

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 Address

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

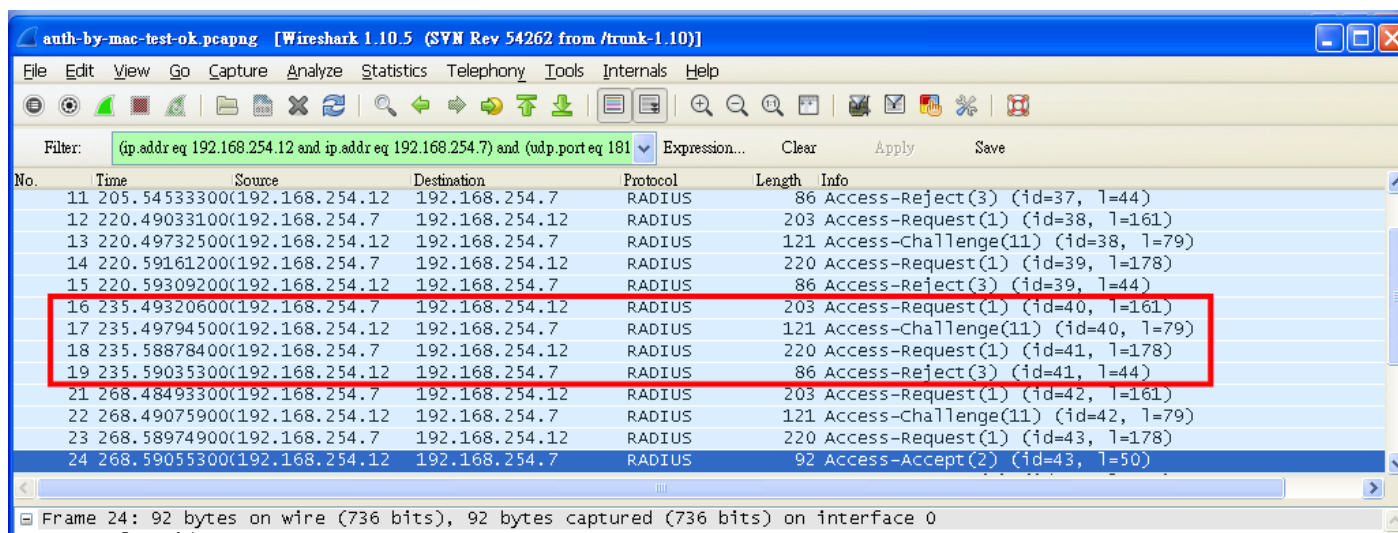
<http://www.ublink.org/index.php/component/content/article/28-vigerswitch/447-vigerswitch-g2260-authentication-by-client-mac-address.html>

