

Nome: Nathan Medeiros Cristiano.

Turma: RED129005

## LABORATÓRIO 7

### USANDO MINHA MÁQUINA / IFSC

### COMPARANDO SOCKETS UDP E TCP

## **\*\*TCP\*\***

1- Você encontrou sockets abertos em todos os hosts (máquinas)?

- Sim!

```
root@Servidor:/# ss -nta | grep -E '33333|Local'
State  Recv-Q Send-Q Local Address:Port  Peer Address:Port Process
LISTEN 1      1      0.0.0.0:33333  0.0.0.0:*
ESTAB  0      0      10.0.0.10:33333 10.0.0.21:33876
ESTAB  0      0      10.0.0.10:33333 10.0.0.20:43722
```

2- Quais parâmetros apresentados para cada um deles?

```
root@Cliente1:/# ss -nta | grep -E '33333|Local'
State Recv-Q Send-Q Local Address:Port  Peer Address:Port Process
ESTAB 0      0      10.0.0.20:43722 10.0.0.10:33333
```

```
root@Cliente2:/# ss -nta | grep -E '33333|Local'
State Recv-Q Send-Q Local Address:Port  Peer Address:Port Process
ESTAB 0      0      10.0.0.21:33876 10.0.0.10:33333
```

3- Qual a relação entre os sockets clientes e servidor, número IP, portas etc?

- O cliente inicia a comunicação, conectando-se ao IP e à porta do servidor a partir de seu próprio IP e de uma porta qualquer. E também a relação é espelhada como visto.

#### Cliente 1

```
ESTAB 0      0      10.0.0.10:33333 10.0.0.20:43722
ESTAB 0      0      10.0.0.20:43722 10.0.0.10:33333
```

#### Cliente 2

```
ESTAB 0      0      10.0.0.21:33876 10.0.0.10:33333
ESTAB 0      0      10.0.0.10:33333 10.0.0.21:33876
```

#### 4-Identifique e "printe" o socket receptivo no Servidor

```
LISTEN 1 1 0.0.0.0:3333 0.0.0.0:*
```

#### 5-Para cada cliente, as três primeiras mensagens trocadas apresentam a camada de aplicação, sim ou não? Explique. O que elas significam (3-way handshake)?

- Não apresentam camada de aplicação pois é apenas estabelecimento de comunicação com o servidor, não estamos enviando requisitando nada! Apenas fizemos o **3-way handshake "SYN (Sincronizar)", SYN-ACK (Sincronizar-Reconhecer), ACK (Reconhecer)**.

#### 6- Encontre a frase/palavra escrita enviada ao servidor (minúscula) e a resposta em maiúscula?

##### Cliente 1-

```
0000 42 00 aa 00 00 02 42 00 aa 00 00 00 08 00 45 00 B....B. ....E.
0010 00 42 b0 e0 40 00 40 06 75 b8 0a 00 00 14 0a 00 .B>@.@. ....
0020 00 0a aa ca 82 35 08 df 13 8f c9 96 75 17 80 18 ....5.. ..u...
0030 01 f6 14 52 00 00 01 01 08 0a fc 8f 5c 84 13 2b ...R.... ..\..+
0040 a0 e3 6f 69 20 64 6f 20 63 6c 69 65 6e 74 65 31 ..oi do cliente1
```

```
0000 42 00 aa 00 00 00 42 00 aa 00 00 02 08 00 45 00 B....B. ....E.
0010 00 42 3e f3 40 00 40 06 e7 a5 0a 00 00 0a 0a 00 .B>@.@. ....
0020 00 14 82 35 aa ca c9 96 75 17 08 df 13 9d 80 18 ....5... u.....
0030 01 fd 14 52 00 00 01 01 08 0a 13 57 e1 e1 fc 8f ...R.... ..W....
0040 5c 84 4f 49 20 44 4f 20 43 4c 49 45 4e 54 45 31 \OI DO CLIENTE1
```

