

Radius

Remote Authentication Dial In User Service

Arthur Cadore Matuella Barcella

Gabriel Luiz Espindola Pedro

Matheus Pires Salazar

12/12/2021



**INSTITUTO
FEDERAL**

Santa Catarina

Câmpus
São José

- 1 Introdução
- 2 RADIUS
- 3 Capturas
- 4 Comparação: RADIUS x Autenticação Convencional
- 5 Conclusão

Introdução

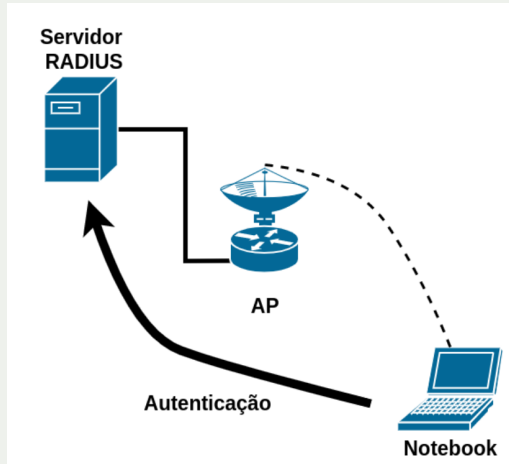
- *RADIUS* é um protocolo para a autenticação de dispositivos do tipo cliente servidor, onde o usuário informa seus dados e o servidor *RADIUS* valida as informações passadas a ele;
- Escolhemos estudá-lo devido a sua presença no nosso cotidiano, sendo utilizado em redes onde várias pessoas possuem acesso, como por exemplo a rede de alunos do IFSC.



RADIUS

- 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 tenham suas credenciais 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.





Essa autenticação estendida é chamada de EAP, diferentemente de uma rede com senha (PSK), o AP faz papel de intermediário (NAS), recebendo as solicitações vindas do dispositivo cliente e as encaminhando para o servidor RADIUS.

- Inicialmente o cliente solicita a conexão com o AP;
- O Ap então solicita os dados de identificação do dispositivo final;
- O cliente então encaminha os dados solicitados para o AP.
- Uma vez com os dados recebidos, o AP os encaminha para o servidor RADIUS solicitando uma liberação de conexão.

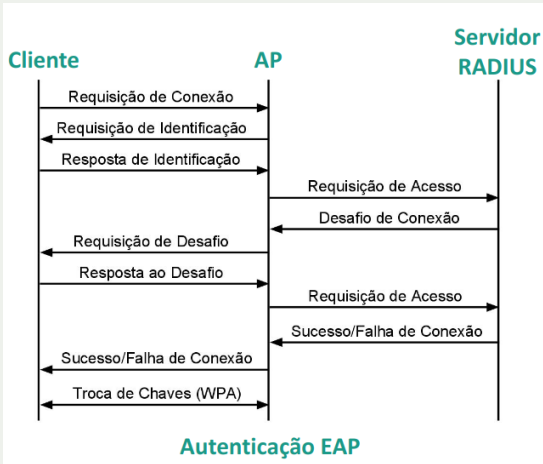


- O servidor então cria um desafio para o cliente, onde o cliente deve resolvê-lo com a senha que possui (**a senha não é encaminhada em nenhum momento para o servidor**).
- O desafio então é recebido pelo cliente, que irá resolvê-lo utilizando sua senha (como um embaralhamento).
- Após ter a resposta, o cliente a encaminha a resposta do desafio ao servidor.



- O servidor então recebe o valor da resposta do desafio, realiza o mesmo cálculo feito pelo cliente, porém com a senha que possui em seu banco de dados.
- Após ter resolvido também o desafio, compara as respostas, caso sejam iguais, significa que o cliente possui a senha correta, e encaminha uma mensagem ao AP informando que a conexão está liberada.
- Após esse procedimento, o AP orienta ao cliente que a conexão foi concluída e então inicia o procedimento de troca de chaves.