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

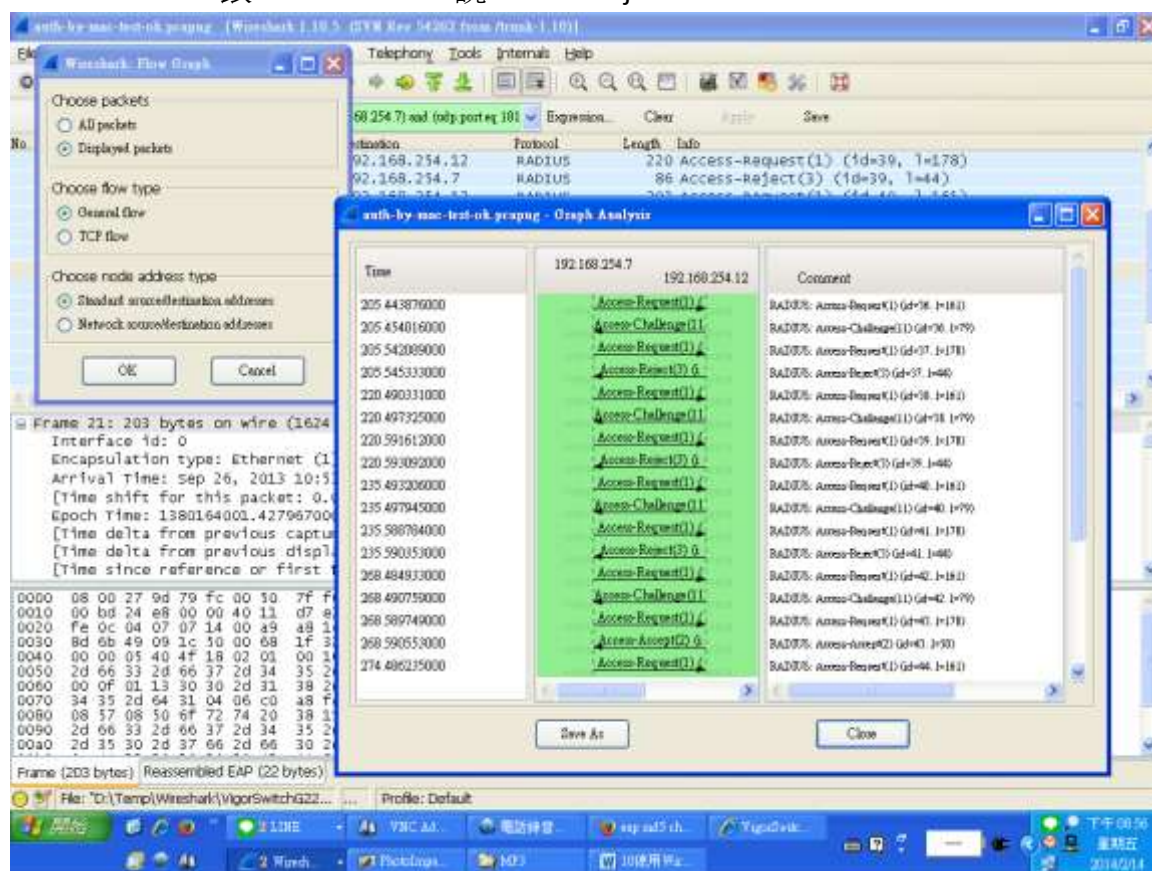
Radius Server 是 192.168.254.12

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

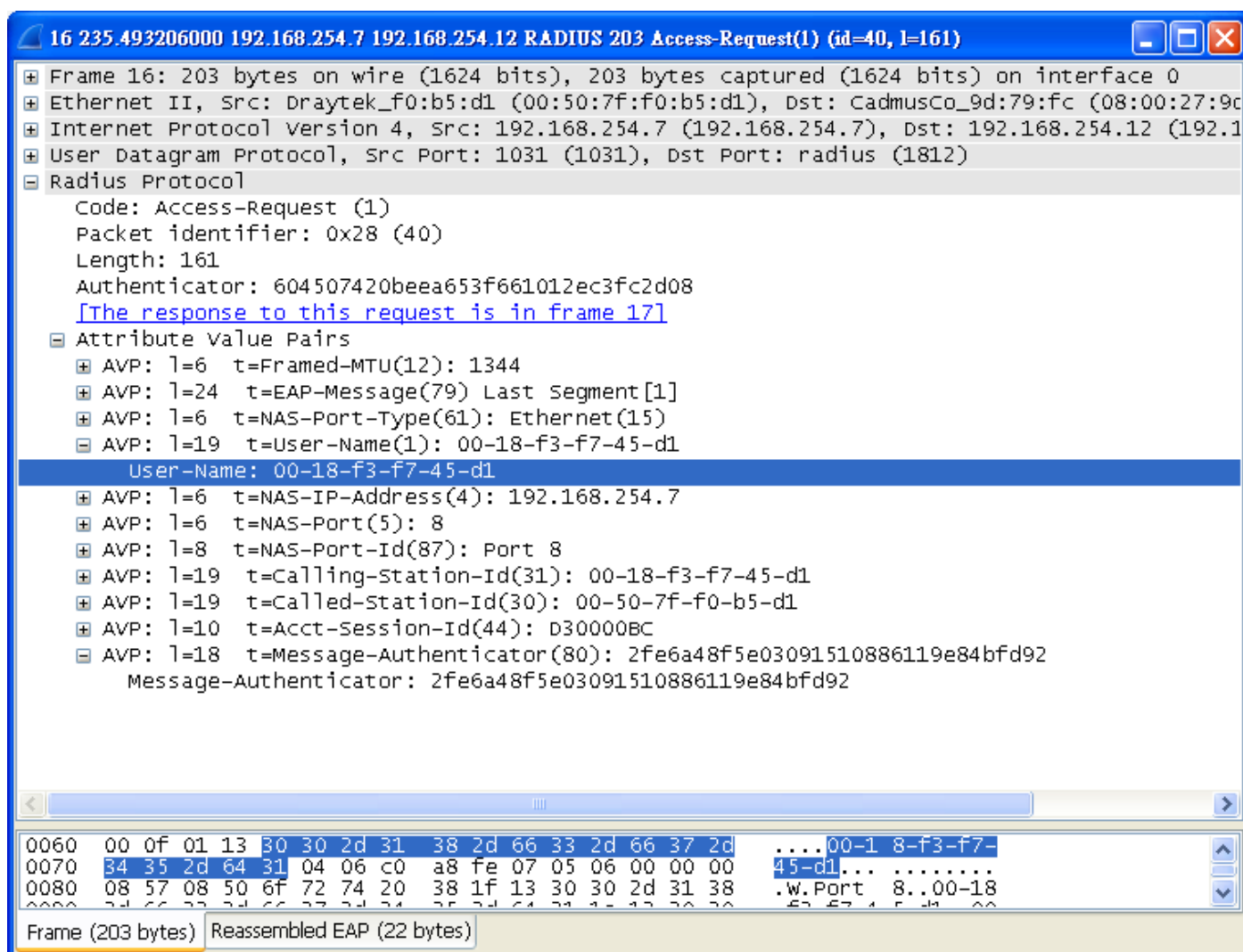
192.168.254.7 再丟回 192.168.254.12 Access-Request

