

無線網路設置管理說明

簡報單位：資訊處

大綱

一、無線網路管理

二、各單位無線網路類型

(一)使用資訊處建置校園無線網路

(二)單位自建無線網路

(三)單位建置無線網路設備配合校園無線網路管理

三、自建無線網路應注意事項

四、無線基地台基本設定

五、學院無線網路介接管理

(一)學院無線網路

(二)學院無線網路管理機制



一、無線網路管理

諮詢窗口：黃先生 分機14101

電子信箱：jason@ccu.edu.tw

一、無線網路管理

1. 請勿使用預設密碼。
2. 基於資安考量，請勿使用危害國家資通安全或大陸廠牌資通產品(例如:TP-LINK、大疆無人機等，建議透過財產管理系統清查)。
3. 資料傳輸宜使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。
4. 無線網路設備應弱點掃描，無中度風險以上。
5. 應有適當管理機制，連線使用應取得授權並留存連線記錄。
6. 使用 D-Link、EDIMAX 及 ZyXel 廠牌設備者，應部署無線網路政府組態基準(GCB)。



二、各單位無線網路類型

二、各單位無線網路類型

- (一)使用資訊處建置校園無線網路
- (二)單位自建無線網路
- (三)單位建置無線網路設備配合校園無線網路管理

(一)使用資訊處建置校園無線網路

SSID：

- CCU：校內學生與教職員使用
- TANetRoaming：其他學校教職員生使用
- eduroam：國際漫遊認證



(一)使用資訊處建置校園無線網路

➤ 校園無線網路使用之SSID

連線名稱(SSID)	適用範圍	認證方式	使用說明
CCU	校園 公共區域	web-based網頁認證	提供本校教職員生使用，使用方便，安全性較低，不需額外設定。
TANetRoaming	臺灣學術 網路無線 漫遊	web-based網頁認證	透過校際漫遊帳號登入，帳號由各校資訊單位提供，詳見本校無線網路使用說明。
eduroam	eduroam 國際漫遊	802.1X認證 (建議使用)	使用802.1X + PEAP認證方式， 安全性較高 ，但需額外設定。裝置第一次使用須設定，再透過校際漫遊帳號登入，帳號由各校資訊單位提供，詳見本校無線網路使用說明。

(二)單位自建無線網路

1. 單位自行購置無線網路設備
2. 使用單位分配IP
3. 自行管理設備、連線帳號及連線使用紀錄
4. 勿使用校園無線網路SSID：
CCU、iCCU、TANetRoaming、eduroam

*自建無線網路應注意事項後述

(三)單位建置無線網路設備配合校園無線網路管理

1. 單位經費支應
2. 資訊處依年度規劃納入校園無線網路建置
3. 設備財產由單位自行保管
4. 連線控管帳號及使用紀錄納入校園無線網路管理
5. 建置分工如下：

建置單位	資訊處
1. 建置經費(含無線基地台、連接用網路交換器、基地台管理授權費、佈線安裝費用) 2. 決定佈放AP數量、位置 3. 設備財產保管(含AP狀況管理) 4. 保固期滿維護費	1. 提供管理機制 2. 留存連線記錄 3. 認證設備管理



