ĐỀ TÀI: RADIUS

GVHD:Th.S VĂN THIÊN HOÀNG

Nhóm thực hiện đề tài

1.Trần Phúc Lợi **2. Lương Quốc Hạnh**

3. Lương Đăng Khoa **4. Huỳnh Mai Khanh**

Radius và quá trình hình thành

RADIUS là một giao thức dùng để chứng thực người dùng từ xa (remote access). Thông tin dùng để chứng thực được lưu tập trung ở RADIUS server. Khi cần chứng thực người dùng NAS (RADIUS client) sẽ chuyển thông tin của người dùng đến RADIUS server để tiến hành kiểm tra.

Giao thức Radius được định nghĩa đầu tiên trong RFC 2058 vào tháng 1 năm 1997

Cũng trong năm 1997 Radius accounting đã được giới thiệu trong RFC 2059

Sau đó vào tháng 4 năm 1997 nhiều bản RFC đã được thay thế bởi RFC 2138 và RFC 2139

Sau đó vào tháng 6 năm 2000 RFC 2865 đã chuẩn hóa Radius và thay thế cho RFC 2138

Cùng thời gian đó RFC 2866 accounting cũng đã thay thế cho RFC 2139

Cơ chế chứng thực AAA

A

Authentication
Xác thực

Xác thực dùng để nhận dạng (identify) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server.

A

Authorization
Cấp quyền

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể

hay trên từng giao thức…

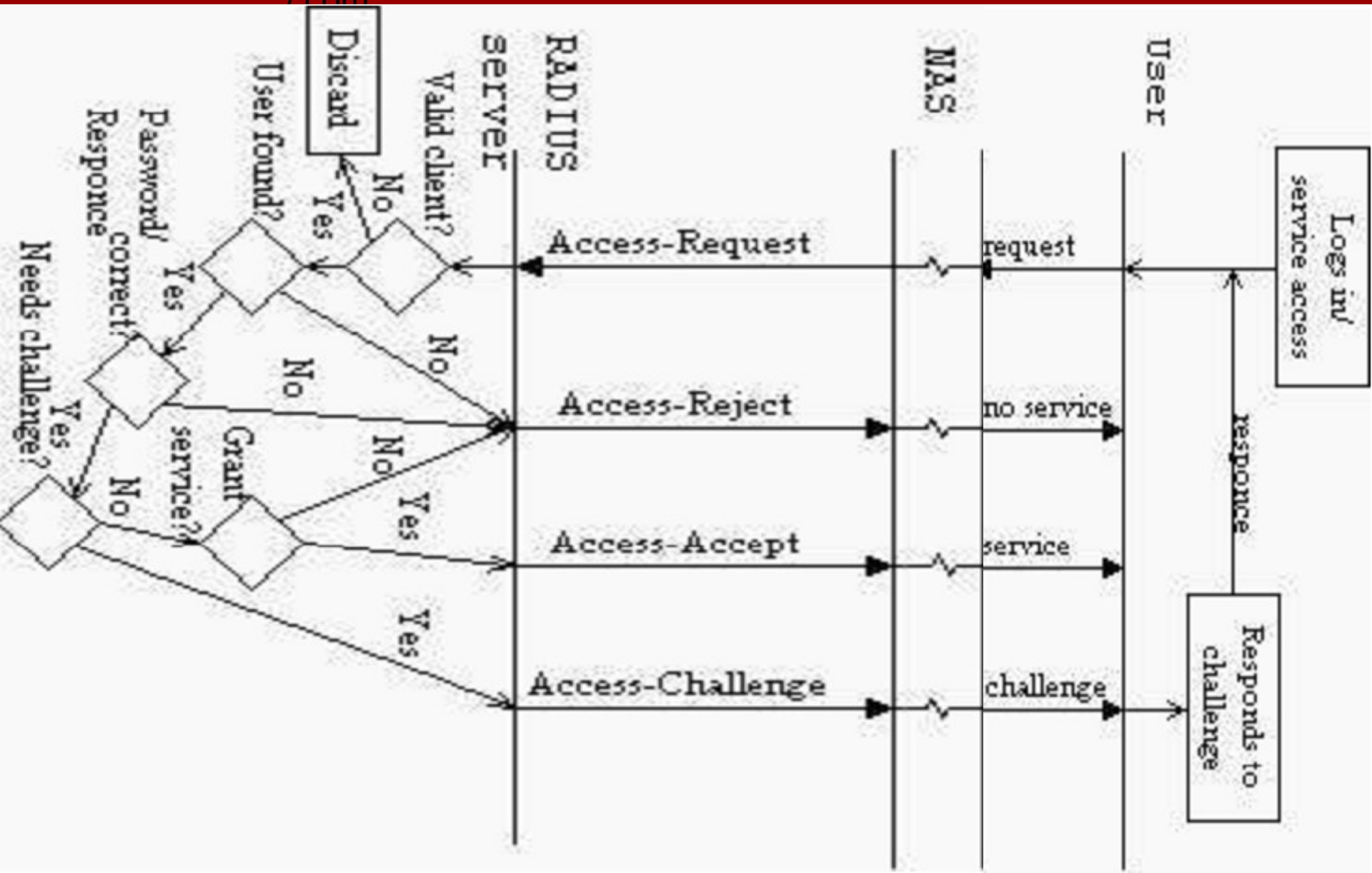
A

Accounting
Kiểm toán

Accounting cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống, các câu lệnh đã thực thi, thống kê lưu lượng, việc sử dụng tài nguyên….

AAA với ba phần xác thực (authentication), cấp quyền (authorization), kiểm toán (accounting) nhằm đảm bảo nhận dạng đúng người dùng và giới hạn thẩm quyền mà người dùng có thể làm trong mạng…

