檔　　號:
保存年限:

屏東縣政府 函

地址：900219屏東縣屏東市自由路527號
聯絡人：洪鈺雯
聯絡電話：08-7364830
電子信箱：yvonnehung@gm.ptc.edu.tw

受文者：屏東縣滿州鄉永港國民小學

發文日期：中華民國114年5月28日
發文字號：屏府教發字第1140128768號
速別：普通件
密等及解密條件或保密期限：
附件：如說明二（376530000A114012876801-1.pdf、376530000A114012876801-2.pdf、376530000A114012876801-3.pdf、376530000A114012876801-4.pdf）

主旨：有關本縣國中小學校內部發生資安及網路異常事件，本縣教育網路中心建置相關處理指引，請查照。

說明：

一、考量本縣國中小學校得初步自行排除校內資安及網路異常事件，本縣教育網路中心建置相關處理指引，學校得依據各指引做初步檢視，若事件仍無法排除，再聯繫教網中心做進一步處理。

二、檢附「屏東縣立國中小校園發生資安事件處理指引」、「屏東縣立國中小全校網路異常簡易處理程序指引」、「屏東縣立國中小學校載具無線網路連線異常排查指引」、「屏東縣立國中小部分資訊設備網路異常簡易處理程序指引」。

正本：各高國中、本縣各國小(不含崇華)、屏東縣內埔鄉榮華國民小學
副本：本府教育處教學發展科 電子公文交換章 2025/05/28 15:51:04

屏東縣立國中小校園發生資安事件處理指引

114.5.8

學校設備資安事件：

步驟1：收到簡訊及信箱通知學校發生資安事件，網管人員前往教育機構資安通報平台(https://info.cert.tanet.edu.tw/prog/index.php)確認資安事件單，並填寫通報應變內容。

步驟2：從資安事件單所提供的資訊，確認受害設備 IP。

步驟3：透過學校防火牆尋找受害設備 IP 位於學校哪個區域的設備。參閱附錄一說明(備註：如不熟悉防火牆操作，請致電屏東縣教育網路中心 08-7364563)

步驟4：尋找到受害設備，請立即切斷設備網路能力。

步驟5：將受害設備進行掃毒、系統還原，如前者無效，請重新安裝作業系統。(不熟悉作業系統安裝，可尋求學校電腦維護廠商)

學校網頁資安事件：

聯絡窗口電話：屏東縣教育網路中心(林先生) 08-7369482

學校網頁內容遭入侵竄改，請立即連繫 NSS WEB 校園網站維護廠商(恆煦資訊)
聯繫電話：03-3579080 分機 220
LINE 線上客服 ID：@263ohszc

附錄一

資安通報事件查詢說明

一、下載資安紀錄

資安事件-查詢

步驟1
- 收到資安事件通知郵件
- 請登入**資安通報平台**

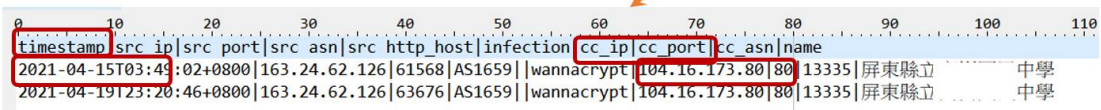
教育機構資安通報平台

事件類型:入侵事件警訊

事件單編號:AISAC-191707

原發布編號	TWCERTCC-INT-202104-0337	原發布時間	2021-04-22 09:30:24
事件類型	殭屍電腦(Bot)	原發現時間	2021-04-15 03:49:02
事件主旨	屏東縣立 [redacted] 設備IP：「163.24.62.126」等，疑遭植入Bot程式成為殭屍網路成員		
事件描述	TWCERT/CC於近日經ShadowServer系統獲得資訊，發現 貴單位資訊設備IP:[163.24.62.126]在 2021-04-15T03:49:02+0800 (UTC+0)期間，疑遭植入Bot程式成為殭屍網路成員。為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		
手法研判	疑遭植入Bot程式成為殭屍網路成員		
建議措施	1. 檢查防火牆紀錄，查看系統是否曾與C2 Server或Port進行異常連線。若發現異常連線，建議移除產生異常連線之程式；若暫時未發現異常行為，建議持續觀察一個星期左右。 2. 請將系統更新至最新版本，若僅移除惡意程式而不修補，再次受相同或類似攻擊的機率極高。 3. 請依貴單位系統入侵回復方式對上述主機進行檢查及處理。		
參考資料	如附件		
此事件需要進行通報，請 貴單位資安聯絡人登入 資安通報應變平台 進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

步驟2
- 於資安通報平台左列點選**事件附檔下載**
- 選擇欲查詢的事件，並點選**Log附檔下載**
- 開啟下載地附檔
- 附檔中提供了**時間 / 攻擊的目標位址 / 攻擊目標連接埠**等資訊



二、使用智慧網管平台 Ncloud 查詢

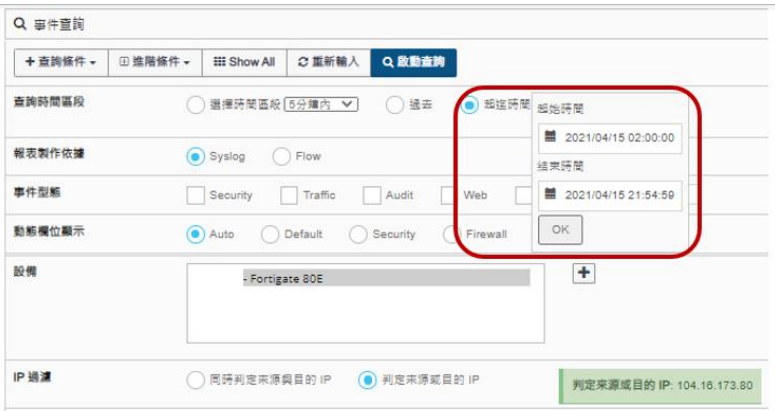
- 資安事件附件提供了**發生時間 / 被攻擊或目的IP**與**埠號**等**資料**

