13)

```
R1-6615(config)#parser view DiogoAntunes-VIEWB
R1-6615(config-view)#secret segurancaaulas
R1-6615(config-view)#commands exec include configure terminal
R1-6615(config-view)#commands configure include interface e0/0
R1-6615(config-view)#commands configure include ip address
R1-6615(config-view)#commands interface include shutdown
R1-6615(config-view)#commands interface include description
R1-6615(config-view)#end
R1-6615#
```

```
R1-6615(config-view)#commands interface include no shutdown
```

```
R1-6615(config)#username adminb615 view DiogoAntunes-VIEWB secret segurancaaul$
R1-6615(config)#
```

```
(adminb615@192.168.200.251) Password:



         Bem Vindo!!!! R1-6615 Ligado!!!!!



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

R1-6615>en
Password:
R1-6615#sh parser view
No view is active ! Currently in Privilege Level Context

R1-6615#enable view DiogoAntunes-VIEWB
Password:
% Authentication failed

R1-6615#enable view DiogoAntunes-VIEWB
Password:

R1-6615#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-6615(config)#int e0/1
                ^
% Invalid input detected at '^' marker.

R1-6615(config)#int e0/0
R1-6615(config-if)#shut
R1-6615(config-if)#no shut
R1-6615(config-if)#
```

14)

```
R1-6615(config)#username adminc615 privilege 10 secret segurancaaulas3
R1-6615(config)#privilege exec level 7 configure terminal
R1-6615(config)#privilege configure level 10 interface
R1-6615(config)#privilege interface level 10 ip address
R1-6615(config)#privilege interface level 10 description
R1-6615(config)#privilege interface level 10 shutdown
R1-6615(config)#privilege interface level 10 no shutdown
R1-6615(config)#privilege exec level 10 configure terminal
R1-6615(config)#
```

```
(adminc615@192.168.200.251) Password:



         Bem Vindo!!!! R1-6615 Ligado!!!!!



          Bem Vindo ao modo EXEC!!!!!
R1-6615#~conf t
       ^
% Invalid input detected at '^' marker.

R1-6615#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-6615(config)#do sh run
               ^
% Invalid input detected at '^' marker.

R1-6615(config)#int e0/0
R1-6615(config-if)#shut
R1-6615(config-if)#no shut
R1-6615(config-if)#ip add 192.168.100.250 255.255.255.0
R1-6615(config-if)#
```

15)

```
R1-6615(config)#parser view DiogoAntunes-VIEWC superview
R1-6615(config-view)#secret segurancaaulas
R1-6615(config-view)#view DiogoAntunes-VIEWA
R1-6615(config-view)#view DiogoAntunes-VIEWB
R1-6615(config-view)#
```

```
R1-6615(config)#username adminc615 view DiogoAntunes-VIEWC secret segurancaaul$
R1-6615(config)#
```

```
(adminc615@192.168.200.251) Password:
(adminc615@192.168.200.251) Password:



         Bem Vindo!!!! R1-6615 Ligado!!!!!



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

R1-6615#
```

```
R1-6615#sh privilege
          ^
% Invalid input detected at '^' marker.

R1-6615#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-6615(config)#int e0/0
R1-6615(config-if)#shut
R1-6615(config-if)#no shut
R1-6615(config-if)#exit
R1-6615(config)#int e0/1
R1-6615(config-if)#do sh parser view
Current view is 'DiogoAntunes-VIEWC'

R1-6615(config-if)#
```

16)

```
root@Toolbox-1:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::42:cff:fe8b:a100  prefixlen 64  scopeid 0x20<link>
        ether 06:23:66:15:aa:00  txqueuelen 1000  (Ethernet)
        RX packets 25  bytes 2749 (2.7 KB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 9  bytes 726 (726.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Toolbox-1:~#
```

```
root@Toolbox-1:~# netstat -tunlp | awk '{print $1, $4}'
Active (only
Proto Local
tcp 0.0.0.0:21
tcp 0.0.0.0:80
tcp 0.0.0.0:514
tcp6 :::80
tcp6 :::514
udp 127.0.0.1:60891
udp 0.0.0.0:514
udp 0.0.0.0:69
udp 0.0.0.0:161
udp 0.0.0.0:162
udp6 :::514
udp6 :::69
udp6 :::161
root@Toolbox-1:~#
```

