



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

Comunicações por Computador Grupo 5

Trabalho Prático No.1 – Protocolos da Camada de Transporte

Hugo Cunha (84656) Maria Pires(86268)
Susana Marques (84167)

3 de Março de 2020

Conteúdo

| | | |
|---|------------|---|
| 1 | Questão 1 | 2 |
| 2 | Questão 2 | 4 |
| 3 | Questão 3 | 6 |
| 4 | Questão 4 | 6 |
| 5 | Conclusões | 8 |

1 Questão 1

| Comando usado | Protocolo de Aplicação (se aplicável) | Protocolo de transporte (se aplicável) | Porta de atendimento (se aplicável) | Overhead de transporte em bytes (se aplicável) |
|---------------------|---------------------------------------|--|-------------------------------------|--|
| Ping | Não Aplicável | Não Aplicável | Não Aplicável | Não Aplicável |
| Traceroute | Traceroute | UDP | 33443* | 8 |
| Telnet | Telnet | TCP | 23 | 20 |
| FTP | FTP | TCP | 21 | 20 |
| TFTP | TFTP | UDP | 69 | 8 |
| Browser/HTTP | HTTP | TCP | 80 | 20 |
| NSLookup | DNS | UDP | 53 | 8 |
| SSH | SSH | TCP | 22 | 20 |

* é apenas um exemplo, visto que existe um conjunto de portas

Figura 1: Tabela em que identifica os protocolos usados para cada comando executado

| | | | | | | |
|---|------------|----------|----------|------|------------------------|-------------------------------|
| 51 | 228.328272 | 10.1.1.1 | 10.3.3.1 | ICMP | 98 Echo (ping) request | id=0x004d, seq=1/256, ttl=61 |
| 52 | 228.328547 | 10.3.3.1 | 10.1.1.1 | ICMP | 98 Echo (ping) reply | id=0x004d, seq=1/256, ttl=64 |
| 53 | 229.336842 | 10.1.1.1 | 10.3.3.1 | ICMP | 98 Echo (ping) request | id=0x004d, seq=2/512, ttl=61 |
| 54 | 229.337245 | 10.3.3.1 | 10.1.1.1 | ICMP | 98 Echo (ping) reply | id=0x004d, seq=2/512, ttl=64 |
| 55 | 230.337455 | 10.1.1.1 | 10.3.3.1 | ICMP | 98 Echo (ping) request | id=0x004d, seq=3/768, ttl=61 |
| 56 | 230.351321 | 10.3.3.1 | 10.1.1.1 | ICMP | 98 Echo (ping) reply | id=0x004d, seq=3/768, ttl=64 |
| 57 | 231.348488 | 10.1.1.1 | 10.3.3.1 | ICMP | 98 Echo (ping) request | id=0x004d, seq=4/1024, ttl=61 |
| 58 | 231.348809 | 10.3.3.1 | 10.1.1.1 | ICMP | 98 Echo (ping) reply | id=0x004d, seq=4/1024, ttl=64 |
| 59 | 232.345205 | 10.1.1.1 | 10.3.3.1 | ICMP | 98 Echo (ping) request | id=0x004d, seq=5/1280, ttl=61 |
| ▶ Frame 59: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) | | | | | | |
| ▶ Ethernet II, Src: 00:00:00_aa:00:10 (00:00:00:aa:00:10), Dst: 00:00:00_aa:00:14 (00:00:00:aa:00:14) | | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 10.3.3.1 (10.3.3.1) | | | | | | |
| ▼ Internet Control Message Protocol | | | | | | |
| Type: 8 (Echo (ping) request) | | | | | | |
| Code: 0 | | | | | | |
| Checksum: 0x25b0 [correct] | | | | | | |
| Identifier (BE): 77 (0x004d) | | | | | | |
| Identifier (LE): 19712 (0x4d00) | | | | | | |
| Sequence number (BE): 5 (0x0005) | | | | | | |
| Sequence number (LE): 1280 (0x0500) | | | | | | |
| [Response In: 60] | | | | | | |
| ▶ Data (56 bytes) | | | | | | |