步驟1
- 到事件 / 事件查詢
- 在右邊視窗的查詢條件下拉呼叫**設備**與**IP過濾**

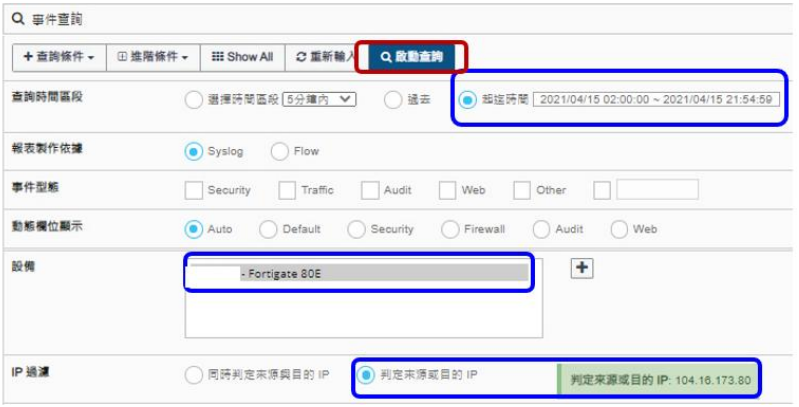
步驟2
- 點選**設備**方框空白處
- 在選取設備對話視窗中務必選擇**學校 Fortigate 80E**
- 點選**確定**按鈕離開對話視窗

步驟3
- 點選**IP過濾**的**判斷來源或目的IP**
- 點選**IP**方框空白處
- 在IP網段過濾條件對話視窗中於**單一IP或網段**輸入要查找的IP(輸入附件**被攻擊的目標位址**)
- 點選**+**按鈕，確認查找IP被輸入
- 點選**確定**按鈕離開對話視窗

步驟4
- 點選查詢時間區段的**起迄時間**，輸入欲**查詢的時間區段(建議時間起迄比事件時間往前後至少1小時)**



步驟5
- 依據聯防紀錄的資訊，將相關查詢條件設定好後(條件有時間區段 / 設備 / IP過濾)，點選**啟動查詢**按鈕



步驟6

- 依據資安事件的附件資訊，將相關查詢條件設定好後，點選**啟動查詢**按鈕
- 查訊的紀錄，可詳看**來源IP**欄位，找出異常的來源IP，並做合適的處理 (查詢的資料有眾多欄位，可左右拖曳查找有用的欄位資訊，例如來源MAC / 來源主機名稱 / 來源IP所屬交換器介面)

屏東縣立國中小全校網路異常簡易處理程序指引

114.5.8

- 使用桌上型電腦檢查電腦是否有取得 IP【附件一】→**有取得 IP**→是否可以連結學校防火牆【附件二】→可以，通知學校租用的電信業者查修學校對外線路狀態(中華電信或凱擘電信)。

- 使用桌上型電腦檢查電腦是否有取得 IP→**沒有取得 IP**→查看學校網路平面圖→依據學校平面圖，判斷該台桌上型電腦可能連結的邊際交換器所在位置→到邊際交換器位置檢查邊際交換器狀態(觀察設備燈號)【附件三】→到骨幹交換器所在位置檢查骨幹交換器狀態(觀察設備燈號)【附件三】→到防火牆所在位置檢查防火牆狀態(觀察設備燈號)【附件四】→網路仍異常，聯繫教網中心協助。

