



Instituto de Computação
Universidade Estadual de Campinas - Unicamp

Exercício 1

Alunos: Carlos Eduardo da Silva Santos e Felipe Correia Labbate
RA: 195396 e 196699

Campinas, 06 de Setembro de 2022

Sumário

1. Considere para esta questão os comando ifconfig e route	2
Quais as opções que devem ser usadas para exibir informações sobre todas as interfaces e uma interface específica, respectivamente?	2
Qual é o endereço de rede do endereço IP da máquina e qual o endereço de broadcast?	3
Indique e explique a tabela de roteamento da máquina e comente cada linha da tabela informando para que ela serve.	3
Comando para exibir a tabela de roteamento da máquina:	3
2. Através da execução do comando nslookup seguido dos parâmetros adequados, responda à seguintes questões	4
Qual o endereço IP do host www.unicamp.br?	4
Teve uma resposta do tipo “authoritative” ou “non-authoritative” na anterior questão? Explique que indica uma resposta de cada tipo como retorno do comando nslookup	4
Indique como usar o comando nslookup para obter o nome do DNS primário para o host www.unicamp.br	4
Indique como obter o DNS autoritativo de um domínio usando a ferramenta nslookup	5
3. Através da execução do comando traceroute seguido dos parâmetros adequados, responda à seguinte questão	6
Identifique o caminho utilizado para alcançar uma máquina dentro da Unicamp, por exemplo, www.dac.unicamp.br	6
Identifique o caminho que é utilizado para alcançar uma máquina dentro da Unicamp, por exemplo, www.google.com. Pelos nomes dos roteadores, quantos deles estão localizados no Brasil?	6
4. Através da execução do comando telnet, seguido dos parâmetros adequados, responda às seguintes questões	7
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?	7
Caso não haja um servidor escutando na porta passada pelo comando telnet, o que ocorre? Justifique	7
A qual a camada da rede o telnet pertence?	7
5. Acesse o site da Unicamp e, em paralelo em um terminal, verifique a saída do comando netstat. Quais são as informações fornecidas a respeito da conexão ao site da Unicamp?	8
6. Considere a ferramenta TCPDUMP, e responda às seguintes questões	9
Utilizando o TCPDUMP corretamente com os filtros é possível somente capturar o tráfego HTTPS? Se sim, execute o comando com os filtros e anexe uma figura que comprove sua resposta no relatório. Se sua resposta foi não, então justifique-a	9
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	9
7. Considere a ferramenta Wireshark para responder às questões a seguir:	10
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 apresente uma tabela comparativa para responder à questão	10
Na sua máquina, habilite o wireshark para capturar todos os tráfegos de redes na interface correta. Abra o navegador e visite o site da Unicamp e pare a captura do tráfego em wireshark. O tráfego capturado foi transportado por TCP ou UDP? Explique sua resposta. Quais são as portas e o endereço IP observados na captura desse tráfego?	10

1. Considere para esta questão os comando ifconfig e route

- Quais as opções que devem ser usadas para exibir informações sobre todas as interfaces e uma interface específica, respectivamente?

Comando para exibir as informações de todas as interfaces:

```
ifconfig
```

```
bash-5.1$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:3a:a9:07:ef txqueuelen 0 (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

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 143.106.16.20 netmask 255.255.255.192 broadcast 143.106.16.63
    inet6 fe80::fab1:56ff:fefc:fb8b prefixlen 64 scopeid 0x20<link>
    ether f8:b1:56:fc:fb:8b txqueuelen 1000 (Ethernet)
    RX packets 339531 bytes 326960002 (311.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 270533 bytes 213966018 (204.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7c00000-f7c20000

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 28 bytes 2976 (2.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2976 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Comando para exibir as informações sobre uma interface específica:

```
ifconfig <nome_da_interface>
```

```
bash-5.1$ ifconfig eno1
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 143.106.16.20 netmask 255.255.255.192 broadcast 143.106.16.63
    inet6 fe80::fab1:56ff:fefc:fb8b prefixlen 64 scopeid 0x20<link>
    ether f8:b1:56:fc:fb:8b txqueuelen 1000 (Ethernet)
    RX packets 339712 bytes 326987543 (311.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 271038 bytes 214547093 (204.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7c00000-f7c20000
```

- b. Qual é o endereço de rede do endereço IP da máquina e qual o endereço de broadcast?

Endereço de rede do endereço IP: 143.106.16.20

Endereço de broadcast: 143.106.16.63