Figura 2: Ping

| | | | | | | |
|--|-----------|----------|----------|-----|-----------------------|-------------------------|
| 11 | 36.833210 | 10.1.1.1 | 10.3.3.1 | UDP | 74 Source port: 42177 | Destination port: 33443 |
| 12 | 36.833461 | 10.1.1.1 | 10.3.3.1 | UDP | 74 Source port: 41232 | Destination port: 33444 |
| 13 | 36.833537 | 10.1.1.1 | 10.3.3.1 | UDP | 74 Source port: 54458 | Destination port: 33445 |
| ▶ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) | | | | | | |
| ▶ Ethernet II, Src: 00:00:00_aa:00:10 (00:00:00:aa:00:10), Dst: 00:00:00_aa:00:14 (00:00:00:aa:00:14) | | | | | | |
| ▼ Internet Protocol Version 4, Src: 10.1.1.1 (10.1.1.1), Dst: 10.3.3.1 (10.3.3.1) | | | | | | |
| Version: 4 | | | | | | |
| Header length: 20 bytes | | | | | | |
| ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport)) | | | | | | |
| Total Length: 60 | | | | | | |
| Identification: 0xbc85 (48261) | | | | | | |
| ▶ Flags: 0x00 | | | | | | |
| Fragment offset: 0 | | | | | | |
| ▶ Time to live: 1 | | | | | | |
| Protocol: UDP (17) | | | | | | |
| ▶ Header checksum: 0xe526 [correct] | | | | | | |
| Source: 10.1.1.1 (10.1.1.1) | | | | | | |
| Destination: 10.3.3.1 (10.3.3.1) | | | | | | |
| ▼ User Datagram Protocol, Src Port: 42177 (42177), Dst Port: 33443 (33443) | | | | | | |
| Source port: 42177 (42177) | | | | | | |
| ▶ Destination port: 33443 (33443) | | | | | | |
| Length: 40 | | | | | | |
| ▶ Checksum: 0x183f [validation disabled] | | | | | | |

Figura 3: Traceroute

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|-----------|-------------------|-------------------|----------|--------|--|
| 11 | 0.116174 | 193.136.9.183 | 10.0.2.15 | TCP | 60 | telnet > 54767 [ACK] Seq=1 Ack=28 Win=65535 Len=0 |
| 12 | 5.013849 | CadmusCo_78:e5:64 | RealtekU_12:35:03 | ARP | 42 | Who has 10.0.2.3? Tell 10.0.2.15 |
| 13 | 5.014166 | RealtekU_12:35:03 | CadmusCo_78:e5:64 | ARP | 60 | 10.0.2.3 is at 52:54:00:12:35:03 |
| 14 | 15.299406 | 193.136.9.183 | 10.0.2.15 | TELNET | 66 | Telnet Data ... |
| 15 | 15.299415 | 10.0.2.15 | 193.136.9.183 | TCP | 54 | 54767 → telnet [ACK] Seq=28 Ack=13 Win=14600 Len=0 |
| 16 | 15.305803 | 193.136.9.183 | 10.0.2.15 | TELNET | 93 | Telnet Data ... |
| ▶ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) | | | | | | |
| ▶ Ethernet II, Src: CadmusCo_78:e5:64 (08:00:27:78:e5:64), Dst: RealtekU_12:35:02 (52:54:00:12:35:02) | | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.183 (193.136.9.183) | | | | | | |
| ▼ Transmission Control Protocol, Src Port: 54767 (54767), Dst Port: telnet (23), Seq: 28, Ack: 13, Len: 0 | | | | | | |
| Source port: 54767 (54767) | | | | | | |
| Destination port: telnet (23) | | | | | | |
| [Stream index: 3] | | | | | | |
| Sequence number: 28 (relative sequence number) | | | | | | |
| Acknowledgement number: 13 (relative ack number) | | | | | | |
| Header length: 20 bytes | | | | | | |
| ▶ Flags: 0x010 (ACK) | | | | | | |
| Window size value: 14600 | | | | | | |
| [Calculated window size: 14600] | | | | | | |
| [Window size scaling factor: -2 (no window scaling used)] | | | | | | |
| 0000 52 54 00 12 35 02 08 00 27 78 e5 64 08 00 45 10 RT..S... 'x.d..E. | | | | | | |
| 0010 00 28 10 ce 40 00 40 06 52 a4 0a 00 02 0f c1 88 .(.@.@. R..... | | | | | | |
| 0020 09 b7 d5 ef 00 17 51 a2 a1 a2 05 51 54 0e 50 10Q. ...QT..P. | | | | | | |
| 0030 39 08 d7 68 00 00 9..h.. | | | | | | |

Figura 4: Telnet

| | | | | | | |
|---|----------|---------------|---------------|-----|----|---|
| 14 | 4.979596 | 10.0.2.15 | 193.136.9.183 | FTP | 63 | Request: USER cc |
| 15 | 4.980243 | 193.136.9.183 | 10.0.2.15 | TCP | 60 | ftp > 43395 [ACK] Seq=21 Ack=10 Win=65535 Len=0 |
| 16 | 4.991277 | 193.136.9.183 | 10.0.2.15 | FTP | 88 | Response: 331 Please specify the password. |
| 17 | 4.991462 | 10.0.2.15 | 193.136.9.183 | TCP | 54 | 43395 > ftp [ACK] Seq=10 Ack=55 Win=14600 Len=0 |
| 18 | 8.709844 | 10.0.2.15 | 193.136.9.183 | FTP | 67 | Request: PASS cc2020 |
| ▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.183 (193.136.9.183) | | | | | | |
| ▼ Transmission Control Protocol, Src Port: 43395 (43395), Dst Port: ftp (21), Seq: 1, Ack: 21, Len: 9 | | | | | | |
| Source port: 43395 (43395) | | | | | | |
| Destination port: ftp (21) | | | | | | |
| [Stream index: 2] | | | | | | |
| Sequence number: 1 (relative sequence number) | | | | | | |
| [Next sequence number: 10 (relative sequence number)] | | | | | | |
| Acknowledgement number: 21 (relative ack number) | | | | | | |
| Header length: 20 bytes | | | | | | |
| ▶ Flags: 0x018 (PSH, ACK) | | | | | | |
| Window size value: 14600 | | | | | | |
| [Calculated window size: 14600] | | | | | | |
| [Window size scaling factor: -2 (no window scaling used)] | | | | | | |
| ▶ Checksum: 0xd771 [validation disabled] | | | | | | |

