檔　　號：
保存年限：

教育部　函

地址：100217 臺北市中正區中山南路5號
承辦人：張睿驊
電話：(02)7712-9057
電子信箱：lisa_chang@mail.moe.gov.tw

受文者：如行文單位
發文日期：
發文字號：臺教資通字第1142702433號
速別：普通件
密等及解密條件或保密期限：
附件：會議紀錄(含簡報)

主旨：檢送114年7月21日臺灣學術網路(TANet)技術小組第97次會議紀錄，請查照。

正本：銘傳大學賴守全教授、財團法人國家衛生研究院莊育秀主任、臺灣學術網路區域網路中心、中央研究院資訊服務處、財團法人國家實驗研究院國家高速網路與計算中心、各直轄市及縣市教育網路中心
副本：

臺灣學術網路(TANet)技術小組第 97 次會議

會議紀錄

時間：114 年 7 月 21 日下午 2 時

地點：教育部資訊及科技教育司 1302 會議室

主持人：教育部資訊及科技教育司 邱副司長仁杰　　紀錄：張睿驊

壹、主席致詞(略)

貳、報告事項:

一、新世代教育學術研究骨幹網路設備採購案建置進度與網路架構規劃。

決議：

(一)有關「新世代教育學術研究骨幹網路設備採購案」建置作業請各單位協助配合相關事宜，另待完成建置後，本部將再召開會議研議 TANet BGP 路由管理政策規劃，屆時將邀請有意願之區網中心與教網中心共同參與討論。

(二)餘洽悉。

二、資安事件單通報時間及知悉時間報告。

決議：

(一)依「資通安全事件通報及應變辦法」第 4 條 1 項規定「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」有關知悉時間定義，建議將確認事件發生，對資訊資產判斷ＣＩＡ衝擊等級的時間做為知悉時間，以利後續追蹤處理。若為複雜的重大資安事件，也應先就已知受損部分（例如發現木馬）立即通報，後續再逐步更新案情，確保不逾時。

(二)餘洽悉。

參、討論事項

一、有關縣市及校園網路設置基準，提請討論。

決議：

(一)請教網中心於8月8日下班前提供網路設置基準相關建議，並回復是否有意願參與本部測速盒子計畫，以利本部彙整研議基準調整及測速盒執行規劃相關事宜。

(二)有關區網中心網路設置基準部分，本部將再參考區網中心期末評核作業，評估產製相關基準以供參考。

二、本部校園雲端電子郵件系統研議限縮使用範圍，提請討論。

決議：

(一)考量資安風險及使用效益，原則同意本部校園雲端電子郵件服務限縮為僅供教職員工使用。為利服務限縮推動，預計先辦理教育部OpenID帳號與電子郵件服務區隔作業，將研議教育部OpenID帳號網域由「@mail.edu.tw」更名為專屬網域(如「@openid.edu.tw」)，以明確其身分認證功能，避免服務混淆；待更名試行及相關配套措施完備後，再實施電子郵件服務限縮作業。

(二)若有縣市希望繼續提供學生使用服務，須配合資安強化相關作業(如實施高強度帳密規則或多因子認證等)，後續可再與本部共同研議。

(三)依資通安全責任等級分級辦法之「附表十資通系統防護基準/存取控制」之帳號管理機制，教育部校園雲端電子郵件帳號如超過180天未登入則視為閒置帳號應予停用，以確保系統及使用者帳號安全。使用者如有設定自動轉寄之情形，本部將再發送停權通知至轉寄信箱，提醒使用者變更密碼及提供申請復權機制。

三、有關精進 TANet DNS RPZ 防護機制，提請討論。

決議：

(一)請各縣市教網中心將 DNS 查詢指令轉送至縣市網 CDN 邊緣主機，以達一致防護功能；非縣市所管中小學則統一指向學校實體位置所在縣市之主機。另無法介接 TANet DNS RPZ 主機(140.111.12.87)，之大專校院，由現行設定至本部遞迴主機改為設定至學校所接區網中心之 CDN 邊緣主機。

(二)待確認前述設定完成後，本部將無需每月彙整阻擋清單發函各縣市週知，以簡化行政處理作業。

(三)目前尚有處分機關發函至部分大專校院(DNS RPZ 自願參與者)，本部將再確認學校介接狀況後，函請衛生福利部等相關處分機關，通知後續由本部統一收受請求停止解析/限制接取之公文，以簡化各單位行政處理程序。

四、有關區網中心辦理營運持續演練作業時，應將機房實體環境納入設計營運持續演練情境考量，並於撰擬營運持續演練計畫，納入資訊通報與協調機制規劃。

決議：

(一)請區網中心在辦理營運持續演練時，將整個機房實體環境異常（例如天災、電力、空調事件，以及門禁管控制度）納入演練情境考量。

(二)在撰擬營運持續演練計畫時，請納入資訊通報與協調機制，例如向相關利害關係人（連接的縣市教網中心、連線單位、教育部）通報(實際演練時需進行通報)。撰擬演練計畫若有相關問題，可洽本部協助。

肆、臨時動議

一、有關曝露在外網之 IoT 物聯網設備清單，轉交區縣市網路中心協助後

續追蹤與支援一事，提請討論。(提案單位：教育部資科司資訊安全科)

決議：

(一)現行 IoT 設備普及，暴露在網際網路上的設備遭網路攻擊利用風險極高，請區網中心持續扮演協助輔導轄內各校之角色。

(二)對於委員建議區網中心建立自動化轉發 IoT 清單機制，降低人員工作量，或直接切斷該 IoT 設備 IP 快速降低其風險，本部後續將研擬相關管制規定授權處理或更適當作法，待未來機制設計完成後，再邀請區網中心一同討論其可行性。

二、有關 TANet 流量統計圖(https://mrtg.tanet.edu.tw/)服務下線規劃，提請討論。(提案單位：教育部資科司學術網路科)

決議:請各區網中心與教網中心於8月8日下班前提供仍有使用需求之mrtg統計圖資網址，本部配合將相關統計圖資整併至臺灣學術網路(TANet)網路流量圖(https://traffic.tanet.edu.tw)內提供。

三、有關 bind.org 已有新的 DNSSEC 機制，TANet 是否比照之前統一提供相關更新機制的設定文件以供參考?(提案單位：高雄市教育網路中心)

決議：考量目前多數 DNS 軟體已支援 DNSSEC 機制，非僅限 BIND，故各單位若尚有本部統一提供設定文件之需求，會後可再與本部討論。

四、有關 115 年起請各縣市自籌編列 90%電路費，教育部後續相關配套措施與規劃為何?(提案單位：雲林縣教育網路中心)

決議：因應財劃法本部預算大幅刪減，故請各縣市協助爭取府內資訊基礎建設預算，以持續提供校園優質網路服務，共同維持臺灣學術網路運行模式；考量此議題涉及未來整體 TANet 網路架構、網路資源與資安防護等多項重要網路服務及採購方式規劃，本部後續將另案召開研商會議，邀集各縣市共同討論協調。

伍、散會(17:10)

臺灣學術網路(TANet)技術小組第97次會議簽到表

序號	單位	參加人員
1	資訊及科技教育司	蔡宜蓁(視訊) [illegible] [illegible] [illegible] [illegible] 黃士峰 [illegible] 裴善成 [illegible] [illegible]
2	中央研究院	呂佳育 [illegible]
3	銘傳大學 賴守全教授	賴守全
4	國家衛生研究院 莊育秀主任	莊育秀
5	財團法人國家實驗研究院國家高速網路與計算中心	視訊 張聖翔

臺灣學術網路(TANet)技術小組第97次會議簽到表

序號	單位	參加人員
1	基隆市教育網路中心	
2	臺北市教育網路中心	
3	新北市教育網路中心	許哲鳴
4	宜蘭縣教育資訊網路中心	視訊 - 陳一鳴
5	桃園市教育網路中心	視訊 陳譽中
6	新竹市教育網路中心	視訊 林朱亭
7	新竹縣教育網路中心	視訊 彭雅君
8	苗栗縣教育網路中心	張奕勛、哈喜琪 顏仰璉(視訊)
9	台中市教育網路中心	沈俊達
10	彰化縣教育網路中心	視訊 林政言
11	南投縣教育網路中心	鄭明彰/楊彥誠 視訊 王登儀 林取德 林淑娟
12	雲林縣教育網路中心	沈慶清
13	嘉義縣網路中心	王嘉田

臺灣學術網路(TANet)技術小組第97次會議簽到表

序號	單位	參加人員
1	國立臺灣大學 (臺北區網中心)	視訊 游子興 李美雯
2	國立政治大學 (臺北第二區網中心)	蔡憶懷
3	國立中央大學 (桃園區網中心)	視訊 許時準 周小慧
4	國立陽明交通大學 (竹苗區網中心)	汪禧弘
5	國立清華大學 (新竹區網中心)	視訊 陳文城
6	國立中興大學 (臺中區網中心)	呂仲聖 視訊 楊棠誠
7	國立暨南國際大學 (南投區網中心)	[illegible]
8	國立宜蘭大學 (宜蘭區網中心)	[illegible] 、[illegible]
9	國立中正大學 (雲嘉區網中心)	[illegible]
10	國立成功大學 (臺南區網中心)	[illegible]
11	國立中山大學 (高屏澎區網中心)	[illegible] (視訊) 余社諄 廖英捷
12	國立東華大學 (花蓮區網中心)	楊[illegible] 劉[illegible]
13	國立臺東大學 (臺東區網中心)	視訊 郭俊賢

14	嘉義市網路中心 ✓	視訊　陳宗儀
15	台南市教育網路中心	呂政諺
16	高雄市教育局電子資料中心 ✓	視訊　張宏明
17	屏東縣網路中心 ✓	視訊　顏凌青
18	花蓮縣網路中心	請假
19	台東縣教育網路中心 ✓	視訊　翁秉逸
20	澎湖縣教育網路中心	楊宗哉　林銘志
21	金門縣教育網路中心	薛松烽　張玉珀
22	連江縣教育網路中心	視訊　葉家裕

臺灣學術網路(TANet)技術小組

第97次會議

教育部

114年7月21日

議程

- 壹、主席致詞
- 貳、報告事項(2案)
- 參、討論事項(4案)
- 肆、臨時動議
- 伍、散會

壹、主席致詞

貳、報告事項

報告事項-1

案由：「新世代教育學術研究骨幹網路設備採購案」建置進度與網路架構規劃。

（報告單位：教育部資科司學術網路科，10分鐘）

報告事項-2

案由：資安事件單通報時間及知悉時間報告。

（報告單位：教育部資科司資訊安全科，10分鐘）

參、討論事項

討論事項-1

案由：有關縣市及校園網路設置基準，提請討論。

說明：因應數位學習全面推動，需強化從資訊基礎設施到資安管理的整體網路支援環境，以確保穩定且高速的網路服務品質，故針對縣市教育網路中心及學校網路環境相關面向，建立具體明確的設置基準，作為一致性評比的依據，提供 後續優化網路環境與推動精進措施的重要參考。

擬辦：

一、初版網路設置基準已於本部114年網路優化補助案提供，本部將持續評估各縣市執行概況，滾動調整設置基準，提供各縣市因應財劃法於縣市內爭取網路優化經費參考。

二、配合網路基準測量作業，本部規劃提供部分測速盒供縣市安裝使用。

討論事項-2

案由：本部校園雲端電子郵件系統研議限縮使用範圍，提請討論。

說明：

一、考量現今科技趨勢，對於學生來說已有多種資通訊服務工具可達聯繫目的，也有多種電子郵件服務可供選擇，爰校園電子郵件服務對學生已無使用之必要性。

二、根據114年上半年帳號使用情形清查結果，校園雲端電子郵件系統總帳號數約103萬個，半年內登入成功帳號僅約3.5萬個（含WEB、POP3、IMAP4），即約96.6%的帳號半年內未被使用(本部已先停用)，未使用之帳號尤以學生帳號占大多數。

三、國中小學生因年齡層較低，難以落實高強度密碼設定原則，且較無具備多因子驗證相關設備，致使遭到偽冒身分登入之資安風險大幅提升。

擬辦：為保障校園雲端電子郵件資訊與個資安全，擬限縮僅提供教職員工使用，並落實高強度密碼設定原則。

討論事項-3(1/2)

案由：有關精進TANet DNS RPZ 防護機制，提請討論。

說明：

一、DNS RPZ依法阻擋內容：詐欺、毒品、性影像、類菸品。

二、各主管機關依法辦理阻擋(停止解析/限制接取)之行政處分公文，現由TWNIC設定在其RPZ主機，本部TANet DNS RPZ主機(140.111.12.87)已與TWNIC RPZ主機定期同步資料，以達阻擋清單一致。

三、TANet依「兒童及少年性剝削防制條例第47條」、「性侵害犯罪防治法第46條」及行政執行法第36條辦理之限制接取作業，**縣市部分已由本部統一收文，並請不當資訊防護系統手動納入阻擋清單**，使高級中等以下學校無法存取前述不當網址；本部亦每月彙整阻擋清單發函22縣市知悉。

討論事項-3(2/2)

案由：有關精進TANet DNS RPZ 防護機制，提請討論。

擬辦：

一、技術面:

(一)本部已於區網中心及縣市教育網路中心的TANet CDN邊緣主機增設DNS resolver功能:

1.具備原CDN功能。

2.區　網：自動導入本部RPZ阻擋清單(含TWNIC)。

3.縣市網：自動導入本部RPZ阻擋清單(含TWNIC)，及兒少不當資訊防護RPZ清單。

(二)請各縣市將DNS查詢指令轉送至縣市網CDN邊緣主機，以達一致防護功能；非縣市所管中小學則統一指向所在縣市之主機。

二、行政面：各縣市如已完成設定，因阻擋清單已自動介接，後續RPZ公文無須再每月彙整函送各縣市。

討論事項-4

案由：有關請區網中心將機房實體環境納入營運持續演練情境考量，提請討論。

說明：依審計部「政府建構網路設施及推動雲端服務執行情形」審核結果，建議區網中心應將與教網中心合作辦理網路備援納入區網演練範圍，請本部檢討改善，以強化網路服務韌性。