  ※邊際交換器、骨幹交換器與防火牆若燈號不正常，請現場拔插設備電源後，觀察設備狀是否恢復正常。

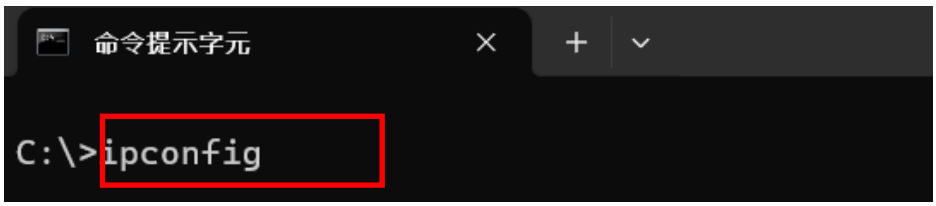
上述程序判斷與檢查且處理後，學校網路仍異常，聯繫教育網路中心協助。

聯絡窗口電話：屏東縣教育網路中心(林先生) 08-7364563

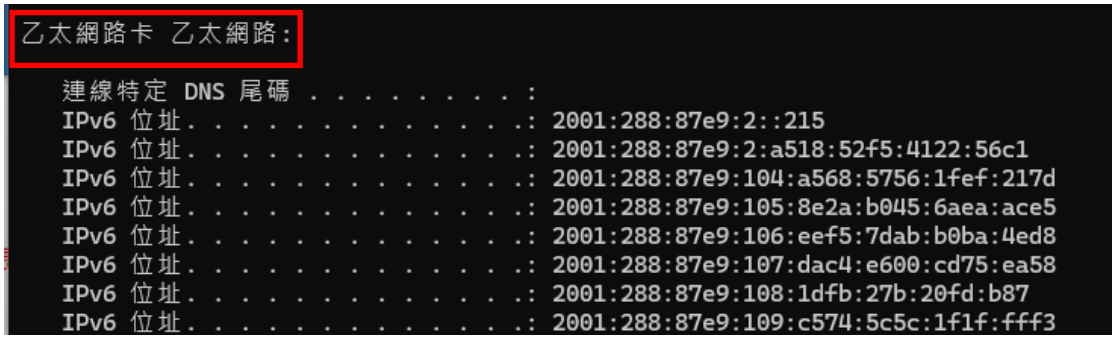
【附件一】：查看電腦 IP 說明

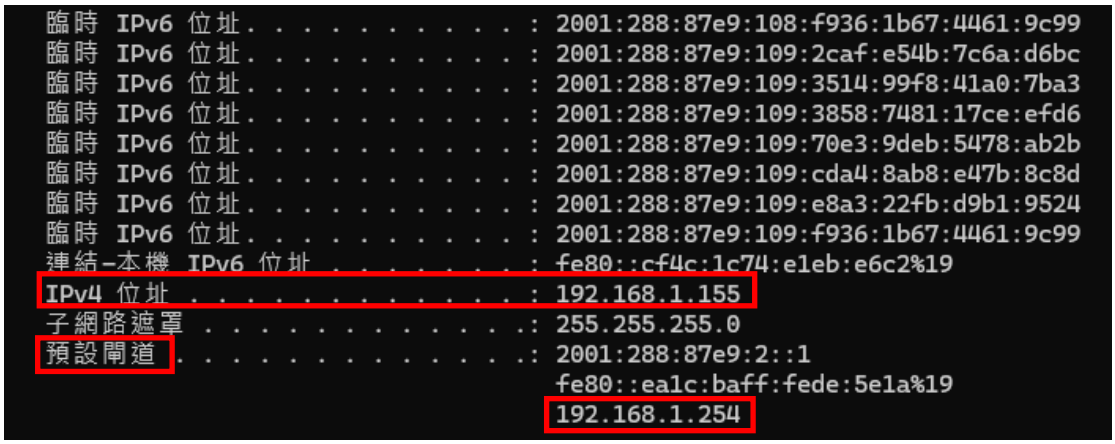
1、電腦作業系統左下方搜尋輸入 cmd 後，按 enter 鍵開啟命令提示字元視窗。

2、在命令提示字元視窗內輸入 ipconfig 後，按 enter 鍵，查看電腦是否有取得 IP 資訊。



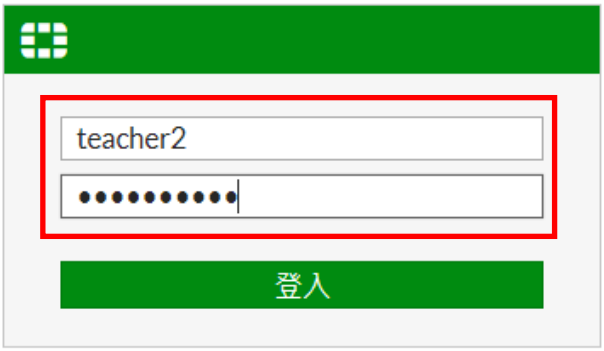
視窗向上拖曳，查看乙太網路卡 乙太網路資訊，IPv4 的 IP、預設閘道等資料。學校內部應取得的 IP 為 192.168.xxx.xxx。





【附件二】如何連結防火牆說明

1、電腦開啟瀏覽器，在網址列輸入 https://*該電腦設定或自動取得的預設閘道IP*，例如 https://192.168.1.254，預設閘道 IP 查詢方式請參閱「查看電腦 IP 說明」，輸入學校管理者帳密，若正常登入可初步判斷防火牆設備屬於正常。



【附件三】邊際交換器/骨幹交換器設備簡易檢查說明

1、檢查設備左方位置的 4 顆燈號，至少 PWR(電源)與 SYS(設備系統)是否亮綠燈，若非綠燈，可將設備電源拔插，觀察設備重啟燈號狀況。

【附件四】防火牆設備簡易檢查說明

1、檢查設備左方位置的 2 顆燈號，POWER(電源)與 STATUS(設備系統狀態)是否亮綠燈，若非綠燈，可將設備電源拔插，觀察設備重啟燈號狀況。

2、檢查 WAN1、WAN2 與 Port 1 是否有綠燈，若無亮燈，檢查連接在防火牆上述 Port 是否有網路線連接。

屏東縣立國中小學校載具無線網路連線異常排查指引

114.5.8

- 載具是否有看到班級訊號 SSID→**有**→檢查載具欲連接的 SSID，WiFi 專用位址功能是否有關閉【附件一】→有，但仍無法連上，查詢該載具 WiFi MAC 資料【附件二】，聯繫教育網路中心協助。

- 載具是否有看到班級訊號 SSID→**無**→檢查班級 AP 狀態是否正常【附件三】→將 AP 電源重啟，若仍無法看到班級訊號 SSID→檢視 AP 與交換器連結檢查【附件四】，請聯繫教育網路中心協助。

