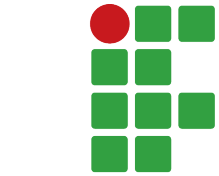


INSTITUTO FEDERAL
Santa Catarina

Câmpus
São José

Procotolo RADIUS

Projeto Final de Redes I

Arthur Cadore Matuella Barcella

Gabriel Luiz Espindola Pedro

Matheus Pires Salazar

22 de novembro de 2022

Sumário

1 Introdução

1.1 Motivação

A motivação por trás do estudo e teste com RADIUS é sua versatilidade para a implementação de redes seguras através da criação de credenciais individuais para cada usuário que permitem um maior controle de quem pode ou não acessar a rede, além de também, tornar a rede muito menos suscetível a ataques aos usuários (como ataques DoS ou packet sniffering).

Dessa forma, redes corporativas, como redes escolares, shoppings, empresas de médio e grande porte, podem utilizar deste protocolo as suas ferramentas e serviços para controlar o acesso dos dispositivos finais a rede.

2 Fundamentação teórica

Segundo o instituto de engenheiros eletricistas e eletrônicos (IEEE), o padrão IEEE 802.X é utilizado com o objetivo de fornecer mecanismos de autenticação, autorização e controle de acesso a dados criticos em redes de computadores.

O controle de acesso através da autenticação 802.1X (tanto através da autenticação estendida "EAP"ou através do meio guiado "Port Based", permite que o administrador da rede proteja os dados dos usuários finais e a comunicação entre dispositivos na rede local que estão devidamente autorizados e autenticados.

3 RADIUS

3.1 O que é?

O protocolo RADIUS é um protocolo para autenticação de dispositivos que opera em topologia cliente e servidor. Para que o cliente possa se conectar a rede, é necessário que ele informe seus dados de acesso, e o servidor RADIUS verifique tais informações passadas.

Um servidor RADIUS regula o acesso à rede verificando a identidade dos usuários através das credenciais de login inseridas.

Por exemplo, uma rede Wi-Fi pública é instalada em um campus universitário. Apenas os alunos que têm a senha podem acessar essas redes. Diferentemente de uma rede convencional, onde o usuário simplesmente utiliza a senha da rede, em uma rede wifi com radius implementado, o cliente precisa realizar uma autenticação estendida.

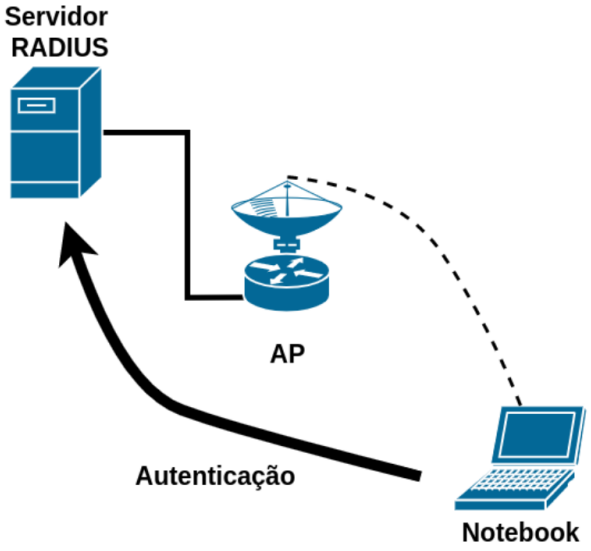


Figura 1: Topologia de autenticação com o protocolo RADIUS

Ao aplicarmos a autenticação via RADIUS em uma rede wireless convencional, necessitamos de uma ponte entre o dispositivo final e o servidor, essa ponte é denominada NAS (Network Access Server). Um dispositivo NAS nada mais é do que um produto que opera como intermediário em uma rede local redirecionando as solicitações feitas pelo cliente e as encaminhando para o servidor fazer a verificação.

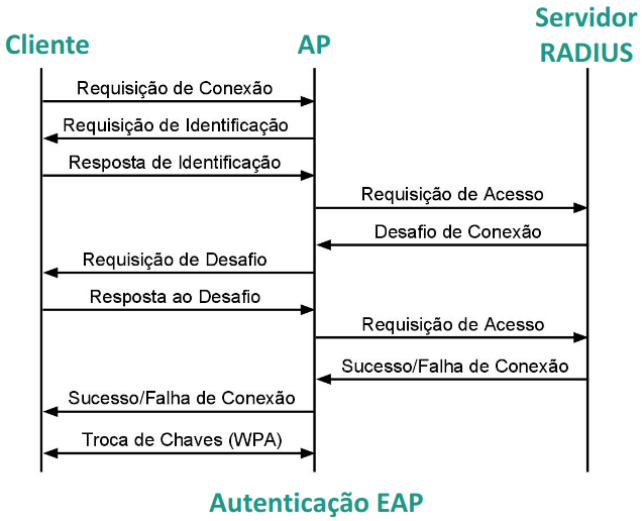


Figura 2: Processo de autenticação entre cliente, NAS e servidor

Quando uma solicitação é recebida no servidor RADIUS, este verifica os dados encaminhados pelo dispositivo NAS (originados no cliente), e então, dispara um "desafio"ao cliente para testar se este dispositivo tem de fato uma senha de acesso válida.

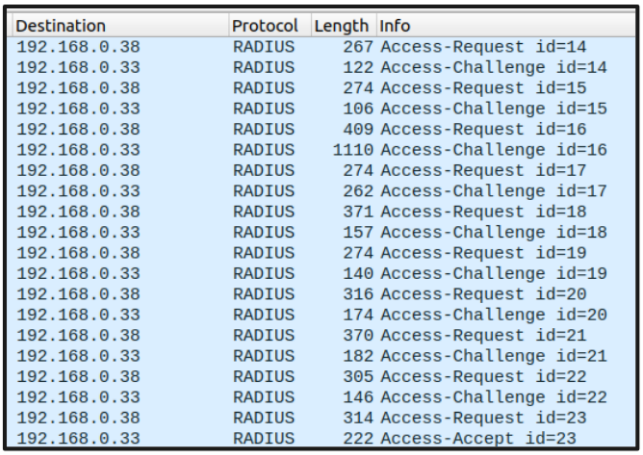
O pacote de desafio originado no servidor RADIUS contem uma hash (código aletatório) que irá ser encaminhada ao cliente. Uma vez que o cliente receber essa hash dada pelo servidor, o cliente utiliza sua senha para gerar outra hash (uma hash de resposta).

Esta hash de resposta é gerada através da combinação da hash original (enviada pelo servidor RADIUS) com a senha que foi passada pelo usuário do dispositivo. Durante esse processo, o servidor realiza o mesmo calculo com a senha do usuário que já está contida em seu banco de dados.

Quando o computador envia sua hash de resposta ao NAS e ele a re-encaminha ao servidor

RADIUS, o servidor compara a hash encaminhada pelo cliente com a que calculou. Caso os valores estejam iguais, o cliente passa no desafio feito pelo servidor. Caso não estejam, o servidor rejeita a conexão.