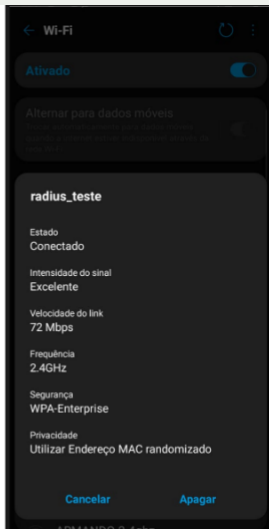
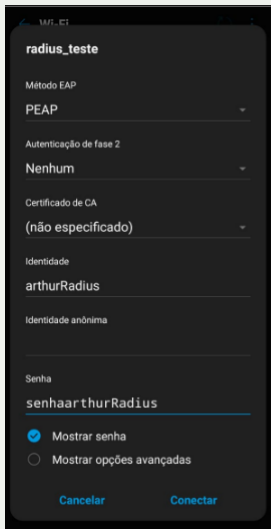


Capturas

- Feita a configuração tanto no dispositivo NAS quanto no servidor, podemos testar a autenticação wireless EAP (com RADIUS).
- Para isso, conectei um celular na rede do AP correspondente a configuração que vimos anteriormente, e utilizei os parâmetros de cliente que configuramos.



Capturas - Testando a autenticação EAP



Capturas - Comunicação dispositivo NAS e servidor

Durante a autenticação, foi possível capturar (no servidor) os pacotes de comunicação RADIUS entre dispositivo NAS e o servidor, conforme exibido abaixo:

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



Capturas - Testando a autenticação EAP

- Ao testarmos com uma senha incorreta (como ao lado), o servidor recebe uma solicitação, e realiza o mesmo procedimento, mas após receber as hashes de retorno do cliente, ele compara com as suas e verifica que a senha do cliente está incorreta, então dispara uma mensagem de rejeição:

No.	Time	Source	Destination	Protocol	Length	Info
216	33.815598113	192.168.0.33	192.168.0.38	RADIUS	267	Access-Request id=0
217	33.816222811	192.168.0.38	192.168.0.33	RADIUS	122	Access-Challenge id=0
218	33.836693648	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=1
219	33.839954535	192.168.0.38	192.168.0.33	RADIUS	106	Access-Challenge id=1
220	33.871232220	192.168.0.33	192.168.0.38	RADIUS	409	Access-Request id=2
221	33.883276975	192.168.0.38	192.168.0.33	RADIUS	1110	Access-Challenge id=2
222	33.909455679	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=3
223	33.910000246	192.168.0.38	192.168.0.33	RADIUS	262	Access-Challenge id=3
224	33.931368276	192.168.0.33	192.168.0.38	RADIUS	371	Access-Request id=4
225	33.932428347	192.168.0.38	192.168.0.33	RADIUS	157	Access-Challenge id=4
226	33.952139022	192.168.0.33	192.168.0.38	RADIUS	274	Access-Request id=5
227	33.952649400	192.168.0.38	192.168.0.33	RADIUS	140	Access-Challenge id=5
228	33.970690098	192.168.0.33	192.168.0.38	RADIUS	316	Access-Request id=6
229	33.971482797	192.168.0.38	192.168.0.33	RADIUS	174	Access-Challenge id=6
230	33.987281997	192.168.0.33	192.168.0.38	RADIUS	370	Access-Request id=7
231	33.990184618	192.168.0.38	192.168.0.33	RADIUS	146	Access-Challenge id=7
232	34.012326309	192.168.0.33	192.168.0.38	RADIUS	314	Access-Request id=8
233	35.014480002	192.168.0.38	192.168.0.33	RADIUS	86	Access-Reject id=8



Capturas - Comunicação dispositivo NAS e servidor

- No pacote de “Access-Request”, o dispositivo NAS encaminha os dados do cliente solicitante para verificação por parte do servidor.
- Podemos notar na captura dois campos que identificam o cliente e o dispositivo NAS, e também o tipo de requisição que está sendo feita.

