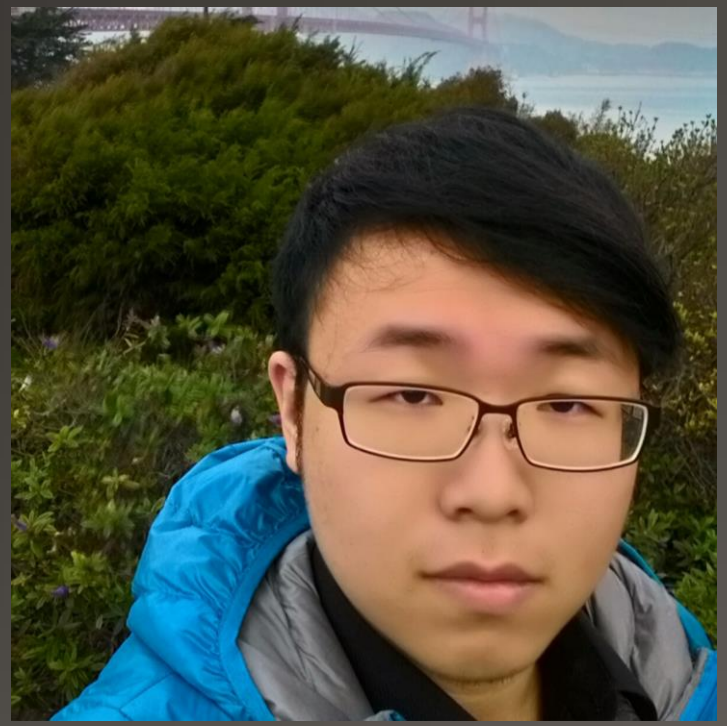

JohnThunder

# 打造自己的綿羊牆

# 自我介紹



- 姜尚德 **aka John Thunder**

- 高應大-資訊工程系-大三
- 網路鑑識 愛好者
- **UCCU** 戰隊核心成員
- 微軟實習生-**RDAA**

- 聯絡資訊：
  **John@johnthunder.one**

# 前言

# 校園宣傳資安

那就做個綿羊牆好了！

# 基本設施

# 綿羊牆所需要素

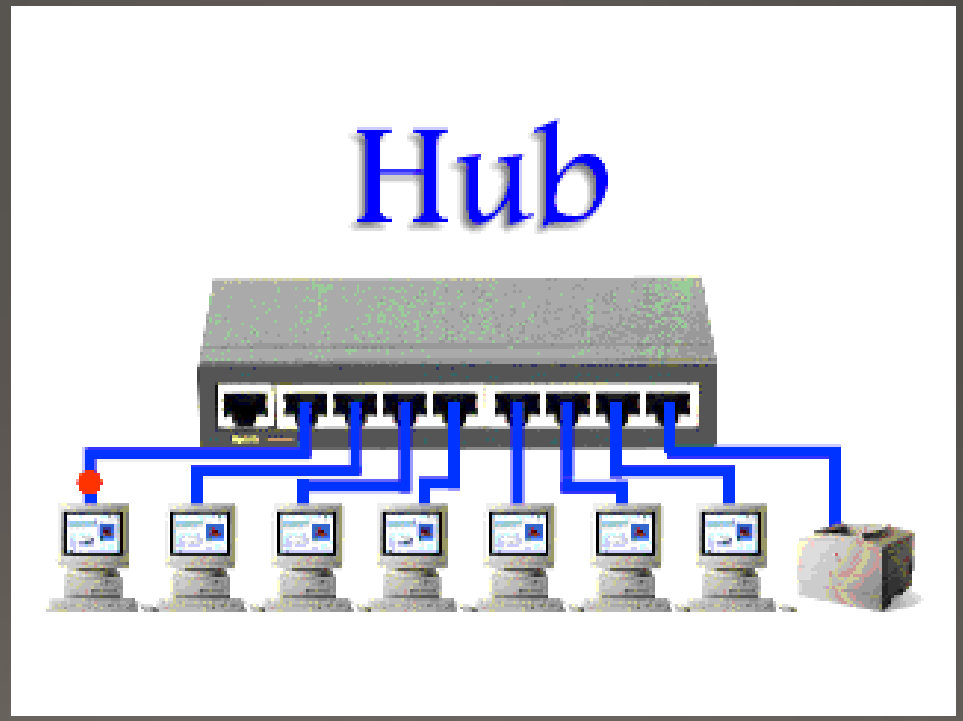
- 網路封包
  - 想盡辦法獲得其他電腦的網路封包
- 封包分析的程式
  - 分析封包未加密的帳號密碼
  - 顯示在綿羊牆的網頁上

# Network Sniffing

- 有線網路
  - **SPAN**
  - **LAN TAP**
  - **Network Hub**
- 無線網路
  - **Wireless Sniff**