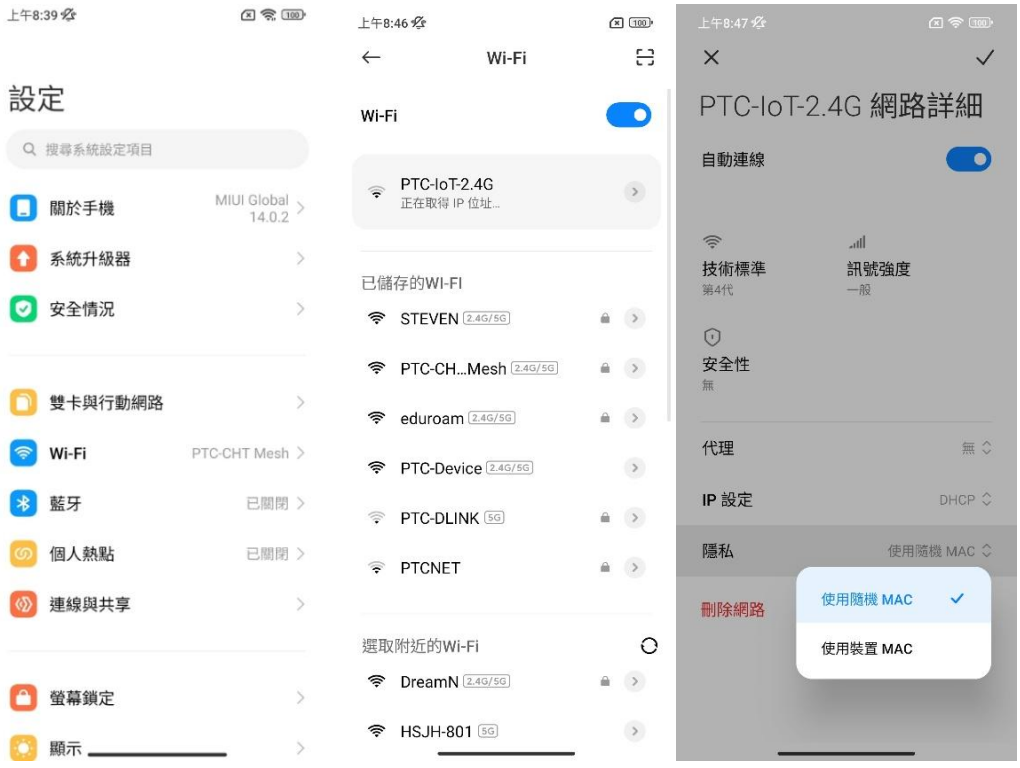
上述程序判斷與檢查且處理後，學校網路仍異常，聯繫教育網路中心協助。

聯絡窗口電話：屏東縣教育網路中心(林先生) 08-7364563

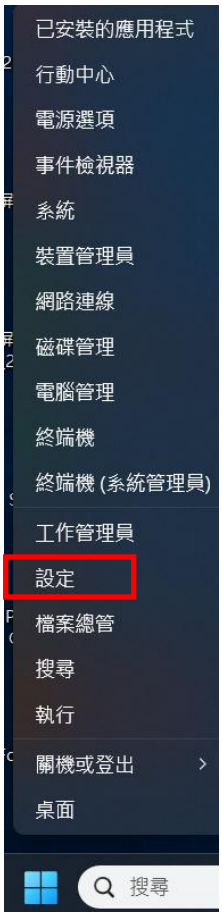
【附件一】查看載具是否有關閉 WiFi 專用位址說明

1、iOS 系統→設定→WiFi→班級 SSID→專用 WiFi 位址，選擇關閉。

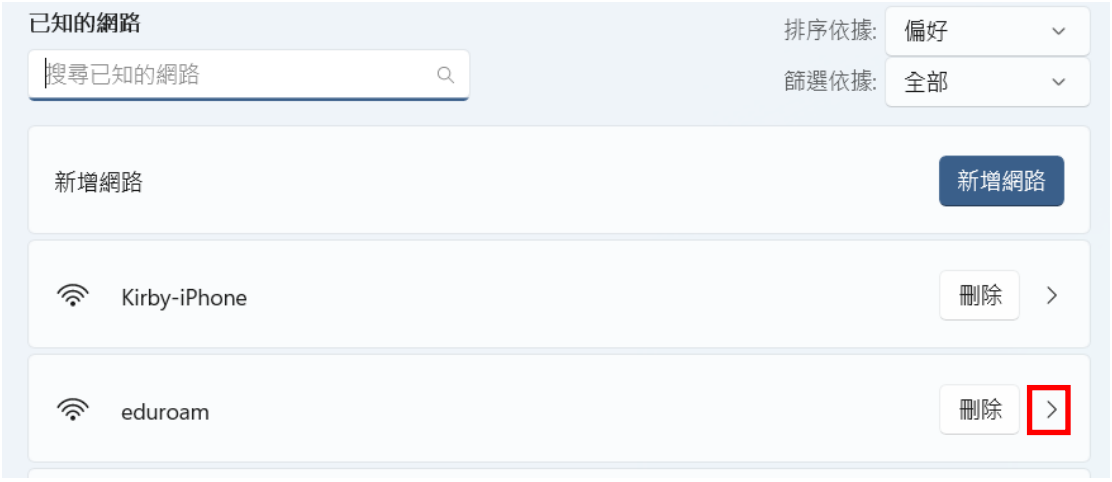
2、Andriod 系統→設定→ WiFi →選擇班級 SSID→隱私，選擇使用裝置 MAC。
(路徑與設定用語僅供參考，不同廠牌載具 Andriod 會有差異)。



3、Windows 系統→滑鼠游標移至視窗左下角「開始」，按滑鼠右鍵，選取「設定」→點選「網路和網際網路」→點選「WiFi」→這邊可看到隨機硬體位址，設定關閉後，繼續點選「管理已知的網路」→選擇要調整的 SSID→將隨機硬體位址設定關閉。



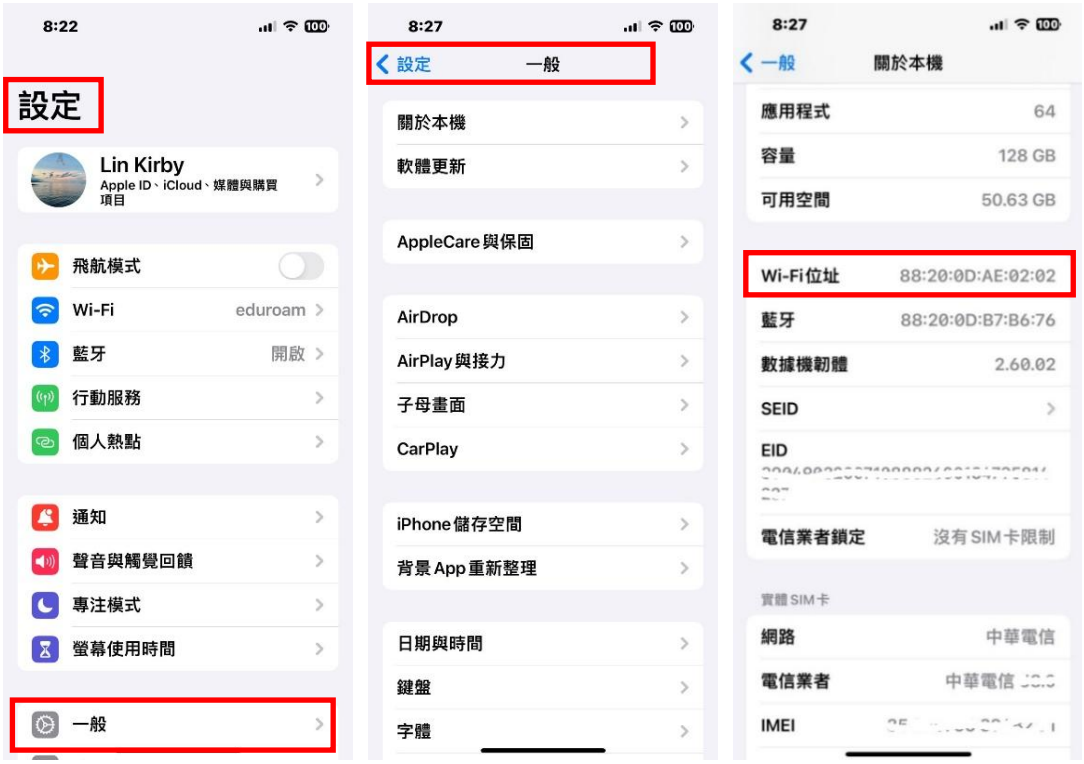

尋找設定
首頁
系統
藍牙與裝置
網路和網際網路
個人化
應用程式
帳戶
時間與語言
遊戲
Wi-Fi
開啟
Kirby-iPhone 屬性
已連線，安全
顯示可用網路
管理已知的網路
新增、移除和編輯網路
硬體內容
檢視及管理 Wi-Fi 介面卡內容
隨機硬體位址
讓其他人更難追蹤您的裝置位置，以協助保護您的隱私權。
關閉


