

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          ttyst source
chargen    19/udp          ttyst 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          nickname
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

12 257.215841 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
13 265.995838 - 192.168.100.250 192.168.100.100 Syslog 137 LOCAL7.NOTICE: 47: *Mar 14 01:08:46.611: %SYS-5-CONFIG_I: Configured from console by admina615 on c
14 316.995120 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
15 366.994759 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
16 419.679586 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
17 477.641784 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
18 533.279425 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAgP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
:
Frame 13: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface -, id 0
Ethernet II, Src: 06:23:66:15:aa:f1 (06:23:66:15:aa:f1), Dst: 06:23:66:15:aa:00 (06:23:66:15:aa:00)
Internet Protocol Version 4, Src: 192.168.100.250, Dst: 192.168.100.100
User Datagram Protocol, Src Port: 60536, Dst Port: 514
Syslog message: LOCAL7.NOTICE: 47: *Mar 14 01:08:46.611: %SYS-5-CONFIG_I: Configured from console by admina615 on console
.... .00 1011 1... = Facility: LOCAL7 - reserved for local use (23)
.... .... .... .101 = Level: NOTICE - normal but significant condition (5)

0000 06 23 66 15 aa 00 06 23 66 15 aa f1 08 00 45 6
0010 00 7b 00 01 00 00 ff 11 70 c1 c0 a8 64 fa c0 8
0020 54 64 ec 78 02 02 00 00 4d 3c 31 38 59 3e 5
0030 5b 4f 20 20 61 00 00 31 34 35 30 39 38 37 3
0040 3a 34 45 21 36 01 31 3a 30 25 53 49 53 2d 35 2
0050 43 4f 4e 46 49 47 5f 49 3a 20 43 6f 6e 66 69 6
0060 75 72 65 64 20 66 72 6f 6d 20 63 6f 6e 73 6f 6
0070 65 20 62 79 20 61 64 6d 69 6e 61 36 31 35 20 6
0080 6e 20 63 6f 6e 73 6f 6c 65

:
0000 06 23 66 15 aa 00 06 23 66 15 aa f1 08 00 45 6
0010 00 7b 00 01 00 00 ff 11 70 c1 c0 a8 64 fa c0 8
0020 54 64 ec 78 02 02 00 00 4d 3c 31 38 59 3e 5
0030 5b 4f 20 20 61 00 00 31 34 35 30 39 38 37 3
0040 3a 34 45 21 36 01 31 3a 30 25 53 49 53 2d 35 2
0050 43 4f 4e 46 49 47 5f 49 3a 20 43 6f 6e 66 69 6
0060 75 72 65 64 20 66 72 6f 6d 20 63 6f 6e 73 6f 6
0070 65 20 62 79 20 61 64 6d 69 6e 61 36 31 35 20 6
0080 6e 20 63 6f 6e 73 6f 6c 65
```

Facility: Local7 (reservado para uso local)

Severity: 5 (mensagem informativa ou evento 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

No. Time If Name Source Destination Protocol Length Info
1 0.000000 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAGP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
2 48.728888 - 06:23:66:15:aa:02 Broadcast ARP 42 Who has 192.168.100.250? Tell 192.168.100.16
3 53.259145 - 06:23:66:15:aa:f1 CDP/VTP/DTP/PAGP/UD.. CDP 391 Device ID: R1-6615.span.com Port ID: Ethernet0/0
4 54.677666 - 192.168.100.250 192.168.100.100 Syslog 241 LOCAL7.WARNING: 49: *Mar 14 02:05:49.052: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: adminb615] [Source: 192.168.100.16]
5 75.311156 - 192.168.100.250 192.168.100.100 Syslog 285 LOCAL7.NOTICE: 50: *Mar 14 02:06:09.700: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: adminb615] [Source: 192.168.100.16

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 Authentication 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.

```
Log Buffer (4096 bytes):

*Mar 17 17:57:49.023: %SYS-5-CONFIG_I: Configured from console by admina615 on console
*Mar 17 18:03:45.875: %SYS-5-CONFIG_I: Configured from console by admina615 on console
*Mar 17 18:05:02.794: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:03.795: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:04.811: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:05.835: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:06.860: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:07.861: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:05:08.875: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
R1-6615#
R1-6615#
```



```
Mar 17 17:51:35 192.168.100.250 87: *Mar 17 17:51:34.758: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admina615] [Source: 192.168.2025
Mar 17 17:52:50 192.168.100.250 88: *Mar 17 17:52:49.380: %SYS-6-LOGOUT: User admina615 has exited tty session 2(192.168.100.16)
Mar 17 17:57:50 192.168.100.250 89: *Mar 17 17:57:49.023: %SYS-5-CONFIG_I: Configured from console by admina615 on console
Mar 17 18:03:46 192.168.100.250 90: *Mar 17 18:03:45.875: %SYS-5-CONFIG_I: Configured from console by admina615 on console
```

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