```
bash-5.1$ ifconfig eno1
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 143.106.16.20 netmask 255.255.255.192 broadcast 143.106.16.63
    inet6 fe80::fab1:56ff:fe8b:fb8b prefixlen 64 scopeid 0x20<link>
    ether f8:b1:56:fc:fb:8b txqueuelen 1000 (Ethernet)
    RX packets 339712 bytes 326987543 (311.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 271038 bytes 214547093 (204.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 20 memory 0xf7c00000-f7c20000
```

- c. Indique e explique a tabela de roteamento da máquina e comente cada linha da tabela informando para que ela serve.

Comando para exibir a tabela de roteamento da máquina:

```
route
```

```
bash-5.1$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 0 0 0 eno1
143.106.16.0 0.0.0.0 255.255.255.192 U 0 0 0 eno1
link-local 0.0.0.0 255.255.0.0 U 1002 0 0 0 eno1
172.17.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0
```

Destination:

- default: caso o tráfego não esteja definido em nenhuma outra regra na *routing table*, essa será a rota utilizada.
- 143.106.16.0: relacionado à rede da Unicamp
- link-local: usado apenas para comunicação entre a sub rede à qual a máquina está conectada.
- 172.17.0.0: relacionado à instalação da aplicação Docker, com o objetivo de conectar os containers com o mundo externo.

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

- a. Qual o endereço IP do host www.unicamp.br?

Endereço IP do host www.unicamp.br: 143.106.143.186

Comando utilizado:

```
nslookup www.unicamp.br
```

```
bash-5.1$ nslookup www.unicamp.br
Server:          143.106.16.144
Address:         143.106.16.144#53

Non-authoritative answer:
www.unicamp.br  canonical name = 143-106-143-186.nuvem.unicamp.br.
Name:   143-106-143-186.nuvem.unicamp.br
Address: 143.106.143.186
```

- b. Teve uma resposta do tipo “authoritative” ou “non-authoritative” na anterior questão? Explique que indica uma resposta de cada tipo como retorno do comando nslookup

Sim, resposta do tipo “Non-authoritative”.

A não autoritativa significa que a resposta não é buscada em um servidor DNS autoritativo, considerando o nome de domínio consultado. Já a resposta autoritativa vem de um DNS considerado autoritativo para este domínio

- c. Indique como usar o comando nslookup para obter o nome do DNS primário para o host www.unicamp.br

Basta usar o comando nslookup com o IP obtido na letra a.

Comando utilizado:

```
nslookup 143.106.143.186
```

```

bash-5.1$ nslookup 143.106.143.186
186.143.106.143.in-addr.arpa      name = 143-106-143-186.nuvem.unicamp.br.

Authoritative answers can be found from:
106.143.in-addr.arpa      nameserver = ns1.ansp.br.
106.143.in-addr.arpa      nameserver = ns3.unicamp.br.
106.143.in-addr.arpa      nameserver = ns1.unicamp.br.
ns3.unicamp.br  internet address = 143.106.2.133
ns1.unicamp.br  internet address = 143.106.2.2
ns3.unicamp.br  has AAAA address 2801:8a:4003::3
ns1.unicamp.br  has AAAA address 2801:8a:2003::2

```

- d. Indique como obter o DNS autoritativo de um domínio usando a ferramenta nslookup

Primeiramente entramos no nslookup usando o comando

```
nslookup
```

Posteriormente, definimos a query e o site

```
set querytype=soa
www.unicamp.br
```

Assim obtemos o dns autoritativo

```
nsmaster.nuvem.unicamp.br
```

```

bash-5.1$ nslookup
> set querytype=soa
> www.unicamp.br
Server:          143.106.16.144
Address:         143.106.16.144#53

Non-authoritative answer:
www.unicamp.br  canonical name = 143-106-143-186.nuvem.unicamp.br.

