Comandos básicos em Linux Shell

Prof. Sergio Johann Filho
sergio.filho@pucrs.br

Introdução

- Abrir um terminal no Linux
- Executar o comando man (manpage)
  - Exibe uma página de manual para os comandos
  - Exemplos:

```
man ifconfig
man iperf
```

- Executar comandos como superusuário (root)
  - Exemplo:

```
sudo ifconfig
```

Ferramentas Básicas

- ifconfig
- wireshark
- tcpdump
- ethtool
- ping
- iperf
- route
- traceroute
- nmap

ifconfig

- Usado para configurar e verificar as configurações das interfaces de rede do computador
- Exemplos:

Verificar o estado atual e configurações das interfaces
$ ifconfig
$ ip a

Desligar uma interface:
$ ifconfig eth3 down
$ ip link set dev eth3 up

Ligar uma interface:
$ ifconfig eth3 up
$ ip link set dev eth3 down

Modificar o endereço de IP de uma interface:
$ ifconfig eth3 10.32.143.212 netmask 255.255.255.0 up
$ ip addr add 10.32.143.212/24 dev eth3

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ ifconfig
eth2      Link encap:Ethernet  HWaddr 00:0a:f7:2b:69:42
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:17

eth3      Link encap:Ethernet  HWaddr a4:1f:72:f5:90:5c
          inet addr:10.32.143.212  Bcast:10.32.143.255  Mask:255.255.255.0
          inet6 addr: fe80::a61f:72ff:fef5:905c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14393 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10023 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15172453 (15.1 MB)  TX bytes:1506875 (1.5 MB)

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:641 errors:0 dropped:0 overruns:0 frame:0
          TX packets:641 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:65322 (65.3 KB)  TX bytes:65322 (65.3 KB)

labredes@labredes-OptiPlex-3010 ~ $
```

Endereço de hardware (MAC)

Endereço IP

Wireshark

- Sniffer de rede: monitora o tráfego de rede recebido por uma interface
- Exemplo:

```
$ sudo wireshark
```

The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)] (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

WIRESHARK

The World's Most Popular Network Protocol Analyzer

Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)

Capture

Interface List

Live list of the capture interfaces
(counts incoming packets)

Start

Choose one or more interfaces to capture from, then **Start**

- eth2
- eth3
- any
- Loopback: lo

Capture Options

Start a capture with detailed options

Capture Help

How to Capture

Step by step to a successful capture setup

Network Media

Specific information for capturing on:

Files

Open

Open a previously captured file

Open Recent:

/home/labredes/projects/networksLab/lab01/pingOut.pcapng [not found]
/home/labredes/projects/networksLab/lab01/pingLocal.pcapng [not found]
/home/labredes/projects/networksLab/lab01/ping.pcapng [not found]
/home/labredes/projects/networksLab/lab01/capture.pcapng [not found]

Sample Captures

A rich assortment of example capture files on the wiki

Ready to load or capture | No Packets | Profile: Default

*eth3 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)] (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	BrocadeC_d6:10:ee	Spanning-tree-(	STP	60	RST. Root = 32768/143/00:12:f2:d6:10:c5
2	0.378715000	Cisco_f0:64:09	PVST+	STP	64	Conf. Root = 32768/0/00:1b:ed:92:29:40
3	0.391748000	10.32.143.188	10.32.143.212	ICMP	98	Echo (ping) request id=0x1578, seq=171/4
4	0.391777000	10.32.143.212	10.32.143.188	ICMP	98	Echo (ping) reply id=0x1578, seq=171/4
5	1.391748000	10.32.143.188	10.32.143.212	ICMP	98	Echo (ping) request id=0x1578, seq=172/4
6	1.391780000	10.32.143.212	10.32.143.188	ICMP	98	Echo (ping) reply id=0x1578, seq=172/4
7	2.000353000	BrocadeC_d6:10:ee	Spanning-tree-(	STP	60	RST. Root = 32768/143/00:12:f2:d6:10:c5
8	2.391730000	10.32.143.188	10.32.143.212	ICMP	98	Echo (ping) request id=0x1578, seq=173/4
9	2.391760000	10.32.143.212	10.32.143.188	ICMP	98	Echo (ping) reply id=0x1578, seq=173/4
10	2.443831000	Cisco_f0:64:09	PVST+	STP	64	Conf. Root = 32768/0/00:1b:ed:92:29:40