```
Mar 17 17:57:50 192.168.100.250 89: *Mar 17 17:57:49.023: %SYS-5-CONFIG_I: Configured from console by admina615 on console
Mar 17 18:03:46 192.168.100.250 90: *Mar 17 18:03:45.875: %SYS-5-CONFIG_I: Configured from console by admina615 on console
Mar 17 18:07:51 192.168.100.250 91: *Mar 17 18:07:50.904: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
Mar 17 18:07:51 192.168.100.250 92: *Mar 17 18:07:51.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
```



```
*Mar 17 18:05:08.875: ICMP: echo reply sent, src 192.168.100.250, dst 192.168.100.16, topology BASE, dscp 0 topoid 0
*Mar 17 18:07:50.904: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Mar 17 18:07:51.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
R1-6615(config-if)#
```

20)

```
R1-6615(config)#archive
R1-6615(config-archive)#path tftp://192.168.100.100/R1-6615-$h-$t
R1-6615(config-archive)#time-period 5
R1-6615(config-archive)#
R1-6615(config-archive)#exit ~
root@Toolbox-1:~# ls -l /tftpboot/
total 16
-rw-rw-rw- 1 tftp tftp 4601 Mar 17 22:44 R1-6615-R1-6615--Mar-17-22-44-28.683-0
-rw-rw-rw- 1 tftp tftp 4611 Mar 17 22:49 R1-6615-R1-6615--Mar-17-22-49-30.570-1
root@Toolbox-1:~#
```



```
root@Toolbox-1:~# diff /tftpboot/R1-6615-R1-6615--Mar-17-22-44-28.683-0 /tftpboot/R1-6615-R1-6615--Mar-17-22-49-30.570-1
108a109
> shutdown
root@Toolbox-1:~#
```

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.

```
Mar 18 00:31:08 192.168.100.250 64: *Mar 18 00:31:07.181: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admina615] [Source: 192.168.100.17] [localport: 22] at 00:31:07 UTC Tue Mar 18 2025
Mar 18 00:31:13 192.168.100.250 65: *Mar 18 00:31:12.872: %PARSER-5-CFGLOG_LOGGEDCMD: User:admina615 logged command:!exec: enable
Mar 18 00:31:22 192.168.100.250 66: *Mar 18 00:31:21.588: %PARSER-5-CFGLOG_LOGGEDCMD: User:admina615 logged command:interface Ethernet0/0
Mar 18 00:31:33 192.168.100.250 67: *Mar 18 00:31:32.614: %PARSER-5-CFGLOG_LOGGEDCMD: User:admina615 logged command:description interface e0/0
Mar 18 00:31:46 192.168.100.250 68: *Mar 18 00:31:45.689: %PARSER-5-CFGLOG_LOGGEDCMD: User:admina615 logged command:exit
Mar 18 00:31:49 192.168.100.250 69: *Mar 18 00:31:48.201: %SYS-5-CONFIG_I: Configured from console by admina615 on vty0 (192.168.100.17)
```

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-arp
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)

```
gns3@box:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 0C:B5:B8:85:00:00
          inet addr:192.168.100.20  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::1eb5:b8ff:fe85:0/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:1 errors:0 dropped:0 overruns:0 frame:0
             TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:70 (70.0 B)  TX bytes:16278 (15.8 KiB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING  MTU:65536  Metric:1
             RX packets:84 errors:0 dropped:0 overruns:0 frame:0
             TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:6720 (6.5 KiB)  TX bytes:6720 (6.5 KiB)

gns3@box:~$ wr
sh: wr: not found
gns3@box:~$ ping 192.168.100.250
PING 192.168.100.250 (192.168.100.250): 56 data bytes
64 bytes from 192.168.100.250: seq=0 ttl=255 time=2.566 ms
64 bytes from 192.168.100.250: seq=1 ttl=255 time=1.990 ms
64 bytes from 192.168.100.250: seq=2 ttl=255 time=5.476 ms
^C
--- 192.168.100.250 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.990/3.344/5.476 ms
gns3@box:~$
```

```
R1-6615(config)#username webadmin privilege 15 secret segurancaaulas
R1-6615(config)#ip http server
R1-6615(config)#ip http authentication local
R1-6615(config)#
```

R1-6615 Home Page

192.168.100.250

Would you like to remember the password for "webadmin" on http://192.168.100.250?

Remember Password

You can access your passwords on all your devices with Sync.

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.
QoS Device Manager - Configure and monitor QoS through the web interface.

Help resources

1. [CCO at www.cisco.com](http://www.cisco.com) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

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.

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: Basic d2ViYWRtaW46c2VndXJhbmlhYXVsYXM=
```

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