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

17 235.497945000 192.168.254.12 192.168.254.7 RADIUS 121 Access-Challenge(11) (id=40, l=79)

- Frame 17: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface 0
- Ethernet II, Src: CadmusCo_9d:79:fc (08:00:27:9d:79:fc), Dst: Draytek_f0:b5:d1 (00:50:7f:f0:b5:d1)
- Internet Protocol Version 4, Src: 192.168.254.12 (192.168.254.12), Dst: 192.168.254.7 (192.168.254.7)
- User Datagram Protocol, Src Port: radius (1812), Dst Port: 1031 (1031)
- Radius Protocol
 - Code: Access-Challenge (11)
 - Packet identifier: 0x28 (40)
 - Length: 79
 - Authenticator: 15c65c7038370b36d65916f1c5eb2882
 - [\[This is a response to a request in frame 16\]](#)
 - [Time from request: 0.004739000 seconds]
 - Attribute Value Pairs
 - AVP: l=41 t=EAP-Message(79) Last Segment[1]
 - EAP fragment
 - Extensible Authentication Protocol
 - Code: Request (1)
 - Id: 190
 - Length: 39
 - Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
 - [Expert Info (warn/Security): vulnerable to MITM attacks. If possible, change EAP type.]
 - [Message: vulnerable to MITM attacks. If possible, change EAP type.]
 - [Severity level: warn]
 - [Group: Security]

0000 01 be 00 27 04 10 15 da 9f 64 29 ee b3 78 3d 02 ... '... .d)..x=.
 0010 c7 8c 51 16 db a0 30 30 2d 31 38 2d 66 33 2d 66 ..Q...00 -18-f3-f
 0020 37 2d 34 35 2d 64 31 7-45-d1

Frame (121 bytes) Reassembled EAP (39 bytes)

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

18 235.588784000 192.168.254.7 192.168.254.12 RADIUS 220 Access-Request(1) (id=41, l=178)