Sơ đồ nguyên lý chứng thực và cấp quyền



Sơ đồ nguyên lý kiểm toán Radius

KIẾN TRÚC RADIUS
DẠNG GÓI CỦA RADIUS

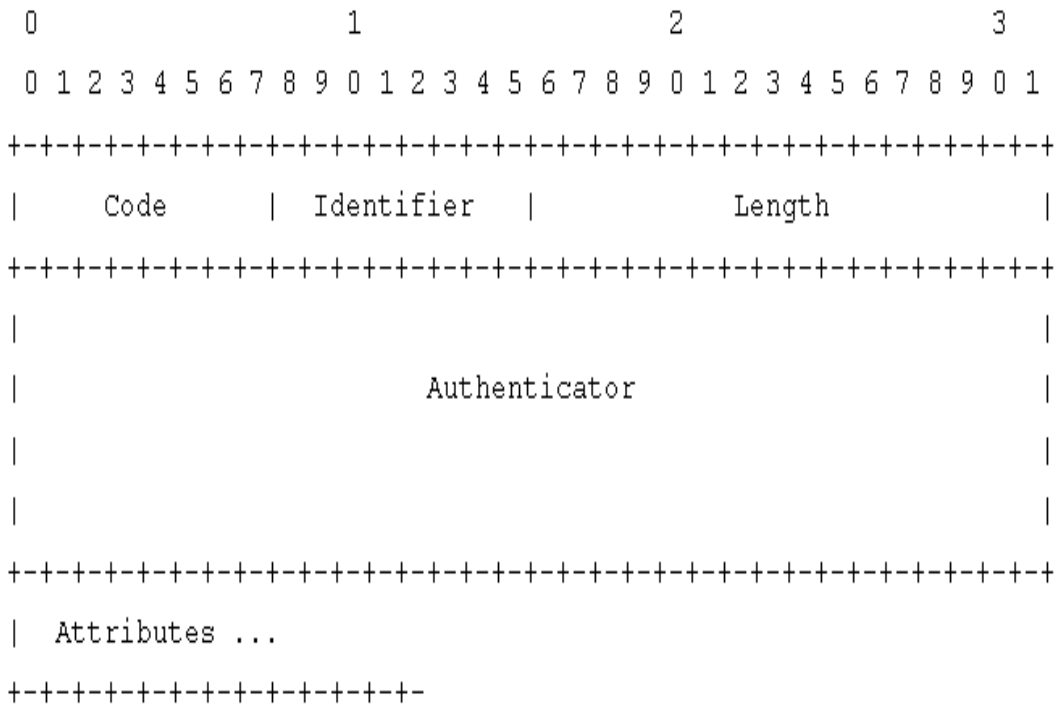
Code field: Code field gồm một octet, xác định kiểu gói của RADIUS. Khi một gói có mã không hợp lệ sẽ không được xác nhận

Identifier field: là trường định danh xác định chỉ IP nguồn và UDP port

Length field: gồm hai octet, nó bao gồm các code field, indentifier, length, authentication và trường thuộc tính.

Authenticator field: gồm 16 octet. Octet lớn nhất được truyền đi đầu tiên. Giá trị này được sử dụng để xác nhận các trả lời từ RADIUS server và được sử dụng trong thuật toán ẩn mật khẩu

Attribute filed: chứa các thuộc tính Của gói

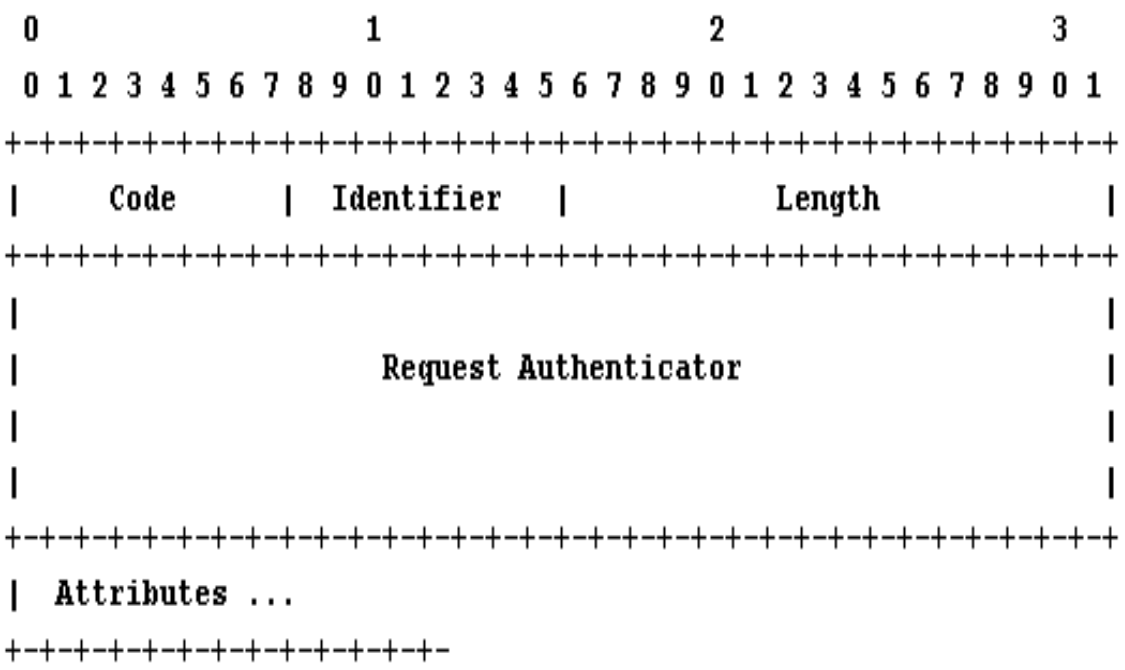


KIẾN TRÚC RADIUS
Gói Access-Request

Gói access-request được gửi tới RADIUS server. Nó chuyên chở thông tin dùng để xác định xem user có được phép truy cập vào NAS và các dịch vụ được phép truy cập.

Code field của gói phải có giá trị 1

Gói access-request phải chứa các thuộc tính user-name, user-password hoặc CHAP-password,và có thể chứa các thuộc tính NAS-IP-Address, NAS-Indentifier, NAS-PORT, NAS-PORT-TYPE ….

