

Open SNMP server 的問題

- **NOTICE** 2019/11/27 網路協進會報告，自2020/02/11(二)起，比照 **open DNS** 的處理，若偵測為 **open SNMP server** 將自動阻斷其IP，請使用者務必修正問題，以免網路遭阻斷。阻斷處理，詳「[不當網路資訊](#)」
- 為幫助本校使用者防治 open SNMP server 的問題，2019/10/16 本頁面上線，以提供更多相關資料。
- 由於軟體及設備種類繁多，歡迎知悉某特定軟體或設備其修正方法者，能不吝提供資料，嘉惠眾人，詳：[資訊設備](#)
 - 若不會用到 SNMP 建議可直接關閉此服務。
 - 若要用 SNMP 請設定 **Access Control List** 限制內網存取，或將預設的 **community public** 改掉，以避免遭濫用。

問題概述

- Open SNMP server 指伺服器(或資訊設備)對外公開且不限使用對象提供 **SNMP** 服務，可能產生以下問題：
 1. 暴露於外界，容易被攻擊或平白損耗系統及網路資源
 2. 容易被外界利用，成為發動 **DDoS** 網路攻擊的一員
 3. 因系統資訊揭露，衍生入侵問題
- 關於利用 SNMP 的反射放大攻擊(reflection and amplification attack)請參閱此連結 [Reflections on reflection \(attacks\)](#)

偵測系統

NEW 為防治 open SNMP server 問題，協助處理校園內電腦或資訊設備，因設定不慎而可能遭攻擊者利用來發動網路攻擊，故本組建置 open SNMP server 偵測系統，並將偵測結果提供各單位網管，以便轉知其使用者參考[建議作法](#)來修正設定及自行檢測問題是否解決，藉以減少本校網路內 open SNMP server 的數量。

最近七天內偵測結果

- **NOTICE** 若已存在本清單的 IP 地址，至少需等待至隔日系統重新偵測，通過後時才會移除，故擬移出本清單者，請先用下方的「[即時檢測服務](#)」，檢查確認該 IP 地址已無問題後，隔日應可自清單中移除。

更新時間 Sat Apr 20 16:45:00 2024 Asia/Taipei

序號	單位	IP 位址	偵測時間	備註
總計 0 筆記錄				

即時檢測服務

NEW 為方便本校使用者自行檢測其電腦或網路設備是否具有 **open SNMP server** 的問題，特建置此即時的檢測服務，目前限由本校 IP 位址來進行檢測。(2019/10/02上線試用)

檢測 open SNMP server IP 位址: . . .

- **NOTICE** 檢測前請先確認目標 IP 位址的電腦或設備狀態為開機且網路連線正常，以免影響檢測結果。

檢測說明

- 採用 <http://opensnmpproject.org/> 的偵測方法，若有類似以下輸出結果，則表具有 **open SNMP server** 問題
 - 不應回覆 **SNMP** 查詢

```
Check open snmp for the target IP 140.114.XX.XX
Time: Wed Oct 2 09:40:32 2019

check_open_snmp: 140.114.XX.XX
check open snmp server with (140.114.XX.XX,,)

Command: /bin/snmpwalk -v 1 -c public 140.114.XX.XX .1.3.6.1.2.1.1

STDOUT: 6
  SNMPv2-MIB::sysDescr.0 = STRING: HP ETHERNET MULTI-
  ENVIRONMENT,ROM R.22.01,JETDIRECT,JD95,EEPROM R.24.06,CIDATE
  10/17/2002
  SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-
  SMI::enterprises.11.2.3.9.1
  DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (109520430) 12
  days, 16:13:24.30
  SNMPv2-MIB::sysContact.0 = STRING:
  SNMPv2-MIB::sysName.0 = STRING: NPI97XXXX
  SNMPv2-MIB::sysLocation.0 = STRING:
  SNMPv2-MIB::sysServices.0 = INTEGER: 64

STDERR: -1

Is 140.114.XX.XX an open snmp server?
ANSWER: YES for 140.114.XX.XX
```

