

Protocolos da Camada de Transporte

Filipa Rebelo, Rúben Rodrigues, and Guilherme Gonçalves

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
email: {a90234,a80960,a88280}@alunos.uminho.pt

1 Questões

1.1 Exercício 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.

A camada de transporte lidou com as perdas e duplicações de pacotes. Para a resolução deste problema, os mecanismos de controlo de erros do protocolo TCP descarta o pacote e reenvia-o, sem alterar a sua integridade. Por outro lado, o protocolo UDP apenas descarta o pacote.

Para evitar problemas de perdas e duplicações, o uso de protocolos TCP, que são orientados a conexões, passam a ser mais usados apesar de estes criarem possíveis atrasos na chegada e processamento de dados, ocorrendo um overhead e penalizando o desempenho. No caso dos protocolos UDP, como existe uma probabilidade de que exista informação perdida, este implica que a sua resolução ocorra na camada da aplicação, penalizando o seu empenho.

1.2 Exercício 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.

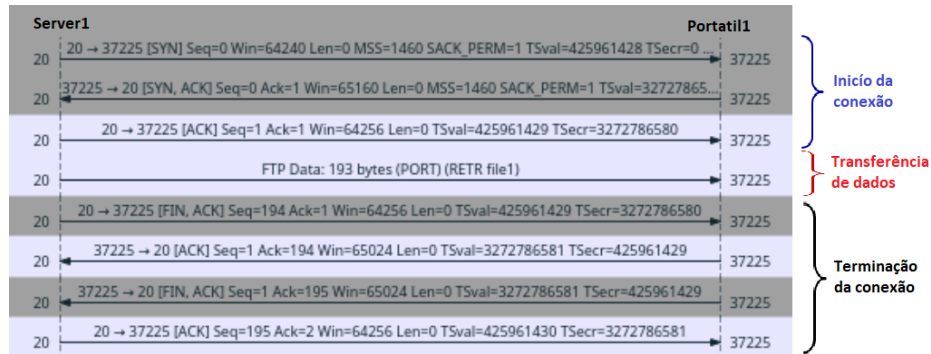


Fig. 1. Diagrama temporal da transferência do file1 por FTP.

57	20.216318424	10.2.2.1	10.1.1.1	TCP	74	20 - 37225 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=425961428 TSecr=0...
58	20.216898943	10.1.1.1	10.2.2.1	TCP	74	37225 - 20 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3272786581 TSecr=425961428...
59	20.216923187	10.2.2.1	10.1.1.1	TCP	66	20 - 37225 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=425961429 TSecr=3272786580...
61	20.216971914	10.2.2.1	10.1.1.1	FTP-DA...	259	FTP Data: 193 bytes (PORT) (RETR file1)
62	20.217385211	10.2.2.1	10.1.1.1	TCP	66	20 - 37225 [FIN, ACK] Seq=194 Ack=1 Win=64256 Len=0 TSval=425961429 TSecr=3272786580...
63	20.217395979	10.1.1.1	10.2.2.1	TCP	66	37225 - 20 [ACK] Seq=1 Ack=194 Win=65024 Len=0 TSval=3272786581 TSecr=425961429...
64	20.218063769	10.1.1.1	10.2.2.1	TCP	66	37225 - 20 [FIN, ACK] Seq=1 Ack=195 Win=65024 Len=0 TSval=3272786581 TSecr=425961429...
65	20.218426345	10.2.2.1	10.1.1.1	TCP	66	20 - 37225 [ACK] Seq=195 Ack=2 Win=64256 Len=0 TSval=425961430 TSecr=3272786581...

Fig. 2. FTP.

