

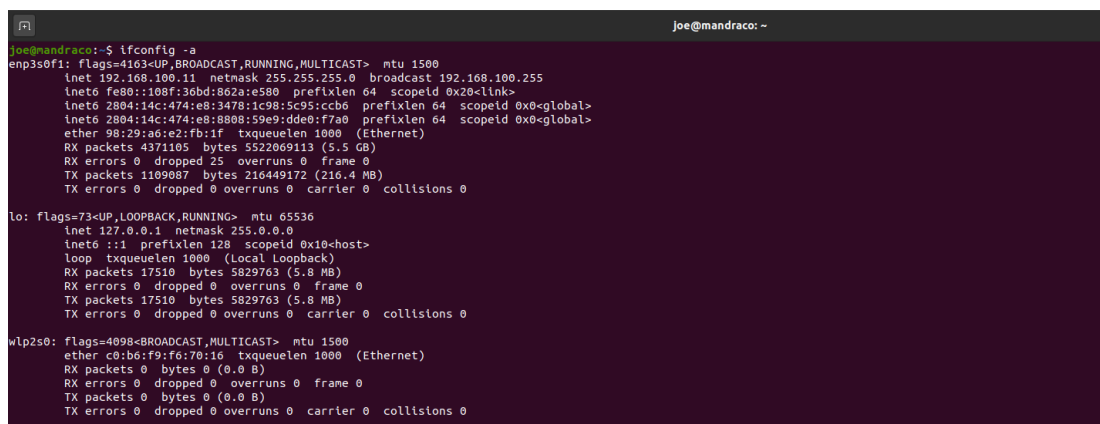
Trabalho 1 - Programação de redes de computadores (MC833)

José Ribeiro Neto - RA 176665

1. Considere para esta questão o comando `ifconfig`.

(a) Qual opção deve ser usada para exibir informações sobre todas as interfaces de rede?

R: Comando usado: `ifconfig -a`. Usamos a flag "a" para mostrar todas as interfaces.



```
joe@mandraco: ~  
joe@mandraco:~$ ifconfig -a  
enp3s9f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.100.11 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::108f:36bd:862a:e580 prefixlen 64 scopeid 0x20<link>  
    inet6 2804:14c:474:e8:3478:1c98:5c95:ccb6 prefixlen 64 scopeid 0x0<global>  
    inet6 2804:14c:474:e8:8808:59e9:dde0:f7a0 prefixlen 64 scopeid 0x0<global>  
    ether 98:29:3a:6a:2:fb:1f txqueuelen 1000 (Ethernet)  
    RX packets 4371105 bytes 5522069113 (5.5 GB)  
    RX errors 0 dropped 25 overruns 0 frame 0  
    TX packets 1109087 bytes 216449172 (216.4 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 17510 bytes 5829763 (5.8 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 17510 bytes 5829763 (5.8 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlp2s0: flags=4098<BROADCAST,MULTICAST> mtu 1500  
    ether c0:b6:f9:f6:70:16 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 1: Resposta da questão 1a

(b) O que deve ser feito para exibir somente informações de uma interface específica?

R: `ifconfig <interface_de_interesse>`. O segundo argumento representa a interface na qual gostaríamos de obter informações.

```
joe@mandraco: ~  
joe@mandraco:~$ ifconfig enp3s0f1  
enp3s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.100.11  netmask 255.255.255.0  broadcast 192.168.100.255  
    inet6 fe80::108f:36bd:862a:e580  prefixlen 64  scopeid 0x20<link>  
    inet6 2804:14c:474:e8:3478:1c98:5c95:ccb6  prefixlen 64  scopeid 0x0<global>  
    inet6 2804:14c:474:e8:8808:59e9:dde0:f7a0  prefixlen 64  scopeid 0x0<global>  
    ether 98:29:a6:e2:fb:1f  txqueuelen 1000  (Ethernet)  
    RX packets 4467383  bytes 5645634982 (5.6 GB)  
    RX errors 0  dropped 26  overruns 0  frame 0  
    TX packets 1129470  bytes 226565300 (226.5 MB)  
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  
joe@mandraco:~$
```

Figure 2: Resposta da questão 1b

2. Através da execução do comando nslookup seguido dos parâmetros adequados, responda à seguinte questões:

(a) Quais são os endereços IP do host `www.unicamp.br`?

R: Endereços IP do host `www.unicamp.br` = $\{143.106.143.186\}$. Neste caso, apenas um IP foi encontrado para o host da unicamp.