# Network Hub

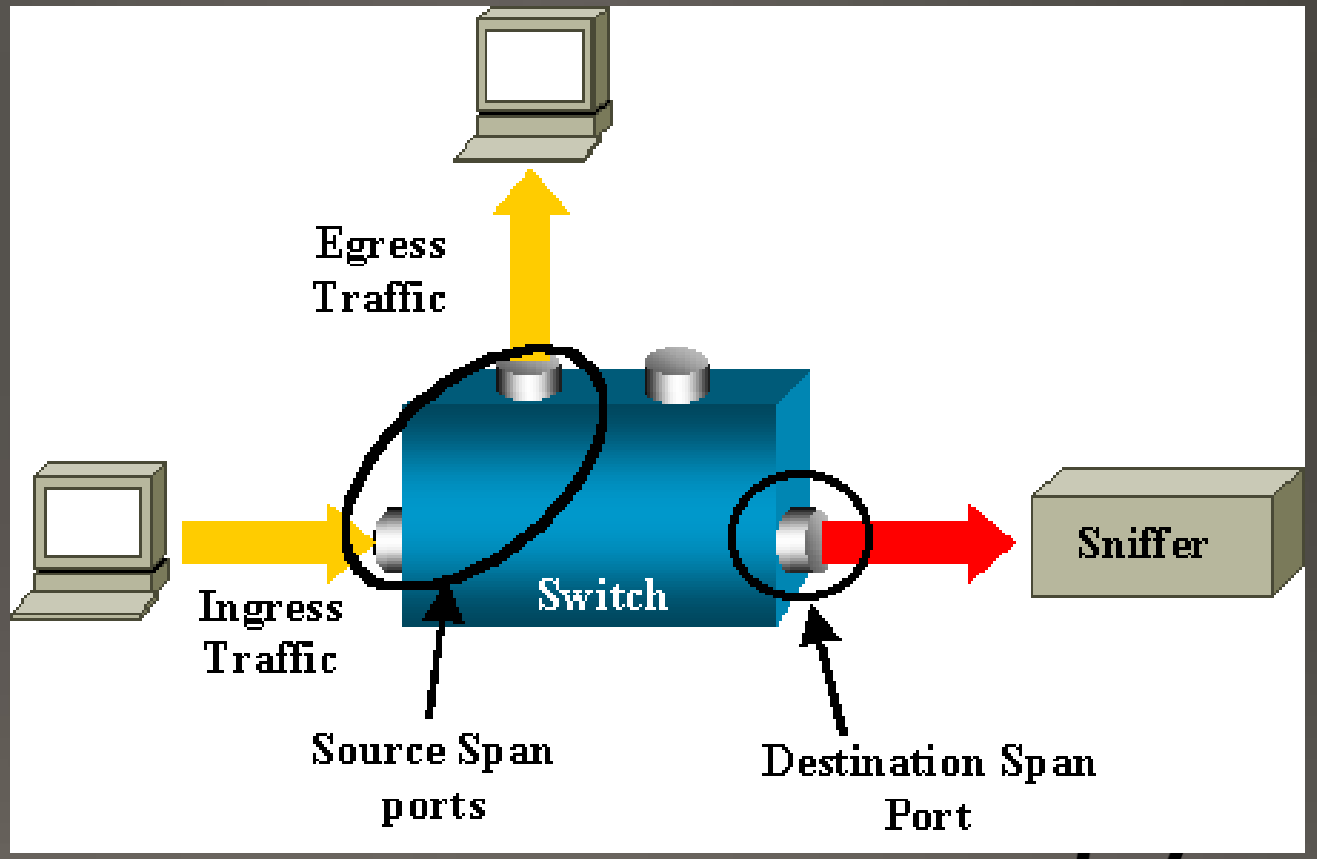
- 優勢
  - 便宜、簡單擴充
- 劣勢
  - 沒有**Gigabit** 的解決方案
  - 降低線路一半的頻寬
  - 潛在的網路故障點




**http://www.directsystems.com/support/diff_h**

# SPAN

- 優勢
  - 不須額外設備
  - 可監控多條線路流量
- 劣勢
  - 流量太大會導致超載、丟包
  - **CPU**工作量加大，**switch**效能降低
  - 不精確的時間標籤
  - **OSI Layer 1**、**2**的錯誤封包無法得知

