10 使用 Wireshark 分析 Radius-EAP 的封包.docx

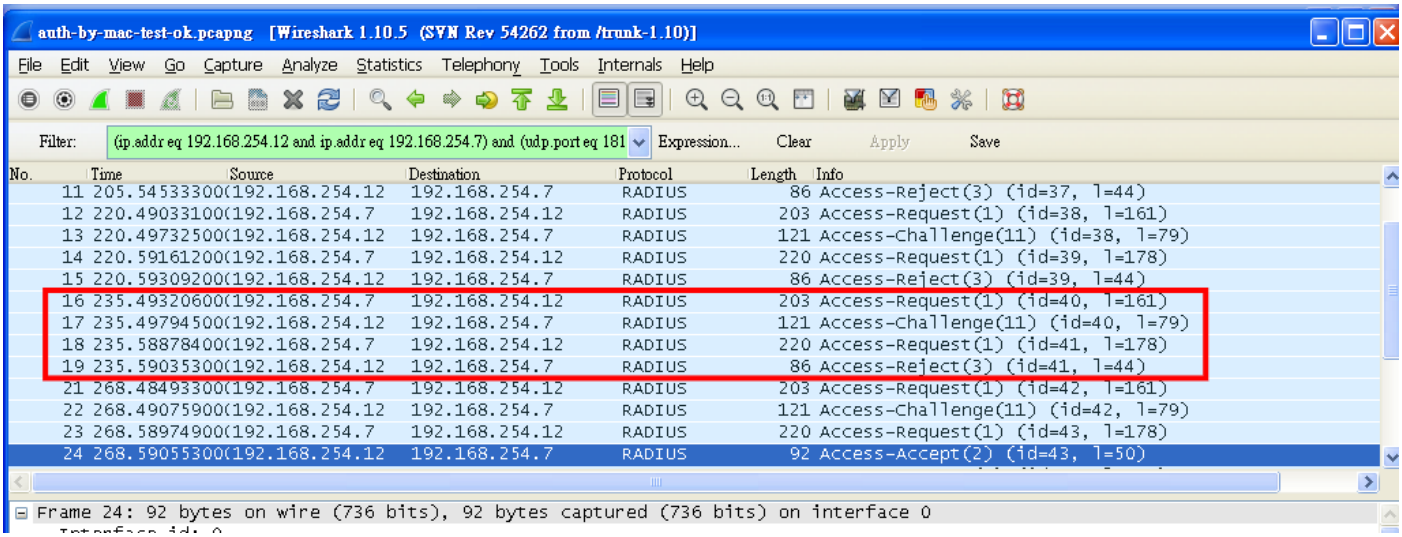
Radius Server 很多設備會使用到的驗證方式
一般是設備設定 Radius Server IP 和 Port 以及 Script 共用密碼
之後就是設備帶 EAP 的封包往 Radius Server 做驗證了

802.1x
EAP 的封包區分
EAP MD5
EAP TLS
還有 PEAP
EAP-MSCHAP
EAP-MSCHAPv2
….
格式挺多的
我們示範
EAP MD5-Challenge

這個測試架構我們是驗證 VigorSwitch G2260 使用 802.1x 做 Auth by MAC Adddress
當電腦插在 VigorSwitch G2260 的 Port 上面之後
Switch 自動把網路卡的卡號當成帳號和密碼
帶往 Radius server 做驗證

相關文章在
VigorSwitch G2260 Authentication By Client MAC Address
http://www.ublink.org/index.php/component/content/article/28-vigorswitch/447-vigorswitch-g2260-authentication-by-client-mac-address.html