已知的網路
搜尋已知的網路
排序依據:
偏好
篩選依據:
全部
新增網路
新增網路
Kirby-iPhone
刪除
eduroam
刪除


eduroam 內容
於範圍內自動連線
計量付費連線
當您與這個網路連線時，有些應用程式可能會有不同的運作以減少數據使用量。
關閉
設定資料限制以協助控制此網路上的數據使用量
隨機硬體位址
在您連線到此網路時，讓其他人更難追蹤您的裝置位置，以協助保護您的隱私權。設定在您下次連線至此網路時才會生效。
關閉
IP 指派:
自動 (DHCP)
編輯
DNS 伺服器指派:
自動 (DHCP)
編輯
進階 Wi-Fi 網路內容
編輯

【附件二】載具 WiFi MAC 查詢說明

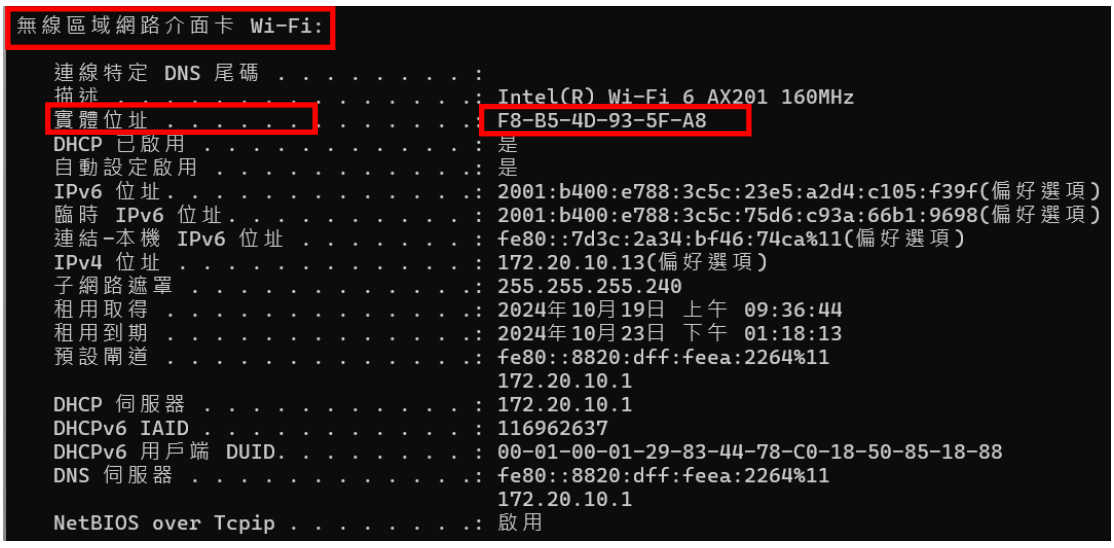
1、iOS 系統→設定→一般→關於本機→WiFi 位址所顯示的區域資料



2、Andriod 系統→設定→關於手機→全部參數與資訊→狀態→裝置的 WiFi MAC 位址(路徑與設定用語僅供參考，不同廠牌載具 Andriod 會有差異)。

3、Windows 系統→在命令提示字元視窗內輸入 ipconfig /all，按 enter 鍵，查看電腦是否有取得 IP 資訊。

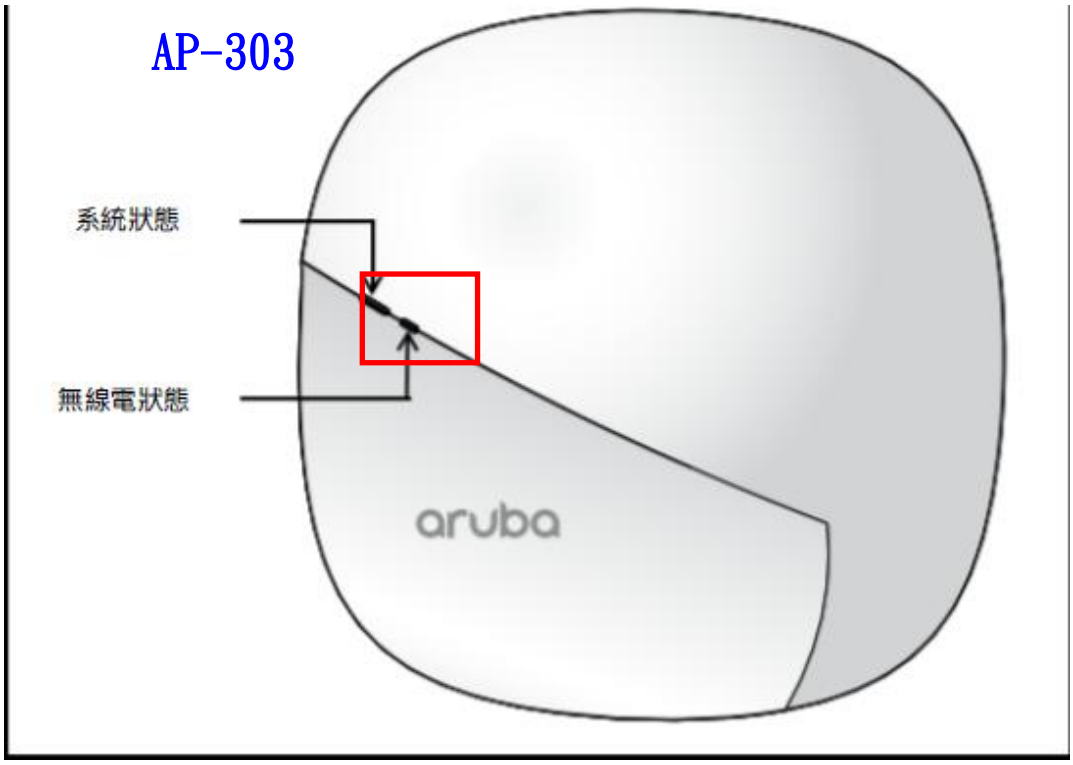
視窗向上拖曳，查看無線區域網路介面卡 Wi-Fi 資訊，實體位址對應的資料及 WiFi 網卡的 MAC



