

Trabalho Prático Nº.1

Protocolos da Camada de Transporte

Grupo nº65



a100824
Gonçalo Daniel Machado
Costa



a100593
Marta Sofia Matos Castela
Queirós Gonçalves



a100743
Marta Raquel da Silva
Rodrigues

Parte I: Instalação, configuração e utilização de serviços de transferência de ficheiros

Resultados Obtidos:

1. Ping

- Portatil1

```
<36711/Portatil1.conf# ping -c 20 10.4.4.1 | tee file-ping-output
PING 10.4.4.1 (10.4.4.1) 56(84) bytes of data.
64 bytes from 10.4.4.1: icmp_seq=1 ttl=61 time=3.15 ms
64 bytes from 10.4.4.1: icmp_seq=2 ttl=61 time=1.62 ms
64 bytes from 10.4.4.1: icmp_seq=3 ttl=61 time=1.77 ms
64 bytes from 10.4.4.1: icmp_seq=4 ttl=61 time=1.11 ms
64 bytes from 10.4.4.1: icmp_seq=5 ttl=61 time=1.92 ms
64 bytes from 10.4.4.1: icmp_seq=6 ttl=61 time=1.27 ms
64 bytes from 10.4.4.1: icmp_seq=7 ttl=61 time=1.81 ms
64 bytes from 10.4.4.1: icmp_seq=8 ttl=61 time=1.79 ms
64 bytes from 10.4.4.1: icmp_seq=9 ttl=61 time=1.88 ms
64 bytes from 10.4.4.1: icmp_seq=10 ttl=61 time=1.52 ms
64 bytes from 10.4.4.1: icmp_seq=11 ttl=61 time=0.458 ms
64 bytes from 10.4.4.1: icmp_seq=12 ttl=61 time=1.68 ms
64 bytes from 10.4.4.1: icmp_seq=13 ttl=61 time=1.88 ms
64 bytes from 10.4.4.1: icmp_seq=14 ttl=61 time=0.426 ms
64 bytes from 10.4.4.1: icmp_seq=15 ttl=61 time=1.33 ms
64 bytes from 10.4.4.1: icmp_seq=16 ttl=61 time=1.93 ms
64 bytes from 10.4.4.1: icmp_seq=17 ttl=61 time=1.96 ms
64 bytes from 10.4.4.1: icmp_seq=18 ttl=61 time=1.24 ms
64 bytes from 10.4.4.1: icmp_seq=19 ttl=61 time=1.94 ms
64 bytes from 10.4.4.1: icmp_seq=20 ttl=61 time=1.80 ms

--- 10.4.4.1 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19050ms
rtt min/avg/max/mdev = 0.426/1.624/3.147/0.565 ms
```

Figura 1 - Output do comando *ping -c 20 10.4.4.1 | tee file-ping-output* para o Portatil1

- PC1

```
<PC1.conf# ping -c 20 10.4.4.1 | tee file-ping-output
PING 10.4.4.1 (10.4.4.1) 56(84) bytes of data.
64 bytes from 10.4.4.1: icmp_seq=1 ttl=61 time=10.6 ms
64 bytes from 10.4.4.1: icmp_seq=2 ttl=61 time=6.20 ms
64 bytes from 10.4.4.1: icmp_seq=3 ttl=61 time=5.82 ms
64 bytes from 10.4.4.1: icmp_seq=4 ttl=61 time=5.93 ms
64 bytes from 10.4.4.1: icmp_seq=4 ttl=61 time=6.91 ms (DUP!)
64 bytes from 10.4.4.1: icmp_seq=5 ttl=61 time=5.44 ms
64 bytes from 10.4.4.1: icmp_seq=6 ttl=61 time=5.33 ms
64 bytes from 10.4.4.1: icmp_seq=7 ttl=61 time=6.83 ms
64 bytes from 10.4.4.1: icmp_seq=8 ttl=61 time=6.41 ms
64 bytes from 10.4.4.1: icmp_seq=9 ttl=61 time=5.73 ms
64 bytes from 10.4.4.1: icmp_seq=11 ttl=61 time=6.82 ms
64 bytes from 10.4.4.1: icmp_seq=11 ttl=61 time=6.82 ms (DUP!)
64 bytes from 10.4.4.1: icmp_seq=13 ttl=61 time=5.42 ms
64 bytes from 10.4.4.1: icmp_seq=14 ttl=61 time=5.34 ms
64 bytes from 10.4.4.1: icmp_seq=15 ttl=61 time=6.01 ms
64 bytes from 10.4.4.1: icmp_seq=16 ttl=61 time=6.92 ms
64 bytes from 10.4.4.1: icmp_seq=17 ttl=61 time=5.60 ms
64 bytes from 10.4.4.1: icmp_seq=18 ttl=61 time=5.61 ms
64 bytes from 10.4.4.1: icmp_seq=19 ttl=61 time=5.78 ms
64 bytes from 10.4.4.1: icmp_seq=19 ttl=61 time=5.78 ms (DUP!)
```

Figura 2 - Output do comando *ping -c 20 10.4.4.1 | tee file-ping-output* para o PC1

2. SFTP

- Portatil1

```
root@Portatil1:/tmp/pycore.36711/Portatil1.conf# sftp core@10.4.4.1
The authenticity of host '10.4.4.1 (10.4.4.1)' can't be established.
RSA key fingerprint is SHA256:7+Mlwuj10MMXlzx6cYr8ACFqUhuyHQxcFYfeZGzntfw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.4.4.1' (RSA) to the list of known hosts.
core@10.4.4.1's password:
Connected to 10.4.4.1.
sftp> pwd
Remote working directory: /home/core
sftp> cd /srv/ftp
sftp> dir
file1 file2
sftp> get file1
Fetching /srv/ftp/file1 to file1
/srv/ftp/file1
sftp> quit
100% 224 58.1KB/s 00:00
```

Figura 3 - Output da transferência do file1 por SFTP para o Portatil1

1027 1530.82498801.. 10.1.1.1	10.4.4.1	TCP	74 55128 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TStamp=157000
1028 1530.8251039.. 10.4.4.1	10.1.1.1	TCP	74 22 - 55128 [SYN, ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TStamp=157000
1029 1530.8252430.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1570002566 TSecr=1228
1030 1530.8255996.. 10.1.1.1	10.4.4.1	SSHV2	107 Client: Protocol (SSH-2.0-OpenSSH_8.2pi Ubuntu-4ubuntu0.3)
1031 1530.8257196.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=1 Ack=42 Win=65152 Len=0 TStamp=1228253196 TSecr=157
1032 1530.8379893.. 10.4.4.1	10.1.1.1	SSHV2	107 Server: Protocol (SSH-2.0-OpenSSH_8.2pi Ubuntu-4ubuntu0.3)
1033 1530.8379595.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=42 Ack=42 Win=64256 Len=0 TStamp=1570002579 TSecr=1228
1034 1530.8380584.. 10.1.1.1	10.4.4.1	TCP	1514 55128 - 22 [ACK] Seq=42 Ack=42 Win=64256 Len=1448 TStamp=1570002579 TSecr=1228
1035 1530.8380589.. 10.1.1.1	10.4.4.1	SSHV2	138 Client: Key Exchange Init
1036 1530.8381969.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=42 Ack=1490 Win=64128 Len=0 TStamp=1228253209 TSecr=1570002582 TSec=1228253209
1037 1530.8381978.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=42 Ack=1554 Win=64128 Len=0 TStamp=1228253209 TSecr=1570002582 TSec=1228253209
1038 1530.84099362.. 10.4.4.1	10.1.1.1	SSHV2	1099 Server: Key Exchange Init
1039 1530.8421554.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1554 Ack=1066 Win=64128 Len=0 TStamp=1570002582 TSecr=1570002582 TSec=1228253209
1040 1530.8439088.. 10.1.1.1	10.4.4.1	SSHV2	114 Client: Diffie-Hellman Key Exchange Init
1041 1530.8442475.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=1066 Ack=1602 Win=64128 Len=0 TStamp=1228253215 TSecr=1570002590 TSec=1228253215
1042 1530.8493190.. 10.4.4.1	10.1.1.1	SSHV2	1182 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (1 byte)
1043 1530.8498519.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1602 Ack=2182 Win=64128 Len=0 TStamp=1570002590 TSecr=1570002590 TSec=1228253215
1044 1535.9023160.. 00:00:00:aa:00:10	00:00:00:aa:00:14	ARP	42 Who has 10.4.4.1? Tell 10.4.4.254
1047 1535.9025034.. 00:00:00:aa:00:14	00:00:00:aa:00:10	ARP	42 Who has 10.4.4.254? Tell 10.4.4.1
1048 1535.9025173.. 00:00:00:aa:00:10	00:00:00:aa:00:14	ARP	42 10.4.4.254 is at 00:00:00:aa:00:10
1049 1535.9025566.. 00:00:00:aa:00:14	00:00:00:aa:00:10	ARP	42 10.4.4.1 is at 00:00:00:aa:00:14
1062 1556.2103373.. 10.1.1.1	10.4.4.1	SSHV2	82 Client: New Keys
1063 1556.2109212.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=2182 Ack=1618 Win=64128 Len=0 TStamp=1228278581 TSecr=1570002590 TSec=1228278581
1064 1556.2110868.. 10.1.1.1	10.4.4.1	SSHV2	118 Client: Encrypted packet (len=44)
1065 1556.212089.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=2182 Ack=1662 Win=64128 Len=0 TStamp=1228278582 TSecr=1570002590 TSec=1228278582
1066 1556.2124268.. 10.4.4.1	10.1.1.1	SSHV2	118 Server: Encrypted packet (len=44)
1067 1556.2123799.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1662 Ack=2226 Win=64128 Len=0 TStamp=1570027952 TSecr=1570027952 TSec=1228278582
1068 1556.2140938.. 10.1.1.1	10.4.4.1	SSHV2	126 Client: Encrypted packet (len=60)
1069 1556.2149331.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=2226 Ack=1722 Win=64128 Len=0 TStamp=1228278582 TSecr=1570002590 TSec=1228278582
1070 1556.2177387.. 10.4.4.1	10.1.1.1	SSHV2	118 Server: Encrypted packet (len=52)
1071 1556.2179943.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1722 Ack=2278 Win=64128 Len=0 TStamp=1570027958 TSecr=1570027958 TSec=1228278582
1074 1558.3021263.. 10.1.1.1	10.4.4.1	SSHV2	158 Client: Encrypted packet (len=84)
1075 1558.3024971.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=2278 Ack=1889 Win=64128 Len=0 TStamp=1228280673 TSecr=1570002590 TSec=1228280673
1076 1558.3174479.. 10.4.4.1	10.1.1.1	SSHV2	94 Server: Encrypted packet (len=28)
1077 1558.3176242.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=1806 Ack=2308 Win=64128 Len=0 TStamp=1570030058 TSecr=1570030058 TSec=1228280673