這篇文章我們重點是放在 Wireshark 分析 EAP 的包成功與否
因此說明失敗流程包
和成功流程的包
和封包的內容



失敗的流程

Radius Client 是 192.168.254.7

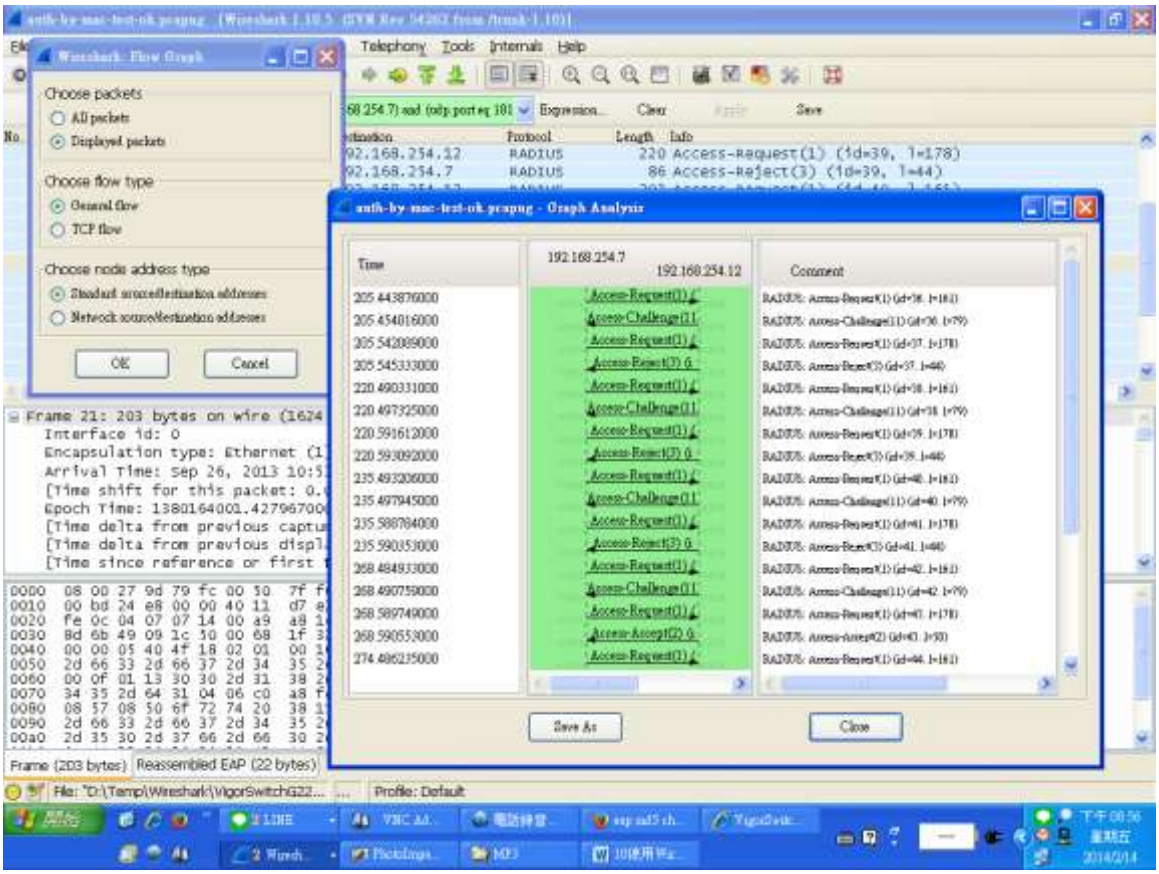
Radius Server 是 192.168.254.12

