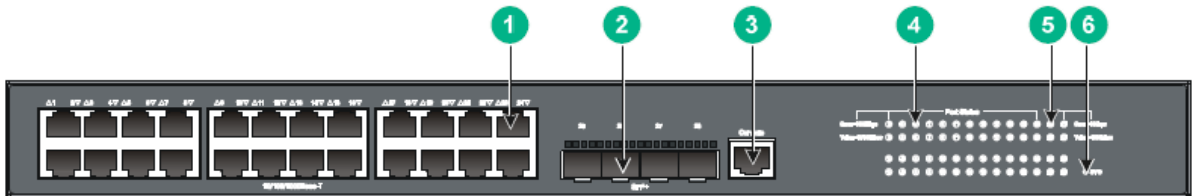


1-1 全新 HPE 5130EI 交換器(出廠預設值)第一次 Console 登入

- 資網中心網路管理實驗室建置 HPE 公司之 HPE FlexNetwork 5130 24G 4SFP+ EI(JG932A) 高階交換器，每人一機以配合本市校園智慧網路建置案之教育訓練。

Front panel



- | | |
|---|---|
| (1) 10/100/1000Base-T autosensing Ethernet port | (2) SFP+ port |
| (3) Console port | (4) 10/100/1000Base-T autosensing Ethernet port LED |
| (5) SFP+ port LED | (6) System status LED (SYS) |

Rear panel



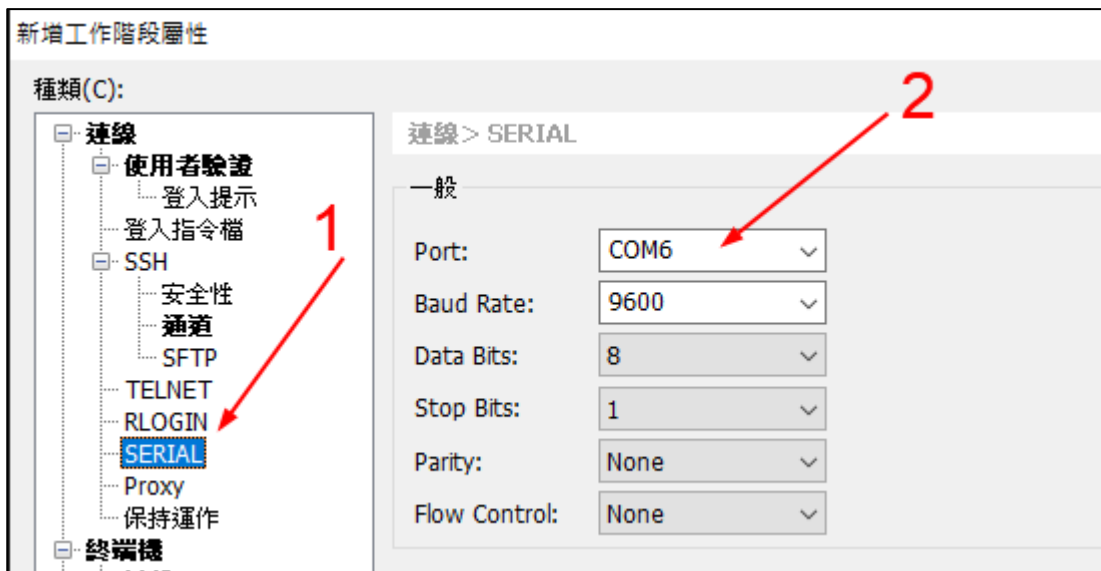
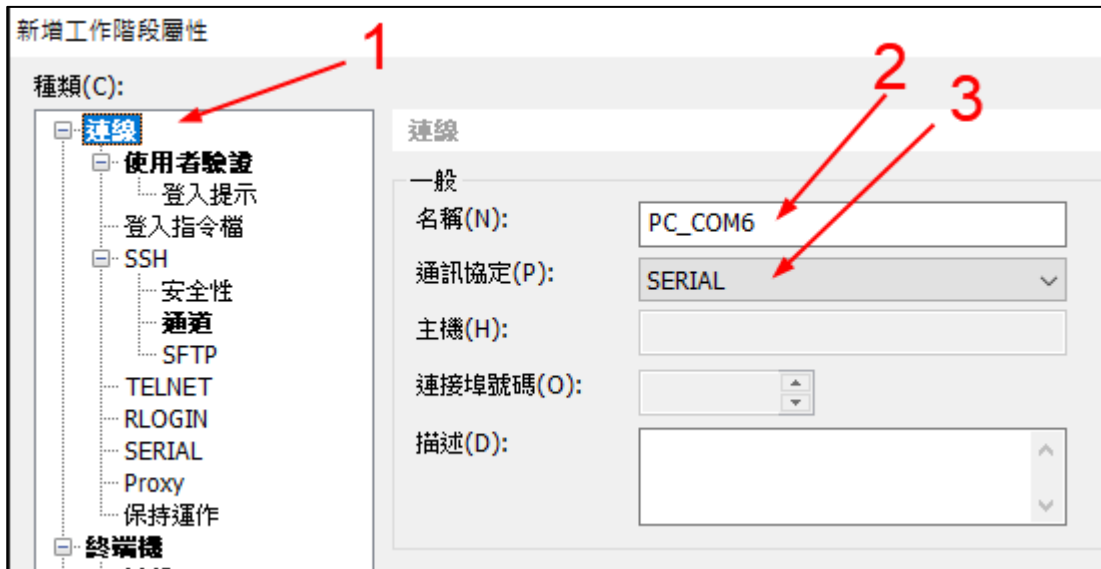
- | | |
|-------------------------------|---------------------|
| (1) AC-input power receptacle | (2) Grounding screw |
|-------------------------------|---------------------|

