10使用Wireshark分析Radius-EAP的封包

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

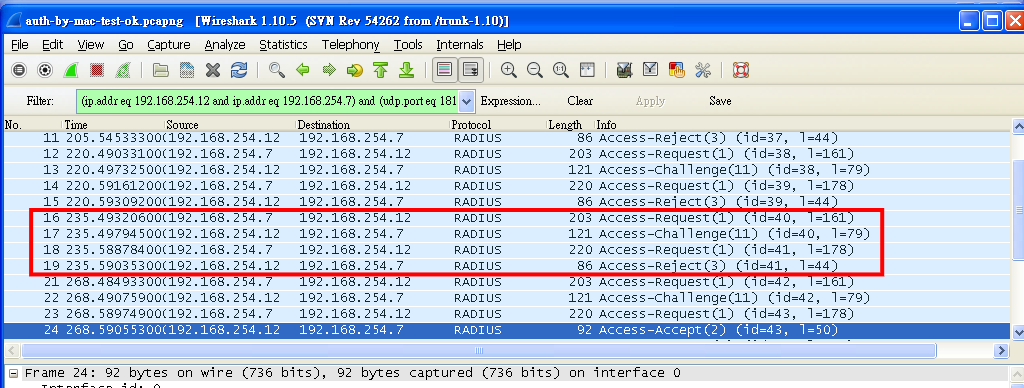
<http://www.ublink.org/index.php/component/content/article/28-vigorswitch/447-vigorswitch-g2260-authentication-by-client-mac-address.html>