O protocolo de autenticação através de desafio é denominado CHAP (Challange-Handshake Authentication Protocol), este protocolo é utilizado como base para o servidor RADIUS garantir a autenticidade dos clientes, visto que o RADIUS o implementa para garantir que o cliente deve passar por vários desafios antes de iniciar uma conexão com a rede de fato.



Destination	Protocol	Length	Info
192.168.0.38	RADIUS	267	Access-Request id=14
192.168.0.33	RADIUS	122	Access-Challenge id=14
192.168.0.38	RADIUS	274	Access-Request id=15
192.168.0.33	RADIUS	106	Access-Challenge id=15
192.168.0.38	RADIUS	409	Access-Request id=16
192.168.0.33	RADIUS	1110	Access-Challenge id=16
192.168.0.38	RADIUS	274	Access-Request id=17
192.168.0.33	RADIUS	262	Access-Challenge id=17
192.168.0.38	RADIUS	371	Access-Request id=18
192.168.0.33	RADIUS	157	Access-Challenge id=18
192.168.0.38	RADIUS	274	Access-Request id=19
192.168.0.33	RADIUS	140	Access-Challenge id=19
192.168.0.38	RADIUS	316	Access-Request id=20
192.168.0.33	RADIUS	174	Access-Challenge id=20
192.168.0.38	RADIUS	370	Access-Request id=21
192.168.0.33	RADIUS	182	Access-Challenge id=21
192.168.0.38	RADIUS	305	Access-Request id=22
192.168.0.33	RADIUS	146	Access-Challenge id=22
192.168.0.38	RADIUS	314	Access-Request id=23
192.168.0.33	RADIUS	222	Access-Accept id=23

Figura 3: Protocolo CHAP.

Durante a autenticação do usuário o CHAP orienta o servidor RADIUS a realizar diversos desafios com o cliente para garantir que a chave utilizada pelo cliente está de fato correta.

Uma vez com a autenticação já finalizada o protocolo RADIUS informa o dispositivo NAS que a conexão do cliente final foi liberada. Quando o dispositivo NAS recebe essa informação, ele inicia o processo padrão de autenticação do cliente em uma rede wireless, entretanto, o cliente não necessita adicionar a senha uma vez que tenha sido liberado pelo RADIUS, isso pelo fato do servidor RADIUS já informar ao dispositivo NAS sobre o acesso do produto a rede.

3.2 Funcionamento:

Para entendermos as vantagens e desvantagens do protocolo RADIUS em relação a uma rede com senha simples (autenticação Pre-Shared Key ou PSK), vamos primeiro entender o funcionamento do RADIUS para a autenticação dos clientes finais na wireless.

Antes de iniciar a autenticação, o celular identifica a rede em que está tentando se conectar, o Access Point informa que está utilizando RADIUS para a autenticação, essa informação é evidente para o cliente através do pacote de beacon frame, que é transmitido periodicamente na wireless para avisar os dispositivos próximos que uma rede está hospedada e suas capacidades.

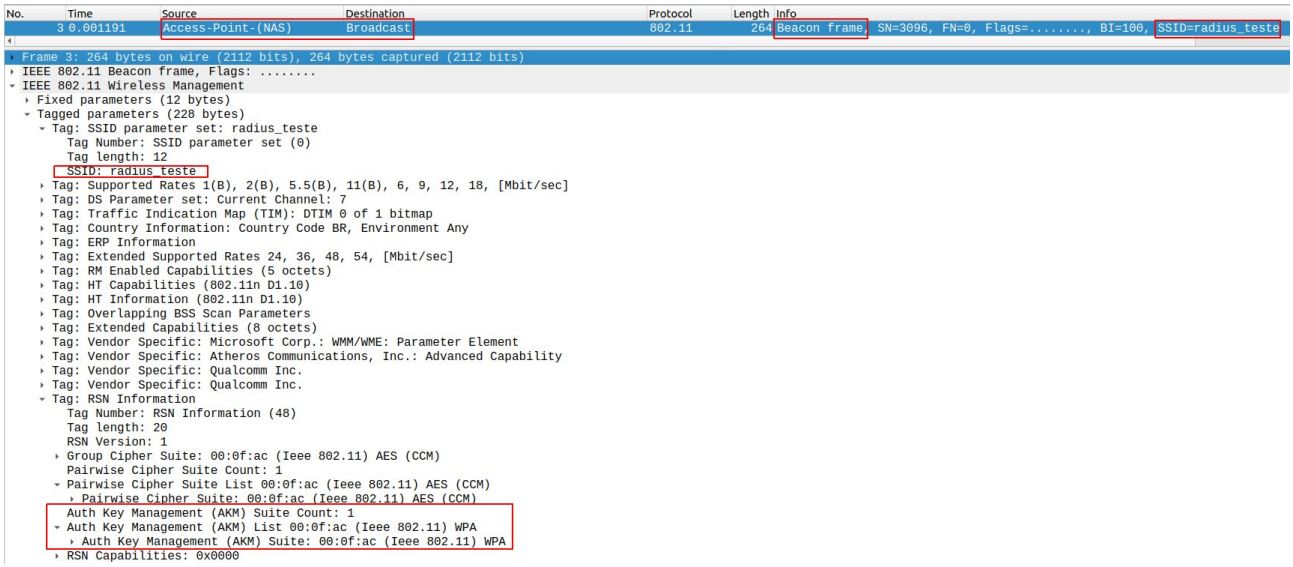


Figura 4: Beacon Frame feito pelo Access Point

Inicialmente o dispositivo cliente (um celular ou notebook por exemplo), realiza uma solicitação de conexão com o Access Point mais próximo. Para realizar a solicitação, o dispositivo final encaminha uma mensagem de "Association Request"para o Access Point.

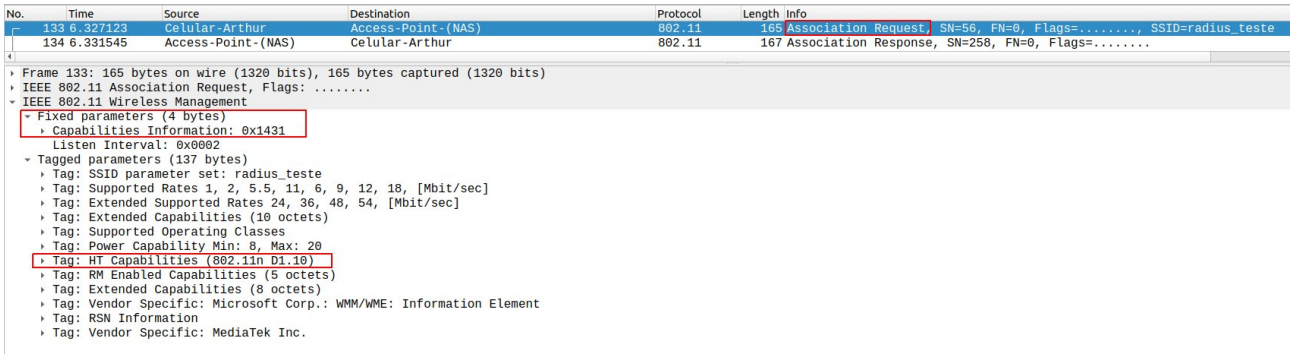


Figura 5: Association Request feito pelo dispositivo final

Ao realizar a solicitação, o dispositivo NAS responde com todos os parâmetros de conexão necessários para que o cliente possa se conectar, dentro da mensagem de resposta, são encaminhadas as informações de capacidade de Hardware "HT Capabilities"e dados de sessão "BSS"responsável pelo gerenciamento das conexões wireless do Access Point. O pacote encaminhado pelo Access Point é denominado "Association Response".