1.3 Exercício 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.

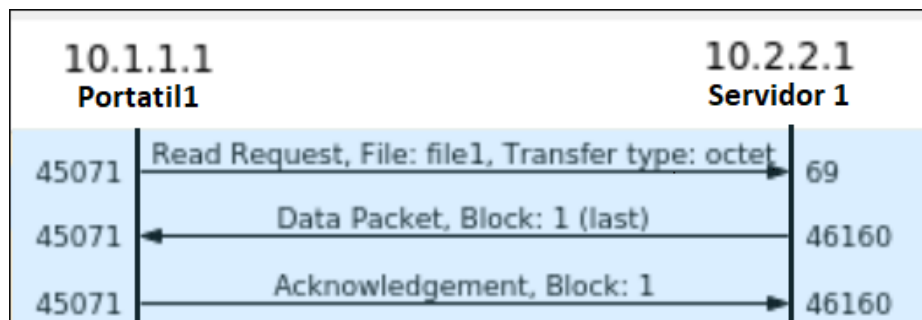


Fig. 3. Diagrama temporal da transferência do file1 por TFTP.

7 3.89689/343	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
8 3.896904224	10.1.1.1	10.2.2.1	TFTP	56 Read Request, File: file1, Transfer type: octet
9 3.906592376	10.2.2.1	10.1.1.1	TFTP	270 Data Packet, Block: 1 (last)
10 3.907732196	10.1.1.1	10.2.2.1	TFTP	40 Acknowledgement, Block: 1
11 3.920000000	10.2.2.1	224.0.0.5	OSPF	72 Hello Packet

Fig. 4. TFTP.

1.4 Exercício 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.

Camada de Transporte: No que diz respeito ao uso da camada de transporte através da análise das quatro aplicações de transferências de ficheiros utilizadas verificamos que SFTP, FTP e HTTP utilizam o protocolo TCP e que TFTP utiliza o protocolo UDP.

Eficiência: Para compararmos os protocolos utilizados em termos de eficiência recorremos ao wireshark para capturar o tráfego de dados tendo sido verificado que :

FTP: Não é um protocolo seguro uma vez que este não utiliza encriptação ficando desta forma os dados utilizados pelos utilizadores vulneráveis e suscetíveis a ataques.

SFTP: Semelhante com FTP porém neste os dados são encriptados sendo a sua conexão mais segura, é o mais eficaz uma vez que se pode transferir vários ficheiros rapidamente.

HTTP: Eficiente na transferência de ficheiros pequenos uma vez que usa o protocolo TCP que é responsável pela verificação de erros.

TFTP: é o mais eficaz de todos os protocolos dado que tem um baixo overhead.

Ordem Crescente de Eficiência: HTTP-FTP-SFTP-TFTP

Complexidade: SFTP: É muito complexo dado que usa o protocolo TCP, protocolo mais complexo da camada de transporte, utilizando mais do que uma conexão e tem de criptografar os dados transferidos.

FTP: É muito complexo dado que utiliza o protocolo TCP, protocolo mais complexo da camada de transporte, e dado que tem permissão para transferir diversos ficheiros em simultâneo cada uma destas transferências cria uma conexão tendo como resultado várias velocidades de conexão.

TFTP: Quando comparado com os outros protocolos é o que apresenta menor complexidade uma vez que este utiliza o protocolo UDP que é um protocolo mais simples.

HTTP: É muito complexo uma vez que utiliza o protocolo TCP, protocolo mais complexo da camada de transporte, mas utiliza apenas uma conexão.

Ordem Crescente de Complexidade: TFTP-HTTP-FTP-SFTP

Segurança: SFTP: É muito seguro uma vez que utiliza o ssh para encriptar os dados de maneira a os dados não serem interceptados por terceiros.

FTP: É pouco seguro dado que não fornece mecanismos de encriptação, podendo qualquer pessoa fazer a captura de pacotes.

TFTP: Não tem nenhuma segurança nem encriptação associada sendo bastante simples e destinado a receber e enviar ficheiros que não comprometam a privacidade do utilizador.

HTTP: É pouco seguro dado que não é encriptado sendo os dados acessíveis a qualquer pessoa.

1.5 Exercício 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.

Para calcular a percentagem de overhead de transporte fizemos $(\text{Header Length} / \text{Total Length}) * 100$.