三、自建無線網路應注意事項

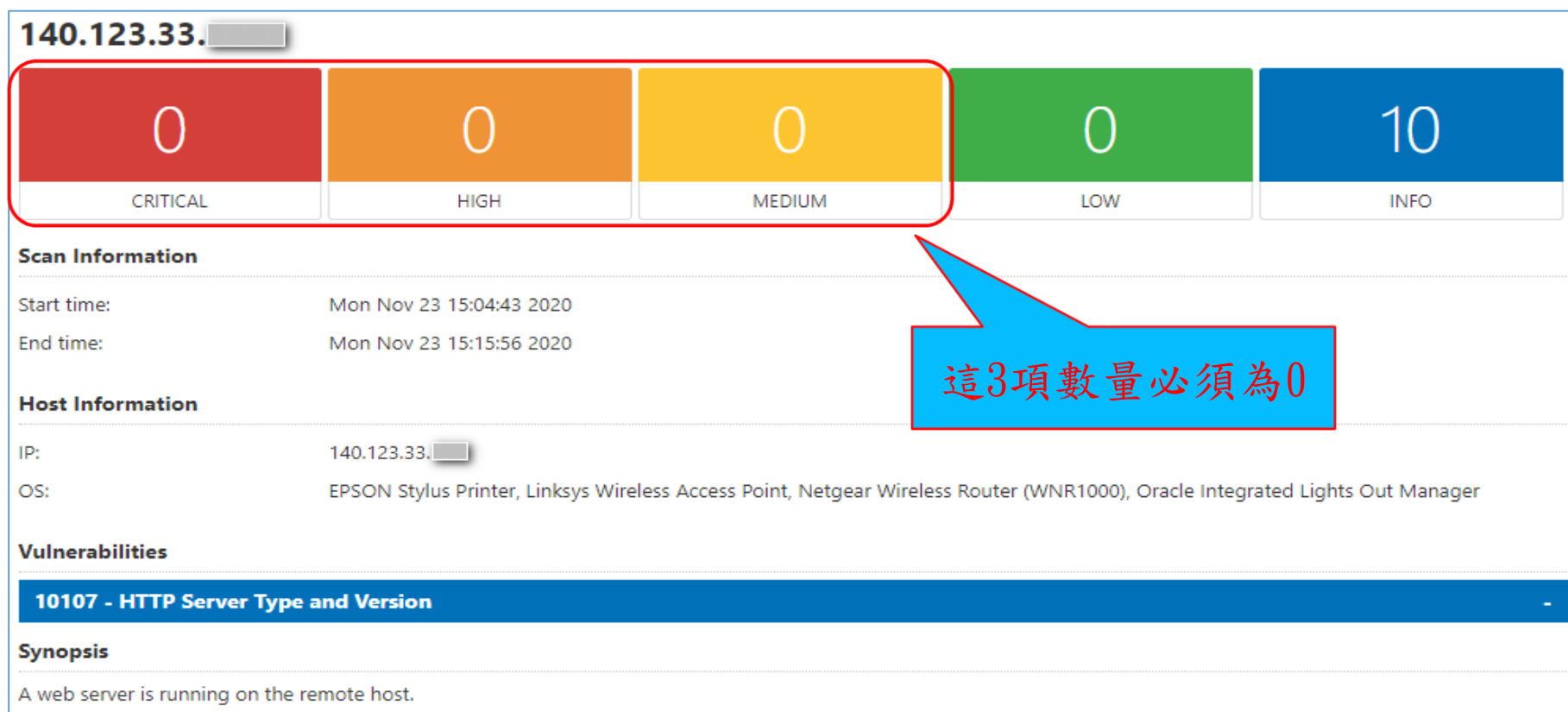
三、自建無線網路應注意事項

➤ 通信與作業管理程序書-無線網路使用之管理

1. 無線網路基地台之使用應經**適當控管**。
2. 無線網路設備之**安裝設定**應經核准。
3. 無線網路設備之使用**應取得授權**，禁止於內部網路私自使用任何無線網路產品。
4. 無線網路設備之使用應有**適當管理機制**，例如：授權使用之IP數量、連接埠、網卡位址（Mac address）過濾等。
5. 無線網路之**資料傳輸**宜使用**加密機制**，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。。

三、自建無線網路應注意事項

- 請勿使用危害國家資通安全或大陸廠牌資通產品
- 設備應弱點掃描無中度風險以上



三、自建無線網路應注意事項

➤ 下列廠牌應部署無線網路政府組態基準(GCB)

D-Link、EDIMAX、ZyXel

➤ 行政院國家資通安全會報技術服務中心

政府組態基準專區網址 <https://www.nccst.nat.gov.tw/GCB>

政府組態基準-無線網路設備([GCB](#))

項次	項 目	項數	合計
1	組態安全	9	19
2	存取控制	5	
3	連線監控	5	

三、自建無線網路應注意事項

➤ 政府組態基準-無線網路設備

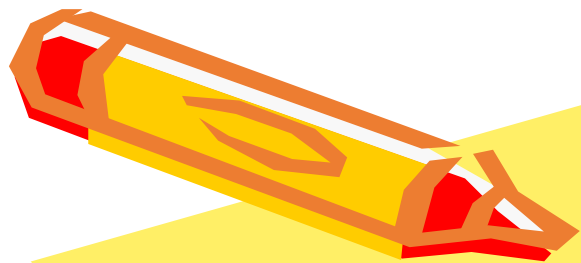
帶*者後面有圖例說明

項次	類別	原則設定名稱
1	組態安全	使用 2 層或 3 層的AES 加密方式 * 關閉未使用的網路設備管理埠 啟用連線逾時功能 變更出廠預設值的密碼內容 * 變更預設SSID * 關閉SSID廣播 * 降低無線網路設備發送訊號功率 * 啟用備份系統組態設定值 * 限制重要功能操作

