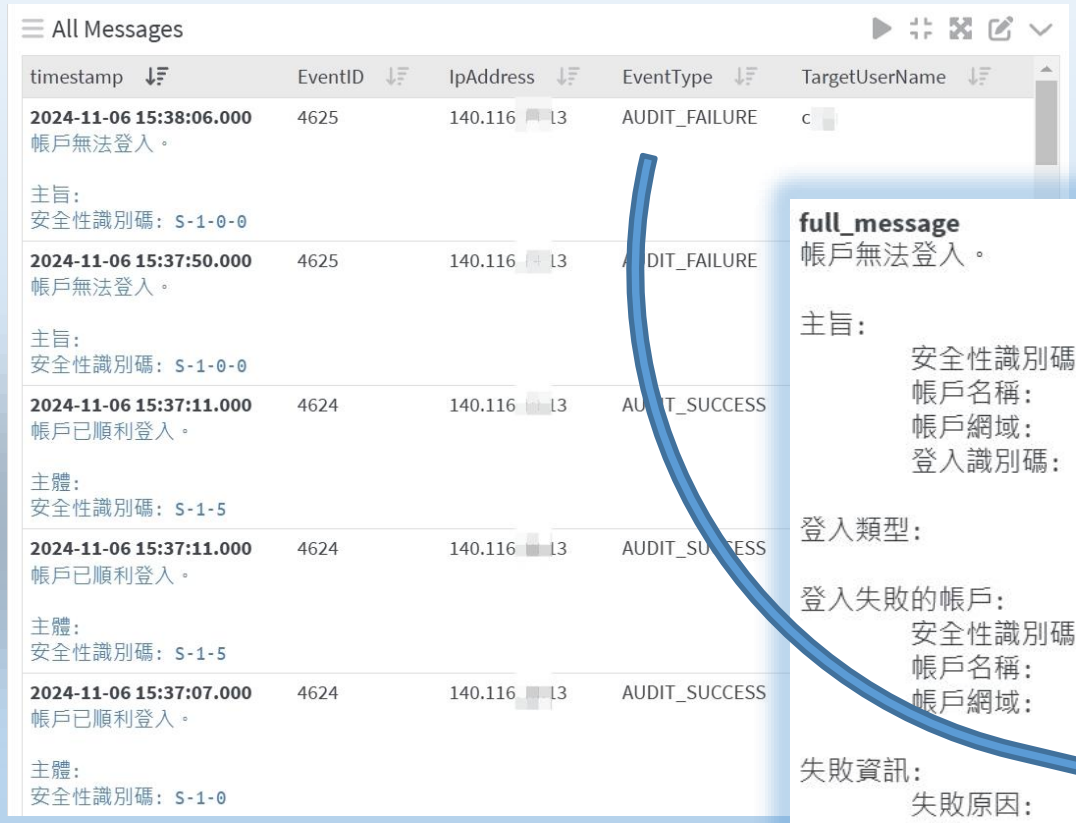
```
RP/0/RP0/CPU0:TANet-NCKU-ASR9912-01#show configuration commit list
Tue Nov  5 15:24:48.228 CST
SNo. Label/ID              User      Line                 Client      Time Stamp
~~~~ ~~~~~~~~~~           ~~~~      ~~~~                 ~~~~~~      ~~~~~~~~~~
1    1000000180            nck       vty0:node0_RP0_CPU   CLI         Thu Oct 24 17:01:39 2024
2    1000000179            nck       vty0:node0_RP0_CPU   CLI         Thu Oct 24 17:00:28 2024
3    1000000178            nck       vty0:node0_RP0_CPU   CLI         Thu Sep 26 12:25:44 2024
4    1000000177            nck       vty0:node0_RP0_CPU   CLI         Mon Aug 19 15:57:07 2024
5    1000000176            nck       vty0:node0_RP0_CPU   CLI         Wed Aug 14 10:07:12 2024
```

Log分析系統-Graylog

管理人員Windows主機被遠端連線紀錄



Log分析系統-Graylog



連線紀錄詳細資訊

full_message

帳戶無法登入。

主旨:
- 安全性識別碼: S-1-0-0