Aplicação Executada	Protocolo de Aplicação	Protocolo de transporte	Porta de atendimento	Overhead de transporte
Ping	--	--	--	--
Tracerout	--	UDP	33434	33%
Telnet	TELNET	TCP	23	35%
Ftp	FTP	TCP	21	38%
Tftp	TFTP	UDP	69	28%
Wget	HTTP	TCP	80	38%
Nslookup	DNS	UDP	53	29%
Ssh	SSHV2	TCP	22	<u>12%</u>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.11	192.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=1/250, ttl=64 (reply in 2)
2	0.024210372	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=1/250, ttl=60 (request in 1)
3	1.002132063	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 4)
4	1.025144329	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=60 (request in 3)
7	2.004087439	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 8)
8	2.027749839	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=60 (request in 7)
13	3.000335646	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=4/1024, ttl=64 (reply in 14)
19	3.029919778	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1024, ttl=60 (request in 13)
22	4.007946751	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 23)
23	4.031511784	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=60 (request in 22)
24	5.009247841	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=6/1536, ttl=64 (reply in 25)
25	5.032977210	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=6/1536, ttl=60 (request in 24)
26	6.010836853	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=7/1792, ttl=64 (reply in 27)
27	6.035024414	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=7/1792, ttl=60 (request in 26)
28	7.013295504	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=8/2048, ttl=64 (reply in 29)
29	7.037038249	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=8/2048, ttl=60 (request in 28)
30	8.016188258	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=9/2304, ttl=64 (reply in 31)
31	8.039599261	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=9/2304, ttl=60 (request in 30)
36	9.018088489	192.168.1.11	142.250.200.100	ICMP	98	Echo (ping) request id=0x0003, seq=10/2560, ttl=64 (reply in 37)
37	9.041159377	142.250.200.100	192.168.1.11	ICMP	98	Echo (ping) reply id=0x0003, seq=10/2560, ttl=60 (request in 36)

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRTSGro_74:30:23 (2c:a1:7d:74:30:23)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 142.250.200.100
 ▶ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xac9c [correct]
 [Checksum Status: Good]
 Identifier (BE): 3 (0x0003)
 Identifier (LE): 768 (0x0300)
 Sequence number (BE): 1 (0x0001)
 Sequence number (LE): 250 (0x0100)
 [Response frame: 2]
 Timestamp from icmp data: Oct 11, 2022 18:46:04.000000000 WEST
 [Timestamp from icmp data (relative): 0.228716966 seconds]
 ▶ Data (48 bytes)

Fig. 5. PING

No.	Time	Source	Destination	Protocol	Length	Info
9	0.514357750	192.168.1.11	193.137.196.247	UDP	74	44532 → 33434 Len=32
10	0.514403042	192.168.1.11	193.137.196.247	UDP	74	40363 → 33435 Len=32
11	0.514650259	192.168.1.11	193.137.196.247	UDP	74	46085 → 33436 Len=32
12	0.514726054	192.168.1.11	193.137.196.247	UDP	74	47200 → 33437 Len=32
13	0.514813099	192.168.1.11	193.137.196.247	UDP	74	45901 → 33438 Len=32
14	0.515049526	192.168.1.11	193.137.196.247	UDP	74	52730 → 33439 Len=32
15	0.515263052	192.168.1.11	193.137.196.247	UDP	74	57818 → 33440 Len=32
16	0.515379059	192.168.1.11	193.137.196.247	UDP	74	59190 → 33441 Len=32
17	0.515444182	192.168.1.11	193.137.196.247	UDP	74	32779 → 33442 Len=32
18	0.515507034	192.168.1.11	193.137.196.247	UDP	74	33987 → 33443 Len=32
19	0.515582192	192.168.1.11	193.137.196.247	UDP	74	41692 → 33444 Len=32
20	0.515645457	192.168.1.11	193.137.196.247	UDP	74	49997 → 33445 Len=32
21	0.515708153	192.168.1.11	193.137.196.247	UDP	74	34204 → 33446 Len=32
22	0.515779581	192.168.1.11	193.137.196.247	UDP	74	36059 → 33447 Len=32
23	0.515842174	192.168.1.11	193.137.196.247	UDP	74	44049 → 33448 Len=32
24	0.515904476	192.168.1.11	193.137.196.247	UDP	74	47268 → 33449 Len=32