擬辦：考量相關區網中心骨幹網路設備由本部管理維運，惟機房實體環境管理仍由各區網中心負責，爰擬請區網中心辦理營運持續演練作業時，將機房實體環境納入設計營運持續演練情境考量，並於撰擬營運持續演練計畫，納入資訊通報與協調機制規劃，建立「通報 - 協調 - 配合應處」之執行機制，以提升整體網路服務韌性及異常應變效能。

肆、臨時動議

臨時動議-1

一、有關曝露在外網之IoT物聯網設備清單，轉交區縣市網路中心協助後續追蹤與支援一事，提請討論。

(提案單位：教育部資科司資訊安全科)

臨時動議-2

二、TANet 流量統計圖(https://mrtg.tanet.edu.tw/)服務下線規劃，提請討論。

(提案單位：教育部資科司學術網路科)

臨時動議-3

三、有關DNSSEC相關機制bind.org已有新的機制, 是否比照TANet之前所以提供之文件方式, 統一律定相關的更新機制? 提請討論。

(提案單位：高雄市政府教育局教育網路中心)

伍、散會

遠傳FET

新世代教育學術研究骨幹網路設備採購案-TANet網路建置說明

版本：1.0
日期：2025/07/20

Agenda

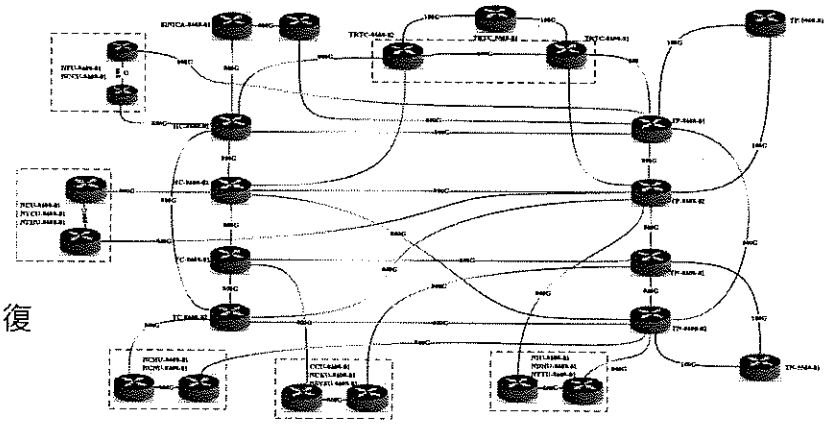
遠傳FET

- 新一代 TANet 400G網路特色
- 新舊世代 TANet 比較
- 專案建置期程說明
- 後續議題討論

新一代TANet 400G網路特色

遠傳FET

- 『主節點對主節點』頻寬以400G為基礎，總頻寬最高達1.6Tbps
- 『區網中心』出口頻寬以400G為基礎，總頻寬最高達1.6Tbps
- 全網完整雙備援架構
  - 全硬體、線路架構HA
- 高效能、低能耗高速網路
  - IPoDWDM、智慧能控
- 高度靈活、彈性骨幹架構
  - 分段路由、EVPN
- 快速自癒、障礙復原
  - 50ms內快速切換服務恢復
- 高度安全運作管理
  - 符合A級機關要求



TANet 400G網路之應用服務

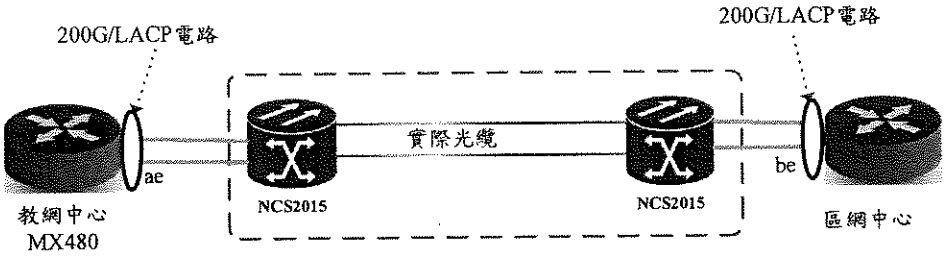
遠傳FET

- IPv4、IPv6上網服務
  - 網際網路之存取
- 多地存取之EVPN服務（待討論）
  - 多校區網路整合
  - 其它

六都教網架構

「六都教網」構連：

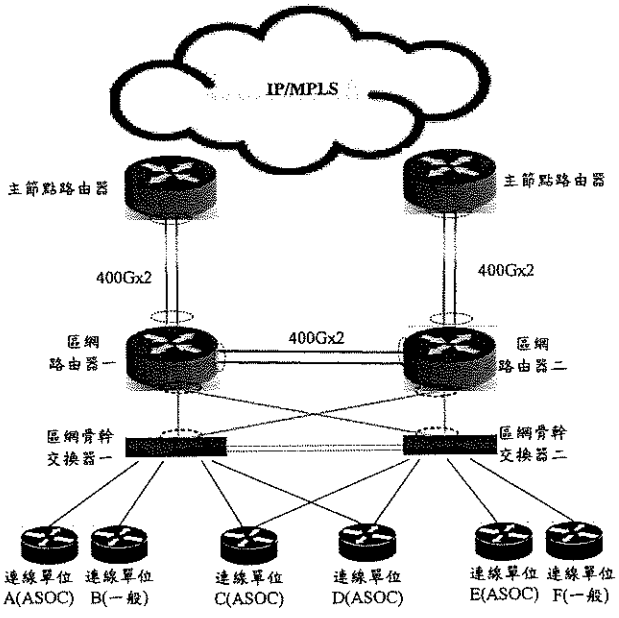
- 以教網既有接入區網中心暗光纖為主
- 依規劃，提供100G兩路電路接入區網中心 = 100G x 2 = 200Gbps
- 本案僅提供利用既有暗光纖將TANet光傳輸網路延伸至六都，本案以提供100G電路為主，不針對六都教網對接網路設備後續施作



連線單位接入架構

400G網路提供多樣的連線單位接入方式

- 專案提供純乙太介面 1/10G速率接入(可另購25G光模組接入)
- 在設備維護的情形下，提供連線單位最小的服務影響
- 在條件允許下，連線單位可獲得更高的HA可用度
- 提供IPv4、IPv6、 L2/L3VPN服務

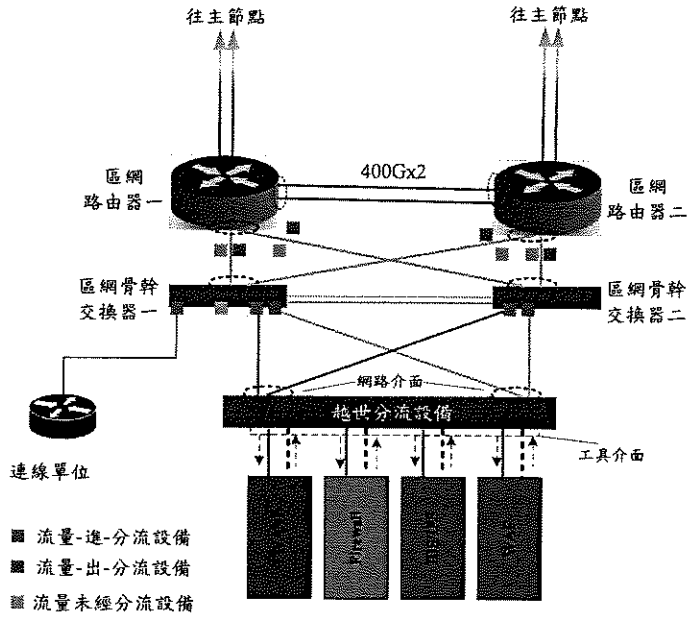


400G分流設備與連線單位

遠傳FET

400G網路提供分流設備供ASOC與其它流量工程使用：

- 與TWAREN共用同一分流設備
- 以VLAN(Bridge-Domain)方式重導流量
- 提供額外處理100G流量生成Flow能力



400G 主要光與IP網路設備

遠傳FET

項次	設備名稱	功能摘要	主節點機	區網中心	六都教網	中繼機房	備註
1	Cisco NCS2015	400G ROADM光傳輸設備	√	√	√		
2	Cisco NCS2006	400G ROADM光訊號放大傳輸設備				√	
3	Cisco 8608	骨幹路由器，400G/100G高集成、高速IP功能路由器	√	√			
4	Cisco NCS5508	邊際路由器，10G/100G高集成、高速IP功能路由器	√				臺北、臺南與科技大樓主節點
5	Cisco Nexus 93180	骨幹交換器，提供1G/10G之連線單位接入匯集	√	√			
6	Cisco C9200	網管交換器，提供10/100/1000Mbps與10G介面集成	√	√		√	僅部分中繼機房安裝
7	越世NPB	分流交換器，提供連線單位流量工程應用	√	√			

Agenda

遠傳FET

- 新一代 TANet 400G網路特色
- 新舊世代 TANet 比較
- 專案建置期程說明
- 後續議題討論

前後期教育學術網路比較

遠傳FET

項目	目前教育學術網路	新一代教育學術網路	優勢分析	備註
基礎架構	IPv4、IPv6 混合各自獨立	骨幹以EVPN方式承載 IPv4、IPv6與其它服務	單一核心架構承載現行服務 更易於維護	未來可轉為IPv6
流量轉發	IPv4、IPv6、MPLS	Segment Routing	統一全域路由轉發機制， 加速路由收斂轉發	未來可轉為 SRv6
骨幹架構	IPv4、IPv6、MPLS 三者骨幹共存	單一SR骨幹	無縫向前相容既有網路，統一各種 網路服務架構，易於流量調度	易於流量工程
骨幹通訊協定	OSPFv2、OSPFv3、 BGP、MPLS、PIM...	IS-IS、BGP、SR	單一控制信令與轉發協定支援IPv4、 IPv6，簡化設定與維護	新一代協定同時 支援IPv4與IPv6
服務與骨幹關係	混合、多層運算	服務各自獨立運算，與 骨幹運算無關	以VPN區分服務，強化效能並可保 護核心骨幹免受外部攻擊	易於管理
架構擴增性	需同時考慮三個骨幹 關係	分別擴充，影響性低	提供連線單位異地備援架構與新一 代多點式可路由EVPN架構服務	MH架構、E- LAN、E-Tree
可靠度	區網/GigaPOP 單一設備節點	全網雙設備節點完整 備援	同時提供雙設備、多路徑400G線路、 雙中心與雙網之骨幹完整備援架構	用戶端線路、設 備除外
節點間總頻寬	200Gbps	1.6Tbps	各區合計1.6Tbps頻寬，平衡流量負 載；提供各種大型內容服務高速應 用	包括未來應用

IP路由架構

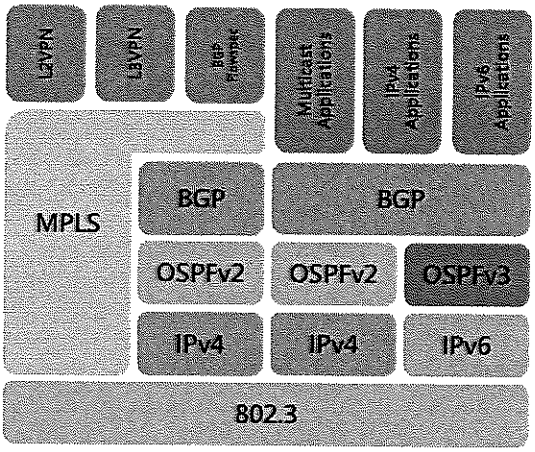
- 介紹100G與400G之網路差異
- 說明400G網IP網路技術

10

目前教育學術網路基礎

遠傳FET

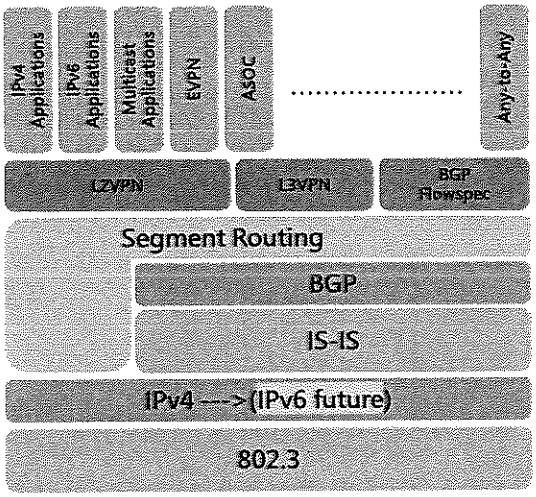
- 以MPLS LDP為主之數據平臺
- 以IPv4、IPv6與MPLS三網之流量轉發
  - 共用同一數據平臺
  - OSPF為共同協定
- BGP協定提供三網之路由訊息交換
- 混合式骨幹架構



教育學術網路協定應用架構示意
(主節點/區網中心)