Figura 5: FTP

| | | | | | | |
|---|----------|-----------|---------------|------|-----|---|
| 2 | 0.099696 | 10.0.2.3 | 10.0.2.15 | DNS | 75 | Standard query response |
| 3 | 0.100004 | 10.0.2.15 | 10.0.2.3 | DNS | 93 | Standard query AAAA cc2020.ddns.net.eduroam.uminho.pt |
| 4 | 0.106125 | 10.0.2.3 | 10.0.2.15 | DNS | 93 | Standard query response, No such name |
| 5 | 0.106421 | 10.0.2.15 | 10.0.2.3 | DNS | 75 | Standard query A cc2020.ddns.net |
| 6 | 0.155314 | 10.0.2.3 | 10.0.2.15 | DNS | 91 | Standard query response A 193.136.9.183 |
| 7 | 0.155984 | 10.0.2.15 | 193.136.9.183 | TFTP | 86 | Read Request, File: file1, Transfer type: octet, tsize=00 |
| 8 | 0.161840 | 10.0.2.2 | 10.0.2.15 | UDP | 76 | Source port: 54865 Destination port: 47161 |
| 9 | 0.162043 | 10.0.2.15 | 10.0.2.2 | UDP | 46 | Source port: 47161 Destination port: 54865 |
| 10 | 0.165984 | 10.0.2.2 | 10.0.2.15 | UDP | 239 | Source port: 54865 Destination port: 47161 |
| 11 | 0.166878 | 10.0.2.15 | 10.0.2.2 | UDP | 46 | Source port: 47161 Destination port: 54865 |
| ▶ Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) | | | | | | |
| ▶ Ethernet II, Src: CadmusCo_78:e5:64 (08:00:27:78:e5:64), Dst: RealtekU_12:35:02 (52:54:00:12:35:02) | | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.183 (193.136.9.183) | | | | | | |
| ▼ User Datagram Protocol, Src Port: 47161 (47161), Dst Port: tftp (69) | | | | | | |
| Source port: 47161 (47161) | | | | | | |
| Destination port: tftp (69) | | | | | | |
| Length: 52 | | | | | | |
| ▶ Checksum: 0xd793 [validation disabled] | | | | | | |

Figura 6: TFTP

| | | | | | |
|---|-----------|---------------|---------------|---------|---|
| 1 | 0.000000 | 10.0.2.15 | 34.73.232.153 | TCP | 54 43779 > https [ACK] Seq=1 Ack=1 Win=31240 Len=0 |
| 2 | 0.000433 | 34.73.232.153 | 10.0.2.15 | TCP | 60 [TCP ACKed lost segment] https > 43779 [ACK] Seq=1 Ack=2 Win=65535 Len=0 |
| 3 | 6.523486 | 34.73.232.153 | 10.0.2.15 | TLSv1.2 | 88 Application Data |
| 4 | 6.524039 | 10.0.2.15 | 34.73.232.153 | TLSv1.2 | 92 Application Data |
| 5 | 6.524408 | 34.73.232.153 | 10.0.2.15 | TCP | 60 https > 43647 [ACK] Seq=35 Ack=39 Win=65535 Len=0 |
| 6 | 10.016337 | 10.0.2.15 | 34.73.232.153 | TCP | 54 [TCP Keep-Alive] 43779 > https [ACK] Seq=1 Ack=1 Win=31240 Len=0 |
| 7 | 10.016756 | 34.73.232.153 | 10.0.2.15 | TCP | 60 [TCP Keep-Alive ACK] https > 43779 [ACK] Seq=1 Ack=2 Win=65535 Len=0 |
| 8 | 20.031289 | 10.0.2.15 | 34.73.232.153 | TCP | 54 [TCP Keep-Alive] 43779 > https [ACK] Seq=1 Ack=1 Win=31240 Len=0 |
| 9 | 20.032250 | 34.73.232.153 | 10.0.2.15 | TCP | 60 [TCP Keep-Alive ACK] https > 43779 [ACK] Seq=1 Ack=2 Win=65535 Len=0 |