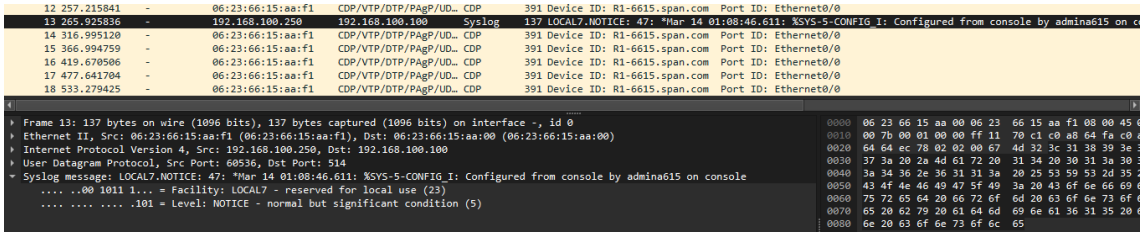
```
root@Toolbox-1:~# cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
bootps          67/udp
bootpc          68/udp
```

O IANA é responsável por atribuir e manter os números de porta usados por protocolos de comunicação.

Essa lista oficial do IANA contém as portas e protocolos padrão, e o arquivo /etc/services é basicamente uma implementação local dessa lista. Ou seja, as portas e os serviços definidos no arquivo /etc/services são amplamente baseados nas recomendações da IANA.

17)

```
R1-6615(config)#logging on
R1-6615(config)#logging host 192.168.100.100
R1-6615(config)#
*Mar 14 01:04:28.531: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.100.100 port 51
4 started - CLI initiated
```



Facility: Local7 (reservado para uso local)

Severity: 5 (mensagem informativa ou envento normal que não é critico)

Data e hora: 14 Março, 01:08:46

Hostname: %SYS -> Indica que a mensagem vem do sistema

Procid: 47

MSGID – CONFIG_I (mostra que é uma mensagem de configuração, o “I”, mostra que foi bem sucedida)

Mensagem -> Configurada pela consola pelo usuário admina615

18)

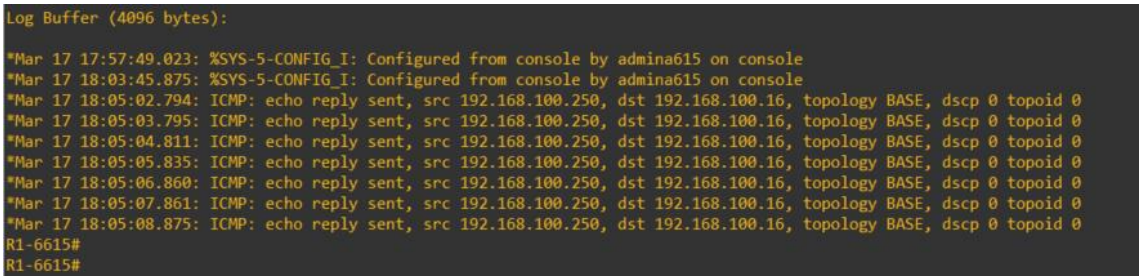
```
R1-6615(config)#logging trap debugging
```