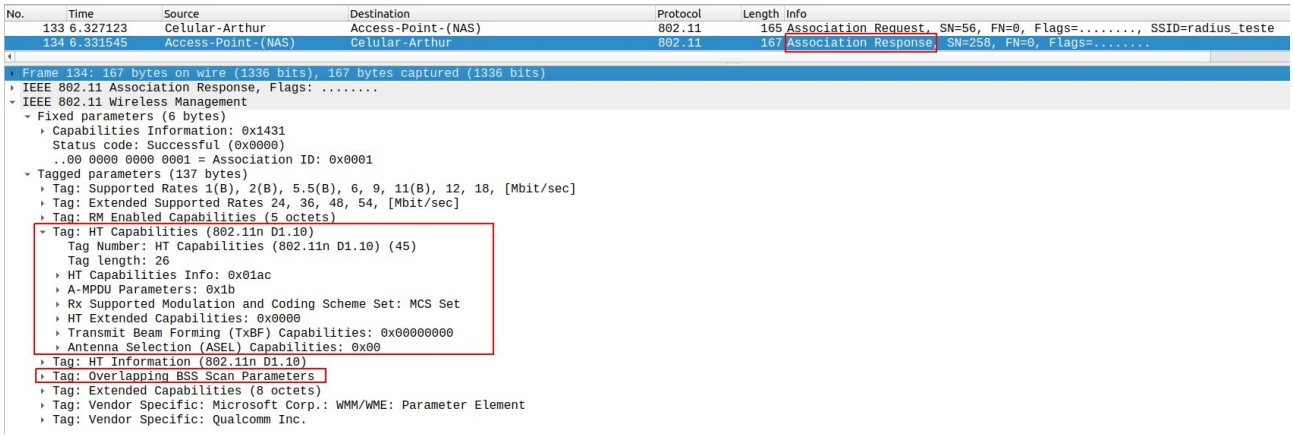


Figura 6: Association Response feito pelo Access Point

Em seguida, o cliente solicita se associar ao SSID "radius-teste"(que utilizamos para os testes e capturas), para isso, o cliente encaminha um pacote ao Access Point solicitando se tornar um vizinho da rede "radius-teste", através da ação "Neighbour Report Request"

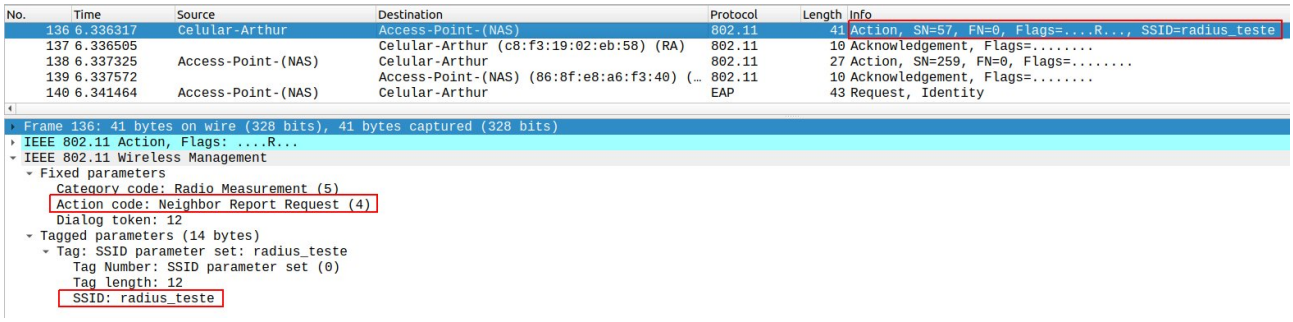


Figura 7: Neighbour Report Request feito pelo dispositivo final

O Access Point então (operando como dispositivo NAS) solicita os dados de identificação do dispositivo final. Como o Access Point já anuncia que a rede possui autenticação estendida, o dispositivo cliente aguarda a solicitação feita pelo Access point. Através dessa solicitação, o cliente informará seus dados em um pacote de resposta (como por exemplo o nome de usuário, email, telefone, entre outros).

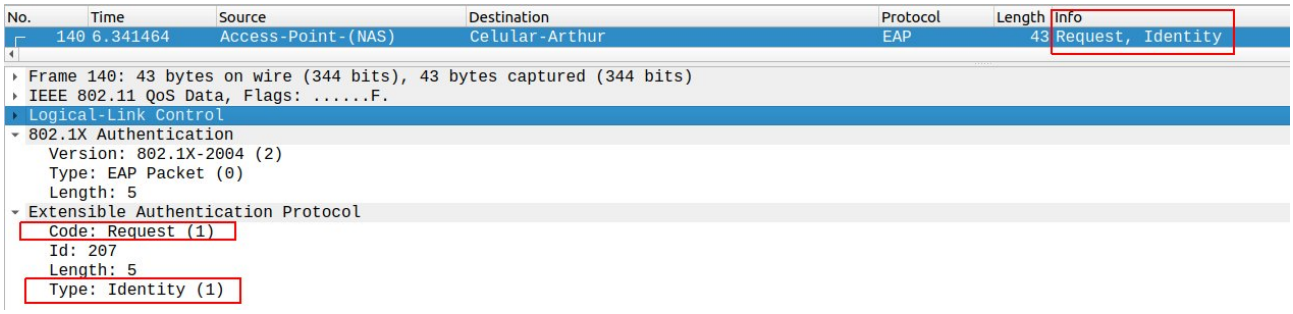


Figura 8: Request Identity feito pelo Access Point

O cliente então responde a solicitação feita pelo dispositivo NAS com os dados necessários para validação (dados que foram informados pelo usuário administrador do sistema), e então, o dispositivo NAS opera como um "intermediário"reencaminhado esses dados para o servidor RADIUS da rede local. No caso deste teste, foi utilizado apenas um parâmetro de identificação, dessa forma, na capturas só irá aparecer o usuário de teste.