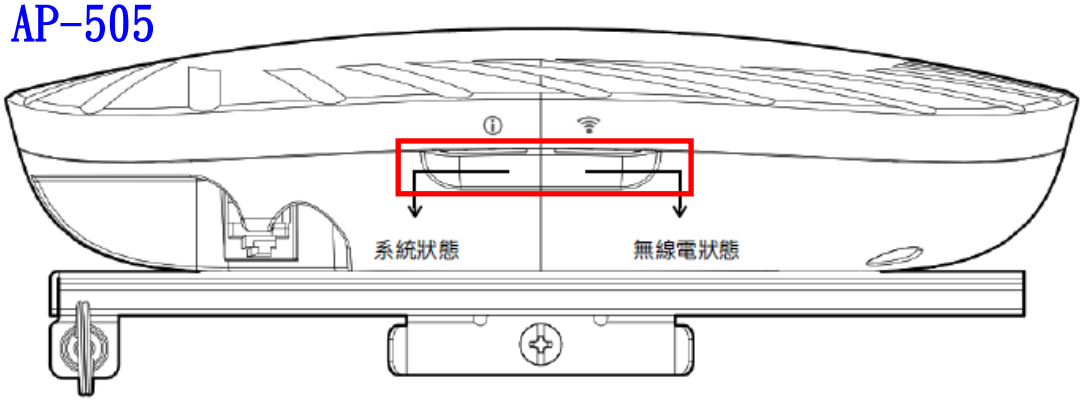
【附件三】AP 是否正常運作檢查

目視檢查 AP 的燈號狀態→系統狀態燈號是否亮燈，燈號應為綠燈恆亮→無線電狀態燈號是否亮燈，燈號應為綠燈恆亮→若上述燈號有異常，重啟 AP 電源後觀察燈號狀態，若仍異常，聯繫教育網路中心協助。

AP-303

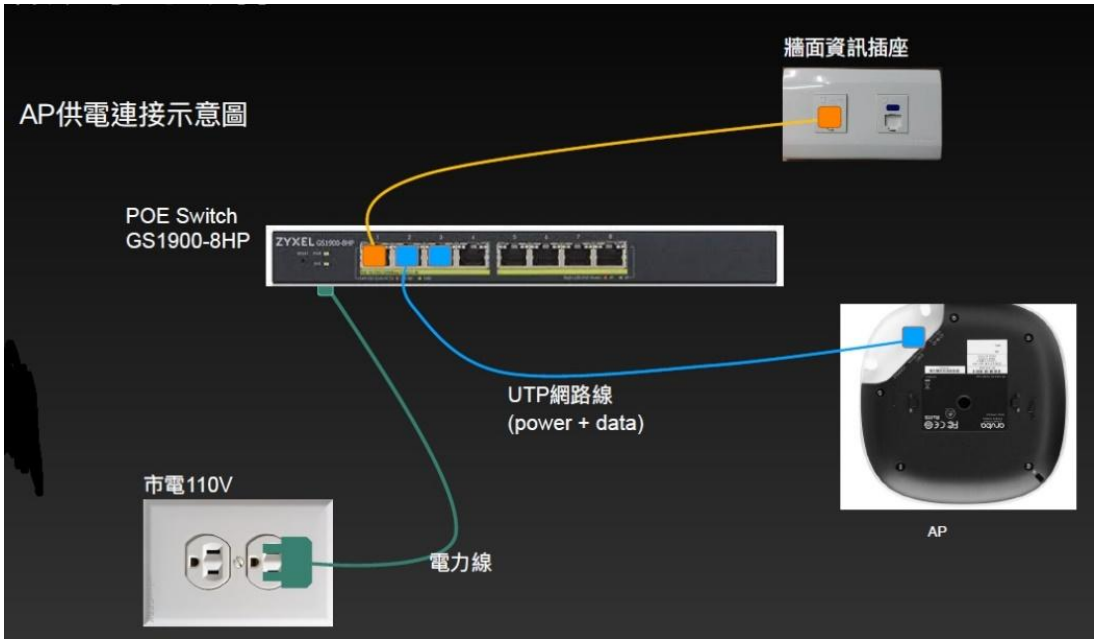


AP-505



【附件四】檢視 AP 與交換器連結檢查

固定在學校班級教室 AP、PoE 交換器與教室網點連接方式必須如下圖，若確認無異常，無線網路仍有問題，請聯繫教網中心。



屏東縣立國中小部分資訊設備網路異常簡易處理程序指引

114.5.8

- 資訊設備檢查是否有取得 IP【附件一】→**有取得 IP**→開啟瀏覽器，網址列輸入上述查看的預設閘道 IP(路由器)判斷是否為學校防火牆【附件二】→是學校防火牆，但資訊設備仍無法上網，聯繫教網中心協助。

- 資訊設備檢查是否有取得 IP【附件一】→**有取得 IP**→開啟瀏覽器，網址列輸入上述查看的預設閘道 IP(路由器)判斷是否為學校防火牆【附件二】→否，為其他資訊設備，聯繫學校網管找出該設備，並將該設備網路線拔除→資訊設備重新啟動後，檢查是否可以上網，若上網仍有問題，聯繫教網中心協助。