1104 1612.7116580.. 10.1.1.1	10.4.4.1	TCP	(...)
1155 1612.7116580.. 10.1.1.1	10.4.4.1	SSHV2	134 Client: Encrypted packet (len=68)
1156 1612.7118526.. 10.4.4.1	10.1.1.1	SSHV2	142 Server: Encrypted packet (len=76)
1157 1612.7119870.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3242 Ack=4146 Win=64128 Len=0 TStamp=1570084453 TSecr=1570002590 TSec=1228278582
1158 1612.7120255.. 10.1.1.1	10.4.4.1	SSHV2	118 Client: Encrypted packet (len=52)
1159 1612.7121852.. 10.4.4.1	10.1.1.1	SSHV2	142 Server: Encrypted packet (len=52)
1160 1612.71226941.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3318 Ack=4198 Win=64128 Len=0 TStamp=1570084453 TSecr=1570002590 TSec=1228278582
1161 1612.71226949.. 10.1.1.1	10.4.4.1	SSHV2	134 Client: Encrypted packet (len=68)
1162 1612.7155340.. 10.4.4.1	10.1.1.1	SSHV2	342 Server: Encrypted packet (len=276)
1163 1612.7157341.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3386 Ack=4474 Win=64128 Len=0 TStamp=1570084456 TSecr=1570002590 TSec=1228278582
1164 1612.7158155.. 10.1.1.1	10.4.4.1	SSHV2	134 Client: Encrypted packet (len=68)
1165 1612.7159739.. 10.4.4.1	10.1.1.1	SSHV2	134 Server: Encrypted packet (len=68)
1166 1612.7166117.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3454 Ack=4542 Win=64128 Len=0 TStamp=1570084457 TSecr=1570002590 TSec=1228278582
1167 1612.7166129.. 10.1.1.1	10.4.4.1	SSHV2	118 Client: Encrypted packet (len=52)
1168 1612.7168211.. 10.4.4.1	10.1.1.1	SSHV2	134 Server: Encrypted packet (len=68)
1169 1612.7170615.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3504 Ack=4616 Win=64128 Len=0 TStamp=1570084458 TSecr=1570002590 TSec=1228278582
1170 1625.3569629.. 10.1.1.1	10.4.4.1	SSHV2	102 Client: Encrypted packet (len=36)
1171 1625.3576244.. 10.4.4.1	10.1.1.1	TCP	66 55128 - 22 [ACK] Seq=3524 Ack=4734 Win=64128 Len=0 TStamp=1570097098 TSecr=1570002590 TSec=1228278582
1172 1625.3578996.. 10.1.1.1	10.4.4.1	SSHV2	190 Server: Encrypted packet (len=124)
1173 1625.3579004.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3542 Ack=4734 Win=64128 Len=0 TStamp=1570097098 TSecr=1570002590 TSec=1228278582
1180 1625.3579018.. 10.1.1.1	10.4.4.1	SSHV2	192 Client: Encrypted packet (len=36)
1181 1625.3579911.. 10.1.1.1	10.4.4.1	SSHV2	126 Client: Encrypted packet (len=60)
1182 1625.3579918.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [FIN, ACK] Seq=3638 Ack=4734 Win=64128 Len=0 TStamp=1570097098 TSecr=1570002590 TSec=1228278582
1183 1625.3588731.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [ACK] Seq=4734 Ack=3639 Win=64128 Len=0 TStamp=1228347729 TSecr=1570002590 TSec=1228347729
1184 1625.3598378.. 10.4.4.1	10.1.1.1	TCP	66 22 - 55128 [FIN, ACK] Seq=4734 Ack=3639 Win=64128 Len=0 TStamp=1228347739 TSecr=1570002590 TSec=1228347739
1185 1625.3605643.. 10.1.1.1	10.4.4.1	TCP	66 55128 - 22 [ACK] Seq=3639 Ack=4735 Win=64128 Len=0 TStamp=1570097101 TSecr=1570002590 TSec=1228347739

Figura 4 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por SFTP para o Portatil1

- PC1

```
root@PC1:/tmp/pycore.36711/PC1.conf# sftp core@10.4.4.1
The authenticity of host '10.4.4.1 (10.4.4.1)' can't be established.
RSA key fingerprint is SHA256:7+MluvJ10MWXlzx6cYr8ACFqUnuyHQxFYfeZGzntfw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.4.4.1' (RSA) to the list of known hosts.
core@10.4.4.1's password:
Connected to 10.4.4.1.
sftp> pwd
Remote working directory: /home/core
sftp> cd /srv/ftp
sftp> dir
file1 file2
sftp> get file1
Fetching /srv/ftp/file1 to file1
/srv/ftp/file1
sftp> quit
                                          100% 224    18.1KB/s  00:00
```

Figura 5 - Output da transferência do file1 por SFTP para o PC1

1269	1763.2279339..	10.2.2.1	10.4.4.1	TCP	74	59858	- 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=293917...
1270	1763.2286628..	10.4.4.1	10.2.2.1	TCP	74	22	- 59858 [SYN, ACK] Seq=1 Ack=1 Win=65100 Len=0 MSS=1460 SACK_PERM=1 TS...
1271	1763.2338651..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2939176474 TSecr=1013...
1272	1763.2388856..	10.4.4.1	10.2.2.1	SSH	107	Server:	Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3)
1273	1763.2447649..	10.2.2.1	10.4.4.1	TCP	66	[TCP Previous segment not captured]	59858 - 22 [ACK] Seq=42 Ack=42 Win=6...
1274	1763.2454491..	10.2.2.1	10.4.4.1	SSH	1514	Client:	Encrypted packet (len=1448)
1275	1763.2454491..	10.4.4.1	10.2.2.1	TCP	78	[TCP Dup ACK 1270#1]	59858 - 22 [PSH, ACK] Seq=42 Ack=1 Win=65280 Len=0 TSval...
1276	1763.2517871..	10.2.2.1	10.4.4.1	TCP	107	[TCP Retransmission]	59858 - 22 [PSH, ACK] Seq=1 Ack=42 Win=64256 Len=41
1277	1763.2525095..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=42 Ack=1490 Win=64128 Len=0 TSval=1013776989 TSecr=...
1278	1763.2526896..	10.4.4.1	10.2.2.1	SSH	1090	Server:	Encrypted packet (len=1024)
1279	1763.2584637..	10.2.2.1	10.4.4.1	SSH	139	Client:	Encrypted packet (len=64)
1280	1763.2584863..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=1554 Ack=1066 Win=64128 Len=0 TSval=2939176499 TSec...
1281	1763.2586168..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=1066 Ack=1554 Win=64128 Len=0 TSval=1013776996 TSec...
1282	1763.2637842..	10.2.2.1	10.4.4.1	SSH	114	Client:	Encrypted packet (len=48)
1283	1763.2647093..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=1066 Ack=1602 Win=64128 Len=0 TSval=1013777001 TSec...
1284	1763.2692595..	10.4.4.1	10.2.2.1	SSH	1182	Server:	Encrypted packet (len=1116)
1285	1763.2744145..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=1692 Ack=2182 Win=64128 Len=0 TSval=2939176516 TSec...
1287	1765.5538940..	10.2.2.1	10.4.4.1	SSH	82	Client:	Encrypted packet (len=16)
1288	1765.5539443..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=2182 Ack=1618 Win=64128 Len=0 TSval=1013779291 TSec...
1289	1765.5593548..	10.2.2.1	10.4.4.1	SSH	110	Client:	Encrypted packet (len=44)
1290	1765.5594967..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=2182 Ack=1662 Win=64128 Len=0 TSval=1013779297 TSec...
1291	1765.5595369..	10.4.4.1	10.2.2.1	SSH	110	Server:	Encrypted packet (len=44)
1292	1765.5646491..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=1662 Ack=2226 Win=64128 Len=0 TSval=2939178806 TSec...
1293	1765.5647298..	10.2.2.1	10.4.4.1	SSH	126	Client:	Encrypted packet (len=60)

(...)

