

網路相關

- [【Cisco】Switch相關指令](#)
- [【Fiddler】玩轉 Fiddler－HTTP\(s\) 抓包能手](#)
- [【Mac】透過console連接網路設備](#)
- [【zabbix】自定義通知\(轉貼\)](#)
- [學習相關連結](#)
- [smokeping install](#)
- [【DNS】台灣地區常用 DNS IP 整合表](#)

【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
#
#
#
```

【Fiddler】玩轉 Fiddler—HTTP(s) 抓包能手

玩轉 Fiddler—HTTP(s) 抓包能手 & 常見「特殊」用途

<https://ryanlee.tw/2021/08/23/fiddler/>

【Mac】透過console連接網路設備

需求：一條usb - console 線

【伽利略】USB CONSOLE Cable FT232 3m(USB232FTD)



CONSOLE Cable

【伽利略】USB CONSOLE Cable FT232 3m(USB232FTD)

06/01~06/30 3C年中大促★下殺95折

滿1件享95折 (說明)

- FT232RL+ZT213
- RJ-45串口配置線
- 傳輸線長: 3m



品號: 5329068

市售價 599 元 促銷價 **488** 元 下單再折 ▾ 賣貴通報

品牌名稱 : 伽利略

結帳方式 : 信用卡 \ 貨到付款 \ 超取付款 \ LINE Pay \ Apple Pay \ Google Pay
\ 街口支付 \ 悠遊付 \ ATM \ 無卡分期 \ 銀聯卡
刷mo卡5%無上限, 含權益3%

接上後，打開終端機，使用screen 登入設備

```
#找到 console 線
ll /dev/tty.*
crw-rw-rw- 1 root wheel  9,  0  6 22 22:26 /dev/tty.Bluetooth-Incoming-Port
crw-rw-rw- 1 root wheel  9,  2  6 24 09:58 /dev/tty.usbserial-A50285BI

#登入設備
screen /dev/tty.usbserial-A50285BI 9600
```

screen其他操作

退出後重連失敗

```
~ ➤ screen /dev/tty.usbserial-A50285BI 9600
Cannot open line '/dev/tty.usbserial-A50285BI' for R/W: Resource busy
```

```
#找到screen pid
screen -list

There are screens on:
  15520.ttys004.Treeman-Mac    (Attached)
  9100.ttys003.Treeman-Mac    (Detached)
2 Sockets in /var/folders/px/8z7kvlwj5278qcf92c71q6_h0000gn/T/.screen.

#方法一 刪除socket 重新連線
#刪除socket screen -X -S {pid} quit
# -X: 執行cmd, -S: screen socket name, quit: 離開
screen -X -S 9100.ttys003.Treeman-Mac quit
#在連線一次
screen /dev/tty.usbserial-A50285BI 9600

#方法二 使用screen pid.name重新連線
screen -R 9100.ttys003.Treeman-Mac

#方法三 重新連線上次中斷screen
screen -r
```


【zabbix】自定義通知(轉貼)

開啟 https://notify-bot.line.me/zh_TW/

登入帳號後，下拉選項，選取「個人頁面」→「發行權杖」→「透過1對1聊天接收LINE Notify的通知」

之後就會得到一組權杖「Token」，這組Token務必要記錄下來，出現後便不再顯示

Zabbix Server端

設定Script

```
sudo vi /usr/lib/zabbix/alertscripts/line_notify.sh
```

```
#!/bin/bash
# LINE Notify Token - Media > "Send to".
TOKEN="$1"
# {ALERT.SUBJECT}
subject="$2"
# {ALERT.MESSAGE}
message="$3"
curl https://notify-api.line.me/api/notify -H "Authorization: Bearer ${TOKEN}" -F "message=${message}"
```