| | | | | | |
|---|--|--|--|--|--|
| ▶ Source: CadmusCo_78:e5:64 (08:00:27:78:e5:64) | | | | | |
| Type: IP (0x0800) | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 34.73.232.153 (34.73.232.153) | | | | | |
| ▼ Transmission Control Protocol, Src Port: 43779 (43779), Dst Port: https (443), Seq: 1, Ack: 1, Len: 0 | | | | | |
| Source port: 43779 (43779) | | | | | |
| Destination port: https (443) | | | | | |
| [Stream index: 0] | | | | | |
| Sequence number: 1 (relative sequence number) | | | | | |
| Acknowledgement number: 1 (relative ack number) | | | | | |
| Header length: 20 bytes | | | | | |
| ▶ Flags: 0x010 (ACK) | | | | | |
| Window size value: 31240 | | | | | |
| [Calculated window size: 31240] | | | | | |
| [Window size scaling factor: -1 (unknown)] | | | | | |
| ▶ Checksum: 0x170c [validation disabled] | | | | | |
| ▶ [SEQ/ACK analysis] | | | | | |

Figura 7: HTTP

| | | | | | |
|----|----------|-----------|---------------|------|---|
| 2 | 0.099696 | 10.0.2.3 | 10.0.2.15 | DNS | 75 Standard query response |
| 3 | 0.100004 | 10.0.2.15 | 10.0.2.3 | DNS | 93 Standard query AAAA cc2020.ddns.net.eduroam.uminho.pt |
| 4 | 0.106125 | 10.0.2.3 | 10.0.2.15 | DNS | 93 Standard query response, No such name |
| 5 | 0.106421 | 10.0.2.15 | 10.0.2.3 | DNS | 75 Standard query A cc2020.ddns.net |
| 6 | 0.155314 | 10.0.2.3 | 10.0.2.15 | DNS | 91 Standard query response A 193.136.9.183 |
| 7 | 0.155984 | 10.0.2.15 | 193.136.9.183 | TFTP | 86 Read Request, File: file1, Transfer type: octet, tsize00 |
| 8 | 0.161840 | 10.0.2.2 | 10.0.2.15 | UDP | 76 Source port: 54865 Destination port: 47161 |
| 9 | 0.162043 | 10.0.2.15 | 10.0.2.2 | UDP | 46 Source port: 47161 Destination port: 54865 |
| 10 | 0.165984 | 10.0.2.2 | 10.0.2.15 | UDP | 239 Source port: 54865 Destination port: 47161 |
| 11 | 0.166878 | 10.0.2.15 | 10.0.2.2 | UDP | 46 Source port: 47161 Destination port: 54865 |

| | | | | | |
|---|--|--|--|--|--|
| ▶ Frame 8: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) | | | | | |
| ▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_78:e5:64 (08:00:27:78:e5:64) | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.2.2 (10.0.2.2), Dst: 10.0.2.15 (10.0.2.15) | | | | | |
| ▼ User Datagram Protocol, Src Port: 54865 (54865), Dst Port: 47161 (47161) | | | | | |
| Source port: 54865 (54865) | | | | | |
| Destination port: 47161 (47161) | | | | | |
| Length: 42 | | | | | |
| ▶ Checksum: 0xb2ff [validation disabled] | | | | | |
| ▶ Data (34 bytes) | | | | | |

Figura 8: NSLookup

| | | | | | |
|-----|------------|-------------------|-------------------|-----|--|
| 109 | 187.438291 | 10.0.2.15 | 193.136.9.183 | TCP | 198 [TCP segment of a reassembled PDU] |
| 110 | 187.439054 | 193.136.9.183 | 10.0.2.15 | TCP | 60 ssh > 53472 [ACK] Seq=1450 Ack=1667 Win=65535 Len=0 |
| 111 | 189.633605 | 193.136.9.183 | 10.0.2.15 | TCP | 118 [TCP segment of a reassembled PDU] |
| 112 | 189.633647 | 10.0.2.15 | 193.136.9.183 | TCP | 54 53472 > ssh [ACK] Seq=1667 Ack=1514 Win=17712 Len=0 |
| 113 | 192.444434 | CadmusCo_78:e5:64 | RealtekU_12:35:02 | ARP | 42 Who has 10.0.2.2? Tell 10.0.2.15 |
| 114 | 192.444733 | RealtekU_12:35:02 | CadmusCo_78:e5:64 | ARP | 60 10.0.2.2 is at 52:54:00:12:35:02 |
| 115 | 196.138077 | 10.0.2.15 | 193.136.9.183 | TCP | 198 [TCP segment of a reassembled PDU] |
| 116 | 196.138727 | 193.136.9.183 | 10.0.2.15 | TCP | 60 ssh > 53472 [ACK] Seq=1514 Ack=1811 Win=65535 Len=0 |
| 117 | 198.511121 | 193.136.9.183 | 10.0.2.15 | TCP | 118 [TCP segment of a reassembled PDU] |
| 118 | 198.511175 | 10.0.2.15 | 193.136.9.183 | TCP | 54 53472 > ssh [ACK] Seq=1811 Ack=1578 Win=17712 Len=0 |