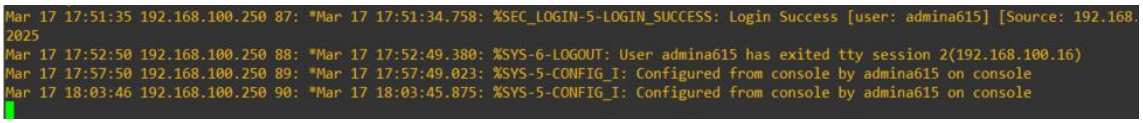

```
Mar 14 02:05:50 192.168.100.250 49: *Mar 14 02:05:49.052: %SEC_LOGIN-4-LOGIN_FAILED: Login
failed [user: adminb615] [Source: 192.168.100.16] [localport: 22] [Reason: Login Authentica
tion Failed] at 02:05:49 UTC Fri Mar 14 2025
Mar 14 02:06:10 192.168.100.250 50: *Mar 14 02:06:09.700: %SEC_LOGIN-5-LOGIN_SUCCESS: Login
 Success [user: adminb615] [Source: 192.168.100.16] [localport: 22] at 02:06:09 UTC Fri Mar
 14 2025
```

19)

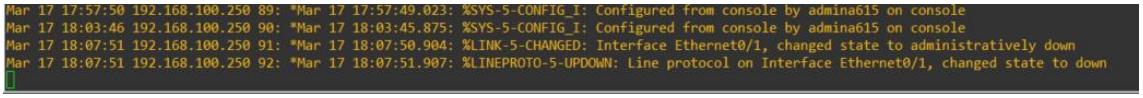
Após desativar a entrega de logs ao serviço Syslog de T1, as mensagens syslog deixam de ser enviadas ao T1, no entanto continuam a ser guardadas localmente pelo R1, onde também continuam a aparecer as mesmas.

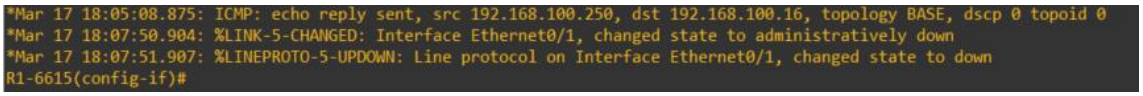
Para testar logs de nível 7, posso fazer um ping para um dos terminais a partir de R1 ou vice-versa, depois de ativar, por exemplo, o comando “debug ip icmp”, para ativar o debug de mensagens icmp.





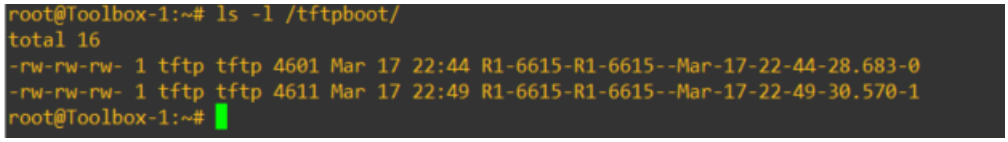
Para testar os logs de nível 6, basta alterar o estado de uma interface para down.

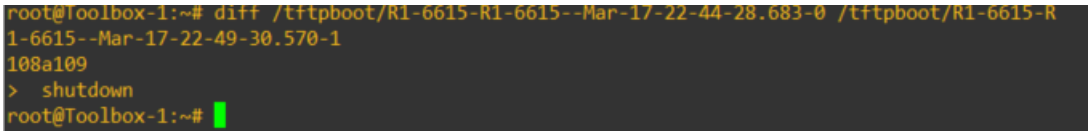




20)

~

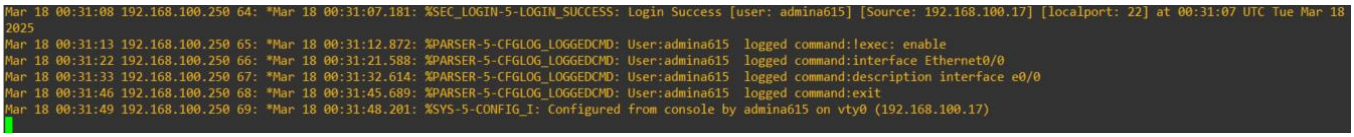




O servidor TFTP, que no caso é o T1 foi configurado no R1 para armazenar os backups da configuração do router em um diretório do servidor TFTP. A cada 5 minutos é guardada uma cópia da configuração de R1 no diretório configurado do servidor TFTP.