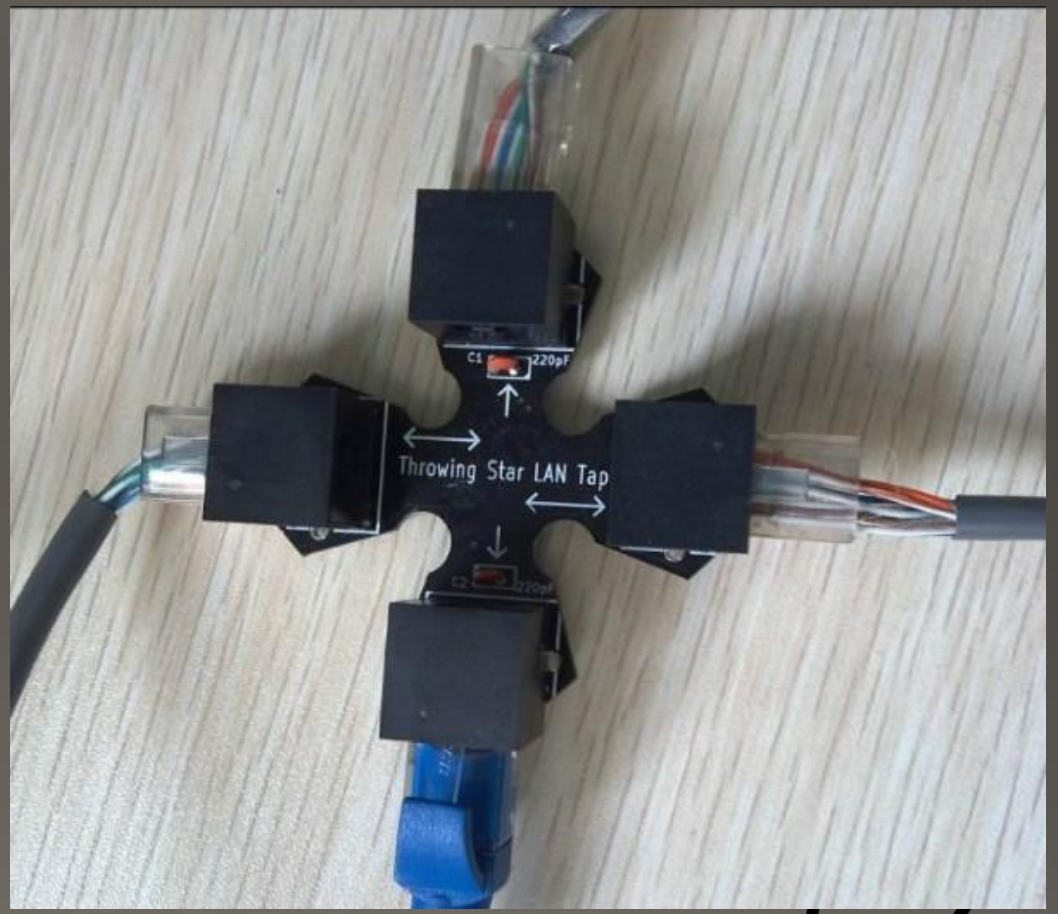



http://www.cisco.com/c/dam/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41d.gif

# LAN TAP

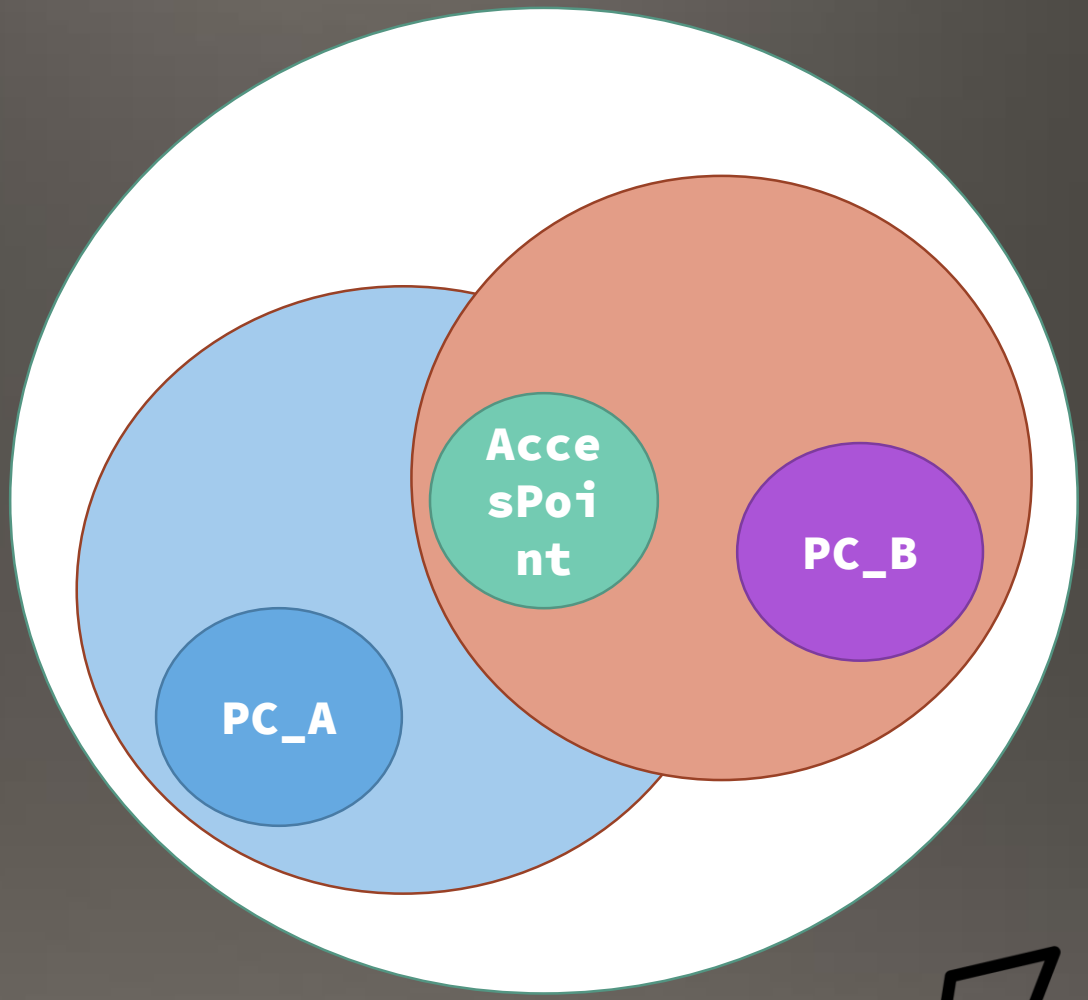
- 優勢
  - 不會丟包
  - 可監測到不規則的資料包，方便於故障排查
  - 沒有延遲和時間標籤錯誤。
  - 一次安裝