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

Frame 132: 267 bytes on wire (2136 bits), 267 bytes captured (2136 bits) on interface enp1s0, id 0

Ethernet II, Src: Intelbra_a0:f3:3f (08:0f:e8:a0:f3:3f), Dst: Dell_fc:fd:44 (8c:04:ba:fc:fd:44)

Internet Protocol Version 4, Src: 192.168.0.33, Dst: 192.168.0.38

User Datagram Protocol, Src Port: 57933, Dst Port: 1812

RADIUS Protocol

Code: Access-Request (1)

Packet identifier: 0xe (14)

Length: 225

Authenticator: acd0157fe199c256b79dcf25a1587fa6

[The response to this request is in frame 133]

Attribute Value Pairs

- AVP: t=User-Name(1) l=14 val=arthurRadius
- AVP: t=NAS-Identifier(32) l=8 val=ap1350
- AVP: t=Called-Station-Id(30) l=32 val=86-8F-E8-A6-F3-40:radius_teste
- AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
- AVP: t=Service-Type(6) l=6 val=Framed(2)
- AVP: t=Calling-Station-Id(31) l=19
- AVP: t=Connect-Info(77) l=23 val=CONNECT 0Mbps 802.11b
- AVP: t=Acct-Session-Id(44) l=18 val=7379F61B78E7315D
- AVP: t=Acct-Multi-Session-Id(50) l=18 val=EC859C50D506D782
- AVP: t=Unknown-Attribute(186) l=6 val=000fac04
- AVP: t=Unknown-Attribute(187) l=6 val=000fac04
- AVP: t=Unknown-Attribute(188) l=6 val=000fac01
- AVP: t=Framed-MTU(12) l=6 val=1400
- AVP: t=EAP-Message(79) l=19 Last Segment[1]
- AVP: t=Message-Authenticator(80) l=18 val=9f570c8e3dafef7b398cf07564b66f80



Capturas - Comunicação dispositivo NAS e servidor

- O pacote de "access-challenge" tem como objetivo encaminhar uma hash para o dispositivo cliente.
- À direita é possível notar o tipo da mensagem que está sendo retornada ao dispositivo NAS para encaminhamento e também a hash que será encaminhada ao cliente.

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

↳ 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 (80:0f: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)**

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



Capturas - Comunicação dispositivo NAS e servidor

- Após todo o processo que vimos ocorrer, e o servidor encaminhar o pacote “access-accept” o dispositivo NAS irá liberar a conexão do cliente.
- No pacote de “access-accept” o servidor informa o código de sucesso para que o NAS entenda que pode liberar a conexão, ele também identifica para qual cliente a liberação está sendo feita.

No.	Time	Source	Destination	Protocol	Length	Info
148	17.644319473	192.168.0.33	192.168.0.38	RADIUS	365	Access-Request id=22
149	17.646165198	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

▶ Frame 151: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface enp1s0, id 0

▶ Ethernet II, Src: Dell_fc:fd:44 (8c:04:ba:fc:fd:44), Dst: Intelbra_a6:f3:3f (00:8f: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-Accept (2)

Packet Identifier: 0x17 (23)

Length: 180

Authenticator: 55cfd9bc7b2648313b99d344f9b6b5b7

[This is a response to a request in frame 150]

[Time from request: 0.001469280 seconds]

▼ Attribute Value Pairs

▶ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)

▶ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)

▼ AVP: t=EAP-Message(79) l=6 Last Segment[1]

Type: 79

Length: 6

EAP fragment: 03d80004

▼ Extensible Authentication Protocol

Code: Success (3)

ID: 216

Length: 4

▶ AVP: t=Message-Authenticator(80) l=18 val=46fe2af6ec80faace74131c1c763c17e

▶ AVP: t=User-Name(1) l=14 val=arthurRadius

Type: 1

Length: 14

User-Name: arthurRadius

▶ AVP: t=Framed-MTU(12) l=6 val=994



Capturas - Pacotes wireless (NAS e dispositivo final)

Abaixo está a comunicação entre dispositivo NAS e cliente final (os pacotes correspondentes a autenticação vista anteriormente estão sinalizados em vermelho):