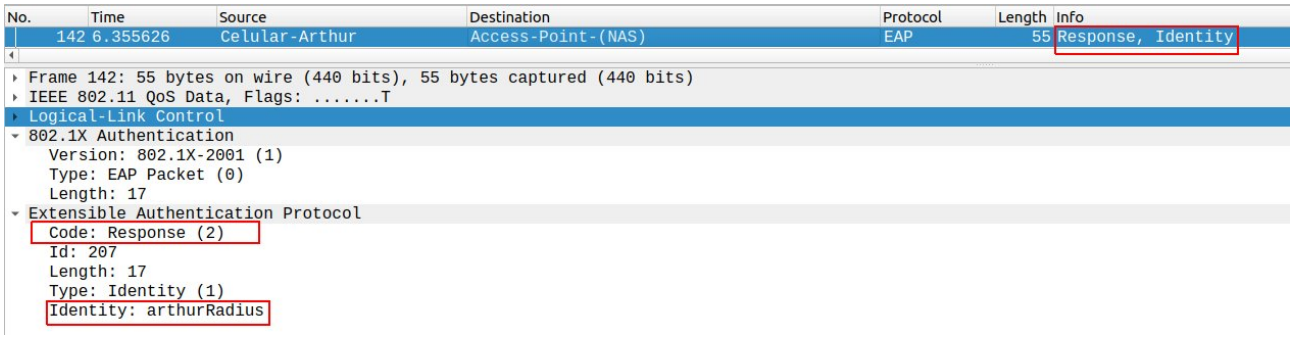


Figura 9: Response Identity feito pelo dispositivo final

No reencaminhamento, o NAS adiciona parâmetros de identificação para que o servidor possa identificar o próprio NAS, e confirmar a autenticidade do NAS que está encaminhando a informação (para evitar possíveis ataques ao servidor, como ataques de negação de serviço "DoS"ou liberação incorreta de clientes).

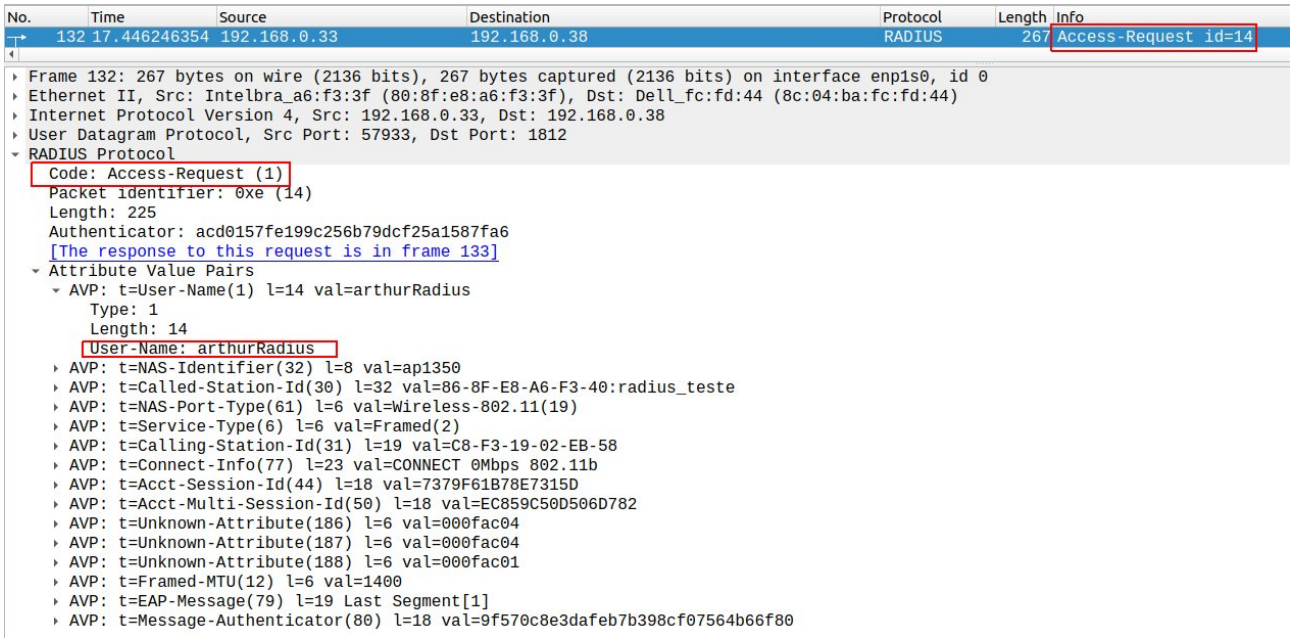


Figura 10: Access Request (NAS Encaminhando para o servidor)

O servidor então, ao receber a solicitação feita pelo cliente e verificar os dados passados em seu banco de dados, onde o objetivo é identificar se os dados de usuário encaminhado pelo NAS constam no banco de dados (onde o cliente já deve possuir previamente esses dados e também a senha).

```
MariaDB [radiusdb]> DESCRIBE userinfo;
+---------------------+------------------+------+-----+---------------------+----------------+
| Field               | Type             | Null | Key | Default             | Extra          |
+---------------------+------------------+------+-----+---------------------+----------------+
| id                  | int(11) unsigned | NO   | PRI | NULL                | auto_increment |
| username            | varchar(128)     | YES  | MUL | NULL                |                |
| firstname           | varchar(200)     | YES  |     | NULL                |                |
| lastname            | varchar(200)     | YES  |     | NULL                |                |
| email               | varchar(200)     | YES  |     | NULL                |                |
| department          | varchar(200)     | YES  |     | NULL                |                |
| company             | varchar(200)     | YES  |     | NULL                |                |
| workphone           | varchar(200)     | YES  |     | NULL                |                |
| homephone           | varchar(200)     | YES  |     | NULL                |                |
| mobilephone         | varchar(200)     | YES  |     | NULL                |                |
| address             | varchar(200)     | YES  |     | NULL                |                |
| city                | varchar(200)     | YES  |     | NULL                |                |
| state               | varchar(200)     | YES  |     | NULL                |                |
| country             | varchar(100)     | YES  |     | NULL                |                |
| zip                 | varchar(200)     | YES  |     | NULL                |                |
| notes               | varchar(200)     | YES  |     | NULL                |                |
| changeuserinfo      | varchar(128)     | YES  |     | NULL                |                |
| portalloginpassword | varchar(128)     | YES  |     |                     |                |
| enableportallogin   | int(32)          | YES  |     | 0                   |                |
| creationdate        | datetime         | YES  |     | 0000-00-00 00:00:00 |                |
| creationby          | varchar(128)     | YES  |     | NULL                |                |
| updatedate          | datetime         | YES  |     | 0000-00-00 00:00:00 |                |
| updateby            | varchar(128)     | YES  |     | NULL                |                |
+---------------------+------------------+------+-----+---------------------+----------------+
23 rows in set (0,002 sec)
```