1354	1798.5700138..	10.2.2.1	10.4.4.1	SSH	118	Client:	Encrypted packet (len=52)
1355	1798.5702539..	10.4.4.1	10.2.2.1	SSH	134	Server:	Encrypted packet (len=68)
1356	1798.6157124..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3106 Ack=3994 Win=64128 Len=0 TSval=2939211857 TSec...
1362	1807.2563561..	10.2.2.1	10.4.4.1	SSH	134	Client:	Encrypted packet (len=68)
1363	1807.2566001..	10.4.4.1	10.2.2.1	SSH	142	Server:	Encrypted packet (len=76)
1364	1807.2617160..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3174 Ack=4070 Win=64128 Len=0 TSval=2939220503 TSec...
1365	1807.2618449..	10.2.2.1	10.4.4.1	SSH	134	Client:	Encrypted packet (len=68)
1366	1807.2620595..	10.4.4.1	10.2.2.1	SSH	142	Server:	Encrypted packet (len=76)
1367	1807.2672356..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3242 Ack=4146 Win=64128 Len=0 TSval=2939220508 TSec...
1368	1807.4762179..	10.2.2.1	10.4.4.1	SSH	142	Client:	Encrypted packet (len=76)
1369	1807.4765514..	10.2.2.1	10.4.4.1	SSH	118	Server:	Encrypted packet (len=52)
1370	1807.4816626..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3318 Ack=4198 Win=64128 Len=0 TSval=2939220723 TSec...
1371	1807.4816892..	10.2.2.1	10.4.4.1	TCP	66	[TCP Dup ACK 1370#1]	59858 - 22 [ACK] Seq=4198 Ack=4198 Win=64128 Len=0 ...
1372	1807.4850352..	10.2.2.1	10.4.4.1	SSH	134	Client:	Encrypted packet (len=68)
1373	1807.4852904..	10.4.4.1	10.2.2.1	SSH	342	Server:	Encrypted packet (len=276)
1374	1807.4913811..	10.2.2.1	10.4.4.1	SSH	134	Client:	Encrypted packet (len=68)
1375	1807.4913817..	10.2.2.1	10.4.4.1	TCP	134	[TCP Retransmission]	59858 - 22 [PSH, ACK] Seq=3386 Ack=4474 Win=64128 L...
1376	1807.4915512..	10.4.4.1	10.2.2.1	TCP	78	22	- 59858 [ACK] Seq=4474 Ack=3544 Win=64128 Len=0 TSval=1013821229 TSec...
1377	1807.4916639..	10.4.4.1	10.2.2.1	SSH	134	Server:	Encrypted packet (len=68)
1378	1807.4971558..	10.2.2.1	10.4.4.1	SSH	118	Client:	Encrypted packet (len=52)
1379	1807.4972810..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=4542 Ack=3506 Win=64128 Len=0 TSval=1013821235 TSec...
1380	1807.4973675..	10.4.4.1	10.2.2.1	SSH	134	Server:	Encrypted packet (len=68)
1381	1807.5439199..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3508 Ack=4610 Win=64128 Len=0 TSval=2939220785 TSec...
1382	1811.2446876..	10.2.2.1	10.4.4.1	SSH	102	Client:	Encrypted packet (len=36)
1385	1811.2450539..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=4610 Ack=3542 Win=64128 Len=0 TSval=1013824982 TSec...
1386	1811.2451615..	10.4.4.1	10.2.2.1	SSH	199	Server:	Encrypted packet (len=124)
1387	1811.2502689..	10.2.2.1	10.4.4.1	TCP	66	59858	- 22 [ACK] Seq=3542 Ack=4734 Win=64128 Len=0 TSval=2939224492 TSec...
1388	1811.2503259..	10.2.2.1	10.4.4.1	SSH	102	Client:	Encrypted packet (len=36)
1389	1811.2504282..	10.2.2.1	10.4.4.1	SSH	126	Client:	Encrypted packet (len=60)
1390	1811.2513524..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=4734 Ack=3638 Win=64128 Len=0 TSval=1013824988 TSec...
1391	1811.2520919..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [FIN, ACK] Seq=4734 Ack=3638 Win=64128 Len=0 TSval=1013824989...
1392	1811.2573296..	10.2.2.1	10.4.4.1	TCP	66	[TCP Previous segment not captured]	59858 - 22 [ACK] Seq=3639 Ack=4735 W...
1393	1811.4682467..	10.2.2.1	10.4.4.1	TCP	66	[TCP Retransmission]	59858 - 22 [FIN, ACK] Seq=3638 Ack=4735 Win=64128 L...
1394	1811.4684325..	10.4.4.1	10.2.2.1	TCP	66	22	- 59858 [ACK] Seq=4735 Ack=3639 Win=64128 Len=0 TSval=1013825206 TSec...

Figura 6 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por SFTP para o PC1

3. FTP

- Portatil1

```
root@Portatil1:/tmp/pycore.36711/Portatil1.conf# ftp 10.4.4.1
Connected to 10.4.4.1.
220 (vsFTPd 3.0.3)
Name (10.4.4.1:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> status
Connected to 10.4.4.1.
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: binary; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmd: on
Tick counter printing: off
ftp> pwd
257 "/" is the current directory
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 224 Sep 29 09:33 file1
-rwxr-xr-x 1 0 0 142144 Sep 29 09:34 file2
226 Directory send OK.
ftp> get file1
local: file1 remote: file1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for file1 (224 bytes).
226 Transfer complete.
224 bytes received in 0.00 secs (481.8282 kB/s)
ftp> quit
221 Goodbye.
```

Figura 7 - Output da transferência do file1 por *FTP* para o *Portatil1*

2659	3862.0961726	10.1.1.1	10.4.4.1	TCP	74 33448 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T\$val=157233...
2660	3862.0963008	10.4.4.1	10.1.1.1	TCP	74 21 - 33448 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...
2661	3862.0964962	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T\$val=1572334009 T\$ecr=123...
2662	3862.0984015	10.4.4.1	10.1.1.1	FTP	88 Response: 220 (vsFTPd 3.0.3)
2663	3862.0999095	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T\$val=1572334011 T\$ecr=123...
2667	3866.15835898	10.1.1.1	10.4.4.1	FTP	82 Request: USER anonymous
2668	3866.15837331	10.4.4.1	10.1.1.1	TCP	66 21 - 33448 [ACK] Seq=1 Ack=1 Win=65280 Len=0 T\$val=1230589126 T\$ecr=15...
2669	3866.15837701	10.4.4.1	10.1.1.1	FTP	66 33448 - 21 [ACK] Seq=17 Ack=1 Win=65280 Len=0 T\$val=1572338496 T\$ecr=12...
2670	3866.15840905	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=17 Ack=55 Win=64256 Len=0 T\$val=1572338496 T\$ecr=12...
2680	3881.1954094	10.1.1.1	10.4.4.1	FTP	98 Request: PASS a106743@uminho.pt
2681	3881.1963475	10.4.4.1	10.1.1.1	TCP	66 21 - 33448 [ACK] Seq=55 Ack=41 Win=65280 Len=0 T\$val=1230603738 T\$ecr=15...
2682	3881.1970942	10.4.4.1	10.1.1.1	FTP	89 Response: 230 Login successful.
2683	3881.1973275	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=41 Ack=78 Win=64256 Len=0 T\$val=1572353109 T\$ecr=12...
2684	3881.1973283	10.1.1.1	10.4.4.1	FTP	72 Request: SYST
2685	3881.1978114	10.4.4.1	10.1.1.1	TCP	66 21 - 33448 [ACK] Seq=78 Ack=47 Win=65280 Len=0 T\$val=1230603740 T\$ecr=15...
2686	3881.1982910	10.4.4.1	10.1.1.1	FTP	85 Response: 215 UNIX Type: L8
2687	3881.1990196	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=47 Ack=97 Win=64256 Len=0 T\$val=1572353111 T\$ecr=12...
2691	3886.5731221	fe80::1c30:66ff:fe6... ff02::fb	MDNS	107 Standard query 0x0000 PTR _ipts._tcp.local, "QM" question PTR _ipts._tcp...	
2694	3890.0851929	fe80::60f7:45ff:fe5... ff02::fb	MDNS	107 Standard query 0x0000 PTR _ipts._tcp.local, "QM" question PTR _ipts._tcp...	
2717	3926.4535702	10.1.1.1	10.4.4.1	FTP	71 Request: PWD
2718	3926.4538793	10.4.4.1	10.1.1.1	TCP	66 21 - 33448 [ACK] Seq=97 Ack=52 Win=65280 Len=0 T\$val=1230649175 T\$ecr=15...
2719	3926.4538816	10.4.4.1	10.1.1.1	FTP	100 Response: 257 "/" is the current directory
2720	3926.4542241	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=52 Ack=131 Win=64256 Len=0 T\$val=1572398546 T\$ecr=1...
2724	3931.4552739	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42 Who has 10.4.4.17 Tell 10.4.4.254
2725	3931.4555421	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42 Who has 10.4.4.254 Tell 10.4.4.1
2726	3931.4555579	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42 10.4.4.254 is at 00:00:00_aa:00:10
2727	3931.4556174	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42 10.4.4.1 is at 00:00:00_aa:00:14
2732	3937.1686730	10.1.1.1	10.4.4.1	FTP	89 Request: PORT 10.1.1.1,151,137
2733	3937.1688475	10.4.4.1	10.1.1.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.
2734	3937.1699367	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=75 Ack=182 Win=64256 Len=0 T\$val=1572409261 T\$ecr=1...
2735	3937.1699375	10.1.1.1	10.4.4.1	FTP	72 Request: LIST
2736	3937.1699393	10.4.4.1	10.1.1.1	TCP	74 20 - 38793 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T\$val=123065...
2737	3937.1694970	10.1.1.1	10.4.4.1	TCP	74 38793 - 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...
2738	3937.1696345	10.4.4.1	10.1.1.1	TCP	66 20 - 38793 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T\$val=1230659891 T\$ecr=157...
2739	3937.1696694	10.4.4.1	10.1.1.1	FTP	105 Response: 159 Here comes the directory listing.
2740	3937.1699961	10.4.4.1	10.1.1.1	FTP-DA...	192 FTP Data: 126 bytes (PORT) (LIST)
2741	3937.1699980	10.4.4.1	10.1.1.1	TCP	66 20 - 38793 [FIN, ACK] Seq=127 Ack=1 Win=64256 Len=0 T\$val=1230659891 T\$e...
2742	3937.1700153	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=81 Ack=221 Win=64256 Len=0 T\$val=1572409261 T\$ecr=1...
2743	3937.1706165	10.1.1.1	10.4.4.1	TCP	66 38793 - 20 [ACK] Seq=1 Ack=127 Win=65152 Len=0 T\$val=1572409262 T\$ecr=12...
2744	3937.1706173	10.1.1.1	10.4.4.1	TCP	66 38793 - 20 [FIN, ACK] Seq=1 Ack=128 Win=65152 Len=0 T\$val=1572409262 T\$ecr=1...
2745	3937.1707561	10.4.4.1	10.1.1.1	TCP	66 20 - 38793 [ACK] Seq=128 Ack=2 Win=64256 Len=0 T\$val=1230659892 T\$ecr=15...
2746	3937.1707832	10.4.4.1	10.1.1.1	FTP	99 Response: 226 Directory send OK.
2747	3937.1709543	10.1.1.1	10.4.4.1	TCP	66 33448 - 21 [ACK] Seq=81 Ack=245 Win=64256 Len=0 T\$val=1572409263 T\$ecr=1...
2758	3955.4149845	10.1.1.1	10.4.4.1	FTP	74 Request: TYPE I
2759	3955.4154624	10.4.4.1	10.1.1.1	FTP	97 Response: 200 Switching to Binary mode.
2760	3955.4156060	10.1.1.1	10.4.4.1	FTP	66 33448 - 21 [ACK] Seq=89 Ack=276 Win=64256 Len=0 T\$val=1572427507 T\$ecr=1...
2761	3955.4156448	10.1.1.1	10.4.4.1	FTP	81 Request: PORT 10.1.1.1,151,125
2762	3955.4157929	10.4.4.1	10.1.1.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.
2763	3955.4159465	10.1.1.1	10.4.4.1	FTP	66 33448 - 21 [ACK] Seq=112 Ack=327 Win=64256 Len=0 T\$val=1572427508 T\$ecr=...
2764	3955.4159474	10.1.1.1	10.4.4.1	FTP	78 Request: RETR file1
2765	3955.4168434	10.4.4.1	10.1.1.1	TCP	74 20 - 39293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T\$val=123067...
2766	3955.4170916	10.1.1.1	10.4.4.1	TCP	74 39293 - 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...