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	celularArthur	AccessPointArthur	802.11	38	Authentication, SN=55, FN=0, Flags=...R...
2	0.000031		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
3	0.002223	AccessPointArthur	celularArthur	802.11	38	Authentication, SN=256, FN=0, Flags=.....
4	0.002481		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
5	0.004771	celularArthur	AccessPointArthur	802.11	165	Association Request, SN=56, FN=0, Flags=....., SSID=radius_teste
6	0.009193	AccessPointArthur	celularArthur	802.11	167	Association Response, SN=258, FN=0, Flags=.....
7	0.009485		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
8	0.013965	celularArthur	AccessPointArthur	802.11	41	Action, SN=57, FN=0, Flags=...R..., SSID=radius_teste
9	0.014153		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
10	0.014973	AccessPointArthur	celularArthur	802.11	27	Action, SN=259, FN=0, Flags=.....
11	0.015229		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
12	0.019112	AccessPointArthur	celularArthur	EAP	43	Request, Identity
13	0.019352		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
14	0.033274	celularArthur	AccessPointArthur	EAP	55	Response, Identity
15	0.033415		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
16	0.050602	AccessPointArthur	celularArthur	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
17	0.050186		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
18	0.052433	celularArthur	AccessPointArthur	EAP	44	Response, Legacy Nak (Response Only)
19	0.052545		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
20	0.071639	AccessPointArthur	celularArthur	EAP	44	Request, Protected EAP (EAP-PEAP)
21	0.071761		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
22	0.093515	celularArthur	AccessPointArthur	TLSv1.2	179	Client Hello
23	0.093652		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
24	0.102972		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
25	0.126508	celularArthur	AccessPointArthur	802.11	24	Null function (No data), SN=33, FN=0, Flags=.....T
26	0.126526		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
27	0.129662	AccessPointArthur	celularArthur	EAP	1042	Request, Protected EAP (EAP-PEAP)
28	0.129927		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
29	0.131359	celularArthur	AccessPointArthur	EAP	44	Response, Protected EAP (EAP-PEAP)
30	0.131638		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
31	0.147172	AccessPointArthur	celularArthur	TLSv1.2	200	Server Hello, Certificate, Server Key Exchange, Server Hello Done
32	0.147454		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
33	0.152944	celularArthur	AccessPointArthur	TLSv1.2	141	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
34	0.153229		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
35	0.178129	AccessPointArthur	celularArthur	TLSv1.2	95	Change Cipher Spec, Encrypted Handshake Message
36	0.178485		AccessPointArthur ..	802.11	10	Acknowledgement, Flags=.....
37	0.172836	celularArthur	AccessPointArthur	EAP	44	Response, Protected EAP (EAP-PEAP)
38	0.172332		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....



Capturas - Pacotes wireless (NAS e dispositivo final)

Após o handshake estar completado e o servidor encaminhar o pacote de “access-accept” ao dispositivo NAS, ele encaminha uma mensagem ao cliente de “success” (destacado em roxo), em seguida, o dispositivo NAS e o dispositivo cliente iniciam uma troca de chaves WPA (para criptografia do enlace) antes do tráfego de dados úteis (essa troca está destacada em azul abaixo):

36	0.170495		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
37	0.172836	celularArthur	AccessPointArthur	EAP		44	Response, Protected EAP (EAP-PEAP)
38	0.172332		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
39	0.188813	AccessPointArthur	celularArthur	TLSv1.2		78	Application Data
40	0.188270		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
41	0.190293	celularArthur	AccessPointArthur	TLSv1.2		86	Application Data
42	0.190571		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
43	0.205688	AccessPointArthur	celularArthur	TLSv1.2		112	Application Data
44	0.205697		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
45	0.288496	celularArthur	AccessPointArthur	TLSv1.2		148	Application Data
46	0.211613	celularArthur	AccessPointArthur	EAP		140	Response, Protected EAP (EAP-PEAP)
47	0.211898		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
48	0.229550	AccessPointArthur	celularArthur	TLSv1.2		120	Application Data
49	0.229801		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
50	0.231193	celularArthur	AccessPointArthur	TLSv1.2		75	Application Data
51	0.231469		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
52	0.249039	AccessPointArthur	celularArthur	TLSv1.2		84	Application Data
53	0.249308		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
54	0.251820	celularArthur	AccessPointArthur	TLSv1.2		84	Application Data
55	0.252899		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
56	0.267433	AccessPointArthur	celularArthur	EAP		42	Success
57	0.267611		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
58	0.278732	AccessPointArthur	celularArthur	EAPOL		155	Key (Message 1 of 4)
59	0.278885		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
60	0.283167		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
61	0.297551	AccessPointArthur	celularArthur	EAPOL		189	Key (Message 3 of 4)
62	0.297732		AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
63	0.301683	celularArthur	AccessPointArthur	EAPOL		133	Key (Message 4 of 4)
64	0.301873		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
65	0.546729		celularArthur	(c8:...	802.11	10	Acknowledgement, Flags=.....
66	0.551763	celularArthur	AccessPointArthur	...	802.11	24	Null function (No data), SN=36, FN=0, Flags=.....