- 若類似以下輸出結果，表不具有 **open SNMP server** 問題
 1. 無 **SNMP** 回應，若電腦已開且網路已通，則此機無問題。

```
Check open snmp for the target IP 140.114.63.252
Time: Wed Oct 2 09:45:36 2019

check_open_snmp: 140.114.63.252
check open snmp server with (140.114.63.252,,)

Command: /bin/snmpwalk -v 1 -c public 140.114.63.252
.1.3.6.1.2.1.1

STDOUT: -1

STDERR: 0
Timeout: No Response from 140.114.63.252
```

```
Is 140.114.63.252 an open snmp server?  
ANSWER: NO for 140.114.63.252
```

建議作法

- 若不會用到 SNMP 建議可直接關閉此服務。
- 若要用 SNMP 至少將預設的 **community public** 改掉，以避免遭濫用。

防火牆作法

- 以防火牆來限制 SNMP 查詢，預設攔阻 161/udp 的封包，再針對開放服務範圍的 IP 位址來開放服務，這種作法效益最好。
 - **NOTICE** 用外部閘道型防火牆來保護內部所有資訊設備的方法甚為簡便，但考慮到閘道型防火牆總有需 bypass 或下線的時候，所以平時最好還是將每部資訊設備本身的安全防護做好來。

SNMP 軟體

- 若不會用到 SNMP 建議可直接關閉此服務。
- 若要用 SNMP 至少將預設的 **community public** 改掉，以避免遭濫用。
 - 例如: [net-snmp 設定檔 snmpd.conf](#)，將以下預設值

```
rocommunity public
```

修改 public 為 xxxxxx (自訂不要外流)，並限定 140.114.63.0/24 才能連線。

```
rocommunity xxxxxx 140.114.63.0/24
```

資訊設備

NOTICE 有些資訊設備（如：網路印表機、無線網路閘道器、IP分享器、或路由器）本身可能具有 open SNMP server 問題，需適當調整設定或以防火牆來處理，由於資訊設備的類型繁多，若您知悉某裝置該如何處理，歡迎提供設備廠牌、型號、軟(韌)體版本、及其設定方式的畫面，寄至 mucheng@cc.nthu.edu.tw 以利製成以下網頁，嘉惠眾人，格式及文字可參考以下作法，謝謝!

Apple Airport routers

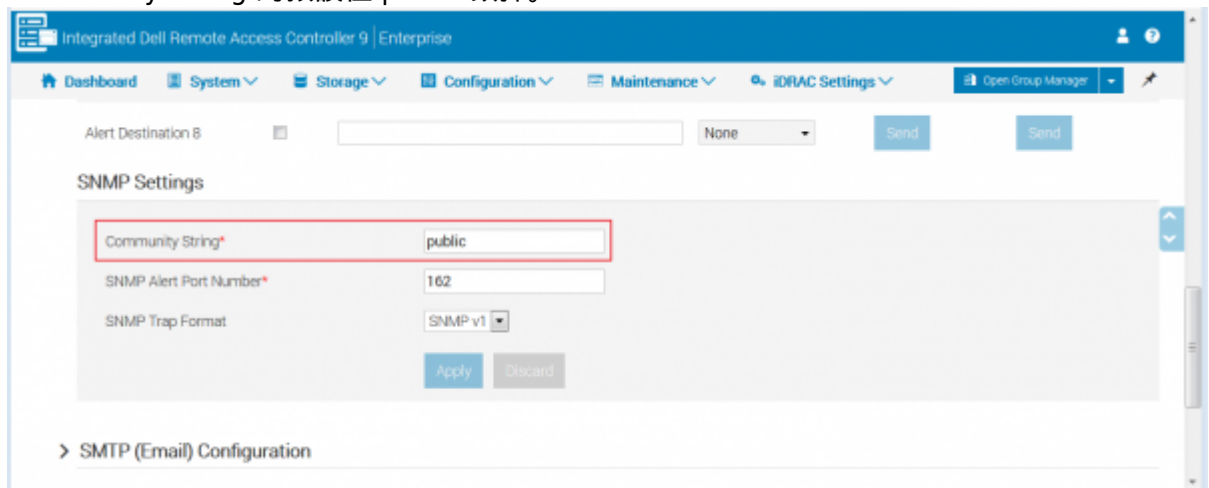
- [How to disable SNMP on Apple Airport routers](#)