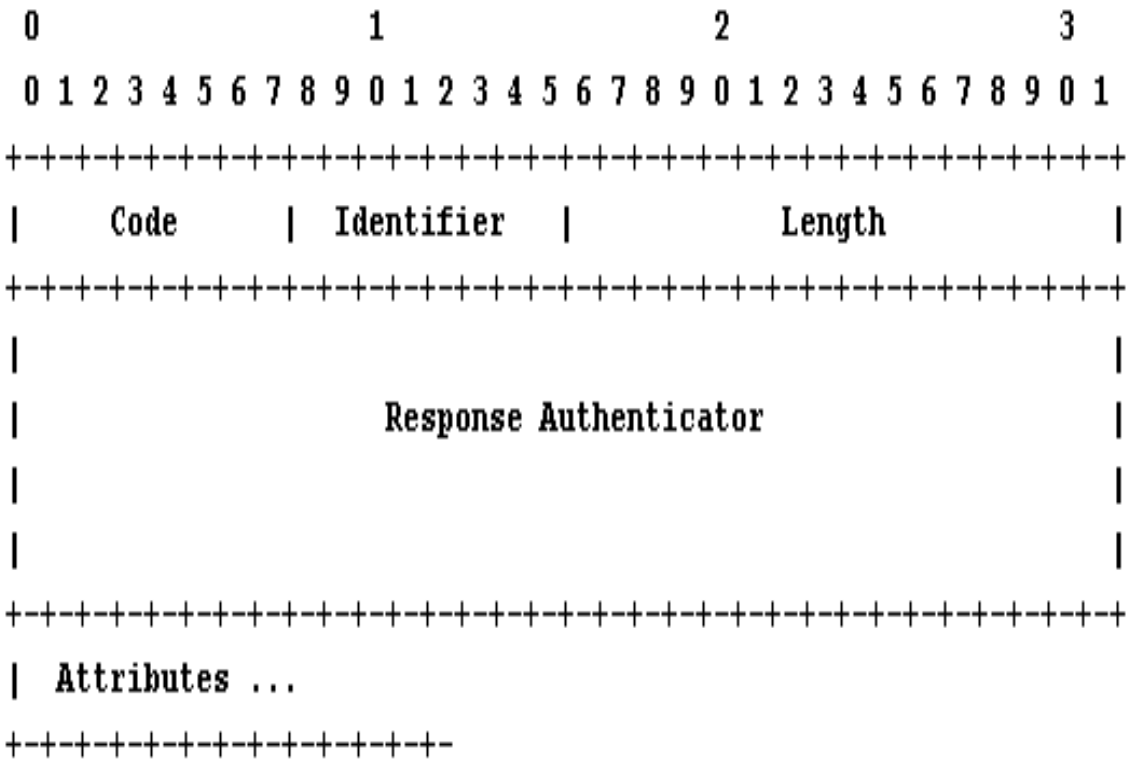


KIẾN TRÚC RADIUS
Gói Access-Accept

Gói access-accept được gởi trả bởi RADIUS server khi tất cả các giá trị thuộc tính của gói access-request. Nó cung cấp thông tin cấu hình cần thiết để cấp phát các dịch vụ cho user.

Code field: phải có giá trị 2.

Gói access-accept nhận được ở NAS phải có trường danh hiệu trùng khớp với access-request tương ứng đã gởi trước đó và phải có xác nhận (response authenticator) phù hợp với thông tin bí mật dùng chung

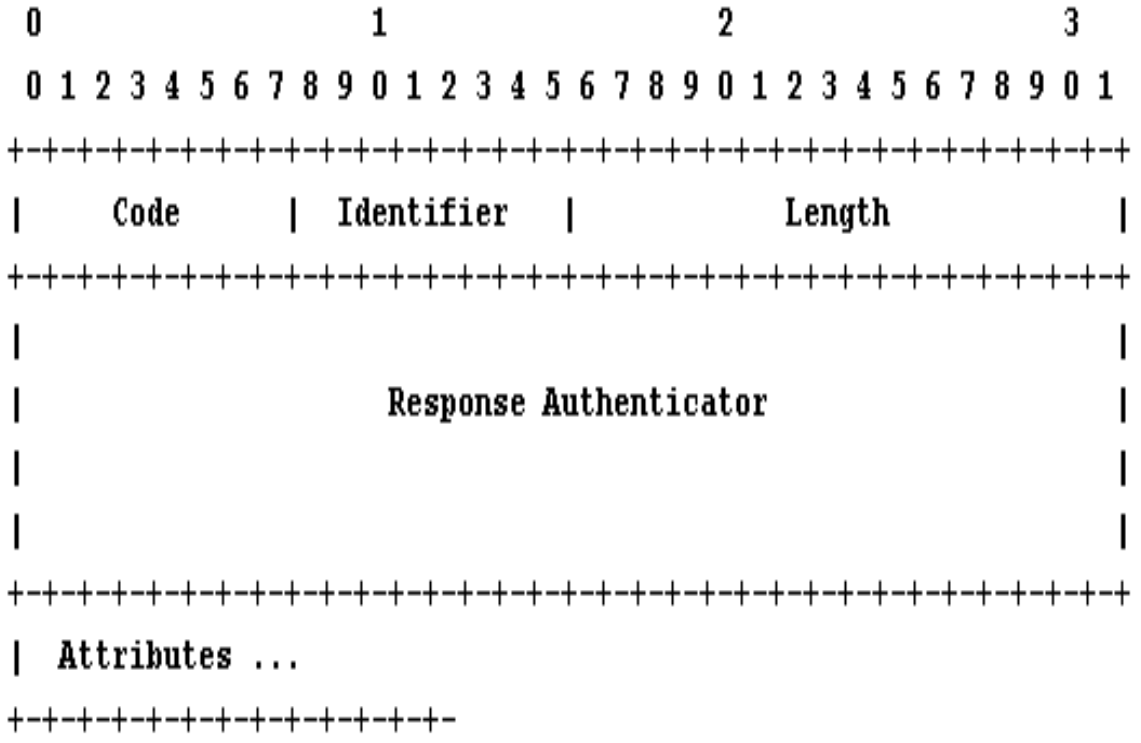


KIẾN TRÚC RADIUS
Gói Access-Chellange

Gói access-challenge được RADIUS server gửi đến user đòi hỏi thêm thông tin cần thiết mà user phải trả lời.

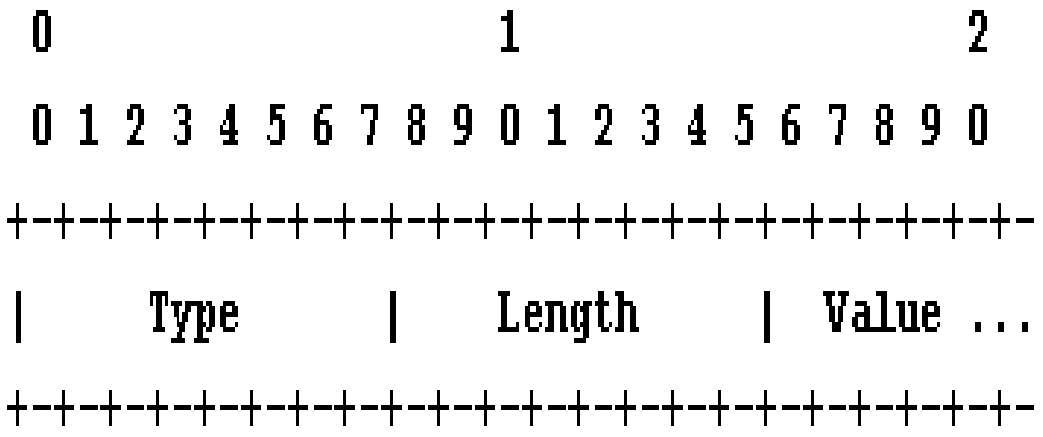
Code field của gói phải có giá trị **11**.

