



個案分析-

ISP 電信數據機資安漏洞 事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/11

I. 事件原由

A. 10/15 部分新聞媒體報導某 ISP 電信 P874 數據機有資安漏洞，可能造成 WiFi 帳號密碼外洩。

B. 中時電子報：【中華電 Wi-Fi 洩個資 民眾氣憤罵很瞎】

註：新聞來源，<http://goo.gl/hfzeKN>

在家上網 WiFi 的帳號密碼居然會被人查到，中華電信內建 WiFi 的數據機爆出資訊安全漏洞，出包的 P874 型號幾乎都用在 50M 光世代用戶的家中，目前用戶至少 90 萬，不過中華電信說祇有開啟遠端搖控的人才會受到影響。

用遠端升級的方式來修正問題，不過帳號密碼被盜也讓人擔心，會不會引發個資外洩，甚至是小額付款功能被破解。

不在家用範圍內，拿著密碼也沒用，但資料有外洩疑慮，消基會批評業者應該主動告知，並且負責損失，主管機關 NCC 也表示會介入調查。

C. 蘋果日報：【中華電 Wi-Fi 數據機洩個資，隱瞞型號 P874 可被攔截帳密「很瞎」】 註：新聞來源，<http://goo.gl/2KMoKg>

【徐 毓莉/台北報導】中華電信內建 Wi-Fi 數據機遭爆資安漏洞。有民眾投訴指中華電信部分 P874 型號數據機，可輕易查出個人的無線網路帳號密碼，造成個資外洩，甚至遭有心人士利用。中華電信坦言知此瑕疵，已在更新改善，但未公布影響範圍。消基會批業者隱匿；民眾也罵：「很瞎！至少該先通知、讓民眾可保護自己。」

該批出包的數據機是內建 Wi-Fi 的 P874 型號，以往多用在 50M 光世代用戶家中，估計現有用戶至少 90 萬戶，但中華電信昨稱僅少部分戶數受影響，未公布確切的受影響戶數。

國家通訊傳播委員會（NCC）表示，會進一步調查。

恐成小額付款漏洞

任職外商科技公司的藍姓工程師向《蘋果》投訴指，近期發現有近 100 組以上的網路位址（IP）掃描他的防火牆漏洞，基於好奇，他也掃了同網段的 IP，發現許多浮動 IP 都有漏洞，再輸入網路上可找到的數據機帳號和密碼，登入後竟看到他人的無線網路服務群組識別碼（SSID）名稱和 Wi-Fi 連線密碼。

藍姓工程師質疑，輕易就可知道鄰居的無線上網密碼，意味著他自己的資料也會被輕易查出，被發現後恐遭用做其他不當用途，相關資料外洩或會造成小額付款漏洞。

《蘋果》記者撥打投訴人查到一組疑為手機號碼組合的密碼，接電話的民眾蘇先生確為 50M 光世代用戶，且表示該組帳號是家中門牌號碼、密碼是手機號碼，獲悉此事批說：「很瞎！中華電信至少應通知，讓民眾懂得保護自己。」

辯稱：拿到也沒用

中華電信回應說，僅 P874 型號中的極少數數據機有瑕疵，都是光世代用戶且用中華電信贈送的家用 Wi-Fi 使用者，但需電腦網路高手使用專業軟體，才可進入 截取少部分數據機的 Wi-Fi SSID 和密碼，且浮動 IP 並無地域性，「知道密碼也沒辦法做什麼動作」，但為免消費者疑慮，4 月起已透過升速陸續進行遠端更新，只要用戶數據機有插電、就可被更新，但未統計影響用戶。