##### Cliente 2-

```
0000 42 00 aa 00 00 02 42 00 aa 00 00 01 08 00 45 00 B....B. ....E.
0010 00 42 a5 ed 40 00 40 06 80 aa 0a 00 00 15 0a 00 .B>@.@. ....
0020 00 0a 84 54 82 35 04 f6 41 85 8f bb 11 8f 80 18 ...T.5.. A.....
0030 01 f6 14 53 00 00 01 01 08 0a d9 ff 3c a7 aa 95 ...S.... ..<...
0040 7a be 6f 69 20 64 6f 20 63 6c 69 65 6e 74 65 32 zoi do cliente2
```

```
0000 42 00 aa 00 00 01 42 00 aa 00 00 02 08 00 45 00 B....B. ....E.
0010 00 42 30 50 40 00 40 06 f6 47 0a 00 00 0a 0a 00 .B0P@.@. .G....
0020 00 15 82 35 84 54 8f bb 11 8f 04 f6 41 93 80 18 ...5.T.. ..A...
0030 01 fd 14 53 00 00 01 01 08 0a aa c1 cb e3 d9 ff ...S.... ....
0040 3c a7 4f 49 20 44 4f 20 43 4c 49 45 4e 54 45 32 <OI DO CLIENTE2
```

7- Qual o tamanho dos pacotes contendo as mensagens: i) *Data* (camada 5) e ii) *Total Length* (camada 3). Qual a relação entre estes valores?

**\*\*PARA AMBOS FORAM O MESMO TAMANHO\*\***

- Total Length: 66
- Data (14 bytes)

8- As últimas 3 mensagens, de cada cliente, contém o fechamento de conexão, explique-as.

- FIN,ACK. Ele encerra a conexão TCP, ele indica que um lado da conexão está pronto para encerrá-la, e ao mesmo tempo confirma o recebimento de dados do outro lado.

9- Qual é o protocolo da camada de transporte nessa troca de mensagens?

- Protocolo TCP!

10- Qual o número identificador de protocolo TCP no pacote IP?  
Dica: na janela central abra o campo *Internet Protocol* e procure a string *Protocol*.

- Protocol: TCP (6)

tcp.port==33333						
No.	Time	Source	Destination	Protocol	Length	Info
3	31.449173	10.0.0.20	10.0.0.10	TCP	74	43722 → 33333 [SYN] Seq=0 W
4	31.449189	10.0.0.10	10.0.0.20	TCP	74	33333 → 43722 [SYN, ACK] Seq
5	31.449207	10.0.0.20	10.0.0.10	TCP	66	43722 → 33333 [ACK] Seq=1 A
7	34.938372	10.0.0.21	10.0.0.10	TCP	74	33876 → 33333 [SYN] Seq=0 W
8	34.938389	10.0.0.10	10.0.0.21	TCP	74	33333 → 33876 [SYN, ACK] Seq
9	34.938406	10.0.0.21	10.0.0.10	TCP	66	33876 → 33333 [ACK] Seq=1 A

tcp.port==33333						
No.	Time	Source	Destination	Protocol	Length	Info
3	31.449173	10.0.0.20	10.0.0.10	TCP	74	43722 → 33333 [SYN] Seq=0 W
4	31.449189	10.0.0.10	10.0.0.20	TCP	74	33333 → 43722 [SYN, ACK]
5	31.449207	10.0.0.20	10.0.0.10	TCP	66	43722 → 33333 [ACK] Seq=1 A
7	34.938372	10.0.0.21	10.0.0.10	TCP	74	33876 → 33333 [SYN] Seq=0 W
8	34.938389	10.0.0.10	10.0.0.21	TCP	74	33333 → 33876 [SYN, ACK]
9	34.938406	10.0.0.21	10.0.0.10	TCP	66	33876 → 33333 [ACK] Seq=1 A
45	2931.671...	10.0.0.20	10.0.0.10	TCP	80	43722 → 33333 [PSH, ACK]
46	2931.671...	10.0.0.10	10.0.0.20	TCP	66	33333 → 43722 [ACK] Seq=1 A
47	2931.671...	10.0.0.10	10.0.0.20	TCP	80	33333 → 43722 [PSH, ACK]
48	2931.671...	10.0.0.20	10.0.0.10	TCP	66	43722 → 33333 [ACK] Seq=1 A
49	2931.671...	10.0.0.10	10.0.0.20	TCP	66	33333 → 43722 [FIN, ACK]
50	2931.671...	10.0.0.20	10.0.0.10	TCP	66	43722 → 33333 [FIN, ACK]
51	2931.671...	10.0.0.10	10.0.0.20	TCP	66	33333 → 43722 [ACK] Seq=1 A
52	2931.671...	10.0.0.20	10.0.0.10	TCP	66	43722 → 33333 [ACK] Seq=1 A
57	2939.295...	10.0.0.21	10.0.0.10	TCP	80	33876 → 33333 [PSH, ACK]
58	2939.295...	10.0.0.10	10.0.0.21	TCP	66	33333 → 33876 [ACK] Seq=1 A
59	2939.295...	10.0.0.10	10.0.0.21	TCP	80	33333 → 33876 [PSH, ACK]
60	2939.295...	10.0.0.21	10.0.0.10	TCP	66	33876 → 33333 [ACK] Seq=1 A
61	2939.295...	10.0.0.10	10.0.0.21	TCP	66	33333 → 33876 [FIN, ACK]
62	2939.295...	10.0.0.21	10.0.0.10	TCP	66	33876 → 33333 [FIN, ACK]
63	2939.295...	10.0.0.10	10.0.0.21	TCP	66	33333 → 33876 [ACK] Seq=1 A
64	2939.296...	10.0.0.21	10.0.0.10	TCP	66	33876 → 33333 [ACK] Seq=1 A

