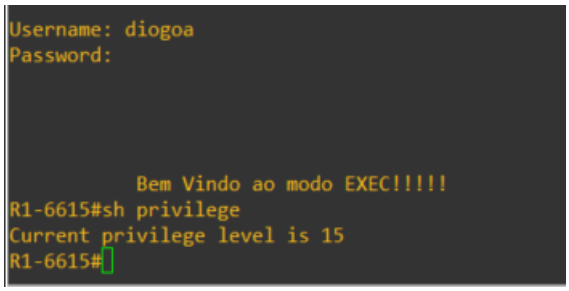
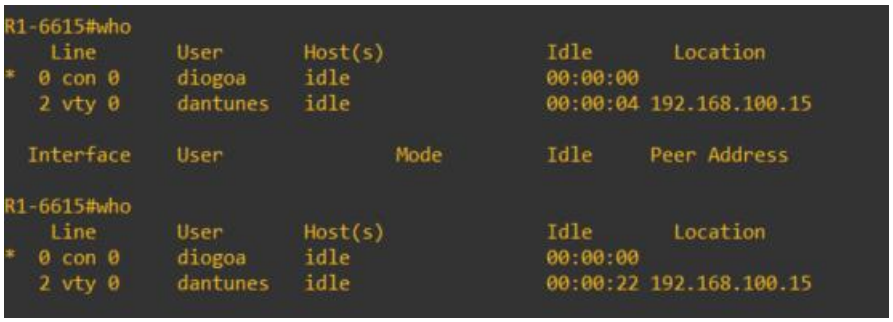
13)



Como se pode verificar na imagem acima consegui me autenticar com sucesso com o utilizador criado no R1, no entanto antes de me conseguir autenticar houve um tempo de espera. Como o servidor Radius estava indisponível, o R1 foi buscar à base de dados local os dados do utilizador, já que a configuração fallback foi feita para prevenir este cenário. Como o utilizador foi criado com o privilégio máximo entrou logo no modo EXEC privilegiado do utilizador e como se pode ver tem o privilégio 15.

14)

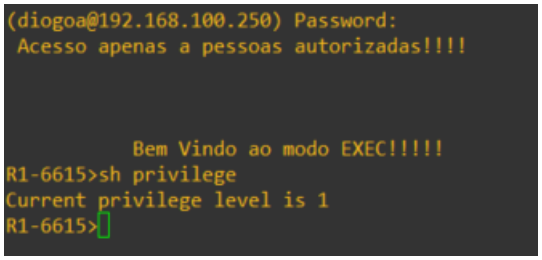


A imagem acima mostra primeiramente na linha do vty 0 do primeiro “who”, que a tentativa da sessão ssh foi iniciada (a senha ainda não tinha sido inserida). No segundo “who”, a senha já tinha sido inserida, no entanto como o servidor Radius ainda está inativo, não me consegui autenticar. A saída é esperada, pois se virmos no campo “Idle”, pode-se verificar que o tempo aumentou, este campo aumenta, pois, este campo mede o tempo de inatividade de uma sessão ou como no caso da linha vty, ele está a medir o tempo que o utilizador está a demorar para se autenticar. Pois mesmo, ele não conseguindo se autenticar, a linha ainda está aberta, ou seja, o tempo vai aumentado.

15)

A diferença foi que quando utilizava o utilizador que está na base de dados Radius, após inserir a password dava um tempo de espera e voltava a pedir a password. No caso do utilizador fallback após inserir a password deu um tempo de espera e depois a conexão ssh encerrou logo.

16)



Como se pode verificar na imagem acima, após inserir o comando pedido, consegui autenticar com o utilizador da conta fallback, no entanto entrou no modo EXEC com o privilégio nível 1. A keyword **if-authenticated**, faz com que mesmo com o servidor Radius inativo, o Router possa autorizar a autenticação de um utilizador, desde que utilize outro método, no caso foi a base de

dados local. No entanto como o utilizador não tem nenhum nível de privilégio definido o Router atribui ao utilizador por padrão o nível 1 na sessão ssh.