Capturas - Pacotes wireless (NAS e dispositivo final)

Os primeiros pacotes relevantes que devemos verificar são os pacotes de request/response identity (onde o NAS solicita o usuário que irá se conectar, para consultar o servidor):

No.	Time	Source	Destination	Protocol	Length	Info
12	0.019112	AccessPointArthur	celularArthur	EAP	43	Request, Identity
13	0.019352	AccessPointArthur	AccessPointArthur	802.11	10	Acknowledgement, Flags=.....
14	0.033274	celularArthur	AccessPointArthur	EAP	55	Response, Identity
Frame 12: 43 bytes on wire (344 bits), 43 bytes captured (344 bits)						
IEEE 802.11 QoS Data, Flags:F.						
Logical-Link Control						
802.1X Authentication						
Version: 802.1X-2004 (2)						
Type: EAP Packet (0)						
Length: 5						
Extensible Authentication Protocol						
Code: Request (1)						
Id: 207						
Length: 5						
Type: Identity (1)						

No.	Time	Source	Destination	Protocol	Length	Info
12	0.019112	AccessPointArthur	celularArthur	EAP	43	Request, Identity
13	0.019352	AccessPointArthur	AccessPointArthur	802.11	10	Acknowledgement, Flags=.....
14	0.033274	celularArthur	AccessPointArthur	EAP	55	Response, Identity
Frame 14: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)						
IEEE 802.11 QoS Data, Flags:T						
Logical-Link Control						
802.1X Authentication						
Version: 802.1X-2001 (1)						
Type: EAP Packet (0)						
Length: 17						
Extensible Authentication Protocol						
Code: Response (2)						
Id: 207						
Length: 17						
Type: Identity (1)						
Identity: arthurRadius						



Capturas - Pacotes wireless (NAS e dispositivo final)

Vamos verificar também um dos pacotes que participam da autenticação via protocolo CHAP (está exibido abaixo). É possível notar a hash passada do dispositivo NAS para o dispositivo cliente para que seja processada (o código “MD5” nada mais é do que o algoritmo utilizado para gerar a hash).

No.	Time	Source	Destination	Protocol	Length	Info
15	0.833415		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
16	0.050062	AccessPointArthur	celularArthur	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
17	0.050186	AccessPointArthur	...	802.11	10	Acknowledgement, Flags=.....
» Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)						
» IEEE 802.11 QoS Data, Flags:F.						
» Logical-Link Control						
» 802.1X Authentication						
Version: 802.1X-2004 (2)						
Type: EAP Packet (0)						
Length: 22						
» Extensible Authentication Protocol						
Code: Request (1)						
Id: 208						
Length: 22						
» Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)						
EAP-MD5 Value-Size: 16						
EAP-MD5 Value: e66238e330424449718ab0da1faaff27						



Capturas - Pacotes wireless (NAS e dispositivo final)

Após todo o handshake, também é importante destacarmos o pacote que informa que a conexão foi bem estabelecida, o pacote “success”. Abaixo está sendo exibido o conteúdo deste pacote:

No.	Time	Source	Destination	Protocol	Length	Info
54	0.251820	celularArthur	AccessPointArthur	TLSv1.2	84	Application Data
55	0.252099		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
56	0.267433	AccessPointArthur	celularArthur	EAP	42	Success
57	0.267611		AccessPointArthur ...	802.11	10	Acknowledgement, Flags=.....
58	0.278732	AccessPointArthur	celularArthur	EAPOL	155	Key (Message 1 of 4)
59	0.278995		AccessPointArthur	802.11	10	Acknowledgement, Flags=.....