Indentifier field của gói access-challenge phải trùng khớp với gói access-request tương ứng đã gửi đi trước đó và phải có trường xác nhận (authenticator field) phù hợp với thông tin bí mật dùng chung.



KIẾN TRÚC RADIUS
Gói Attribute

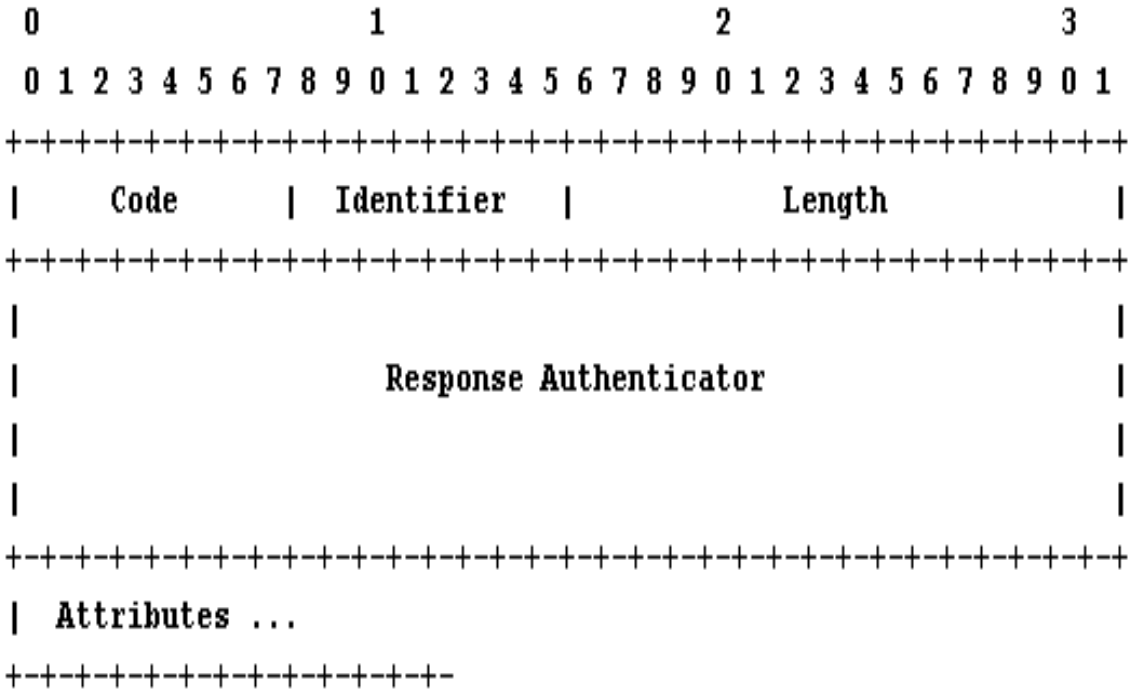
Type field gồm một octet, giá trị từ 192-223 là dành riêng cho nghiên cứu, giá trị từ 224-240 là dành cho việc thực hiện cụ thể, 241-255 là dành riêng và không nên sử dụng.
Length *biểu thị độ dài của thuộc tính*
Value *(trường giá trị) Có 4 loại dữ liệu cho trường giá trị như sau*:



Text 1-253 octets containing UTF-8 encoded character.
String 1-253 octets containing binary data
Integer 32 bit unsigned value, most significant octet first
Time 32 bit unsigned value, most significant octet first

KIẾN TRÚC RADIUS
Gói Access-Reject

Gói access-reject được gởi trả từ RADIUS server khi có giá trị thuộc tính không được thỏa. **Code field** của mã phải có giá trị 3. Gói có thể chứa 1 hay nhiều thuộc tính reply-message với một thông báo dạng văn bản mà NAS sẽ hiển thị nó với user. **indentifier field** của gói access-reject chính là bản sao của gói access-request tương ứng



KIẾN TRÚC RADIUS
PHƯƠNG THỨC MÃ HÓA VÀ GIẢI MÃ

Gọi “thông tin bí mật chung” là **S**
Request authentication 128 bit là **RA**
Các ký tự NULL được thêm vào mật khẩu là **p1, p2**
Các khối mật mã dạng văn bản (ciphertext blocks) là **c(1), c(2)**
Các giá trị trung gian là **b1, b2**…
Dấu + là phép cộng chuỗi
MD5 băm một chiều (one-way MD5 hash) sẽ được xây dựng từ chuỗi các byte của “thông tin bí mật chung” giữa NAS và RADIUS server và thường xác nhận yêu cầu.Giá trị tính được sẽ XOR với đoạn 16 byte đầu tiên của mật khẩu, kết quả sẽ được đặt vào 16 byte đầu tiên của trường giá trị của thuộc tính user-password.