DELL 遠端存取控制器

- **NEW** DELL 伺服器的 iDRAC 9 (Integrated Dell Remote Access Controller 9) 遠端存取控制器：避免

open SNMP resolver 問題之設定方式請參考下圖(2019/10/18)。

- 進入 Configuration > System Settings > SNMP Traps Configuration > SNMP Settings 將 Community String 的預設值 public 改掉。



Extreme 交換器

- **NEW** Extreme 交換器：避免 open SNMP resolver 問題之設定方式請參考以下，本資料感謝工科系何孟軒先生提供(2022/10/21)
 - 參考

<https://www.plixer.com/blog/extreme-networks-enabling-and-disabling-snmpv1-snmpv2-and-snmpv3/>

1. 以下三行新設定一個 SNMPv3 的身分

```
configure SNMPv3 add user <user> authentication md5 <authpassword>
priv des <privpassword>
configure SNMPv3 add group <group> user <user> sec-model usm
configure SNMPv3 add access <group> sec-model usm sec-level priv
read-view defaultAdminView write-view defaultAdminView notify-view
defaultAdminView
```

2. 接著三行取消原本預設的身分跟群組

```
disable SNMP access SNMP-v1v2c
disable SNMPv3 default-user
disable SNMPv3 default-group
```

```
Press the <tab> or '?' key at any time for completions.
Remember to save your configuration changes.

X430-24t.1 # configure SNMPv3 add user [redacted] authentication md5 [redacted]
65 privacy des [redacted]
* X430-24t.2 # configure SNMPv3 add group [redacted] user [redacted] sec-model usm
* X430-24t.3 # configure SNMPv3 add access [redacted] sec-model usm sec-level priv
read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminV
iew
* X430-24t.4 # disable SNMP access SNMP-v1v2c
* X430-24t.5 # disable SNMPv3 default-user
* X430-24t.6 # disable SNMPv3 default-group
```

3. 驗證是否成功

show management

```
* X430-24t.7 # show management
CLI idle timeout           : Enabled (20 minutes)
CLI max number of login attempts : 3
CLI max number of sessions  : 8
CLI paging                 : Enabled (this session only)
CLI space-completion       : Disabled (this session only)
CLI configuration logging   : Disabled
CLI scripting               : Disabled (this session only)
CLI scripting error mode    : Ignore-Error (this session only)
CLI persistent mode        : Persistent (this session only)
CLI prompting               : Disabled (this session only)
Telnet access               : Enabled (tcp port 23 vr all)
                           : Access Profile : not set
SSH Access                  : ssh module not loaded.
Web access                  : Disabled (tcp port 80)
                           : Access Profile : not set
Total Read Only Communities : 1
Total Read Write Communities : 1
RMON                        : Disabled
SNMP access                 : v1,v2c Disabled, v3 Enabled,
                           : v3DefaultGroup Disabled
                           : Access Profile : not set
SNMP Traps                  : Enabled
SNMP v1/v2c TrapReceivers   : None
```

HP 網路印表機

- **NEW** HP LaserJet M506 網路印表機：避免 open SNMP resolver 問題之設定方式請參考下圖，本資料感謝醫環系黃琤雯小姐提供(2019/10/25)
 - 進入 網路 > 網路設定 > SNMP 不要「啟動」SNMPv1/v2 及 SNMPv3