- 劣勢
  - 需額外花費購買分路器**TAP**，很貴，還佔用機架空間
  - 一次只能看一條線路。



# Wireless Sniff

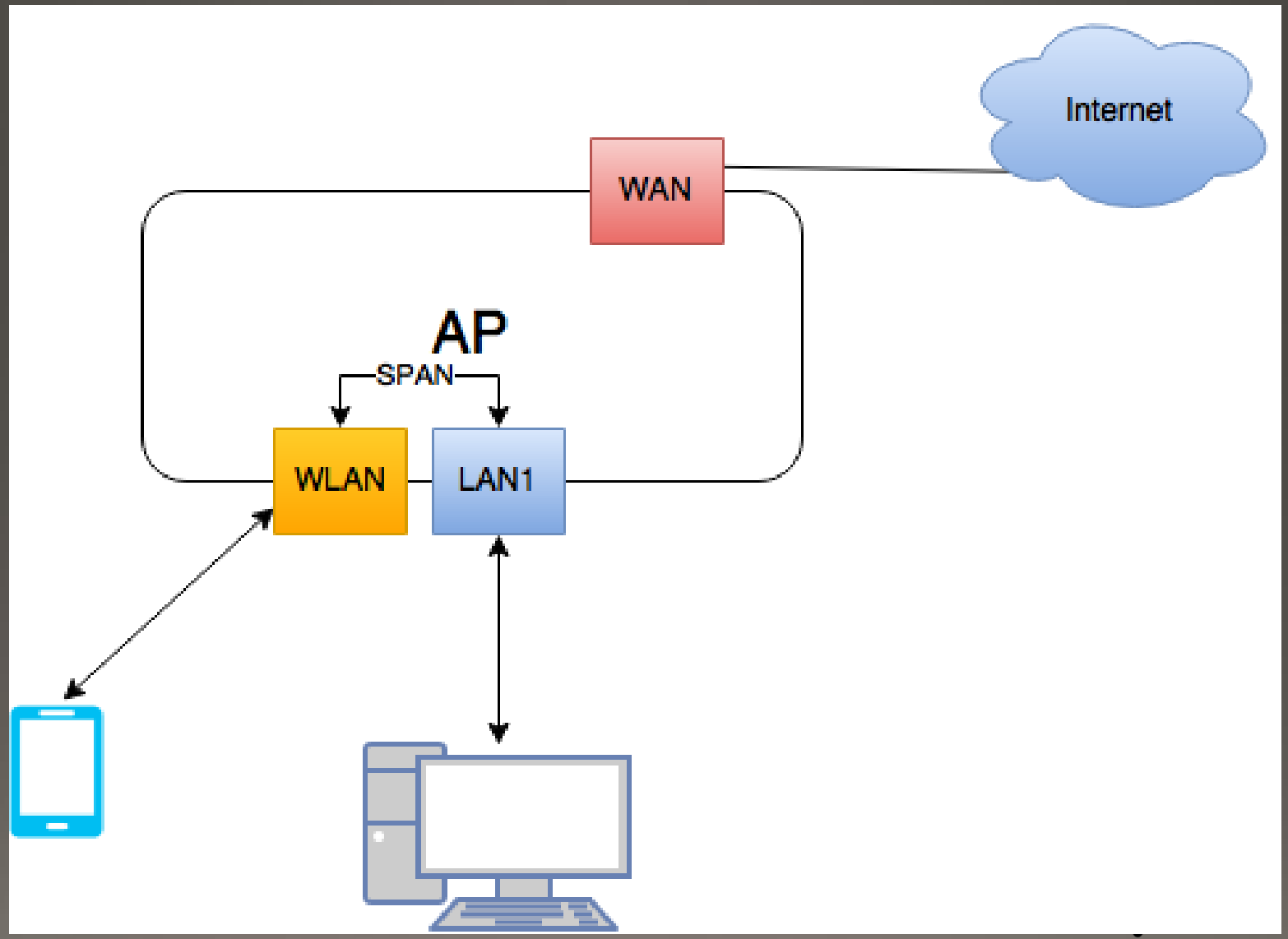
- 優勢
  - 可以同時監聽多個無線網路頻道
- 劣勢
  - 需要無線網路的密碼
  - 許多開源綿羊牆、分析器不支援解析**802.11**封包內容