```
joe@mandraco: ~  
joe@mandraco:~$ nslookup www.unicamp.br  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
www.unicamp.br canonical name = 143-106-143-186.nuven.unicamp.br.  
Name:   143-106-143-186.nuven.unicamp.br  
Address: 143.106.143.186  
joe@mandraco:~$
```

Figure 3: Resposta da questão 2a

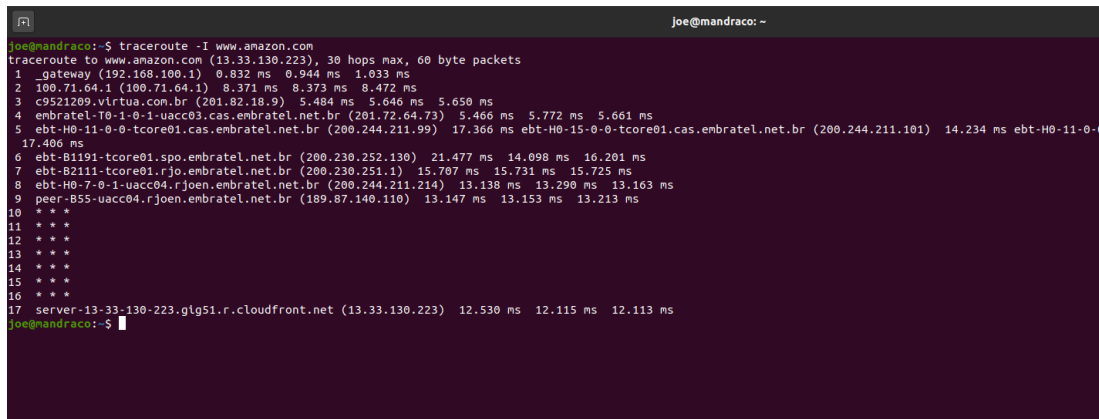
(b) Há alguma vantagem em haver mais de um endereço IP?

R: Vários endereços associados com o mesmo host DNS permitem redundância de servidores, isto é, se um servidor com IP X cair, tem disponível outro servidor com IP Y pra responder request realizazdos. Também, podemos implementar um esquema de load-balancing na existência de múltiplos IPs associados com o mesmo host DNS; assim, metade dos requests podem ser direcionados ao servidor X e a outra metade ao servidor Y.

3. Através da execução do comando traceroute seguido dos parâmetros adequados, responda à seguinte questão:

- (a) Quantos roteadores estão entre a sua estação e o host `www.amazon.com`? Pelos nomes dos roteadores, quantos deles estão localizados no Brasil?

R: Rodamos o comando `traceroute -I` para mostrar o caminho de roteadores percorrido até que o pacote atinja o host de destino. Usamos a flag `-I` para forçar o uso do protocolo ICMP. Foram encontrados no caminho 10 roteadores entre minha estação e o host da amazon. Pelo nome, 7 possuem o domínio `br` (portanto, estão no brasil), e 2 eu sei que estão localizados no Brasil, pois são os roteadores do meu ISP (2) e o roteador da minha casa (1).



```
joe@mandraco: ~  
joe@mandraco:~$ traceroute -I www.amazon.com  
traceroute to www.amazon.com (13.33.130.223), 30 hops max, 60 byte packets  
1 _gateway (192.168.100.1) 0.832 ms 0.944 ms 1.033 ms  
2 100.71.64.1 (100.71.64.1) 8.371 ms 8.373 ms 8.472 ms  
3 c9521209.virtua.com.br (201.82.18.9) 5.484 ms 5.646 ms 5.650 ms  
4 embratel-T0-1-0-1-uacc03.cas.embratel.net.br (201.72.64.73) 5.466 ms 5.772 ms 5.661 ms  
5 ebt-H0-11-0-0-tcore01.cas.embratel.net.br (200.244.211.99) 17.366 ms ebt-H0-15-0-0-tcore01.cas.embratel.net.br (200.244.211.101) 14.234 ms ebt-H0-11-0-0-  
17.406 ms  
6 ebt-B1191-tcore01.spo.embratel.net.br (200.230.252.130) 21.477 ms 14.098 ms 16.201 ms  
7 ebt-B2111-tcore01.rjo.embratel.net.br (200.230.251.1) 15.707 ms 15.731 ms 15.725 ms  
8 ebt-H0-7-0-1-uacc04.rjoen.embratel.net.br (200.244.211.214) 13.138 ms 13.290 ms 13.163 ms  
9 peer-B55-uacc04.rjoen.embratel.net.br (189.87.140.110) 13.147 ms 13.153 ms 13.213 ms  
10 * * *  
11 * * *  
12 * * *  
13 * * *  
14 * * *  
15 * * *  
16 * * *  
17 server-13-33-130-223.glg51.r.cloudfront.net (13.33.130.223) 12.530 ms 12.115 ms 12.113 ms  
joe@mandraco:~$
```

Figure 4: Resposta da questão 3a

4. Através da execução do comando telnet, seguido dos parâmetros adequados, responda às seguintes questões:

- (a) É possível conectar-se com este comando em um servidor HTTP? Se sim, como deve-se executar o comando para conectar-se no host `www.amazon.com` na porta padrão do HTTP?

R: Sim, podemos. Basta especificarmos o IP servidor (ou host DNS) seguido da porta na qual queremos nos conectar. Ou seja, `telnet <host> <porta>`