2767 3955.4171270...	10.4.4.1	10.1.1.1	TCP	66 20 -- 39293 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=1230678139 TSecr=157...
2768 3955.4171670...	10.4.4.1	10.1.1.1	FTP	130 Response: 150 Opening BINARY mode data connection for file1 (224 bytes).
2769 3955.4175749...	10.4.4.1	10.1.1.1	FTP-DA...	290 FTP Data: 224 bytes (PORT) (RETR file1)
2770 3955.4175776...	10.4.4.1	10.1.1.1	TCP	66 20 -- 39293 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0 TStamp=1230678139 TSecr=...
2771 3955.4175936...	10.1.1.1	10.4.4.1	TCP	66 33448 -- 21 [ACK] Seq=124 Ack=391 Win=64256 Len=0 TStamp=1572427599 TSecr=...
2772 3955.4177384...	10.1.1.1	10.4.4.1	TCP	66 39293 -- 20 [ACK] Seq=1 Ack=225 Win=65924 Len=0 TStamp=1572427599 TSecr=12...
2773 3955.4178981...	10.1.1.1	10.4.4.1	TCP	66 39293 -- 20 [FIN, ACK] Seq=1 Ack=226 Win=65924 Len=0 TStamp=1572427599 TSecr=...
2774 3955.4180220...	10.4.4.1	10.1.1.1	TCP	66 20 -- 39293 [ACK] Seq=226 Ack=2 Win=64256 Len=0 TStamp=1230678140 TSecr=15...
2775 3955.4180820...	10.4.4.1	10.1.1.1	FTP	99 Response: 226 Transfer complete.
2776 3955.4184795...	10.1.1.1	10.4.4.1	TCP	66 33448 -- 21 [ACK] Seq=124 Ack=415 Win=64256 Len=0 TStamp=1572427510 TSecr=...
2788 3974.1947520...	10.1.1.1	10.4.4.1	FTP	72 Request: QUIT
2789 3974.1956992...	10.4.4.1	10.1.1.1	FTP	80 Response: 221 Goodbye.
2790 3974.1957017...	10.4.4.1	10.1.1.1	TCP	66 21 -- 33448 [FIN, ACK] Seq=429 Ack=130 Win=65280 Len=0 TStamp=1230696917 T...
2791 3974.1959518...	10.1.1.1	10.4.4.1	TCP	66 33448 -- 21 [ACK] Seq=130 Ack=429 Win=64256 Len=0 TStamp=1572446287 TSecr=...
2792 3974.1966746...	10.1.1.1	10.4.4.1	TCP	66 33448 -- 21 [FIN, ACK] Seq=130 Ack=430 Win=64256 Len=0 TStamp=1572446288 T...
2793 3974.1968944...	10.4.4.1	10.1.1.1	TCP	66 21 -- 33448 [ACK] Seq=430 Ack=131 Win=65280 Len=0 TStamp=1230696918 TSecr=...

Figura 8 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por *FTP* para o *Portatil1*

- PC1

```
root@PC1:/tmp/pycore.36711/PC1.conf# ftp 10.4.4.1
Connected to 10.4.4.1.
220 (vsFTPd 3.0.3)
Name (10.4.4.1:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> status
Connected to 10.4.4.1.
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: binary; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmd: on
Tick counter printing: off
ftp> pwd
257 "/" is the current directory
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 224 Sep 29 09:33 file1
-rwxr-xr-x 1 0 0 142144 Sep 29 09:34 file2
226 Directory send OK.
ftp> get file1
local: file1 remote: file1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for file1 (224 bytes).
226 Transfer complete.
224 bytes received in 0.00 secs (1.9780 MB/s)
ftp> quit
221 Goodbye.
root@PC1:/tmp/pycore.36711/PC1.conf#
```

Figura 9 - Output da transferência do file1 por *FTP* para o *PC1*

2938 4210.7168132_	10.2.2.1	10.4.4.1	TCP	74 59882 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T... 2939 4210.7169478_	10.4.4.1	TCP	74 21 - 59882 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T... 2940 4210.7226648_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2941624143 TSecr=1016...
2941 4210.7242137_	10.4.4.1	10.2.2.1	FTP	86 Response: 220 (vsFTPd 3.0.3)							
2942 4210.7292499_	10.2.2.1	10.4.4.1	FTP	66 59882 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=2941624150 TSecr=101...							
2943 4215.7872533_	10.2.2.1	10.4.4.1	FTP	82 Request: USER anonymous							
2947 4215.7873932_	10.4.4.1	10.2.2.1	TCP	66 21 - 59882 [ACK] Seq=21 Ack=17 Win=65280 Len=0 TSval=1016229704 TSecr=29...							
2948 4215.7874480_	10.4.4.1	10.2.2.1	FTP	100 Response: 331 Please specify the password.							
2949 4215.7931858_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=17 Ack=55 Win=64256 Len=0 TSval=2941629213 TSecr=10...							
2950 4223.9411379_	10.2.2.1	10.4.4.1	FTP	99 Request: PASS a100743@uminho.pt							
2954 4223.9417608_	10.4.4.1	10.2.2.1	TCP	66 21 - 59882 [ACK] Seq=55 Ack=41 Win=65280 Len=0 TSval=1016237858 TSecr=29...							
2957 4223.9431108_	10.4.4.1	10.2.2.1	FTP	89 Response: 230 Login successful.							
2958 4223.9482292_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=41 Ack=78 Win=64256 Len=0 TSval=2941637369 TSecr=10...							
2959 4223.9482699_	10.2.2.1	10.4.4.1	FTP	72 Request: SYST							
2960 4223.9483929_	10.4.4.1	10.2.2.1	TCP	66 21 - 59882 [ACK] Seq=78 Ack=47 Win=65280 Len=0 TSval=1016237865 TSecr=29...							
2961 4223.9484412_	10.4.4.1	10.2.2.1	FTP	85 Response: 215 UNIX Type: L8							
2962 4223.9535483_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=47 Ack=97 Win=64256 Len=0 TSval=2941637374 TSecr=10...							
2972 4237.9515251_	10.2.2.1	10.4.4.1	FTP	71 Request: PWD							
2973 4237.9517630_	10.4.4.1	10.2.2.1	FTP	100 Response: 257 "/" is the current directory							
2974 4237.9568271_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=52 Ack=131 Win=64256 Len=0 TSval=2941650477 TSecr=1...							
2976 4239.6783663_	10.2.2.1	10.4.4.1	FTP	88 Request: PORT 16,2,2,1,168,93							
2977 4239.6785236_	10.4.4.1	10.2.2.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.							
2978 4239.6836490_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=74 Ack=182 Win=64256 Len=0 TSval=2941653104 TSecr=1...							
2979 4239.6836994_	10.2.2.1	10.4.4.1	FTP	72 Request: LIST							
2980 4239.6839923_	10.4.4.1	10.2.2.1	TCP	74 20 - 43101 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=101625...							
2981 4239.6891245_	10.2.2.1	10.4.4.1	TCP	74 43101 - 20 [ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...							
2982 4239.6892894_	10.4.4.1	10.2.2.1	TCP	66 20 - 43101 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1016253606 TSecr=2941...							
2983 4239.6893527_	10.4.4.1	10.2.2.1	FTP	105 Response: 192 Here comes the directory listing.							
2984 4239.6899561_	10.4.4.1	10.2.2.1	FTP-DA...	192 FTP Data: 126 bytes (PORT) (LIST)							
2985 4239.6899584_	10.4.4.1	10.2.2.1	TCP	66 20 - 43101 [FIN, ACK] Seq=127 Ack=1 Win=64256 Len=0 TSval=1016253606 TSe...							
2986 4239.6944834_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=80 Ack=221 Win=64256 Len=0 TSval=2941653115 TSecr=1...							
2987 4239.6950812_	10.2.2.1	10.4.4.1	TCP	66 43101 - 20 [ACK] Seq=1 Ack=127 Win=65152 Len=0 TSval=2941653116 TSecr=10...							
2988 4239.6951325_	10.2.2.1	10.4.4.1	TCP	66 43101 - 20 [FIN, ACK] Seq=1 Ack=128 Win=65152 Len=0 TSval=2941653116 TSe...							
2989 4239.6952853_	10.4.4.1	10.2.2.1	TCP	66 20 - 43101 [ACK] Seq=128 Ack=2 Win=64256 Len=0 TSval=1016253612 TSecr=29...							
2990 4239.6953294_	10.4.4.1	10.2.2.1	FTP	99 Response: 226 Directory send OK.							
2991 4239.7010188_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=80 Ack=245 Win=64256 Len=0 TSval=2941653121 TSecr=1...							
2992 4239.7010189_	10.2.2.1	10.4.4.1	TCP	66 [TCP Dup ACK 2991#1] 59882 - 21 [ACK] Seq=80 Ack=245 Win=64256 Len=0 TSV...							
2995 4243.3835561_	10.2.2.1	10.4.4.1	FTP	74 Request: TYPE I							
2996 4243.3837431_	10.4.4.1	10.2.2.1	FTP	97 Response: 200 Switching to Binary mode.							
2997 4243.3895265_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=88 Ack=276 Win=64256 Len=0 TSval=2941656810 TSecr=1...							
2999 4243.3895273_	10.2.2.1	10.4.4.1	FTP	89 Request: PORT 10,2,2,1,201,139							
3000 4243.3895734_	10.2.2.1	10.4.4.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.							
3001 4243.3956742_	10.4.4.1	10.2.2.1	TCP	78 Request: RETR file1							
3002 4243.4006818_	10.2.2.1	10.4.4.1	TCP	74 20 - 51595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=101625...							
3003 4243.4006952_	10.4.4.1	10.2.2.1	TCP	74 51595 - 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...							
3004 4243.4006969_	10.2.2.1	10.4.4.1	TCP	66 20 - 51595 [ACK] Seq=1 Ack=1 Win=65160 Len=0 TSval=1016253718 TSecr=2941...							
3005 4243.4010157_	10.4.4.1	10.2.2.1	FTP	139 Response: 156 Opening BINARY mode data connection for file1 (224 bytes).							
3006 4243.4011668_	10.4.4.1	10.2.2.1	FTP-DA...	299 FTP Data: 224 bytes (PORT) (RETR file1)							
3007 4243.4011676_	10.4.4.1	10.2.2.1	TCP	66 20 - 51595 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0 TSval=1016257318 TSe...							
3008 4243.4011681_	10.4.4.1	10.2.2.1	TCP	66 [TCP Dup ACK 3003#1] 20 - 51595 [ACK] Seq=226 Ack=1 Win=64256 Len=0 TSva...							
3009 4243.4063361_	10.2.2.1	10.4.4.1	TCP	66 51595 - 20 [FIN, ACK] Seq=1 Ack=226 Win=65024 Len=0 TSval=2941656827 TSe...							
3010 4243.4064717_	10.4.4.1	10.2.2.1	TCP	66 20 - 51595 [ACK] Seq=226 Ack=2 Win=64256 Len=0 TSval=1016257323 TSecr=29...							
3011 4243.4065352_	10.4.4.1	10.2.2.1	FTP	99 Response: 226 Transfer complete.							
3012 4243.4119248_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [ACK] Seq=123 Ack=415 Win=64256 Len=0 TSval=2941656832 TSecr=...							
3014 4246.3109385_	10.2.2.1	10.4.4.1	FTP	72 Request: QUIT							
3015 4246.3116217_	10.4.4.1	10.2.2.1	FTP	80 Response: 221 Goodbye.							
3016 4246.3116244_	10.4.4.1	10.2.2.1	TCP	66 21 - 59882 [FIN, ACK] Seq=49 Ack=129 Win=65280 Len=0 TSval=1016260228 T...							
3017 4246.3116982_	10.2.2.1	10.4.4.1	TCP	66 59882 - 21 [FIN, ACK] Seq=129 Ack=430 Win=64256 Len=0 TSval=2941659738 T...							
3018 4246.3171276_	10.4.4.1	10.2.2.1	TCP	66 21 - 59882 [ACK] Seq=430 Ack=130 Win=65280 Len=0 TSval=1016260234 TSecr=...							