17)

```
R1-6615(config)#aaa authorization exec default group radius local
R1-6615(config)#
```

```
(diogoa@192.168.100.250) Password:
 Acesso apenas a pessoas autorizadas!!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615>sh privilege
Current privilege level is 1
R1-6615>
```

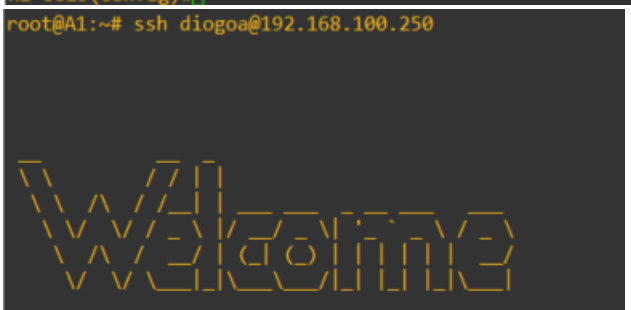
Como se pode verificar na imagem acima, após atualizar o comando, quando concluo a autenticação com o utilizador da conta fallback, volta a entrar na sessão ssh no modo EXEC e com o nível de privilégio 1.

O comando **aaa authorization exec default group radius local** faz com que o R1 tente autenticar o utilizador através do RADIUS. Caso não consiga, ele recorre ao método local, que usa as credenciais locais definidas no R1. Como a conta do utilizador não apresenta níveis de privilégios definidos, nem a linha vty apresenta níveis de privilégios definidos, quando se conclui a autenticação, o utilizador fallback fica no modo EXEC com o privilégio 1 por padrão.

18)

```
R1-6615(config)#no username diogoa
This operation will remove all username related configurations with same name.Do you want t
o continue? [confirm]
R1-6615(config)#usrname diogoa privilege 15 secret utilizadorlocal
                ^
% Invalid input detected at '^' marker.

R1-6615(config)#username diogoa privilege 15 secret utilizadorlocal
R1-6615(config)#
```

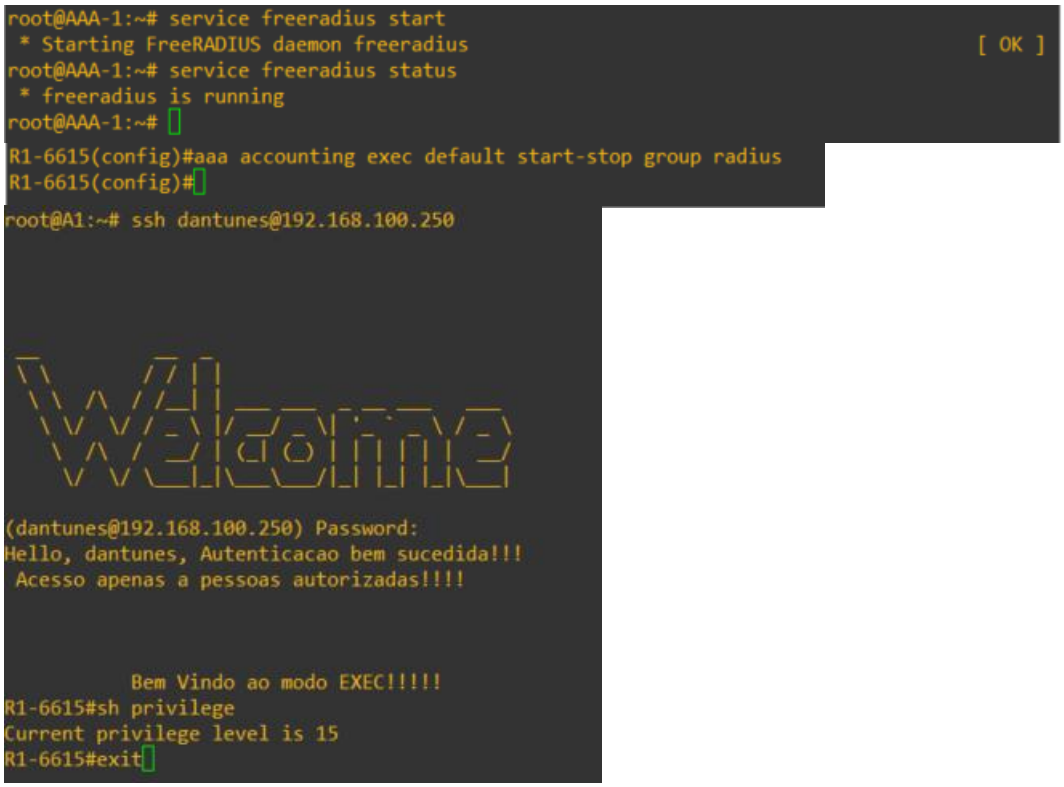
```
root@A1:~# ssh diogoa@192.168.100.250
```