▶ Frame 25: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRTSGro_74:30:23 (2c:a1:7d:74:30:23)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 193.137.196.247
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0xffcd (65485)
 Flags: 0x0000
 Fragment offset: 0
 Time to live: 1
 Protocol: UDP (17)
 Header checksum: 0x71af [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.11
 Destination: 193.137.196.247
 ▶ User Datagram Protocol, Src Port: 44532, Dst Port: 33434
 Source Port: 44532
 Destination Port: 33434
 Length: 40
 Checksum: 0x486e [unverified]
 [Checksum Status: Unverified]
 [Stream index: 4]
 ▶ [Timestamps]
 ▶ Data (32 bytes)

Fig. 6. TRACEROUT

109	96.903651725	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1728039 TS...
110	96.904182561	192.168.1.11	213.136.8.188	TCP	93	Telnet Data ...
111	96.957283597	213.136.8.188	192.168.1.11	TELNET	72	Telnet Data ...
112	96.957304434	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=7 Win=64256 Len=0 TSval=1728093 T...
113	96.958214093	213.136.8.188	192.168.1.11	TCP	66	23 → 33984 [ACK] Seq=7 Ack=28 Win=65280 Len=0 TSval=928171660...
114	97.010698419	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
115	97.010711361	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=995 Win=64128 Len=0 TSval=1728146...
116	103.632303787	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
117	103.632323193	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=1983 Win=64128 Len=0 TSval=173476...
118	113.647718681	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
119	113.647733202	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=2971 Win=64128 Len=0 TSval=174478...
120	113.781637354	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
121	113.781651569	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=3959 Win=64128 Len=0 TSval=174491...
122	114.783075962	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
123	114.783088669	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=4947 Win=64128 Len=0 TSval=174591...
124	115.183829778	213.136.8.188	192.168.1.11	TELNET	1054	Telnet Data ...
125	115.183844041	192.168.1.11	213.136.8.188	TCP	66	33984 → 23 [ACK] Seq=28 Ack=5035 Win=64128 Len=0 TSval=174631...
▶ Frame 118: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface enp0s3, id 0						
▶ Ethernet II, Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro_74:30:23 (2c:a1:7d:74:30:23)						
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 213.136.8.188						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
▶ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)						
Total Length: 79						
Identification: 0x5a25 (23077)						
▶ Flags: 0x4000, Don't fragment						
Fragment offset: 0						
Time to live: 64						
Protocol: TCP (6)						
Header checksum status: Unverified						
Source: 192.168.1.11						
Destination: 213.136.8.188						
▶ Transmission Control Protocol, Src Port: 33984, Dst Port: 23, Seq: 1, Ack: 1, Len: 27						
Source Port: 33984						
Destination Port: 23						
[Stream index: 1]						
[TCP Segment Len: 27]						
Sequence number: 1 (relative sequence number)						
Sequence number (raw): 4126417611						
[Next sequence number: 28 (relative sequence number)]						
Acknowledgment number: 1 (relative ack number)						
Acknowledgment number (raw): 3944946427						
1000 = Header Length: 32 bytes (8)						
▶ Flags: 0x018 (PSH, ACK)						
Window size value: 502						
[Calculated window size: 64256]						
[Window size scaling factor: 128]						
Checksum: 0xa839 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
▶ [SEQ/ACK analysis]						
▶ [Timestamps]						
TCP payload (27 bytes)						