| | | | | | |
|--|--|--|--|--|--|
| ▶ Frame 118: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) | | | | | |
| ▶ Ethernet II, Src: CadmusCo_78:e5:64 (08:00:27:78:e5:64), Dst: RealtekU_12:35:02 (52:54:00:12:35:02) | | | | | |
| ▶ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.183 (193.136.9.183) | | | | | |
| ▼ Transmission Control Protocol, Src Port: 53472 (53472), Dst Port: ssh (22), Seq: 1811, Ack: 1578, Len: 0 | | | | | |
| Source port: 53472 (53472) | | | | | |
| Destination port: ssh (22) | | | | | |
| [Stream index: 11] | | | | | |
| Sequence number: 1811 (relative sequence number) | | | | | |
| Acknowledgement number: 1578 (relative ack number) | | | | | |
| Header length: 20 bytes | | | | | |

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0000 | 52 54 00 12 35 02 08 00 | 27 78 e5 64 08 00 45 00 | RT..5... 'x.d..E. |
| 0010 | 00 28 cb 0b 40 00 40 06 | 98 76 0a 00 02 0f c1 88 | .(..@.@. .V..... |
| 0020 | 09 b7 d0 e0 00 16 c0 65 | 4a 7d 08 f1 16 2b 50 10 |e J}...+P. |
| 0030 | 45 30 d7 68 00 00 | | E0.h.. |

Figura 9: SSH

2 Questão 2

Uma representação num diagrama temporal das transferências da file1 por FTP e TFTP respetivamente. Se for caso disso, identifique as fases de estabelecimento de conexão, transferência de dados e fim de conexão. Identifica também claramente os

tipos de segmentos trocados e os números de sequência usados quer nos dados como nas confirmações.