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

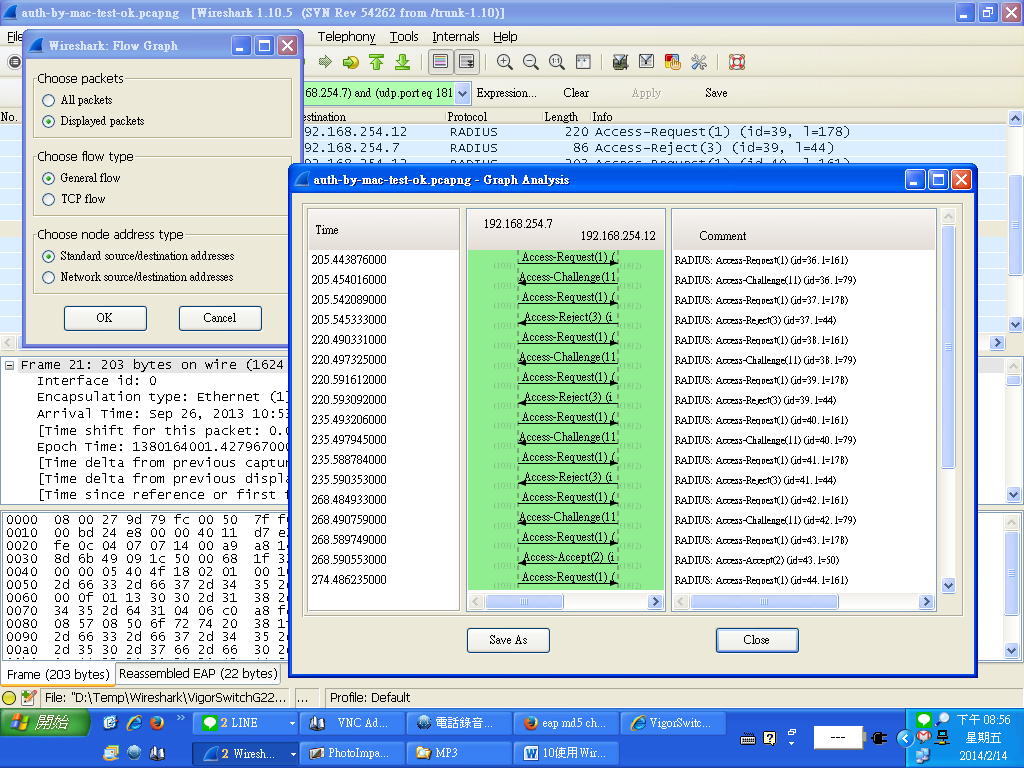
Radius Server是192.168.254.12

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

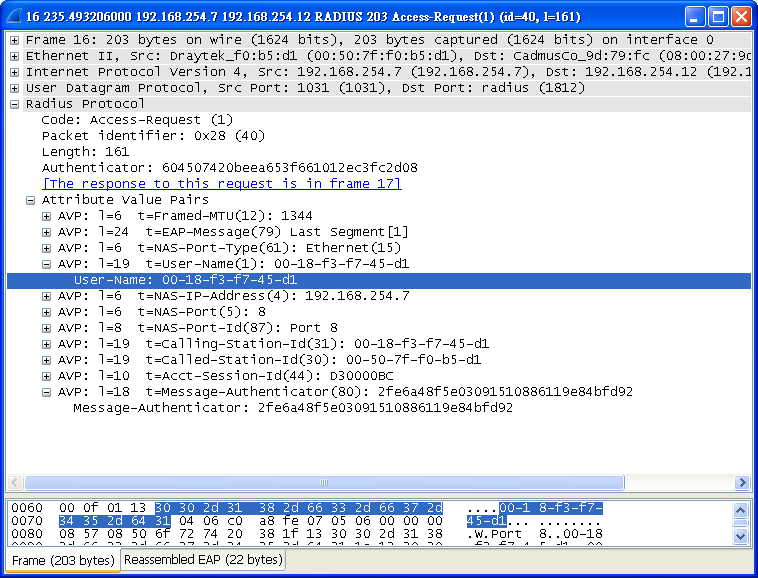
192.168.254.7再丟回192.168.254.12 Access-Request

