



Universidade do Minho
Escola de Engenharia

Comunicações por Computador

Grupo 6.12
2022/2023

TP1 - Protocolos da Camada de Transporte

Alexandra Santos (A94523)
Inês Ferreira (A97372)
Joana Branco (A96584)

Braga, 13 de outubro de 2022

Índice

Parte B

Questão 1	2
Questão 2	2
Questão 3	4
Questão 4	4
Questão 5	6

Conclusão	11
------------------	-----------

Parte B

Questão 1

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

R: Tendo em conta os resultados observados, as perdas e duplicações de pacotes causam um decréscimo no desempenho das aplicações e sobrecarga na rede. Com isto, o processo de envio ou reenvio é atrasado o que provoca uma taxa de transferência menor e de menor velocidade de envio esperada.

A duplicação de pacotes também afeta a capacidade de armazenamento.

A camada que lidou com os problemas mencionados é a camada de transporte, sendo esta a responsável pela respetiva transferência de dados entre duas máquinas.

Questão 2

Obtenha a partir do Wireshark , ou desenhe manualmente, um diagrama temporal para a transferência do ficheiro file1 por FTP realizada em A.3. Foque-se apenas na transferência de dados [ftp-data] e não na conexão de controlo (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 tanto nos dados como nas confirmações.

R: As figuras seguintes podem ser traduzidas com a seguinte legenda: a vermelho é a fase de início de conexão, a verde está identificada a fase de transferência de dados e a azul é o fim da conexão. Já os segmentos podem ser identificados pelo filtro ip.addr == 10.2.2.1 na figura 3.

13	19.278412516	fe80::f428:ecff:fe9...	ff02::2	ICMPv6	70 Router Solicitation from 06:cf:61:55:10:df
14	20.015024772	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
15	21.917291642	00:00:00:aa:00:10	Broadcast	ARP	42 Who has 10.2.2.1? Tell 10.2.2.254
16	21.918929030	00:00:00:aa:00:14	00:00:00:aa:00:10	ARP	42 10.2.2.1 is at 00:00:00:aa:00:14
17	21.918948492	10.1.1.1	10.2.2.1	TCP	74 52496 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
18	21.919700840	10.2.2.1	10.1.1.1	TCP	74 21 → 52496 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
19	21.920189649	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2344798312...
20	21.923410572	10.2.2.1	10.1.1.1	FTP	86 Response: 220 (vsFTPd 3.0.3)
21	21.923860404	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=234479831...
22	22.016105069	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
23	24.017088039	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
24	25.567412435	10.1.1.1	10.2.2.1	FTP	77 Request: USER core
25	25.568076258	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=21 Ack=12 Win=65280 Len=0 TSval=15267804...
26	25.568561313	10.2.2.1	10.1.1.1	FTP	100 Response: 331 Please specify the password.
27	25.569051093	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=12 Ack=55 Win=64256 Len=0 TSval=23448019...
28	25.654312721	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
29	26.017703595	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
30	28.018057165	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
31	28.147582832	10.1.1.1	10.2.2.1	FTP	77 Request: PASS core
32	28.148307255	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=55 Ack=23 Win=65280 Len=0 TSval=15267830...
33	28.165653015	10.2.2.1	10.1.1.1	FTP	89 Response: 230 Login successful.
34	28.166254276	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=23 Ack=78 Win=64256 Len=0 TSval=23448045...
35	28.166894935	10.1.1.1	10.2.2.1	FTP	72 Request: SYST
36	28.167042169	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=78 Ack=29 Win=65280 Len=0 TSval=15267830...
37	28.167544953	10.2.2.1	10.1.1.1	FTP	85 Response: 215 UNIX Type: L8
38	28.168022494	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=29 Ack=97 Win=64256 Len=0 TSval=23448045...
39	30.019374803	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
40	32.019825706	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
41	34.020781650	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
42	35.625076093	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
43	36.022046232	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
44	38.022345295	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
45	39.048612876	fe80::f428:ecff:fe9...	ff02::fb	NDNS	203 Standard query 0x0000 PTR _nfs_.tcp.local, "QM" question PTR ...
46	40.022711773	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
47	42.025306604	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
48	43.054272519	fe80::200:ff:feaa:15	ff02::2	ICMPv6	70 Router Solicitation from 00:00:00:aa:00:15
49	44.040500996	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
50	45.010930389	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
51	46.045404493	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
52	47.056926037	10.1.1.1	10.2.2.1	FTP	71 Request: PWD
53	47.057086288	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=97 Ack=34 Win=65280 Len=0 TSval=15268019...
54	47.057521656	10.2.2.1	10.1.1.1	FTP	109 Response: 257 "/home/core" is the current directory
55	47.058095496	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=34 Ack=140 Win=64256 Len=0 TSval=2344823...
56	48.045803078	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
57	50.024331555	fe80::200:ff:feaa:14	ff02::2	ICMPv6	70 Router Solicitation from 00:00:00:aa:00:14
58	50.046902426	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
59	51.209993922	10.1.1.1	10.2.2.1	FTP	89 Request: PORT 10,1,1,1,219,151
60	51.211095902	10.2.2.1	10.1.1.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.