- 帳戶名稱: -
- 帳戶網域: -
- 登入識別碼: 0x0

登入類型: 3

登入失敗的帳戶:
- 安全性識別碼: S-1-0-0
- 帳戶名稱: c
- 帳戶網域: .

失敗資訊:
- 失敗原因: 不明的使用者名稱或錯誤密碼。
- 狀態: 0xC000006D
- 子狀態: 0xC000006A

處理程序資訊:
- 呼叫者處理程序識別碼: 0x0
- 呼叫者處理程序名稱: -

Netflow蒐集及分析-N-Cloud

資料時間範圍: 2024/11/05 16:49:53 ~ 2024/11/05 16:50:29　總筆數: 20000

時間	設備	來源 IP	目的 IP	來源 Port	目的 Port	來源 IP 名稱解析	目的 IP 名稱解析	來源區域	目的區域	協定	Bytes	Packets
2024/11/05 16:50:29	ASR9K	203.163.[redacted].97	192.192.[redacted].63	58646	3128	是方電訊股份有限公司	TNRC - 嘉南藥理大學	TW (臺灣)	TW (臺灣)	TCP	441.88K	5.31K
2024/11/05 16:50:29	ASR9K	118.171.[redacted].243	192.192.[redacted].63	50952	3128	中華電信股份有限公司	TNRC - 嘉南藥理大學	TW (臺灣)	TW (臺灣)	TCP	8.25K	128
2024/11/05 16:50:29	ASR9K	120.114.[redacted].110	31.13.[redacted].52	65019	443	TNRC - 國立臺南護理專科學校	Facebook	TW (臺灣)	TW (臺灣)	UDP	14.63K	192
2024/11/05 16:50:29	ASR9K	120.114.[redacted].110	31.13.[redacted].52	63881	443	TNRC - 國立臺南護理專科學校	Facebook	TW (臺灣)	TW (臺灣)	UDP	118.38K	320