Figura 11: Tabela de informações de usuários no banco de dados do RADIUS

Caso o usuário exista, o servidor cria uma hash (um código, tipicamente no padrão MD5), envia uma resposta para o dispositivo NAS que é endereçada ao dispositivo final (cliente solicitante). Nessa mensagem está contida a hash MD5, este pacote é chamado de "desafio".

```
No.  Time          Source          Destination     Protocol  Length  Info
 133 17.447046711 192.168.0.38    192.168.0.33    RADIUS       122 Access-Challenge id=14

▸ Frame 133: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface enp1s0, id 0
▸ Ethernet II, Src: Dell_fc:fd:44 (8c:04:ba:fc:fd:44), Dst: Intelbra_a6:f3:3f (80:8f:e8:a6:f3:3f)
▸ Internet Protocol Version 4, Src: 192.168.0.38, Dst: 192.168.0.33
▸ User Datagram Protocol, Src Port: 1812, Dst Port: 57933
▾ RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0xe (14)
    Length: 80
    Authenticator: f1154f1e2d7d5b1a4d7c9fbb725cdf1e
    [This is a response to a request in frame 132]
    [Time from request: 0.000800357 seconds]
  ▾ Attribute Value Pairs
    ▾ AVP: t=EAP-Message(79) l=24 Last Segment[1]
        Type: 79
        Length: 24
        EAP fragment: 01d000160410e66238e330424449718ab0da1faaff27
      ▾ Extensible Authentication Protocol
          Code: Request (1)
          Id: 208
          Length: 22
        ▾ Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
          ▸ [Expert Info (Warning/Security): Vulnerable to MITM attacks. If possible, change EAP type.]
          EAP-MD5 Value-Size: 16
          EAP-MD5 Value: e66238e330424449718ab0da1faaff27
    ▸ AVP: t=Message-Authenticator(80) l=18 val=7e661e7b5b7b0f17afdd9be16418fc37
    ▸ AVP: t=State(24) l=18 val=46ef1bce463f1f633e02eaf60df7d252
```

Figura 12: Access Challange encaminhado para o NAS

O objetivo do envio da hash ao cliente é realizar a autenticação do cliente sem que o cliente precise encaminhar a senha pela rede até o servidor para validação (isso é necessário para garantir que nenhum dispositivo realizando sniffering na rede consiga capturar os pacotes com a senha e

descriptografar os pacotes seguintes).

Quando o cliente recebe a hash, ele combina a hash com a senha que o usuário administrador informou, gerando uma nova hash a partir dessa combinação (nessa combinação tipicamente é utilizada a criptografia RC4). Para isso, o dispositivo NAS encaminha a hash gerada pelo servidor para o dispositivo cliente, para que ele possa resolve-la.

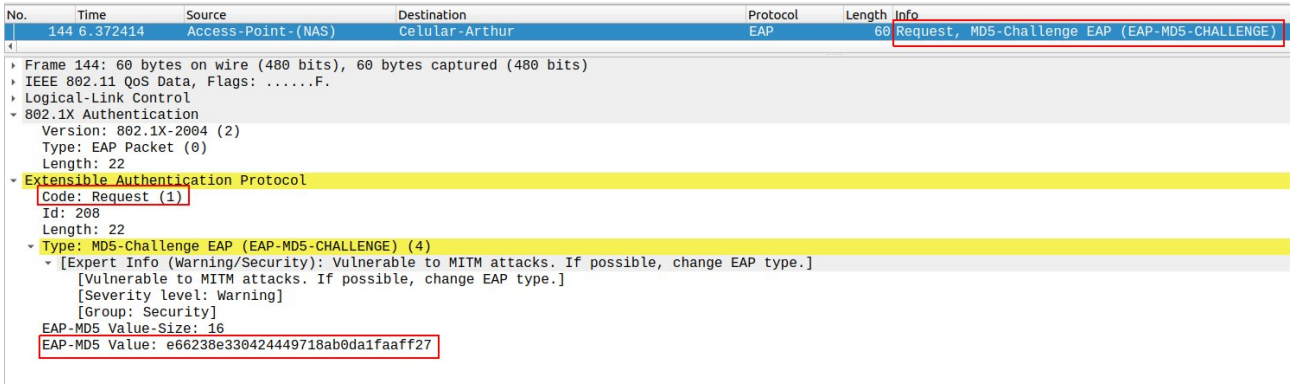


Figura 13: Access Challange (wireless) encaminhado do NAS para o cliente

Com a hash de resposta já pronta, o dispositivo cliente refaz o pacote de solicitação, contendo novamente seus dados de identificação (nome de usuário, email, telefone), e a hash de resposta. Ao mesmo tempo, o servidor RADIUS faz o mesmo calculo para uma hash de resposta igual a do cliente (com a mesma senha a hash será igual, caso a senha esteja errada, as hash serão diferentes).

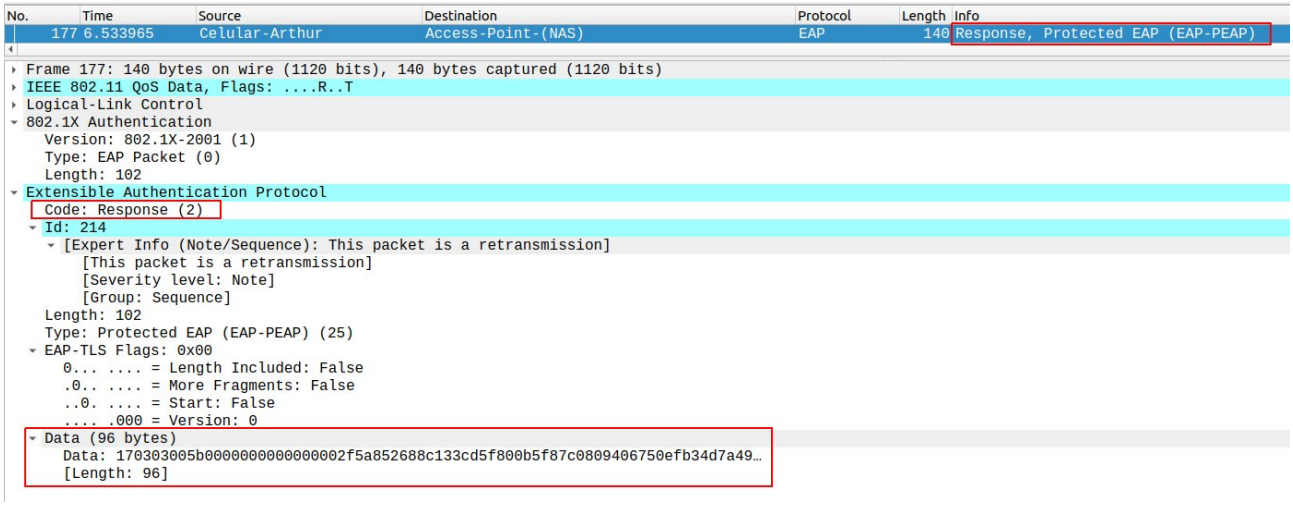


Figura 14: Challange response (wireless) encaminhado do cliente para o NAS

O pacote de resposta é encaminhado novamente para o servidor RADIUS, seguindo o mesmo procedimento visto anteriormente (cliente final -> dispositivo NAS -> servidor RADIUS), realizando uma nova solicitação de conexão de "access request". Quando o pacote com a hash de resposta do cliente chega ao servidor, o servidor compara a hash calculada pelo cliente com a hash que ele calculo, caso sejam iguais, ele entende que a senha é igual, caso sejam diferentes, ele entende que a senha está errada.