# 綿羊牆架構

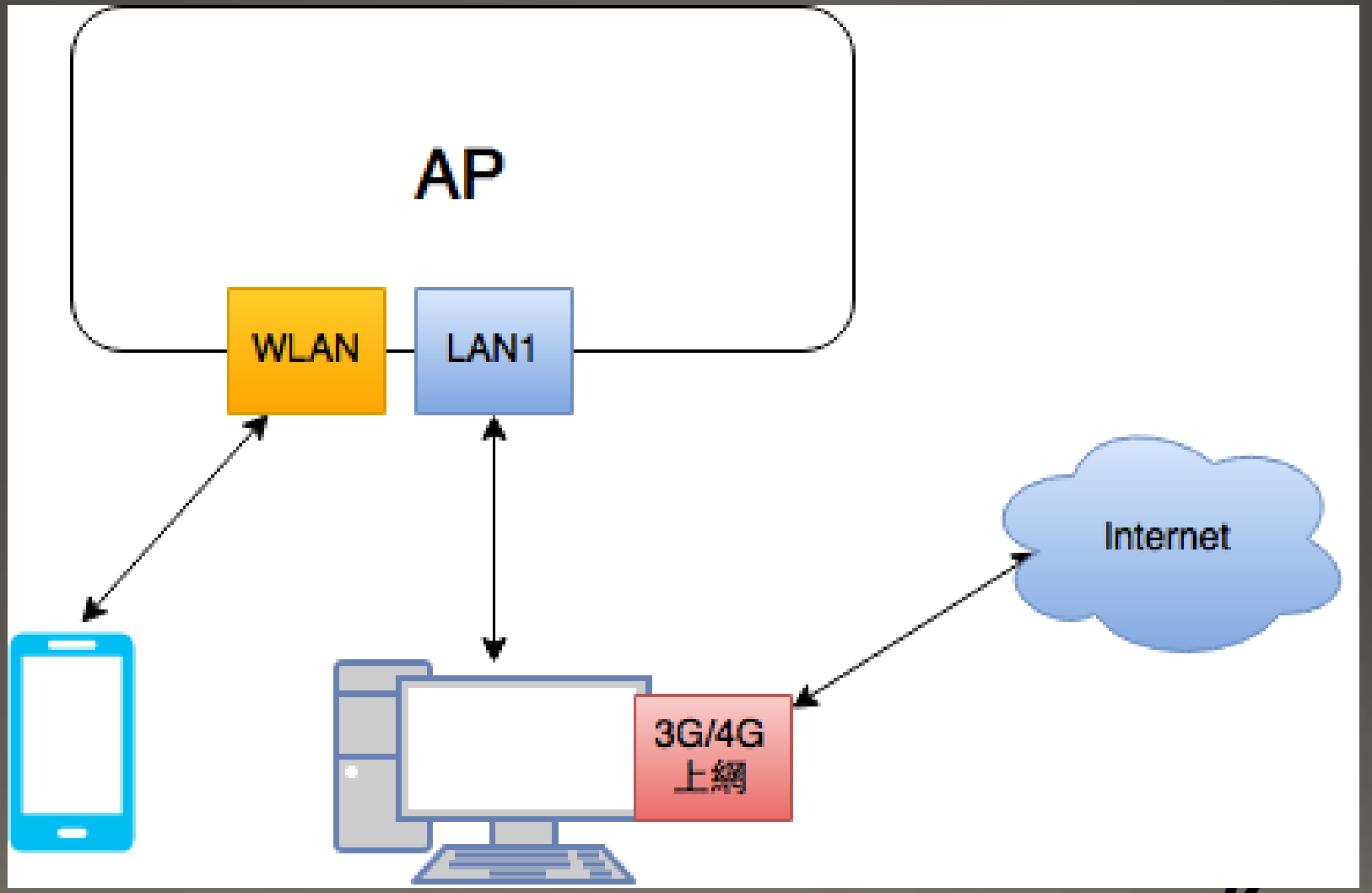
# 方法-1

- 情況：
  - 需能控制**AP**設定
- 優點：
  - 佈置簡單
- 缺點：
  - **AP**可能不支援**SPAN**



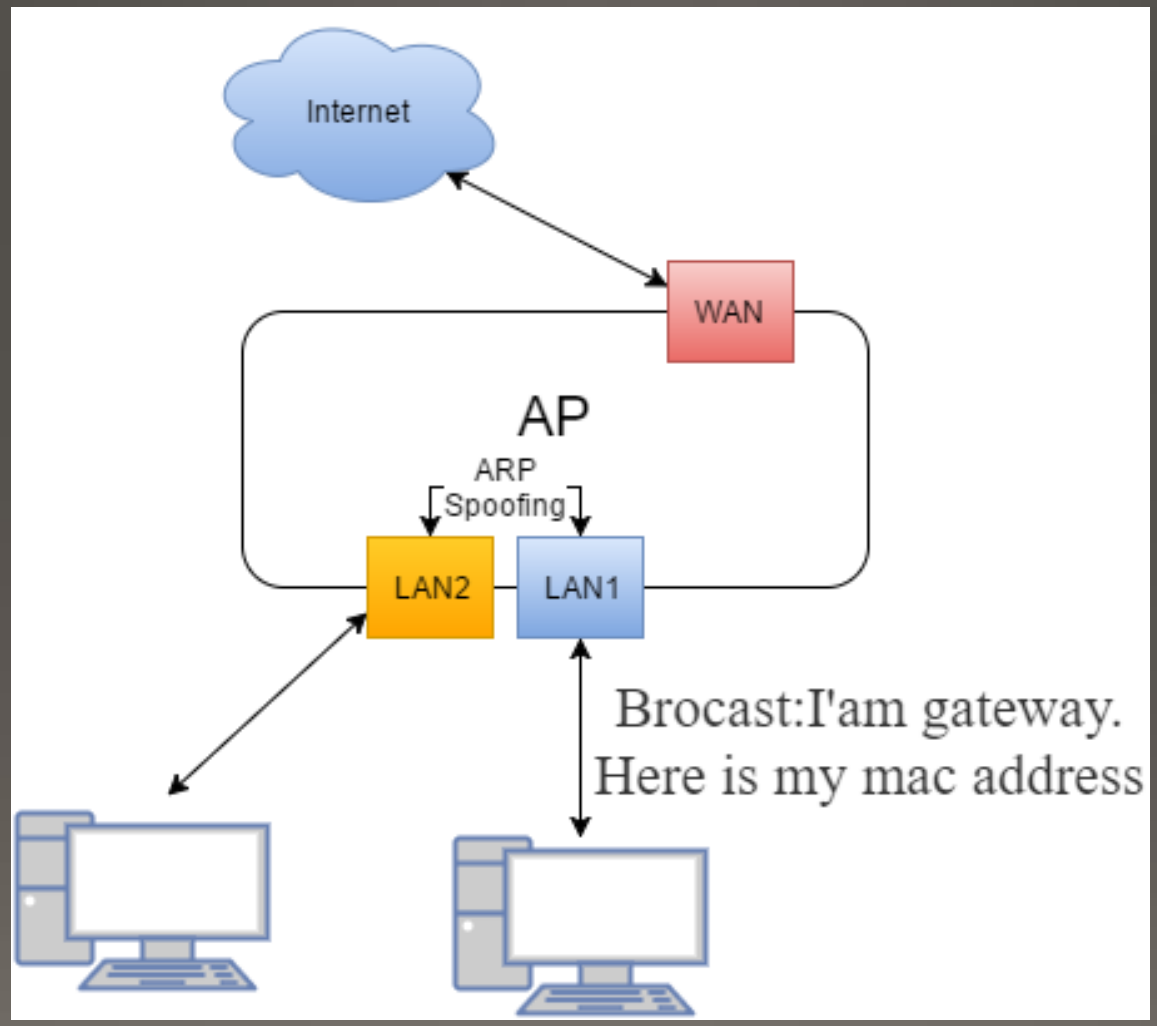