```
sudo chmod 755 /usr/lib/zabbix/alertscripts/line_notify.sh
```

```
sudo chown zabbix:zabbix line_notify.sh
```

Zabbix Ui 設定

1. 「管理」→「示警媒介類型」→「創建示警媒介類型」

示警媒介類型

名稱	Line Notify												
類型	腳本 ▼												
腳本名稱	line_notify.sh												
Script parameters	<table><thead><tr><th>參數</th><th>動作</th></tr></thead><tbody><tr><td>{ALERT.SENDTO}</td><td>移除</td></tr><tr><td>{ALERT.SUBJECT}</td><td>移除</td></tr><tr><td>{ALERT.MESSAGE}</td><td>移除</td></tr><tr><td colspan="2">新增</td></tr></tbody></table>			參數	動作	{ALERT.SENDTO}	移除	{ALERT.SUBJECT}	移除	{ALERT.MESSAGE}	移除	新增	
參數	動作												
{ALERT.SENDTO}	移除												
{ALERT.SUBJECT}	移除												
{ALERT.MESSAGE}	移除												
新增													

Name : Line Notify
Type : Script
Script name : line_notify.sh
Script parameters :
{ALERT.SENDTO}
{ALERT.SUBJECT}
{ALERT.MESSAGE}

2. 「管理」→「用戶」→「Admin」→「示警媒介」→「新增」

示警媒介

類型 Line Notify ▼

收件人

當作用中時

用此如果示警度 ☒ 未分類
☒ 資訊
☒ 警告
☒ 一般嚴重
☒ 嚴重
☒ 災難

已啟用 ☒

新增 取消

Send to：填入上面步驟拿到的`TOKEN`

3.「組態」→「動作」→「創建動作」

名稱

計算方式 Or ▼ A or B or C

條件	標示	名稱	動作
A		觸發器示警度 = 災難	移除
B		觸發器示警度 = 嚴重	移除
C		觸發器示警度 = 一般嚴重	移除

新的觸發條件

觸發器示警度 ▼ = ▼ 未分類 ▼

[新增](#)

動作 操作 Recovery operations

預設操作步驟停留時間 (最少60秒)

預設主旨

預設訊息

主機名稱: {HOSTNAME1}

發生時間: {EVENT.DATE} {EVENT.TIME}

警示等級: {TRIGGER.SEVERITY}

警示訊息: {TRIGGER.NAME}

警示項目: {TRIGGER.KEY1}

問題說明: {ITEM.NAME}: {ITEM.VALUE}

當前狀態: {TRIGGER.STATUS}: {ITEM.VALUE1}

{HOST.NAME1}: {TRIGGER.STATUS}: {TRIGGER.NAME}

主機名稱: {HOSTNAME1}
發生時間: {EVENT.DATE} {EVENT.TIME}
警示等級: {TRIGGER.SEVERITY}
警示訊息: {TRIGGER.NAME}
警示項目: {TRIGGER.KEY1}
問題說明: {ITEM.NAME}: {ITEM.VALUE}
當前狀態: {TRIGGER.STATUS}: {ITEM.VALUE1}
事件ID: {EVENT.ID}

備註：**Recovery operations** 的欄位主旨和訊息都和這邊一樣

動作

操作

Recovery operations

預設操作步驟停留時間

3600 (最少60秒)

預設主旨

{HOST.NAME1}: {TRIGGER.STATUS}: {TRIGGER.NAME}

預設訊息

主機名稱: {HOSTNAME1}
發生時間: {EVENT.DATE} {EVENT.TIME}
警示等級: {TRIGGER.SEVERITY}
警示訊息: {TRIGGER.NAME}
警示項目: {TRIGGER.KEY1}
問題說明: {ITEM.NAME}: {ITEM.VALUE}
當前狀態: {TRIGGER.STATUS}: {ITEM.VALUE1}

Pause operations while in maintenance

☒

操作

步驟

細節

開始於

持續時間(秒)

動作

新的

操作細節

步驟

1

-

1

(0 - infinitely)

步驟持續時間

0

(最少 60 秒, 0 為預設值)

操作類型

送出訊息

送到用戶群組

用戶群組

動作

新增

送到用戶

用戶

Admin (Zabbix Administrator)

動作

新增

移除

僅送到

Line Notify

預設訊息

☒

條件

標示

名稱

動作

新的

新增

取消

Recovery operations 的操作配置

操作細節

操作類型

Send recovery message ▼

預設訊息



[新增](#) [取消](#)

配置完成後，進行測試

將監控主機關機，五分鐘後，LINE就會進行報警



【Zabbix測試】主機名稱: Line
發生時間: 2019.08.28 15:34:30
警示等級: Average
警示訊息: Zabbix agent on LINE is
unreachable for 5 minutes
警示項目: [agent.ping](#)
問題說明: Agent ping: Up (1)
當前狀態: PROBLEM: Up (1)
事件ID: 257

下午 3:35

出處： ([Linux](#)) [Zabbix LINE Notify 警報通知](#) | [工程師的江湖 - 點部落 \(dotblogs.com.tw\)](#)

學習相關連結

《网工程のPython之路》教学文章、视总 - 知乎 (zhihu.com)

smokeping install