Fig. 7. TELNET

7	0.319570438	192.168.1.11	195.144.107.198	TCP	66	48948	-	21	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2409771082..
8	0.385140663	195.144.107.198	192.168.1.11	FTP	93	Response:	220	Microsoft FTP Service	
9	0.385175154	192.168.1.11	195.144.107.198	TCP	66	48948	-	21	[ACK] Seq=1 Ack=28 Win=64256 Len=0 TSval=240977115..
10	0.385459982	192.168.1.11	195.144.107.198	FTP	77	Request:	USER	demo	
11	0.459981954	195.144.107.198	192.168.1.11	FTP	99	Response:	331	Password required for demo.	
12	0.459997396	192.168.1.11	195.144.107.198	TCP	66	48948	-	21	[ACK] Seq=12 Ack=61 Win=64256 Len=0 TSval=24097712..
13	0.460146453	192.168.1.11	195.144.107.198	FTP	81	Request:	PASS	password	
14	0.535859946	195.144.107.198	192.168.1.11	FTP	87	Response:	230	User logged in.	
15	0.535885510	192.168.1.11	195.144.107.198	TCP	66	48948	-	21	[ACK] Seq=27 Ack=82 Win=64256 Len=0 TSval=24097713..
16	0.536165142	192.168.1.11	195.144.107.198	FTP	72	Request:	SYST		
17	0.611832155	195.144.107.198	192.168.1.11	FTP	82	Response:	215	Windows_NT	
18	0.612024059	192.168.1.11	195.144.107.198	FTP	71	Request:	PWD		
19	0.686697610	195.144.107.198	192.168.1.11	FTP	97	Response:	257	"/" is current directory.	
20	0.686936324	192.168.1.11	195.144.107.198	FTP	74	Request:	TYPE	I	
21	0.761959294	195.144.107.198	192.168.1.11	FTP	86	Response:	200	Type set to I.	
22	0.762251092	192.168.1.11	195.144.107.198	FTP	72	Request:	PASV		
23	0.836946543	195.144.107.198	192.168.1.11	FTP	116	Response:	227	Entering Passive Mode (195,144,107,198,4,5).	

▶ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro_74:30:23 (2c:a1:7d:74:30:23)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 195.144.107.198
 0100 = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x2df0 (11760)
 ▶ Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 Header checksum: 0x1bca [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.11
 Destination: 195.144.107.198
 ▶ Transmission Control Protocol, Src Port: 48948, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
 Source Port: 48948
 Destination Port: 21
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Sequence number (raw): 2814533242
 [Next sequence number: 1 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 Acknowledgment number (raw): 529145598
 1000 = Header Length: 32 bytes (8)
 ▶ Flags: 0x010 (ACK)
 Window size value: 592
 [Calculated window size: 64256]
 [Window size scaling factor: 128]
 Checksum: 0xf130 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 ▶ [SEQ/ACK analysis]
 ▶ [Timestamps]

Fig. 8. FTP

5	0.050128475	192.168.1.11	223.94.106.126	FTP	86	Read Request, File: file1, Transfer type: octet, tsize=0, blk...
19	7.294427091	192.168.1.11	223.94.106.126	FTP	86	Read Request, File: file1, Transfer type: octet, tsize=0, blk...
20	14.300650407	192.168.1.11	223.94.106.126	FTP	86	Read Request, File: file1, Transfer type: octet, tsize=0, blk...
22	24.245626234	192.168.1.11	223.94.106.126	FTP	86	Read Request, File: file1, Transfer type: octet, tsize=0, blk...

▶ Frame 5: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface enp0s3, id 0
 ▶ Ethernet II, Src: PcsCompu_d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro_74:30:23 (2c:a1:7d:74:30:23)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 223.94.106.126
 0100 = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 72
 Identification: 0x70f5 (28917)
 ▶ Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xbe1f [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.11
 Destination: 223.94.106.126
 ▶ User Datagram Protocol, Src Port: 60063, Dst Port: 69
 Source Port: 60063
 Destination Port: 69
 Length: 52
 Checksum: 0x0bd6 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 2]
 ▶ [Timestamps]
 ▶ Trivial File Transfer Protocol