Figura 10 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por *FTP* para o *PC1*

4. TFTP

- Portatil1

```
root@Portatil1:/tmp/pycore.45761/Portatil1.conf# atftp 10.4.4.1
tftp> status
Connected: 10.4.4.1 port 69
Mode: octet
Verbose: off
Trace: off
Options:
  tsize: disabled
  blksize: disabled
  timeout: disabled
  multicast: disabled
mtftp variables
  client-port: 76
  mcast-ip: 0.0.0.0
  listen-delay: 2
  timeout-delay: 2
Last command: ---
tftp> get file1
tftp> quit
```

Figura 11 - Output da transferência do file1 por *TFTP* para o *Portatil1*

204	335.759626345	10.1.1.1	10.4.4.1	TFTP	56 Read Request, File: file1, Transfer type: octet
205	335.769845072	10.4.4.1	10.1.1.1	TFTP	270 Data Packet, Block: 1 (last)
206	335.770381436	10.1.1.1	10.4.4.1	TFTP	46 Acknowledgement, Block: 1

Figura 12 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por TFTP para o Portatil1

- PC1

```
root@PC1:/tmp/pycore.45761/PC1.conf# atftp 10.4.4.1
tftp> status
Connected: 10.4.4.1 port 69
Mode: octet
Verbose: off
Trace: off
Options
  tsize: disabled
  blksize: disabled
  timeout: disabled
  multicast: disabled
mtftp variables
  client-port: 76
  mcast-ip: 0.0.0.0
  listen-delay: 2
  timeout-delay: 2
Last command: quit
tftp> get file1
Overwrite local file [y/n]? y
tftp> quit
```

Figura 13 - Output da transferência do file1 por TFTP para o PC1

322	522.651967864	10.2.2.1	10.4.4.1	TFTP	56 Read Request, File: file1, Transfer type: octet
323	522.651969529	10.2.2.1	10.4.4.1	TFTP	56 Read Request, File: file1, Transfer type: octet
324	522.652813082	10.4.4.1	10.2.2.1	TFTP	270 Data Packet, Block: 1 (last)
325	522.653426726	10.4.4.1	10.2.2.1	TFTP	270 Data Packet, Block: 0 (last)
326	522.659418973	10.2.2.1	10.4.4.1	TFTP	46 Acknowledgement, Block: 1
327	522.659419970	10.2.2.1	10.4.4.1	ICMP	298 Destination unreachable (Port unreachable)

Figura 14 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por TFTP para o PC1

5. HTTP

- Portatil1

```
root@Portatil1:/tmp/pycore.39963/Portatil1.conf# wget http://10.4.4.1/file1
--2023-10-03 22:33:06-- http://10.4.4.1/file1
Connecting to 10.4.4.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 224 [text/plain]
Saving to: 'file1'

file1          100%[=====]     224 --.-KB/s   in 0s

2023-10-03 22:33:06 (60,0 MB/s) - 'file1' saved [224/224]
```

Figura 15 - Output da transferência do file1 por HTTP para o Portatil1

256	391.016856286	00:00:00_aa:00:10	Broadcast	ARP	42 Who has 10.4.4.1? Tell 10.4.4.254
257	391.016982876	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42 10.4.4.1 is at 00:00:00_aa:00:14
258	391.016984978	10.1.1.1	10.4.4.1	TCP	74 55754 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=267991...
259	391.017116245	10.4.4.1	10.1.1.1	TCP	74 80 - 55754 [SYN, ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...
260	391.017397138	10.1.1.1	10.4.4.1	TCP	66 55754 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2679919257 TSecr=2892...
261	391.017397950	10.1.1.1	10.4.4.1	HTTP	206 GET /file1 HTTP/1.1
262	391.017670112	10.4.4.1	10.1.1.1	TCP	66 80 - 55754 [ACK] Seq=1 Ack=141 Win=65024 Len=0 TSval=2892701169 TSecr=26...
263	391.018775646	10.4.4.1	10.1.1.1	HTTP	508 HTTP/1.1 200 OK [text/plain]
264	391.019765886	10.1.1.1	10.4.4.1	TCP	66 55754 - 80 [FIN, ACK] Seq=141 Ack=444 Win=64128 Len=0 TSval=2679919259 T...
265	391.020185594	10.4.4.1	10.1.1.1	TCP	66 80 - 55754 [ACK] Seq=444 Ack=142 Win=65024 Len=0 TSval=2892701172 TSecr=...
270	396.272326468	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42 Who has 10.4.4.254? Tell 10.4.4.1
271	396.272336089	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42 10.4.4.254 is at 00:00:00_aa:00:10

Figura 16 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por *HTTP* para o *Portatil1*

```
root@Portatil1:/tmp/pycore.39963/Portatil1.conf# wget http://10.4.4.1/file2
--2023-10-03 22:35:24-- http://10.4.4.1/file2
Connecting to 10.4.4.1:80... connected.
HTTP request sent, awaiting response... 200 Ok
Length: 142144 (139K) [text/plain]
Saving to: 'file2'

file2          100%[=====] 138,81K  --.-KB/s   in 0,003s

2023-10-03 22:35:24 (49.8 MB/s) - 'file2' saved [142144/142144]
```

Figura 17 - Output da transferência do file2 por *HTTP* para o *Portatil1*

471	529.694075097	10.4.4.1	10.1.1.1	TCP	1514 80 - 45802 [ACK] Seq=139009 Ack=141 Win=65024 Len=1448 TSval=2892839846 ...
472	529.694091462	10.4.4.1	10.1.1.1	TCP	1514 80 - 45802 [PSH, ACK] Seq=140457 Ack=1448 Win=65024 Len=1448 TSval=289283...
473	529.694097735	10.4.4.1	10.1.1.1	TCP	527 80 - 45802 [FIN, PSH, ACK] Seq=141905 Ack=141 Win=65024 Len=461 TSval=28...
474	529.694160643	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=103936 Len=0 ...
475	529.694161412	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=106752 Len=0 ...
476	529.694162184	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=109696 Len=0 ...
477	529.694162935	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=112512 Len=0 ...
478	529.694163657	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=115456 Len=0 ...
479	529.694164376	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=118400 Len=0 ...
480	529.694165094	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=121216 Len=0 ...
481	529.694165834	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=124160 Len=0 ...
482	529.694166559	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=127104 Len=0 ...
483	529.6942437510	10.4.4.1	10.1.1.1	TCP	1514 80 - 45802 [ACK] Seq=82537 Ack=141 Win=65024 Len=1448.
484	529.694244706	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=83985 Ack=141 Win=65024 Len=1448.
485	529.694245535	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=85433 Ack=141 Win=65024 Len=1448.
486	529.694246351	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=86881 Ack=141 Win=65024 Len=1448...
487	529.694247230	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=88329 Ack=141 Win=65024 Len=1448...
488	529.694248942	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=89777 Ack=141 Win=65024 Len=1448...
489	529.694248864	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=91225 Ack=141 Win=65024 Len=1448...
490	529.694378333	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=92673 Ack=141 Win=65024 Len=1448...
491	529.694379547	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=94121 Ack=141 Win=65024 Len=1448...
492	529.694412581	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=129920 Len=0 ...
493	529.694413361	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=132864 Len=0 ...
494	529.694414137	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=135680 Len=0 ...
495	529.694414987	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=138624 Len=0 ...
496	529.694415659	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=141568 Len=0 ...
497	529.694416402	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=144384 Len=0 ...
498	529.694417128	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=147328 Len=0 ...
499	529.694417852	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=150272 Len=0 ...
500	529.694418581	10.1.1.1	10.4.4.1	TCP	78 [TCP Window Update] 45882 - 80 [ACK] Seq=141 Ack=82537 Win=153088 Len=0 ...
501	529.694417521	10.4.4.1	10.1.1.1	TCP	1514 80 - 45802 [ACK] Seq=95569 Ack=141 Win=65024 Len=1448.
502	529.694476307	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=97017 Ack=141 Win=65024 Len=1448.
503	529.694477157	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=98465 Ack=141 Win=65024 Len=1448.
504	529.694477988	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=99913 Ack=141 Win=65024 Len=1448...
505	529.694477861	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=101361 Ack=141 Win=65024 Len=144...
506	529.694479677	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=102899 Ack=141 Win=65024 Len=144...
507	529.694498487	10.4.4.1	10.1.1.1	TCP	1514 [TCP Out-Of-Order] 80 - 45802 [ACK] Seq=104257 Ack=141 Win=65024 Len=144...
508	529.694531983	10.1.1.1	10.4.4.1	TCP	78 45882 - 80 [ACK] Seq=141 Ack=83985 Win=156932 Len=0 TSval=2680057934 TSe...
509	529.694532750	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=85433 Win=158848 Len=0 TSval=2680057934 TSe...
510	529.694533519	10.1.1.1	10.4.4.1	TCP	78 45882 - 80 [ACK] Seq=141 Ack=86881 Win=161792 Len=0 TSval=2680057934 TSe...
511	529.694534261	10.1.1.1	10.4.4.1	TCP	78 45882 - 80 [ACK] Seq=141 Ack=88329 Win=164736 Len=0 TSval=2680057934 TSe...
512	529.694535008	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=89777 Win=167552 Len=0 TSval=2680057934 TSe...
513	529.694535744	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=91228 Win=178496 Len=0 TSval=2680057934 TSe...
514	529.694536474	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=92673 Win=173440 Len=0 TSval=2680057934 TSe...
515	529.694602824	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=94121 Win=176256 Len=0 TSval=2680057935 TSe...
516	529.694603616	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=95569 Win=179200 Len=0 TSval=2680057935 TSe...
517	529.694657621	10.4.4.1	10.1.1.1	TCP	1514 [TCP Retransmission] 80 - 45802 [ACK] Seqs=105795 Ack=141 Win=65024 Len=1...
518	529.694738021	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=97017 Win=182016 Len=0 TSval=2680057935 TSe...
519	529.694738866	10.1.1.1	10.4.4.1	TCP	78 45802 - 80 [ACK] Seq=141 Ack=98465 Win=184960 Len=0 TSval=2680057935 TSe...