192.168.254.7 先發出 Access-Request 給 192.168.254.12

192.168.254.12 丟回給 192.168.254.7 說他要 Access-Challenge

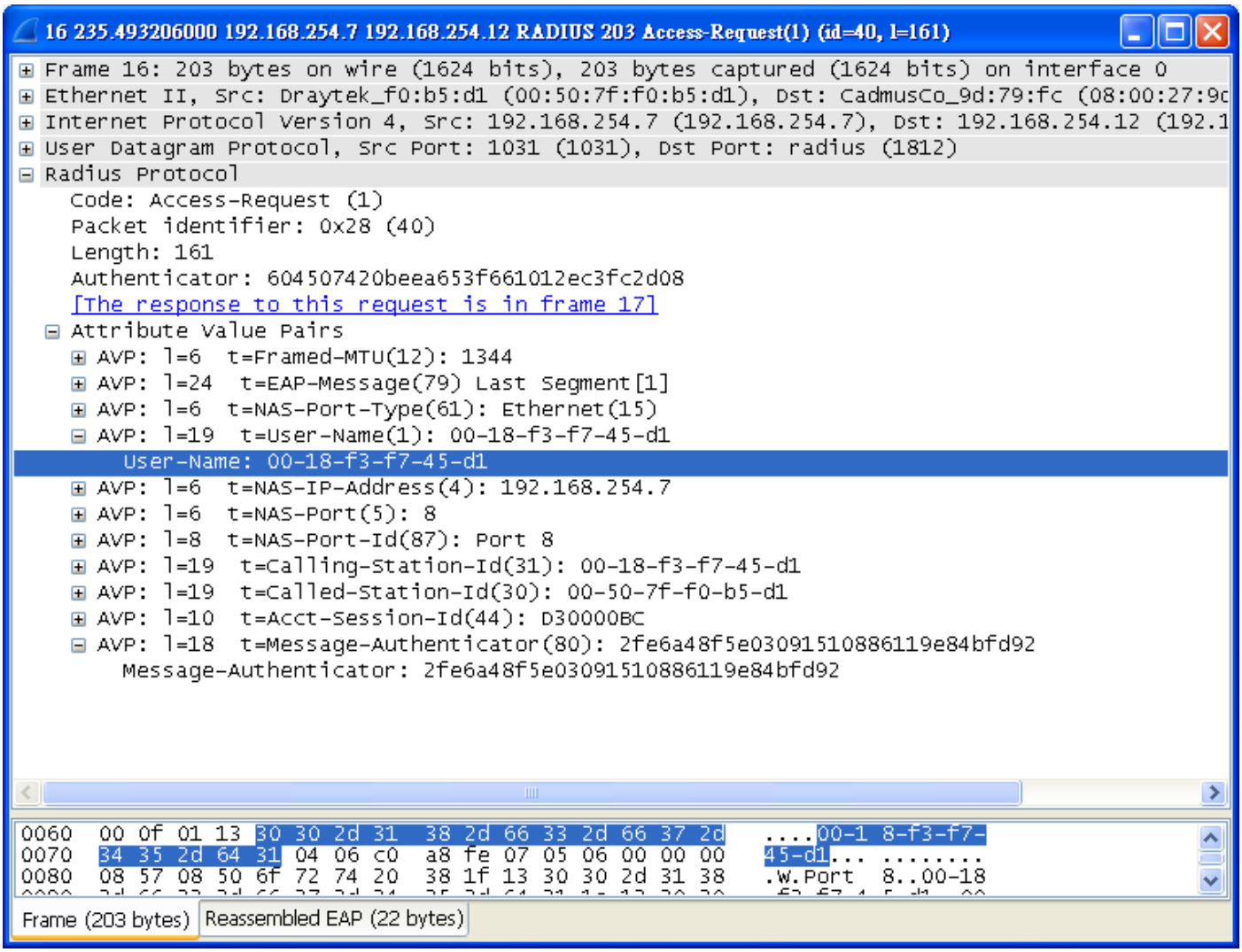
192.168.254.7 再丟回 192.168.254.12 Access-Request