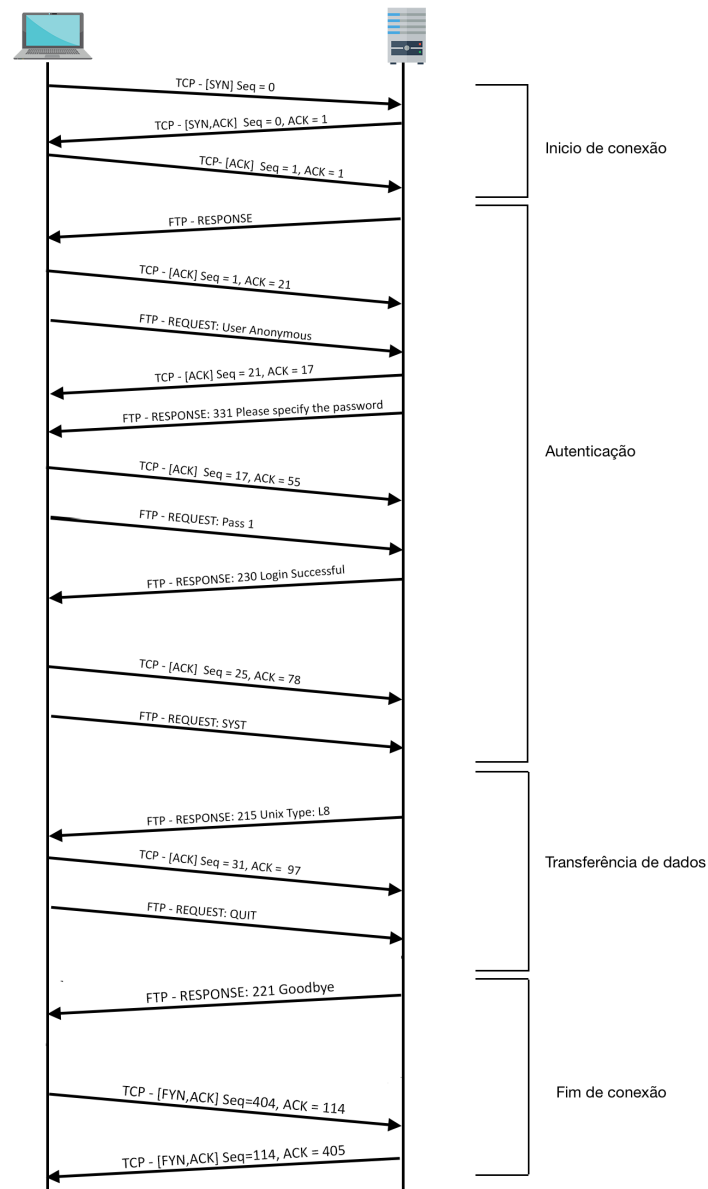


Figura 10: Diagrama de transferência do ficheiro por FTP

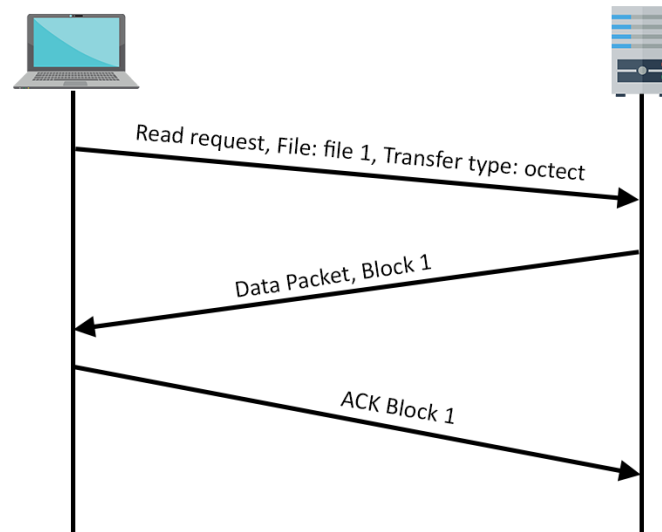


Figura 11: Diagrama de transferência do ficheiro por TFTP

3 Questão 3

Com base nas experiências realizadas, distinga e compare sucintamente as quatro aplicações de transferência de ficheiros que usou nos seguintes pontos (i) uso da camada de transporte; (ii) eficiência na transferência; (iii) complexidade; (iv) segurança;

Pelo que podemos observar através da análise dos pacotes no Wireshark do router 1, os protocolos que utilizam o protocolo TCP como protocolo da camada de transporte são o HTTP, FTP e SFTP. No caso do HTTP, embora implemente vários esquemas de autenticação, é inseguro pois qualquer pessoa na rede consegue ver o conteúdo dos ficheiros antes de chegar ao receptor.

O FTP é um serviço básico de transferência fiável de ficheiros, pois utiliza o protocolo TCP, contudo não aparenta implementar nenhuma segurança adicional (até podemos verificar que no processo de autenticação, que este permite, as palavras-chave são transmitidas na rede em texto claro), sendo por isso bastante simples apesar de permitir uma grande variedade de opções e comandos. Este protocolo tem alguns problemas em termos de eficiência devido ao elevado valor do overhead. O SFTP é um protocolo muito seguro que, tal como o FTP, requer autenticação cliente-servidor. Comparativamente com FTP, o SFTP é mais seguro uma vez que usa ligações SSH. O uso destas ligações causa um overhead que diminui a eficiência da transmissão. O TFTP é um serviço de transferência não fiável devido ao uso do protocolo UDP. Este protocolo é bastante simples, não implementa qualquer segurança adicional e não tem qualquer mecanismo de autenticação, contudo é mais eficiente na transmissão uma vez que o seu overhead é menor que o dos restantes devido a usar UDP e não TCP.

4 Questão 4

As características das ligações de rede têm uma enorme influência nos níveis de Transporte e de Aplicação. Discuta, relacionando a resposta com as experiências realizadas, as influências das situações de perda ou duplicação de pacotes IP no desempenho global de Aplicações fiáveis (se possível, relacionando com alguns dos mecanismos de transporte envolvidos).

É enorme a influência das características das ligações de rede nos níveis de Transporte e de Aplicação uma vez que existem protocolos nestes níveis compostos por processos bastantes complexos que exigem a troca de muitos pacotes entre ambas as partes da aplicação. Por exemplo, para um protocolo de transporte fiável, como o TCP, que garante que todos os pacotes são enviados na ordem correta e sem erros, para cada pacote recebido é sempre enviado pelo menos um Acknowledgment(ACK) que sinaliza a recepção do pacote com sucesso. Quando estamos numa rede de menor qualidade como é o caso do sistema Alfa que tem conectividade ao Backbone através de um link entre o switch SwitchLan2 e o router Router4 com 5% de probabilidade de perda e 10% de probabilidade de duplicação, são perdidos e corrompidos diversos pacotes o que obriga a que sejam transmitidas mensagens de erro e a que sejam reenviados os vários pacotes causando mais sobrecarga na rede e atrasos (quanto maior a percentagem de perda e de duplicações mais reenvios serão feitos como se conseguiu verificar pelos teste feitos com ajustes nesses parâmetros).