Công Thức Mã Hóa Password

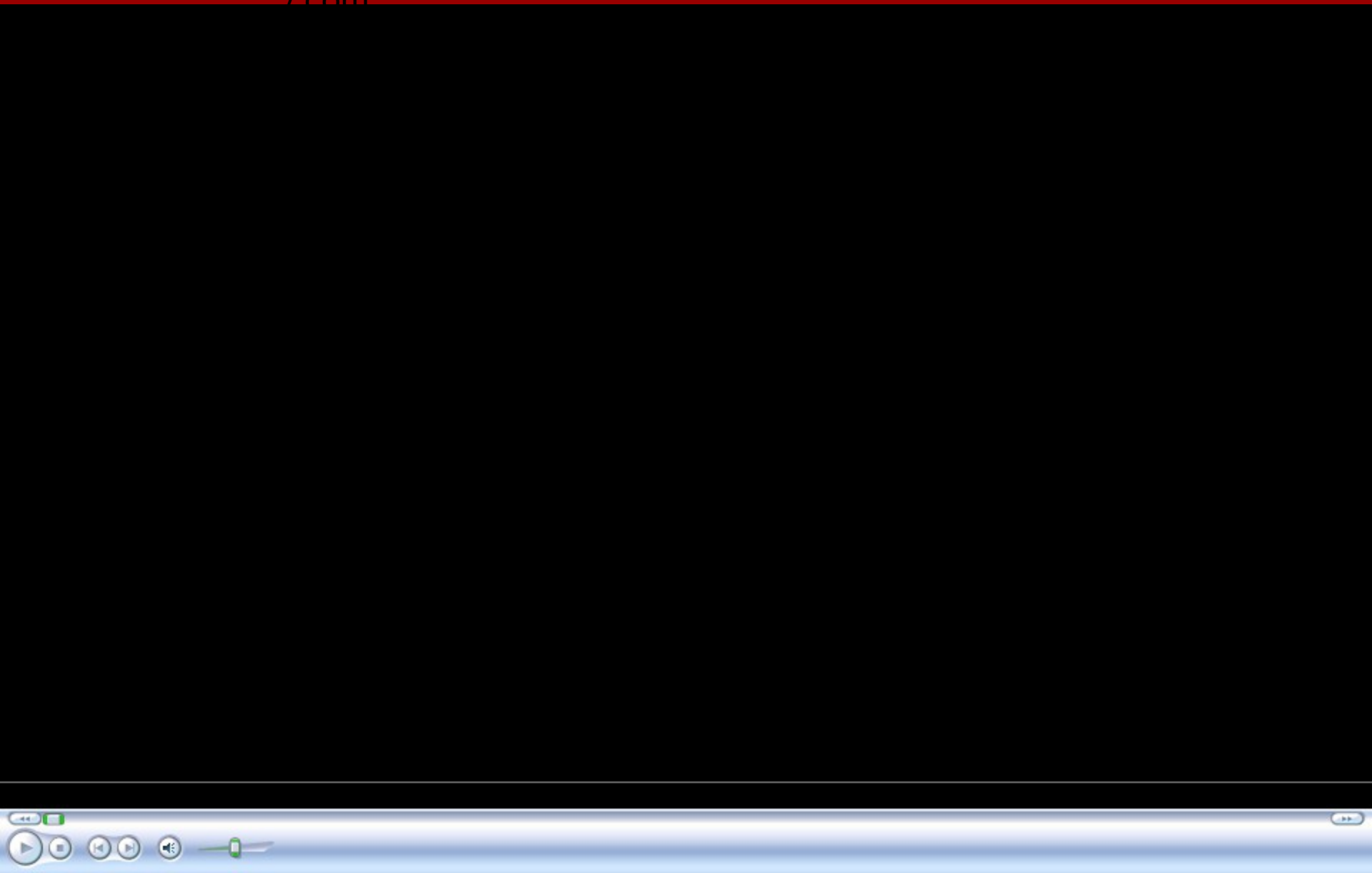
b1 = MD5(S + RA)	c(1) = p1 xor b1
b2 = MD5(S + RA)	c(2) = p2 xor b2
b3 = MD5(S + RA)	c(3) = p3 xor b3
.	.
.	.
.	.
.	.

b1 b2 b3 phụ thuộc vào chiều dài của mật khẩu (tối đa 128 ký tự)

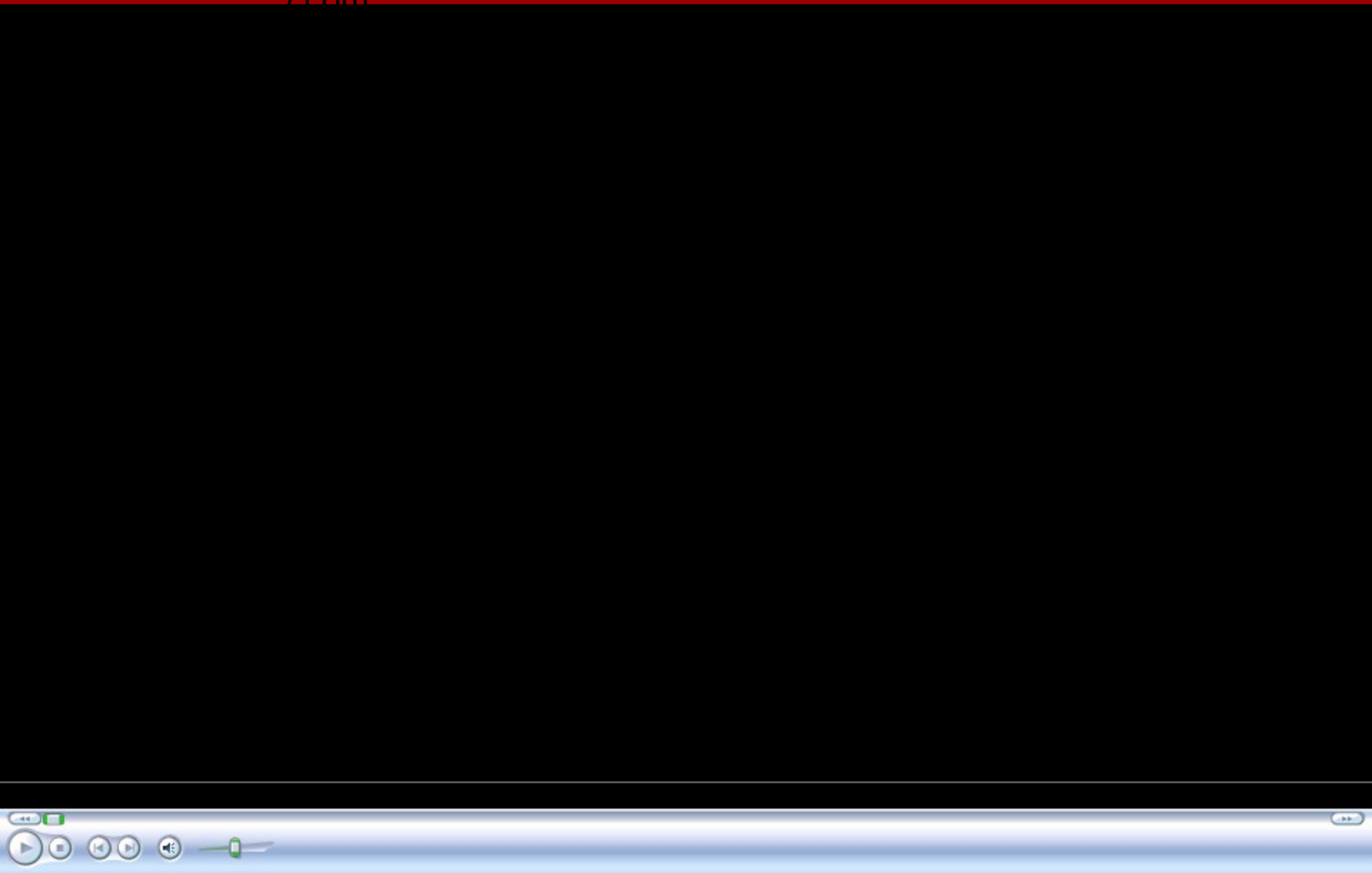
KẾT QUẢ THỰC NGHIỆM CÁC BƯỚC THỰC HIỆN TRÊN AD