Authoritative answers can be found from:
nuvem.unicamp.br
    origin = nsmaster.nuvem.unicamp.br
    mail addr = suporte-infra.ccuec.unicamp.br
    serial = 2022082301
    refresh = 10800
    retry = 1800
    expire = 3600000
    minimum = 86400

```

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

- a. Identifique o caminho utilizado para alcançar uma máquina dentro da Unicamp, por exemplo, www.dac.unicamp.br

O caminho é obtido através do seguinte comando

```
traceroute www.dac.unicamp.br
```

```
bash-5.1$ traceroute www.dac.unicamp.br
traceroute to www.dac.unicamp.br (143.106.227.165), 30 hops max, 60 byte packets
 1 _gateway (143.106.16.62)  0.695 ms  1.080 ms  1.339 ms
 2 area2-gw.unicamp.br (143.106.1.65)  0.641 ms  0.630 ms  0.619 ms
 3 ptp-rtr-wan-tc04_sw-bb-tc04.unicamp.br (143.106.199.69)  1.291 ms  1.731 ms  ptp-rtr-wan-tc09_sw-bb-tc0
4.unicamp.br (143.106.199.85)  1.267 ms
 4 tc01-cor01-nuvem-gw.unicamp.br (143.106.199.212)  2.525 ms tc04-cor01-nuvem-gw.unicamp.br (143.106.199
.211)  1.244 ms tc01-cor01-nuvem-gw.unicamp.br (143.106.199.212)  2.500 ms
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
```

- b. Identifique o caminho que é utilizado para alcançar uma máquina dentro da Unicamp, por exemplo, www.google.com. Pelos nomes dos roteadores, quantos deles estão localizados no Brasil?

Utilizando o seguinte comando traçamos a rota

```
traceroute www.google.com
```

Pelos endereços é possível identificar 3 localizados no Brasil (terminado em .br)

```
bash-5.1$ traceroute www.google.com
traceroute to www.google.com (142.251.132.36), 30 hops max, 60 byte packets
 1 * * *
 2 area2-gw.unicamp.br (143.106.1.65)  0.505 ms  0.493 ms  0.481 ms
 3 ptp-rtr-wan-tc09_sw-bb-tc04.unicamp.br (143.106.199.85)  1.406 ms  1.759 ms  2.056 ms
 4 as15169.saopaulo.sp.ix.br (187.16.218.58)  4.418 ms  4.408 ms  4.397 ms
 5 74.125.243.1 (74.125.243.1)  4.385 ms  4.375 ms 74.125.243.65 (74.125.243.65)  5.730 ms
 6 216.239.56.193 (216.239.56.193)  4.621 ms  4.458 ms  4.437 ms
 7 gru14s36-in-f4.1e100.net (142.251.132.36)  4.425 ms  4.322 ms  4.527 ms
```

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?

Sim, é possível se conectar com um servidor HTTP usando o comando *telnet*. Deve-se usar a porta 80 para HTTP.

Comando utilizado:

```
telnet www.amazon.com 80
```

```
flabbate@BRCPQN0348:~$ telnet www.amazon.com 80
Trying 108.139.172.128...
Connected to d3ag4hukkh62yn.cloudfront.net.
Escape character is '^]'.

```

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

O comando fica em *hold* tentando se conectar com o servidor através da porta.

```
bash-5.1$ telnet www.amazon.com 9999
Trying 23.47.177.185...
```

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

O *telnet* pertence à camada de aplicação.

5. Acesse o site da Unicamp e, em paralelo em um terminal, verifique a saída do comando `netstat`. Quais são as informações fornecidas a respeito da conexão ao site da Unicamp?

Primeiramente executamos o comando

```
nslookup www.unicamp.br
```

para obter o endereço IP do site da Unicamp, `143.106.143.186`.

Comando `netstat` utilizado (executado com acesso *root* - `sudo`):

```
Comando: netstat -nltpa
```

juntamente de um `grep` com o IP obtido anteriormente para pegar apenas os resultados correspondentes ao site da Unicamp.

As informações retornadas são: Proto (protocolo), Recv-Q, Send-Q, Local Address, Foreign Address, State, PID/Program name

```
Flabbate@BRCPQN0348:~$ 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.nuvem.unicamp.br.
Name:   143-106-143-186.nuvem.unicamp.br
Address: 143.106.143.186