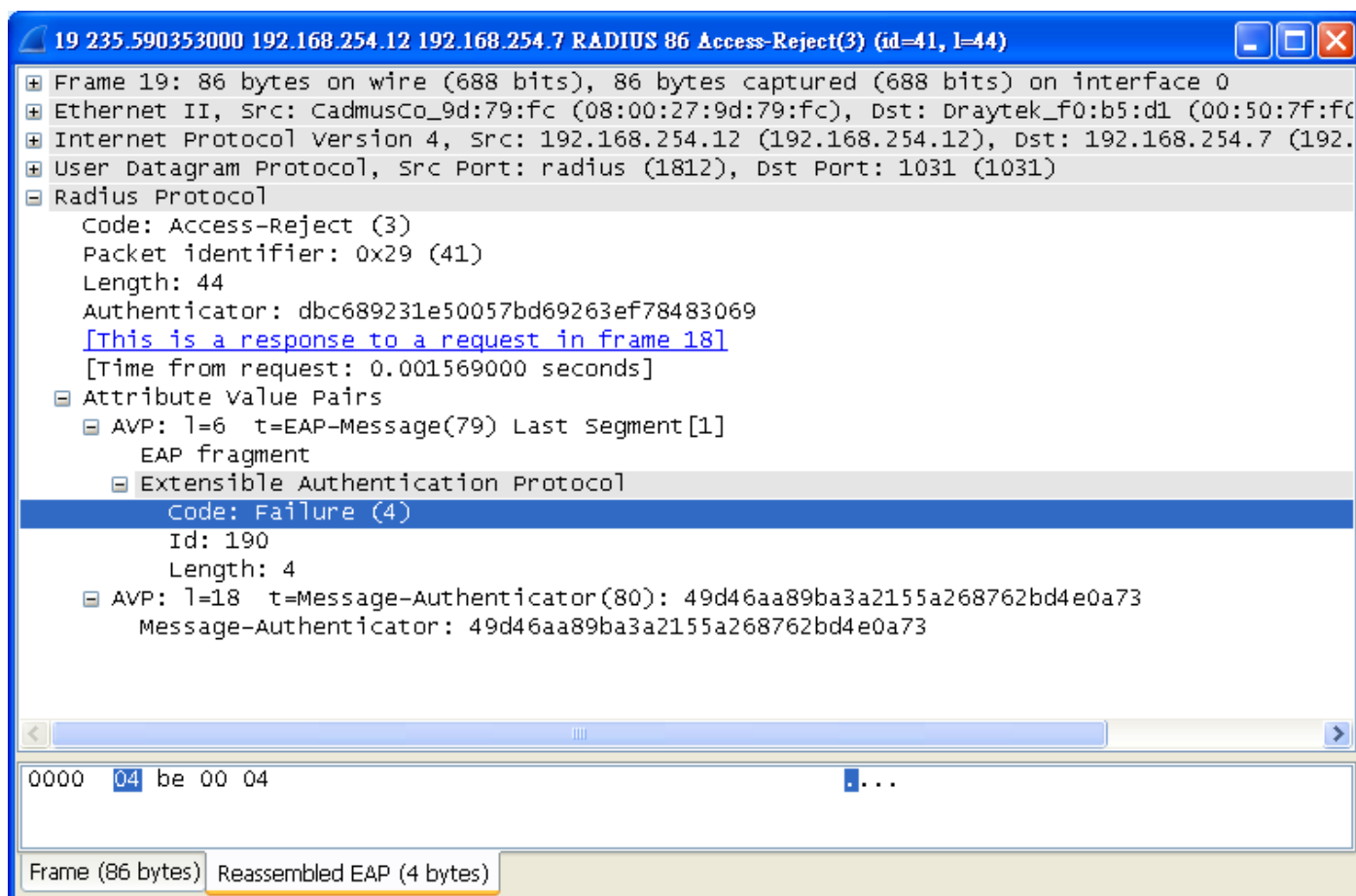
- Frame 18: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface 0
- Ethernet II, Src: Draytek_f0:b5:d1 (00:50:7f:f0:b5:d1), Dst: CadmusCo_9d:79:fc (08:00:27:9d:79:fc)
- Internet Protocol Version 4, Src: 192.168.254.7 (192.168.254.7), Dst: 192.168.254.12 (192.168.254.12)
- User Datagram Protocol, Src Port: 1031 (1031), Dst Port: radius (1812)
- Radius Protocol
 - Code: Access-Request (1)
 - Packet identifier: 0x29 (41)
 - Length: 178
 - Authenticator: f8409e057215584181a71c15a840d657
 - [\[The response to this request is in frame 19\]](#)
- Attribute Value Pairs
 - AVP: l=6 t=Framed-MTU(12): 1344
 - AVP: l=41 t=EAP-Message(79) Last Segment[1]
 - EAP fragment
 - Extensible Authentication Protocol
 - Code: Response (2)
 - Id: 190
 - Length: 39
 - Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
 - [Expert Info (warn/Security): vulnerable to MITM attacks. If possible, change EAP type.]
 - [Message: vulnerable to MITM attacks. If possible, change EAP type.]
 - [Severity level: warn]
 - [Group: Security]
 - EAP-MD5 Value-Size: 16
 - EAP-MD5 Value: 9f0f24fcc59519d94d83954792bd37e4
 - EAP-MD5 Extra Data: 30302d31382d66332d66372d34352d6431
 - AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
 - AVP: l=19 t=User-Name(1): 00-18-f3-f7-45-d1
 - User-Name: 00-18-f3-f7-45-d1
 - AVP: l=6 t=NAS-IP-Address(4): 192.168.254.7