/ com

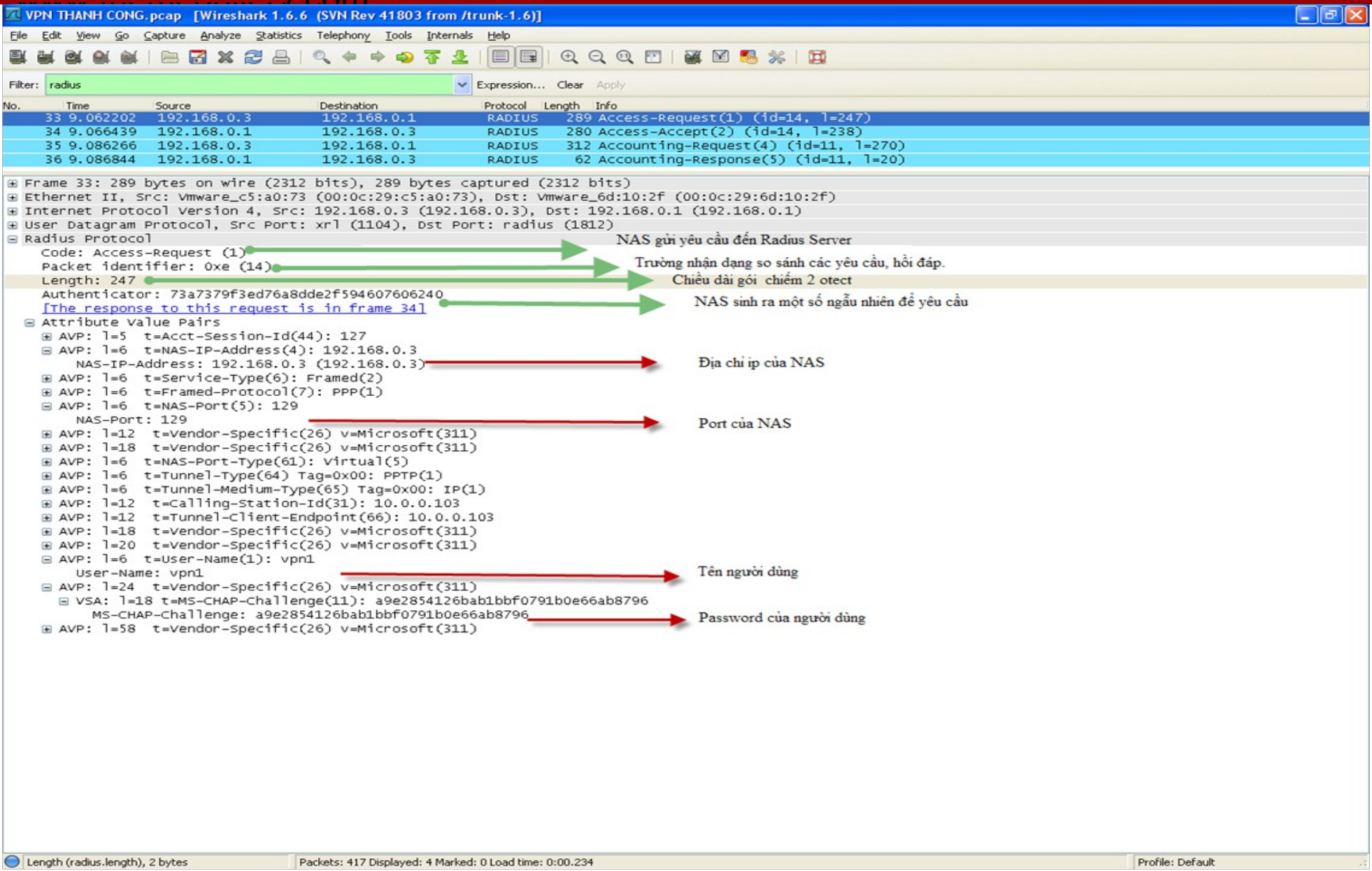
KẾT QUẢ THỰC NGHIỆM
CÁC BƯỚC THỰC HIỆN TRÊN NAS



KẾT QUẢ THỰC NGHIỆM
KẾT QUẢ QUAY VPN THÀNH CÔNG



KẾT QUẢ PHÂN TÍCH GÓI ACCESS REQUEST



PHÂN TÍCH CÁC TRƯỜNG TRONG GÓI ACCESS REQUEST


```
Code: Access-Request (1)
Packet identifier: 0xe (14)
Length: 247
Authenticator: 73A7379F3ED76A8DDE2F59460760624O
[The response to this request is in frame 34]
```

Code field: Khi user vpn vào NAS thì lúc đó NAS chuyển các thông tin của user đến Radius Server, với code = 1 nghĩa là NAS gửi yêu cầu đến radius server

Packet identifier: là trường nhận dạng, trướng này có chiều dài 1 otect, , mục đích của trường này lá để so sánh với những yêu cầu, trả lời. Địa chỉ nguồn, cổng Udp của Client được sử dụng để so sánh cho nhận dạng này.

Length: chiều dài gói tin chiếm 2 otects. Tất cả các gói tin radius có các trường: mã, nhận dạng, chiều dài, và trường xác thực, chiều dài thấp nhất của gói tin là 20 otects vì vậy giá trị thấp nhất của chiều dài là 20, giá trị lớn nhất là 4096. ……..