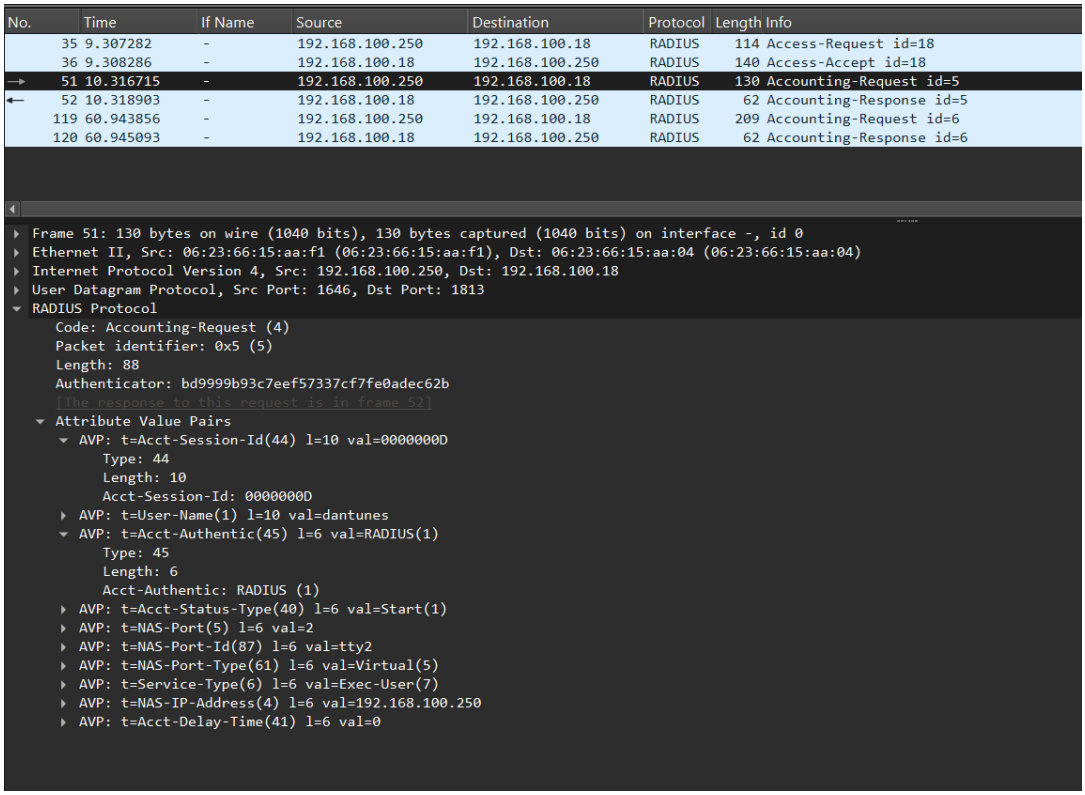


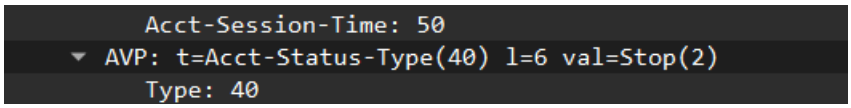
```
(diogoa@192.168.100.250) Password:
 Acesso apenas a pessoas autorizadas!!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615#sh privilege
Current privilege level is 15
R1-6615#
```