192.168.254.12 跟 192.168.254.7 說 Access-Reject



Wireshark Flow Graph 的功能

我們先看第一個包是送啥

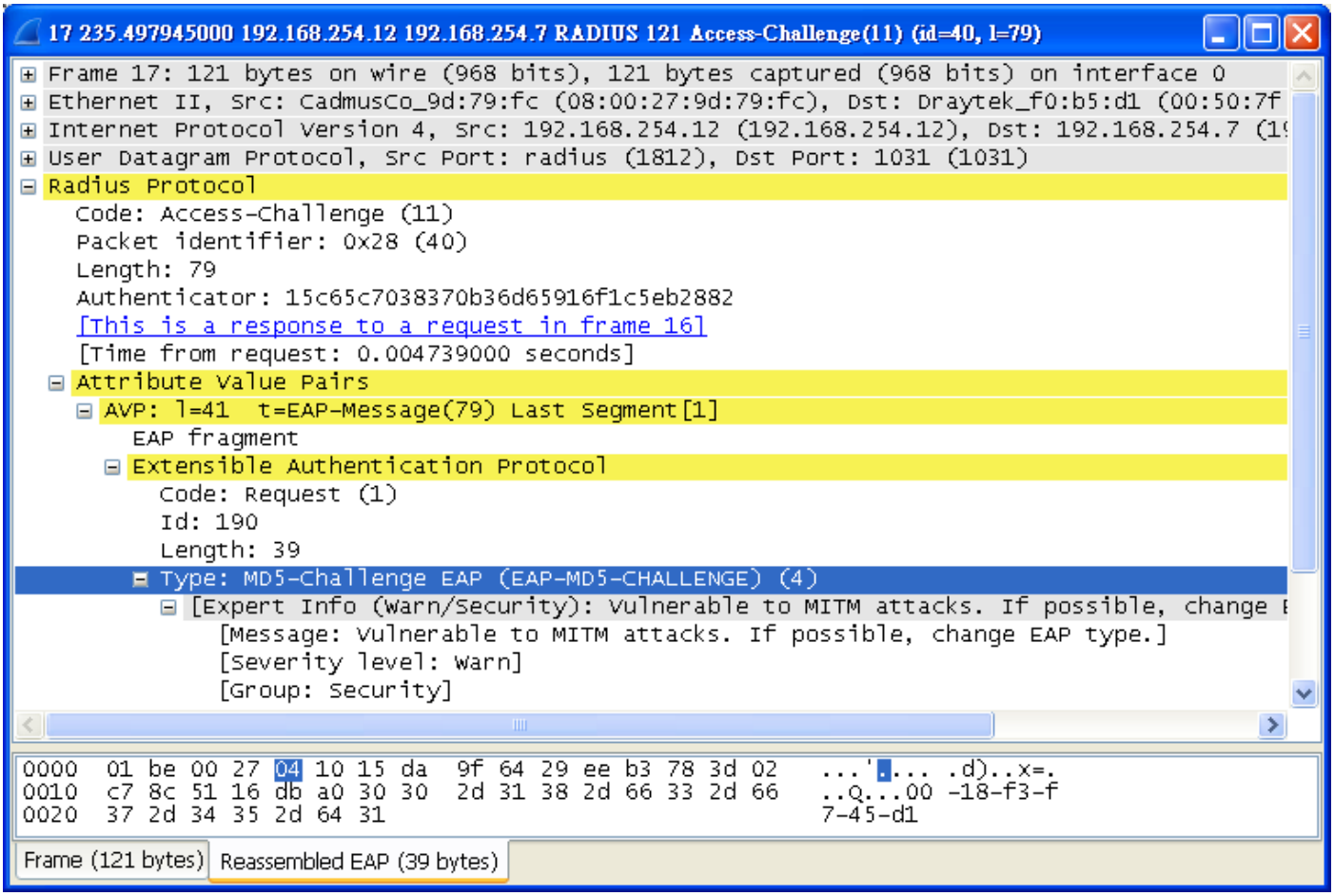


我們看重點