- ▶ Frame 56: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- ▶ IEEE 802.11 QoS Data, Flags:F.
- ▶ Logical-Link Control
- ▼ 802.1X Authentication
 - Version: 802.1X-2004 (2)
 - Type: EAP Packet (0)
 - Length: 4
- ▼ Extensible Authentication Protocol
 - Code: Success (3)
 - Id: 216
 - Length: 4



Capturas - Pacotes wireless (NAS e dispositivo final)

No caso da autenticação ser recusada (como vimos anteriormente), o processo será o mesmo, mas ao invés do dispositivo NAS encaminhar o pacote “success”, será encaminhado um pacote com o conteúdo “failure”, informando que houve falha da conexão, como exibido abaixo (nesse caso, como não foi devidamente autenticado, o cliente não terá como trocar chaves WPA com o dispositivo NAS):

No.	Time	Source	Destination	Protocol	Length	Info
47	0.198186		celularArthur (c8:...	802.11	10	Acknowledgement, Flags=.....
48	0.215641	AccessPointArthur	celularArthur	EAP	84	Request, Protected EAP (EAP-PEAP)
49	0.215910		AccessPointArthur ...	802.11	10	Acknowledgement, Flags=.....
50	0.219230	celularArthur	AccessPointArthur	EAP	84	Response, Protected EAP (EAP-PEAP)
51	0.220253	celularArthur	AccessPointArthur	EAP	84	Response, Protected EAP (EAP-PEAP)
52	1.239184	AccessPointArthur	celularArthur	EAP	42	Failure

- ▶ Frame 52: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- ▶ IEEE 802.11 QoS Data, Flags:F.
- ▶ Logical-Link Control
- ▼ 802.1X Authentication
 - Version: 802.1X-2004 (2)
 - Type: EAP Packet (0)
 - Length: 4
- ▼ Extensible Authentication Protocol
 - Code: Failure (4)
 - Id: 111
 - Length: 4



- Como dito anteriormente, também é importante notar a troca de chaves WPA após a aprovação da conexão por parte do servidor.
- No proximo slide está exibido o conteúdo da primeira troca de chave (1 de 4).
- O conteúdo teórico da troca de chaves está disponibilizado em outro material.



Capturas - Pacotes wireless (NAS e dispositivo final)

No.	Time	Source	Destination	Protocol	Length	Info
54	0.251820	celularArthur	AccessPointArthur	TLSv1.2	84	Application Data
55	0.252099		celularArthur (c8:...	802.11	18	Acknowledgement, Flags=.....
56	0.267433	AccessPointArthur	celularArthur	EAP	42	Success
57	0.267611		AccessPointArthur	802.11	18	Acknowledgement, Flags=.....
58	0.278732	AccessPointArthur	celularArthur	EAPOL	155	Key (Message 1 of 4)
59	0.278885		AccessPointArthur ...	802.11	18	Acknowledgement, Flags=.....
60	0.283167		celularArthur (c8:...	802.11	18	Acknowledgement, Flags=.....
61	0.297551	AccessPointArthur	celularArthur	EAPOL	189	Key (Message 3 of 4)

▶ Frame 58: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)

▶ IEEE 802.11 QoS Data, Flags:F.

▶ Logical-Link Control

▶ 802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

▶ Key Information: 0x008a

Key Length: 16

Replay Counter: 1

WPA Key Nonce: 9a3c7022b84b4be12573dd88542ddc20752c0d6ffef4a56c06931d815accc77e

Key IV: 00000000000000000000000000000000

WPA Key RSC: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 00000000000000000000000000000000

WPA Key Data Length: 22

▶ WPA Key Data: dd14000fac040b7fe063c0a9bde50c95ebd3c853a00d

▶ Tag: Vendor Specific: Ieee 802.11: RSN PMKID

Tag Number: Vendor Specific (221)

Tag length: 20

OUI: 00:0f:ac (Ieee 802.11)

Vendor Specific OUI Type: 4

PMKID: 0b7fe063c0a9bde50c95ebd3c853a00d



Comparação: RADIUS x Autenticação Convencional

Comparação: RADIUS x Autenticação Convencional

	RADIUS	Aut. Convencional
Credenciais individuais	opcional	não
Tempo de autenticação	maior	menor
Escalabilidade	maior	menor
Configuração inicial	complexa	simples



Conclusão

O RADIUS é um ótimo protocolo de segurança para autenticação quando comparado a autenticação convencional, pelas possibilidades que se abrem, porém o tempo de conexão é relativamente mais alto, mas o RADIUS cumpre o que promete para uma rede com autenticação mais segura.



Radius

Remote Authentication Dial In User Service

Arthur Cadore Matuella Barcella

Gabriel Luiz Espindola Pedro

Matheus Pires Salazar

12/12/2021



**INSTITUTO
FEDERAL**

Santa Catarina

Câmpus
São José