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|---|
| 5 | 18.907730 | 00:00:00:aa:00:10 | Broadcast | ARP | 42 | Who has 10.3.3.1? Tell 10.3.3.254 |
| 6 | 18.907790 | 00:00:00:aa:00:14 | 00:00:00:aa:00:10 | ARP | 42 | 10.3.3.1 is at 00:00:00:aa:00:14 |
| 7 | 18.908177 | 10.2.2.1 | 10.3.3.1 | TCP | 74 | 57526 > ftp [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=104840 TSecr=0 WS=16 |
| 8 | 18.908202 | 10.3.3.1 | 10.2.2.1 | TCP | 74 | ftp > 57526 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=104843 TSecr=104843 WS=16 |
| 9 | 18.913571 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=104843 TSecr=104843 |
| 10 | 18.918960 | 10.3.3.1 | 10.2.2.1 | FTP | 86 | Response: 220 (vsFTPd 2.3.5) |
| 11 | 18.924283 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=1 Ack=21 Win=14608 Len=0 TSval=104846 TSecr=104846 |
| 14 | 24.774742 | 10.2.2.1 | 10.3.3.1 | FTP | 82 | Request: USER anonymous |
| 15 | 24.774765 | 10.3.3.1 | 10.2.2.1 | TCP | 66 | ftp > 57526 [ACK] Seq=21 Ack=17 Win=14480 Len=0 TSval=106309 TSecr=106308 |
| 16 | 24.774851 | 10.3.3.1 | 10.2.2.1 | FTP | 100 | Response: 331 Please specify the password. |
| 17 | 24.781646 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=17 Ack=55 Win=14608 Len=0 TSval=106310 TSecr=106309 |
| 18 | 24.781683 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | [TCP Dup ACK 17#1] 57526 > ftp [ACK] Seq=17 Ack=55 Win=14608 Len=0 TSval=106310 TSecr=106309 |
| 19 | 25.344151 | 10.2.2.1 | 10.3.3.1 | FTP | 74 | Request: PASS s |
| 20 | 25.350946 | 10.3.3.1 | 10.2.2.1 | FTP | 89 | Response: 230 Login successful. |
| 21 | 25.356563 | 10.2.2.1 | 10.3.3.1 | FTP | 72 | Request: SYST |
| 22 | 25.356682 | 10.3.3.1 | 10.2.2.1 | FTP | 85 | Response: 215 UNIX Type: L8 |
| 23 | 25.401133 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=31 Ack=97 Win=14608 Len=0 TSval=106465 TSecr=106455 |
| 26 | 32.189210 | 10.2.2.1 | 10.3.3.1 | FTP | 71 | Request: PWD |
| 27 | 32.189225 | 10.2.2.1 | 10.3.3.1 | TCP | 74 | ftp-data > 57526 [RST] Seq=0 Win=0 Len=0 |
| 28 | 32.189242 | 10.3.3.1 | 10.2.2.1 | TCP | 78 | ftp > 57526 [ACK] Seq=97 Ack=36 Win=14480 Len=0 TSval=108163 TSecr=108162 SLE=31 SRE=36 |
| 29 | 32.189332 | 10.3.3.1 | 10.2.2.1 | FTP | 75 | Response: 257 "/" |
| 30 | 32.190845 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=36 Ack=106 Win=14608 Len=0 TSval=108163 TSecr=108163 |
| 31 | 35.498814 | 10.2.2.1 | 10.3.3.1 | FTP | 88 | Request: PORT 10,2,2,1,235,59 |
| 32 | 35.498942 | 10.3.3.1 | 10.2.2.1 | FTP | 117 | Response: 200 PORT command successful. Consider using PASV. |
| 33 | 35.505807 | 10.2.2.1 | 10.3.3.1 | TCP | 66 | 57526 > ftp [ACK] Seq=58 Ack=157 Win=14608 Len=0 TSval=108991 TSecr=108990 |
| 34 | 35.505852 | 10.2.2.1 | 10.3.3.1 | FTP | 72 | Request: LIST |
| 35 | 35.506192 | 10.3.3.1 | 10.2.2.1 | TCP | 74 | ftp-data > 59707 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=108992 TSecr=0 WS=16 |

Figura 12: Pedido de retransmissão de um pacote numa transferência da file1 por FTP a partir do sistema Alfa na LAN2

| Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|--------|---|
| 3 | 8.715003 | 10.1.1.1 | 10.3.3.1 | TCP | 74 51905 > ftp [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2706956 TSecr=0 WS=16 |
| 4 | 8.715003 | 00:00:00:aa:00:14 | Broadcast | ARP | 42 Who has 10.3.3.254? Tell 10.3.3.1 |
| 5 | 8.715159 | 00:00:00:aa:00:10 | 00:00:00:aa:00:14 | ARP | 42 10.3.3.254 is at 00:00:00:aa:00:10 |
| 6 | 8.715166 | 10.3.3.1 | 10.1.1.1 | TCP | 74 ftp > 51905 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=2706956 TSecr=2706956 WS=16 |
| 7 | 8.716797 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=2706956 TSecr=2706956 |
| 8 | 8.722564 | 10.3.3.1 | 10.1.1.1 | FTP | 86 Response: 220 (vsFTPd 2.3.5) |
| 9 | 8.725088 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=1 Ack=21 Win=14608 Len=0 TSval=2706958 TSecr=2706958 |
| 12 | 11.631225 | 10.1.1.1 | 10.3.3.1 | FTP | 82 Request: USER anonymous |
| 13 | 11.631252 | 10.3.3.1 | 10.1.1.1 | TCP | 66 ftp > 51905 [ACK] Seq=21 Ack=97 Win=14480 Len=0 TSval=2707685 TSecr=2707685 |
| 14 | 11.631639 | 10.3.3.1 | 10.1.1.1 | FTP | 100 Response: 331 Please specify the password. |
| 15 | 11.633231 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=17 Ack=55 Win=14608 Len=0 TSval=2707686 TSecr=2707685 |
| 16 | 12.212529 | 10.1.1.1 | 10.3.3.1 | FTP | 74 Request: PASS l |
| 17 | 12.224630 | 10.3.3.1 | 10.1.1.1 | FTP | 89 Response: 230 Login successful. |
| 18 | 12.227027 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=25 Ack=78 Win=14608 Len=0 TSval=2707834 TSecr=2707834 |
| 19 | 12.227046 | 10.1.1.1 | 10.3.3.1 | FTP | 72 Request: SYST |
| 20 | 12.227170 | 10.3.3.1 | 10.1.1.1 | FTP | 85 Response: 215 UNIX Type: L8 |
| 21 | 12.265926 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=31 Ack=97 Win=14608 Len=0 TSval=2707844 TSecr=2707834 |
| 22 | 13.720908 | 00:00:00:aa:00:10 | 00:00:00:aa:00:14 | ARP | 42 Who has 10.3.3.1? Tell 10.3.3.254 |
| 23 | 13.721007 | 00:00:00:aa:00:14 | 00:00:00:aa:00:10 | ARP | 42 10.3.3.1 is at 00:00:00:aa:00:14 |
| 24 | 17.154693 | 10.1.1.1 | 10.3.3.1 | FTP | 71 Request: PWD |
| 25 | 17.154693 | 10.3.3.1 | 10.1.1.1 | FTP | 75 Response: 257 "/" |
| 26 | 17.156753 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=36 Ack=106 Win=14608 Len=0 TSval=2709067 TSecr=2709066 |
| 28 | 20.180030 | 10.1.1.1 | 10.3.3.1 | FTP | 89 Request: PORT 10,1,1,1,128,246 |
| 29 | 20.183900 | 10.3.3.1 | 10.1.1.1 | FTP | 117 Response: 200 PORT command successful. Consider using PASV. |
| 30 | 20.190728 | 10.1.1.1 | 10.3.3.1 | TCP | 66 51905 > ftp [ACK] Seq=59 Ack=157 Win=14608 Len=0 TSval=2709825 TSecr=2709824 |
| 31 | 20.190800 | 10.1.1.1 | 10.3.3.1 | FTP | 72 Request: LIST |
| 32 | 20.191207 | 10.3.3.1 | 10.1.1.1 | TCP | 74 ftp-data > 33014 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2709825 TSecr=0 WS=16 |
| 33 | 20.191928 | 10.1.1.1 | 10.3.3.1 | TCP | 74 33014 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=2709825 TSecr=2709825 WS=16 |

Figura 13: Transferência da file1 por FTP a partir do sistema Portatil1 na LAN1 sem pedido de retransmissão de pacote

Pelas figuras acima podemos concluir que numa rede de menor qualidade (link do sistema Alfa) existe uma maior sobrecarga na rede devido pedidos de retransmissão de pacotes que em redes com melhor qualidade (link do sistema Portatil1) ocorrem com menos frequência ou até podem não ocorrer.

Em protocolos não fiáveis, tal como o UDP, que contribuem para a redução da latência de ligação, como não fazem verificações de pacotes recebidos com sucesso, não existe sobrecarga da rede nem com Acknowledgment nem com reenvios de pacotes em condições de redes menos favoráveis.

5 Conclusões

Este trabalho serviu de complemento às aulas teóricas permitindo-nos aplicar os conhecimentos e compreender melhor o modo como as aplicações recorrem aos serviços da camada inferior, através dos protocolos de aplicação e transporte, e ainda observar quais as suas portas de atendimento e o overhead associado ao transporte. Foi efetuada a transferência de um ficheiro através de quatro serviços diferentes, o que nos permitiu analisar o tráfego gerado pelo uso dos diferentes protocolos quer de Aplicação quer de Transporte recorrendo ao Wireshark. Posteriormente, elaboramos um diagrama temporal para os protocolos FTP e TFTP onde traduzimos a análise efetuada anteriormente. De seguida foi feita uma comparação entre as características dos quatro protocolos utilizados, do qual concluímos que todos eles apresentam vantagens e desvantagens em relação uns aos outros, dependendo do contexto da sua aplicação. Finalmente, observamos as diferenças entre o TCP e o UDP na maneira como lidam com os datagramas.