資安網站「大砲開講」站長邱春樹表示，此可能風險包括有心人可透過進入數據機取得相關資料，恐造成個資外洩、電腦中毒、被當殭屍電腦運用、遭詐騙等。

專家：應全面回收

東華大學資訊工程系教授張瑞雄也說，若有瑕疵，業者有責任告知受影響的使用者，「萬一在解決之前民眾有損失，該由誰負責？就像買東西有瑕疵，應全面回收處理。」

消基會秘書長雷立芬表示，涉及個資外洩，發現當下就應主動告知消費者，如汽車有瑕疵就召回，而非隱匿不通知，若真的有人利用資料做壞事，損失就應由業者負責。

II. 數據機 P874 機型檢測

- A. 使用筆者自家的數據機進行檢查，實地檢測數據機是否有如報導所言。
- B. 透過自家內部網路電腦的私有 IP 連到數據機 LAN 的預設 IP 192.168.1.1。
- C. 數據機網頁管理資訊：
 1. 系統資訊，確認韌體版本預設設定。
 2. WAN 端資訊，表示數據機有做硬體撥接，故有取得公開 IP 在 WAN 端上，使內部網路電腦能 DHCP 取得私有 IP，透過 NAT 轉出上網。
 3. 預設 Access Control List 資訊

| 一般資訊: |
|---|
| 系統名稱: P874 韌體版本: P874N5AP_20120106W |
| 區域網路資訊: |
| MAC位址: 50:67:f0:71:06:68 IP位址: 192.168.1.1 IP子網路遮罩: 255.255.255.0 DHCP: Server DHCP 開始 IP: 192.168.1.101 DHCP 結束 IP: 192.168.1.200 |
| 無線網路資訊: |
| 名稱 (SSID): [模糊] 頻道: 1 安全模式: psk |

WAN Info

| VLAN Mux | 802.1P | Con. ID | Service | Interface | Protocol | Igmp | NAT | QoS | State | Status | IP Address |
|----------|--------|---------|---------------|-----------|----------|------|-----|-----|-------|--------------|-------------|
| Off | Off | 1 | NMS | ptm0_1 | IPoE | Off | Off | On | On | Connected | 128.0.1.2 |
| Off | Off | 2 | br_0_0_1_2 | ptm0_2 | Bridge | Off | Off | On | On | Connected | 0.0.0.0 |
| Off | Off | 4 | ipoe_0_0_1_4 | ptm0_4 | IPoE | Off | On | On | Off | Unconfigured | 0.0.0.0 |
| Off | Off | 3 | pppoe_0_0_1_3 | ppp0_3 | PPPoE | Off | On | On | On | Connected | 1. [模糊] 108 |

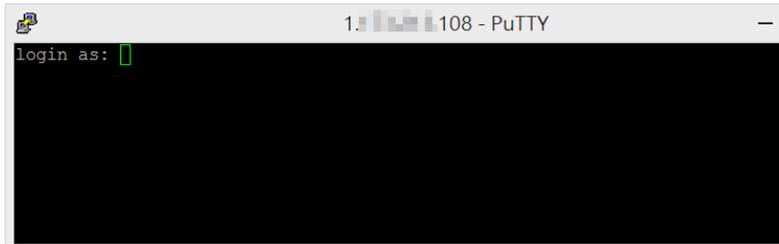
Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

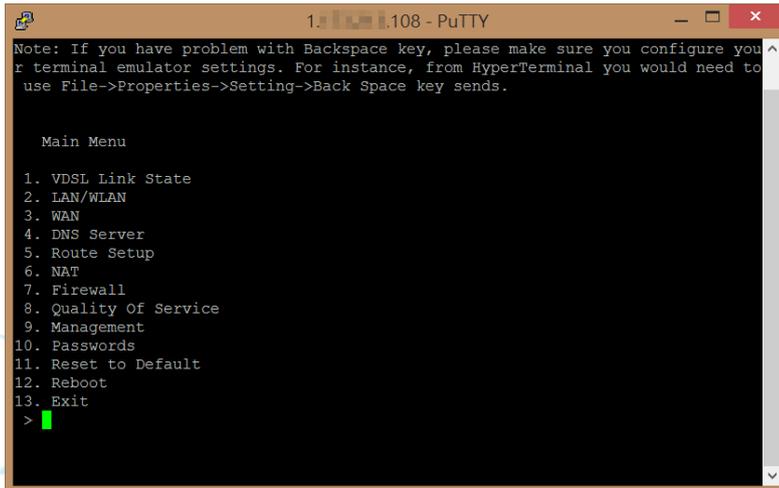
| Services | LAN | WAN |
|----------|--|--|
| FTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| HTTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| ICMP | Enable | <input type="checkbox"/> Enable |
| SNMP | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| SSH | <input checked="" type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable |
| TELNET | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TFTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |

Save/Apply

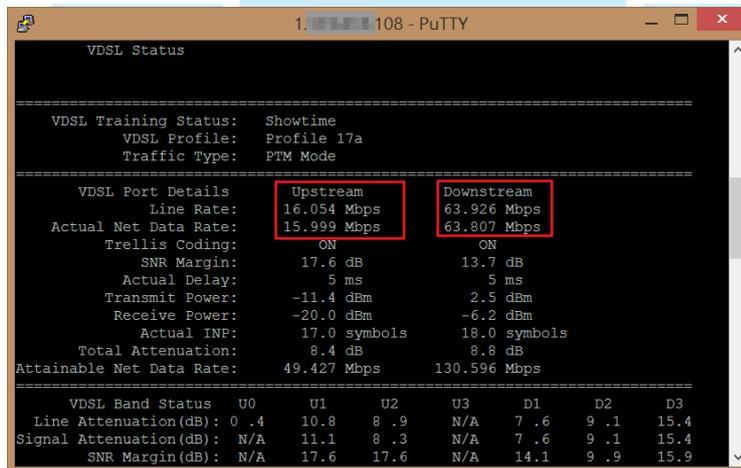
D. 預設的 ACL 中，WAN 端的 SSH 是 Enable 的，表示網際網路上的有心人士可以嘗試使用 SSH 連線登入數據機。



- E. 預設的登入帳號密碼在網路上是公開的，可能是使管理者易於登入管理，但同時也易於駭客入侵，登入後的頁面如下。



- F. 登入後發現所有進階的功能都能在此設定。
1. VDSL Link State：此處能觀測到使用者租用的頻寬資訊。



2. WAN：此處能看到用戶數據機的 WAN 介面資訊，有出現 PPPOE 的公開 IP。

```

1. 108 - PuTTY
Note: If you have problem with Backspace key, please make sure you configure your terminal emulator settings. For instance, from HyperTerminal you would need to use File->Properties->Setting->Back Space key sends.

WAN Menu
1. Configure
2. Delete
3. Show
4. Exit
/WAN > 3
VLAN 802.1P Con. Service Interface Proto. IGMP NAT QoS State Status IP
Mux ID Name Name Address
Off Off 1 NMS ptm0_1 IPoE Off Off On Enable Connected 128.0.1.2
Off Off 2 br_0_0_1_2 ptm0_2 Bridged Off Off On Enable Connected
Off Off 4 ipoe_0_0_1_4 ptm0_4 IPoE Off On On Disable Unconfigured 0.0.0.0
Off Off 3 pppoe_0_0_1_3 ppp0_3 PPPoE Off On On Enable Connected 1.1.1.108

Hit <enter> to continue

```

3. 第 10 項遠端管理的 Password 可以直接被修改，可能為駭客獨佔所用。
4. 第 12 項的 Reboot 可以做為重開機，使用中的用戶網路被中斷，然後重開機後 PPPOE 取得的動態 IP 可能就不會一樣。
5. Management：此為最重要的選項，裡面有個 Backup 選項可以將用戶的 VDSL 撥接設定透過 TFTP 方式匯出，並存成“XXX.conf”檔案。

```

1. 108 - PuTTY
Note: If you have problem with Backspace key, please make sure you configure your terminal emulator settings. For instance, from HyperTerminal you would need to use File->Properties->Setting->Back Space key sends.

Settings Menu
1. Backup
2. Update
3. Dump
4. Exit
/Management/Settings >