```
▶ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
▼ Ethernet II, Src: Dell_f5:90:4a (a4:1f:72:f5:90:4a), Dst: Dell_f5:90:5c (a4:1f:72:f5:90:5c)
  ▶ Destination: Dell_f5:90:5c (a4:1f:72:f5:90:5c)
  ▶ Source: Dell_f5:90:4a (a4:1f:72:f5:90:4a)
    Type: IP (0x0800)
▼ Internet Protocol Version 4, Src: 10.32.143.188 (10.32.143.188), Dst: 10.32.143.212 (10.32.143.212)
    Version: 4
    Header length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0000 (0)
  ▶ Flags: 0x02 (Don't Fragment)
```

```
0000  a4 1f 72 f5 90 5c a4 1f  72 f5 90 4a 08 00 45 00   ..r..\.. r..J..E.
0010  00 54 00 00 40 00 40 01  06 d9 0a 20 8f bc 0a 20   .T..@.@. ... ...
0020  8f d4 08 00 6b 7c 15 78  00 ab 62 13 e9 53 00 00   ....k|.x ..b..S..
0030  00 00 63 26 09 00 00 00  00 00 10 11 12 13 14 15   ..c&.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Ethernet (eth), 14 bytes | Packets: 22 · Displayed: 22 (100,0%) · Dro... | Profile: Default

tcpdump

- Sniffer de rede: monitora o tráfego de rede recebido por uma interface
- Funciona somente em modo texto
- Permite filtrar o tráfego diretamente na linha de comando
- Exemplo:

Monitorar o tráfego da interface eth3

```
$ sudo tcpdump –i eth3 –v
```

Filtrar o tráfego por endereço de destino:

```
$ sudo tcpdump –i eth3 dst host 10.32.143.188
```

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ sudo tcpdump -i eth3 -c 8 -v
tcpdump: listening on eth3, link-type EN10MB (Ethernet), capture size 65535 bytes
16:14:59.590824 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 84)
    labredes-OptiPlex-3011.local > labredes-OptiPlex-3010.local: ICMP echo request, id 5496, seq
 892, length 64
16:14:59.590860 IP (tos 0x0, ttl 64, id 8809, offset 0, flags [none], proto ICMP (1), length 84)
    labredes-OptiPlex-3010.local > labredes-OptiPlex-3011.local: ICMP echo reply, id 5496, seq 8
92, length 64
16:14:59.591551 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 72)
    labredes-OptiPlex-3010.local.16826 > tanatau.pucrsnet.br.domain: 37764+ PTR? 212.143.32.10.i
n-addr.arpa. (44)
16:14:59.592284 IP (tos 0x0, ttl 125, id 18944, offset 0, flags [none], proto UDP (17), length 1
48)
    tanatau.pucrsnet.br.domain > labredes-OptiPlex-3010.local.16826: 37764 NXDomain* 0/1/0 (120)
16:14:59.592957 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 72)
    labredes-OptiPlex-3010.local.48862 > tanatau.pucrsnet.br.domain: 55045+ PTR? 188.143.32.10.i
n-addr.arpa. (44)
16:14:59.593611 IP (tos 0x0, ttl 125, id 18945, offset 0, flags [none], proto UDP (17), length 1
48)
    tanatau.pucrsnet.br.domain > labredes-OptiPlex-3010.local.48862: 55045 NXDomain* 0/1/0 (120)
16:14:59.594140 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 70)
    labredes-OptiPlex-3010.local.49146 > tanatau.pucrsnet.br.domain: 24036+ PTR? 25.48.40.10.in-
addr.arpa. (42)
16:14:59.596875 IP (tos 0x0, ttl 125, id 18946, offset 0, flags [none], proto UDP (17), length 1
03)
    tanatau.pucrsnet.br.domain > labredes-OptiPlex-3010.local.49146: 24036* 1/0/0 25.48.40.10.in
-addr.arpa. PTR tanatau.pucrsnet.br. (75)
8 packets captured
8 packets received by filter
0 packets dropped by kernel
labredes@labredes-OptiPlex-3010 ~ $
```

ethtool

- Verificar o estado atual e configurar uma interface Ethernet
- Caso não esteja instalado:
  - sudo apt-get install ethtool
- Exemplos:

Verificar o estado atual de uma interface:
$ ethtool eth3

Forçar a velocidade para 10 Mbps
$ sudo ethtool –s eth3 speed 10 duplex full

Forçar a velocidade para 10 Mbps
$ sudo ethtool –s eth3 speed 100 duplex full

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ ethtool eth3
Settings for eth3:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Advertised pause frame use: Symmetric Receive-only
        Advertised auto-negotiation: Yes
        Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                             100baseT/Half 100baseT/Full
        Link partner advertised pause frame use: No
        Link partner advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
Cannot get wake-on-lan settings: Operation not permitted
        Current message level: 0x00000033 (51)
                               drv probe ifdown ifup
        Link detected: yes
labredes@labredes-OptiPlex-3010 ~ $
```