Figura 18 - Captura do Wireshark a partir do Router 1 durante a transferência do file2 por *HTTP* para o *Portatil1*

- PC1

```
root@PC1:/tmp/pycore.39963/PC1.conf# wget http://10.4.4.1/file1
--2023-10-03 22:40:04-- http://10.4.4.1/file1
Connecting to 10.4.4.1:80... connected.
HTTP request sent, awaiting response... 200 Ok
Length: 224 [text/plain]
Saving to: 'file1'

file1          100%[=====] 224 --.-KB/s   in 0s

2023-10-03 22:40:04 (60,7 MB/s) - 'file1' saved [224/224]
```

Figura 19 - Output da transferência do file1 por *HTTP* para o *PC1*

783 889.126798855 10.2.2.1	10.4.4.1	TCP	74 42352 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1507325581 TSecr=2685...
785 889.132064376 10.2.2.1	10.4.4.1	TCP	66 42352 - 80 [ACK] Seq=1 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...
786 889.132330382 10.2.2.1	10.4.4.1	HTTP	206 GET /file1 HTTP/1.1
787 889.132471434 10.4.4.1	10.2.2.1	TCP	66 80 - 42352 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1507325581 TSecr=2685...
788 889.132582015 10.4.4.1	10.2.2.1	HTTP	508 HTTP/1.1 200 Ok (text/plain)
789 889.138008242 10.2.2.1	10.4.4.1	TCP	66 42352 - 80 [FIN, ACK] Seq=141 Ack=444 Win=64128 Len=0 TSval=1507325587 T...
790 889.138325178 10.4.4.1	10.2.2.1	TCP	66 80 - 42352 [ACK] Seq=444 Ack=142 Win=65024 Len=0 TSval=268581174 TSecr=1...

Figura 20 - Captura do Wireshark a partir do Router 1 durante a transferência do file1 por *HTTP* para o *PC1*

```
root@PC1:/tmp/pycore.39963/PC1.conf# wget http://10.4.4.1/file2
--2023-10-03 22:41:30-- http://10.4.4.1/file2
Connecting to 10.4.4.1:80... connected.
HTTP request sent, awaiting response... 200 Ok
Length: 142144 (139K) [text/plain]
Saving to: 'file2'

file2          100%[=====] 138,81K --.-KB/s   in 0,03s

2023-10-03 22:41:30 (4,03 MB/s) - 'file2' saved [142144/142144]
```

Figura 21 - Output da transferência do file2 por *HTTP* para o *PC1*

879 895.615847197 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=123081 Ack=141 Win=65024 Len=1448 TSval=268667652 T...
880 895.615848039 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=124529 Ack=141 Win=65024 Len=1448 TSval=268667652 T...
881 895.615848881 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=159777 Ack=141 Win=65024 Len=1448 TSval=268667652 T...
882 895.615849837 10.4.4.1	10.2.2.1	TCP	1514 [TCP Previous segment not captured] 80 - 48922 [ACK] Seq=128873 Ack=141 ...
883 895.615856683 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=130321 Ack=141 Win=65024 Len=1448 TSval=268667652 T...
884 895.615851555 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [PSH, ACK] Seq=131769 Ack=141 Win=65024 Len=1448 TSval=268667...
885 895.6208967130 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=147 Ack=79641 Win=147328 Len=0 TSval=1507412070 TSe...
886 895.6208668697 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=142 Ack=81089 Win=150272 Len=0 TSval=1507412070 TSe...
887 895.620893938 10.2.2.1	10.4.4.1	TCP	66 [TCP Dup ACK 886#1] 48922 - 80 [ACK] Seq=141 Ack=81089 Win=150272 Len=0 ...
888 895.620840955 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=82537 Win=153988 Len=0 TSval=1507412070 TSe...
889 895.620892561 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=133217 Ack=141 Win=65024 Len=1448 TSval=268667657 T...
890 895.620895555 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=134665 Ack=141 Win=65024 Len=1448 TSval=268667657 T...
891 895.620897460 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=136113 Ack=141 Win=65024 Len=1448 TSval=268667657 T...
892 895.620899076 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=137561 Ack=141 Win=65024 Len=1448 TSval=268667657 T...
893 895.620900994 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [ACK] Seq=139909 Ack=141 Win=65024 Len=1448 TSval=268667657 T...
894 895.620948651 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=85433 Win=158848 Len=0 TSval=1507412070 TSe...
895 895.620950193 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=142 Ack=86881 Win=161792 Len=0 TSval=1507412070 TSe...
896 895.621022048 10.4.4.1	10.2.2.1	TCP	1514 80 - 48922 [PSH, ACK] Seq=140457 Ack=141 Win=65024 Len=1448 TSval=268667...
897 895.621024463 10.4.4.1	10.2.2.1	TCP	527 80 - 48922 [FIN, PSH, ACK] Seq=141995 Ack=141 Win=65024 Len=461 TSval=268667...
898 895.621060932 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=88329 Win=164736 Len=0 TSval=1507412070 TSe...
899 895.621061582 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=89777 Win=167552 Len=0 TSval=1507412070 TSe...
900 895.621121796 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=91225 Win=170496 Len=0 TSval=1507412070 TSe...
901 895.626660563 10.2.2.1	10.4.4.1	TCP	86 48922 - 80 [ACK] Seq=142 Ack=102809 Win=187520 Len=0 TSval=1507412070 TSe...
902 895.626860819 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [ACK] Seq=162809 Ack=141 Win=65024 Len=1...
903 895.626811097 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [ACK] Seq=184257 Ack=141 Win=65024 Len=1...
904 895.626812777 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [ACK] Seq=105705 Ack=141 Win=65024 Len=1...
905 895.627023877 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [ACK] Seq=107153 Ack=141 Win=65024 Len=1...
906 895.627026714 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [PSH, ACK] Seq=108601 Ack=141 Win=65024 ...
907 895.632159836 10.2.2.1	10.4.4.1	TCP	86 48922 - 80 [ACK] Seq=141 Ack=184764 Win=0 TSval=1507412081 TS...
908 895.632161381 10.2.2.1	10.4.4.1	TCP	86 48922 - 80 [ACK] Seq=141 Ack=187153 Win=183298 Len=0 TSval=1507412082 TS...
909 895.632308713 10.2.2.1	10.4.4.1	TCP	78 48922 - 80 [ACK] Seq=141 Ack=127425 Win=167168 Len=0 TSval=1507412082 TS...
910 895.632353889 10.4.4.1	10.2.2.1	TCP	1514 [TCP Retransmission] 80 - 48922 [ACK] Seq=127425 Ack=141 Win=65024 Len=1...
911 895.637515619 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [ACK] Seq=141 Ack=142367 Win=181760 Len=0 TSval=1507412087 TS...
912 895.638252341 10.2.2.1	10.4.4.1	TCP	66 48922 - 80 [FIN, ACK] Seq=141 Ack=142367 Win=188160 Len=0 TSval=15074120...
913 895.638714867 10.4.4.1	10.2.2.1	TCP	66 80 - 48922 [ACK] Seq=142367 Ack=142 Win=65024 Len=0 TSval=268667675 TSe...

Figura 22 - Captura do Wireshark a partir do Router 1 durante a transferência do file2 por *HTTP* para o *PC1*

Questão 1:

De que forma as perdas e duplicações de pacotes afetaram o desempenho das aplicações? Que camada lidou com as perdas e duplicações: transporte ou aplicação? Responda com base nas experiências feitas e nos resultados observados.

Resposta:

As diferentes aplicações são afetadas de maneiras diferentes pelas perdas e duplicações, sendo bastante relevante o protocolo de transporte utilizado.

De um modo geral, perdas e duplicações diminuem a eficiência da aplicação uma vez que esta tem de lidar com mais pacotes do que aqueles que são estritamente necessários. No caso das duplicações, aparece um pacote a mais que deve ser identificado e descartado e, no caso das perdas, é necessário pedir retransmissão, de modo a não interferir com a integridade dos dados. O protocolo de transporte TCP (Transmission Control Protocol), faz precisamente isso, enquanto o UDP (User Datagram Protocol) não tem essa capacidade, deixando esse trabalho para a aplicação.

De qualquer forma, lidar com perdas e duplicações demora algum tempo, podendo tornar a aplicação menos eficiente e mais lenta devido a atrasos na transmissão de pacotes e não lidar com estes erros pode comprometer a integridade dos dados.