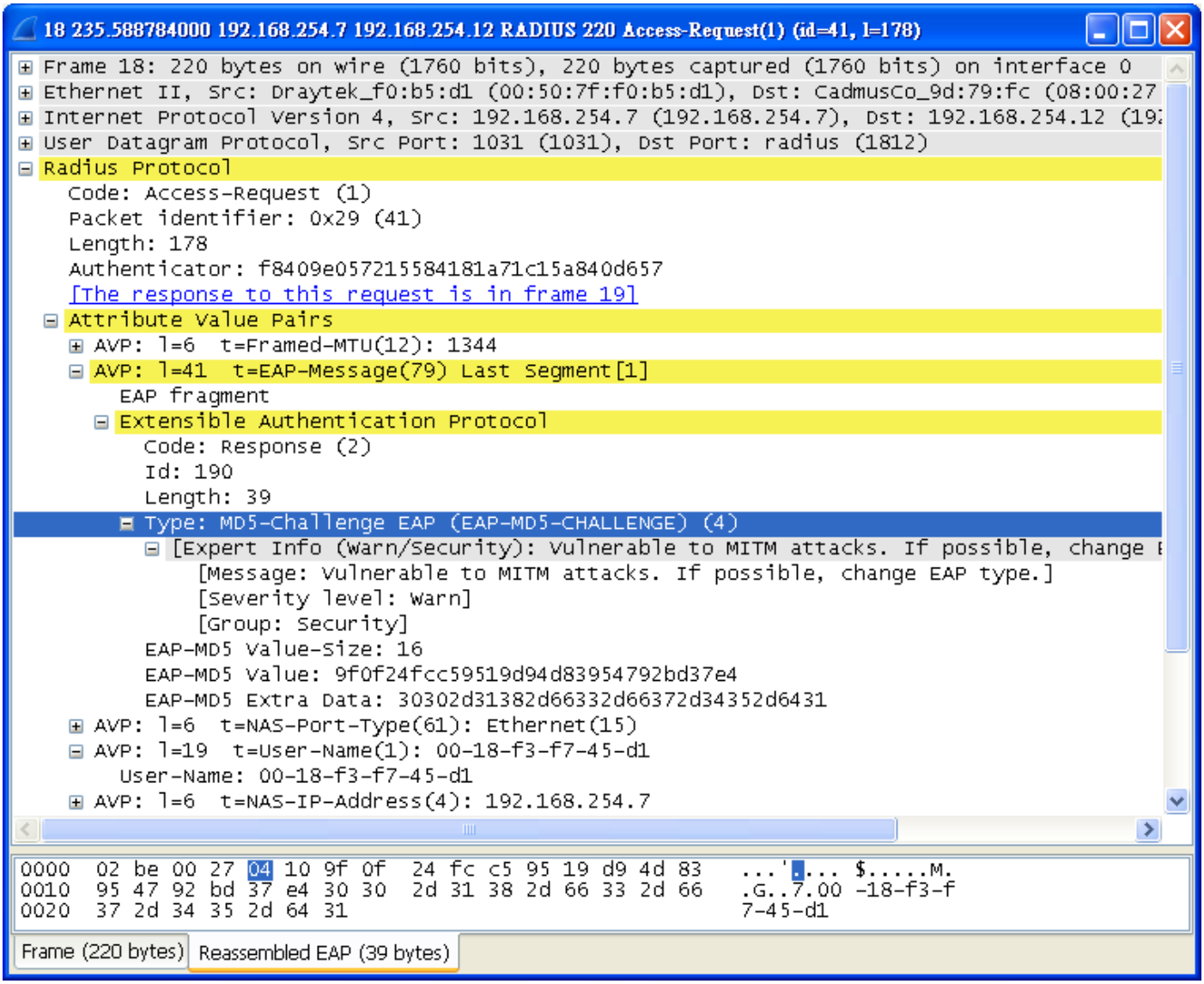
Radius Protocol

Attribute Value Pairs

User-Name:是 Switch Port 帶出的正確 MAC Address

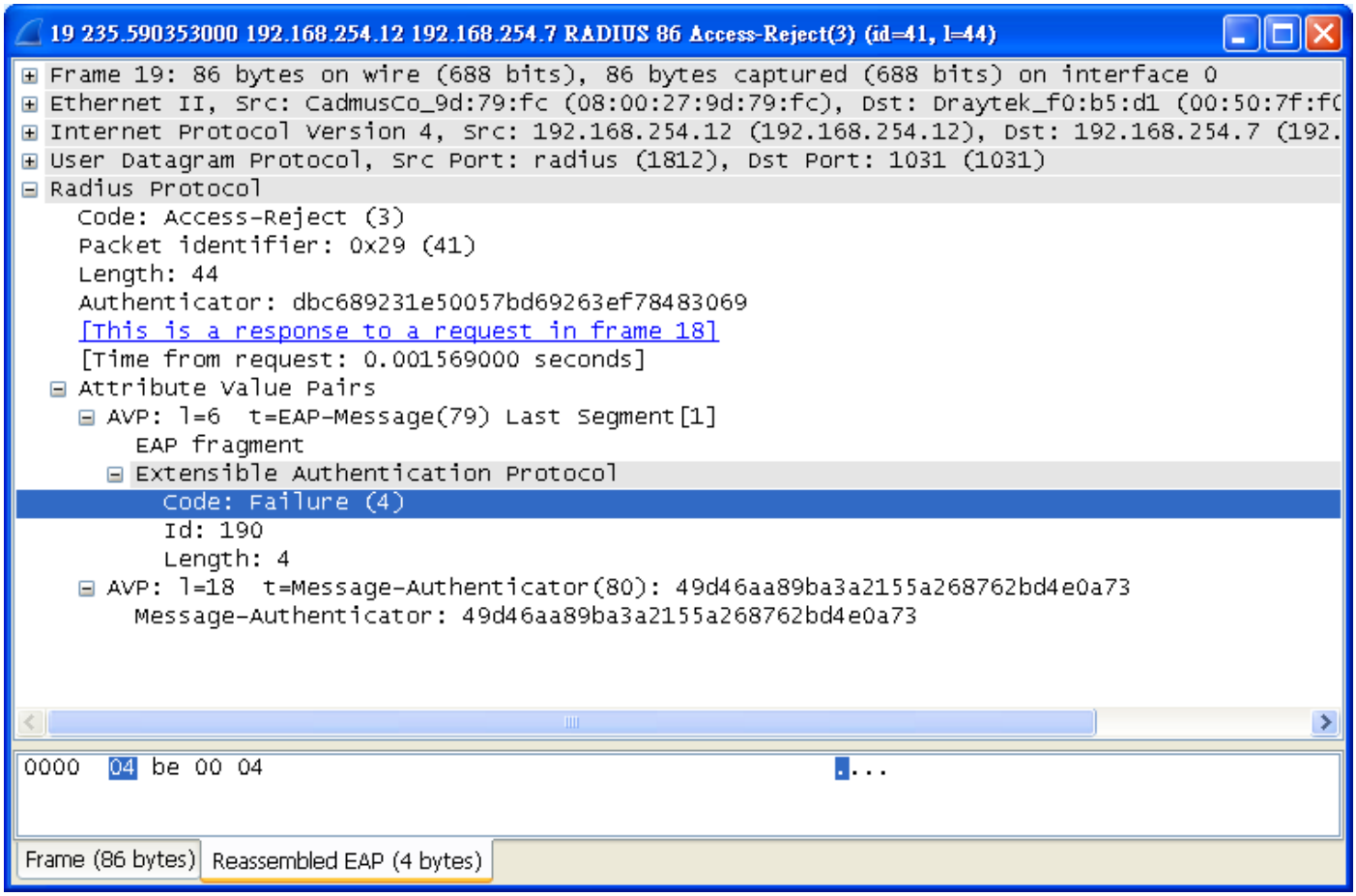