21)

É útil fazer os logs, para rastrear quem fez alterações, quando e que comandos foram executados. Facilita a análise de problemas e detecção de alterações não autorizadas.



Archive: Habilita o recurso de arquivamento das configurações.

Log config: Ativa a geração de logs para as configurações realizadas e regista automaticamente todas as alterações feitas no modo de configuração global.

Logging enable: Habilita a funcionalidade de logging.

Logging size 100: Define o tamanho do buffer de logging para 100 entradas.

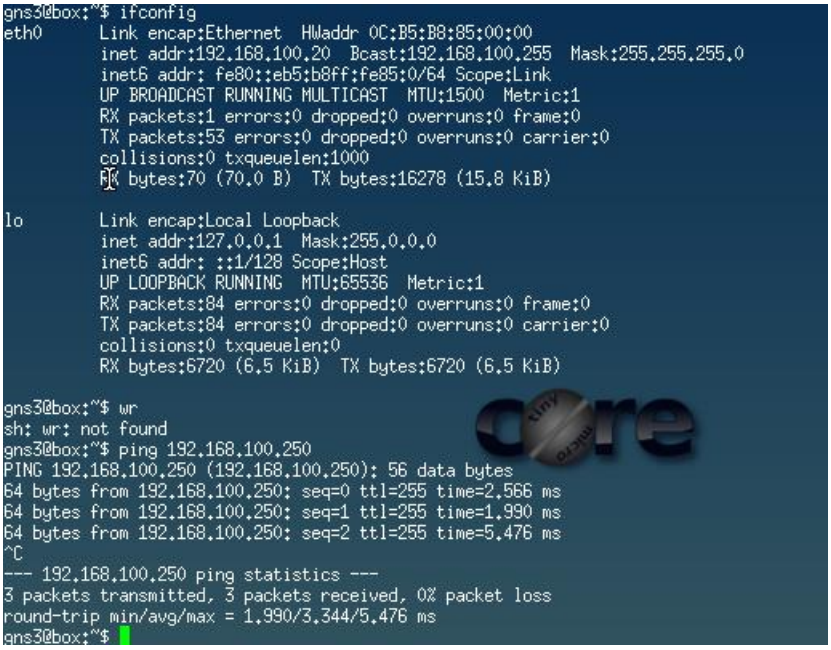
Notify syslog: Envia os logs gerados para um servidor Syslog configurado, no caso para T1.

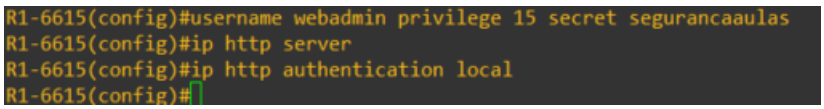
Hidekeys: Oculta senhas e chaves secretas nos logs.