```
joe@mandraco: ~  
joe@mandraco:~$ telnet www.amazon.com 80  
Trying 23.62.56.133...  
Connected to e15316.e22.akamaiedge.net.  
Escape character is '^['.
```

Figure 5: Resposta da questão 4a

- (b) Caso não haja um servidor escutando na porta passada pelo comando telnet, o que ocorre? Justifique.

R: Telnet tenta abrir conexão com o servidor na porta especificada. Após um determinado tempo sem obter êxito (devido a inexistência de processo escutando na porta especificada), o telnet retorna mensagem de erro, devido ao timeout excedido.

```
joe@mandraco:~$ telnet www.amazon.com 81  
Trying 65.8.213.9...  
telnet: Unable to connect to remote host: Connection timed out  
joe@mandraco:~$
```

Figure 6: Resposta da questão 4b

- (c) A qual a camada da rede o telnet pertence?

R: Camada de aplicação

5. Acesse o site da DAC (<https://www.dac.unicamp.br/>) e, em paralelo em um terminal, verifique a saída do comando netstat. Quais são as informações fornecidas a respeito da conexão ao site da DAC?

R: Com a execução do comando, é mostrado que uma conexão TCP foi estabelecida (ESTABLISHED) corretamente entre cliente (mandraco, na porta 37162) com servidor (143.106.227.165, na porta 80). Então, após o estabelecimento, o fechamento da conexão pelo servidor é requisitada, na qual deve ser confirmada com o envio do acknowledgment do cliente. Então, após enviar o acknowledgment, o cliente entra em TIME_WAIT para esperar a confirmação de que o servidor recebeu o acknowledgment.

```
Joe@mandraco: ~  
joe@mandraco:~$ netstat | grep 143.106.227.165  
tcp        0      0 0 mandraco:37162    143-106-227-165.n:https ESTABLISHED  
tcp        0      0 0 mandraco:37160    143-106-227-165.n:https TIME_WAIT  
joe@mandraco:~$
```

Figure 7: Resposta da questão 5a

6. Considere a ferramenta TCPDUMP, e responda às seguintes questões (precisa de acesso root):

- (a) Utilizando o TCPDUMP corretamente com os filtros é possível somente capturar o tráfego HTTPS? Se sim, execute o comando junto com os filtros e anexe uma figura que comprove sua resposta no relatório. Se sua resposta foi não, então justifique-a

R: Sim. Basta que especifiquemos a porta da conexão destinada ao HTTP (porta 80).

```
root@mandraco: /home/joe  
root@mandraco:/home/joe# tcpdump port 80  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on enp3s0f1, link-type EN10MB (Ethernet), capture size 262144 bytes  
17:50:55.078620 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [S], seq 1154542986, win 64240, options [mss 1460,sackOK,TS val 1390454  
17:50:55.223686 IP 156.99.224.35.bc.googleusercontent.com.http > mandraco.52122: Flags [S.], seq 903256805, ack 1154542987, win 28160, options [mss 1412,sackO  
7], Length 0  
17:50:55.223718 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 1390454271 ecr 3281950636]  
17:50:55.223778 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 1390454271 ecr  
17:50:55.368740 IP 156.99.224.35.bc.googleusercontent.com.http > mandraco.52122: Flags [.], ack 88, win 204, options [nop,nop,TS val 3281950794 ecr 1390454271  
17:50:55.369258 IP 156.99.224.35.bc.googleusercontent.com.http > mandraco.52122: Flags [P.], seq 1:149, ack 88, win 204, options [nop,nop,TS val 3281950795 ec  
No Content  
17:50:55.369265 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [.], ack 149, win 501, options [nop,nop,TS val 1390454416 ecr 328195079  
17:50:55.369355 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [F.], seq 88, ack 149, win 501, options [nop,nop,TS val 1390454417 ecr  
17:50:55.369436 IP 156.99.224.35.bc.googleusercontent.com.http > mandraco.52122: Flags [F.], seq 149, ack 88, win 204, options [nop,nop,TS val 3281950795 ecr  
17:50:55.369445 IP mandraco.52122 > 156.99.224.35.bc.googleusercontent.com.http: Flags [.], ack 150, win 501, options [nop,nop,TS val 1390454417 ecr 328195079  
17:50:55.513468 IP 156.99.224.35.bc.googleusercontent.com.http > mandraco.52122: Flags [.], ack 89, win 204, options [nop,nop,TS val 3281950939 ecr 1390454417
```

Figure 8: Resposta da questão 6a

- (b) Utilizando o comando TCPDUMP seguido dos parâmetros corretos imprima somente os pacotes superiores a 64 bits. Indique qual foi a sequência de comandos utilizada.

R: Comando utilizado: tcpdump greater 64