192.168.254.12 Radius Server 回給 192.168.254.7 說他要的 Type 是 MD5-Challenge

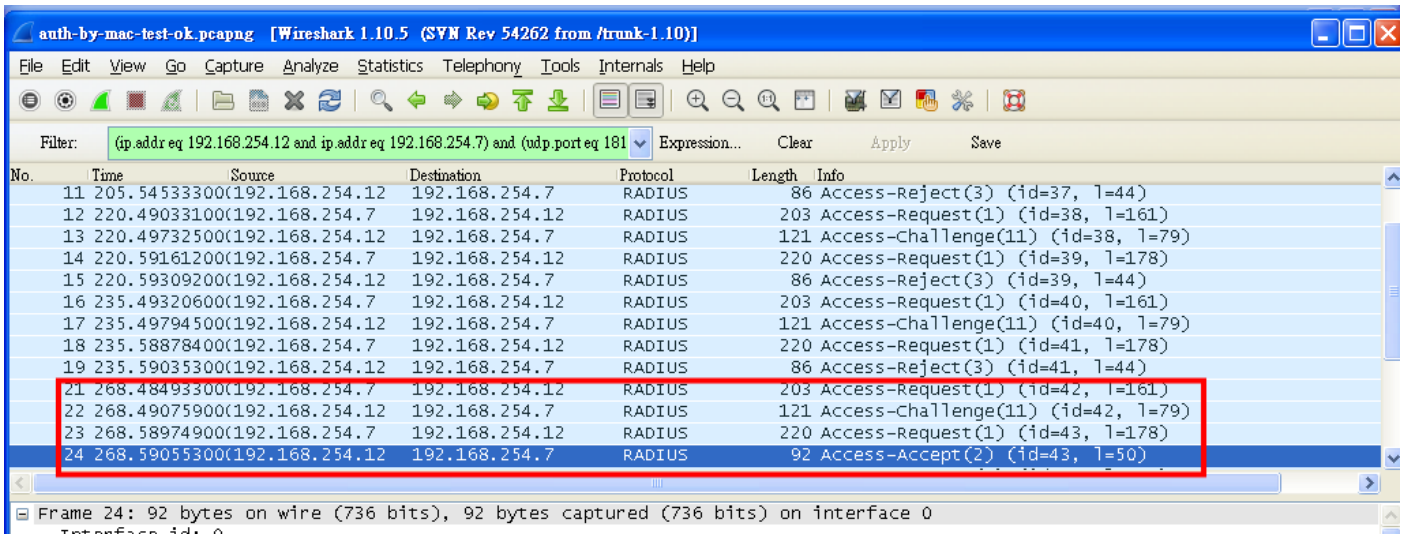


Ok