Figura 1: Primeira parte da transferência do ficheiro file1 por FTP

61	51.212776154	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=57 Ack=191 Win=64256 Len=0 TSval=2344827...
62	51.214420536	10.1.1.1	10.2.2.1	FTP	72 Request: LIST
63	51.216460484	10.2.2.1	10.1.1.1	TCP	74 20 → 56215 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
64	51.217052225	10.1.1.1	10.2.2.1	TCP	74 56215 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
65	51.217642159	10.2.2.1	10.1.1.1	TCP	66 20 → 56215 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1526806115...
66	51.218396260	10.2.2.1	10.1.1.1	FTP	105 Response: 150 Here comes the directory listing.
67	51.219071985	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=63 Ack=230 Win=64256 Len=0 TSval=2344827...
68	51.219963604	10.2.2.1	10.1.1.1	FTP-DA...	1280 FTP Data: 1214 bytes (PORT) (LIST)
69	51.219970890	10.2.2.1	10.1.1.1	TCP	66 20 → 56215 [FIN, ACK] Seq=1215 Ack=1 Win=64256 Len=0 TSval=15...
70	51.221014061	10.1.1.1	10.2.2.1	TCP	66 56215 → 20 [ACK] Seq=1 Ack=1215 Win=64128 Len=0 TSval=2344827...
71	51.221051135	10.1.1.1	10.2.2.1	TCP	66 56215 → 20 [FIN, ACK] Seq=1 Ack=1216 Win=64128 Len=0 TSval=23...
72	51.221399700	10.2.2.1	10.1.1.1	TCP	66 20 → 56215 [ACK] Seq=1216 Ack=2 Win=64256 Len=0 TSval=1526806...
73	51.222360213	10.2.2.1	10.1.1.1	FTP	90 Response: 226 Directory send OK.
74	51.223169259	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=63 Ack=254 Win=64256 Len=0 TSval=2344827...
75	52.046018247	fe80::d85d:5eff:fe7... ff02::2	224.0.0.5	ICMPv6	70 Router Solicitation from da:5d:5e:73:d9:cd
76	52.047870955	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
77	52.997907975	fe80::d85d:5eff:fe7... ff02::fb	224.0.0.5	MDNS	203 Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR ...
78	54.049562765	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
79	55.641439937	fe80::200:ff:feaa:10 ff02::5	224.0.0.5	OSPF	90 Hello Packet
80	56.050916935	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
81	56.582725653	10.1.1.1	10.2.2.1	FTP	74 Request: TYPE I
82	56.583687853	10.2.2.1	10.1.1.1	FTP	97 Response: 200 Switching to Binary mode.
83	56.586648870	10.1.1.1	10.2.2.1	FTP	87 Request: PORT 10,1,1,198,9
84	56.586662392	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=71 Ack=285 Win=64256 Len=0 TSval=2344832...
85	56.588362433	10.2.2.1	10.1.1.1	FTP	117 Response: 200 PORT command successful. Consider using PASV.
86	56.588691818	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=92 Ack=336 Win=64256 Len=0 TSval=2344832...
87	56.589386884	10.1.1.1	10.2.2.1	FTP	78 Request: RETR file1
88	56.595006759	10.2.2.1	10.1.1.1	TCP	74 20 → 50697 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
89	56.595660946	10.1.1.1	10.2.2.1	TCP	74 50697 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
90	56.596310325	10.2.2.1	10.1.1.1	TCP	66 20 → 50697 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1526811494...
91	56.597335543	10.2.2.1	10.1.1.1	FTP	130 Response: 150 Opening BINARY mode data connection for file1 (...)
92	56.598123941	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=104 Ack=400 Win=64256 Len=0 TSval=234483...
93	56.598545377	10.2.2.1	10.1.1.1	FTP-DA...	290 FTP Data: 224 bytes (PORT) (RETR file1)
94	56.599684731	10.2.2.1	10.1.1.1	TCP	66 20 → 50697 [FIN, ACK] Seq=225 Ack=1 Win=64256 Len=0 TSval=152...
95	56.599752319	10.1.1.1	10.2.2.1	TCP	66 50697 → 20 [ACK] Seq=1 Ack=225 Win=65024 Len=0 TSval=23448329...
96	56.600888625	10.1.1.1	10.2.2.1	TCP	66 50697 → 20 [FIN, ACK] Seq=1 Ack=226 Win=65024 Len=0 TSval=234...
97	56.601437164	10.2.2.1	10.1.1.1	TCP	66 20 → 50697 [ACK] Seq=226 Ack=2 Win=64256 Len=0 TSval=15268114...
98	56.601856134	10.2.2.1	10.1.1.1	FTP	90 Response: 226 Transfer complete.
99	56.602565971	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=104 Ack=424 Win=64256 Len=0 TSval=234483...
100	58.051834505	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
101	60.050961214	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
102	60.701106641	10.1.1.1	10.2.2.1	FTP	72 Request: QUIT