# 方法-2

- 情況：
  - 需能控制**AP**設定
- 優點：
  - 設定不複雜
  - 不被設備功能侷限
- 缺點：
  - 分析器需兩張**NIC**



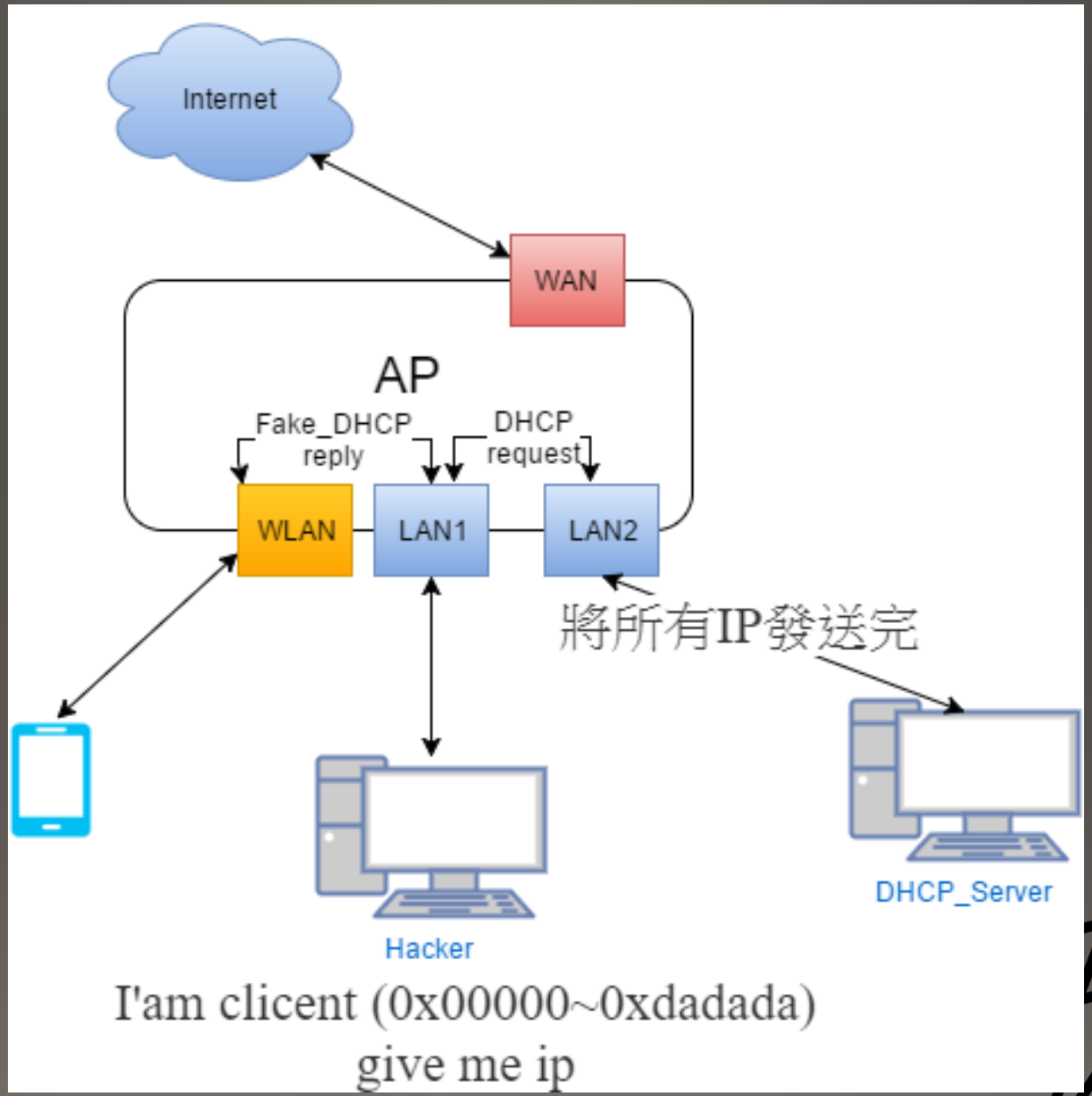
# 方法-3(ARP Spoofing )