Velocidade da interface

ping

- Verificar a conectivade entre dois computadores
  - Envia pacotes do tipo ICMP ECHO_REQUEST para hosts na rede
- Exemplos:

Testar a conectivadade com um endereço na Internet.
$ ping www.terra.com.br

Testar a conectivadade com um computador na rede local (limitar em 4 pacotes)
$ ping 10.32.143.188 –c 4

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ ping 10.32.143.188 -c 10
PING 10.32.143.188 (10.32.143.188) 56(84) bytes of data.
64 bytes from 10.32.143.188: icmp_seq=1 ttl=64 time=0.208 ms
64 bytes from 10.32.143.188: icmp_seq=2 ttl=64 time=0.143 ms
64 bytes from 10.32.143.188: icmp_seq=3 ttl=64 time=0.192 ms
64 bytes from 10.32.143.188: icmp_seq=4 ttl=64 time=0.151 ms
64 bytes from 10.32.143.188: icmp_seq=5 ttl=64 time=0.234 ms
64 bytes from 10.32.143.188: icmp_seq=6 ttl=64 time=0.215 ms
64 bytes from 10.32.143.188: icmp_seq=7 ttl=64 time=0.170 ms
64 bytes from 10.32.143.188: icmp_seq=8 ttl=64 time=0.218 ms
64 bytes from 10.32.143.188: icmp_seq=9 ttl=64 time=0.173 ms
64 bytes from 10.32.143.188: icmp_seq=10 ttl=64 time=0.208 ms

--- 10.32.143.188 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.143/0.191/0.234/0.030 ms
labredes@labredes-OptiPlex-3010 ~ $
```

iperf

- Testar a capacidade de transmissão máxima entre dois computadores
  - Mede o desempenho da rede (largura de banda)
- Exemplos:

Iniciar o servidor em um computador:
$ iperf –s

Inicar o cliente em outro computador informando o endereço IP do servidor:
$ iperf –c 10.32.143.212

PC1 (servidor)

```
labredes@labredes-OptiPlex-3010 ~ $ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 10.32.143.212 port 5001 connected with 10.32.143.188 port 36430
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec   112 MBytes  94.1 Mbits/sec
```

PC2 (cliente)