Figura 2: Segunda parte da transferência do ficheiro file1 por FTP

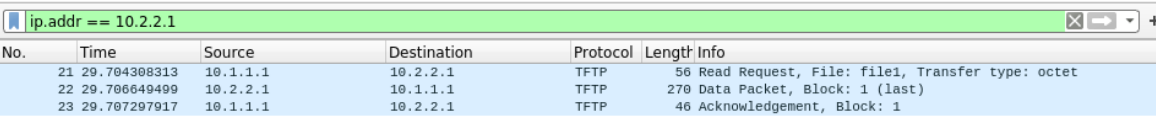
ip.addr == 10.2.2.1						
No.	Time	Source	Destination	Protocol	Length	Info
56	87.937357043	10.1.1.1	10.2.2.1	TCP	74	47506 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
57	87.937896294	10.2.2.1	10.1.1.1	TCP	74	21 → 47506 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
58	87.938749512	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4007927899...
59	87.947472863	10.2.2.1	10.1.1.1	FTP	86	Response: 220 (vsFTPD 3.0.3)
60	87.948245116	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=400792790...
63	90.844482888	10.1.1.1	10.2.2.1	FTP	77	Request: USER core
64	90.845303983	10.2.2.1	10.1.1.1	TCP	66	21 → 47506 [ACK] Seq=21 Ack=12 Win=65280 Len=0 TSval=37403429...
65	90.846087797	10.2.2.1	10.1.1.1	FTP	100	Response: 331 Please specify the password.
66	90.848004708	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=12 Ack=55 Win=64256 Len=0 TSval=40079308...
68	93.701482550	10.1.1.1	10.2.2.1	FTP	77	Request: PASS core
69	93.702955836	10.2.2.1	10.1.1.1	TCP	66	21 → 47506 [ACK] Seq=55 Ack=23 Win=65280 Len=0 TSval=37403457...
70	93.743686781	10.2.2.1	10.1.1.1	FTP	89	Response: 230 Login successful.
71	93.744490760	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=23 Ack=78 Win=64256 Len=0 TSval=40079337...
72	93.746269059	10.1.1.1	10.2.2.1	FTP	72	Request: SYST
73	93.747463796	10.2.2.1	10.1.1.1	TCP	66	21 → 47506 [ACK] Seq=78 Ack=29 Win=65280 Len=0 TSval=37403458...
74	93.748150563	10.2.2.1	10.1.1.1	FTP	85	Response: 215 UNIX Type: L8
75	93.749496840	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=29 Ack=97 Win=64256 Len=0 TSval=40079337...
84	105.549792615	10.1.1.1	10.2.2.1	FTP	71	Request: PWD
85	105.550525247	10.2.2.1	10.1.1.1	TCP	66	21 → 47506 [ACK] Seq=97 Ack=34 Win=65280 Len=0 TSval=37403576...
86	105.551096752	10.2.2.1	10.1.1.1	FTP	109	Response: 257 "/home/core" is the current directory
87	105.552145717	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=34 Ack=140 Win=64256 Len=0 TSval=4007945...
92	107.678644832	10.1.1.1	10.2.2.1	FTP	89	Request: PORT 10,1,1,166,233
93	107.681860039	10.2.2.1	10.1.1.1	FTP	117	Response: 200 PORT command successful. Consider using PASV.
94	107.682776176	10.1.1.1	10.2.2.1	TCP	66	47506 → 21 [ACK] Seq=57 Ack=191 Win=64256 Len=0 TSval=4007947...
95	107.683448252	10.1.1.1	10.2.2.1	FTP	72	Request: LIST
96	107.686151293	10.2.2.1	10.1.1.1	TCP	74	20 → 47229 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
97	107.687164066	10.1.1.1	10.2.2.1	TCP	74	47229 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
98	107.690455030	10.2.2.1	10.1.1.1	TCP	66	20 → 47229 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=374035766...