新一代教育學術網路基礎

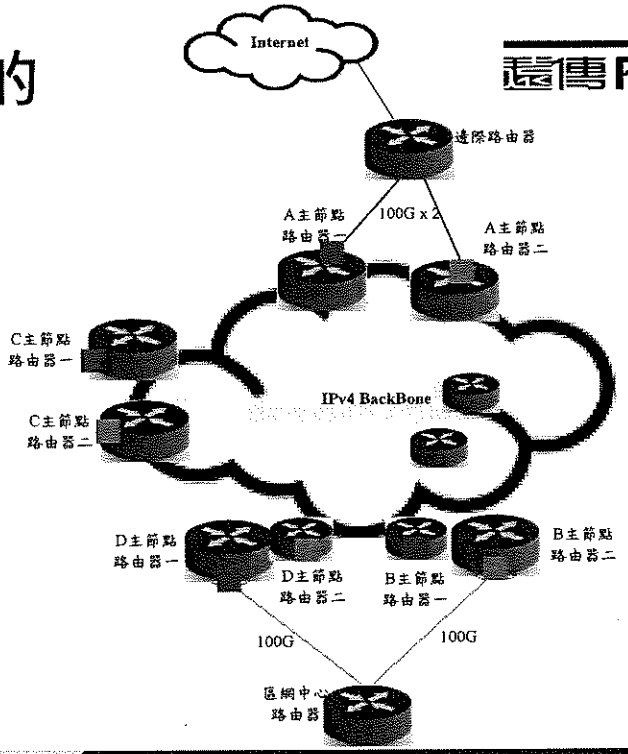
- 以Segment Routing取代MPLS
- TANet應用皆以VPN服務為替代
- 以服務計營商之架構應用
- 核心骨幹以IPv4為基礎，未來可替換為IPv6，提高安全性
- 提供獨立路由運算與交換角色(RR)



新一代教育學術網路協定
應用架構示意(主節點/區網中心)

100G/400G TANet的差異比較

TANet原100G架構：
(1) 100G線路速率之路由骨幹。
(2) 區網中心僅為單一路由器。
(3) 區網中心對雙中心之路由為主備(Active/Standby)
(4) IPv4與IPv6、MPLS/VPN服務為共用骨幹路由設備之三張網路架構



100G/400G TANet的差異比較

TANet新400G架構：

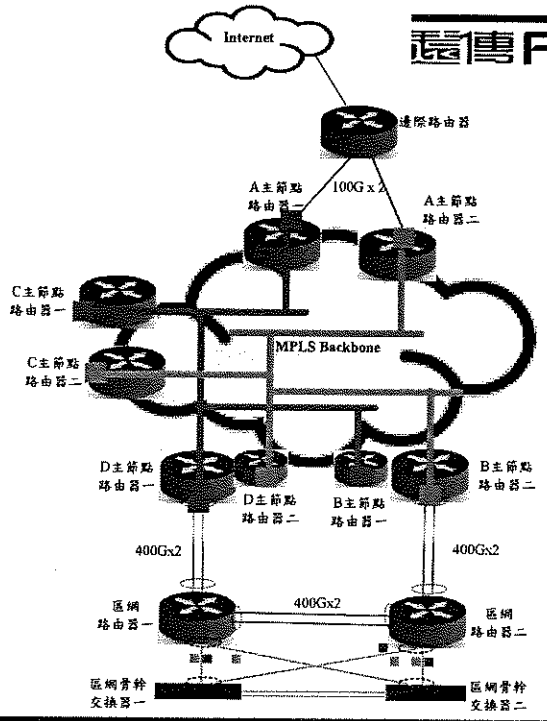
(1) 以SR取代MPLS，相關服務是以EVPN形式提供。

(2) IP為EVPN服務，路由轉發是以SR為基礎之運作模式。

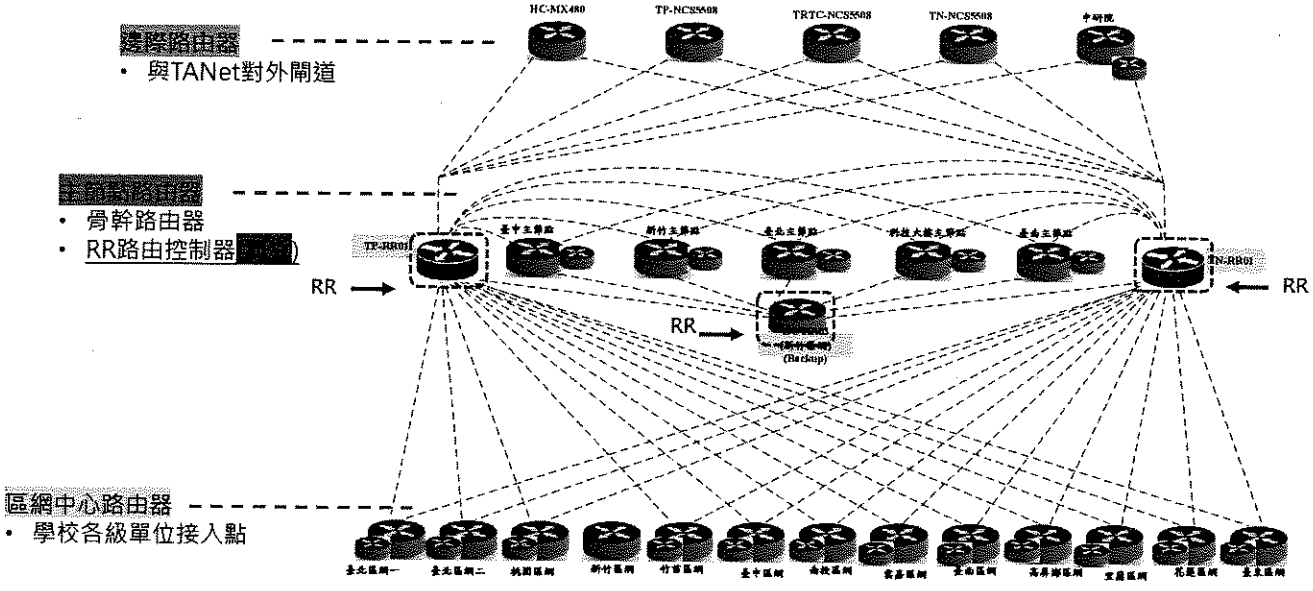
(3) 骨幹提供兩個EVPN 進行IP流量負載平衡，如圖示。

(4) 獨立的路由運算交換架構

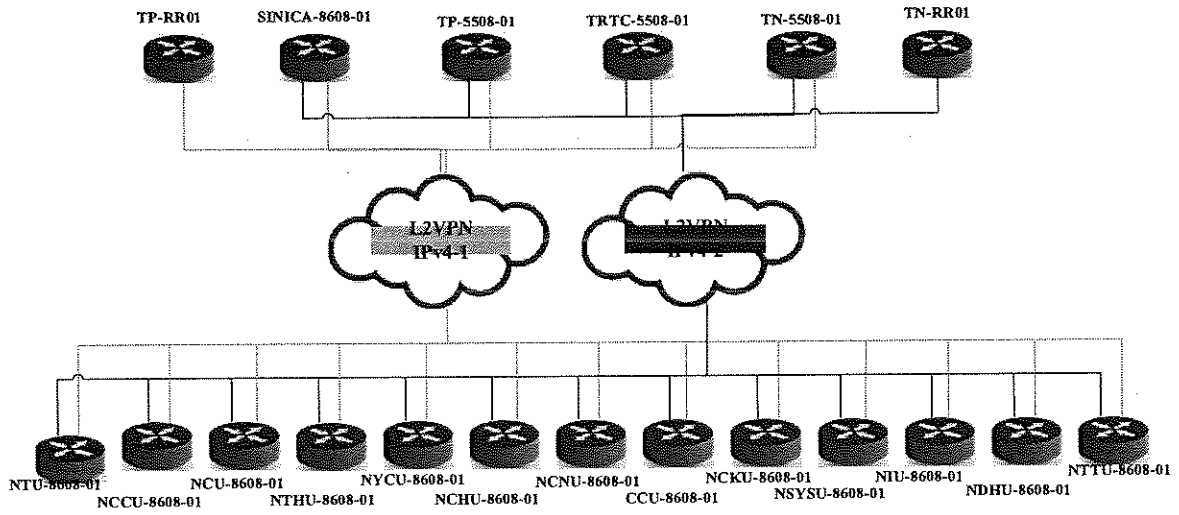
(5) 連線單位路由設備利用ECMP的路由機制，提供負載平衡及HA的功能。



TANet 400G通訊架構



IP EVPN之連線示意圖(負載平衡)



路由交換選擇基礎規則（待討論）

1.路由若是未有指定之BGP community時，則路由僅存在於接取本地端，預設RR不進行交換、轉發。

2.路由需出網時，則需標示正確之BGP community，才允許轉發至全域

3.各區網中心可藉由統一之路由標示，可選擇是否接收、傳送相關路由

4.區網中心發送之路由，RR將依一致之中心轉發規則分配至各節點

5. TANet預設不提供路由Transit之相關交換

6.建議連線單位，逐步改為BGP為主之連線協定，未申請ASN者，可由TANet統一核以Private BGP ASN，提供連線單位連線使用。

7.路由應以「明確網段」為主，域內不使用預設路由轉發流量，但區網中心可依需求使用預設路由(0.0.0.0/0)。

RR交換路由規則（待討論）

遠傳FET

- TANet RR預設僅針對以下的BGP Community進行交換
  - 1659:6666 當路由帶有此標籤時，RR予以交換至域內各節點
  - 1659:8888 當路由帶有此標籤時，RR予以交換至邊際路由器
  - 預設RR全數送出所有路由，由接收端自行取決路由

邊際路由路ISP路由標示（待討論）

遠傳FET

- 由eBGP 鄰居交換到的路由進行標示
- 邊際路由器的標示方式
  - 如 Telstra 『 17717:4367 』當由邊際路由器接收到來自此ASN 4367的路由時，以此community區別路由來源。
  - 如 Hinet 『 1659:3462 』當由邊際路由器接收到來自此ASN 3462的路由時，以此community區別路由來源。
  - 此路由仍需藉由RR允許之路由標示才予以交換

註：BGP community的碼，可另討論制定為最後版本。

主節點/區網中心外部路由標示（待討論）

遠傳FET

- 在主節點/區網中心標示
  - 因部分業者在區網中心布接的線路，做為流量負載分散使用，因此在接收到此路由時，需以下法標示：
    - 如Hinet在新竹主節點有此接線時，則需標示為『業者ASN:主節點代號』方式標示『3462:11003』
    - 如 Hinet在臺北區網一有一接入時，則需標示為『業者ASN:區網代號』方式標示『3462:11101』
    - 其餘依此類推
    - 此路由仍需藉由RR允許之路由標示才予以交換

註：BGP community可同時多重疊加、置換取代。

連線單位路由 – 縣市網中心（待討論）

遠傳FET

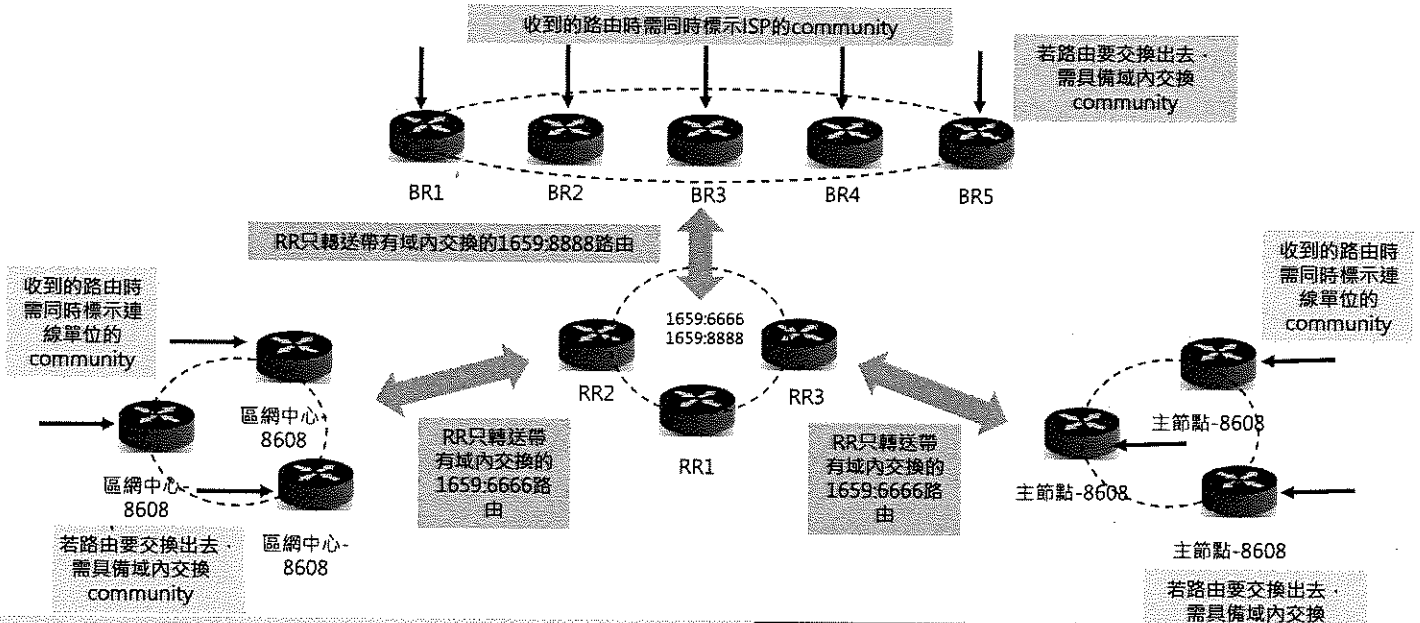
- 外部路由除了國內外的業者外，另指相關之相線單位。
- 連線單位可分為縣市網中心與其它兩個部分。
- 縣市網中心目前是以ISIS的協定接入，未來應考慮轉換至BGP為主，以利控管。
- 縣市網中心的路由接入時，以所在之區網中心為主，其標示應為『區網中心代碼: 縣市網中心ASN 』。
  - 如 臺北市網中心接入點為臺北區網一，則BGP代碼表示為『11101:65001 』。
  - 此路由仍需藉由RR允許之路由標示才予以交換