Fig. 9. TFTP

No.	Time	Source	Destination	Protocol	Length	Info
5	1.426779623	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=486041585
6	1.427108316	192.168.1.11	90.130.70.73	HTTP	219	GET /1MB.zip HTTP/1.1
7	1.474887961	90.130.70.73	192.168.1.11	TCP	66	80 → 60890 [ACK] Seq=1 Ack=154 Win=45056 Len=0 TSval=20851807
8	1.476609917	90.130.70.73	192.168.1.11	TCP	1514	80 → 60890 [ACK] Seq=1 Ack=154 Win=45056 Len=1448 TSval=20851
9	1.476617056	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=1449 Win=64128 Len=0 TSval=48604
10	1.477434757	90.130.70.73	192.168.1.11	TCP	13098	80 → 60890 [ACK] Seq=1449 Ack=154 Win=45056 Len=13032 TSval=2
11	1.477447395	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=14481 Win=56832 Len=0 TSval=4860
12	1.522105551	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=14481 Ack=154 Win=45056 Len=2896 TSval=2
13	1.522122399	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=17377 Win=63488 Len=0 TSval=4860
14	1.523564772	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=17377 Ack=154 Win=45056 Len=2896 TSval=2
15	1.523571034	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=20273 Win=69888 Len=0 TSval=4860
16	1.526693708	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=20273 Ack=154 Win=45056 Len=2896 TSval=2
17	1.526709645	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=23169 Win=75776 Len=0 TSval=4860
18	1.530907815	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=23169 Ack=154 Win=45056 Len=2896 TSval=2
19	1.530104294	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=26065 Win=81536 Len=0 TSval=4860
20	1.542309638	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=26065 Ack=154 Win=45056 Len=2896 TSval=2
21	1.542329439	192.168.1.11	90.130.70.73	TCP	66	60890 → 80 [ACK] Seq=154 Ack=28961 Win=81536 Len=0 TSval=4860
22	1.549210469	90.130.70.73	192.168.1.11	TCP	2962	80 → 60890 [ACK] Seq=28961 Ack=154 Win=45056 Len=2896 TSval=2
▶ Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0 ▶ Ethernet II, Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro_74:30:23 (2c:a1:7d:74:30:23) ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 90.130.70.73 0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 52 Identification: 0x78e2 (30946) ▶ Flags: 0x4000, Don't fragment Fragment offset: 0 Time to live: 64 Protocol: TCP (6) Header checksum: 0x5f63 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.11 Destination: 90.130.70.73 ▶ Transmission Control Protocol, Src Port: 60890, Dst Port: 80, Seq: 154, Ack: 1449, Len: 0 Source Port: 60890 Destination Port: 80 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 154 (relative sequence number) Sequence number (raw): 109070462 [Next sequence number: 154 (relative sequence number)] Acknowledgment number: 1449 (relative ack number) Acknowledgment number (raw): 2503698338 1000 = Header Length: 32 bytes (8) ▶ Flags: 0x010 (ACK) Window size value: 501 [Calculated window size: 64128] [Window size scaling factor: 128] Checksum: 0x62a5 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps ▶ [SEQ/ACK analysis] ▶ [Timestamps]						

Fig. 10. WGET

7	8.207421797	192.168.1.11	62.169.70.160	DNS	84	Standard query 0xaaee AAAA www.uminho.pt OPT
8	8.229510699	62.169.70.160	192.168.1.11	DNS	138	Standard query response 0xaaee AAAA www.uminho.pt SOA dns.umi
▶ Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface enp0s3, id 0 ▶ Ethernet II, Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro_74:30:23 (2c:a1:7d:74:30:23) ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 62.169.70.160 0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 76 Identification: 0xe191 (57745) ▶ Flags: 0x4000, Don't fragment Fragment offset: 0 Time to live: 64 Protocol: UDP (17) Header checksum: 0x1219 [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.11 Destination: 62.169.70.160 ▶ User Datagram Protocol, Src Port: 34279, Dst Port: 53 Source Port: 34279 Destination Port: 53 Length: 50 Checksum: 0x4740 [unverified] [Checksum Status: Unverified] [Stream index: 0] ▶ [Timestamps] ▶ Domain Name System (query)						