Certas aplicações como SFTP, FTP e HTTP utilizam o TCP como protocolo de transporte, como se pode ver nas imagens de capturas do Wireshark correspondentes a essas aplicações cuja coluna “Protocol” dos pacotes vai apresentando valores que alternam entre o nome da aplicação utilizada e “TCP”. Nestas aplicações, sempre que ocorre uma perda de um pacote verifica-se a existência de um pacote TCP a pedir a sua retransmissão (“[TCP Retransmission]”) e quando ocorre a duplicação de um pacote verifica-se que existe um pacote TCP a informar dessa ocorrência (“[TCP Dup ACK ...]”). Estes pacotes encontram-se representados a preto nas imagens. Concluímos então que nestas aplicações a camada que lida com perdas e duplicações é a camada de transporte e que o TCP lida bem tanto com as duplicações, conseguindo geralmente identificá-las e descartá-las para que não interfiram com o resto, como com as perdas, pedindo imediatamente a retransmissão do pacote em falta.

No caso da aplicação TFTP, o protocolo de transporte utilizado é o UDP como se pode ver na imagem a seguir apresentada:

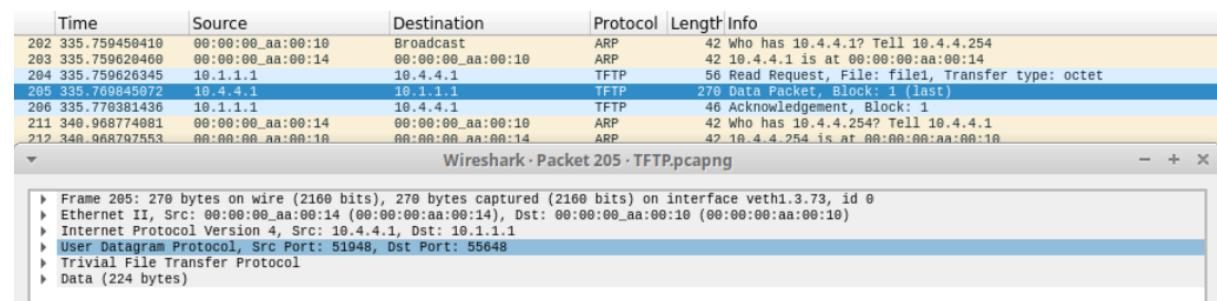


Figura 23 - Informações sobre pacote TFTP como o seu protocolo de transporte (UDP)

Este protocolo de transporte, ao contrário do TCP, não lida com as perdas, ou seja, não pede automaticamente retransmissões nem deteta e corrige a ocorrência de duplicações. Assim sendo, a responsabilidade de tratar das perdas e duplicações fica para a camada da aplicação que terá os seus próprios métodos para lidar com estas. No caso apresentado (imagem 14) em que ocorreu uma duplicação, verifica-se que a aplicação só estava à espera de da chegada de um pacote e chegam 2, pelo que, a partir do momento em que chega o primeiro, a aplicação fecha o socket e não recebe mais pacotes, sendo enviado um pacote ICMP a avisar que o destino é inatingível.

Questão 2:

Obtenha a partir do wireshark, ou desenhe manualmente, um diagrama temporal para a transferência de file1 por FTP. Foque-se apenas na transferência de dados [ftp-data] e não na conexão de controlo, pois o FTP usa mais que uma conexão em simultâneo. Identifique, se aplicável, as fases de início de conexão, transferência de dados e fim de conexão. Identifique também os tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações.

Resposta:

225 277.739148525 10.1.1.1	10.4.4.1	FTP	78 Request: RETR file1
226 277.739367013 10.4.4.1	10.1.1.1	TCP	74 20 → 37909 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM=1 TSval=124021...
227 277.739500427 10.1.1.1	10.4.4.1	TCP	74 37909 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK PERM=1 T...
228 277.739643027 10.4.4.1	10.1.1.1	TCP	66 20 → 37909 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1240219243 TSecr=3552...
229 277.739712557 10.4.4.1	10.1.1.1	FTP	130 Response: 150 Opening BINARY mode data connection for file1 (224 bytes).
230 277.742313851 10.4.4.1	10.1.1.1	FTP-DA...	298 FTP Data: 224 bytes (PORT) (RETR file1)
231 277.742452076 10.4.4.1	10.1.1.1	TCP	66 20 → 37909 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0 TSval=1240219246 TSe...
232 277.742509362 10.1.1.1	10.4.4.1	TCP	66 37909 → 20 [ACK] Seq=1 Ack=225 Win=65024 Len=0 TSval=3552738435 TSecr=12...
233 277.742600944 10.1.1.1	10.4.4.1	TCP	66 37909 → 20 [FIN, ACK] Seq=1 Ack=226 Win=65024 Len=0 TSval=3552738435 TSe...
234 277.742724716 10.4.4.1	10.1.1.1	TCP	66 20 → 37909 [ACK] Seq=226 Ack=2 Win=64256 Len=0 TSval=1240219247 TSecr=35...
235 277.742768603 10.4.4.1	10.1.1.1	FTP	90 Response: 226 Transfer complete.

Figura 24 - Captura das tramas da transferência do file1 por FTP a partir do Portatil1
(excerto da figura 8)

A partir do conjunto de tramas acima identificadas, correspondentes à transferência do file1 por FTP obteve-se o seguinte diagrama temporal:

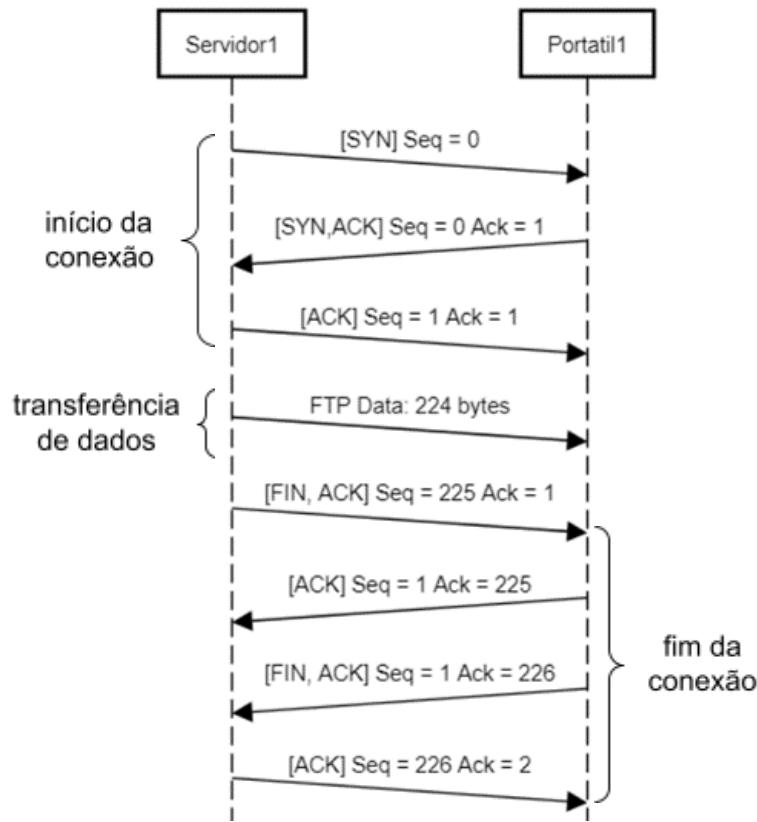


Figura 25 - Transferência File1 por FTP no Portatil1

361	399.403410977	10.4.4.1	10.2.2.1	FTP
362	399.488658826	10.2.2.1	10.4.4.1	78 Request: RETR file1
363	399.488946412	10.4.4.1	10.2.2.1	TCP 74 20 - 45513 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=367211...
364	399.494070265	10.2.2.1	10.4.4.1	TCP 74 45513 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 T...
365	399.494215860	10.4.4.1	10.2.2.1	TCP 66 20 - 45513 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=367211327 TSeср=1850...
366	399.494300637	10.4.4.1	10.2.2.1	FTP 130 Response: 150 Opening BINARY mode data connection for file1 (224 bytes).
367	399.494739615	10.4.4.1	10.2.2.1	FTP-DA... 299 FTP Data: 224 bytes (PORT) (RETR file1)
368	399.494741926	10.4.4.1	10.2.2.1	TCP 66 20 - 45513 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0 TSval=367211327 TSe...
369	399.499879926	10.2.2.1	10.4.4.1	TCP 66 45513 - 20 [ACK] Seq=1 Ack=225 Win=65024 Len=0 TSval=1850876758 TSeср=36...
370	399.542196814	10.2.2.1	10.4.4.1	TCP 66 54942 - 21 [ACK] Seq=124 Ack=391 Win=64256 Len=0 TSval=1850876800 TSeср=...
371	399.709510745	10.4.4.1	10.2.2.1	TCP 66 [TCP Retransmission] 20 - 45513 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0...
372	399.710583269	10.2.2.1	10.4.4.1	TCP 66 45513 - 20 [FIN, ACK] Seq=1 Ack=226 Win=65024 Len=0 TSval=1850876908 TSe...
373	399.710706322	10.4.4.1	10.2.2.1	TCP 66 20 - 45513 [ACK] Seq=226 Ack=2 Win=64256 Len=0 TSval=3672113543 TSeср=18...
374	399.710962353	10.4.4.1	10.2.2.1	FTP 99 Response: 226 Transfer complete.