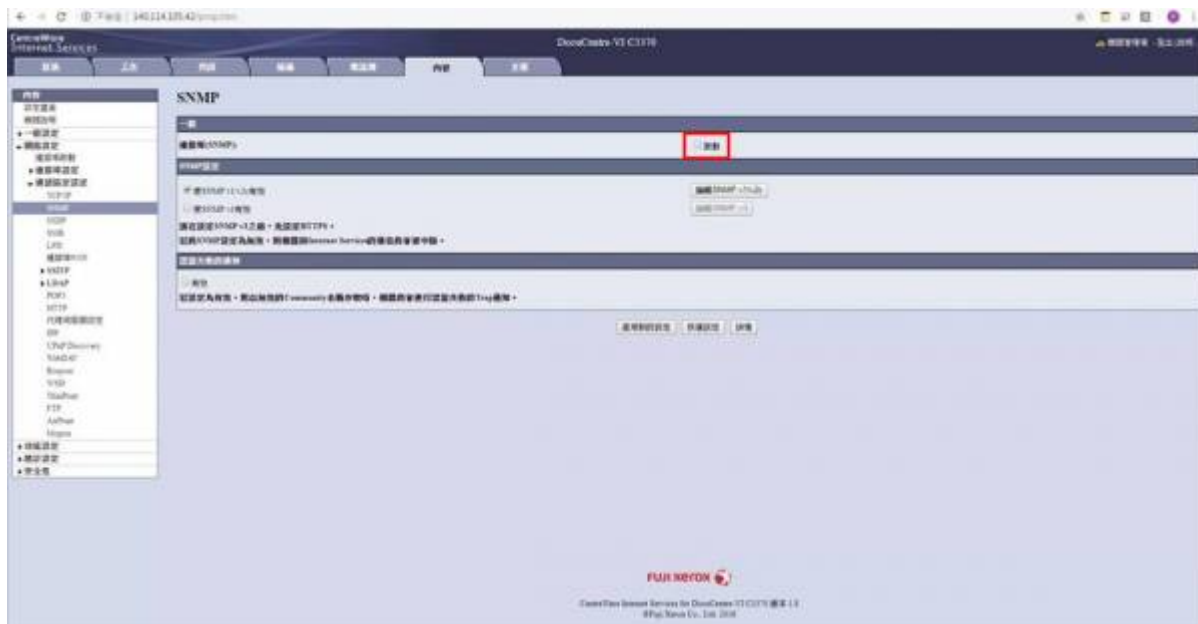




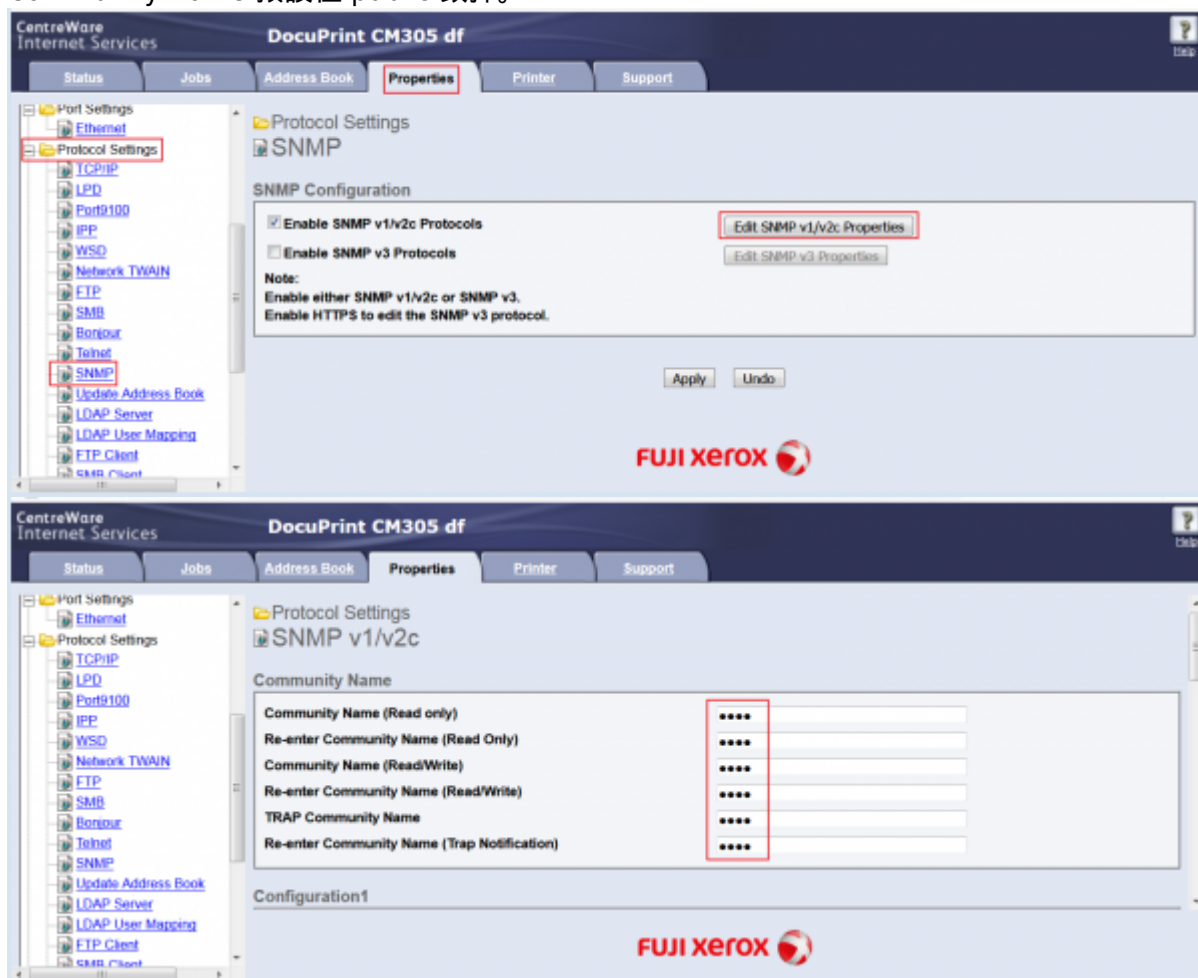
Fuji Xerox 網路印表機

- NEW** Fuji Xerox DocuCentre-VI C3370 網路印表機：避免 open SNMP resolver 問題之設定方式請參考下圖，本資料感謝醫環系黃琤雯小姐提供(2019/10/25)
 - 進入 內容 > 通訊協定設定 > SNMP 不要「啟動」。





- **NEW** Fuji Xerox DocuPrint CM305 df 網路印表機：避免 open SNMP resolver 問題之設定方式請參考下圖(2019/10/18)。
 - 進入 Properties > Protocol Settings > SNMP 再 Edit SNMP properties 將所有的 Community Name 預設值 public 改掉。



Ricoh 網路印表機

- **NEW** Ricoh SP C252SF 網路印表機：避免 open SNMP resolver 問題之設定方式請參考下圖，本資料

感謝工科系何孟軒先生提供(2020/02/10)

- 進入 網路設定 > SNMP > 設定 SNMP 無效」。

RICOH SP C252SF Web image monitor

首頁
系統設定
單鍵撥號目的地
掃描目的地
傳真快速撥號目的地
特殊傳送者
限制可用功能
網路設定
IPsec設定
列印清單/報告
管理員工具

網路設定

網路狀態 IPv6設置 網路應用程式 DNS 自動電子郵件通知 **SNMP**

SNMP

■ SNMP : ☐ 有效 ☒ 無效

Trap

■ 目標Trap : ☐ 有效 ☒ 無效

■ SNMP管理主機1 :