Fig. 11. NSLOOKUP

44	11.005765274	192.168.1.11	193.136.19.165	SSHv2	150 Client: Encrypted packet (len=84)
45	11.024737451	193.136.19.165	192.168.1.11	SSHv2	110 Server: Encrypted packet (len=44)
46	11.024753313	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=1906 Ack=2066 Win=64128 Len=0 TSval=1412..
47	11.024944900	192.168.1.11	193.136.19.165	SSHv2	150 Client: Encrypted packet (len=84)
48	11.041097336	193.136.19.165	192.168.1.11	SSHv2	94 Server: Encrypted packet (len=28)
49	11.041093256	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=1990 Ack=2094 Win=64128 Len=0 TSval=1412..
50	11.041347399	192.168.1.11	193.136.19.165	SSHv2	178 Client: Encrypted packet (len=112)
51	11.095891577	193.136.19.165	192.168.1.11	TCP	66 22 → 55588 [ACK] Seq=2094 Ack=2102 Win=32000 Len=0 TSval=1984..
52	11.273566360	193.136.19.165	192.168.1.11	SSHv2	638 Server: Encrypted packet (len=572)
53	11.273628808	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=2102 Ack=2666 Win=64128 Len=0 TSval=1412..
54	11.288229864	193.136.19.165	192.168.1.11	SSHv2	110 Server: Encrypted packet (len=44)
55	11.288241327	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=2102 Ack=2710 Win=64128 Len=0 TSval=1412..
56	11.288478802	192.168.1.11	193.136.19.165	SSHv2	1230 Client: Encrypted packet (len=1164)
57	11.304331219	193.136.19.165	192.168.1.11	TCP	66 22 → 55588 [ACK] Seq=2710 Ack=3266 Win=34944 Len=0 TSval=1984..
58	11.315806750	193.136.19.165	192.168.1.11	SSHv2	174 Server: Encrypted packet (len=108)
59	11.318042595	193.136.19.165	192.168.1.11	SSHv2	2182 Server: Encrypted packet (len=2116)
60	11.318159206	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=3266 Ack=4934 Win=64128 Len=0 TSval=1412..
61	11.633289600	193.136.19.165	192.168.1.11	SSHv2	158 Server: Encrypted packet (len=92)
62	11.676123045	192.168.1.11	193.136.19.165	TCP	66 55588 → 22 [ACK] Seq=3266 Ack=5026 Win=64128 Len=0 TSval=1412..

▶	Frame 50: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface enp0s3, id 0
▶	Ethernet II, Src: PcsCompu d1:8b:d0 (08:00:27:d1:8b:d0), Dst: ARRISGro 74:30:23 (2c:a1:7d:74:30:23)
▶	Internet Protocol Version 4, Src: 192.168.1.11, Dst: 193.136.19.165
▶	0100 ... = Version: 4
▶ 0101 = Header Length: 20 bytes (5)
▶	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
▶	Total Length: 164
▶	Identification: 0x67de (26590)
▶	Flags: 0x4000, Don't fragment
▶	Fragment offset: 0
▶	Time to live: 64
▶	Protocol: TCP (6)
▶	Header checksum: 0x3b95 [validation disabled]
▶	[Header checksum status: Unverified]
▶	Source: 192.168.1.11
▶	Destination: 193.136.19.165
▼	Transmission Control Protocol, Src Port: 55588, Dst Port: 22, Seq: 1990, Ack: 2094, Len: 112
▶	Source Port: 55588
▶	Destination Port: 22
▶	[Stream index: 0]
▶	[TCP Segment Len: 112]
▶	Sequence number: 1990 (relative sequence number)
▶	Sequence number (raw): 971721555
▶	[Next sequence number: 2102 (relative sequence number)]
▶	Acknowledgment number: 2094 (relative ack number)
▶	Acknowledgment number (raw): 2075259002
▶	1000 ... = Header Length: 32 bytes (8)
▶	Window size value: 501
▶	[Calculated window size: 64128]
▶	[Window size scaling factor: 128]
▶	Checksum: 0x9777 [unverified]
▶	[Checksum Status: Unverified]
▶	Urgent pointer: 0
▶	Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
▶	[SEQ/ACK analysis]

Fig. 12. SSH

2 Conclusão

A realização deste trabalho prático permitiu-nos consolidar alguns dos conhecimentos abordados nas aulas teóricas relativos à camada de transporte e aos seus protocolos.

Foi ainda possível identificar as diferenças entre os protocolos TCP e UDP e o seu impacto e analisar outros protocolos tais como TFTP, HTTP, SFTP e FTP.

Em conclusão, acreditamos ter obtido o aproveitamento esperado na realização deste trabalho e também conhecimentos importantes relativos ao tema do mesmo.