2024/11/05 16:50:29	ASR9K	5.59.[redacted].51	120.114.[redacted].223	48405	8881	-	TNRC - 國立臺南護理專科學校	IT (義大利)	TW (臺灣)	TCP	10.13K	192
2024/11/05 16:50:29	ASR9K	209.14[redacted].148	120.114.[redacted].238	8208	53	-	TNRC - 國立臺南護理專科學校	US (美國)	TW (臺灣)	UDP	21.25K	256
2024/11/05 16:50:29	ASR9K	164.52.[redacted].90	120.114.[redacted].201	42894	119	-	TNRC - 國立臺南護理專科學校	JP (日本)	TW (臺灣)	TCP	3.63K	64
2024/11/05 16:50:29	ASR9K	164.52.[redacted].90	120.114.[redacted].201	42895	119	-	TNRC - 國立臺南護理專科學校	JP (日本)	TW (臺灣)	TCP	14.5K	256
2024/11/05 16:50:29	ASR9K	194.18[redacted].71	120.114.[redacted].73	50826	10567	-	TNRC - 國立臺南護理專科學校	DE (德國)	TW (臺灣)	TCP	3.38K	64
2024/11/05 16:50:29	ASR9K	184.10[redacted].9.77	120.114.[redacted].61	50276	8880	-	TNRC - 國立臺南護理專科學校	US (美國)	TW (臺灣)	TCP	3.38K	64
2024/11/05 16:50:29	ASR9K	173.23[redacted].3.48	120.114.[redacted].163	38173	17000	-	TNRC - 國立臺南護理專科學校	US (美國)	TW (臺灣)	TCP	3.38K	64