```
root@mandraco:/home/joe

root@mandraco:/home/joe# tcpdump greater 64
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:51:50.081099 IP 192.168.100.17.49154 > 255.255.255.255.6667: UDP, length 188
17:51:50.089106 IP6 mandraco.40906 > 2804:14c:420:672:201:82:0:69.domain: 43693+ [Iau] PTR? 17.100.168.192.in-addr.arpa. (56)
17:51:50.092403 IP6 2804:14c:420:672:201:82:0:69.domain > mandraco.40906: 43693 ServFail 0/0/1 (56)
17:51:50.092562 IP6 mandraco.40906 > 2804:14c:420:672:201:82:0:69.domain: 43693+ PTR? 17.100.168.192.in-addr.arpa. (45)
17:51:50.096211 IP6 2804:14c:420:672:201:82:0:69.domain > mandraco.40906: 43693 ServFail 0/0/0 (45)
17:51:50.096394 IP6 mandraco.60525 > 2804:14c:420:672:201:82:0:69.domain: 43693+ [Iau] PTR? 17.100.168.192.in-addr.arpa. (56)
17:51:50.096632 IP6 2804:14c:420:672:201:82:0:69.domain > mandraco.60525: 43693 ServFail 0/0/1 (56)
17:51:50.099726 IP6 mandraco.60525 > 2804:14c:420:672:201:82:0:69.domain: 43693+ PTR? 17.100.168.192.in-addr.arpa. (45)
17:51:50.103104 IP6 2804:14c:420:672:201:82:0:69.domain > mandraco.60525: 43693 ServFail 0/0/0 (45)
17:51:50.103250 IP mandraco.35954 > _gateway.domain: 43693+ [Iau] PTR? 17.100.168.192.in-addr.arpa. (56)
17:51:50.108708 IP _gateway.domain > mandraco.35954: 43693 ServFail 0/0/1 (56)
17:51:50.108797 IP mandraco.35954 > _gateway.domain: 43693+ PTR? 17.100.168.192.in-addr.arpa. (45)
17:51:50.114779 IP _gateway.domain > mandraco.35954: 43693 ServFail 0/0/0 (45)
17:51:50.117116 IP mandraco.45202 > _gateway.domain: 14932+ [Iau] PTR? 0.6.0.0.0.0.0.2.8.0.0.1.0.2.0.2.7.6.0.0.2.4.0.c.4.1.0.4.0.8.2.ip6.arpa. (101)
17:51:50.117733 IP _gateway.domain > mandraco.45202: 14932 NXDomain 0/0/1 (101)
17:51:50.117810 IP mandraco.45202 > _gateway.domain: 14932+ PTR? 0.6.0.0.0.0.0.2.8.0.0.1.0.2.0.2.7.6.0.0.2.4.0.c.4.1.0.4.0.8.2.ip6.arpa. (90)
17:51:50.118232 IP _gateway.domain > mandraco.45202: 14932 NXDomain 0/0/0 (90)
17:51:50.120444 IP mandraco.53529 > _gateway.domain: 7294+ [Iau] PTR? 6.b.c.c.5.9.c.5.8.9.c.1.8.7.4.3.8.e.0.0.4.7.4.0.c.4.1.0.4.0.8.2.ip6.arpa. (101)
17:51:50.121116 IP _gateway.domain > mandraco.53529: 7294 NXDomain 0/0/1 (101)
17:51:50.121187 IP mandraco.53529 > _gateway.domain: 7294+ PTR? 6.b.c.c.5.9.c.5.8.9.c.1.8.7.4.3.8.e.0.0.4.7.4.0.c.4.1.0.4.0.8.2.ip6.arpa. (90)
17:51:50.121681 IP _gateway.domain > mandraco.53529: 7294 NXDomain 0/0/0 (90)
```

Figure 9: Resposta da questão 6b

- (c) Utilizando o TCPDUMP seguido de filtros, imprima somente os resultados que tiverem a flag ‘ACK’. Insira o comando seguido dos filtros e uma figura no seu relatório para comprovar o sucesso.

R: Comando utilizado: `tcpdump 'tcp[tcpflags] == tcp-ack'`. Utilizamos o “tcpflags” pra indicar que estamos interessados no octeto 13 do cabeçalho TCP, e mais especificamente, utilizamos o ‘tcbpck’ para indicar que estamos interessados em mostrar pacotes com a flag ACK do octeto setada.