Figura 3: filtro ip.addr == 10.2.2.1

Questão 3

Obtenha a partir do Wireshark , ou desenhe manualmente, um diagrama temporal para a transferência do ficheiro file1 por TFTP realizada em A.4. 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 tanto nos dados como nas confirmações.

R: A conexão para a transferência de dados por TFTP é feita pelo o protocolo UDP. Percebemos que estamos a lidar com UDP e não TCP pois este último protocolo tipicamente usa uma mensagem de “request” para assegurar a conectividade ao recetor que pretende enviar dados e nesta situação isso não aconteceu (não encontramos frames com mensagem de “request ” e de confirmação). Como vemos na figura o ficheiro foi transferido de uma só vez, num único bloco logo só houve uma interação na troca de dados (apenas é enviado sem garantia de sucesso) e assim o segmentos e números de sequência usados não estão declarados.



No.	Time	Source	Destination	Protocol	Length	Info
21	29.704308313	10.1.1.1	10.2.2.1	TFTP	56	Read Request, File: file1, Transfer type: octet
22	29.706649499	10.2.2.1	10.1.1.1	TFTP	270	Data Packet, Block: 1 (last)
23	29.707297917	10.1.1.1	10.2.2.1	TFTP	46	Acknowledgement, Block: 1

Figura 4: Transferência do ficheiro file1 por TFTP

Questão 4

Compare sucintamente as quatro aplicações de transferência de ficheiros que usou, tendo em consideração os seguintes aspetos: (i) identificação da camada de transporte; (ii) eficiência; (iii) complexidade; (iv) segurança.

R:

(i) identificação da camada de transporte

TFTP- UDP

FTP- TCP

HTTP-TCP

SPTF-TCP

(ii) eficiência

Em termos de eficiência (velocidade de transmissão dos dados, por exemplo), a aplicação de transferência que se destaca é o TFTP pois este usa protocolo UDP ao contrário do resto. Este protocolo em questão não é tão exigente nas questões conectividade “sender-receiver” e “receiver-sender”, isto é, envia os datagramas sem assegurar que estes chegaram ao destino, tendo assim um menor tempo de envio em relação aos que usam TCP.

Ao fazermos a transferência do do “file1” com 230 bytes para as 4 aplicações observadas notamos o número de bytes capturados e o tamanho do header e verificamos que a transferência por TFTP foi a mais rápida (como era de esperar (porque o header de controlo do UDP é mais reduzido

Em termos de eficiência podemos organizar do maior para o menor por: TFTP, FTP, HTTP, SFTP.

(iii) complexidade

As aplicações que implicam maior trabalho e complexidade para serem utilizadas são o TFTP e o FTP, dentro das que estudamos. Estas requerem um maior esforço pela nossa parte como utilizadores pois para efetuar transferências é necessário configurar e ativar os servidores. Em termos de complexidade, do nível mais alto para o mais baixo, segue HTTP, de mais simples utilização e, por fim, o SFTP.

(iv) segurança

As ligações SSH que são usadas por SFTP formam uma ligação segura e encriptada, que permite uma comunicação segura entre dois componentes. Sendo considerada esta a aplicação mais segura entre todas as estudadas. Quando as outras ligações não usam protocolos criptográficos na informação tornam-se menos seguras. O protocolo FTP à primeira vista pode parecer seguro por requerer *login* e *password*, porém como podemos ver abaixo na captura do *wireshark* é possível termos acesso à *password*, logo é apenas uma falsa ideia de segurança.