三、自建無線網路應注意事項

➤ 政府組態基準-無線網路設備

項次	類別	原則設定名稱
2	存取控制	啟用MAC位置過濾 * 關閉DHCP協定 * 啟用允許存取網路時段 * 啟用存取行為管控 啟用黑名單管控
3	連線監控	啟用並設定log 紀錄 * 啟用外部網路異常行為監控 啟用流量偵測功能 啟用流量調節功能 啟用登入錯誤次數限制



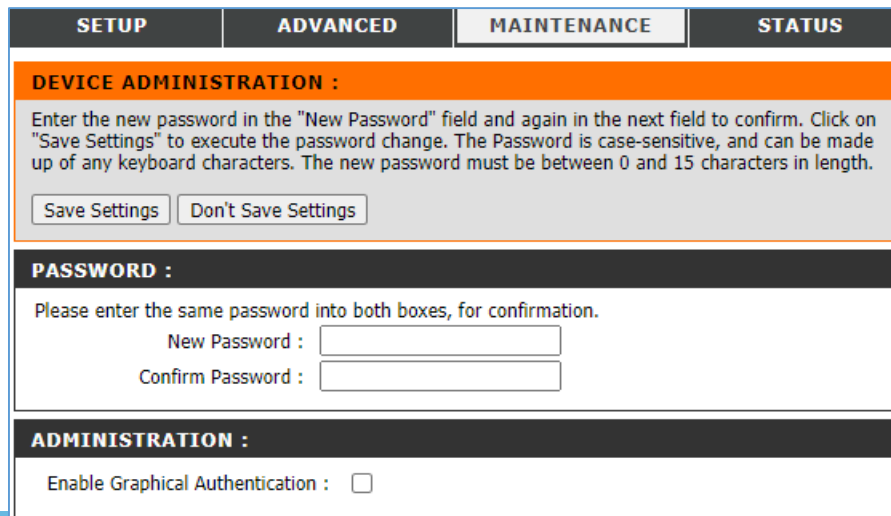
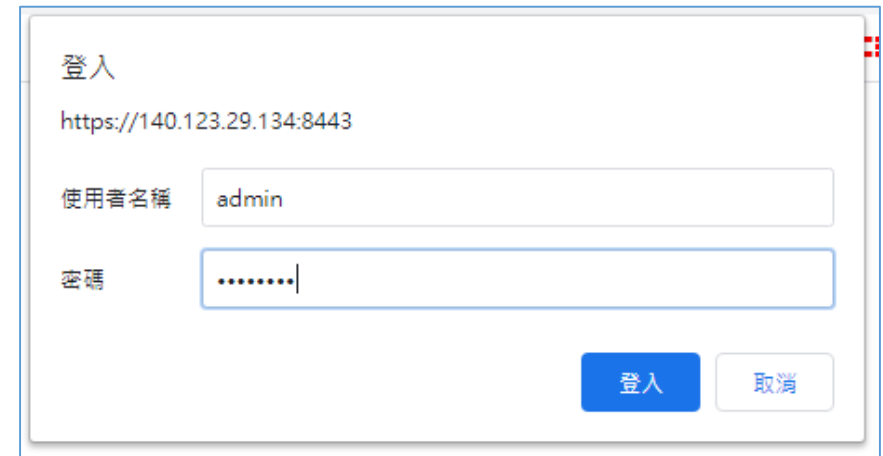
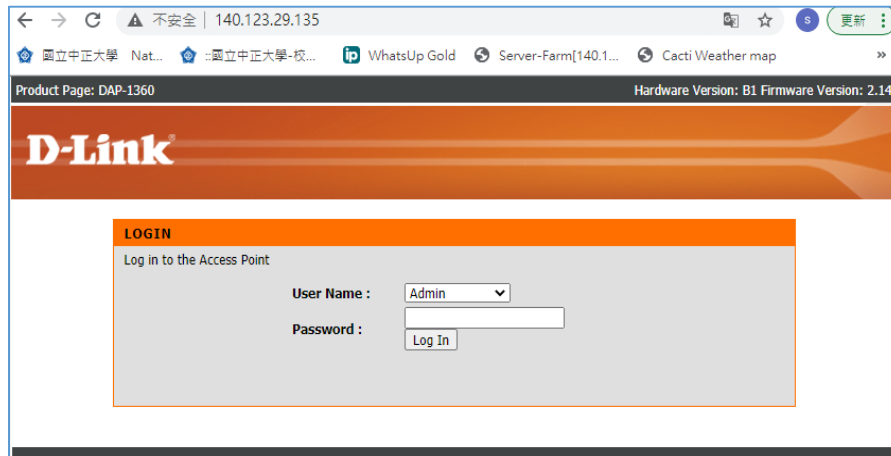
四、無線基地台基本設定