Figura 26 - Captura das tramas da transferência do file1 por FTP a partir do PC1
(excerto da figura 10)

Da captura das tramas correspondentes à transferência do file1 a partir do PC1, representadas acima, obteve-se o seguinte diagrama temporal:

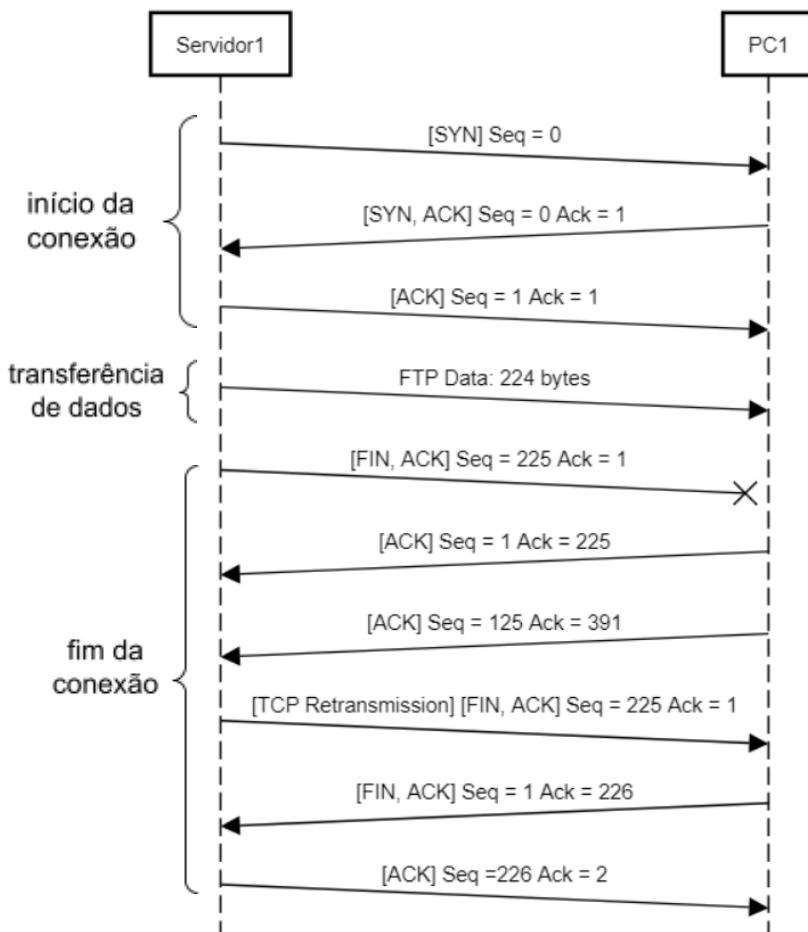


Figura 27 - Transferência File1 por FTP no PC1

Neste diagrama temporal, podemos ver como o protocolo atua caso ocorram erros, como acontece no segmento $[FIN,ACK]$ Seq = 225, encarregue por indicar que o envio de dados terminou, que acaba por se perder e é, assim, retransmitido quando o Servidor1 se apercebe que a flag não foi recebida pelo PC1.

Questão 3:

Obtenha a partir do wireshark, ou desenhe manualmente, um diagrama temporal para a transferência de file1 por TFTP. Identifique, se aplicável, as fases de início de conexão, transferência de dados e fim de conexão. Identifique também os tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações.

Resposta:

A conexão é estabelecida a partir do protocolo ARP e, de seguida, são apresentados os diagramas temporais da transferência do file1 por TFTP através do Portatil1 e através do PC1 onde se verifica a ocorrência de uma duplicação. É possível verificar que não se estabelece a conexão ao nível do transporte, logo não se aplica a existência de início e fim da conexão e que o UDP, para transferir ficheiros apenas realiza o pedido, envia o ficheiro indicando a que “block” se refere e se é o último e informa que o ficheiro foi recebido enviando o número do “block”.

No.	Time	Source	Destination	Protocol	Length	Info
282	335.759450410	00:00:00_aa:00:10	Broadcast	ARP	42	Who has 10.4.4.1? Tell 10.4.4.254
283	335.759620460	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42	10.4.4.1 is at 00:00:00_aa:00:14
284	335.759626345	10.1.1.1	10.4.4.1	TFTP	56	Read Request, File: file1, Transfer type: octet
285	335.769845072	10.4.4.1	10.1.1.1	TFTP	270	Data Packet, Block: 1 (last)
286	335.770381436	10.1.1.1	10.4.4.1	TFTP	46	Acknowledgement, Block: 1
211	340.968774081	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42	Who has 10.4.4.254? Tell 10.4.4.1
212	340.968797553	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42	10.4.4.254 is at 00:00:00_aa:00:10

Figura 28 - Captura das tramas da transferência do file1 por TFTP a partir do Portatil1

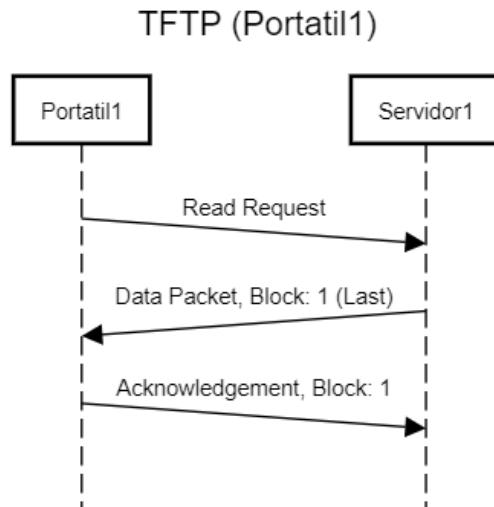


Figura 29 - Transferência File1 por TFTP no Portatil1

322	522.651967864	10.2.2.1	10.4.4.1	TFTP	56	Read Request, File: file1, Transfer type: octet
323	522.651969529	10.2.2.1	10.4.4.1	TFTP	56	Read Request, File: file1, Transfer type: octet
324	522.652813882	10.4.4.1	10.2.2.1	TFTP	270	Data Packet, Block: 1 (last)
325	522.653426726	10.4.4.1	10.2.2.1	TFTP	270	Data Packet, Block: 0 (last)
326	522.659418973	10.2.2.1	10.4.4.1	TFTP	46	Acknowledgement, Block: 1
327	522.659419970	10.2.2.1	10.4.4.1	ICMP	298	Destination unreachable (Port unreachable)
330	527.848305141	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42	Who has 10.4.4.1? Tell 10.4.4.254
331	527.848585686	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42	Who has 10.4.4.254? Tell 10.4.4.1
332	527.848590432	00:00:00_aa:00:14	00:00:00_aa:00:10	ARP	42	10.4.4.1 is at 00:00:00_aa:00:14
333	527.848597442	00:00:00_aa:00:10	00:00:00_aa:00:14	ARP	42	10.4.4.254 is at 00:00:00_aa:00:10

Figura 30 - Captura das tramas da transferência do file1 por TFTP a partir do PC1

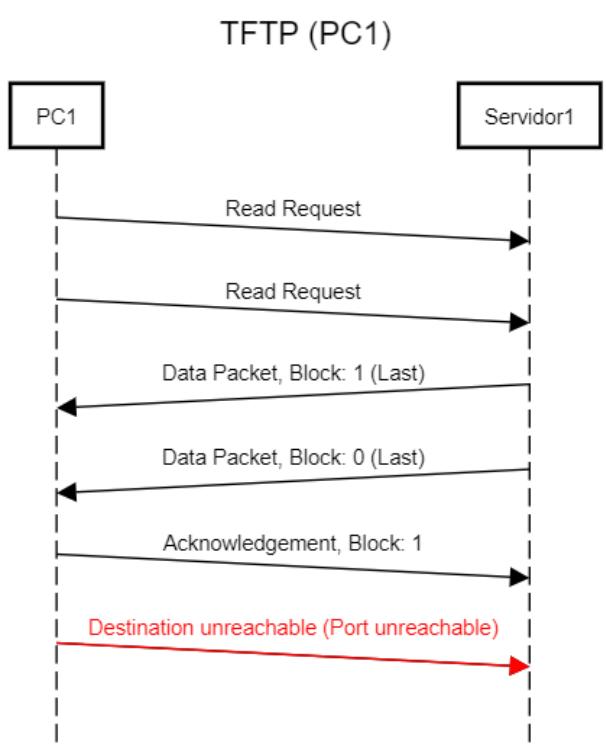


Figura 31 - Transferência File1 por TFTP no PC1

Questão 4:

Compare sucintamente as quatro aplicações de transferência de ficheiros que usou nos seguintes pontos (i) uso da camada de transporte; (ii) eficiência; (iii) complexidade; (iv) segurança;

Resposta:

Protocolo	Uso da Camada de Transporte (i)	Eficiência (ii)	Complexidade (iii)	Segurança (iv)
SFTP	TCP	Baixa	Alta - recorre a mecanismos de autenticação e encriptação	Muito seguro – o protocolo usa SSH para transferir dados. Estes são encriptados e enviados para o receptor
FTP	TCP	Média	Média – possui uma elevada variedade de mensagens que podem ser transmitidas	Baixa – possui autenticação, mas passwords são enviadas em modo texto através da rede e qualquer um pode aceder e dados não são encriptados
TFTP	UDP	Alta – rápido com poucos recursos	Baixa	Baixa – não possui encriptação de dados
HTTP	TCP	Alta - no entanto, quanto maior for o tamanho dos ficheiros, maior o número de segmentos	Baixa	Baixa – não existe qualquer tipo de encriptação e o conteúdo dos ficheiros partilhados podem ser visualizados antes de chegar ao receptor e não possui autenticação. Pode ser melhorada através de https

Parte II: Uso da camada de transporte por parte das aplicações

Comando usado (aplicação)	Protocolo de Aplicação (se aplicável)	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)	Overhead de transporte em bytes (se aplicável)
wget, lynx ou via browser	HTTP	TCP	Porta 80 - HTTP Porta 443 - HTTPS	20 a 40 (TCP)
ssh, sftp	SSH	TCP	Porta 22	40 a 60 (TCP)
ftp	FTP	TCP	Porta - 21 (conexão de controlo) Porta - 20 (conexão de dados)	Conexão controlo - 20 a 40 Conexão dados - 40 +/-
Tftp	TFTP	UDP	Porta - 69	8
telnet	TELNET	TCP	Porta - 23	40 a 50
nslookup ou dig	DNS	Não Específico	Porta - 53	8 (UDP) 20 (TCP)
Ping	ICMP	Não específico, opera diretamente sobre o ICMP	Não aplicável	Valor bastante mínimo Consiste principalmente nos cabeçalhos ICMP, cujo tamanho é relativamente pequeno.
Traceroute	ICMP	Não específico, opera diretamente sobre o ICMP	Não aplicável	Valor bastante mínimo Consiste principalmente nos cabeçalhos ICMP, cujo tamanho é relativamente pequeno.
Minecraft	Usa o próprio protocol “Minecraft Protocol”	TCP	Porta - 25565 (TCP)	20
Valorant	Protocolo Próprio	UDP	Varia dependendo da configuração do jogo e da rede. Portas UDP diferentes podem ser usadas para diferentes recursos de jogabilidade, como o jogo em si e o voice chat.	8
Youtube	HTTP / HTTP/2	tTCP	Porta - 80 (HTTP) Porta - 443(HTTP/2)	40 a 60