Como se pode verificar na imagem acima, agora com o utilizador criado com privilégio nível 15, quando acesso ao router por ssh, ele entra automaticamente no modo EXEC privilegiado do utilizador, com o privilégio 15. Como foi explicado anteriormente, configuramos de modo que se falhas-se a autenticação a partir da base de dados do servidor Radius recorríamos à base de dados local. Como na base de dados local o utilizador da conta fallback, neste momento foi configurado com o nível de privilégio 15, ao iniciar a sessão por ssh, ele vai ter esses níveis de privilégio.

19)

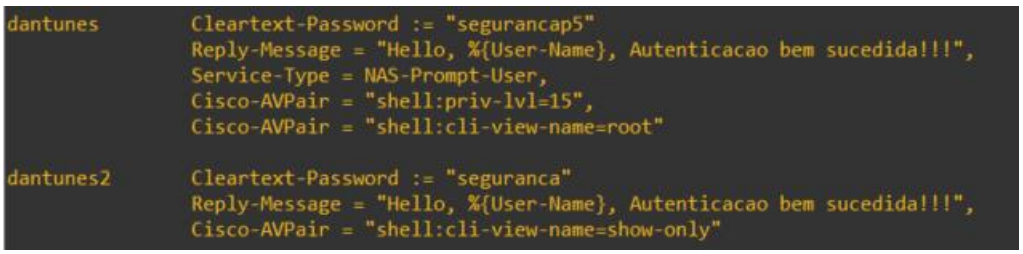






Como podemos verificar na imagem acima, agora podemos verificar as PDUS Accounting. E aparece na última PDU Accounting Request um campo onde se pode verificar que a sessão terminou.

20)



```
R1-6615(config)#parser view show-only
R1-6615(config-view)#commands exec include all show
% Password not set for the view show-only

R1-6615(config-view)#secret seguranca
R1-6615(config-view)#commands exec include all show
R1-6615(config-view)#end
R1-6615#wr
Building configuration...
[OK]
R1-6615#
```

```
R1-6615#sh parser view
Current view is 'show-only'

R1-6615#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.100.250 YES NVRAM  up                    up
Ethernet0/1                192.168.200.251 YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
Ethernet1/3                unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down

R1-6615#conf t
       ^
% Invalid input detected at '^' marker.

R1-6615#
```

```
(dantunes2@192.168.100.250) Password:
Hello, dantunes2, Autenticacao bem sucedida!!!
 Acesso apenas a pessoas autorizadas!!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615>sh parser view
Current view is 'show-only'

R1-6615>sh privilege
Currently in View Context with view 'show-only'
R1-6615>
```

```
▼ VSA: t=Cisco-AVPair(1) l=31 val=shell:cli-view-name=show-only
    Type: 1
    Length: 31
    Cisco-AVPair: shell:cli-view-name=show-only
```

Como se pode verificar nas imagens acima, depois de fazer as configurações corretamente, quando me conectei por ssh com o novo utilizador criado, entrámos inicialmente com o modo EXEC do utilizador e com a view criada e devidamente associada ativa.

Pode-se também verificar que na PDU Access-Accept apareceu um novo campo que mostra que o utilizador iniciou a sessão ssh, com a nova view ativa e que esta está devidamente associada.

```
(dantunes@192.168.100.250) Password:
Hello, dantunes, Autenticacao bem sucedida!!!
 Acesso apenas a pessoas autorizadas!!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615#sh parser view
Current view is 'root'

R1-6615#sh privilege
Currently in View Context with view 'root'
R1-6615#
```

```
▼ VSA: t=Cisco-AVPair(1) l=26 val=shell:cli-view-name=root
      Type: 1
      Length: 26
      Cisco-AVPair: shell:cli-view-name=root
```