24	25.567412435	10.1.1.1	10.2.2.1	FTP	77 Request: USER core
25	25.568076258	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=21 Ack=12 Win=65280 Len=0 TSval=15267804...
26	25.568561313	10.2.2.1	10.1.1.1	FTP	109 Response: 331 Please specify the password.
27	25.569051093	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=12 Ack=55 Win=64256 Len=0 TSval=23448019...
28	25.654312721	fe80::200:ff:feaa:10	ff02::5	OSPF	90 Hello Packet
29	26.017703595	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
30	28.018057165	10.2.2.254	224.0.0.5	OSPF	78 Hello Packet
31	28.147582832	10.1.1.1	10.2.2.1	FTP	77 Request: PASS core
32	28.148307255	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=55 Ack=23 Win=65280 Len=0 TSval=15267830...
33	28.165653015	10.2.2.1	10.1.1.1	FTP	89 Response: 230 Login successful.
34	28.166254276	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=23 Ack=78 Win=64256 Len=0 TSval=23448045...
35	28.166894935	10.1.1.1	10.2.2.1	FTP	72 Request: SYST
36	28.167042169	10.2.2.1	10.1.1.1	TCP	66 21 → 52496 [ACK] Seq=78 Ack=29 Win=65280 Len=0 TSval=15267830...
37	28.167544953	10.2.2.1	10.1.1.1	FTP	85 Response: 215 UNIX Type: L8
38	28.168022494	10.1.1.1	10.2.2.1	TCP	66 52496 → 21 [ACK] Seq=29 Ack=97 Win=64256 Len=0 TSval=23448045...

Figura 5: Insegurança do FTP

```

root@Portatil1:/tmp/pycore,36111/Portatil1.conf# ftp 10.2.2.1
connected to 10.2.2.1.
220 (vsFTPd 3.0.3)
name (10.2.2.1:root): core
331 Please specify the password.
password:
30 Login successful.
remote system type is UNIX.
using binary mode to transfer files.
ftp> status
connected to 10.2.2.1.
to 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
trans: off
map: off
hash mark printing: off; Use of PORT cmds: on
tick counter printing: off

```

Figura 6: Insegurança do FTP

Questão 5

Com base no trabalho realizado, construa uma tabela informativa identificando, para cada aplicação executada (ping, traceroute, telnet, ftp, tftp, wget/lynx, nslookup, ssh, etc.), qual o protocolo de aplicação, o protocolo de transporte, a porta de atendimento e o overhead de transporte.

R:

	Protocolo de aplicação	Protocolo de transporte	Porta de atendimento	Overhead de transporte
ping	–	–	–	–
traceroute	–	–	–	–
telnet	TELNET	TCP	80	20
ftp	FTP	TCP	21	20
tftp	TFTP	UDP	69	8
wget/lynx	HTTP	TCP	80	20
nslookup	DNS	UDP	53	8
ssh	SSH	TCP	22	20

De forma a justificar a tabela anteriormente apresentada são apresentados diversos tráfegos:

```
core@xubuncore:~$ ping www.google.pt
PING www.google.pt (216.58.215.131) 56(84) bytes of data.
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=1 ttl=113 time=57.0 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=2 ttl=113 time=57.8 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=3 ttl=113 time=54.4 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=4 ttl=113 time=55.9 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=5 ttl=113 time=65.5 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=6 ttl=113 time=57.0 ms
64 bytes from mad41s04-in-f3.1e100.net (216.58.215.131): icmp_seq=7 ttl=113 time=55.3 ms
^C
--- www.google.pt ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 54.418/57.544/65.476/3.406 ms
```

Figura 7 : Aplicação ping

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0909090909	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 2)
2	0.057026220	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=113 (request in 1)
3	1.002819770	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 4)
4	1.000510878	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=113 (request in 3)
5	2.004962042	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 6)
6	2.059316990	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=113 (request in 5)
7	3.006742875	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply in 8)
8	3.062548201	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=113 (request in 7)
9	4.007974501	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 10)
10	4.073386097	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=113 (request in 9)
11	5.010106754	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=6/1536, ttl=64 (reply in 12)
12	5.067024729	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=6/1536, ttl=113 (request in 11)
13	5.130275840	PcsCompu_06:03:48	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
14	5.131602168	RealtekU_12:35:02	PcsCompu_06:03:48	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
15	6.011944248	10.0.2.15	216.58.215.131	ICMP	98	Echo (ping) request id=0x0003, seq=7/1792, ttl=64 (reply in 16)
16	6.067171226	216.58.215.131	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0003, seq=7/1792, ttl=113 (request in 15)