D-Link DAP-1360 VS Netgear R7000



四、無線基地台基本設定

➤ 變更出廠預設值的密碼內容



四、無線基地台基本設定

➤ 使用2層或3層的AES加密方式

WIRELESS SECURITY MODE :

Security Mode :

WPA-Personal

WPA

Use **WPA of WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access some gaming and legacy devices work only in this mode.

To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher)

WPA Mode :

WPA2 only

Cipher Type :

AES

PRE-SHARED KEY

Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

Security Mode : WPA-Personal

- None
- WEP
- WPA-Personal
- WPA-Enterprise

WPA Mode : WPA2 only
Cipher Type : WPA2 only

四、無線基地台基本設定

➤ 變更預設SSID

➤ 關閉SSID廣播

WIRELESS NETWORK SETTINGS :

Enable Wireless : ☒ Always

Wireless Mode : Access Point

Wireless Network Name : dap-1360 (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 6

Enable Auto Channel Scan : ☒

Channel Width : Auto 20/40MHz

Visibility Status : ☒ (Also called Disable SSID Broadcast)

SETTINGS :

Enable Wireless : ☒ Always

Wireless Mode : Access Point

Wireless Network Name : dap-1360 (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 6

Enable Auto Channel Scan : ☒

Channel Width : Auto 20/40MHz

Visibility Status : ☐ (Also called Disable SSID Broadcast)

四、無線基地台基本設定

➤ 降低無線網路設備發送訊號功率

ADVANCED WIRELESS SETTINGS :

Transmit Power :	100% ▼
WMM Enable :	100%
Short GI :	50%
IGMP Snooping :	25%
IGMP Snooping :	12.5%
WLAN Partition :	☐

➤ 啟用備份系統組態設定值

SAVE AND RESTORE :

Save Settings To Local Hard Drive :	Save
Load Settings From Local Hard Drive :	選擇檔案 未選擇任何檔案
	Upload Settings
Restore To Factory Default Settings :	Restore Device
Reboot The Device :	Reboot

四、無線基地台基本設定

- 使用2層或3層的AES加密方式、降低無線網路設備發送訊號功率、變更預設SSID、關閉SSID廣播

無線設定

套用 ▶ ✕ 取消

地區選擇
地區: 臺灣 ▼

☐ 啟用 Smart Connect - 讓路由器自動選擇最適合您 WiFi 連線的 WiFi 頻寬 2.4 GHz 或 5 GHz。Smart Connect 要求 2.4 GHz 和 5 GHz 網路使用相同的 WiFi 網路名稱 (SSID)、安全性選項和密碼。

無線網路 (2.4GHz b/g/n)
☐ 啟用 SSID 廣播
☒ 啟用 20/40 MHz 共存

無線網路名稱 (SSID): NETGEAR82

頻道: 自動 ▼

模式: 最大 600 Mbps ▼

傳輸功率控制: 100% ▼

安全性選項
☐ 無
☐ WPA2-PSK[AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
☒ WPA/WPA2 Enterprise

WPA/WPA2 Enterprise
加密模式: WPA2-PSK[AES] ▼

群組金鑰更新間隔: 3600 秒

RADIUS 伺服器 IP 位址: 0 . 0 . 0 . 0

RADIUS 伺服器連接埠: 1812

RADIUS 伺服器共享密碼:

四、無線基地台基本設定

➤ 啟用允許存取網路時段

ADD SCHEDULE RULE :

Name :

Day(s) : ☐ All Week ☒ Select Day(s)

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

All Day - 24 hrs : ☐

Time format :

Start Time : : AM (hour:minute)

End Time : : AM (hour:minute)

SCHEDULE RULES LIST :

Name	Day(s)	Time Frame		
上班時間	Mon Tue Wed Thu	08:00 AM-06:00 PM		

排程

套用 ▶

✕ 取消

在下列日期進行封鎖 ::

- ☐ 每天
- ☒ 星期天
- ☐ 星期一
- ☐ 星期二
- ☐ 星期三
- ☐ 星期四
- ☐ 星期五
- ☒ 星期六

在下列時間進行封鎖 : (使用 24 小時制)

- ☒ 全天

封鎖開始時間

時 分

封鎖結束時間

時 分

四、無線基地台基本設定

➤ 關閉DHCP協定

DHCP SERVER SETTINGS :

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server : ☐

DHCP IP Address Range : to
(addresses within the LAN subnet)

Always Broadcast : ☒

Gateway :

WINS :

DNS :

DHCP Lease Time : 1 Hour ▾

不能打勾

LAN 設定

[套用 ▶](#) [× 取消](#)

裝置名稱 R7000 [編輯](#)

LAN TCP/IP 設定

IP 位址 . . .

IP 子網路遮罩 . . .

RIP 方向 雙向 ▾

RIP 版本 已停用 ▾

☐ 將路由器用作 DHCP 伺服器

起始 IP 位址 . . .

結束 IP 位址 . . .

位址保留

#	IP 位址	裝置名稱	MAC 位址
---	-------	------	--------

[+ 新增](#) [編輯](#) [× 刪除](#)

四、無線基地台基本設定

➤ 啟用MAC位置過濾

MAC ADDRESS FILTER :

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

WIRELESS ACCESS SETTINGS

Configure MAC Filtering below :

Turn MAC Filtering ON and ALLOW computers listed to access the network ▼

Turn MAC Filtering OFF

Turn MAC Filtering ON and ALLOW computers listed to access the network

Turn MAC Filtering ON and DENY computers listed to access the network

MAC Address	<<	MAC Address		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear
00:00:00:00:00:00	<<	MAC Address ▼		Clear

存取控制

套用 ▶

✕ 取消

您可以使用「存取控制」功能來允許或封鎖電腦或電子裝置存取您的網路。

☒ 開啟存取控制

存取規則：這是通用規則，您也可以允許或封鎖個別裝置。

☐ 允許所有新裝置連線

☒ 封鎖所有新裝置連線

允許

封鎖

編輯

重新整理

■	狀態	裝置名稱	IP 位址	MAC 位址	連線類型
☐	已封鎖	sony 10	192.168.1.2	9A:95:A9:B5:6C:3F	無線(NETGEAR82)

▶ 檢視目前沒有連線至網路的許可裝置清單

▶ 檢視目前沒有連線至網路的封鎖裝置清單

四、無線基地台基本設定

➤ 啟用並設定log 紀錄

VIEW LOG :
View Log displays the activities occurring on the DAP-1360.

LOG OPTIONS :
LOG OPTIONS : ☒ System Activity ☐ Debug Information ☒ Attacks
☐ Dropped Packets ☒ Notice

LOG DETAILS :

page 5 of 5

Time	Message
Jan 1 08:25:59	br0: port 3(wlan0) entering disabled state
Jan 1 08:26:04	device eth0 entered promiscuous mode

記錄

當前時間: 星期一, 二月 01, 2021 10:26:16

[Access Control] Device sony 10 with MAC address 9A:95:A9:B5:6C:3F is allowed to access the network
Monday, Feb 01, 2021 10:15:34
[Access Control] Device with MAC address 9A:95:A9:B5:6C:3F is blocked to access the network.
Monday, Feb 01, 2021 10:14:53
[Remote login] from source 140.123.29.131, Monday, Feb 01, 2021 10:13:47
[Remote login] from source 140.123.29.131, Monday, Feb 01, 2021 10:07:20
[Remote login] from source 140.123.29.131, Monday, Feb 01, 2021 09:53:27
[Remote login] from source 140.123.29.131, Monday, Feb 01, 2021 09:44:07
[Remote login] from source 140.123.29.131, Monday, Feb