1. 請將 Console 線一端接入 switch 的 Console port 另一端插入電腦(筆電)的 USB 孔，請從裝置管理員確認目前是 COM?



2. 啟動 XShell，新增一個工作階段，
名稱：PC_COM?
通訊協定：SERIAL
Port：COM?

輸入完成後，點選「連線」即可進入 Command Line Interface(CLI)



預設進入 User View 模式，提示符號為<>，輸入 system-view 指令後，進入 System View 模式，提示符號為[]

<HPE>

<HPE>**system-view**

System View: return to User View with Ctrl+Z.

[HPE]

1-2HPE 5130EI 交換器基礎設定

1. 基本指令：

<HPE>**display current-configuration** 顯示儲存在記憶體中的當前設定組態 (Cisco : show running-configuration)

<HPE>**display version** 顯示交換器的軟硬體版本及規格(Cisco : show version)

<HPE>**display interface brief** 查看各介面的狀態(Cisco : show interface status)

<HPE>**system-view** 進入 config 模式(Cisco : enable 加 configure terminal)

[HPE]**sysname** 設定交換器名稱(Cisco : hostname)

[HPE]**save** 儲存設定(Cisco : write)

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait....

Saved the current configuration to mainboard device successfully.

Configuration is saved to device successfully.

[HPE]**display this** 顯示返在介面的相關設定

[HPE]**quit** 返回上一層

[HPE]**ping** 送出 ICMP 封包

[HPE]**tracert** 使用 traceroute 功能

<HPE>**reboot** 重開機(Cisco : reload)

<HPE>**startup saved-configuration** startup.cfg 指定下次開機使用的組態設定檔

<HPE>**reset saved-configuration** 清除 config

<HPE>**restore factory-default** 回復原廠設定(Cisco : write erase)

<HPE>**undo terminal monitor** 關閉訊息顯示

Cisco :

no logging console

no logging monitor

2. 設定交換器的 ip 位址(vlan1)、dns Server 及預設閘道

[HPE]**interface vlan-interface 1** #進入 vlan1 介面(所有交換器預設的 vlan 都是 vlan1)

[HPE-Vlan-interface1]**ip address 140.128.52.xxx 255.255.255.248**

(HP5130 請設第一個可用 IP，Cisco2960 請設第二個可用 IP)

[HPE-Vlan-interface1]**quit**

[HPE]**ip route-static 0.0.0.0 0.0.0.0 140.128.52.yyy**(FG 的 lan1 位址)

(Cisco :ip default-gateway)