Figura 8: Tráfego relativo ao ping

```

core@xubuncore:~$ telnet telehack.com
Trying 64.13.139.230...
Connected to telehack.com.
Escape character is '^]'.

Connected to TELEHACK port 43

It is 4:35      n Wednesday, October 12, 2022 in Mount   View, California, USA.
There are 7    ocal users. There ar 26642 hosts on the  twork.

Type HELP for a detailed comma  st.
Type NEWUSER to create an accou
Press control-C to interrupt any command.

May the com   d line live forever.

Command, on   f the following:
2048          ?          a2          ac          advent          aquarium
basic         bf         c8         calc         callsign        ching
clear         clock        cowsay       date          ddate           echo
eliza         factor       figlet       finger        fnord           geoip
gif           help        ipaddr      joke          login           mac
mineswee er   orse        notes       octopus       phoon           pig
ping          ng          primes      qr            rain            rand
rig           13         salvo       sleep         starwars        sudoku
typespeed     its         uptime      usenet        users           uumap
uupath        uplot       weather     when          zc              zork

.rain         0

          -
        /- \
      |||.||
      \-/
        -
          -
        / \
      | 0 |
      \ /
        -
0

```

Figura 9 : Aplicação telnet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	64.13.139.230	TCP	74	45046 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=...
2	0.196607448	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.196709166	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.198244309	10.0.2.15	64.13.139.230	TELNET	81	Telnet Data ...
5	0.198854930	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1 Ack=28 Win=65535 Len=0
6	0.393255202	64.13.139.230	10.0.2.15	TELNET	60	Telnet Data ...
7	0.393417365	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=28 Ack=4 Win=64237 Len=0
8	0.629739693	64.13.139.230	10.0.2.15	TELNET	105	Telnet Data ...
9	0.629797533	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=28 Ack=55 Win=64186 Len=0
10	0.630341428	10.0.2.15	64.13.139.230	TELNET	72	Telnet Data ...
11	0.631164504	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=55 Ack=46 Win=65535 Len=0
12	0.828270171	64.13.139.230	10.0.2.15	TELNET	1233	Telnet Data ...
13	0.828386129	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=46 Ack=1234 Win=63666 Len=0
14	0.829624636	10.0.2.15	64.13.139.230	TELNET	80	Telnet Data ...
15	0.831210910	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1234 Ack=72 Win=65535 Len=0
16	6.389200630	10.0.2.15	64.13.139.230	TELNET	55	Telnet Data ...
17	6.390241780	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1234 Ack=73 Win=65535 Len=0
18	6.518955104	10.0.2.15	64.13.139.230	TELNET	55	Telnet Data ...
19	6.519913052	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1234 Ack=74 Win=65535 Len=0
20	6.588868462	64.13.139.230	10.0.2.15	TELNET	60	Telnet Data ...
21	6.588913755	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=74 Ack=1235 Win=63666 Len=0
22	6.827528235	64.13.139.230	10.0.2.15	TELNET	60	Telnet Data ...
23	6.827572879	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=74 Ack=1236 Win=63666 Len=0
24	7.363493417	10.0.2.15	64.13.139.230	TELNET	55	Telnet Data ...
25	7.364472621	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1236 Ack=75 Win=65535 Len=0
26	7.563689011	64.13.139.230	10.0.2.15	TELNET	60	Telnet Data ...
27	7.563754237	10.0.2.15	64.13.139.230	TCP	54	45046 → 23 [ACK] Seq=75 Ack=1237 Win=63666 Len=0
28	8.042892347	10.0.2.15	64.13.139.230	TELNET	55	Telnet Data ...
29	8.043739999	64.13.139.230	10.0.2.15	TCP	60	23 → 45046 [ACK] Seq=1237 Ack=76 Win=65535 Len=0