連線單位路由 – 其它（待討論）

- 其它連線單位目前可能以利用以下路由接入
  - 靜態路由 (無法路由交換)
  - OSPF (有限制之交換)
  - BGP (建議以BGP為主，以利控管)
- 相關之連線單位路由接入時，以所在之區網中心為主，其標示應為『區網中心代碼: 連線單位ASN編號 』。
  - 如 連線單位接入點為臺北區網一，則BGP代碼表示為『11101:65xxx 』。

註：連線單位ASN編碼，若該單位無此編碼時，需統一制定，建議為全域(TANet)唯一編碼。

BGP交換示意圖



代碼參考表（待討論）

地區名稱	代碼	地區名稱	代碼	地區名稱	代碼	地區名稱	代碼
臺北主節點	11001	臺北區網一	11101	臺北市教網	65001	臺南市教網	65014
科技大樓	11002	臺北區網二	11102	新北市教網	65002	高雄市教網	65015
新竹主節點	11003	桃園區網	11103	基隆市教網	65003	屏東縣教網	65016
臺中主節點	11004	新竹區網	11104	桃園市教網	65004	澎湖縣教網	65017
臺南主節點	11005	竹苗區網	11105	新竹市教網	65005	金門縣教網	65018
中研院	11006	臺中區網	11106	新竹縣教網	65006	連江縣教網	65019
		南投區網	11107	苗栗縣教網	65007	宜蘭縣教網	65020
		雲嘉區網	11108	臺中市教網	65008	花蓮縣教網	65021
		臺南區網	11109	彰化縣教網	65009	臺東縣教網	65022
		高屏澎區網	11110	南投縣教網	65010		
		宜蘭區網	11111	雲林縣教網	65011		
		花蓮區網	11112	嘉義市教網	65012		
		臺東區網	11113	嘉義縣教網	65013		

註：其餘連線單位之代碼，可參考制定。

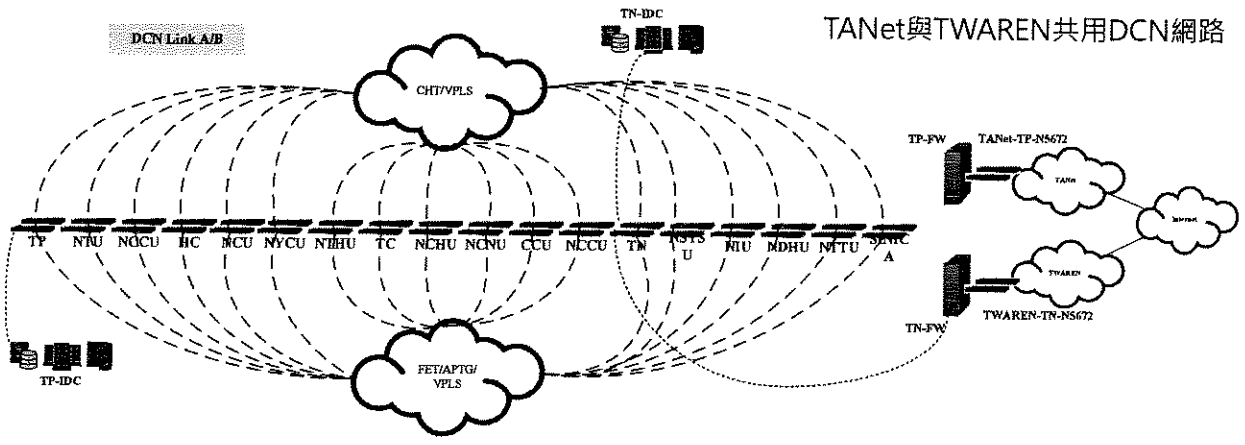
DCN網管網路

- 介紹新舊之網管網路差異
- 說明新網管網路特色

DCN管理網路特色

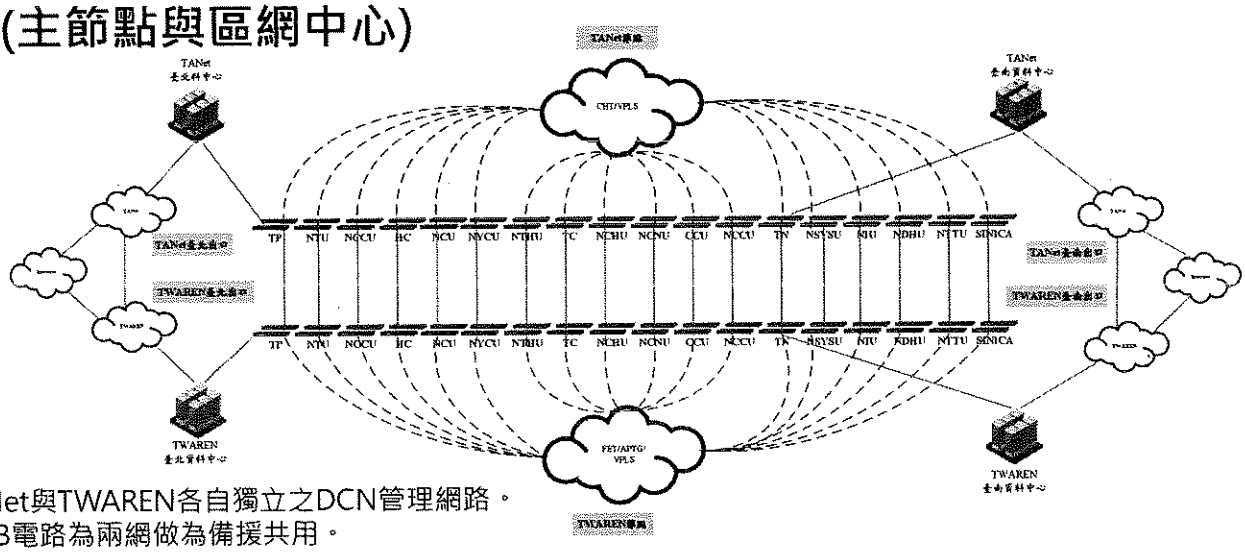
- 符合A級機關之資安要求
  - 多因子認證
  - 正向表列資安存取規則
  - GCB/VANS
- 單一入口存取
  - 所有管理與維護連線皆採「SSLVPN」形式登入
  - 所有管理與維護連線皆需經由「存取中繼閘道(跳板機)」操作
- 完整存取記錄稽核
  - 任何人員的連線起始至結束皆全程錄影、記錄

100G暨有DCN架構圖
(主節點與區網中心)



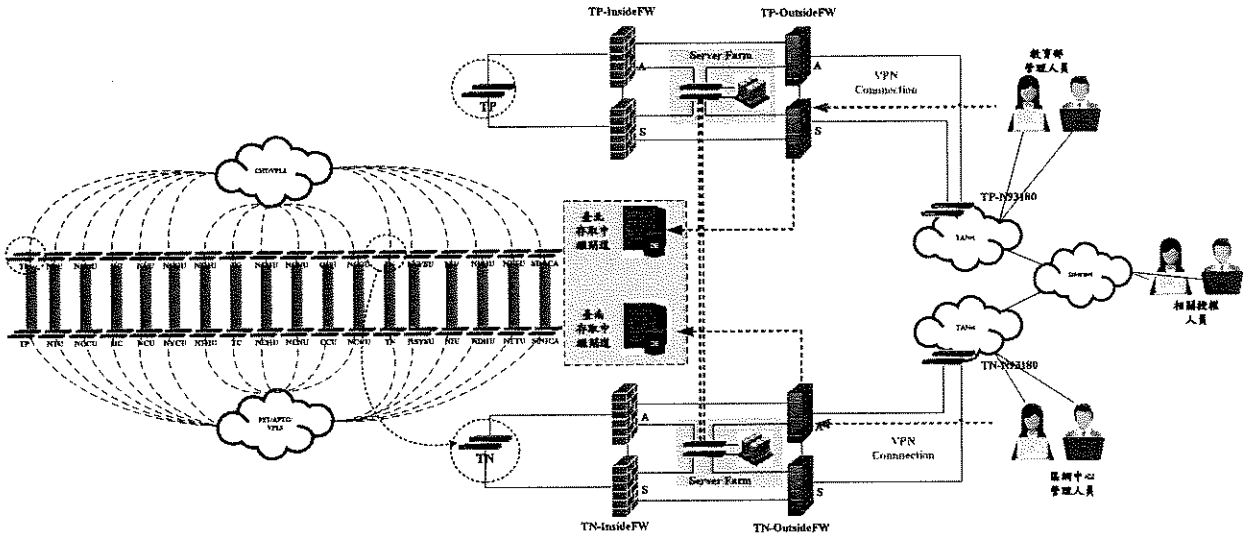
400G 雙網獨立管理架構

(主節點與區網中心)



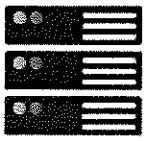
TANet與TWAREN各自獨立之DCN管理網路。
OOB電路為兩網做為備援共用。

TANet 400G 資料中心架構圖



400G網路管理資安角色

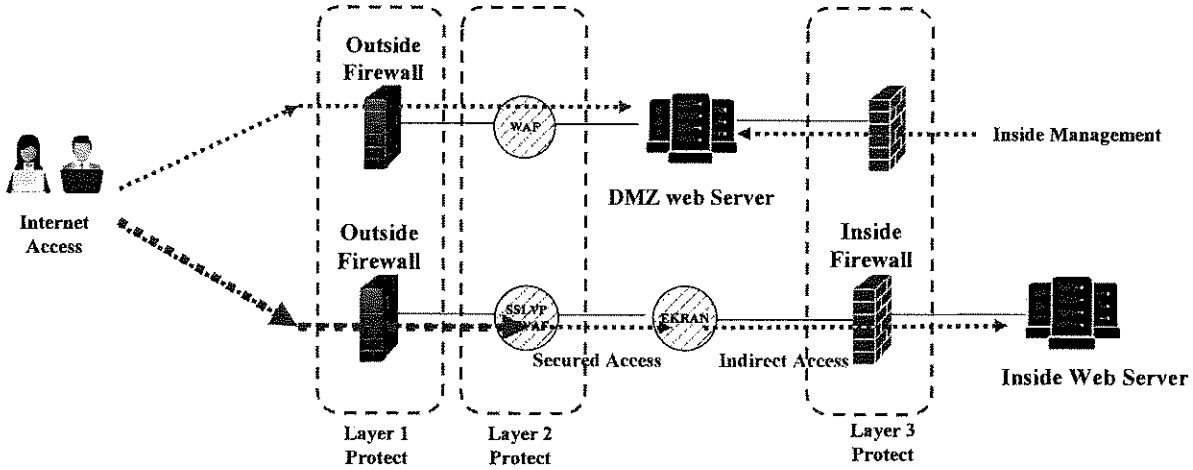
遠傳FET

VPN閘道器	AD 網域控制器	中繼存取閘道 (跳板機)	雙因子認證 IDExpert	Cisco ISE	外部防火牆	內部防火牆
						
用於管理或維修人員由外部登入連線至DCN之閘道器，提供SSL 或IPSec 等方之VPN加密通道存取	本專案中用來建立本案系統中預設所有用戶的帳號管理，並提供DNS服務。 用於用戶的第一階之帳密管理	多用戶登入平臺，所有人員皆需經由此一設備來進行DCN之設備與系統管理；本系統將完整側錄所有登入人員的所有操作行為	本設備提供多因子認證/單一登入機制，本案中人員登入皆採雙因子的機制進行登入管制	思科之身份認證系統，用於管理基於RADIUS或TACACS的設備進行人員認證、操作權限、稽核記錄	外部防火牆的角色用於面對網際網路端，用於區隔與DCN之安全通訊防護	內部防火牆的角色用於區隔各區網或GigaPOP與資料中心之安全通訊防護