Como se pode verificar na imagem acima, quando conclui a comunicação ssh com o utilizador original, entrei com o modo EXEC priviligiado do utilizador e com a view root ativa. Também se pode verificar na PDU Access acept o novo campo Cisco-AVPair criado com a view root.

```
Username: dantunes
Password:
Hello, dantunes, Autenticacao bem sucedida!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615#sh parser view
No view is active ! Currently in Privilege Level Context

R1-6615#sh privilege
Current privilege level is 15
R1-6615#
```

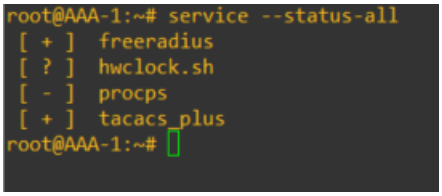
```
R1-6615(config)#aaa authorization console
```

```
Username: dantunes
Password:
Hello, dantunes, Autenticacao bem sucedida!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615#sh parser view
Current view is 'root'

R1-6615#
```

Como se pode verificar quando entrei com o utilizador original no router por consola, entrou sem a view ativa, no modo EXEC privilegiado com o privilégio 15. Ou seja, verificou-se uma incongruência entre a sessão ssh e por consola. Isto acontece, pois, na sessão SSH, a view configurada é aplicada automaticamente via Radius. O mesmo não acontece com a consola. Para isso configurei o comando sugerido pelo professor “aaa authorization console”, e quando

entrei novamente por consola no router com o utilizador original, verificou-se que a view já estava ativa.

21)



O **RADIUS** (Remote Authentication Dial-In User Service) e o **TACACS+** (Terminal Access Controller Access Control System Plus) são protocolos usados para gerenciar o acesso remoto a redes e dispositivos, mas têm diferenças importantes:

1. Arquitetura e Funcionalidade:

- **RADIUS**: Baseado em **UDP**, combina autenticação, autorização e contabilização (AAA) em um único processo, com criptografia limitada (apenas a senha é criptografada). Ideal para serviços como Wi-Fi e VPNs.
- **TACACS+**: Baseado em **TCP**, separa autenticação, autorização e contabilização, permitindo mais flexibilidade e maior segurança, já que criptografa toda a comunicação, incluindo o nome de usuário e senha. Usado principalmente em dispositivos Cisco.

2. Autenticação e Autorização:

- **RADIUS**: A autenticação e a autorização ocorrem juntas, com a autorização sendo realizada logo após a autenticação.
- **TACACS+**: Autenticação e autorização são tratadas separadamente, permitindo um controle mais detalhado sobre as permissões do usuário.

3. Segurança:

- **RADIUS**: Criptografa apenas a senha do usuário, deixando outros dados em texto claro.
- **TACACS+**: Oferece **criptografia total** de todos os dados transmitidos, proporcionando maior segurança.

4. Usos Comuns:

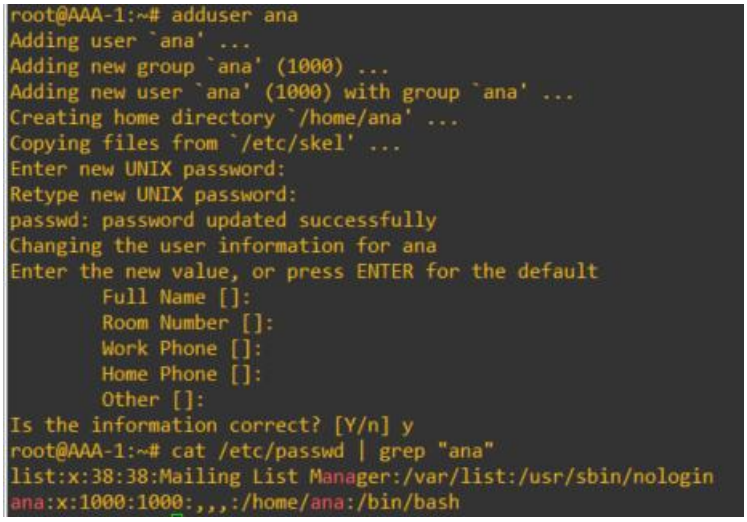
- **RADIUS**: Usado principalmente em redes de acesso remoto e serviços de rede, como Wi-Fi e VPNs.
- **TACACS+**: Mais utilizado em ambientes corporativos, especialmente em dispositivos Cisco, devido à sua capacidade de controle granular.