```
root@mandraco:/home/joe

root@mandraco:/home/joe# tcpdump 'tcp[tcpflags] == tcp-ack'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:59:26.738751 IP mandraco.43318 > 104.16.30.34.https: Flags [.], ack 3937388776, win 501, length 0
17:59:26.738810 IP mandraco.37030 > a104-110-64-216.deploy.static.akamaitechnologies.com.https: Flags [.], ack 565398945, win 501, options [nop,nop,TS val 277
17:59:26.741803 IP a104-110-64-216.deploy.static.akamaitechnologies.com.https > mandraco.37030: Flags [.], ack 1, win 250, options [nop,nop,TS val 461623076 e
17:59:26.745363 IP 104.16.30.34.https > mandraco.43318: Flags [.], ack 1, win 67, length 0
17:59:28.181853 IP mandraco.56788 > 192.168.100.12.8009: Flags [.], ack 1146154349, win 6157, options [nop,nop,TS val 347068342 ecr 5646998], length 0
17:59:28.786988 IP mandraco.37494 > 151.101.129.69.https: Flags [.], ack 401838122, win 1485, options [nop,nop,TS val 3642413310 ecr 2883976613], length 0
17:59:28.793929 IP 151.101.129.69.https > mandraco.37494: Flags [.], ack 1, win 70, options [nop,nop,TS val 2883987877 ecr 3642231852], length 0
17:59:29.090504 IP mandraco.42884 > 192.168.100.15.8009: Flags [.], ack 3105215740, win 6203, options [nop,nop,TS val 3291261038 ecr 2720503993], length 0
17:59:30.834743 IP mandraco.57358 > stackoverflow.com.https: Flags [.], ack 524800583, win 501, options [nop,nop,TS val 1393565456 ecr 1127756090], length 0
17:59:30.954155 IP stackoverflow.com.https > mandraco.57358: Flags [.], ack 1, win 61, options [nop,nop,TS val 1127803130 ecr 1393381394], length 0
```

Figure 10: Resposta da questão 6c

7. Considere a ferramenta Wireshark para responder às questões a seguir: (pergunta teórica)

- (a) Comparado às demais ferramentas apresentadas na aula de MC833 descreva quais são principais diferenças e vantagens de usar o Wireshark? Escolha pelo menos uma ferramenta/sniffer e elabore uma tabela comparativa para responder a questão.

R: Wireshark é uma ferramenta poderosa, tendo como principais diferenças o fato de possuir uma Graphics User Interface (GUI), e como principal vantagem seu esquema de

filtragem e seleção de pacotes, que permite a realização de queries mais elaborados, além de uma simples e rápida visualização do conteúdo de um pacote.

Sniffer	GUI	Multi-file Dumping	Display de Estatísticas
Tcpdump	Não	Não	Não
Wireshark	Sim	Sim	Sim

Wireshark pode fazer o dumping dos pacotes em múltiplos arquivos, enquanto que o tcpdump não pode. Wireshark também pode mostrar múltiplas estatísticas, sejam elas gerais (gráficos de IO de pacotes ao longo do tempo, sumário da captura, etc), como também específicas de protocolos (tempo de resposta entre o request e a resposta do mesmo).

- (b) Com o conhecimento adquirido sobre ferramentas e sniffers responda: Em uma rede com vários processos acontecendo ao mesmo tempo é possível gerenciar de forma isolada um único processo específico na rede utilizando ferramentas/sniffers apresentados nesta disciplina? Se sim, quais ferramentas e/ou sniffers você usaria? Justifique sua resposta. (OBS: Não é necessário apresentar comandos ou prints)

R: Sim, é possível. Basta que saibamos a porta X no qual o processo está conectado. Então podemos utilizar um tcpdump para mostrar somente informações recebidas na porta X. Outra forma de monitoramento, seria descobrir se o processo é o único no host a utilizar um dado protocolo. Então, ao invés de monitoramento por porta, poderíamos realizar as filtrações dos pacotes por protocolo.