[HPE]**dns server 168.95.1.1** (Cisco :ip name-server)

[HPE]**display ip interface** (Cisco :show ip interface)

[HPE]**display ip routing-table** (Cisco :show ip route)L3 Switch 才有的功能

網路校時

```
[HPE]display clock 顯示系統目前時間(Cisco :show clock)
[HPE]clock timezone Taipei add 8 設定時區 (Cisco :clock timezone Taipei 8)
[HPE]ntp-service unicast-server 118.163.81.61 source Vlan-interface 1 設定 ntp
server 位址及來源介面
(Cisco: ntp server 118.163.81.61 source vlan 1)
[HPE]ntp-service enable 啟用網路校時
[HPE]display ntp-service status
(Cisco:
show ntp status
show ntp associations)
```

3. 建立一個本機帳戶 admin，允許使用 ssh，console 及 web 方式連入

```
[HPE]local-user admin
New local user added.
[HPE-luser-admin]authorization-attribute user-role network-admin (HP5120 指令
authorization-attribute level 3)
[HPE-luser-admin]service-type ssh terminal https
[HPE-luser-admin]password-control aging 90
[HPE-luser-admin]password-control length 6
[HPE-luser-admin]password simple xxxxxx
[HPE-luser-admin]quit
[HPE]display local-user
```

```
Cisco :
service password-encryption
username admin privilege 15 password xxxxxx
```

4. 啟用需要的服務

```
[HPE]telnet server enable
```

```
[HPE]ip http enable
```

```
(Cisco:
ip http server
ip http authentication local)
```

```
[HPE]ip https enable (Cisco: ip http secure-server)
```

```
[HPE]public-key local create rsa
```

```
[HPE]ssh server enable
```

```
Cisco:
ip domain-name wres.tc.edu.tw
crypto key generate rsa
```

設定 telnet 和 ssh 的認證方法

```
[HPE]line vty 0 4
```

```
[HPE-line-vty0-4]authentication-mode scheme (Cisco: login local)
```

```
[HPE]quit
```

```
[HPE]save
```

建議啟用 ssh 及 https 就好

5. 設定 console 連入密碼

```
[HPE]line aux 0
```

```
[HPE-ui-aux0]authentication-mode password
```

```
[HPE-ui-aux0]set authentication password simple xxxxxx
```

```
[HPE-ui-aux0]user privilege level 15
```

若要使用帳號及密碼登入 console，則上面 2~4 行改為

```
HPE-ui-aux0]authentication-mode scheme
```

(Cisco:

```
line console 0
```

```
login local)
```

請分別用 ssh 和瀏覽器(https)連入交換器

確認已成功 ssh 登入後，再從 console 登入一次

1-3 交換器 STP 與 edge port(PortFast)設定與 BPDU 保護

- 1 預設 HPE5130 與 Cisco2960S 交換器均啟用 STP

- 2 HPE 進入介面個別設定(trunk port 不要設定)

```
[HPE]interface range gi1/0/2 to gi1/0/22
```

```
[HPE-if-range]stp edged-port
```

所有啟用 portfast 功能的連接埠，啟用 bpdu 保護

```
[HPE]stp bpdu-protection
```

- 3 Cisco 進入介面個別設定(trunk port 不要設定)

```
Switch(config)int range gi1/0/1-22
```

```
Switch(config-if-range) spanning-tree portfast
```

```
Switch(config-if-range)spanning-tree bpduguard enable
```

- 4 Cisco 也可全域快速設定

```
Switch(config)#spanning-tree portfast default
```

所有啟用 portfast 功能的連接埠，啟用 bpdu 保護

```
Switch(config)#spanning-tree portfast bpduguard default
```