2024/11/05 16:50:29	ASR9K	205.21[redacted].177	120.114.[redacted].82	55402	6000	Google	TNRC - 國立臺南護理專科學校	US (美國)	TW (臺灣)	TCP	18.13K	320

專線優惠

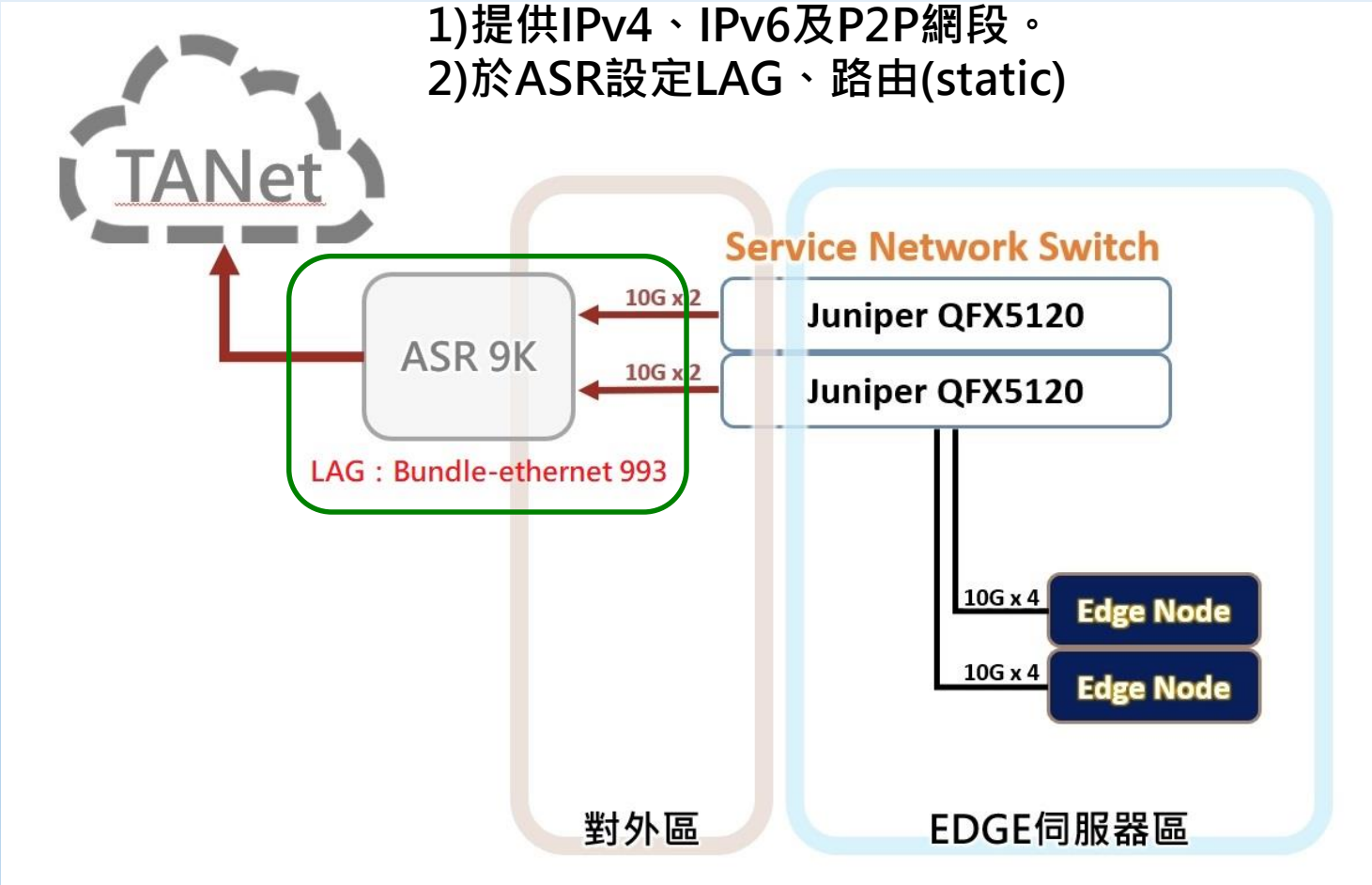
適用對象	中嘉寬頻優惠方案		
台南市高中職	可供裝區域(東區、南區、北區、中西區、安南區及安平區)		
	頻寬	300M	500M
	費用	$6,600/月	$9,600/月

協助建置TANet CDN

協助事項：

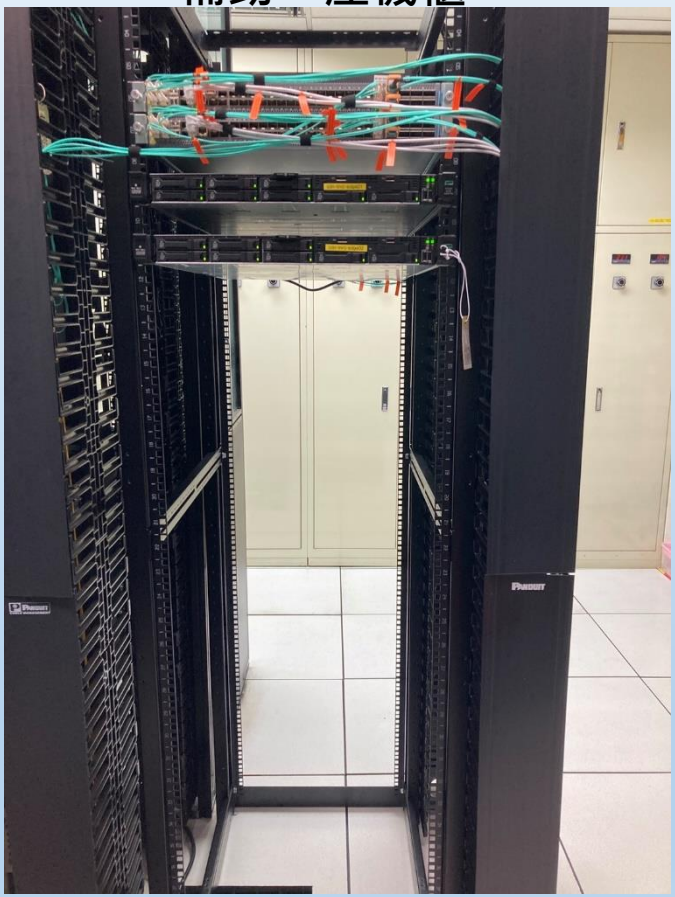
1)提供IPv4、IPv6及P2P網段。

2)於ASR設定LAG、路由(static)

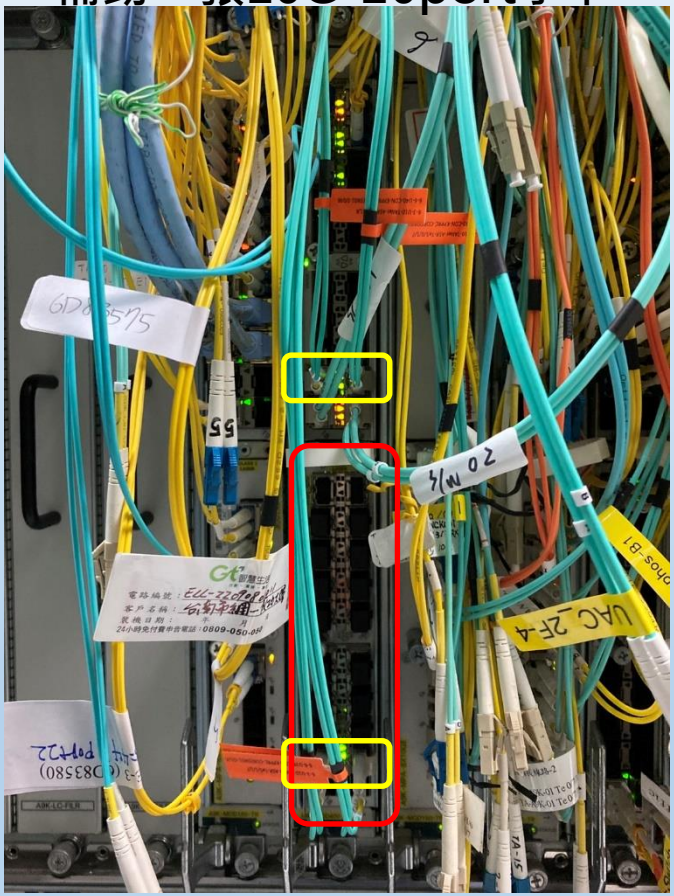


協助建置TANet CDN

補助一座機櫃



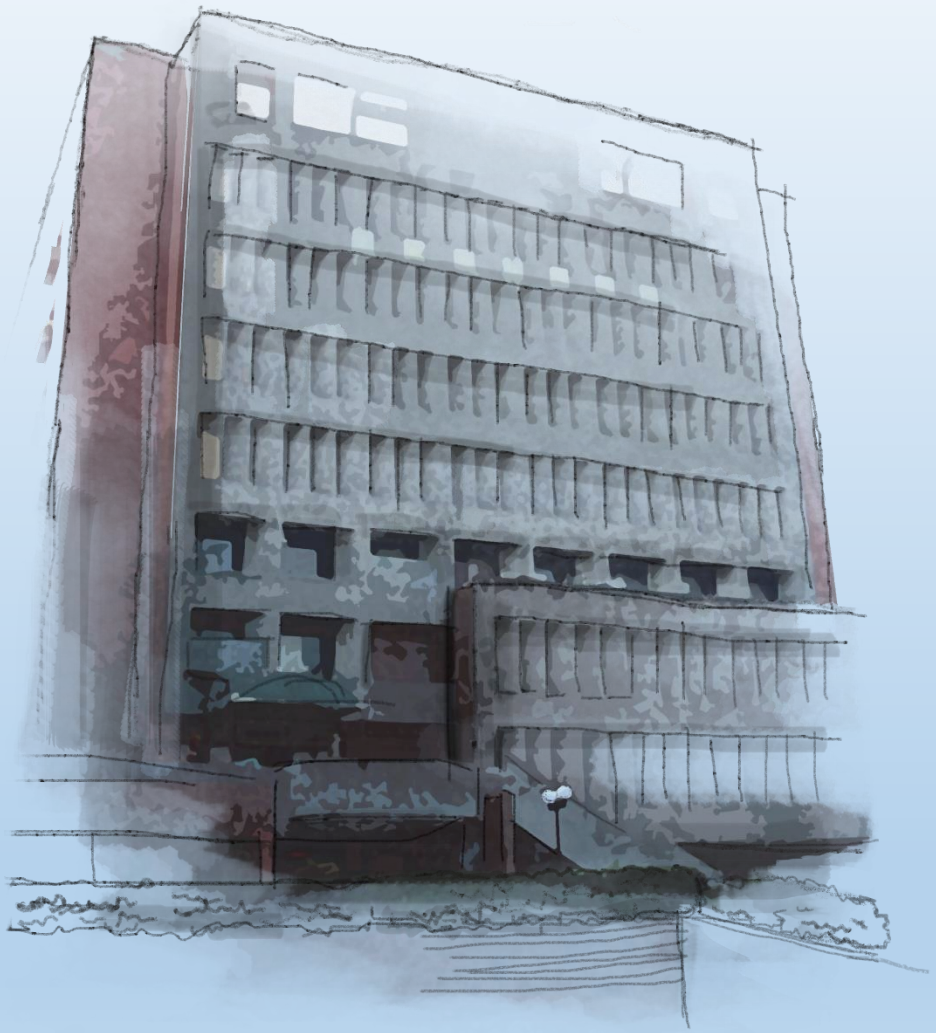
補助一張10G*20port子卡



網路管理-其他各項措施

1. 連線單位檢核
   - 國立臺南大學、中華醫事科技大學、台南應用科技大學、長榮大學、南臺科技大學、崑山科技大學、嘉南藥理大學及遠東科技大學。
2. 提供不當資訊防禦機制
   - 經教育部及中山大學TANWP團隊協助，防護臺南市教育網路中心所屬國中、小學以及臺南區域網路中心所屬高中職連線單位。
3. 提供分流機制：Google Global Cache(GGC)服務
   - 10/29日更換一顆硬碟。
4. 提供網路技術諮詢管道
   1) 提供承辦人服務分機：5*8小時。
   2) 臺南區域網路中心LINE群組：7*24小時。

資安管理

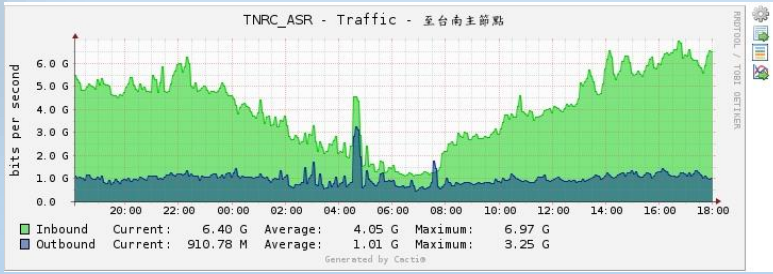