Figura 10: Tráfego relativo ao telnet

```
core@xubuncore:~$ ftp ftp.gnu.org
Connected to ftp.gnu.org.
220 GNU FTP server ready.
Name (ftp.gnu.org:core): anonymous
230-NOTICE (Updated October 15 2021):
230-
230-If you maintain scripts used to access ftp.gnu.org over FTP,
230-we strongly encourage you to change them to use HTTPS instead.
230-
230-Eventually we hope to shut down FTP protocol access, but plan
230-to give notice here and other places for several months ahead
230-of time.
230-
230-
230-
230-Due to U.S. Export Regulations, all cryptographic software on this
230-site is subject to the following legal notice:
230-
230-   This site includes publicly available encryption source code
230-   which, together with object code resulting from the compiling of
230-   publicly available source code, may be exported from the United
230-   States under License Exception "TSU" pursuant to 15 C.F.R. Section
230-   740.13(e).
230-
230-This legal notice applies to cryptographic software only. Please see
230-the Bureau of Industry and Security (www.bxa.doc.gov) for more
230-information about current U.S. regulations.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figura 11: Aplicação ftp

No.	Time	Source	Destination	Protocol	Length	Info
9	1.395040758	209.51.188.20	10.0.2.15	FTP	81	Response: 220 GNU FTP server ready.
11	8.304405109	10.0.2.15	209.51.188.20	FTP	70	Request: USER anonymous
13	8.522277548	209.51.188.20	10.0.2.15	FTP	233	Response: 230-NOTICE (Updated October 15 2021):
15	8.522278080	209.51.188.20	10.0.2.15	FTP	223	Response: 230-
17	8.644738340	209.51.188.20	10.0.2.15	FTP	723	Response: 230-
19	8.645064307	10.0.2.15	209.51.188.20	FTP	60	Request: SYST
21	8.768555881	209.51.188.20	10.0.2.15	FTP	73	Response: 215 UNIX Type: L8

Figura 12: Tráfego relativo ao ftp

```
core@xubuncore:~$ nslookup www.uminho.pt
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.uminho.pt
Address: 193.137.9.114
```

Figura 13: Aplicação nslookup

No.	Time	Source	Destination	Protocol	Length	Info
2276	1.869740528	90.130.70.73	10.0.2.15	TCP	42394	80 → 49734 [ACK] Seq=11360651 Ack=1 Win=65535 Len=42340
2277	1.869813819	10.0.2.15	90.130.70.73	TCP	54	49734 → 80 [ACK] Seq=1 Ack=11402991 Win=65535 Len=0
2278	1.870107348	90.130.70.73	10.0.2.15	TCP	1514	80 → 49734 [PSH, ACK] Seq=11402991 Ack=1 Win=65535 Len=1460
2279	1.870903016	90.130.70.73	10.0.2.15	TCP	604	80 → 49734 [PSH, ACK] Seq=11404451 Ack=1 Win=65535 Len=550
2280	1.870917190	10.0.2.15	90.130.70.73	TCP	54	49734 → 80 [ACK] Seq=1 Ack=11405001 Win=65535 Len=0
2281	1.885921143	10.0.2.15	193.137.16.145	DNS	84	Standard query 0x072c A www.uminho.pt OPT
2282	1.889694116	90.130.70.73	10.0.2.15	TCP	13804	80 → 49734 [PSH, ACK] Seq=11405001 Ack=1 Win=65535 Len=13750
2283	1.889810156	10.0.2.15	90.130.70.73	TCP	54	49734 → 80 [ACK] Seq=1 Ack=11418751 Win=65535 Len=0
2284	1.890795935	90.130.70.73	10.0.2.15	TCP	30714	80 → 49734 [ACK] Seq=11418751 Ack=1 Win=65535 Len=30660
2285	1.890930694	90.130.70.73	10.0.2.15	TCP	18144	80 → 49734 [PSH, ACK] Seq=11449411 Ack=1 Win=65535 Len=18090
2286	1.891703098	10.0.2.15	90.130.70.73	TCP	54	49734 → 80 [ACK] Seq=1 Ack=11467501 Win=65535 Len=0
2287	1.898870545	90.130.70.73	10.0.2.15	TCP	33634	80 → 49734 [ACK] Seq=11467501 Ack=1 Win=65535 Len=33580
2288	1.898908865	10.0.2.15	90.130.70.73	TCP	54	49734 → 80 [ACK] Seq=1 Ack=11501081 Win=65535 Len=0

Figura 14: Tráfego relativo ao nslookup