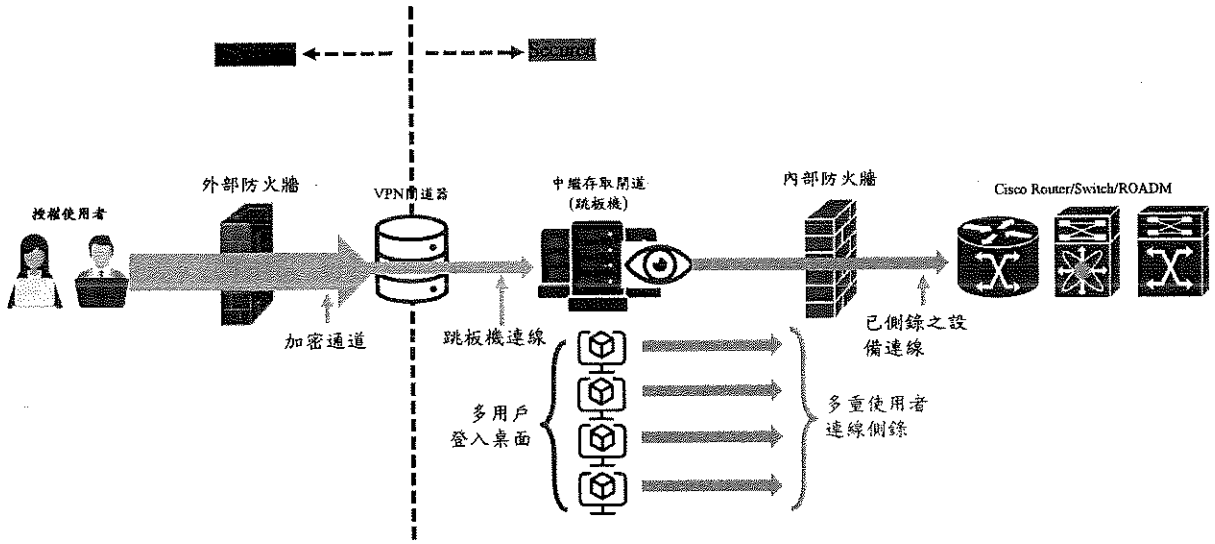
遠端連線 – VPN/WAF佈建規則

遠傳FET

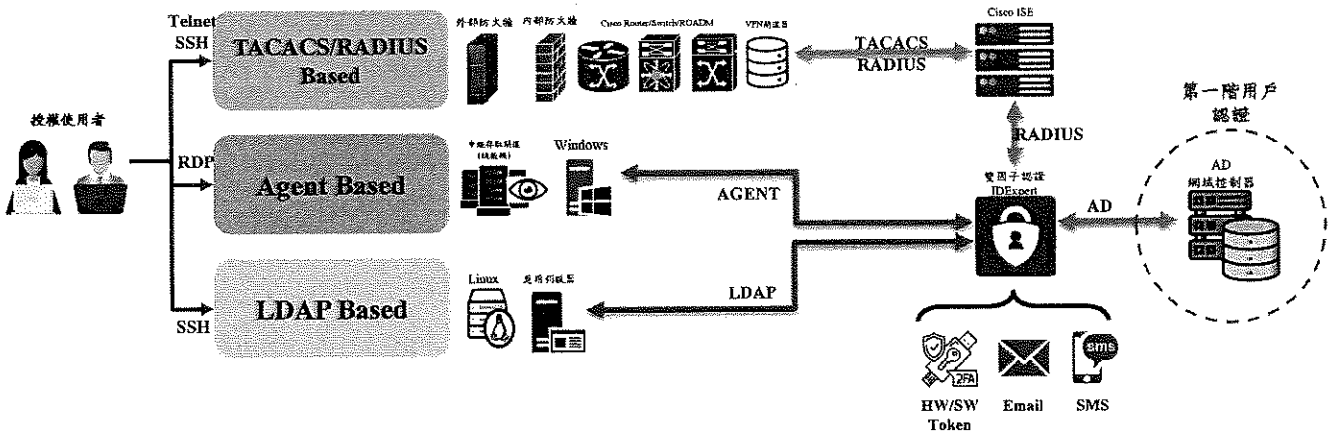
- 第一對介面將SSLVPN與WAF整合，保護位於內部防火牆之網站
- WAF另一對介面提供保護位於DMZ區之網站伺服器



管理維護人員連線存取路徑



人員身份驗證- 多因子認證機制



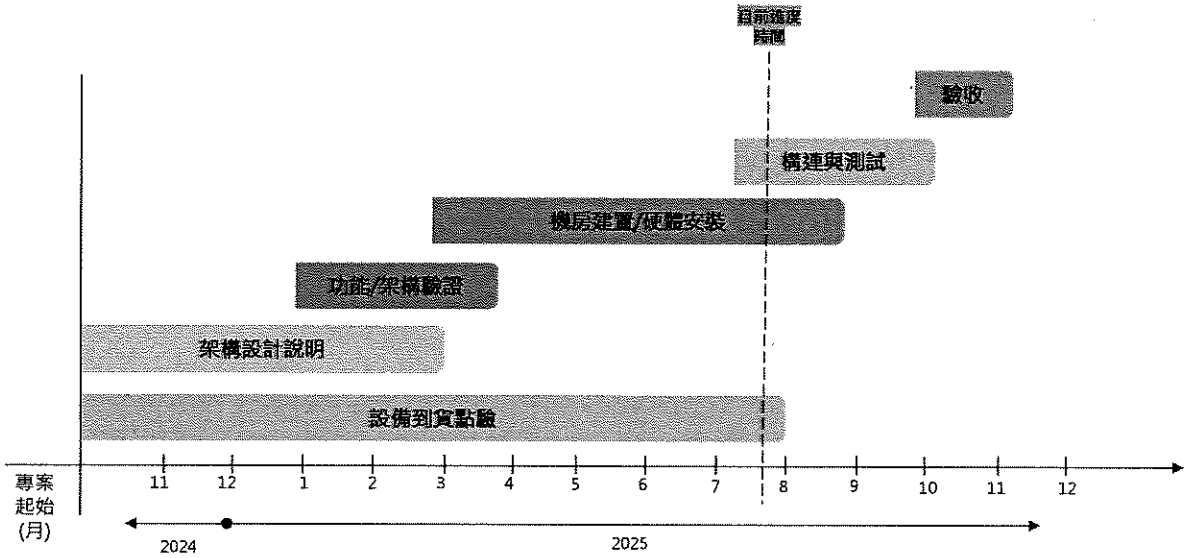
Agenda

遠傳FET

- 新一代 TANet 400G網路特色
- 新舊世代 TANet 比較
- 專案建置期程說明
- 後續議題討論

專案建置時程

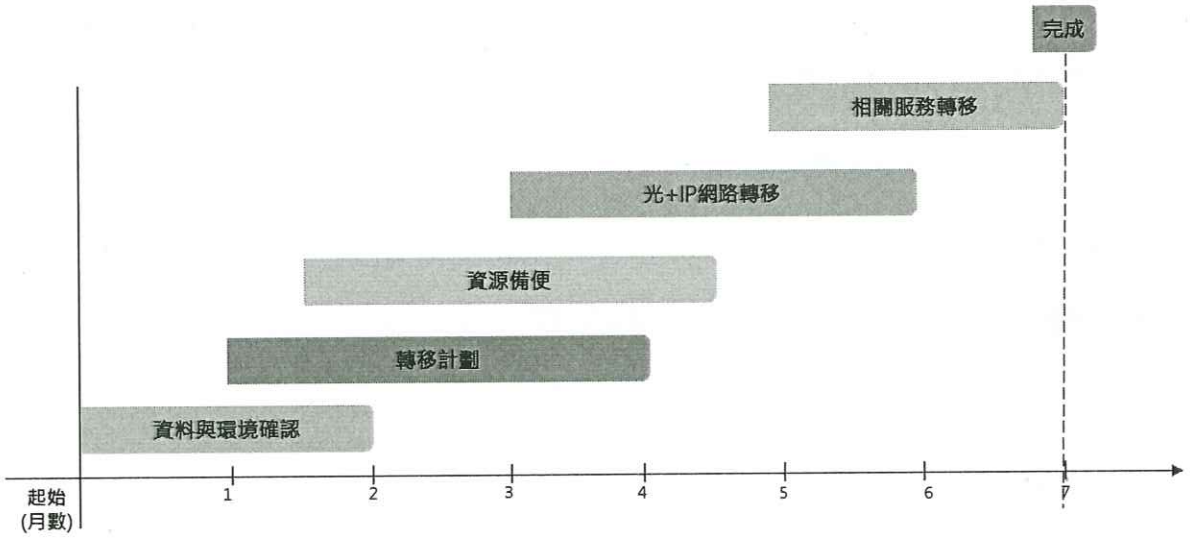
遠傳FET



專案建置配合事項

階段	階段名稱	工作摘要	教育部/國網	區網中心	遠傳團隊	備註
1	設備到貨點驗	依出貨期程點驗交付本案軟硬體	√		√	
2	架構設計說明	依RFP與建議書提報確認佈建架構	√		√	
3	功能架構驗證	建置LAB並將重點項目功能測預化試驗證	√		√	
4	機房建置/硬體安裝	依本案建置需求進行機房建置安裝	√	√	√	
5	構連與測試	相關傳輸、網路與系統依本案驗收架構上線運作，且需獲得功能驗證	√	√	√	
6	驗收	依各區驗收項目範圍進行查驗	√	√	√	

服務轉移時程(預估)



服務轉移配合事項

遠傳FET

階段	階段名稱	工作摘要	教育部/國網	區網中心	遠傳團隊	備註
1	資料與環境確認	收集各區機房之既有接線、介面、服務型態並確認轉移之方式	√	√	√	區網與六都配合調查
2	轉移計劃	進行線路佈建、服務設計轉移之對應與方式，並製作計劃及確認	√	√	√	區網與六都配合實施
3	資源備便	確認轉移之人力、時間、佈線與所需之資料配合	√	√	√	
4	光傳輸+IP網路轉移	轉換骨幹與各節點之光傳輸/IP網路，將流量開始導入新網(不含連線單位)	√	√	√	六都既有維護商需配合電路轉移
5	相關受務轉移	連線單位之服務配合轉移改接	√	√	√	
6	完成	確認服務轉移完成且正常運作	√	√	√	

Agenda

遠傳FET

- 新一代 TANet 400G網路特色
- 新舊世代 TANet 比較
- 專案建置期程說明
- 後續議題討論

後續討論議題一

遠傳FET

- **TANet BGP路由管理政策...**
  - TANet對外與ISP之間網段與BGP Community標示規則
  - TANet內部之BGP Community標示規則
  - TANet路由政策
  - 縣市網接入之路由方式

後續討論議題二

遠傳FET

一. 區網中心後續改接配合事項討論...
二. 連線單位分校校區跨區網中心之整合架構討論...

遠傳FET

只有遠傳 沒有距離

臺灣學術網路(TANet)技術小組第97次會議

討論事項-1
縣市及校園網路設置基準

資科司學網科

- **說明：**

  因應數位學習全面推動，需強化從資訊基礎設施到資安管理的整體網路支援環境，以確保穩定且高速的網路服務品質，故針對縣市教育網路中心及學校網路環境相關面向，建立具體明確的設置基準，作為一致性評比的依據，提供 後續優化網路環境與推動精進措施的重要參考。

- **擬辦：**

  1. 初版網路設置基準已於本部114年網路優化補助案提供，本部將持續評估各縣市執行概況，滾動調整設置基準，提供各縣市因應財劃法於縣市內爭取網路優化經費參考。
  2. 配合網路基準測量作業，本部規劃提供部分測速盒供縣市安裝使用。

縣市教網中心 網路檢核項目

縣市教網中心 網路檢核項目

一、維運管理人員的能力培養		
項目	說明	檢核方式
維運管理人員能力	縣市配置網管人員且具備基本能力	*網路管理經驗年資、參加教育訓練時數、資訊證照等網路管理基本能力佐證資料
教育訓練	提供資訊窗口關於網路設備、智慧網路監控、網路問題排除等基礎教育訓練課程	*定期提供網管人員專業教育訓練

縣市教網中心 網路檢核項目

二、網路維運		
項目	說明	檢核方式
網路架構	• 定期更新網路架構圖(依網路圖繪製標準) • 骨幹網路設備具有效期內保固維護合約(合約內明訂定有保固完修時間) • 縣市網骨幹網路作用中頻寬(不含備援電路頻寬)大於或等於連接區網中心之網路總頻寬(教育部租用電路頻寬)	*網路架構圖更新日期為今年 *骨幹網路係指縣市網路中心內將區網連接至學校(集縮)電路間之網路架構 *在保固維護效期內或合約刻正簽辦中文件 *縣市網骨幹網路作用中頻寬數
網路韌性	• 中心網路架構設計具備足夠韌性，不因單一障礙影響重要服務運作 • 定期辦理網路障礙緊急應變演練(網路設備或電路故障之應變演練)	*縣市網中心之網路服務可用率達99.9% *最近辦理網路障礙應變演練結果
支援IPv6	• 網路傳輸及網路基礎服務支援IPv6(如：DNS等)	*學校電腦連接sp.tanet.edu.tw可呈現IPv6位址

縣市教網中心 網路檢核項目

三、無線網路		
項目	說明	檢核方式
存取控制	• 設置學習載具無線上網存取管控機制(縣市統一管控或學校自行管控)	*縣市網學習載具無線上網存取管控機制
無線漫遊	• 提供eduroam無線網路雙向漫遊服務	*縣市eduraom服務主機運作概況
支援IPv6	• 行動學習載具配發IPv6位址並可連接網際網路	*學習行動載具連接sp.tanet.edu.tw可呈現IPv6位址

縣市教網中心 網路檢核項目

四、網路管理		
項目	說明	檢核方式
電路流量監測	• 對區網中心電路進行流量監測(bps/pps) • 對學校集縮電路進行流量監測(bps/pps)	*縣市網至區網電路之bps及pps *縣市網至學校(集縮)電路之bps及pps
異常自動告警	• 對區網中心及學校之網路監測設有告警值並主動通知網管人員	*對區網電路流量設有告警值且有斷線告警機制 *學校(集縮)電路流量設有告警值，且對各學校網路連通有斷線告警機制
網路障礙處理	• 訂有網路障礙處理程序並落實執行 • 設有單一報修窗口協助學校處理網路障礙	*網路障礙處理程序及相關紀錄 *網路報修單一窗口資料及相關紀錄

學校 網路檢核項目

學校 網路檢核項目

一、校園網路維運		
項目	說明	檢核方式
網路維運人力	• 設置網路管理人員並作為學校網路管理窗口	*網路管理人員聯絡資訊
校園網路架構	• 依網路架構繪製標準繪製學校網路架構圖	*學校網路架構圖 *學校網路連線架構以至多三層次為原則
對外電路頻寬	• 學校對外電路頻寬符合班級數對應頻寬規定 • 學校對外可用最大頻寬達租用頻寬之70%	*sp.tanet.edu.tw之單台有線網路量測結果
對外電路監控	• 對學校對外電路進行流量監測(bps/pps)	*學校連接至縣市網電路之bps及pps
智慧網路管理	• 設置有智慧網路管理系統	*學校連接縣市網電路流量設有告警值且有斷線告警機制 *監測校園網路設備設且有異常告警機制

學校 網路檢核項目

二、校園無線網路		
項目	說明	檢核方式
無線網路存取	• 設置無線上網管控機制(縣市統一管控或學校自行管控)	*學校學習載具無線上網存取管控機制
無線頻道管理	• 5GHz與2.4GHz頻道分別設置SSID • 全校各班級教室需通過無線網路品質檢測	*設有5GHz SSID供行動學習載具優先使用 *以班級人數之學習載具進行網路品質量測(sp.tanet.edu.tw)，全數載具通過6Mpbs群組測試
支援無線漫遊	• 若學校提供訪客無線網路服務，應同時提供eduroam 服務。	*在學校可使用該縣市之帳號透過eduroam連接sp.tanet.edu.tw *在學校可使用非該縣市之帳號透過eduroam連接sp.tanet.edu.tw