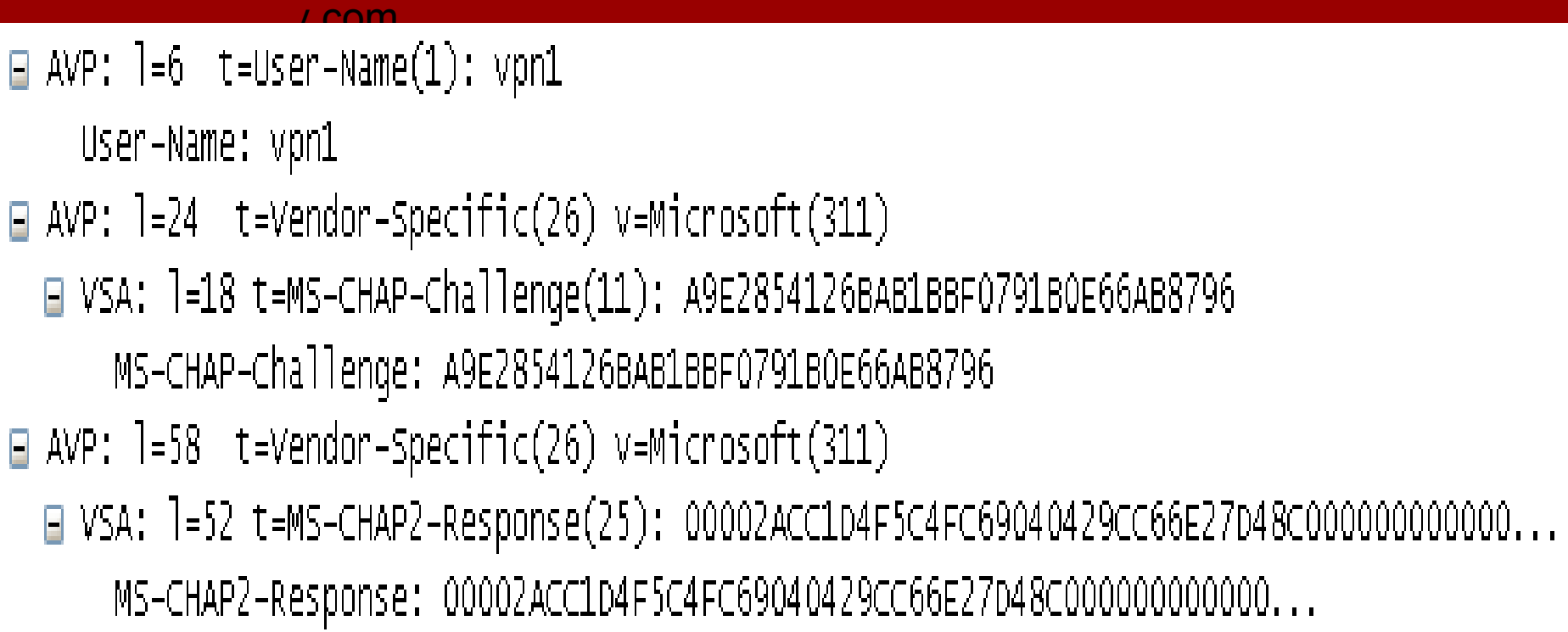
Authenticator: là trường xác thực. trường này có 16 otect và hầu hết là các otect quan trọng . Nó trả lời việc xác thực từ radius server đến nas, và cũng sử dụng để mã hóa các thuộc tính pass người dùng.

PHÂN TÍCH CÁC TRƯỜNG TRONG GÓI ACCESS REQUEST

```
AVP: l=6  t=NAS-IP-Address(4): 192.168.0.3
  NAS-IP-Address: 192.168.0.3 (192.168.0.3)
AVP: l=6  t=Service-Type(6): Framed-User(2)
  Service-Type: Framed-User (2)
AVP: l=6  t=Framed-Protocol(7): PPP(1)
  Framed-Protocol: PPP (1)
AVP: l=6  t=NAS-Port(5): 129
  NAS-Port: 129
```

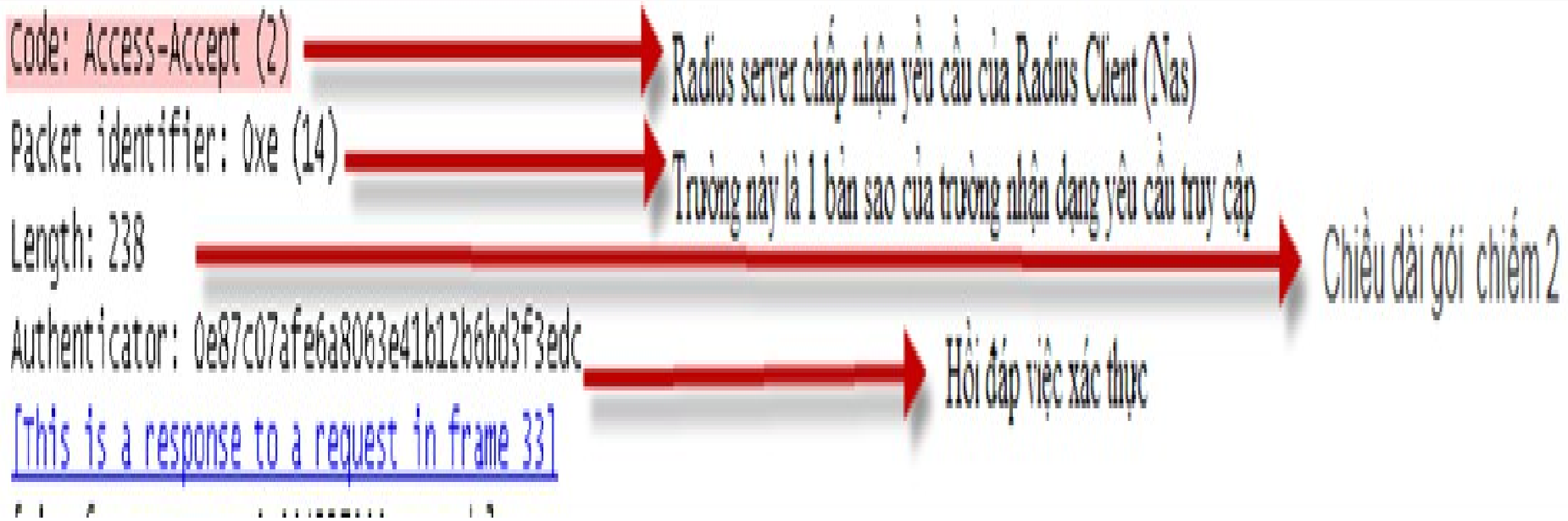
Trong đó NAS-IP-Address: trường mô tả địa chỉ ip của Radius client
Service type: Là trường mô tả loại dịch vụ được yêu cầu bởi người dùng
Frame protocol: Trường mô tả giao thức kết nối
NAS port: Là trường mô tả cổng mà NAS sử dụng để tạo kết nối đến Radius server