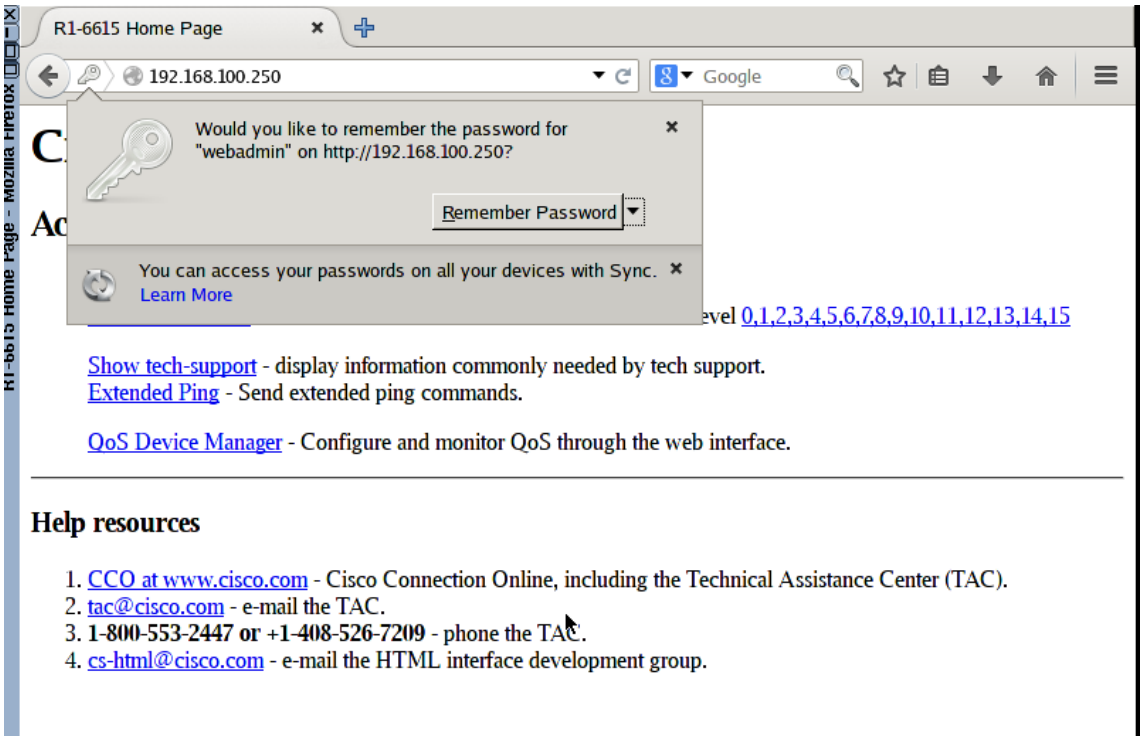
22)

```
root@Toolbox-1:~# diff /tftpboot/R1-6615-backup /tftpboot/R1-6615-backup-2
3c3
< ! Last configuration change at 00:31:48 UTC Tue Mar 18 2025 by admina615
---
> ! Last configuration change at 00:51:24 UTC Tue Mar 18 2025 by admina615
6,7c6,10
< service timestamps debug datetime msec
< service timestamps log datetime msec
---
> no service pad
> service tcp-keepalives-in
> service tcp-keepalives-out
> service timestamps debug datetime msec localtime show-timezone
> service timestamps log datetime msec localtime show-timezone
8a12
> service sequence-numbers
15a20
> security authentication failure rate 10 log
16a22
> logging console critical
17a24
> enable password 7 095F4B0E0C17161C080D053F27253B62
22a30
> aaa authentication login local_auth local
42a51,52
> no ip source-route
> no ip gratuitous-arps
57a68
> no ip bootp server
88a100
> no cdp run
90a103,109
> ip tcp intercept list autosec_tcp_intercept_list
> ip tcp intercept connection-timeout 3600
> ip tcp intercept watch-timeout 15
> ip tcp intercept max-incomplete low 450 high 550
> ip tcp intercept drop-mode random
> ip ssh time-out 60
> ip ssh authentication-retries 2
```

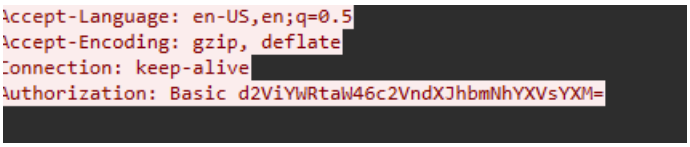
23)







A partir da interface web do router, podemos por lá fazer configurações, aceder a uma lista de comandos de configuração filtrados por nível de privilegio, aceder ao ficheiro de configuração, ficheiro de logs, comando de ping.



A password não aparece em clear texto, aparece codificada em Base64, na linha do "Authorization: ", no entanto esta é muito fácil de descodificar.