```

- a. 用一般的記事本開啟發現裡面的設定是用 XML 紀錄，包含使用者的「撥接的帳號和密碼」及「遠端管理的帳號和密碼」。
- b. 其中「遠端管理的帳號和密碼」是明文顯示

```

<ManagementServer>
<URL>http://cosmos1.ims1.cht.com.tw/core/Cosmos/ACSServer</URL>
<PeriodicInformEnable>TRUE</PeriodicInformEnable>
<PeriodicInformInterval>3600</PeriodicInformInterval>
<PeriodicInformTime>2010-01-01T00:13:48+00:00</PeriodicInformTime>
<ConnectionRequestUsername>admin</ConnectionRequestUsername>
<ConnectionRequestPassword>123456</ConnectionRequestPassword>
</ManagementServer>

```

- c. 而「撥接的帳號和密碼」的帳號是明文，密碼則是用簡易的 Base64 加密字串，透過 Base64 Decoder 就能輕易解開。

```

<WANPPPPConnection instance="1">
  <Enable>TRUE</Enable>
  <ConnectionType>IP_Routed</ConnectionType>
  <Name>pppoe_o_o_1_3</Name>
  <Username>87- [REDACTED] @hinet.net</Username>
  <Password>Mm [REDACTED] kA</Password>
  <X_BROADCOM_COM_ConnectionId>3</X_BROADCOM_COM_ConnectionId>
  <X_BROADCOM_COM_IfName>pppo_3</X_BROADCOM_COM_IfName>
  <X_BROADCOM_COM_BcastAddr>255.255.255.255</X_BROADCOM_COM_BcastAddr>
  <DNSServers>168.95.192.1,168.95.1.1</DNSServers>
  <PortMappingNumberOfEntries>0</PortMappingNumberOfEntries>
</WANPPPPConnection>

```

G. 通常有做硬體撥接的數據機都使因為預設 Wireless 是 enable 的，故常會將 wireless 的登入密碼用手機或市話號碼，此為明文記錄在設定檔裡。

III. 網段掃描檢測

A. 透過上面的自我檢測後，追查是否為個案或通案，故掃描同網段其他動態分配到的數據機 IP 是否也有相同問題，port SSH 是開啟的。

| IP | Ping | Hostname | Ports [2+] |
|-------------------|--------|--|------------|
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 12 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 22 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 22 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 12 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 11 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 12 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 40 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 11 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | -17 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 12 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 21 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 22 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |
| 1.173. [REDACTED] | 11 ms | 1-173- [REDACTED] .dynamic. [REDACTED] | 22 |