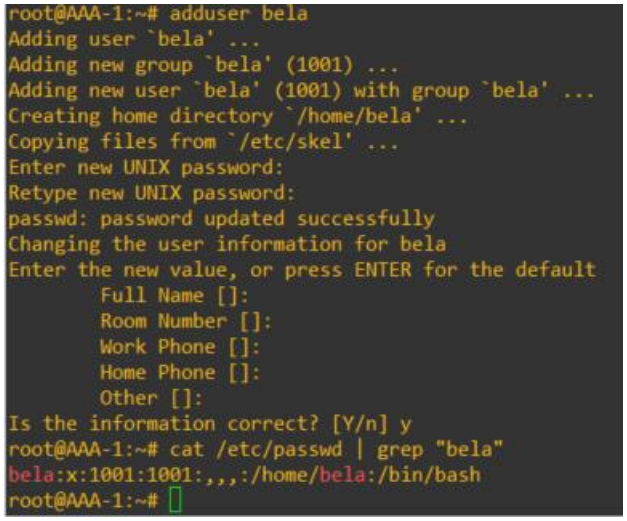
RFC 8907:

A RFC 8907 descreve o **TACACS+** como um protocolo flexível e seguro, que pode autenticar usuários, autorizar o acesso a serviços e gerenciar a contabilização do uso de recursos, proporcionando um controle detalhado das atividades de rede.

Essas diferenças tornam o **TACACS+** uma escolha preferida para ambientes que exigem maior controle sobre a autorização e a segurança, enquanto o **RADIUS** é mais adequado para autenticação simples em redes de acesso remoto.

22)





```
root@AAA-1:~# adduser carla
Adding user `carla' ...
Adding new group `carla' (1002) ...
Adding new user `carla' (1002) with group `carla' ...
Creating home directory `/home/carla' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for carla
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@AAA-1:~# cat /etc/passwd | grep "carla"
carla:x:1002:1002:,,,:/home/carla:/bin/bash
root@AAA-1:~#
```

```
root@AAA-1:~# apt update
Get:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [102 kB]
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [102 kB]
Get:1 http://archive.ubuntu.com/ubuntu bionic InRelease [242 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [1637 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [102 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/restricted amd64 Packages [1688 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [23.8 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [1728 kB]
Get:9 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [3373 kB]
Get:10 http://archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [2411 kB]
Get:11 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [3786 kB]
Get:12 http://archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [30.8 kB]
Get:13 http://archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [11.3 MB]
Get:14 http://archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [186 kB]
Get:15 http://archive.ubuntu.com/ubuntu bionic/restricted amd64 Packages [13.5 kB]
Get:16 http://archive.ubuntu.com/ubuntu bionic/main amd64 Packages [1344 kB]
Get:17 http://archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [20.6 kB]
Get:18 http://archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [64.0 kB]
Fetched 16.9 MB in 3s (5679 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
root@AAA-1:~# apt install -y pwgen
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  pwgen
0 upgraded, 1 newly installed, 0 to remove and 94 not upgraded.
Need to get 18.0 kB of archives.
After this operation, 52.2 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic/universe amd64 pwgen amd64 2.08-1 [18.0 kB]
Fetched 18.0 kB in 0s (46.1 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package pwgen.
(Reading database ... 11752 files and directories currently installed.)
Preparing to unpack .../pwgen_2.08-1_amd64.deb ...
Unpacking pwgen (2.08-1) ...
Setting up pwgen (2.08-1) ...
```

```
user = gns3 {
    name = "Admin User"
    member = admin
    login = des AxKP5aUynXxrg
                service = junos-exec {
                        local-user-name = remote-admin
        }
}

user = readonly {
    name = "R/O User"
    member = read-only
    login =  des AxKP5aUynXxrg
        service = junos-exec {
            local-user-name = remote-read-only
               }
}

group = admin {
        default service = permit
        service = exec {
                priv-lvl = 15
                }
        }
```