Flabbate@BRCPQN0348:~$ sudo netstat -nltpa | grep -e 143.106.143.186 -e State
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp    25        0 100.112.116.231:58582   143.106.143.186:443    CLOSE_WAIT 327074/chrome --typ
tcp    0         0 100.112.116.231:58584   143.106.143.186:443    ESTABLISHED 327074/chrome --typ
Flabbate@BRCPQN0348:~$
```

6. Considere a ferramenta TCPDUMP, e responda às seguintes questões

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

Sim, é possível capturar somente o tráfego HTTPS através do filtro da porta 443, porém o conteúdo é retornado encriptado, pois o tráfego do HTTPS é criptografado. Comando utilizado:

```
tcpdump -X port 443
```

```
Flabbate@BRCPQN0348:~$ sudo tcpdump -X port 443
[sudo] password for Flabbate:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:23:49.757938 IP BRCPQN0348.59920 > ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https: Flags [P.], seq 2166745298:2166745352, ack 3291807929, win 501, options [nop,nop,TS val 632779317 ecr 1507481427], length 54
 0x0000: 4500 006a da00 4000 32cd 6470 74e7 E..].@.2.dpt.
 0x0010: 12e7 417a ea10 01bb 8125 e90d c435 00b9 ..AZ.....%.5..
 0x0020: 8018 01f5 2e15 0000 0101 080a 25b7 7235 .....%.r5
 0x0030: 59da 5753 1703 0300 3198 d2a3 db8d dd0b Y.WS....1.....
 0x0040: 4d00 4456 3547 5c89 9555 0635 49fb 6ba2 M.OV5G\..UF5I.k.
 0x0050: fbee 3afe 5152 0209 13a8 44ba 9c0b 3354 ...QR....D...3T
 0x0060: af15 17ec 33b5 eef7 0ac9 .....3.....
20:23:49.772930 IP ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https > BRCPQN0348.59920: Flags [.], ack 54, win 8, options [nop,nop,TS val 1507485095 ecr 632779317], length 0
 0x0000: 4500 0034 f6d1 4000 3586 21ca 12e7 417a E..4.A@.5.1...Az
 0x0010: 6470 74e7 01bb ea10 c435 00b9 8125 e908 dpt.....S...%.
 0x0020: 8010 0008 d6a5 0000 0101 080a 59da 65a7 .....%.r5
 0x0030: 25b7 7235 .....%.r5
20:23:49.772967 IP ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https > BRCPQN0348.59920: Flags [P.], seq 1:57, ack 54, win 8, options [nop,nop,TS val 1507485096 ecr 632779317], length 56
 0x0000: 4500 006c f6d2 4000 3586 2191 12e7 417a E..l.B@.5.1...Az
 0x0010: 6470 74e7 01bb ea10 c435 00b9 8125 e908 dpt.....S...%.
 0x0020: 8018 0008 633d 0000 0101 080a 59da 65a8 ....C=.....Y.e.
 0x0030: 25b7 7235 1703 0300 338f 2b78 809e f9c5 %.r5....3..x....
 0x0040: 6e75 6894 22d3 1e02 0610 bfde 8ca0 0a8a nu..Y.....
 0x0050: 4e5b 7195 6463 2e59 4830 9f03 47b7 2e5c N[q.dc.YH0..G..
 0x0060: 3548 7932 2307 61a9 a108 067f SHy2#.a.....
20:23:49.772988 IP BRCPQN0348.59920 > ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https: Flags [.], ack 57, win 501, options [nop,nop,TS val 632779332 ecr 1507485096], length 0
 0x0000: 4500 0034 da09 4000 4000 3302 6470 74e7 E..4..@.3.dpt.
 0x0010: 12e7 417a ea10 01bb 8125 e908 c435 00f1 ..AZ.....%.5..
 0x0020: 8010 01f5 2ddf 0000 0101 080a 25b7 7244 .....%.rD
 0x0030: 59da 65a8 Y.e.
```

- b. Utilizando o TCPDUMP seguido de filtros, imprima somente os resultados que tiverem a flag 'ACK'. Insira o comando seguido dos filtros e uma figura na seu relatório para comprovar o sucesso

Comando utilizado (requer acesso *root* - sudo):