```
timedatectl set-timezone Asia/Taipei
```

install docker

```
curl -fsSL https://get.docker.com | bash -s docker
```

run smokeping in docker

```
mkdir -p /home/monitor/smokeping/config
mkdir -p /home/monitor/smokeping/data
chown -R monitor /home/monitor/smokeping/

systemctl enable docker
systemctl start docker

docker pull linuxserver/smokeping
docker run -d \
--name=smokeping \
-e PUID=1000 \
-e PGID=1000 \
-e TZ=Asia/Taipei \
-p 9080:80 \
-v /home/monitor/smokeping/config:/config \
-v /home/monitor/smokeping/data:/data \
--restart unless-stopped \
linuxserver/smokeping
```

fix config

路 /home/monitor/smokeping/config/Targets

```
#!/bin/bash
docker rm -f smokeping

docker run -d \
--name=smokeping \
-e PUID=1000 \
-e PGID=1000 \
-e TZ=Asia/Taipei \
-p 9080:80 \
-v /home/monitor/smokeping/config:/config \
-v /home/monitor/smokeping/data:/data \
--restart unless-stopped \
linuxserver/smokeping
```

page

<http://localhost:9080/smokeping/?target=InternetSites>

<https://www.ssvip.net/971.html>

【DNS】台灣地區常用 DNS IP 整合表

台灣地區常用 DNS IP 整合表：

業者	主用 DNS IP	備用 / 區域性 DNS IP	備註說明
中華電信	168.95.1.1	168.95.192.1	全台通用
台灣大哥大	203.73.24.1	203.73.25.1、61.31.233.1	固網與行動使用者常見 IP，會依區域調整
遠傳電信 (SeedNet)	139.175.1.1	139.175.55.244、8.8.8.8 (Google DNS)、其他區域性如下：	官方資料來源 SeedNet
→ 北區	139.175.55.244	139.175.252.16	台北、桃園、新竹等
→ 中區	139.175.150.20	139.175.55.244	台中、彰化、南投等
→ 南區	139.175.10.20	139.175.55.244	高雄、台南、嘉義等
亞太電信	多沿用中華電信		建議手動指定 168.95.1.1
台固媒體	203.75.129.130	203.75.129.131	固定使用者常見 DNS

國際公共 DNS（可自由選擇）：

服務商	主用 DNS IP	備用 DNS IP	備註
Google DNS	8.8.8.8	8.8.4.4	全球穩定快速
Cloudflare	1.1.1.1	1.0.0.1	快速且注重隱私
Quad9	9.9.9.9	149.112.112.112	防惡意網站 DNS
OpenDNS	208.67.222.222	208.67.220.220	可選擇家長過濾功能