再進入介面個別取消 portfast 及 bpduguard 設定

1-4 HPE 5130EI 交換器 VLAN 設定

1. 各廠牌交換器預設所有 port 都隸屬於 vlan1

查看目前 vlan 狀況：

```
display vlan all (Cisco: show vlan)
```

2. 本次研習把 port1-8 設為 van1，port9-16 設為 van2，port17-22 設為 vlan3

3. 建立 vlan2，並將 port9-16 設定到 vlan2，建立 vlan3，並將 port17-22 設定到 vlan3

```
[HPE]vlan 2
```

```
[HPE-vlan2]vlan 3
```

```
[HPE] interface range gi1/0/9 to gi1/0/16 (Cisco: interface range gi1/0/9-16)
```

```
[HPE -if-range] port link-type access(Cisco: switchport mode access)
```

```
[HPE -if-range] port access vlan 2(Cisco: switchport access vlan 2)
```

```
[HPE -if-range] quit
[HPE] interface range gi1/0/17 to gi1/0/22
[HPE -if-range] port link-type access
[HPE -if-range] port access vlan 3
[HPE -if-range] quit
```

4. 查看目前 Vlan 設定狀況
[HPE]display vlan brief (Cisco: show vlan brief)

跨交換器 Vlan Trunk

5. HPE 交換器設定 802.1Q Trunk Port (例如設定 Port 24 為 Trunk Port，允許所有 vlan 封包)
[HP]interface gi1/0/24
[HPE-GigabitEthernet1/0/24]port link-type trunk
[HPE-GigabitEthernet1/0/24]port trunk permit vlan all
6. Cisco 交換器設定 802.1Q Trunk Port (例如設定 Port 24 為 Trunk Port，允許所有 vlan 封包)
[HP]interface gi1/0/24
Switch(config-if)switchport mode trunk
Switch(config-if)switchport trunk allowed vlan all

1-5HPE 5130EI 交換器 DHCP Snooping 設定

1. 本次研習假設 DHCP Server 接在 Port1，其他 Port 不允許有 DHCP Server
2. 查看目前 dhcp snooping 狀況
<HPE>display dhcp snooping trust
3. 啟用 dhcp snooping 功能
[HPE]dhcp snooping enable
4. 允許 port1 可以有 DHCP Server
[HPE]interface GigabitEthernet 1/0/1
[HPE-GigabitEthernet1/0/1]dhcp snooping trust
5. 若是沒有 Port 設成 dhcp snooping trust,那麼這台 Switch 就沒有 Client 可以從 DHCP Server 拿到 IP
6. Cisco 指令
ip dhcp snooping
ip dhcp snooping vlan 1-3,5
interface gi1/0/1
ip dhcp snooping trust

1-6HPE 5130EI 交換器 SNMP 設定

1. [HPE]snmp-agent
[HPE]snmp-agent community read public
[HPE]snmp-agent community write private
[HPE]snmp-agent sys-info location InfoCenter
[HPE]snmp-agent sys-info contact mis@wres.tc.edu.tw
[HPE]snmp-agent sys-info version v1 v2c
2. 也可從網頁管理介面設定

1-7 HPE5130EI 交換器 Port Security 設定

1. 查閱交換器的全部 mac address table

```
<HPE>display mac-address (Cisco: show mac address-table)
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0002-4661-41fd    1        LEARNED        GigabitEthernet1/0/1  AGING
0007-e910-3ad2    1        LEARNED        GigabitEthernet1/0/1  AGING
000c-2926-d00a    1        LEARNED        GigabitEthernet1/0/1  AGING
000c-2943-3a2e    1        LEARNED        GigabitEthernet1/0/1  AGING
```

2. 查詢特定 mac address 出現在哪一個 port

```
<HPE>display mac-address 1c87-2ccb-732a
(Cisco: show mac address-table address 1c87-2ccb-732a)
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
1c87-2ccb-732a    1        LEARNED        GigabitEthernet1/0/8  AGING
```

```
--- 1 MAC address(es) found ---
```

3. 查詢特定的 port 下面有哪些 mac address

```
<HPE>display mac-address interface gi1/0/4 (Cisco: show mac address-table interface gi1/0/4)
```

4. 透過 Port Security，我們可以將特定的設備與交換器特定的 port 做綁定，可以簡單的實現網路安全管理

5. 首先啟用 port security

```
[HPE]port-security enable
```

6. 進入我們想要綁定的 port，這邊假設是 port13

```
[HPE]interface GigabitEthernet 1/0/13
```

7. 調整 port 允許的最大 MAC 學習數量為 1，設定模式為自動學習，並綁定一個 MAC address 與指定 vlan

```
[HPE-GigabitEthernet1/0/13]port-security max-mac-count 1
```

```
[HPE-GigabitEthernet1/0/13]port-security port-mode autolearn
```