學校 網路檢核項目

三、協助辦理事項		
項目	說明	檢核方式
資訊文件化	• 學校訂有IP位址配置管理程序並有IP位址配置紀錄 • 學校訂有網路障礙處理程序(或由縣市統一訂定)	*IP配置紀錄表 *學校網路障礙報修程序
網路異常處理	• 網路管理人員知悉縣市教網中心服務窗口 • 網路管理人員依網路障礙處理程序辦理(網路障礙處理紀錄)	*縣市網服務窗口聯絡資訊 *學校網路障礙報修紀錄
資安事件通報	• 網路管理人員知悉資安事件通報程序	*學校通報資安事件程序文件

延伸事項

(測試盒子)

背景說明

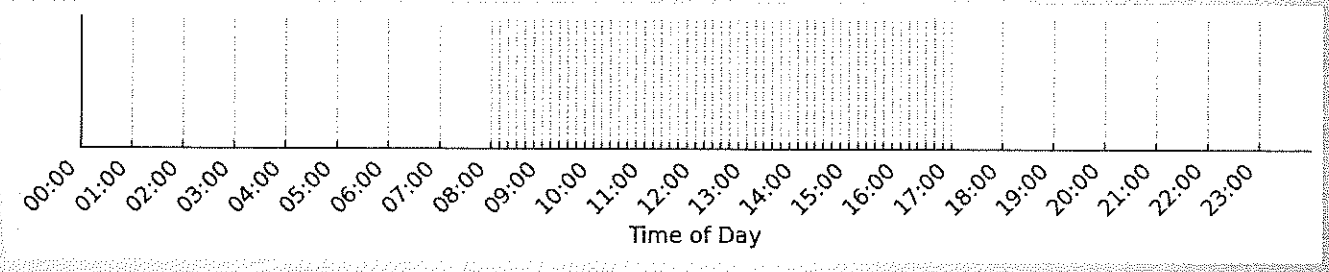
- 為了解校園聯外網路頻寬使用效能，以確保有穩定且順暢的上網服務因應數位學習使用，本部規劃以「測速盒子」協助本部及縣市了解校園聯外網路服務品質，以作為後續頻寬提升、網路精進之評估參考。

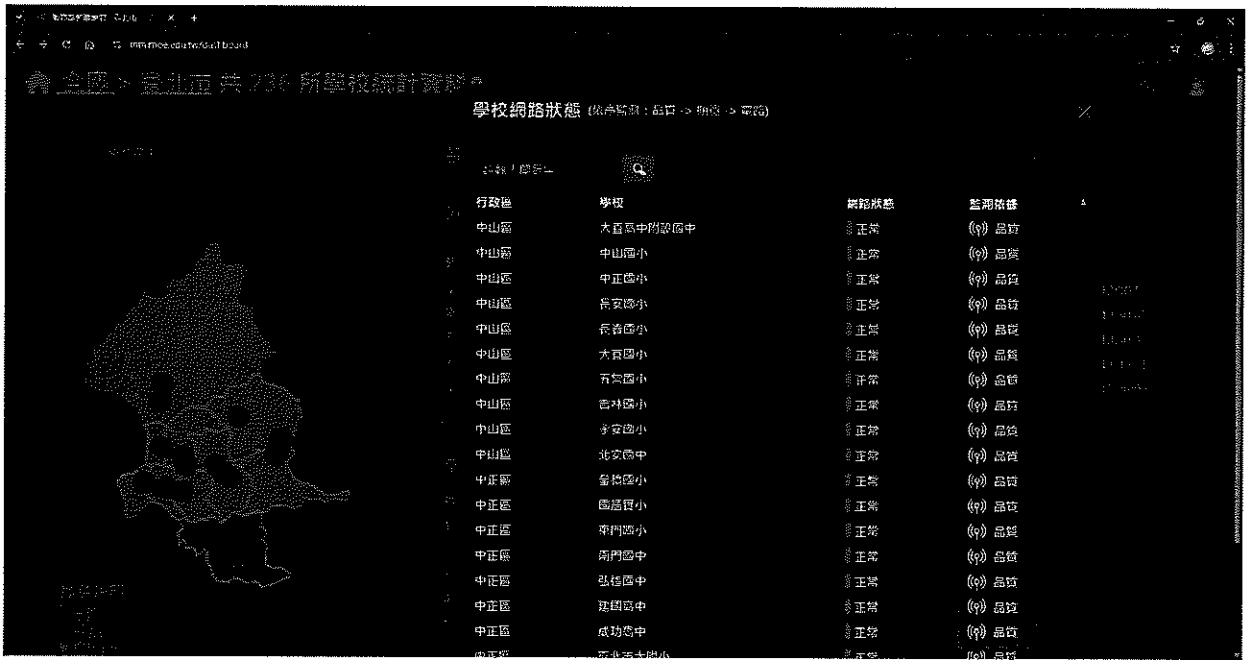
背景說明

- 目前已有縣市至區網、區網至區網間的TANet網路品質測試，校園至縣市網路品質測量為最後一哩路。

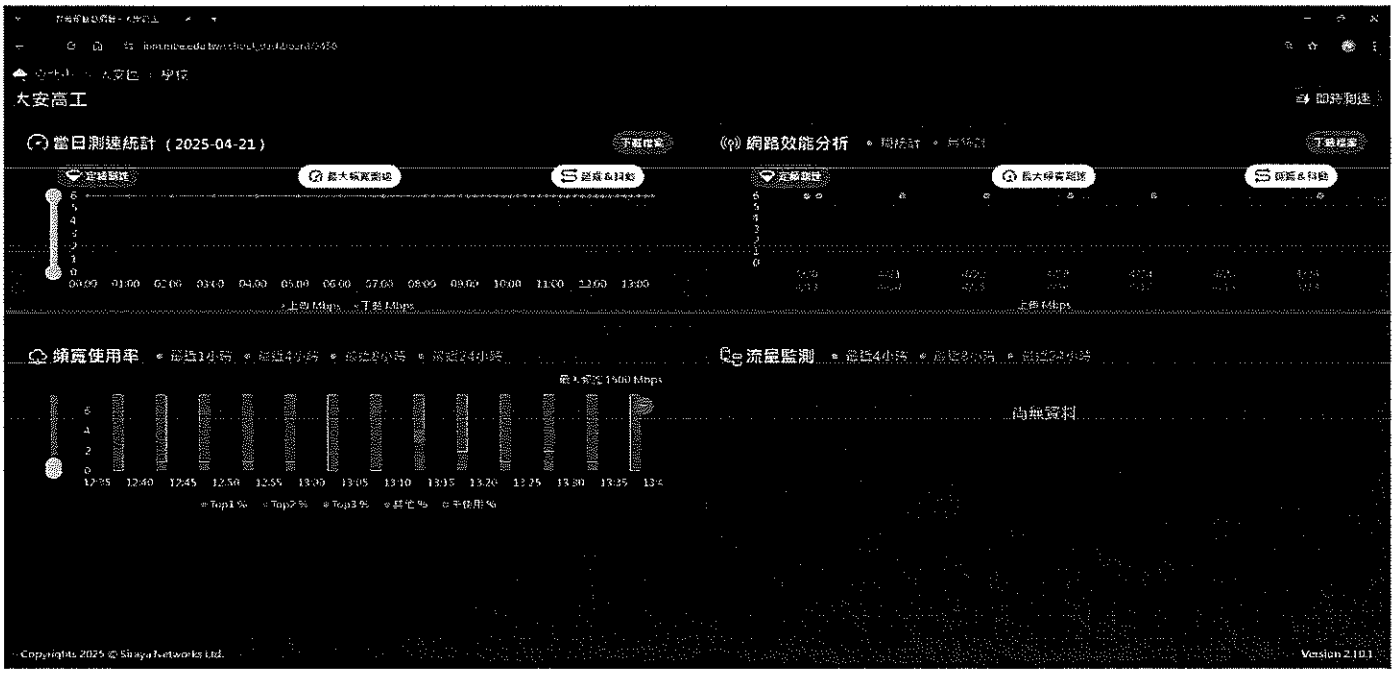
◆ 自動化測速機制說明

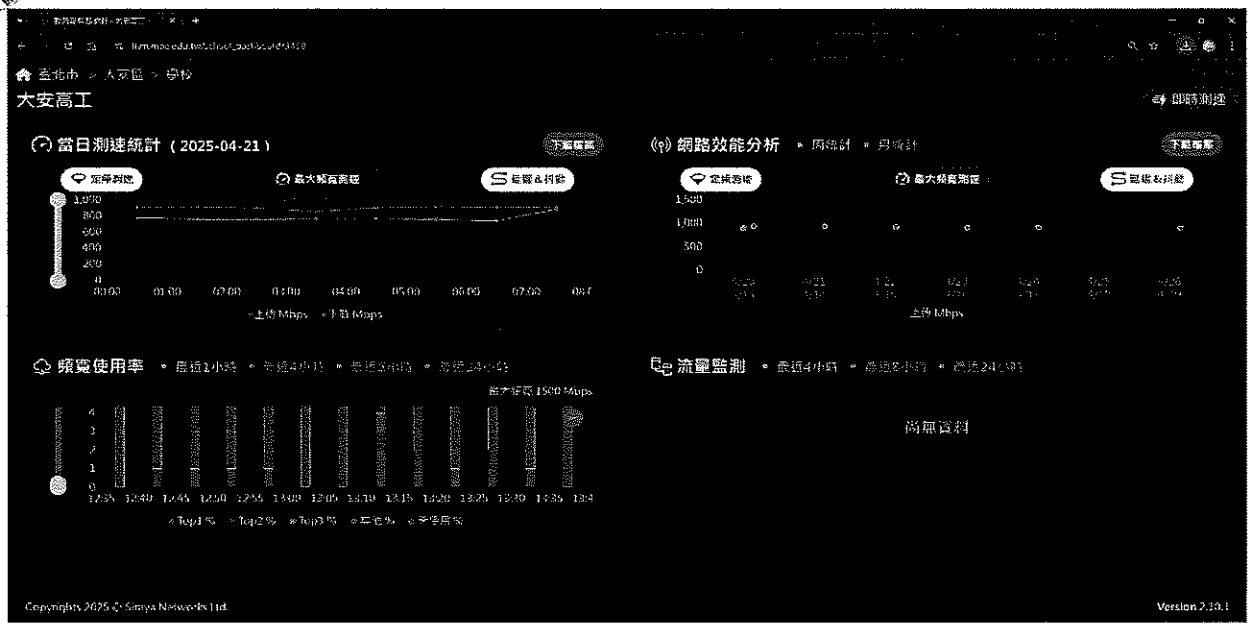
測試模組	測試內容	頻率
網路可用性測試	6Mbps測速(8AM-5PM)	每10分鐘
壓力測試	1Gbps全速測試(Others)	每小時
多協議測試	UDP、TCP	-
封包遺失及延遲測試	6M UDP 流量下的遺失率	同6M測速
	-	-



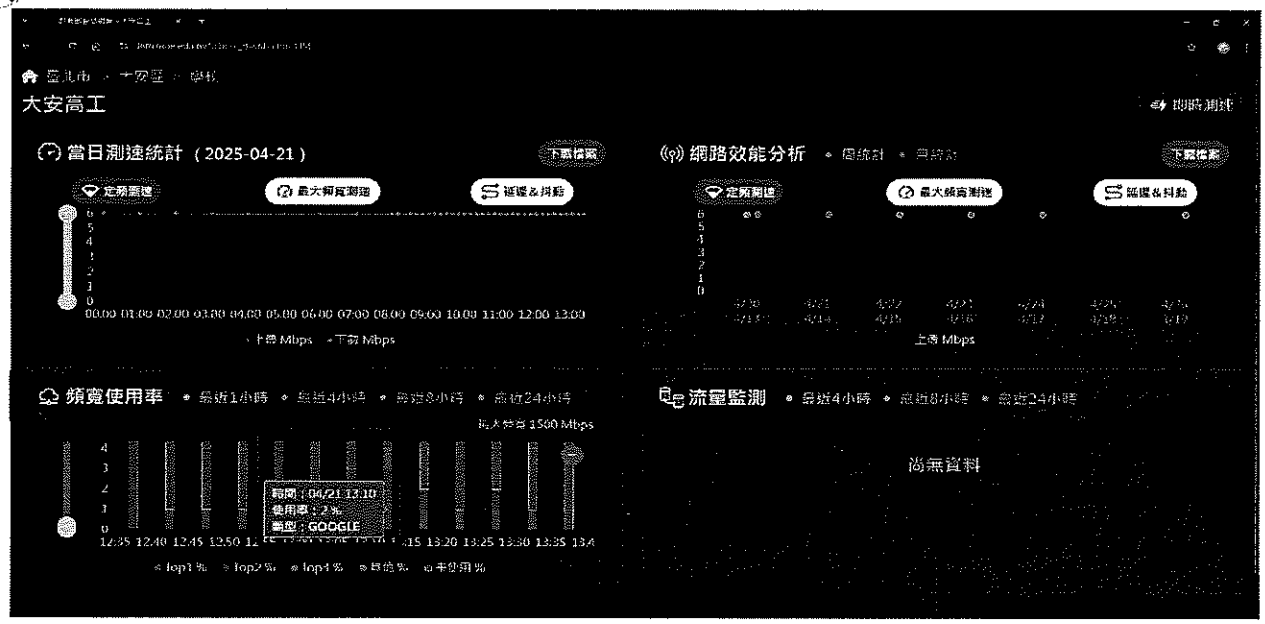


◆可透過儀表錶觀測當日學校各時段測速統計(定頻、最大頻寬及延遲、抖動狀態)