- 情況：
  - 沒有**AP**控制權
- 優點：
  - 可輕鬆達到目標
- 缺點：
  - 設備可能有防止 **ARP Spoofing**



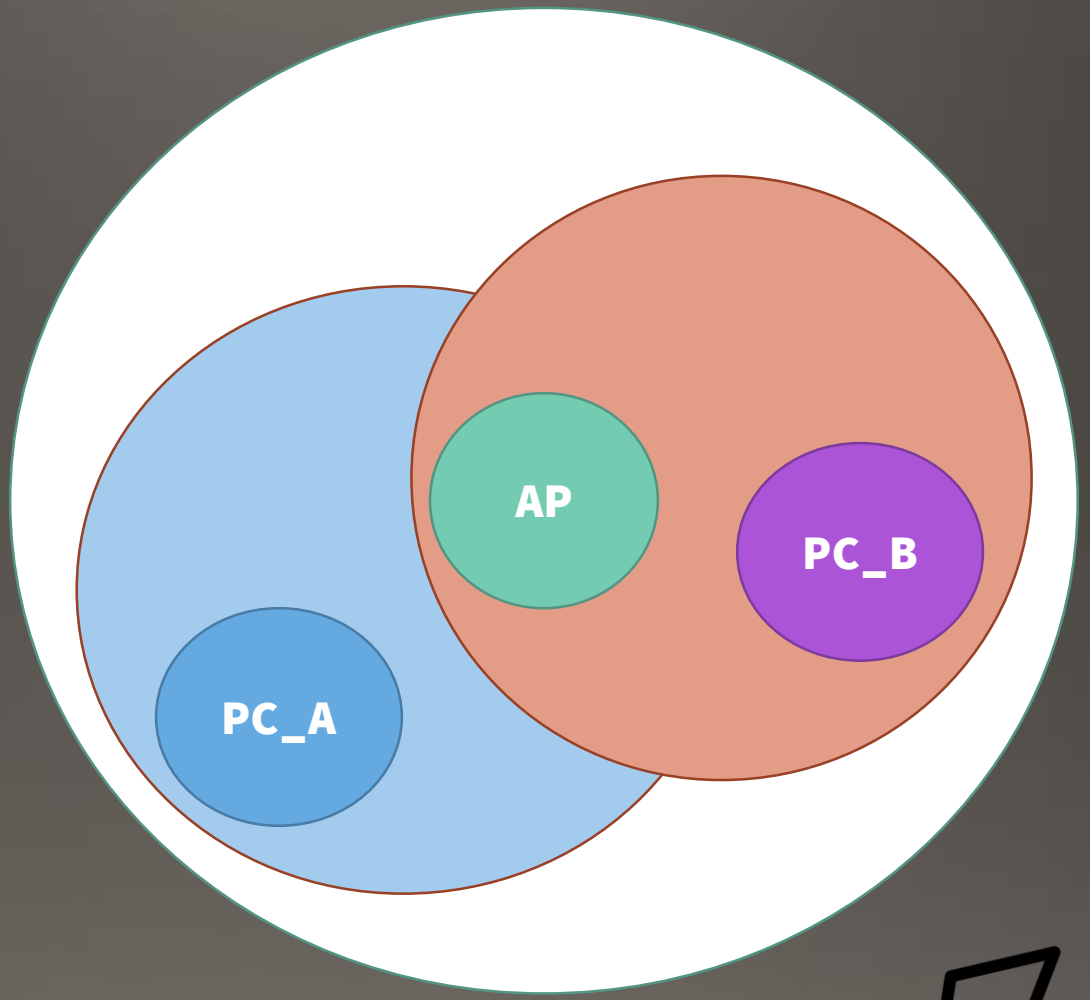
# 方法-4 (DHCP Attack )

- 情況：
  - 沒有**AP**控制權
- 優點：
  - 不用**ARP Spoofing**也可以攻擊
- 缺點：
  - 需要先癱瘓**DHCP Server**
  - 需自建**DHCP Server**