- 資訊設備檢查是否有取得 IP【附件一】→**無法取得 IP**→若資訊設備使用有線網路：
  - 檢查網路線是否正確連接在設備網卡
  - 檢查網路線另一端連接在交換器上孔位的燈號是否正常【附件三】
    →若資訊設備使用無線網路：
  - 檢查是否連接上正確的無線網路訊號
  - 無線網路帳號密碼輸入是否正確
  - 資訊設備的 WiFi 專用位址是否有關閉【參閱 2.學校載具無線網路連線異常排查指引】
  - 資訊設備的 WiFi MAC 是否提供給教網中心【參閱 2.學校載具無線網路連線異常排查指引】
    →上述狀況都確認無誤，若上網仍有問題，聯繫教網中心協助。

上述程序判斷與檢查且處理後，資訊設備網路仍異常，聯繫教育網路中心協助。

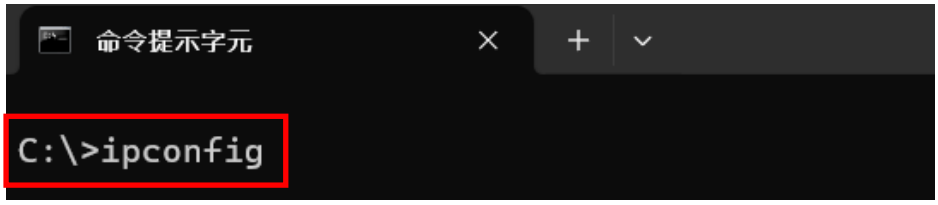
聯絡窗口電話：屏東縣教育網路中心(林先生) 08-7364563

【附件一】：查看資訊設備 IP 說明

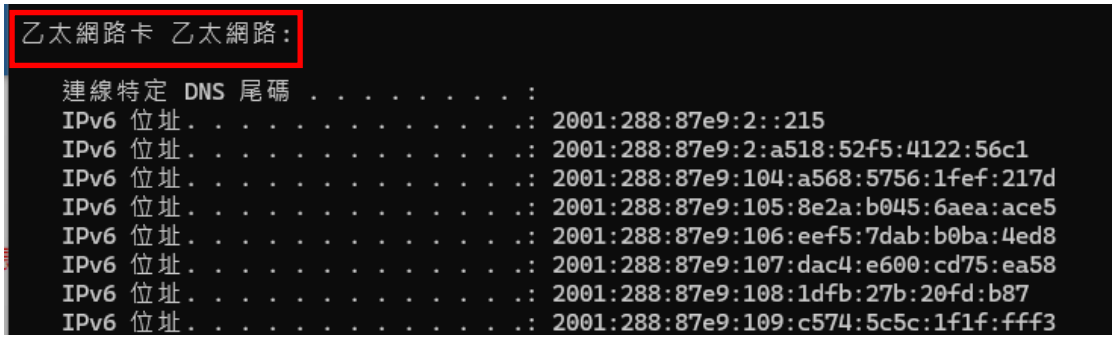
1、Windows 系統

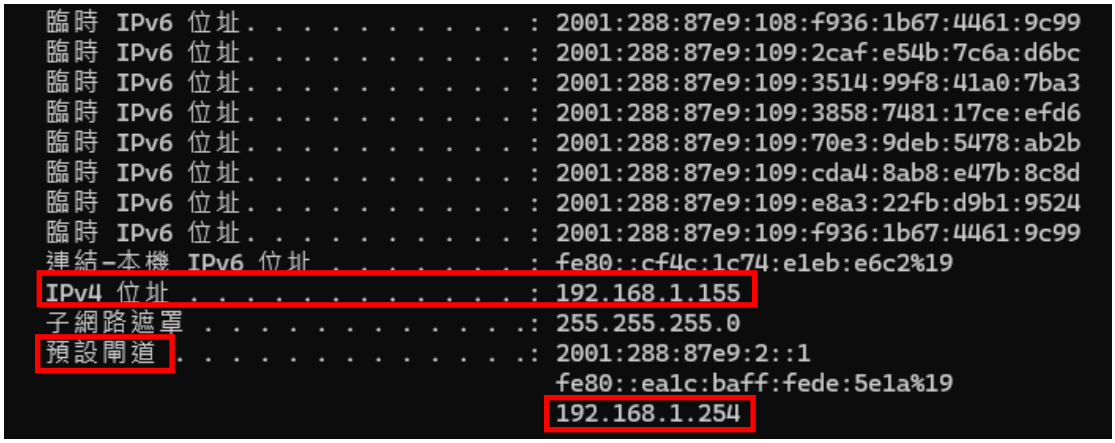
電腦作業系統左下方搜尋輸入 cmd 後，按 enter 鍵開啟命令提示字元視窗。