也可以自己預先指定

```
[HPE-GigabitEthernet1/0/13] port-security mac-address security sticky 001b-11c3-065d vlan 2
```

設定完之後，用 display port-security 的方式檢視

8. 發生時，暫時關閉該 port

9. [HPE-GigabitEthernet1/0/13] port-security intrusion-mode disableport-temporarily

設置 Intrusion Protection 特性被觸發後，暫時關閉該 port

10. [HPE]port-security timer disableport 30 關閉時間為 30 秒。

Cisco

```
Switch(config)interface gi1/0/13
```

```
Switch(config-if)switchport mode access
```

```
Switch(config-if)switchport port-security
```

```
Switch(config-if)switchport port-security maximum 1
```

自動學習

```
Switch(config-if)switchport port-security mac-address sticky
```

或手動指定

```
Switch(config-if)switchport port-security mac-address sticky 001b.117c.697e
```

發生時關閉該 port

```
Switch(config-if)switchport port-security violation shutdown  
或燈號照亮但無法連線
```

```
Switch(config-if)switchport port-security violation protect
```

```
Switch#show port-security
```

```
Switch#show port-security address
```

```
Switch#show port-security interface gi1/0/13
```

1-8 HPE 5130EI 交換器 IP-MAC-Port Binding 設定

1. 使用連接埠綁定，可以將用戶端的 MAC 地址和 IP 地址綁定到指定的連接埠上。進行綁定操作後，交換機只對從該端口收到的指定 MAC 地址和 IP 地址的用戶發出的封包進行轉發，提高了系統的安全性，增強了對網路安全的監控。
2. 將 Port14 綁定 IP 位址及 MAC 位址

```
[HPE]interface gi1/0/14  
[HPE-GigabitEthernet1/0/14]ip source binding ip-address 192.168.50.14 mac-address 1234-5678-9abc  
[HPE-GigabitEthernet1/0/14] ip verify source ip-address mac-address
```
3. 建議：指定 IP-MAC Binding 在全域(system-view)，然後在各個介面啟用 ip verify source ip-address mac-address

1-9 HPE 5130EI 交換器 LACP 設定

1. 設定 Link Aggregation 及 Vlan：

```
[HPE]interface Bridge-Aggregation 1  
[HPE-Bridge-Aggregation1]port link-type access  
[HPE-Bridge-Aggregation1]port access vlan 2  
[HPE-Bridge-Aggregation1]link-aggregation mode dynamic
```

如果 LACP 聚合 port 後端不是接 NAS 或 Server，而是要接交換器做 trunk

```
[HPE-Bridge-Aggregation1]port link-type trunk  
[HPE-Bridge-Aggregation1]port trunk permit vlan all  
[HPE-Bridge-Aggregation1]link-aggregation mode dynamic
```
2. 本次研習把 port23 及 port24 設為 Link Aggregation

```
[HPE]interface range gi1/0/23 to gi1/0/24  
[HPE-if-range] port link-aggregation group 1
```
3. 檢視 LACP 狀況

```
[HPE]display link-aggregation verbose Bridge-Aggregation 1  
[HPE]display interface Bridge-Aggregation 1
```

1-10 Cisco 2960S 交換器 EtherChannel(LACP)設定

1. 設定 port-channel 及 Vlan：


```
Switch(config)interface Port-channel 1
```

```
Switch(config-if)switchport mode access
```

```
Switch(config-if)switchport access vlan 2
```

如果 LACP 聚合 port 後端不是接 NAS 或 Server，而是要接交換器做 trunk

```
Switch(config-if)switchport mode trunk
```

```
Switch(config-if)switchport trunk allowed vlan all
```

2. 本次研習把 port23 及 port24 設為 EtherChannel

```
Switch(config)interface range gi1/0/23-24
```

```
Switch(config-if-range)no switchport mode
```

```
Switch(config-if-range)channel-group 2 mode active
```

3. 檢視 EtherChannel 狀況

```
Switch# show etherchannel summary
```

```
Switch# show interfaces port-channel 1
```