日誌包括
☒ 試圖訪問被允許的網站
☒ 試圖訪問被限制的網站和服務
☒ 連接到本路由器的Web介面
☒ 路由器操作 (啟動、獲取時間等)
☒ 已知的 DoS 攻擊和掃描
☒ 連接埠轉送 / 連接埠觸發
☒ 無線接入
☒ 自動重設網際網路連線
☒ 按排程關閉無線訊號

無使用者連線紀錄、log紀錄無法長期保存

Log紀錄不易長期保存

中正大學 資訊處

26

四、無線基地台基本設定

➤ D-Link DAP-1360 VS Netgear R7000 功能比較

功能項目	DAP-1360	R7000
使用 2 層或 3 層的AES 加密方式	可	可
關閉未使用的網路設備管理埠	無	可
啟用連線逾時功能	可	可
變更出廠預設值的密碼內容	可	可
變更預設SSID	可	可
關閉SSID廣播	可	可
降低無線網路設備發送訊號功率	可	可
啟用備份系統組態設定值	可	可
限制重要功能操作	無	可

功能項目	DAP-1360	R7000
啟用MAC位置過濾	可	可
關閉DHCP 協定	可	可
啟用允許存取網路時段	可	可
啟用存取行為管控	無	可
啟用黑名單管控	無	部分
啟用並設定log 紀錄	部分	部分
啟用外部網路異常行為監控	無	無
啟用流量偵測功能	無	無
啟用流量調節功能	無	可
啟用登入錯誤次數限制	無	無

四、無線基地台基本設定

➤ 限制連線網段

- 管理介面只能單位網段可以連線
- 關閉網際網路Ping的回應

➤ log紀錄保存

- 連線使用者紀錄
- 使用者對外連線紀錄



五、學院無線網路介接管理

(一)學院無線網路-公共區域

SSID訊號：

- CCU-College：校內教職員生(免重複驗證90天)
- eduroam：國際漫遊認證

各學院大樓公共區域	
地點	基地台
文學院	1
法學院	1
社科院	1
管理學院	1
教育學院	2
理學院	2
工學院	3
總計	11



- ✓ 111年建置各學院介接端口交換設備及獨立光纖網路
- ✓ 112年建置各學院大樓公共地區高密度無線基地台(7學院安全連線示範點)
- ✓ 113年建置無線網路控制器、伺服器叢集安全架構(Cluster)，並建立學院介接管理制度及導入環球跨域無線漫遊認證服務，提升校園全面資安防護

(一)學院無線網路-連線速率

● 連線速率測試：Wi-Fi 6平均上傳235 Mbps、下載268 Mbps

各學院平均速率分布



工學院速率



理學院速率



管理學院速率



(二)學院無線網路-管理機制

➤各學院介接安全無線網路規範

- ✓向資訊處提出介接申請(ISMS-208-05)
- ✓需提供學院(系所)無線網路管理人資訊
- ✓管理系統帳號申請並限定連線IP(ISMS-208-01)
- ✓處理各學院內部無線網路連線問題

➤介接特點

- ✓連線速度穩定、安全認證機制及符合資安規範

(二)學院無線網路-建置需求調查

各學院無線網路建置需求調查表(填寫範例)¹

申請單位	法學院		
學院管理人	林○○	申請日期	113 年 01 月 01 日
電子信箱	abc@ccu.edu.tw	分機	11111
建置地點：			
系所	地點	數量	
院本部	XXX 辦公室、XXX 會議室、XXX 演講廳....	3	
A 系所	XXX 教室、XXX 電腦教室、XXX 辦公室、XXX 會議室、XXX 演講廳....	5	
B 系所	XXX 教室、XXX 電腦教室、XXX 會議室、XXX 演講廳....	4	
C 系所	XXX 教室、XXX 辦公室、XXX 會議室、XXX 演講廳....	4	
合 計		16	
申請人 (簽章)		單位主管 (簽章)	院長簽章

*欄位若不足請自行新增或調整。

THANK
YOU

簡報完畢