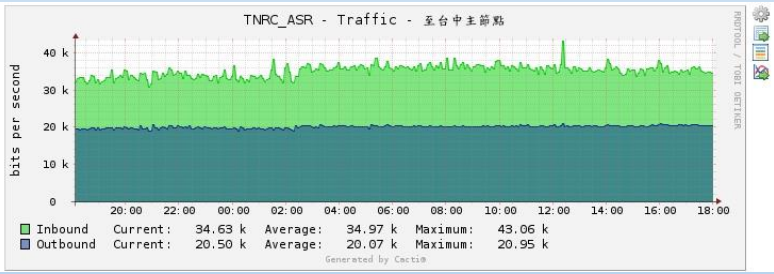
資安通報統計

1. 連線單位1、2級資安事件通報：
   - ◆通報平均時數：0.08 小時
   - ◆應變處理平均時數：0.49 小時
   - ◆事件處理平均時數：2.87 小時
   - ◆通報完成率：100%
   - ◆事件完成率：100%
2. 連線單位3、4級資安事件通報：
   - ◆113年度無3、4級資安事件。
3. 區網中心事件通報審核平均時數：0.75小時
4. 臺南區網連線單位資料完整度：100%

流量分析圖(Cacti)

- 網址： https://cacti.tnrc.edu.tw
- 蒐集資訊：
  - 主幹線路、各連線單位線路、教育雲南部IDC、國教署向上集中計畫、教育單位弱點檢測、TWAREN線路及ISP Peering等。





IP位址流量排名表

1. 網址：https://netflow.tnrc.edu.tw

2024-09-11 Top 100 | 2024 年 11 月 6 日 · Top 100 查詢 | 單IP查詢

Pos	IP	區網外 Giga Byte(s)		區網內 Giga Byte(s)		Giga Byte(s)	
		Send(流出)	Receive(流入)	Send(流出)	Receive(流入)	Total	UL/DL
1	163.28.114.37	0.00000	3743.20276	0.00000	0.00001	3743.20276	0.00
2	163.28.114.36	0.00000	3624.61177	0.00000	0.00001	3624.61178	0.00
3	120.116.1.43	559.39831	2576.56063	15.81312	29.73566	3181.50772	0.22
4	140.116.1.143	402.93220	2372.43648	3.26820	1.35967	2779.99655	0.17