0000 02 be 00 27 04 10 9f 0f 24 fc c5 95 19 d9 4d 83 ...'...'\$.M.
 0010 95 47 92 bd 37 e4 30 30 2d 31 38 2d 66 33 2d 66 .G..7.00 -18-f3-f
 0020 37 2d 34 35 2d 64 31 7-45-d1

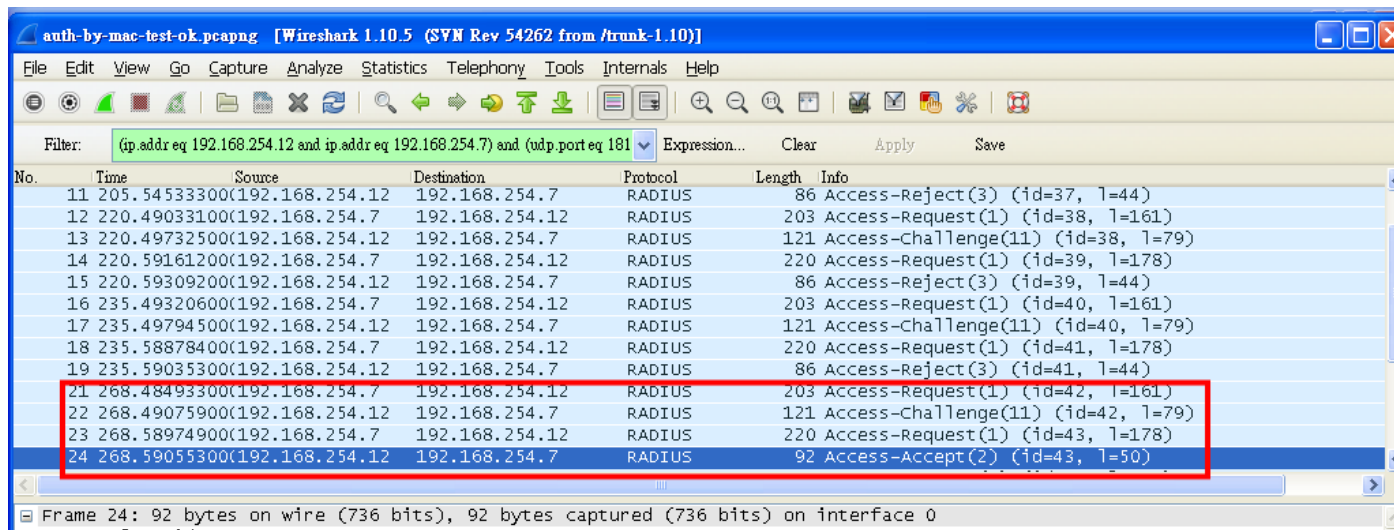
Frame (220 bytes) Reassembled EAP (39 bytes)