B. 因為數據機只要 reboot 後 WAN 取得的 IP 都是變動的，除非是有設定固定 IP，因此儼然已成為嚴重資安漏洞，因為一般用戶根本不會自行去關閉 PORT SSH。

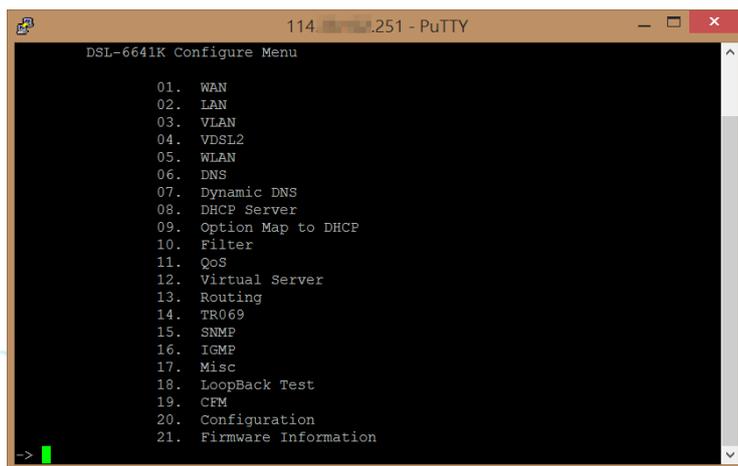
IV. 撥接帳號與密碼的用處

- A. 使用者取得撥接的帳號密碼就能夠登入電信業者的網站，取得個人相關資料，例如帳單資訊、固定 IP 位址查詢、查詢及修改註冊人 email 或者可能作為「小額付費」的其他用途。
- B. 固定 IP 常作為伺服器使用，例如 web server、NAS 或監視器等，駭客透過帳號密碼查詢到固定 IP 後就能嘗試登入，竊取個資和植入後門程式。
- C. 數據機的 WIFI 密碼駭客也能進行修改，讓服務中斷或竊取 client 的設備資訊。

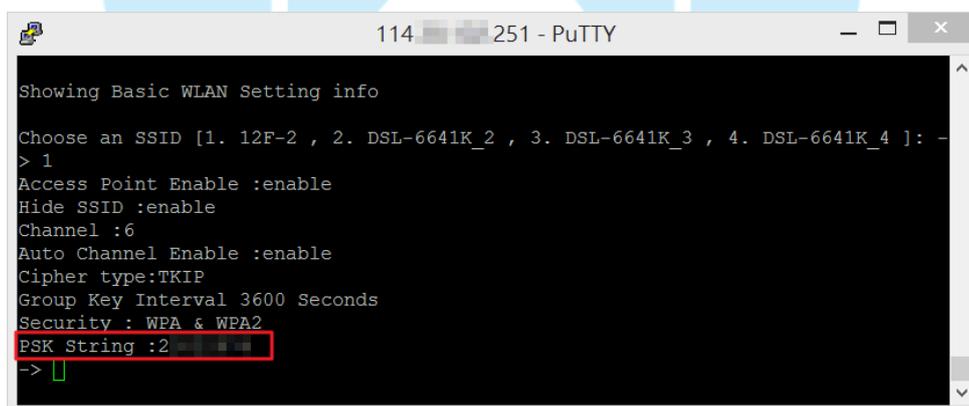
- D. 如果駭客已經取得用戶的市內電話號碼，可能變用戶的頻寬租約等。
- E. 目前測試無法使用他人帳密在其他地方進行撥接上網。

V. 數據機 DSL-6641 檢測

- A. 透過朋友允許測試租用的 DSL-6641 數據機，該數據機因為啟用 WIFI 功能，故有硬體撥接在 WAN 介面上會有一個實體 IP。
- B. 赫然發現該機型的 SSH 協定是 Enabled，而且無論是 WAN 或 LAN 都能用預設帳號密碼登入。



- C. 值得注意的是在設定選單中無法手動關閉此 SSH 協定，只能透過更改預設帳號密碼防止駭客輕易登入，或者使用 Filter 限制連入來源。
- D. 透過檢視 WLAN 設定可以看到 WIFI SSID 的登入密碼“PSK String”，通常用戶都會用電話做為密碼，也就是用戶的附掛電話或手機號碼。