5	203.68.93.220	0.05581	1.53016	1650.68287	893.93478	2546.20362	1.84
6	120.114.234.155	0.06275	0.03043	893.91242	1650.67810	2544.68370	0.54
7	140.116.1.141	361.83820	2098.42284	3.49067	1.10931	2464.86102	0.17
8	120.114.249.100	285.16827	1492.23159	1.59828	0.21310	1779.21123	0.19
9	140.116.56.169	1316.75431	24.47764	0.00000	0.00000	1341.23195	53.79
10	140.116.102.184	13.00266	805.99201	0.11290	0.00000	819.10757	0.02

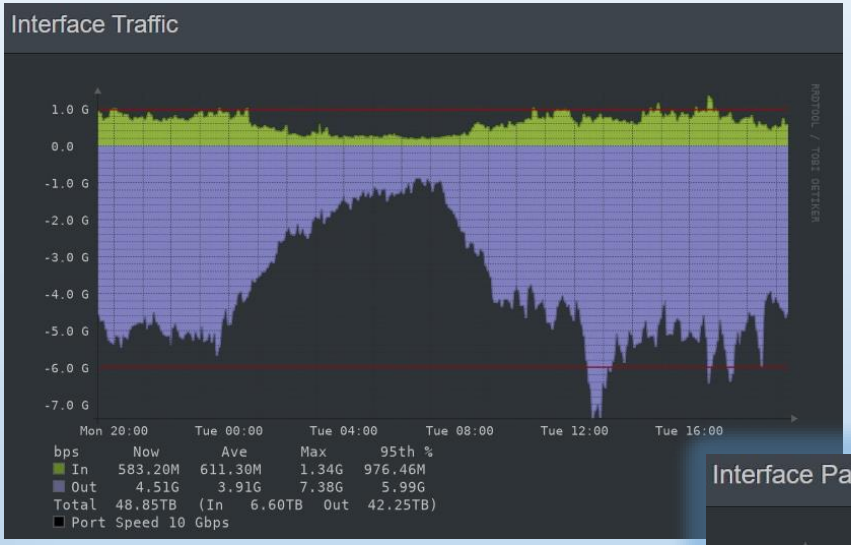
2. 運作目的：
   - 提供各連線單位觀察各自流量及IP位址流量使用狀況
   - 資安人員每日至少兩次觀看各單位MRTG流量圖，查看當日流量有無異常。配合IP位址流量排名表確認可疑之IP位址。

網路設備監控系統-LibreNMS

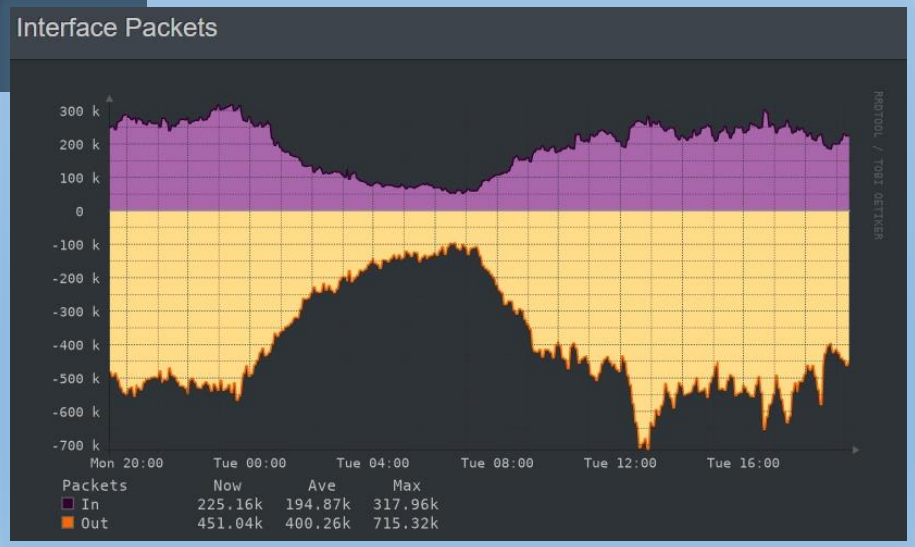
支援雙因子驗證

網路設備監控系統-LibreNMS

介面Traffic資訊



介面packets資訊

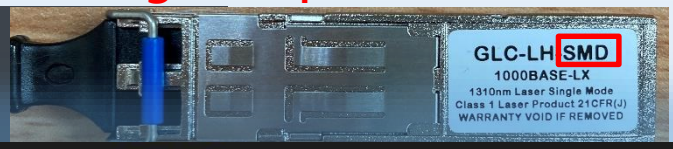


網路設備監控系統-LibreNMS

介面transceiver資訊 DOM;Digital Optical Monitoring

TenGigE0/7/1/0

10GBASE-SR SFP+ Module for MMF



PN: SFP-10G-SR

SN: JC4651[redacted]

Rev: V02