```
labredes@labredes-OptiPlex-3010 ~ $ iperf -c 10.32.143.212
------------------------------------------------------------
Client connecting to 10.32.143.212, TCP port 5001
TCP window size: 22.9 KByte (default)
------------------------------------------------------------
[  3] local 10.32.143.188 port 36430 connected with 10.32.143.212 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec   112 MBytes  94.2 Mbits/sec
labredes@labredes-OptiPlex-3010 ~ $
```

route

- Verificar as configurações de roteamento do computador local
  - Normalmente apenas a rota padrão (gateway)

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.32.143.1     0.0.0.0         UG    0      0        0 eth3
10.32.143.0     0.0.0.0         255.255.255.0   U     1      0        0 eth3
labredes@labredes-OptiPlex-3010 ~ $ ip route
default via 10.32.143.1 dev eth3  proto static
10.32.143.0/24 dev eth3  proto kernel  scope link  src 10.32.143.212  metric 1
labredes@labredes-OptiPlex-3010 ~ $
```

traceroute

- Determinar a rota utilizada por pacotes IP para atingir um host de destino
  - Informa a sequência de roteadores intermediários
- Exemplos:

Verificar a rota para um endereço na internet
$ traceroute www.terra.com.br

Verificar a rota para um endereço na PUCRS:
$ traceroute www.pucrs.br

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ traceroute www.terra.com.br
traceroute to www.terra.com.br (208.84.244.116), 30 hops max, 60 byte packets
 1  10.32.143.1 (10.32.143.1)  0.216 ms  0.214 ms  0.272 ms
 2  10.30.73.251 (10.30.73.251)  1.358 ms  1.432 ms  1.662 ms
 3  10.0.7.18 (10.0.7.18)  1.358 ms  1.655 ms  1.709 ms
 4  10.0.7.4 (10.0.7.4)  1.728 ms  1.743 ms  1.949 ms
 5  201.54.129.1 (201.54.129.1)  1.867 ms  1.862 ms  1.873 ms
 6  puc.metropoa.tche.br (200.132.73.45)  1.941 ms  1.022 ms  1.013 ms
 7  mlx.poa.tche.br (200.19.246.4)  1.420 ms  1.452 ms  1.516 ms
 8  mxrs-lanrs-10g.bkb.rnp.br (200.143.255.161)  1.555 ms  1.544 ms  1.565 ms
 9  sc-rs-oi.bkb.rnp.br (200.143.252.58)  8.648 ms pr-rs-oi.bkb.rnp.br (200.143.
252.54)  16.490 ms sc-rs-oi.bkb.rnp.br (200.143.252.58)  8.647 ms
10  sp-pr-oi.bkb.rnp.br (200.143.252.61)  22.436 ms sp-sc-oi.bkb.rnp.br (200.143
.252.65)  22.336 ms  22.342 ms
11  * * *
12  198.32.125.76 (198.32.125.76)  172.576 ms  172.503 ms  172.466 ms
13  terra-v-100-dsw01-nap.tc.terra.com (98.142.238.209)  175.154 ms  175.185 ms
 175.121 ms
14  terra-v-91-dsw01-mia.tc.terra.com (98.142.238.226)  172.405 ms  172.013 ms
172.018 ms
15  www.terra.com.br (208.84.244.116)  173.464 ms  172.948 ms  172.928 ms
labredes@labredes-OptiPlex-3010 ~ $
```

nmap

- Explorar a rede e verificar presença de vulnerabilidades de segurança
  - Permite escanear redes e hosts rapidamente
- Exemplos:

Verificar quais as portas (serviços) estão abertas em um computador
$ sudo nmap 10.32.143.188

Descobrir todos os computadores ligados na rede local:
$ sudo nmap 10.32.143.0/24

Terminal

File Edit View Search Terminal Help

```
labredes@labredes-OptiPlex-3010 ~ $ sudo nmap 10.32.143.188

Starting Nmap 6.40 ( http://nmap.org ) at 2014-08-11 17:02 BRT
Nmap scan report for 10.32.143.188
Host is up (0.00018s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3000/tcp open  ppp
MAC Address: A4:1F:72:F5:90:4A (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
labredes@labredes-OptiPlex-3010 ~ $
```