```
core@xubuncore:~$ wget -O /dev/null http://speedtest.tele2.net/10GB.zip
--2022-10-13 10:18:28-- http://speedtest.tele2.net/10GB.zip
Resolving speedtest.tele2.net (speedtest.tele2.net)... 90.130.70.73, 2a00:800:1010::1
Connecting to speedtest.tele2.net (speedtest.tele2.net)|90.130.70.73|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10737418240 (10G) [application/zip]
Saving to: '/dev/null'

/dev/null      100%[=====>] 10,00G  17,8MB/s   in 14m 35s

2022-10-13 10:33:03 (11,7 MB/s) - '/dev/null' saved [10737418240/10737418240]
```

Figura 15 : Aplicação HTTP

http						
No.	Time	Source	Destination	Protocol	Length	Info
8	0.070499344	10.0.2.15	90.130.70.73	HTTP	208	GET /10GB.zip HT
30453	32.141680414	90.130.70.73	10.0.2.15	HTTP	19034	Continuation
30454	32.141739236	90.130.70.73	10.0.2.15	HTTP	10274	Continuation
30456	32.141843568	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30457	32.141947593	90.130.70.73	10.0.2.15	HTTP	16114	Continuation
30458	32.142117978	90.130.70.73	10.0.2.15	HTTP	32174	Continuation
30460	32.142237499	90.130.70.73	10.0.2.15	HTTP	16114	Continuation
30461	32.142256893	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30462	32.142320247	90.130.70.73	10.0.2.15	HTTP	17574	Continuation
30463	32.142385122	90.130.70.73	10.0.2.15	HTTP	17574	Continuation
30464	32.142441787	90.130.70.73	10.0.2.15	HTTP	11734	Continuation
30466	32.142562321	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30467	32.142562408	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30469	32.142708030	90.130.70.73	10.0.2.15	HTTP	40934	Continuation
30470	32.143076461	90.130.70.73	10.0.2.15	HTTP	21954	Continuation
30471	32.143092516	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30473	32.143237658	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30474	32.143654880	90.130.70.73	10.0.2.15	HTTP	62834	Continuation
30476	32.144899133	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30477	32.145096054	90.130.70.73	10.0.2.15	HTTP	62834	Continuation
30479	32.149024864	90.130.70.73	10.0.2.15	HTTP	1514	Continuation
30480	32.149025020	90.130.70.73	10.0.2.15	HTTP	10274	Continuation
30481	32.149121699	90.130.70.73	10.0.2.15	HTTP	26334	Continuation
30482	32.149190237	90.130.70.73	10.0.2.15	HTTP	17574	Continuation
▶ Frame 8: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface enp0s3, id 0 ▶ Ethernet II, Src: PcsCompu_06:03:48 (08:00:27:06:03:48), Dst: RealtekU_12:35:02 (52:54:00:12:35:02) ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 90.130.70.73 ▼ Transmission Control Protocol, Src Port: 49930, Dst Port: 80, Seq: 1, Ack: 1, Len: 154 Source Port: 49930 Destination Port: 80 [Stream index: 0] [TCP Segment Len: 154] Sequence number: 1 (relative sequence number) Sequence number (raw): 605389832 [Next sequence number: 155 (relative sequence number)] Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 17920002 0101 = Header Length: 20 bytes (5) ▶ Flags: 0x018 (PSH, ACK) Window size value: 64240 [Calculated window size: 64240] [Window size scaling factor: -2 (no window scaling used)] Checksum: 0xad8e [unverified] [Checksum Status: Unverified] Urgent pointer: 0 ▶ [SEQ/ACK analysis] ▶ [Timestamps] TCP payload (154 bytes) ▶ Hypertext Transfer Protocol						

Figura 16: Tráfego relativo a HTTP

Conclusão

Neste trabalho conseguimos desenvolver o nosso conhecimento a nível dos softwares de controle e administração de redes, como o Wireshark e o Core fornecido.

Fundamentamos conceitos importantes, que são um objetivo final da aprendizagem desta unidade curricular como os protocolos da camada de transporte. Não foram sentidas muitas dificuldades na utilização do Core por causa dos conhecimentos adquiridos provenientes da unidade curricular de Redes de Computadores.

Acreditamos que este trabalho foi relevante para perceber, identificar e analisar detalhadamente protocolos TCP, UDP e ainda o funcionamento de outros protocolos de aplicação como FTP, HTTP, SFTP, HTTP.