```
RP/0/RP0/CPU0:TANet-NCKU-ASR9912-01#show controllers dwdm 0/7/1/0 optics
Wed Nov  6 18:24:24.891 CST

Optics Status

        Optics Type:  SFP-10G-SR
        Wavelength Info: C-Band, MSA ITU Channel= N/A, Frequency=352.69THz, Wavelength=850.017nm
        TX Power = -2.86 dBm
        RX Power = -2.90 dBm
```

Module Mau 0/7/1/0 - Power Tx 0/7/1/0	0.516 mW
Module Mau 0/7/1/0 - Power Rx 0/7/1/0	0.511 mW
module mau 0/7/1/0 - power Tx 0/7/1/0	-2.874 dBm
module mau 0/7/1/0 - power Rx 0/7/1/0	-2.916 dBm
Module Mau 0/7/1/0 - Current 0/7/1/0	5.3 mA
Module Mau 0/7/1/0 - 0/7/1/0	32.8 °C
Module Mau 0/7/1/0 - Voltage 0/7/1/0	3.323 V

網路設備監控系統-LibreNMS

告警機制：Line notify、E-mail

資安連線管理-ISMS認證

1. 98年通過「教育體系資通安全管理規範」認證。
2. 112年11月ISO/IEC 27001:2013進行追蹤稽核驗證通過。
3. 113年11月ISO/IEC 27001:2022重新驗證稽核中。


證書 TW22/00001176

SGS

國立成功大學

ISO/IEC 27001:2013

Stephen Pao
Deputy Director

配合教育部相關資安措施

1. 113/1/24 ASR分位升級
2. 113/2/20 關閉區網骨幹設備Telnet連線機制。
3. 113/8/6 區網骨幹設備備份還原演練。

```
SNo.  Label/ID          User      Line                 Client     Time Stamp
~~~~  ~~~~~~~~~~        ~~~~      ~~~~                 ~~~~~~     ~~~~~~~~~~
1     1000000180        ncku      vty0:node0_RP0_CPU   CLI        Thu Oct 24 17:01:39 2024
2     1000000179        ncku      vty0:node0_RP0_CPU   CLI        Thu Oct 24 17:00:28 2024
3     1000000178        ncku      vty0:node0_RP0_CPU   CLI        Thu Sep 26 12:25:44 2024
4     1000000177        ncku      vty0:node0_RP0_CPU   CLI        Mon Aug 19 15:57:07 2024
5     1000000176        ncku      vty0:node0_RP0_CPU   CLI        Wed Aug 14 10:07:12 2024
6     1000000175        ncku      vty0:node0_RP0_CPU   CLI        Wed Aug 14 10:05:24 2024
7     1000000174        ncku      vty0:node0_RP0_CPU   CLI        Wed Aug 14 10:00:35 2024
8     1000000173        ncku      vty0:node0_RP0_CPU   CLI        Wed Aug 14 09:55:18 2024
9     1000000172        ncku      vty0:node0_RP0_CPU   CLI        Wed Aug 14 09:45:42 2024
10    1000000171        pete      vty0:node0_RP0_CPU   Rollback   Tue Aug  6 11:07:58 2024
11    TANet_NCKU_TEST   pete      vty0:node0_RP0_CPU   CLI        Tue Aug  6 11:06:03 2024
12    1000000169        pete      vty0:node0_RP0_CPU   CLI        Tue Aug  6 10:57:08 2024
```