- E. 設定選單中的 Backup 選項中可以匯出數據機設定檔，只是該設定檔為 bin 格式檔，內部的設定無法直接用文件編輯器解析出來，但若為高階駭客也許可以破解出其中的撥接帳號密碼。

```

114 .251 - PuTTY
DSL-6641K Configure Menu
01. Save and Reboot
02. ConfigPassword
03. Backup
04. Restore
05. Factory Reset
06. Factory Reset(In-band Management)
07. Back
-> 3
->

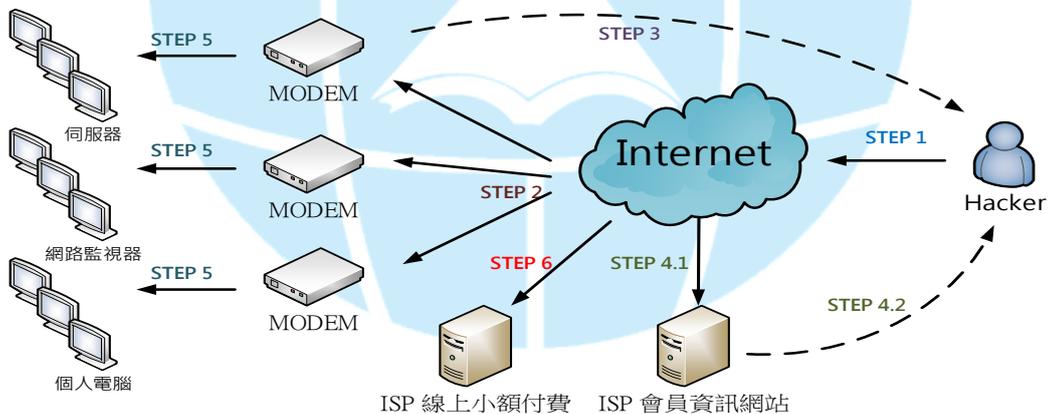
```

```

114 .251 - PuTTY
DSL-6641K Configure Menu
01. WAN DSL Settings
02. Show WAN_DSL
03. Back
-> 2
Connection 1:
Mode: Bridge
Interface: eth2
IP: 0.0.0.0
Connection 2:
Mode: PPPoE
Interface: ppp0
IP: 114. .251
Username: @wifi.hinet.net
Password: *****
Service Name:
AC Name:
IP Control: Dynamic IP
Static IP Address: 0.0.0.0
MTU: 1500
Default Route: 2
Connection 3: Disable

```

VI. 網路入侵架構圖



- STEP 1:** 駭客使用IP Port Scan 找尋WAN端SSH或HTTP開啟的數據機。
- STEP 2:** 駭客找到可入侵的數據機後開始用公開預設的帳號密碼登入管理。
- STEP 3:** 駭客使用Backup竊出PPPOE撥接的帳號密碼。
- STEP 4.1-4.2:** 駭客透過PPPOE帳密可在ISP會員網站查詢到個資及申請的固定IP。
- STEP 5:** 駭客可能入侵固定IP的設備，如監視器系統或其他伺服器。
- STEP 6:** 駭客可能利用帳密啟用線上小額付款機制消費。

VII. 數據機漏洞可能造成的影響

A. 以上 P874 和 DSL-6641 兩種機型的出廠預設值皆有重大漏洞，外部網路

- 的人都能透過 IP scan 的方式去找出有開啟 TCP PORT 的數據機。
- B. 電信業者的數據機製作廠商預設上皆是讓 SSH 或 HTTP 能夠從 WAN 端連入，只是預設工程帳號密碼卻是網路上被公開的，輕易開啟大門讓駭客進入。
 - C. 根據韌體版本的不同，可能啟用的 WAN PORT 也會有差，但都能掌控數據機所有設定。
 - D. 一旦撥接帳號密碼及電話被竊取，就能輕易透過網站查到登記人的資訊，例如固定 IP 通常用來作為伺服器或監視器系統用，可能就能被駭客所破解登入。
 - E. 個資外洩之外還可能用來做線上小額付款，或者線上修改撥接密碼，無須額外的身分認證機制，例如手機簡訊驗證碼機制，讓用戶無法得知密碼被竊改。

VIII. 建議措施

- A. 請使用者透過內部網路 192.168.1.X 登入數據機管理介面 192.168.1.1 進行管理密碼修改。
- B. 關閉 WAN 端所有 PORT 的服務，僅允許內部 LAN IP 進行登入。
- C. 盡速修改 PPPOE 撥接上網的密碼，以避免被駭客竊改後無法使用。
- D. DSL-6641 因為無法手動關閉 WAN 的 SSH，故建議請 ISP 業者更換其他機型設備，並確認 WAN 的服務已關閉。
- E. PPPOE 撥接上網密碼因最多只能設置 8 個字元，且不能有特殊符號，故建議定期修改以避免被破解。
- F. 若數據機本身有啟用 WIFI AP 功能，請不要設定 SSID 密碼為家用電話或手機號碼，避免容易被破解。