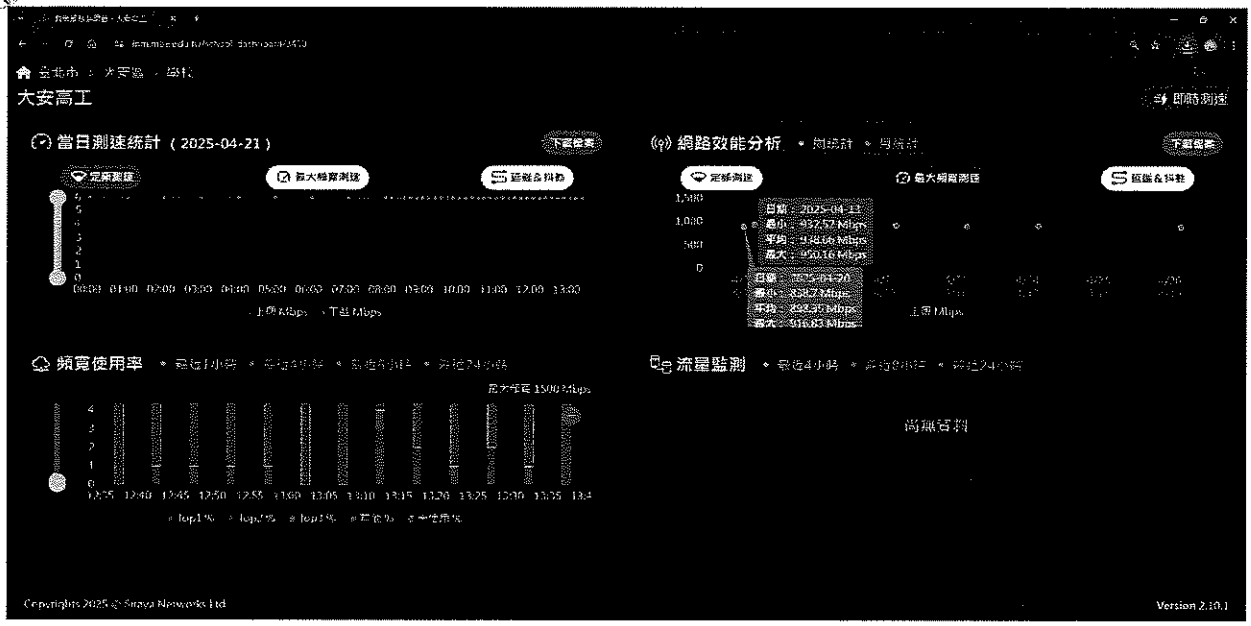




◆可透過儀表錶觀測學校各時段寬頻使用率 (明確看出是否教學使用網頁或其他分類)



◆可觀測學校網路效能分析 (依週統計或月統計)



◆可透過下載檔案得到相關報表 (依週統計或月統計)

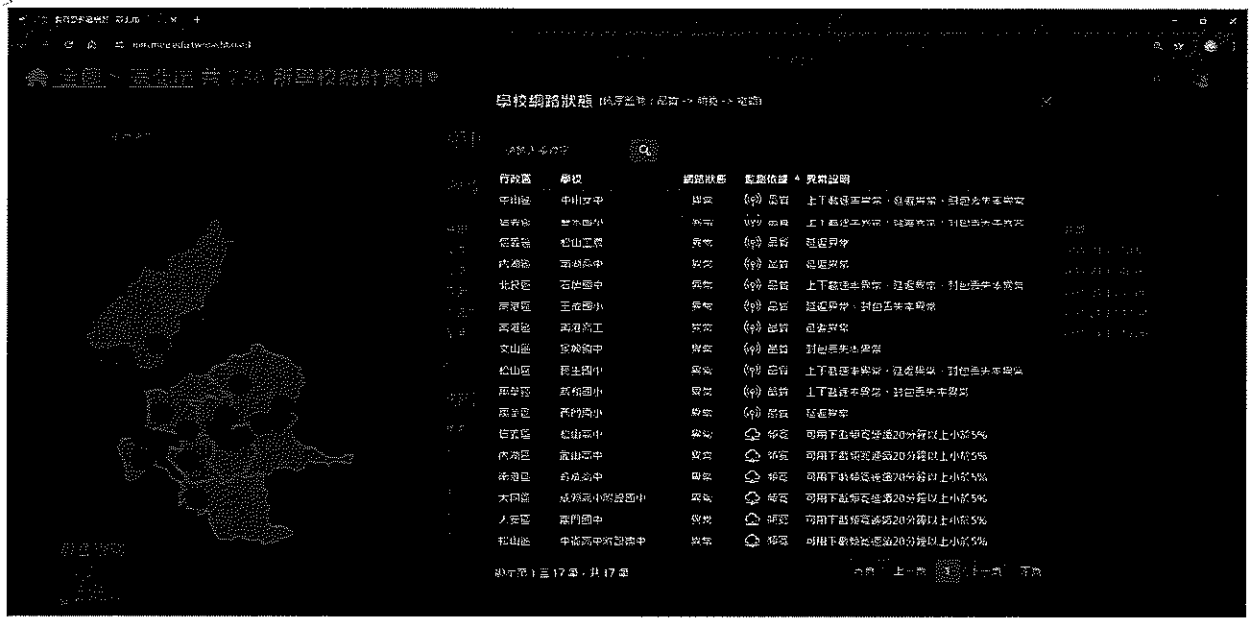
當日測速統計

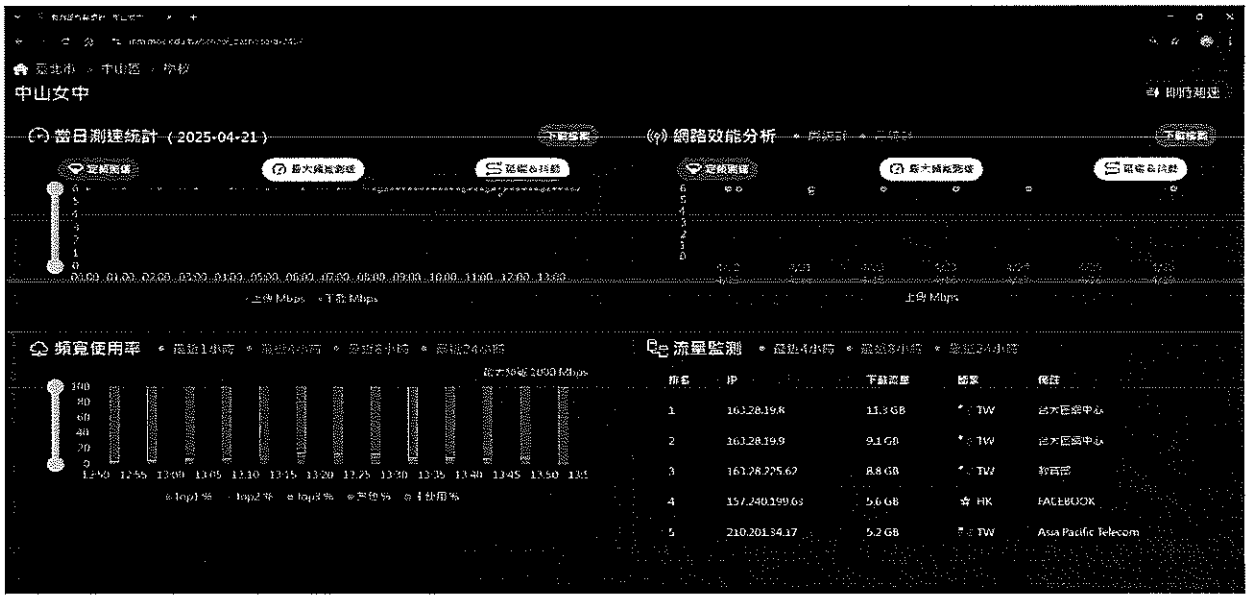
時間	定頻測速		最大頻寬測速		延遲 & 抖動	
	上傳(Mbps)	下載(Mbps)	上傳(Mbps)	下載(Mbps)	延遲(ms)	抖動(ms)
00:00	6	6			5.384	0.942
00:30			905.06	775.63	5.587	1.017
01:00	5.98	6			5.216	1.121
01:30			913.21	758.6	5.449	1.022
02:00	6	6			5.925	0.999
02:30			895.76	756.64	5.572	0.896
03:00	5.98	6			5.395	1.185
03:30			852.59	764.48	4.422	1.013
04:00	6	5.98			5.482	0.891
04:30			902.44	764.35	5.464	1.304
05:00	5.98	6			5.647	1.363
05:30			912.87	758.99	5.309	0.728
06:00	5.98	6			5.641	1.011
06:30			905.9	739.27	6.028	1.778
07:00	5.98	6			5.926	1.731
07:30			909.08	882.28	5.593	0.887
08:00	5.98	6			5.854	1.636
08:10	5.98	6			6.146	1.881
08:30	5.98	6			7.064	2.958
08:40	5.98	6			4.706	0.412
08:50	6	6			5.173	1.101
09:00	5.98	6			4.058	0.49
09:10	6	6			4.585	0.443
09:20	5.98	6			6.525	2.672
09:30	6	6			6.299	1.671
09:40	6	6			6.391	1.361
09:50	6	5.98			3.305	0.592
10:00	6	5.98			9.953	10.257
10:10	6	6			5.251	0.284
10:20	6	6			6.11	0.978
10:30	6	6			8.607	5.876
10:40	6	5.98			5.937	1.185
10:50	6	6			6.215	1.275
11:00	5.98	6			5.682	1.44

當月測速統計

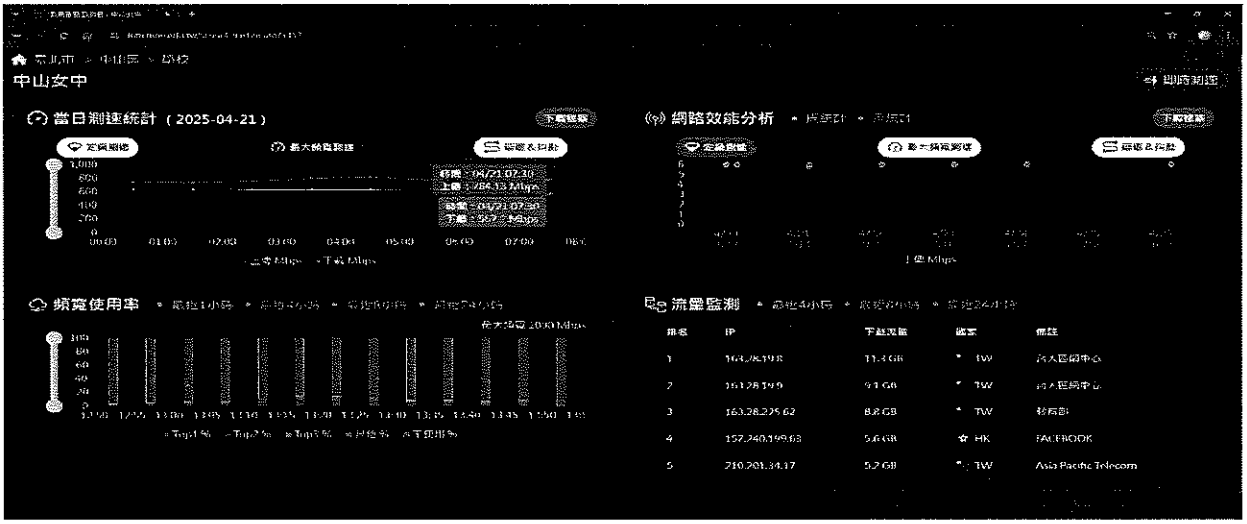
日期	定頻測速						最大頻寬測速						延遲 & 抖動					
	上傳(Mbps)			下載(Mbps)			上傳(Mbps)			下載(Mbps)			延遲(ms)			抖動(ms)		
	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	
2025-04-01	6	5.96	5.99	6	4.42	5.93	938.83	925.02	933.87	930.11	924.61	928.01	285.47	4.316	19.495	62.117	0.224	8.4
2025-04-02	6	5.92	5.99	6	5.75	5.95	947.08	934.3	939.96	930.11	845.42	921.92	166.37	4.065	11.132	29.3	0.273	2.4
2025-04-03	6	5.93	5.98	5.98	5.92	5.95	947.64	931.97	937.97	930.2	927.03	928.36	8.528	4.248	5.515	3.751	0.248	1.2
2025-04-04	6	5.94	5.99	5.99	5.93	5.96	950.44	931.66	938.04	930.69	924.82	928.67	26.965	4.325	6.145	48.398	0.289	2.0
2025-04-05	6	5.93	5.99	5.98	5.92	5.96	938.65	933.24	936.66	930.81	924.95	928.17	9.959	3.845	5.985	11.849	0.45	2.1
2025-04-06	6	5.93	5.99	5.98	5.92	5.96	935.7	930.96	935.04	930.82	923.18	928.49	16.437	4.523	6.52	19.725	0.346	2.6
2025-04-07	6	5.89	5.99	5.99	5.14	5.93	939.69	872.05	931.22	936.96	913.41	928.83	233.531	4.478	27.064	111.551	0.23	9.1
2025-04-08	6	5.98	6	6	4.19	5.94	942.4	888.7	931.34	937.38	904.32	933.7	288.036	4.52	25.215	256.072	0.321	7.6
2025-04-09	6	5.97	6	6	5.76	5.99	935.46	915.89	933.91	937.91	885.23	931.15	185.241	4.625	16.366	44.672	0.284	4.1
2025-04-10	6	5.98	6	6	5.45	5.96	939.1	926.91	935.72	937.7	931.62	935.73	205.862	4.413	25.935	39.397	0.47	5.2
2025-04-11	6	5.97	6	6	5.97	6	938	929.73	935.32	937.65	810.47	926.95	35.264	4.216	7.2	1396.774	0.251	20
2025-04-12	6	5.97	5.98	6	5.97	6	952.36	930.17	937.56	937.63	929.09	935.76	16.503	4.146	5.823	4.107	0.212	1.3
2025-04-13	6	5.92	6	6	5.97	5.99	950.16	932.52	938.66	937.97	932.09	936.1	8.717	3.982	5.591	5.828	0.47	1.6
2025-04-14	6	5.92	6	6	5.77	5.95	938.93	936.44	937.8	937.38	931.78	935.49	203.225	3.967	25.692	49.892	0.353	4.5
2025-04-15	6	5.97	6	6	5.97	6	938.63	876.36	924.7	937.73	731.23	885.58	206.653	4.553	8.864	663.969	0.206	30
2025-04-16	6	5.97	5.99	6	5.97	6	919.55	874.58	905.1	926.63	727.91	795.13	9.104	4.713	6.177	4.214	0.57	1.7
2025-04-17	6	5.97	5.99	6	5.97	6	918.22	896.86	909.95	930.49	722.7	804.4	109.594	4.585	7.832	223.083	0.175	5.1
2025-04-18																		
2025-04-19	6	5.98	5.99	6	5.98	6	917.38	852.03	891.28	929.44	726.85	782.89	6.379	4.751	5.372	2.909	0.691	1.1
2025-04-20	6	5.97	5.99	6	5.97	6	916.83	838.7	896.35	783.14	725.26	757.94	7.893	3.978	5.417	4.852	0.272	1.1