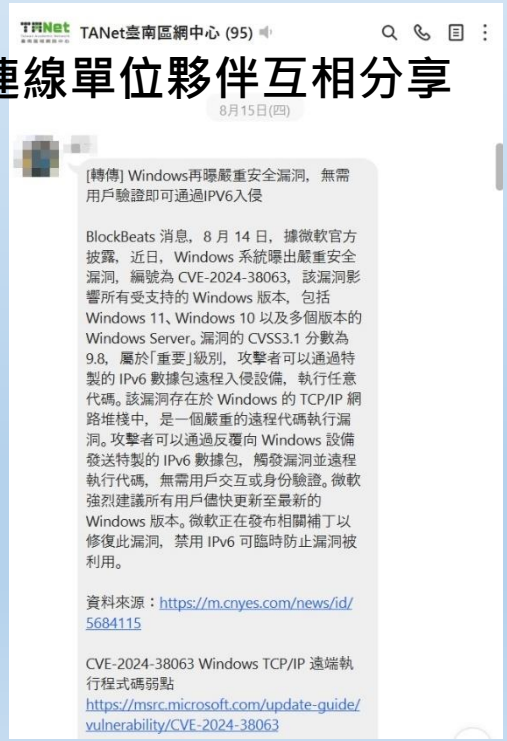
情資分享或通知

1. ANA情資。
2. TANet ASOC通報
   - 每月IoT設備安全性問題。

分享方式：Line、E-mail

gz710@mail.ncku.edu.tw	FW:【漏洞預警】立即科技企業雲端資料庫存在多個重大資安漏洞	2024/10/18 (週五) 下午 1:17
gz710@mail.ncku.edu.tw	FW:【漏洞預警】ESi直通國際 AIM LINE行銷平台存在重大資安漏洞(CVE-2024-9982)	2024/10/18 (週五) 下午 1:14
gz710@mail.ncku.edu.tw	FW:【漏洞預警】台灣數位學習科技 ee-class 存在多個重大資安漏洞	2024/10/18 (週五) 下午 1:11
gz710@mail.ncku.edu.tw	FW:【漏洞預警】昌佳企業財產管理資訊系統存在重大資安漏洞(CVE-2024-9972)	2024/10/18 (週五) 下午 1:09
gz710@mail.ncku.edu.tw	FW:【漏洞預警】新人類科技資訊 FlowMaster BPM Plus 存在多個重大資安漏洞	2024/10/18 (週五) 下午 1:06
gz710@mail.ncku.edu.tw	FW:【漏洞預警】新人類科技資訊 WebEIP v3.0 存在重大資安漏洞(CVE-2024-9968)	2024/10/18 (週五) 下午 1:04
gz710@mail.ncku.edu.tw	FW:【漏洞預警】桓基科技 OAKlouds - Arbitrary File Read And Delete	2024/10/18 (週五) 下午 1:00

連線單位夥伴互相分享



服務推動特色

教育單位弱點檢測平台計畫

- 原建置於成功大學電機系，於108年改移至臺南區網
- 提供區網IP位址以提供服務
  - 163.28.114.0/28
- 協助調查連線單位弱掃及修復狀況。
- 提供主機資源(成大內部資源)：
  - Web虛擬主機
  - Acunetix Engine 虛擬主機
  - 防火牆設備

國教署向上集中計畫

- 每月定期開會討論2次
- 支援項目：
  - GCB、VANS軟體
  - ISMS及稽核相關事項
  - 機房空間及錄影監視
- 網路相關教育訓練
- 協助系統壓力測試
  - 壓力測試合理性及方式
- 協助排除網路連線異常狀況(DDoS攻擊)
  - 與TANet清洗中心協調合作事項：
    - 同意一旦發現攻擊現象，清洗中心可主動清洗再通知。
    - 原由臺南區網中心協助掛名進行清洗流程行政程序，後續由清洗中心自行記錄即可。

國立成功大學
National Cheng Kung University

工作成效及未來推動目標

TWNet 臺南區域網路中心 Taiwan Academic Network

工作成效

項 目	項次	內 容	執行情形
TANet臺南地區連線服務	一	骨幹基礎環境之妥善率，目標99.999%	99.999%
	二	連線學校之網路妥善率，目標值=中斷4小時以上之連線單位數/總連線單位數，目標95%。	99.98%
	三	1.提供連線單位諮詢服務。 2.臺南區域網路中心LINE群組。 3.目標值：自收到詢問時，8小時內回覆連線單位。	100%
	四	1.連線學校之IPv4/IPv6推動完成率。 2. IPv6目標值，完成各學校IPv6電路點對點設定。	IPv4：100% IPv6：100%

工作成效

項　目	項次	內　　容	執行情形
資訊安全與網路監測服務	一	依行政院資通安全規定之辦理連線單位資安通報審核。目標：2小時	100%
	二	網路監測與統計： 1.連線單位網路流量監測 2.全區網IP位址流量排行榜 3.IP位址管理系統 4.Log分析系統 5.網路設備監控系統 6.服務平台妥善率，目標：90%	95%

工作成效

項　目	項次	內　　容	執行情形
區網中心行政事務	一	維運區網中心專屬網頁，網頁妥善率目標90%。	100%
	二	召開區網管理會，每年至少2次，並呈現完整會議紀錄。	50%
	三	1.辦理研習活動：網路管理、網路新知、網路安全等主題。 2.本年度預計辦理20節。	100%

工作成效

項　目	項次	內　　容	執行情形
與ISP及ICP互連	—	1.維護TANet與ISP多點互連計畫，包括：HiNet、SeedNet、SoNet…等ISP。 2.連線妥善率目標99.999%	100%
	— —	1.持續維護Google Global Cache： 2.連線妥善率目標99.999%	100%

未來推動目標

(一)TANet相關：

1. 擴充既有平台儲存空間，以延長Log資訊存續時間 。
2. 因應Line Notify將結束服務，尋找其它告警機制。
3. 即時流量分析系統Cacti改版作業。

(二)配合教育部工作重點：

1. 網路管理
   - 網路使用及流量統計分析
   - 機房監控與管理
2. 資通安全管理
   - 建立網路安全防範機制
   - 建立符合行政院資通安全規定之通報機制
   - SPAM Mail檢舉處理機制
   - 智財權檢舉案件追蹤
3. 維運教育部教育雲南部資料中心

未來推動目標

(三)區網中心工作重點：

1. 處理連線單位TANet連線問題
2. 推廣網路相關應用服務
3. 辦理研討會或研習課程
4. 定期召開管理會
5. 提供連線單位網路諮詢服務
6. 將教育部政策或通知轉達連線單位

國立成功大學
National Cheng Kung University

THANK YOU FOR YOUR ATTENTION.

TWNet 臺南區域網路中心 Taiwan Academic Network