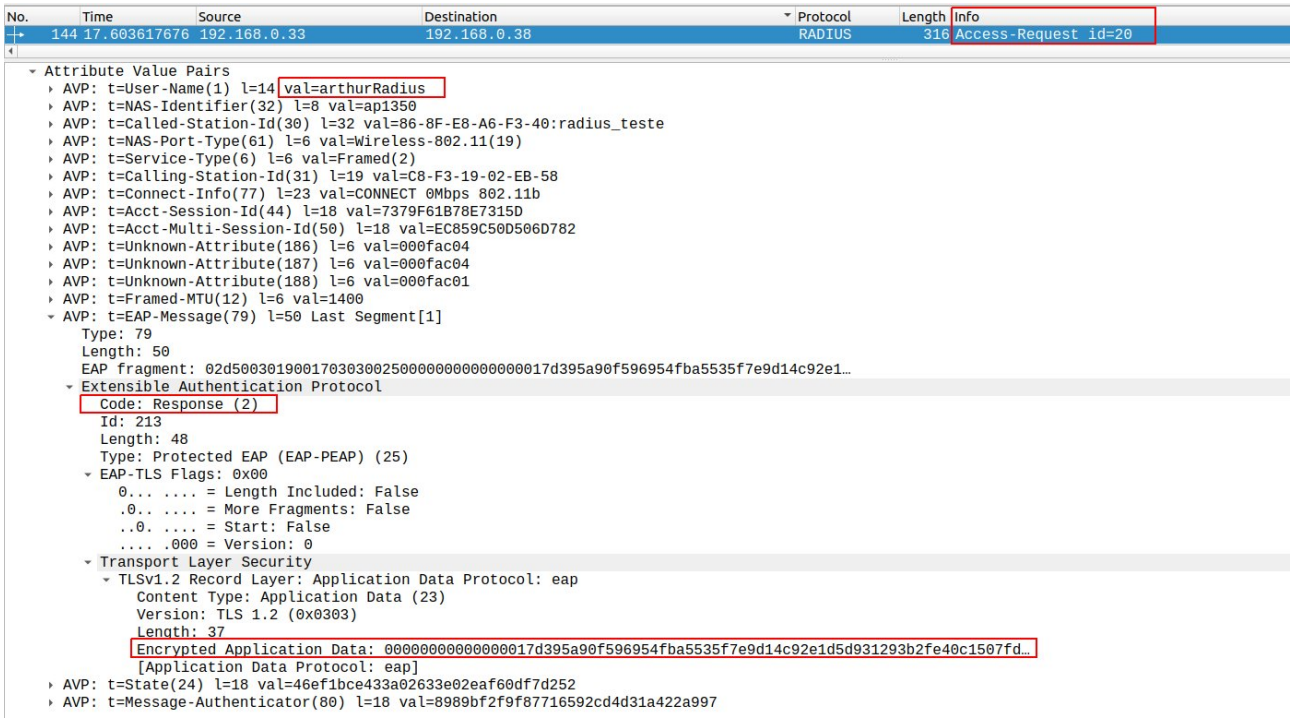


Figura 15: Access Request encaminhado pelo NAS para o servidor

Esse procedimento de comparação de hashes é denominado "desafio", o procedimento de desafio pode-se repetir diversas vezes até que o servidor tenha certeza que a senha do cliente está de fato correto, tipicamente são feitas de 10 á 15 vezes.

No.	Time	Source	Destination	Protocol	Length	Info
132	17.446246354	192.168.0.33	192.168.0.38	RADIUS	267	Access-Request id=14
133	17.447046711	192.168.0.38	192.168.0.33	RADIUS	122	Access-Challenge id=14
134	17.465627306	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=15
135	17.469286364	192.168.0.38	192.168.0.33	RADIUS	106	Access-Challenge id=15
136	17.506784402	192.168.0.33	192.168.0.38	RADIUS	409	Access-Request id=16
137	17.513056586	192.168.0.38	192.168.0.33	RADIUS	1110	Access-Challenge id=16
138	17.544701244	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=17
139	17.545381951	192.168.0.38	192.168.0.33	RADIUS	262	Access-Challenge id=17
140	17.566290920	192.168.0.33	192.168.0.38	RADIUS	371	Access-Request id=18
141	17.567884029	192.168.0.38	192.168.0.33	RADIUS	157	Access-Challenge id=18
142	17.585367722	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=19
143	17.585977752	192.168.0.38	192.168.0.33	RADIUS	140	Access-Challenge id=19
144	17.603617676	192.168.0.33	192.168.0.38	RADIUS	316	Access-Request id=20
145	17.604362896	192.168.0.38	192.168.0.33	RADIUS	174	Access-Challenge id=20
146	17.624778126	192.168.0.33	192.168.0.38	RADIUS	370	Access-Request id=21
147	17.628543440	192.168.0.38	192.168.0.33	RADIUS	182	Access-Challenge id=21
148	17.644319473	192.168.0.33	192.168.0.38	RADIUS	305	Access-Request id=22
149	17.648165190	192.168.0.38	192.168.0.33	RADIUS	146	Access-Challenge id=22
150	17.665125670	192.168.0.33	192.168.0.38	RADIUS	314	Access-Request id=23
151	17.666594950	192.168.0.38	192.168.0.33	RADIUS	222	Access-Accept id=23

Figura 16: Desafios feios pelo servidor RADIUS (mensagens trocadas entre servidor e NAS)

Uma vez que o servidor tenha certeza que a senha do cliente está de fato correta, o servidor envia um pacote de resposta ao NAS e também ao cliente final chamado de "success". Esse pacote informa ao NAS e ao cliente que a conexão foi liberada para que ele e o cliente possam iniciar um procedimento de negociação de chaves WPA.