已經帶 MD5-Challenge 的包過來了

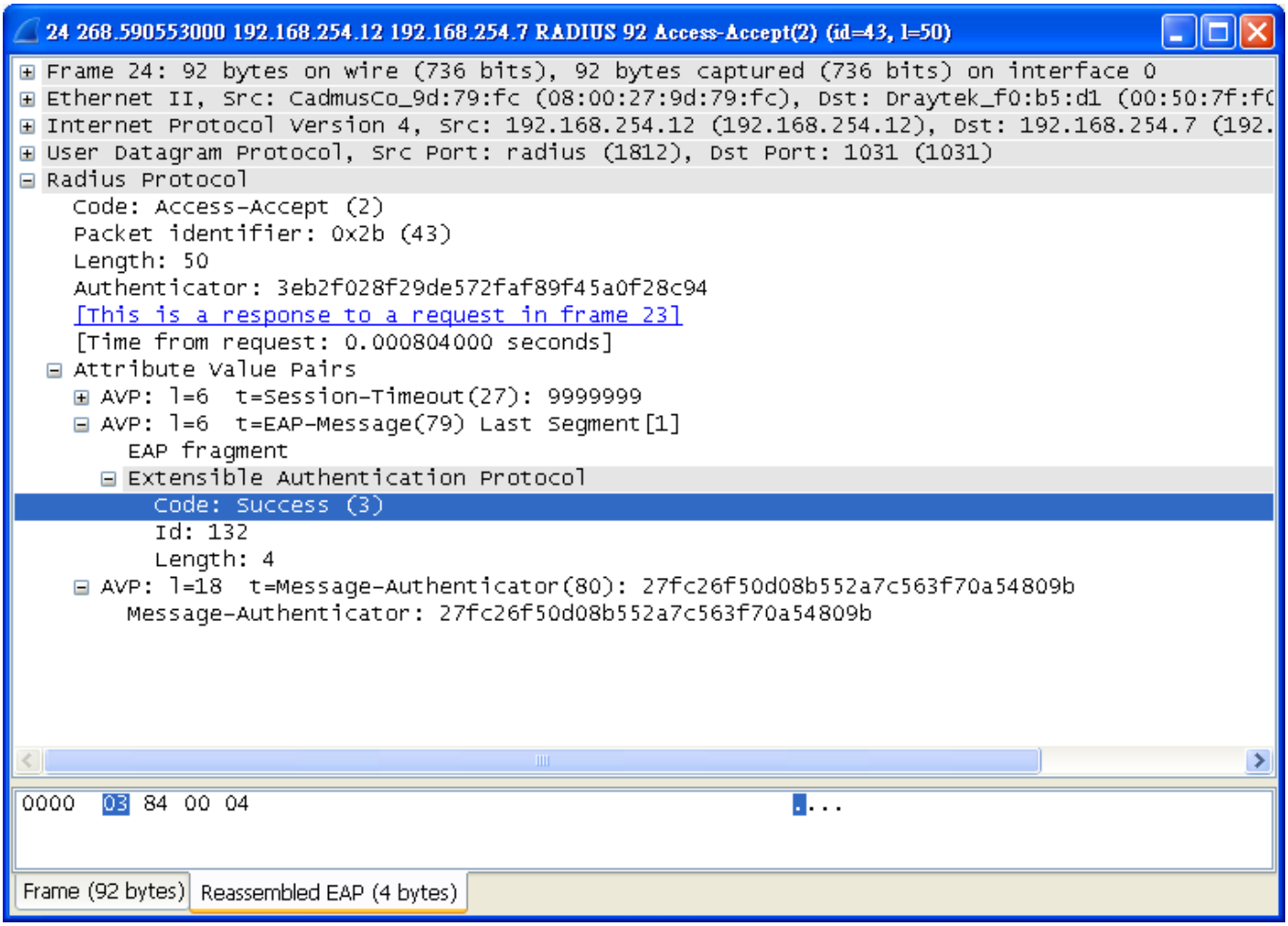


驗證錯誤被 Reject 了



成功的流程

差在最後一個包



Radius Server 確定帳號和密碼都對

回應 Code:Success