在命令提示字元視窗內輸入 ipconfig 後，按 enter 鍵，查看電腦是否有取得 IP 資訊。



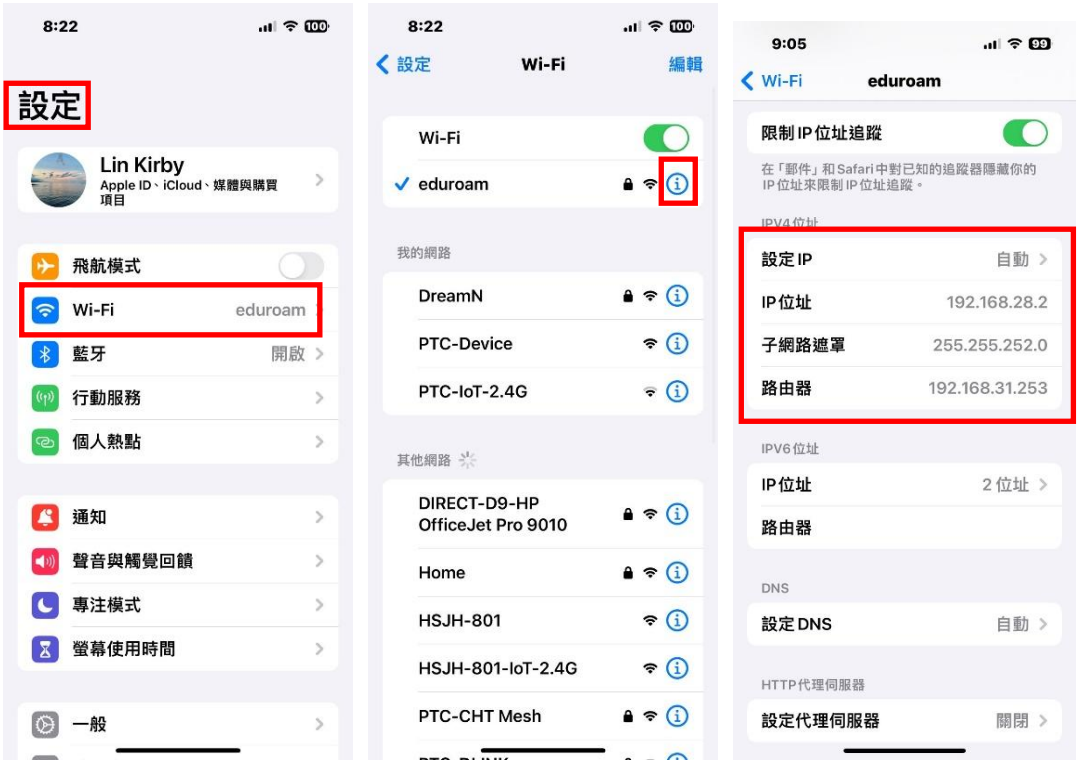
視窗向上拖曳，查看乙太網路卡 乙太網路資訊，IPv4 的 IP、預設閘道等資料。學校內部應取得的 IP 為 192.168.xxx.xxx。





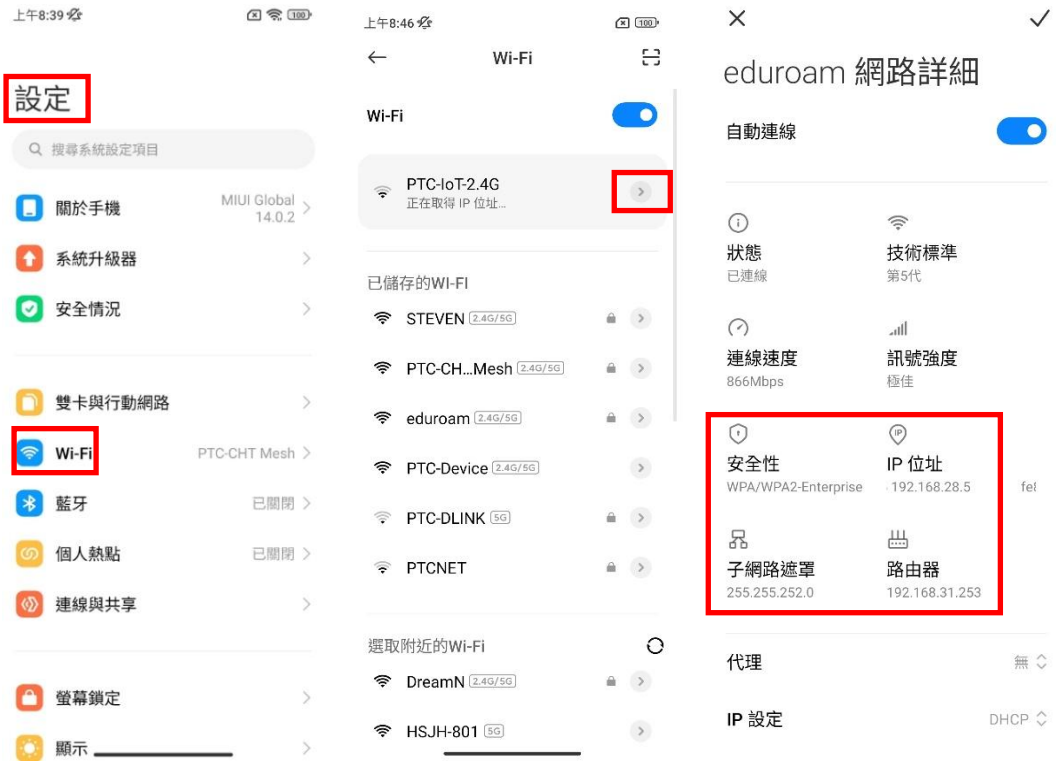
2、iOS 系統

設定→WiFi→班級 SSID→專用 WiFi 位址，選擇關閉。



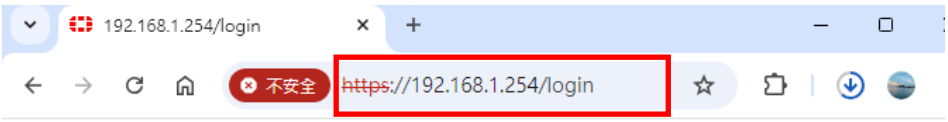
3、Andriod 系統

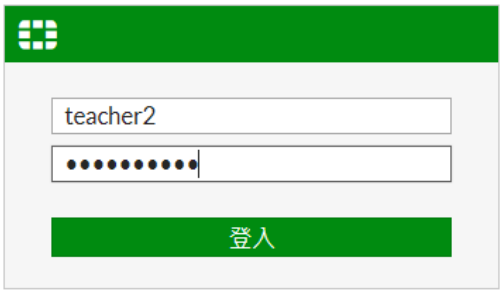
設定→ WiFi →選擇連線的 SSID→點選 > 圖示，查看 IP 資訊。(路徑與設定用語僅供參考，不同廠牌載具 Andriod 會有差異)。



【附件二】如何連結防火牆說明

1、電腦開啟瀏覽器，在網址列輸入 https://*該電腦設定或自動取得的預設閘道 IP*，例如 https://192.168.1.254，預設閘道 IP 查詢方式請參閱「查看電腦 IP 說明」，輸入學校管理者帳密，若正常登入可初步判斷防火牆設備屬於正常。





【附件三】如何查看交換器網路線接孔燈號說明

1、依據網路線路編號，到交換器找出相同線編以及網路孔位，查看孔位燈號是否有亮且閃爍（沒亮：異常；綠燈：1G 速率；紅燈：100M 速率）