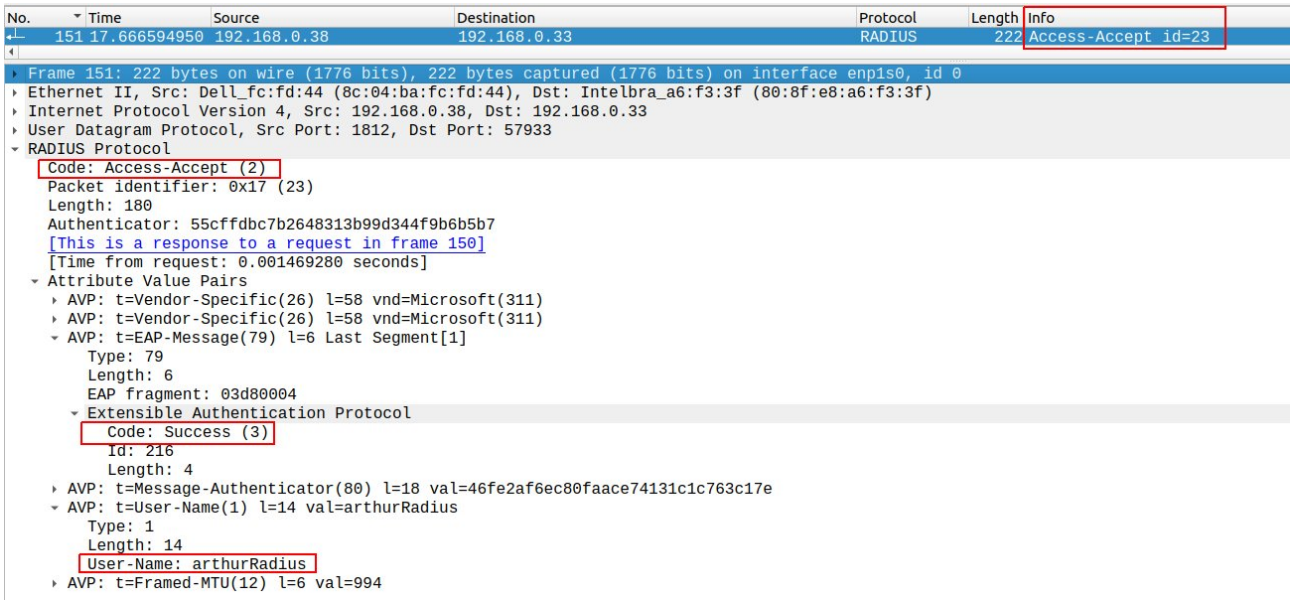


Figura 17: Access Accept enviado pelo servidor RADIUS ao NAS)

Com a autenticação do RAIDUS já finalziada, o Access Point e o dispositivo cliente inciam o processo de troca de chaves WPA. O processo de autenticação WPA é utilizado para negociar chaves de criptografia entre cliente e servidor para garantir que as mensagens enviadas pelo cliente sejam protegidas.

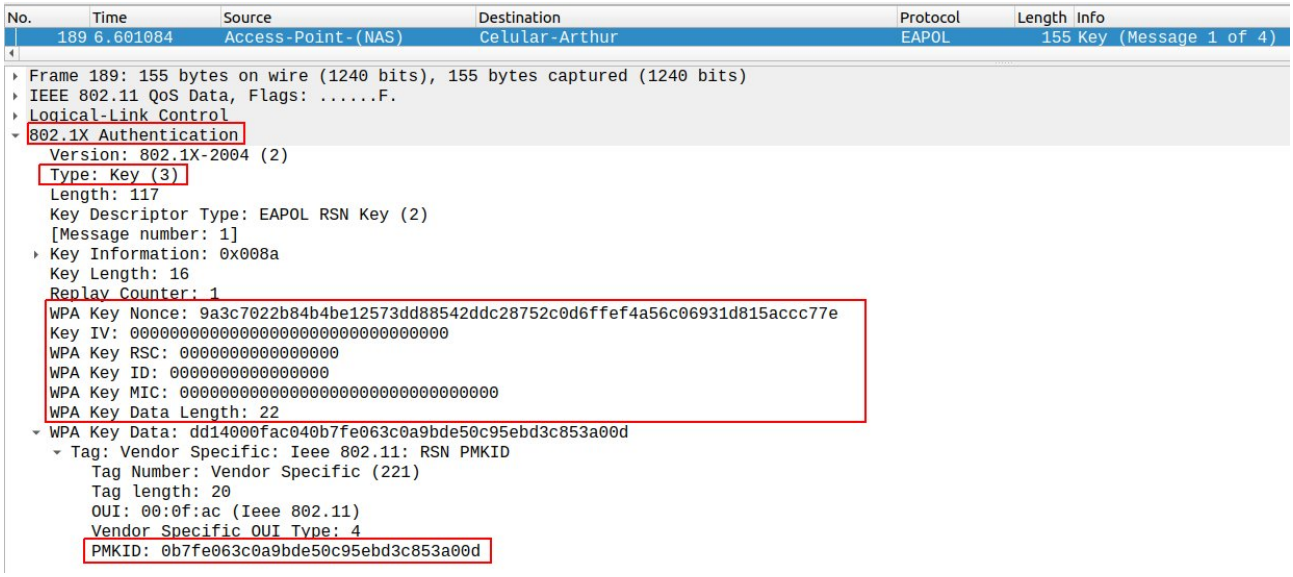


Figura 18: Primeiro pacote de negociação WPA negociado entre Access Point e cliente

O processo de negociação de chaves WPA é dividido em 4 partes, em cada sessão, os dispositivos negociam chaves de criptografia diferentes, onde as primeiras sessões são negociadas chaves base como a "Pairwise Master Key"ou PMK, para gerar as demais chaves.

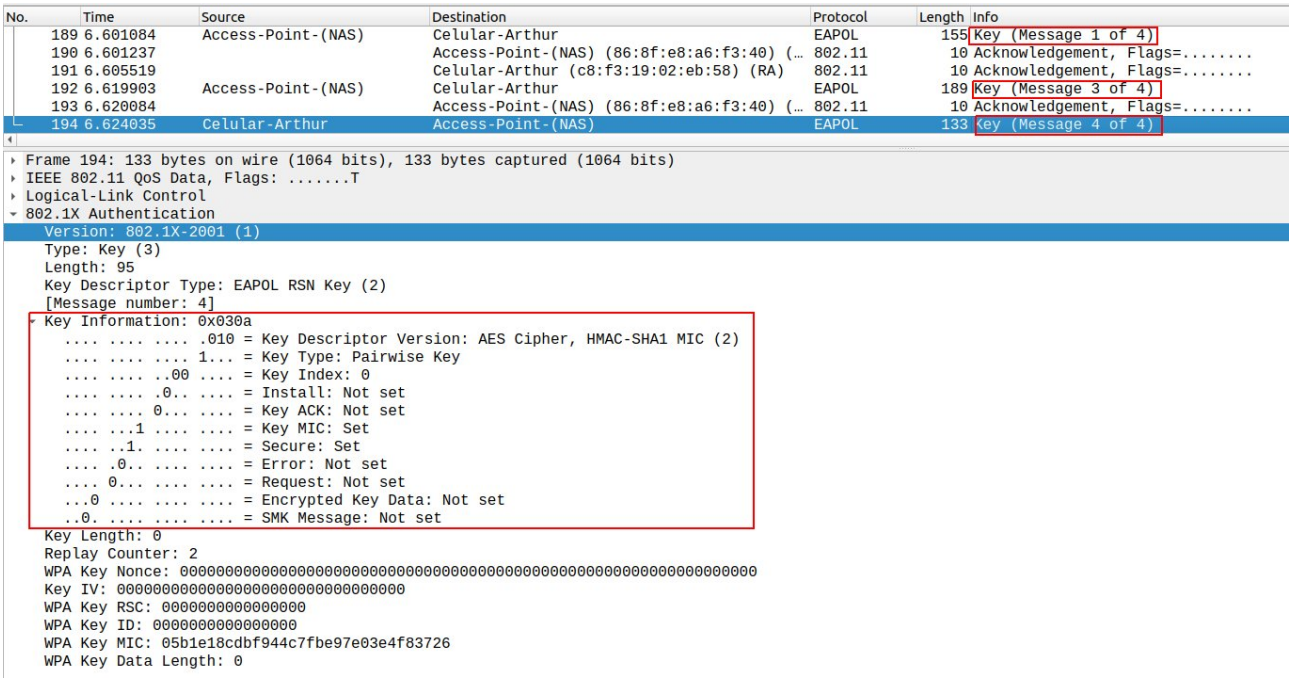


Figura 19: Ultimo pacotete de negociação WPA entre Access Point e cliente

Observação: Na captura wireless, o dispositivo realizando sniferring não capturou o pacote de negociação número 2. Foram capturados apenas os pacotes 1, 3 e 4 respectivamente, dessa forma, estão exibidos apenas esses pacotes na captura.