## **\*\*UDP\*\***

### **1- Verifique os sockets**

- **Identifique e anote os sockets abertos.**

Socket Cliente 1: 10.0.0.20:52544

Socket Cliente 1: 10.0.0.21:39120

- **Identifique e anote o socket receptivo do servidor.**

O socket receptivo do servidor é : 10.0.0.10:22222

```
root@Cliente1:/# ss -ua
State  Recv-Q  Send-Q      Local Address:Port      Peer Address:Port    Process
ESTAB  0          0          10.0.0.20:52544        10.0.0.10:22222
root@Cliente1:/# █
```

```
root@Cliente2:/# ss -ua
State  Recv-Q  Send-Q      Local Address:Port      Peer Address:Port    Process
ESTAB  0          0          10.0.0.21:39120        10.0.0.10:22222
root@Cliente2:/# █
```

### **2. PERGUNTAS baseadas na captura:**

udp.port==22222						
No.	Time	Source	Destination	Protocol	Length	Info
4	68.501297	10.0.0.20	10.0.0.10	UDP	45	52544 → 22222 Len=3
5	68.501416	10.0.0.10	10.0.0.20	UDP	45	22222 → 52544 Len=3
10	76.365001	10.0.0.21	10.0.0.10	UDP	46	39120 → 22222 Len=4
11	76.365102	10.0.0.10	10.0.0.21	UDP	46	22222 → 39120 Len=4

```
root@Cliente1:/# netcat -u 10.0.0.10 22222
oi
OI
█
```

```
root@Cliente2:/# netcat -u 10.0.0.10 22222
ola
OLA
█
```

- Em algum momento foi identificado algum procedimento para estabelecimento de conexão?

Não! Ele envia dados diretamente para o servidor.

- Em algum campo do UDP existe numeração de mensagens?

Não! O cabeçalho do UDP é muito simples e não possui um campo para número de sequência.

- Qual o número identificador de protocolo UDP no pacote IP? Dica: na janela central abra o campo *Internet Protocol* e procure a string *Protocol*.

Protocol: UDP (17)

- Qual é o *checksum* no pacote (datagrama) UDP? Qual é o formato apresentado? Quantos bits ele possui?

Ele é um campo no cabeçalho UDP usado para verificação de erros básicos. É apresentado em binário, complemento de 1, e ele possui 16 bits.

- É possível capturar toda a troca de mensagens e inclusive capturar o texto passado do cliente para o servidor?

Se não estiverem criptografados, sim, é possível!

- Qual foi a sequência numérica do campo *Data* em seu teste? Qual o significado?

Isso é um "oi" em hexadecimal e ASCII.

▾ Data (3 bytes)  
Data: 6f690a  
[Length: 3]

- Qual é o protocolo da camada de transporte nessa troca de mensagens?

UDP, User Datagram Protocol.

### 3- Comparativo entre TCP e UDP:

- Quantas mensagens foram trocadas entre o servidor e o cliente em cada um dos protocolos para atingir o mesmo objetivo?

No TCP foram cerca 20 e no UDP foram apenas 4

- O que justifica a diferença na quantidade de mensagens trocadas?

O protocolo UDP, não utiliza o 3 way handshake para cada pacote enviado, economizando processamento e troca de mensagens cliente-servidor.

- Discuta as vantagens e desvantagens de cada protocolo.

- **TCP:** Maior confiabilidade e garantia dos pacotes transitados, porém tem menor velocidade e mais processamento
- **UDP:** Maior velocidade, menos processamento, menor custo, porém bem menos confiável não se encaixando em alguns usos.