■ SNMP管理主機2 :

社群

■ Get社群 :

■ Trap社群 :

系統

■ 位置 :

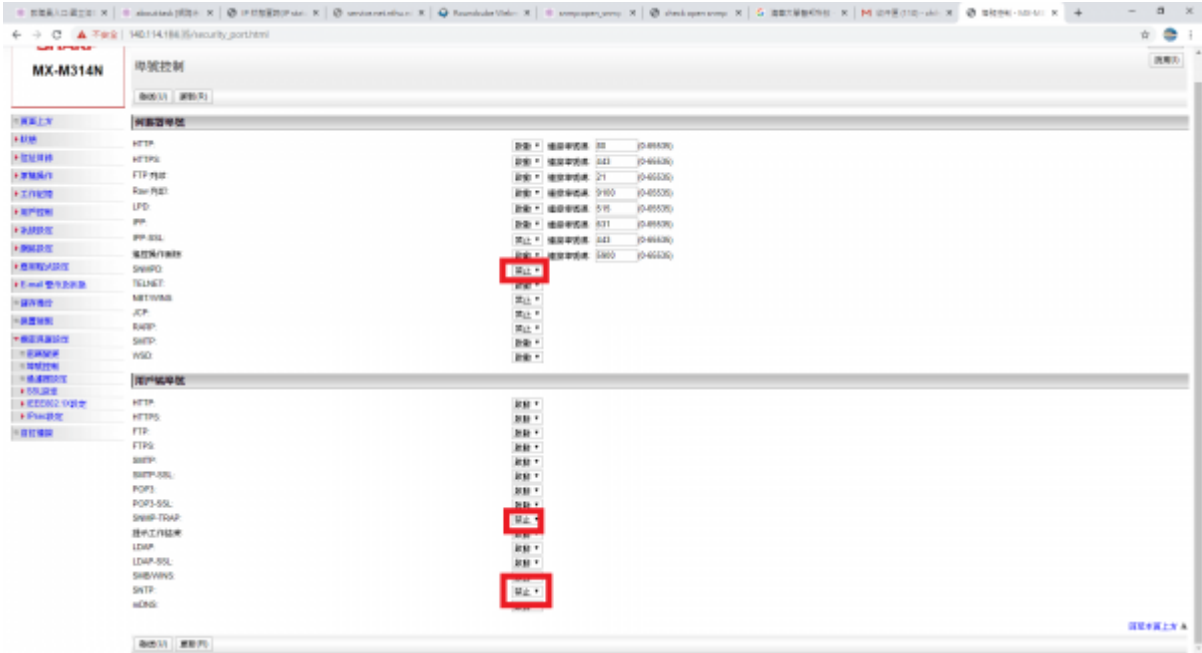
■ 聯絡 :

請輸入管理員密碼。

確定 取消

Sharp 網路印表機

- **NEW** Sharp MX-M314N 網路印表機：避免 open SNMP resolver 問題之設定方式請參考下圖，本資料感謝體育室鄧智予先生提供(2020/02/26)
 - 進入 埠號控制 > 將「伺服器埠號」的 SNMPD 設定為「禁止」。



KYOCERA

- KYOCERA 避免 open SNMP resolver 問題之設定方式請參考下圖，本資料感謝工科系何孟軒先生提供 (2021/06/25)
 - 進入 網路 > 網路設定 > 協定 > 其他協定，不要「啟動」SNMPv1/v2c 及 SNMPv3



其他協定

*SNMPv1/v2c :

☐ 開啟 ☒ 關閉

注意：
有關詳細設定，請按一下這裏， [SNMP 設定](#)

*SNMPv3 :

☐ 開啟 ☒ 關閉

注意：
有關詳細設定，請按一下這裏， [SNMP 設定](#)

參考資料

- [Open SNMP Project](#)

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/snmp:open_snmp

Last update: **2022/10/21 10:36**

