

【Cisco】Switch相關指令

LAB 2-1:Switch基本環境設定

清除Switch的組態設定

```
Switch>enable
Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload
```

Switch設主機名稱

```
Switch#configure terminal
Switch(config)#hostname lab2
```

console閒置設0分,啟用logging訊息輸出後自動換行功能

```
lab2(config)#line console 0
lab2(config-line)#exec-timeout 0 (閒置登出)
lab2(config-line)#logging synchronous (訊息同步)
```

停用網域名稱反查

```
lab2(config-line)#exit
lab2(config)#no ip domain-lookup
```

設定界面資訊(description),雙工(duplex)模式及介面速度(speed)

```
lab2(config)#interface fastEthernet 0/12
lab2(config-if)#description TORouter
lab2(config-if)#duplex auto (預設auto)
lab2(config-if)#speed auto (預設auto)
lab2(config-if)#exit
```

設定Switch IP及Gateway (L2 Switch訂IP管理用)

```
lab2(config)#interface vlan 1
lab2(config-if)#ip address 192.168.0.250 255.255.255.0
lab2(config-if)#no shutdown
lab2(config-if)#exit
lab2(config)#ip default-gateway 192.168.0.254 (跨網段管理)
```

show 相關設定,存入NVRAM

```
lab2#show running-config
lab2#show vlan 1
lab2#show interfaces fastEthernet 0/12
lab2#copy running-config startup-config
```

LAB 2-2:Switch安全防護設定

設定Console及vty密碼

```
lab2#configure terminal
lab2(config)#line console 0
lab2(config-line)#password console
lab2(config-line)#login
lab2(config-line)#exit
lab2(config)#line vty 0 15
lab2(config-line)#password vty
lab2(config-line)#login
lab2(config-line)#exit
```

設定privileged mode的密碼並檢視

```
lab2(config)#enable password password
lab2(config)#enable secret cisco
lab2(config)#end
lab2#sh running-config
```

設定SSH

```
lab2#configure terminal
lab2(config)#ip domain-name example.com
lab2(config)#crypto key generate rsa
lab2(config)#username netadmin password netadmin
```

```
lab2(config)#ip ssh version 2
lab2(config)#line vty 0 15
lab2(config-line)#login local
lab2(config-line)#transport input ssh telnet
```

直接進入特權模式

```
lab2(config)#no username {netadmin}
lab2(config)#username {name} privilege 15 password {password}
```

啟用密碼加密服務

```
lab2#conf t
lab2(config)#service password-encryption
lab2(config)#do show running-config | begin line
```

設定Login banner

```
lab2(config)#banner login >
HI !!!! >
LAB 2-3:Port Security(防非法MAC存取)
```

Port security 只能針對Access mode的Port設定

```
enable port security
(Optional)設定最大MAC數量,預設 1 sh不顯示,Cisco設備預設值通常不顯示
違規時switch的動作violation{ shutdown預設 | restrict | protect}
1~4只防阻MAC Flooding攻擊,每一個port只能有1個MAC通過,但還不能防止非法MAC接到設備上,把合法MAC寫到table,只要MAC有錯port shutdown
在Switch上查看MAC-Address-Table
lab2#show mac-address-table (有些版本 show mac address-table)
```

將FA0/24啟用Port-Security功能,指定只學習一筆MAC資訊,使用Sticky方式學習到PC的MAC,並設定違規處理方式為Shutdown

```
lab2#configure terminal
lab2(config)#interface fastEthernet 0/24 (多個Port可用range)
lab2(config-if)#switchport mode access (將Port改成Access Mode)
lab2(config-if)#switchport port-security (啟用Port Security)
lab2(config-if)#switchport port-security maximum 1 (設定最大的MAC數量)
lab2(config-if)#switchport port-security mac-address sticky
lab2(config-if)#switchport port-security violation shutdown(預設,處理err-disabled)
或
lab2(config-if)#switchport port-security violation restrict (合法MAC接回就會通)
```

range 多個Port要設定

```
lab2(config)#interface range fastEthernet 0/4 - 7 , fastEthernet 0/9 - 11
lab2(config-if-range)#switchport mode accesss
```

檢查所有界面的狀態(Port,Description Name,Status,Vlan,Duplex,Speed,Type)

```
lab2#sh interfaces status
```

檢查Switch上有哪些Port啟用Port-security

```
lab2(config-if)#do sh port-security
```

檢查Switch上有哪些Port有sticky或手動輸入合法MAC Address

```
lab2(config-if)#do sh port-security address
```

檢查Fa0/24的Port-security的詳細設定

```
lab2(config-if)#do sh port-security interface fastethernet 0/24
```

檢查Fa0/24的介面狀態(注意err-disabled)

```
lab2(config-if)#do sh int fa 0/24
```

將Fa0/24接另一台PC,因為Fa0/24有啟用Port-security,並將之前自動學習到的MAC以Sticky記錄,檢查Fa0/24的介面狀態會出現err-disabled:以下處理方法

```
lab2#sh int fa 0/24
FastEthernet0/24 is down, line protocol is down (err-disabled)
lab2#sh run | begin FastEthernet0/24
!
interface FastEthernet0/24
switchport mode access
```

```
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0030.F22D.9A05
!
lab2#conf t
lab2(config)#int fa 0/24
lab2(config-if)#no switchport port-security mac-address sticky 0030.F22D.9A05
lab2(config-if)#do sh int fa 0/24
FastEthernet0/24 is down, line protocol is down (err-disabled)
lab2(config-if)#shutdown
lab2(config-if)#no shutdown
LAB 2-4:CDP與檔案備份練習
```

CDP查詢鄰近設備

```
lab2#sh cdp neighbors (Device ID =>ro)
lab2#sh cdp entry ro
```

將Switch的fa0/3介面CDP功能關閉

```
lab2(config)#int fa 0/3
lab2(config-if)#no cdp enable
```

將設備cdp功能關閉

```
lab2(config)#no cdp run
```

將Switch的IOS與startup-config複製到TFTP

```
lab2#sh flash
lab2#copy flash tftp
lab2#copy running-config startup-config
lab2#copy startup-config tftp
```

show 的使用

```
lab2#sh running-config | begin line
lab2#sh running-config | include line
lab2#sh interfaces status
lab2#sh mac address-table
#
#
#
```

🕒 修訂版本 #1

★ 由 treeman 建立於 15 📅 2022 22:12:55

✎ 由 treeman 更新於 5 📅 2023 10:14:58