```
tcpdump "tcp[tcpflags] & (tcp-ack) != 0"
```

```
Flabbate@BRCPQN0348:~$ sudo tcpdump "tcp[tcpflags] & (tcp-ack) != 0"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:55:09.757972 IP BRCPQN0348.59920 > ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https: Flag
s [P.], seq 2166732482:2166732536, ack 3291781178, win 501, options [nop,nop,TS val 631059317 ecr 1
505755128], length 54
19:55:09.767172 IP ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https > BRCPQN0348.59920: Flag
s [.], ack 54, win 8, options [nop,nop,TS val 1505765127 ecr 631059317], length 0
19:55:09.767203 IP ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https > BRCPQN0348.59920: Flag
s [P.], seq 1:57, ack 54, win 8, options [nop,nop,TS val 1505765127 ecr 631059317], length 56
19:55:09.767223 IP BRCPQN0348.59920 > ec2-18-231-65-122.sa-east-1.compute.amazonaws.com.https: Flag
s [.], ack 57, win 501, options [nop,nop,TS val 631059326 ecr 1505765127], length 0
19:55:09.985949 IP BRCPQN0348.39334 > ec2-3-232-49-37.compute-1.amazonaws.com.https: Flags [P.], se
q 1662882578:1662882629, ack 3712964412, win 501, options [nop,nop,TS val 725535714 ecr 623618547],
length 51
19:55:10.154604 IP ec2-3-232-49-37.compute-1.amazonaws.com.https > BRCPQN0348.39334: Flags [P.], se
q 1:29, ack 51, win 114, options [nop,nop,TS val 623628547 ecr 725535714], length 28
19:55:10.154673 IP BRCPQN0348.39334 > ec2-3-232-49-37.compute-1.amazonaws.com.https: Flags [.], ack
29, win 501, options [nop,nop,TS val 725535882 ecr 623628547], length 0
19:55:10.206790 IP BRCPQN0348.46132 > ec2-54-236-127-231.compute-1.amazonaws.com.https: Flags [P.],
seq 3437311395:3437311476, ack 232631373, win 501, options [nop,nop,TS val 4147453597 ecr 11520065
60], length 81
19:55:10.360457 IP ec2-54-236-127-231.compute-1.amazonaws.com.https > BRCPQN0348.46132: Flags [P.],
seq 1:55, ack 81, win 122, options [nop,nop,TS val 1152016557 ecr 4147453597], length 54
19:55:10.360525 IP BRCPQN0348.46132 > ec2-54-236-127-231.compute-1.amazonaws.com.https: Flags [.],
ack 55, win 501, options [nop,nop,TS val 4147453751 ecr 1152016557], length 0
19:55:10.712144 IP BRCPQN0348.48584 > 20.190.173.146.https: Flags [.], ack 443931737, win 501, le
ngth 0
11 packets captured
12 packets received by filter
0 packets dropped by kernel
```

7. Considere a ferramenta Wireshark para responder às questões a seguir:

- 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 apresente uma tabela comparativa para responder à questão

A principal notável diferença e vantagem é que o wireshark utiliza interface gráfica para realizar suas ações, facilitando a utilização para usuários que não estão acostumados com linhas de comando, tal qual executamos com o tcpdump. Abaixo temos uma tabela comparando alguns aspectos entre o Wireshark e o tcpdump

	Wireshark	tcpdump
Interface Gráfica	Sim	Não
Interfaces de rede	Avançadas	Convencionais
Decodificação de pacotes	Possui	Menos eficiente
Filtros	Complexos	Simples

- Na sua máquina, habilite o wireshark para capturar todos os tráfegos de redes na interface correta. Abra o navegador e visite o site da Unicamp e pare a captura do tráfego em wireshark. O tráfego capturado foi transportado por TCP ou UDP? Explique sua resposta. Quais são as portas e o endereço IP observados na captura desse tráfego?

O tráfego foi transportado por TCP, conforme indicado na coluna “Protocol”
Endereços IP e portas observados (formato <endereço_ip>:<porta>):

- 100.112.116.231:58596, 100.112.116.231:58600
- 143.106.143.186:443 (endereço IP do host www.unicamp.br)