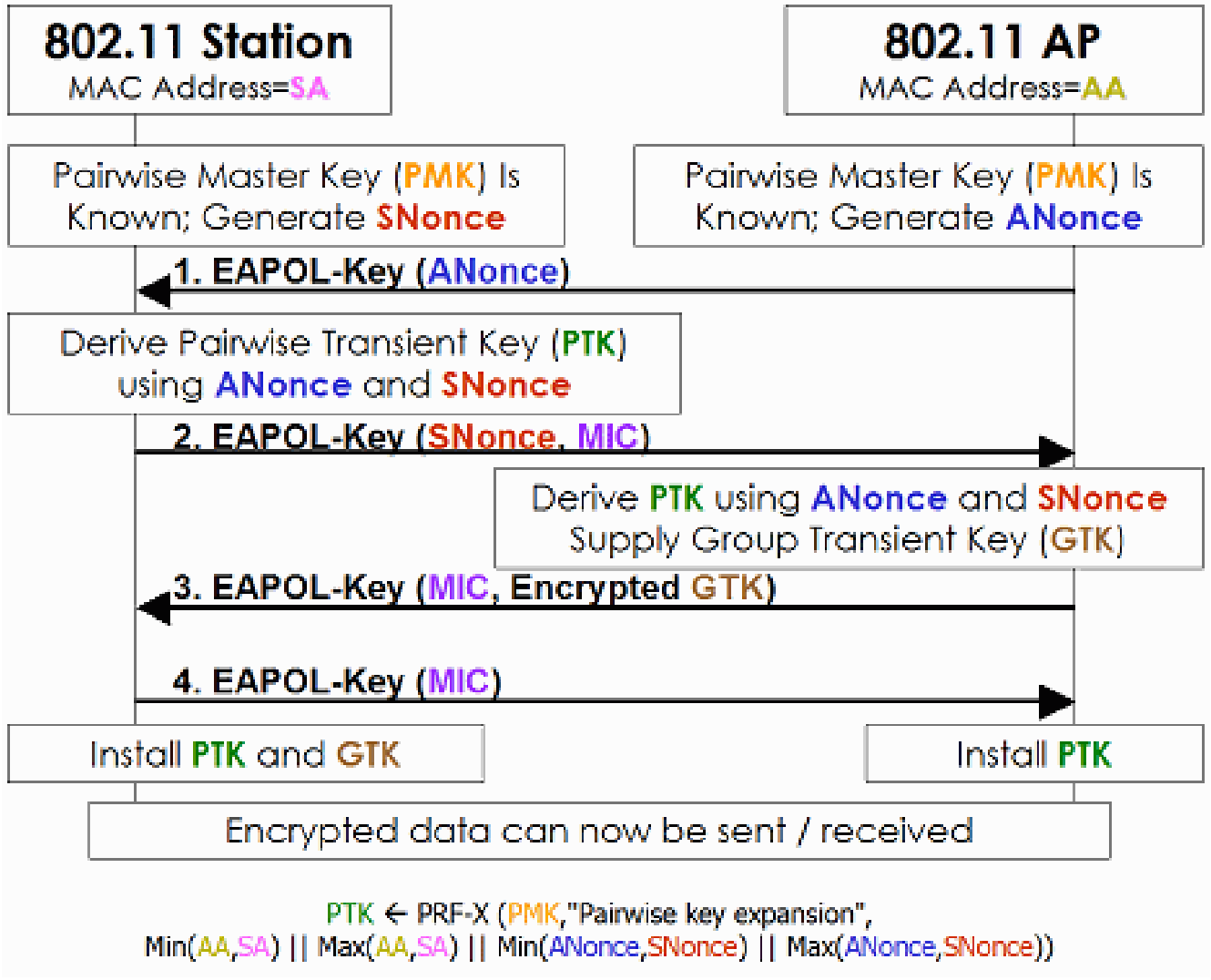
# 方法-5
# 側錄無線封包

- 優點：
  - 不受到設備限制
  - 輕鬆獲取封包
- 缺點：
  - 只能接收到所屬訊號區的封包
  - 只有無線網路的資訊
  - 特定無線網卡限制**(monitor mode)**



# WPA 四向交握

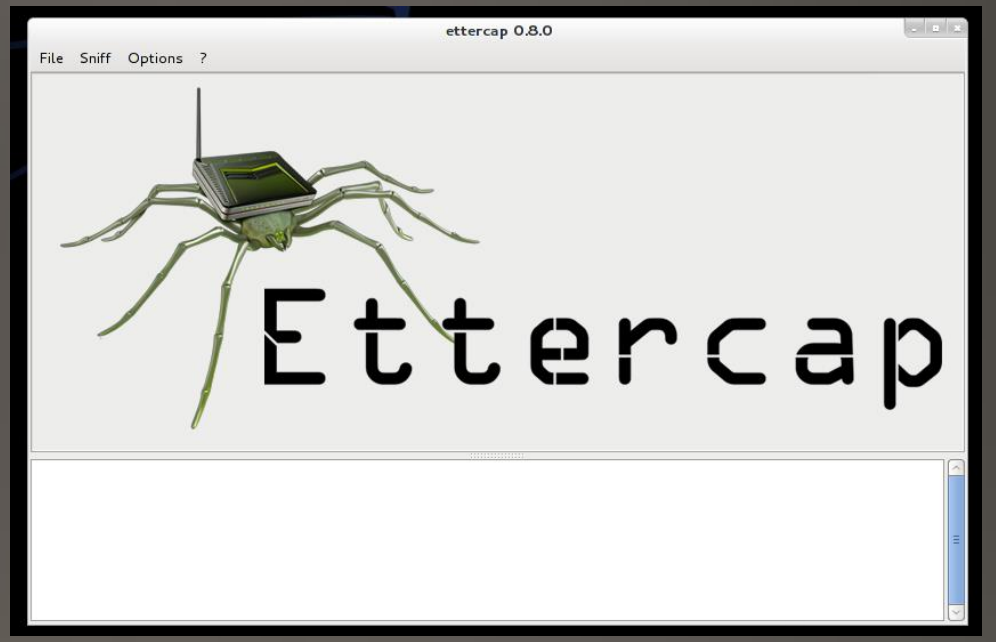
- 目的
  - **AP**證明自己的身份
  - 產生**traffic**用的**encryption key**



# 帳密獲取

# Ettercap

- **MITM** 的攻擊整合工具
  - **5種Sniffing**的模式
  - **Arp spoofing**
  - **Passive os fingerprinting**
- 不需要**libpcap**、**libnet** 常用的**lib**支援
- 網路上有許多以**Ettercap** 輸出**Log**來分析進而做出的綿羊牆
- 綿羊牆範例：**https://goo.gl/lPzosx**



# 用Python 自己架

- 利用**Scapy**
  - 抓包(利用**tcpdump**)
  - 分析協定
  - 分析**payload**

- 常用帳號密碼欄位
  - **Ex:'log','login', 'wpname', 'ahd_username', 'unickname', 'nickname'….**
  - **Ex:'ahd_password', 'pass', 'password', '_password', 'passwd'…**

# Scapy-分析協定

- 已知有些協定帳密固定欄位
  - **IRC 、POP、IMAP、NTLM…**
- 未知協定猜測是**HTTP Packet**去解析
  - **HTTP**的時代，就算不是走**80**、**443**不代表他就不是**HTTP** 封包

# Demo 無線側錄


192.168.67.133:8080
Search
你的網路安全嗎？
User
Password
Target site
1*3
1*3
69.32.182.86:80
d*b
w*f
69.32.182.86:80
U**U
U**U
140.127.113.12:80
Site
Method
Source IP
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
demo.opencart.com
GET
192.168.67.133
fonts.googleapis.com
GET
192.168.67.133
fonts.googleapis.com
GET
192.168.67.133

# 還可以做更多有趣的功能

- **MAC address vendor lookup**
  - 猜測使用者上網的裝置
- 學號對應姓名
  - 利用 合法的方法將學校對應登入符號顯示姓名
- 結合**OSINT** 顯示其它結果
  - 可以得出更多有趣的資訊


Q&A