PHÂN TÍCH CÁC TRƯỜNG TRONG GÓI ACCESS REQUEST



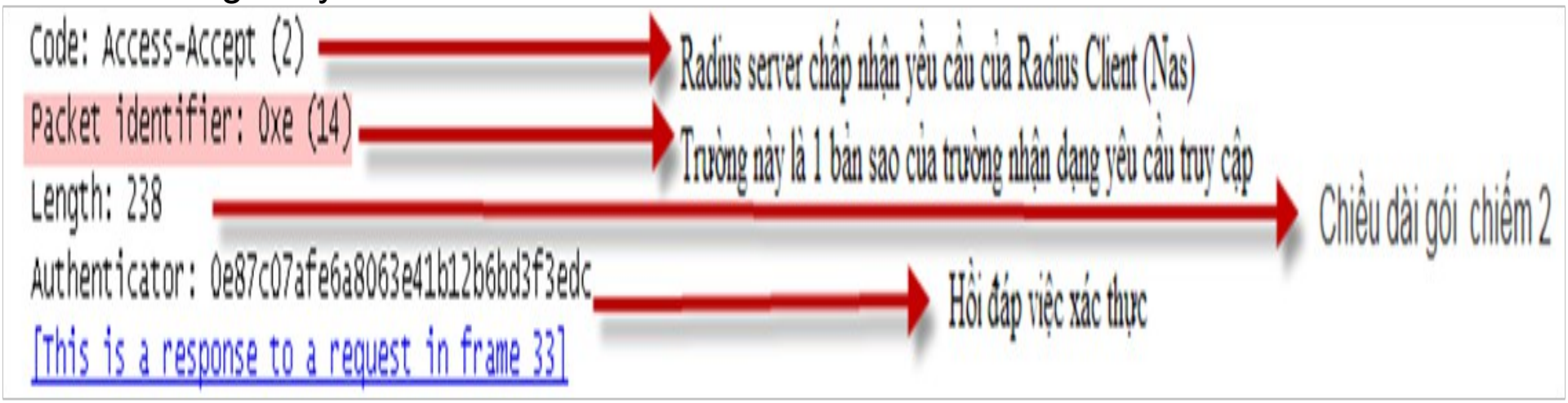
Trong đó **User – name** là thông tin tài khoản người dùng
MS – CHAP – Challenge là trường password của người dùng được mã hóa.

PHÂN TÍCH GÓI ACCESS ACCEPT



Gói tin access- accept được gửi bởi radius server, và được Raidius server cung cấp thông tin cấu hình cần thiết để bắt đầu phân phát dịch vụ cho người dùng. Nếu tất cả giá trị thuộc tính đã nhận được trong access request được chấp nhận thì Radius cần thực hiện truyền gói tin với code bằng 2

CÁC TRƯỜNG TRONG GÓI ACCESS ACCEPT



Trường nhận dạng của gói access accept là một bản sao của trường nhận dạng Access Request

Length là trường chiều dài của gói access accept

Trường Authenticator dùng để xác nhận mã nhận dạng gói tin, chiều dài gói, mã bí mật và các thuộc tính mà người dùng đã gửi trong gói access request …

KẾT QUẢ PHÂN TÍCH GÓI ACCESS ACCOUNTING

35 9.086266	192.168.0.3	192.168.0.1	RADIUS	Accounting-Request(4) (id=11, l=270)
36 9.086844	192.168.0.1	192.168.0.3	RADIUS	Accounting-Response(5) (id=11, l=20)

```
⊞ AVP: l=6  t=Acct-Delay-Time(41): 0
⊟ AVP: l=6  t=NAS-IP-Address(4): 192.168.0.3
    NAS-IP-Address: 192.168.0.3 (192.168.0.3)
⊞ AVP: l=6  t=Service-Type(6): Framed-User(2)
⊞ AVP: l=6  t=Framed-Protocol(7): PPP(1)
⊞ AVP: l=6  t=NAS-Port(5): 129
⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
⊞ AVP: l=18  t=Vendor-Specific(26) v=Microsoft(311)
⊞ AVP: l=6  t=NAS-Port-Type(61): Virtual(5)
⊞ AVP: l=6  t=Tunnel-Type(64) Tag=0x00: PPTP(1)
⊞ AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IP(1)
⊞ AVP: l=12  t=Calling-Station-Id(31): 10.0.0.103
⊞ AVP: l=12  t=Tunnel-Client-Endpoint(66): 10.0.0.103
⊟ AVP: l=18  t=Vendor-Specific(26) v=Microsoft(311)
  ⊞ VSA: l=12 t=Unknown-Attribute(35): 4D5352415356352E3130
⊟ AVP: l=20  t=Vendor-Specific(26) v=Microsoft(311)
  ⊞ VSA: l=14 t=Unknown-Attribute(34): 4D535241532D302D4B543035
⊞ AVP: l=32  t=Class(25): 468704CC000001370001C0A8000101CD1C7C4361E9280000...
⊟ AVP: l=15  t=Vendor-Specific(26) v=Microsoft(311)
  ⊞ VSA: l=9 t=MS-CHAP-Domain(10): \000DOMAIN
⊞ AVP: l=5  t=Acct-Session-Id(44): 127
⊟ AVP: l=6  t=User-Name(1): vpn1
    User-Name: vpn1
⊞ AVP: l=6  t=Framed-IP-Address(8): 192.168.0.106
⊞ AVP: l=6  t=Framed-MTU(12): 1400
⊞ AVP: l=4  t=Acct-Multi-Session-Id(50): 23
⊞ AVP: l=6  t=Acct-Link-Count(51): 1
⊞ AVP: l=6  t=Event-Timestamp(55): Apr 17, 2012 16:52:34.000000000
⊟ AVP: l=6  t=Acct-Authentic(45): RADIUS(1)
    Acct-Authentic: RADIUS (1)
⊟ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
  ⊞ VSA: l=6 t=MS-MPPE-Encryption-Types(8): RC4-128(4)
```

KẾT QUẢ THỰC NGHIỆM PHÂN TÍCH GÓI ACCESS ACCOUNTING

Sau khi xác thực người dùng NAS gửi gói yêu cầu kiểm toán đến Radius server để kiểm toán những dịch vụ được yêu cầu bởi người dùng.

Khi nhận gói yêu cầu kiểm toán Radius server sẽ ghi lại những dịch vụ, thuộc tính và các thông tin cần xác thực của người dùng để bắt đầu quá trình kiểm toán.

Sau đó Radius server sẽ gửi gói trả lời đáp ứng yêu cầu kiểm toán đến NAS