◆透過儀錶版觀測異常資訊

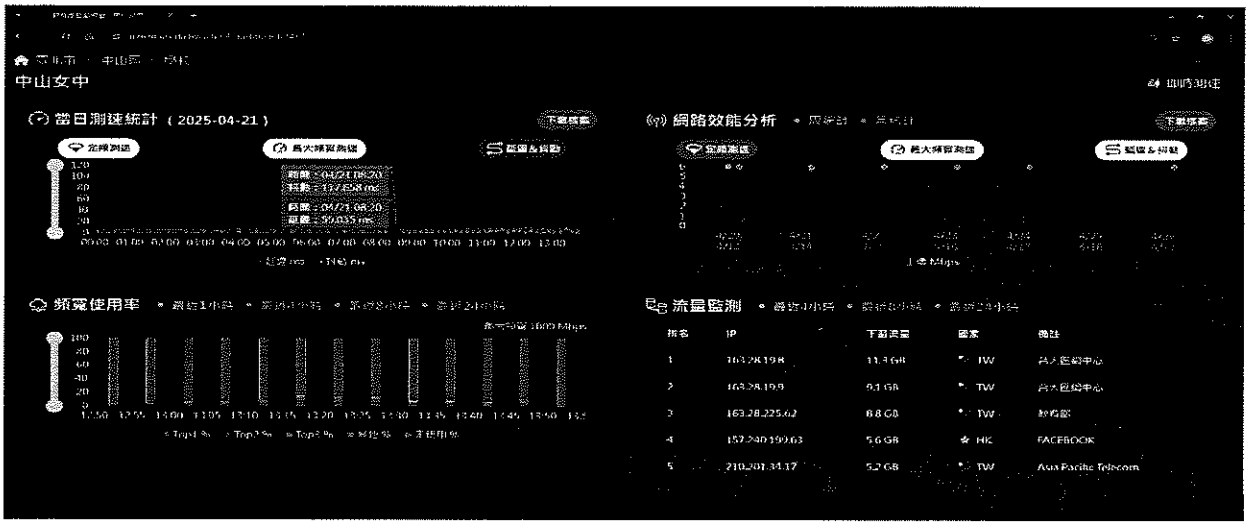



中山女中
當日測速統計（2025-04-21）
網路效能分析
頻寬使用率
流量監測
排名 IP 下載流量 國家 備註
1 163.28.19.8 11.3 GB TW 台大醫療中心
2 163.28.19.9 9.1 GB TW 台大醫療中心
3 163.28.225.62 8.8 GB TW 新百部
4 157.240.199.63 5.6 GB HK FACEBOOK
5 210.201.34.17 5.2 GB TW Asia Pacific Telecom

上下載速率異常


中山女中
當日測速統計（2025-04-21）
網路效能分析
頻寬使用率
流量監測
排名 IP 下載流量 國家 備註
1 163.28.19.8 11.3 GB TW 台大醫療中心
2 163.28.19.9 9.1 GB TW 台大醫療中心
3 163.28.225.62 8.8 GB TW 新百部
4 157.240.199.63 5.6 GB HK FACEBOOK
5 210.201.34.17 5.2 GB TW Asia Pacific Telecom

抖動異常


中山女中
當日測速統計（2025-04-21）
網路效能分析
頻寬使用率
流量監測
排名
IP
下載流量
國家
備註
1
163.28.19.8
11.3 GB
TW
2
163.28.19.9
9.1 GB
TW
3
163.28.225.62
6.8 GB
TW
4
157.240.190.63
5.6 GB
HK
FACEBOOK
5
210.201.34.17
5.2 GB
TW
Asia Pacific Telecom

TLP:WHITE

臺灣學術網路 電腦危機處理中心

資安事件單
通報時間及知悉時間

臺灣學術網路
電腦危機處理中心
TACERT

Tel: 07-5250211
VoIP代表號：98400000
service@cert.tanet.edu.tw
804高雄市鼓山區蓮海路70號

cert.tanet.edu.tw
TACERT

事件單處理流程

事件發生 → **通報處理** → **事件審核** → **事件結案**

事件發生
- 產生通知：
  -新進告知通報通知
  (簡訊+MAIL)

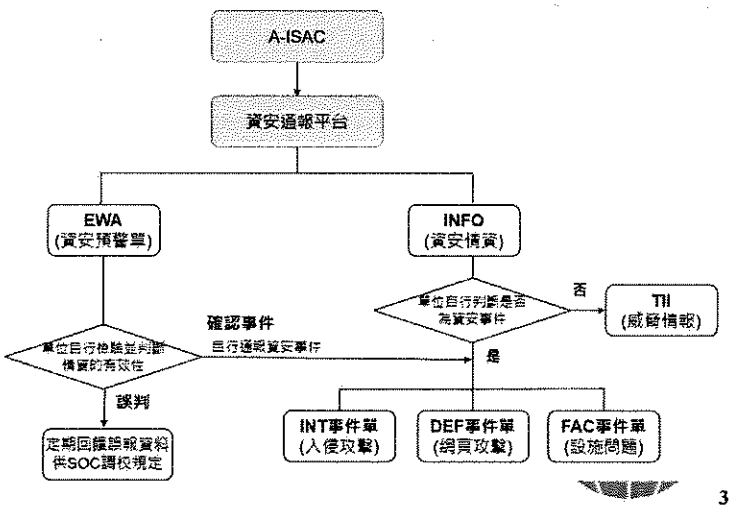
通報處理
- 處理時效：
  -通報**1小時**
  -應變**36/72小時**
- 產生通知：
  -通報應變相關通知
  -待審核通知
  (MAIL)

事件審核
- 審核時效：
  於通報完成後**2/8小時**內
- 產生通知：
  -審核相關通知
  (MAIL)

事件結案
- TACERT覆核完畢後事件結案進入歷史工單
- 產生通知：
  -結案通知
  (MAIL)

資安通報平台威脅情報說明

- 當收到資安情資後，經適當且有效的系統調查後，並未發現有直接或間接證據可證明系統遭受到資安事件之威脅即可選擇TII(威脅情報，Threat Intelligence Information)
- 建議您在進行系統調查時進行下列步驟：
  ① 檢查系統或網路相關 LOG 資訊，查看是否有異常之處
  ② 利用如 TCPVIEW 工具軟體或 netstat 指令來查看系統
  ③ 是否有開啟可疑之服務或是否有可疑之來源連線
  ④ 查看防火牆之連線記錄，確認是否有可疑之連線
  ⑤ 如果有設置入侵偵測軟體（IDS），進行查看是否有惡意的連線行為



知悉時間

知悉時間：確認該情資為資安事件之時，而不是收到通知或簡訊的當下。

2. 事件發生時間：	2025-05-30 02:13:58
3. 確認(知悉)為資安事件時間：	2025-05-30 11:11:48

收到簡訊或通報通知當下就是知悉時間嗎？
不一定！收到通知 ≠ 立即確認為事件

若在下班時間收到簡訊，是不是要立刻回報？
可於上班時間登入平台確認後再定義知悉時間

建議：
事件通報處理需確認有明確事件事實，並與單位資訊資產相關，且確認對CIA造成影響，再將「確認完成」的時間作為知悉時間。

資通安全事件判別舉例

事件主旨	[HITCON ZeroDay] 資安通報-]疑似存在反射型跨站腳本攻擊（Reflected Cross-Site Scripting）漏洞
事件描述	[HITCON ZeroDay漏洞編號:]，TACERT 接獲 HITCON ZeroDay 團隊通知，發現責單位[ ]網頁程式疑似存在反射型跨站腳本攻擊 (Reflected Cross-Site Scripting)漏洞，攻擊者可能經由該漏洞竊取使用者身份，或進行掛碼、轉址等攻擊行為，煩請協助處理，並於漏洞處理完畢後回覆至資安通報應變小組信箱 (service@cert.tanet.edu.tw)，以利進行事件複檢及狀態更新，問題網址： https://

收到情資後，至資安通報平台
「事件附檔下載」查看事件漏洞詳情

確認漏洞確實存在
(若無造成損害可填寫為TII)

漏洞描述:
該網站未對使用者輸入的 srch_title 參數進行適當的過濾與編碼處理，導致惡意腳本可被注入至網頁中。攻擊者可藉由特製連結，誘發瀏覽器執行 JavaScript 代碼，例如：onmouseover=prompt(1)，當使用者將滑鼠移至特定元素時，即會跳出提示視窗。此類行為可被進一步利用進行 Cookie 竊取、釣魚攻擊等安全風險。

修補建議

對所有輸入參數進行嚴格的輸入驗證與轉義處理。

輸出至 HTML 屬性前應使用適當的編碼方式（如 HTML attribute encoding）。

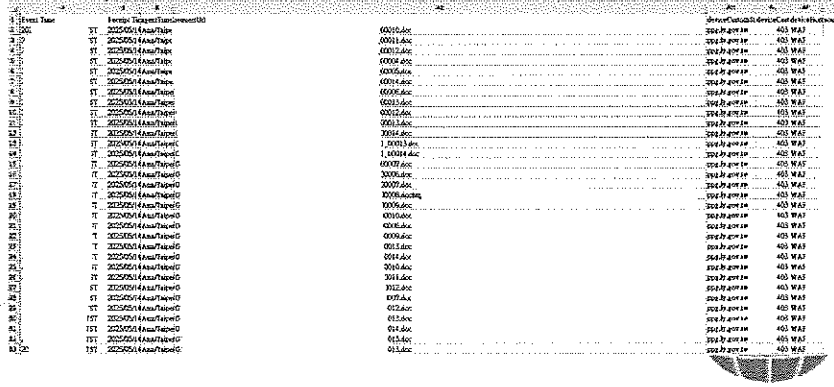
可考慮使用 CSP（Content Security Policy）等方式減少 XSS 攻擊面。

資通安全事件判別舉例

事件主旨	教育部資安通告-]內部主機進行URL操控或注入攻擊(NASOC-Rule WEB Abnormal URL Structure With Injection Pattern)
事件描述	北區ASOC經由外部單位通報，於 檢測到IP 的可疑 Web 請求，針對 " " 進行 URL 操控或注入攻擊，意圖存取未授權資源。
手法研判	
處理建議	1.查詢當時相關 LOG 是否有以上情形 2.使用防毒軟體掃描 3.確認使用者的行為 4.確保作業系統與應用程式為最新的版本

收到情資後，至資安通報平台
「事件附檔下載」查看事件相關LOG

確認描述狀況相符即為資安事件



臨時動議

有關曝露在外網之IoT物聯網設備清單，轉交區縣市網路中心協助後續追蹤與支援一事，提請討論。

目的

- 鑒於學術網路IP數量眾多，在IoT設備普及的環境下，設備發生遭入侵、控制，甚至是資料外洩的風險極高。

IOT情資類型	數量
網路印表機使用預設密碼	497
使用中國品牌的IOT設備	60
IOT設備存在漏洞	34
小計	591

統計區間:114/1/1-114/6/30

IoT設備安全管理建議：

- 設備清查
- 修補更新
- 設備管理: 將設備放置於內部網路(虛擬IP)
- 設備管制: 需外部網路存取，設定ACL管制連線IP。
- 帳密控管: 修改預設帳密、關閉匿名登入服務。

流程

1) ASOC團隊每月偵蒐高曝險IOT設備並將結果依據各區網管轄範圍進行分類。

2) ASOC團為將IOT曝險清單寄給各區網。

3) 區網通知該IOT設備所屬連線單位移除或降低該設備曝險狀況。

4) 區網追蹤IOT曝險清單處理狀況。

5) 該IOT設備完成曝險狀況改善後即可結案。

區網中心協處項目

(1)轉發IOT曝險清單至相關連線單位

(2)協助連線單位降低IOT設備曝險狀況

■信件內容包含：詳細IP清單、以及建議處理措施。

■IOT曝險清單類型：(1)網路攝影機(2)網路印表機(3)IP分享器

(3)區縣市網收到所轄單位處理方式及支援需求等，回覆給SOC團隊處理情形。

技術參考文件:
臺灣學術網路危機處理中心團隊(TACERT)製 IOT設備資安防護指南
https://portal.cert.tanet.edu.tw/docs/pdf/20221104041140407198627396083 09.pdf
技術支援:臺灣學術網路危機處理中心團隊07-5250211