No ficheiro de configuração TACACS+ tem registado o user gn3, com o nome Admin User que pertence ao grupo admin. Alterei-o para ter os dados corretos.

```
user = admin {
    name = "Admin User"
    member = admin
    login = des AxKP5aUynXxrg
                service = junos-exec {
                        local-user-name = remote-admin
        }
}

user = readonly {
    name = "R/O User"
    member = read-only
    login =  des AxKP5aUynXxrg
        service = junos-exec {
            local-user-name = remote-read-only
               }
}

group = admin {
        default service = permit
        service = exec {
                priv-lvl = 15
                }
```

```
root@AAA-1:~# pwgen 16 1
Deighahh5ge9aSh1
```

```
R1-6615(config)#tacacs server TACACS-SERVER
R1-6615(config-server-tacacs)#address ipv4 192.168.100.18
R1-6615(config-server-tacacs)#key Deighahh5ge9aSh1
R1-6615(config-server-tacacs)#
```

```
accounting file = /var/log/tac_plus.acct

# This is the key that clients have to use to access Tacacs+

key = Deighahh5ge9aSh1
```

```
R1-6615(config)#aaa authentication login default group tacacs+ local
R1-6615(config)#aaa authorization exec default group tacacs+ local
R1-6615(config)#aaa accounting exec default start-stop group tacacs+
R1-6615(config)#
```

```
root@AAA-1:~# tac_pwd -p
tac_pwd: invalid option -- 'p'
Usage: tac_pwd [-ehm] [<salt>]
        -e      do not echo the password
        -h      display this message
        -m      generate MD5 crypt
root@AAA-1:~# tac_pwd -m
Password to be encrypted: adminpass
$1$.k$DeC02ZXRMj/0nuKfPpL8m1
```

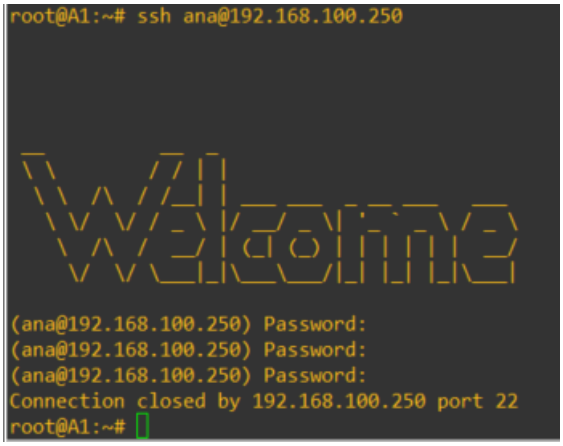
```
user = admin {
    name = "Admin User"
    member = admin
    login = des $1$.k$DeC02ZXRMj/0nuKfPpL8m1
                service = junos-exec {
                        local-user-name = remote-admin
        }
}
```

```
group = admin_users {
        default service = permit
        login = file /etc/passwd
        service = exec {
                priv-lvl = 15
                }       }
```

```
group = tacacs_users {
        default service = permit
        login = file /etc/passwd
        service = exec {
        priv-lvl = 15
        }
        cmd = show {
                permit .*
        }
        cmd = exit {
                permit .*
                }
        cmd = logout {
                permit .*
                }
        cmd = configure {
                deny .*
        }
    }
```

´

```
user = ana {
        name = "Ana"
        member = tacacs_users
}

user = clara {
        name = "Clara"
        member = admin_users
}

user = bela {
        name = "Bela"
        member = admin_users
}
```



Após terminar a configuração, tentei de tudo, no entanto não consigo aceder por ssh ao router com nenhum dos utilizadores criados no servidor TACACS+, aparecem os PDUS TACACS+ Authentication no wireshark, no entanto nunca consigo concluir a autenticação.