Zyxel 設備自動偵測與識別實作指南 (Debian 13)

1. 專案概述

本專案旨在解決網管人員在 Linux (Debian 13) 環境下，無法使用原廠 Zyxel One Network (ZON) Utility 的限制。透過分析 Zyxel Discovery Protocol (ZDP) 協定，我們開發了客製化的 Nmap Scripting Engine (NSE) 腳本，實現跨平台的 Layer 2 設備偵測、資產盤點與 IP 識別功能。

2. 技術原理：ZDP 協定深度解析

本次實作基於對封包行為 (Traffic Analysis) 的逆向工程，核心發現如下：

2.1 通訊層級與特徵

- **運作層級**：Data Link Layer (Layer 2)，不依賴 IP 路由，可發現無 IP 或 IP 設定錯誤的設備。
- **EtherType**：`0xc1c1` (Zyxel 專有協定)。
- **目標 MAC**：`01:a0:c5:11:11:11` (特定多播群組)。

2.2 探測機制 (Probe Mechanism)

ZDP 採用「請求/回應 (Request/Response)」模式。

- **關鍵發現**：探測封包必須包含 **Request List**。若封包內容為空或僅有標頭，設備僅會回傳 OpCode `00ff` 的簡易回應 (僅含 MAC)。
- **有效 Payload 結構**：
    1. **ZDP Header**: `00 01 80 00` (Ver 1, Request)
    2. **Source MAC**: 發送者的 MAC 位址。
    3. **Transaction ID**: 識別該次查詢的 ID。
    4. **Request List**: 明確指定欲查詢的欄位 Tag (如 `02 00 03 00 04 00...`)。

2.3 資訊解碼 (TLV Parsing)

設備回應採用 TLV (Type-Length-Value) 格式，本腳本解析以下關鍵 Tag：

- **Tag `0x03` / Header**: MAC Address (硬體位址)
- **Tag `0x04`**: Model Name (設備型號，如 XS3800-28)
- **Tag `0x05`**: Firmware Version (韌體版本)
- **Tag `0x06`**: System Name (系統名稱，用於識別設備用途)
- **Tag `0x07`**: IPv4 Address (主要的管理 IP)
- **Tag `0x10`**: Management IP Info (其他 IP 資訊)

3. 環境準備 (Debian 13)

在 Debian 13 (Trixie) 上，您僅需安裝 Nmap 即可執行此腳本。

3.1 安裝套件

開啟終端機並執行以下指令：

```
# 更新套件庫
sudo apt update

# 安裝 Nmap (包含 nmap, nping, nse 引擎)
sudo apt install nmap -y

# (選用) 安裝 tcpdump 用於除錯封包
sudo apt install tcpdump -y
```

3.2 確認網路介面

執行 `ip a` 確認您要掃描的實體網卡名稱 (例如 `eth0`, `enp3s0` 等)。

- **注意**：由於 ZDP 是 Layer 2 廣播協定，掃描僅在**同一個廣播網域 (Broadcast Domain)** 內有效。若設備位於不同 VLAN，需將網卡接入該 VLAN。

4. 腳本部署

將開發完成的腳本儲存為 `zyxel-discover.nse`。

核心功能亮點

1. **Raw Packet Injection**：利用 Nmap 的 `dnet` 函式庫發送自定義 EtherType `0xc1c1` 封包。
2. **Smart Parsing**：自動處理不同設備回傳的封包格式差異 (完整回應 vs 簡易回應)。
3. **IP Sorting**：輸出結果依據 IP 位址數值排序，方便閱讀。
4. **Flat Output**：產生 Tab 分隔的清單格式，易於複製到 Excel 或資料庫。

5. 執行與操作指南

5.1 基本掃描指令

使用 `sudo` 權限執行 (發送原始封包所需)，並透過 `-e` 指定介面。

```
# 語法：sudo nmap --script <腳本路徑> -e <介面名稱>
sudo nmap --script ./zyxel-discover.nse -e enp5s0
```

5.2 進階除錯模式

若掃描無結果，可加上 `-d` (Debug) 參數查看詳細的封包收發流程。

```
sudo nmap -d --script ./zyxel-discover.nse -e enp5s0
```

5.3 預期輸出結果

腳本將輸出如下格式的資訊列表：

```
Pre-scan script results:
| zyxel-discover:
| Model | Firmware Version | MAC Address | IP Address | System Name
| GS1900-8 | V2.90(AAHH.0) | 10/24/2024 | 50-E0-39-F7-9F-47 | 163.26.171.239 |
GS1900-8-04
| GS1900-8 | V2.90(AAHH.1) | 03/04/2025 | 5C-6A-80-FF-C5-6B | 163.26.171.240 |
Switch-Lab-01
| ...
| Unknown Device| - | F4-4D-5C-98-7A-57 | - | -
```

6. 常見問題排除 (Troubleshooting)

問題現象	可能原因	解決方案
No Zyxel devices found	1. 介面指定錯誤 2. 該網段無 Zyxel 設備 3. 防火牆阻擋	1. 檢查 `ip a` 確認介面 2. 確認設備是否在同一 VLAN 3. 檢查 iptables 是否阻擋 `0xc1c1`
Model 顯示 Unknown	設備回傳了回應，但缺少 Tag 0x04	腳本已設計容錯機制，會顯示 MAC 以供識別。這可能是極舊款設備或非標準 ZDP 實作。
Operation not permitted	未使用 root 權限	請務必在指令前加上 `sudo`。