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

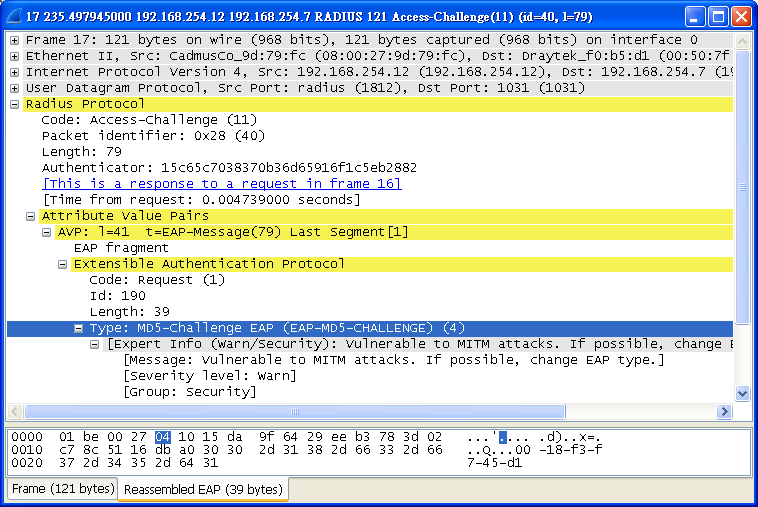


我們看重點

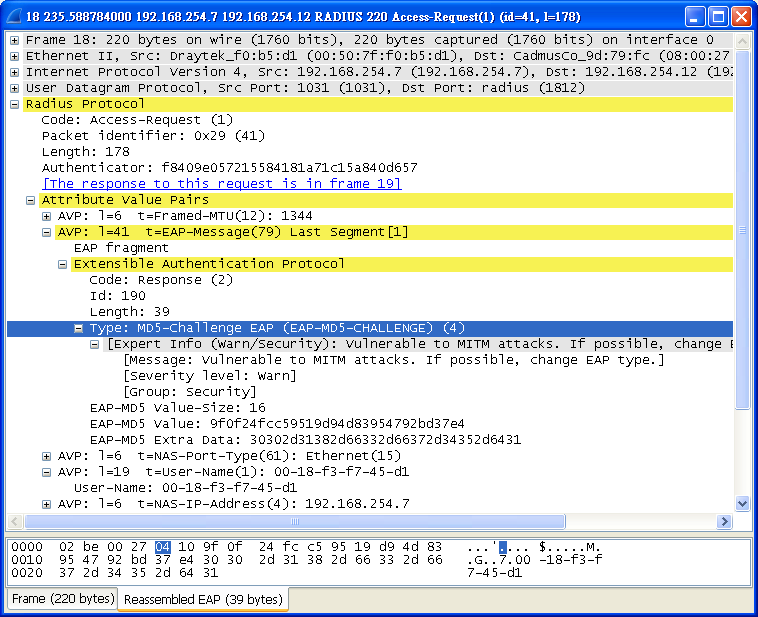
Radius Protocol

Attribute Value Pairs

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

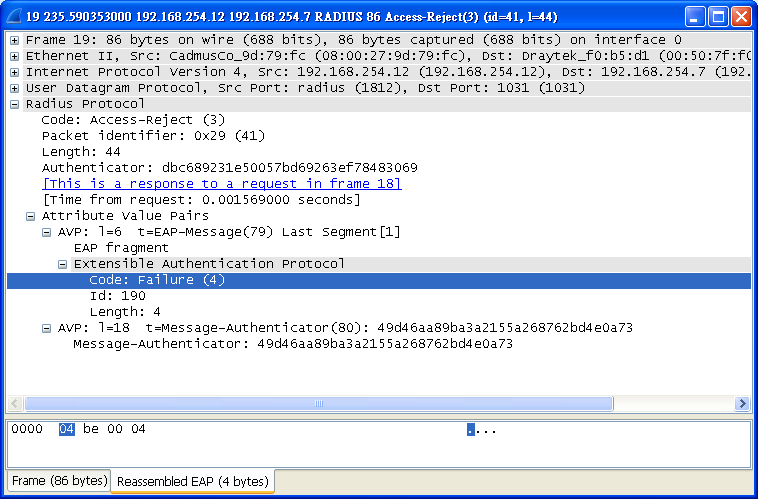


192.168.254.12 Radius Server回給192.168.254.7說他要的Type是 MD5-Challenge

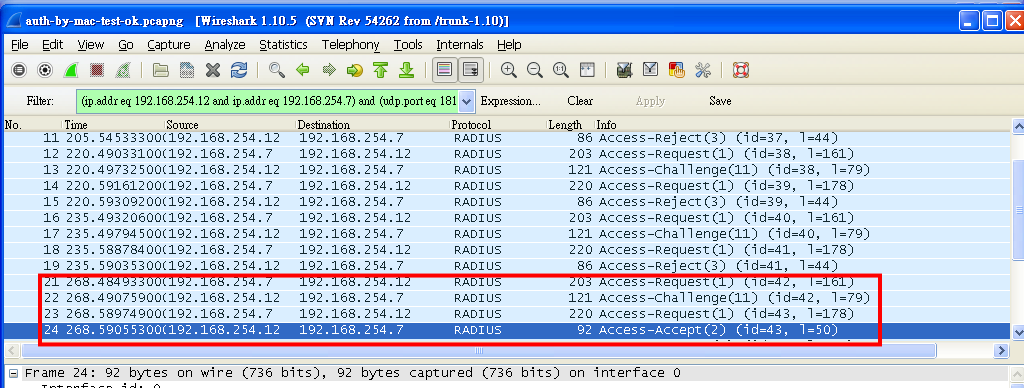


Ok

已經帶MD5-Challenge的包過來了

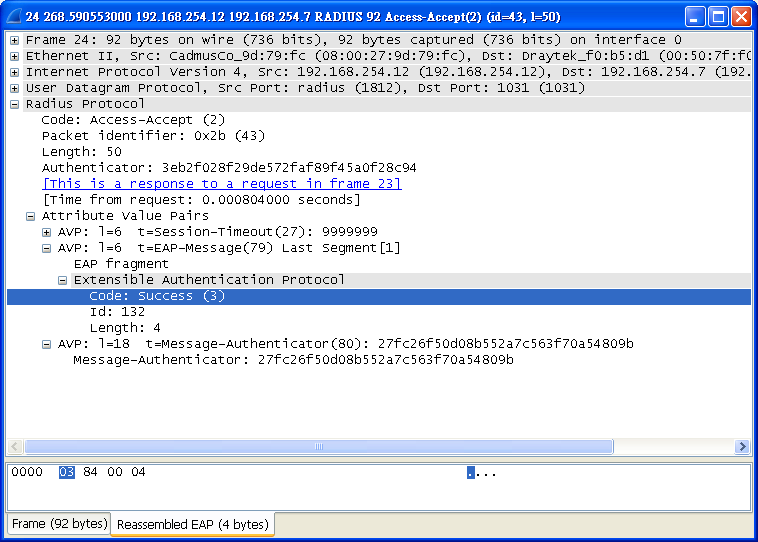


驗證錯誤被Reject了



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