Com as chaves de criptografia já estabelecidas entre cliente e servidor, a autenticação entre cliente e access point foi finalizada, e dispositivo cliente pode iniciar o tráfego de dados entre cliente e servidor.

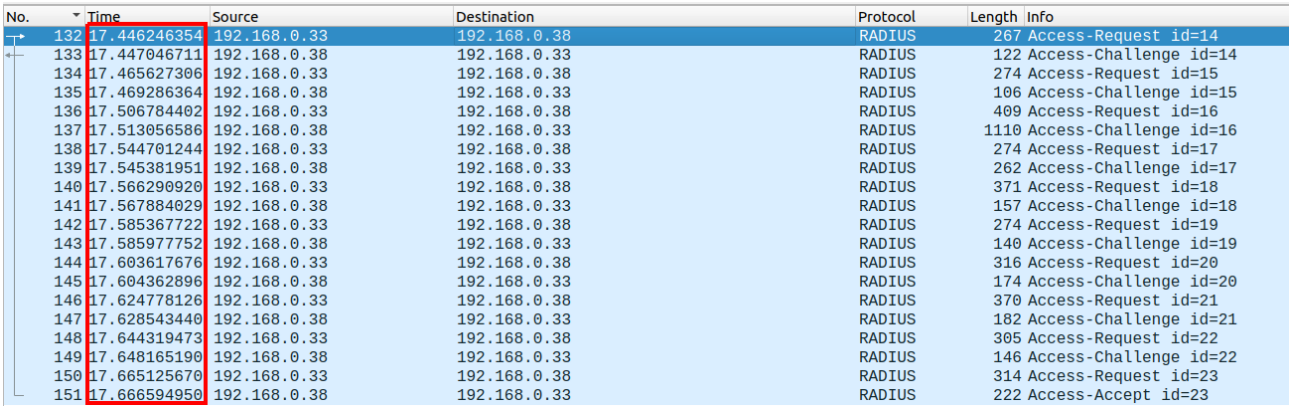
3.3 Vantagens

A maneira como a autenticação via RADIUS ocorre (topologia cliente / servidor) pode-se adotar como uma das grandes vantagens do uso do protocolo RADIUS para autenticação estendida na wireless ao compararmos com a troca de chaves PSK no padrão WPA, WPA2 ou WPA3, pois como em nenhum momento a chave foi encaminhada através da wireless.

Dessa forma, a segurança no momento de acessar a rede é maior, pois caso um dispositivo tente capturar os pacotes trafegados na wireless, este não conseguirá obter a chave de sessão e descriptografar os pacotes, pois cada cliente possui uma chave de sessão vinculada ao ser perfil, portanto uma chave individual.

3.4 Desvantagens

Como vimos, o processo de autenticação entre servidor RADIUS e cliente requer vários passos para liberar o acesso a rede, e portanto, o protocolo exige um tempo relativamente maior para a autenticação se comparado a autenticação base para os dispositivos wireless atuais (WPA, WPA2 ou WPA3).



No.	Time	Source	Destination	Protocol	Length	Info
132	17.446246354	192.168.0.33	192.168.0.38	RADIUS	267	Access-Request id=14
133	17.447046711	192.168.0.38	192.168.0.33	RADIUS	122	Access-Challenge id=14
134	17.465627306	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=15
135	17.469286364	192.168.0.38	192.168.0.33	RADIUS	106	Access-Challenge id=15
136	17.506784402	192.168.0.33	192.168.0.38	RADIUS	409	Access-Request id=16
137	17.513056586	192.168.0.38	192.168.0.33	RADIUS	1110	Access-Challenge id=16
138	17.544701244	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=17
139	17.545381951	192.168.0.38	192.168.0.33	RADIUS	262	Access-Challenge id=17
140	17.566290920	192.168.0.33	192.168.0.38	RADIUS	371	Access-Request id=18
141	17.567884029	192.168.0.38	192.168.0.33	RADIUS	157	Access-Challenge id=18
142	17.585367722	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=19
143	17.585977752	192.168.0.38	192.168.0.33	RADIUS	140	Access-Challenge id=19
144	17.603617676	192.168.0.33	192.168.0.38	RADIUS	316	Access-Request id=20
145	17.604362896	192.168.0.38	192.168.0.33	RADIUS	174	Access-Challenge id=20
146	17.624778126	192.168.0.33	192.168.0.38	RADIUS	370	Access-Request id=21
147	17.628543440	192.168.0.38	192.168.0.33	RADIUS	182	Access-Challenge id=21
148	17.644319473	192.168.0.33	192.168.0.38	RADIUS	305	Access-Request id=22
149	17.648165190	192.168.0.38	192.168.0.33	RADIUS	146	Access-Challenge id=22
150	17.665125670	192.168.0.33	192.168.0.38	RADIUS	314	Access-Request id=23
151	17.666594950	192.168.0.38	192.168.0.33	RADIUS	222	Access-Accept id=23

Figura 20: Tempo de autenticação entre o primeiro "request"e o "accept"do servidor

Neste exemplo, o tempo de conexão foi de aproximadamente 0.220348596s ou 220,348596ms (descontando a troca de criptografia WPA). Esse custo maior de tempo está associado principalmente a negociação de autenticação ser feita não diretamente com o Access Points mas através dele.

E também, pela quantidade de solicitações previas de autenticação para garantir que a senha está correta (pacotes de desafio), pela troca de chaves WPA após a finalização da consulta, pela liberação do cliente por parte do servidor, e também pelo tempo de consulta do servidor no banco de dados.

4 Conclusão

Tendo em vista os aspectos observados podemos concluir que o Radius é um ótimo protocolo para segurança de autenticação em uma rede quando comparado a redes que utilizam PSK para a troca de chaves, pois o processo que se tem antes de ocorrer a conexão do cliente a rede é bem estruturado e quase sem risco a uma interceptação de chave, porém o tempo gasto na tentativa de se conectar é maior, mas se visarmos a segurança que cada vez mais é um ponto importante na era tecnológica, o protocolo Radius cumpre seu objetivo com êxito.

5 Referências bibliográficas

802.1X-2020 - IEEE Standard for Local and Metropolitan Area Networks
IEEE 802.1X Standard
802.1X: Port-Based Network Access Control
Cisco 802.1X devices basic configuration