Ok

已經帶 MD5-Challenge 的包過來了

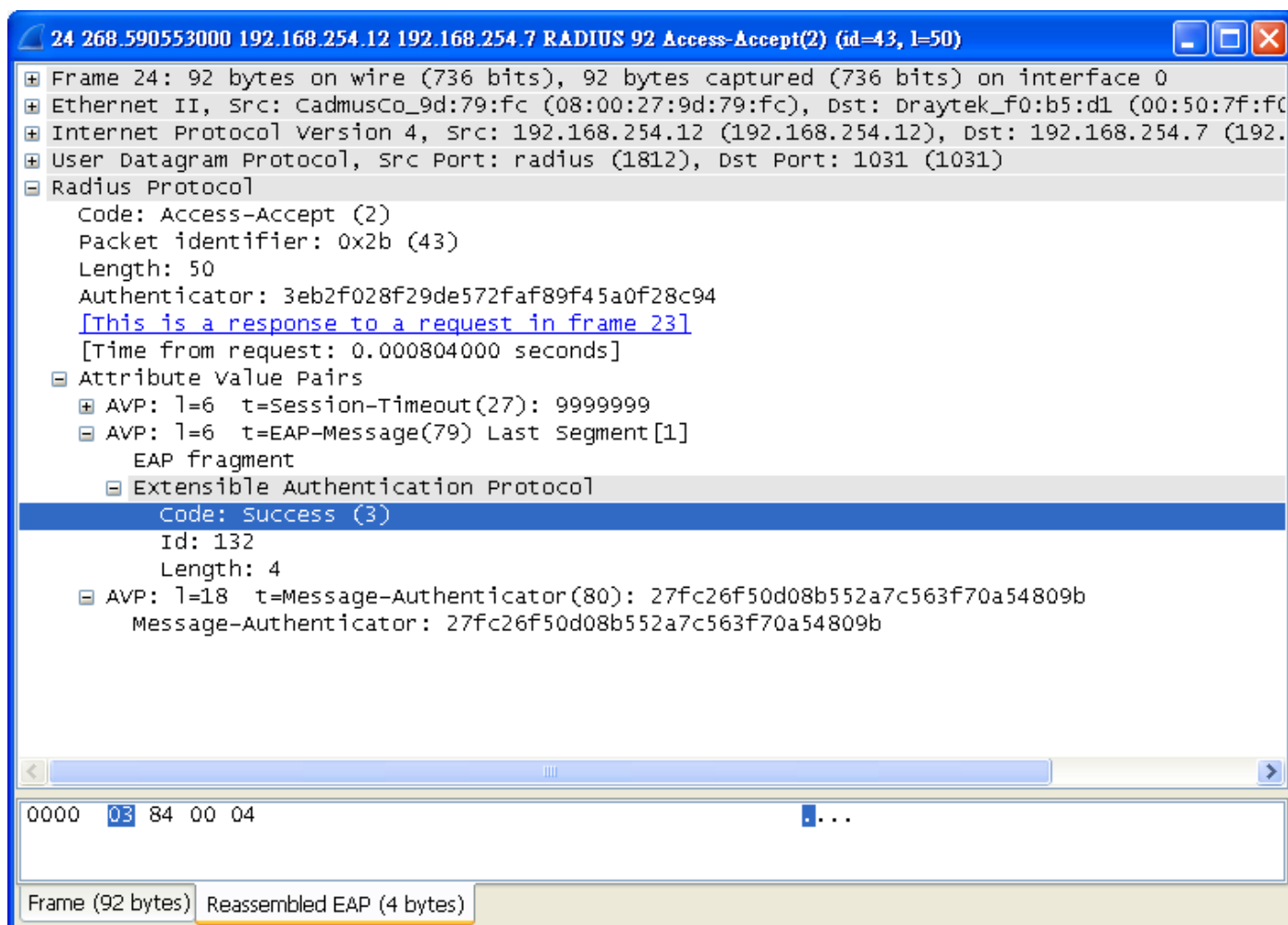


驗證錯誤被 Reject 了



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