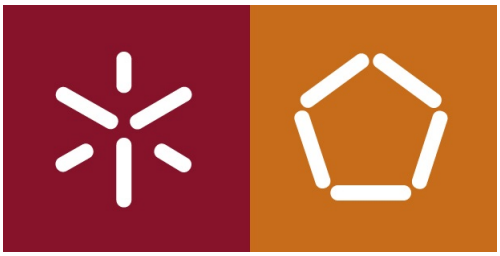
Universidade do Minho

Mestrado Integrado em Engenharia Informática



TP1 - Protocolos da Camada de Transporte

Comunicações por Computador

PL2 Grupo 4

Adriana Meireles

A82582

Helena Martins

A82500

Mariana Pereira

A81146

4 de Março de 2020

Conteúdo

0.1 Questões e Respostas

0.1.1 Questão 1:

Inclua no relatório uma tabela em que identifique, para cada comando executado, qual o protocolo de aplicação, o protocolo de transporte, porta de atendimento e overhead de transporte, como ilustrado no exemplo seguinte:

Comando usado	Protocolo de Aplicações	Protocolo de Transporte	Porta de Atendimento	Overhead de Transporte em bytes
Ping	PING	-	-	-
Traceroute	TRACEROUTE	UDP	33443	(8/40)*100
Telnet	TELNET	TCP	23	(20/47)*100
FTP	FTP	TCP	21	(20/26)*100
TFTP	TFPT	UDP	69	(8/52)*100
Browser/http	HTTP	TCP	80	(20/331)*100
nslookup	DNS	UDP	53	(8/39)*100
SSH	SSH	TCP	22	(20/332)*100

- **Ping:**

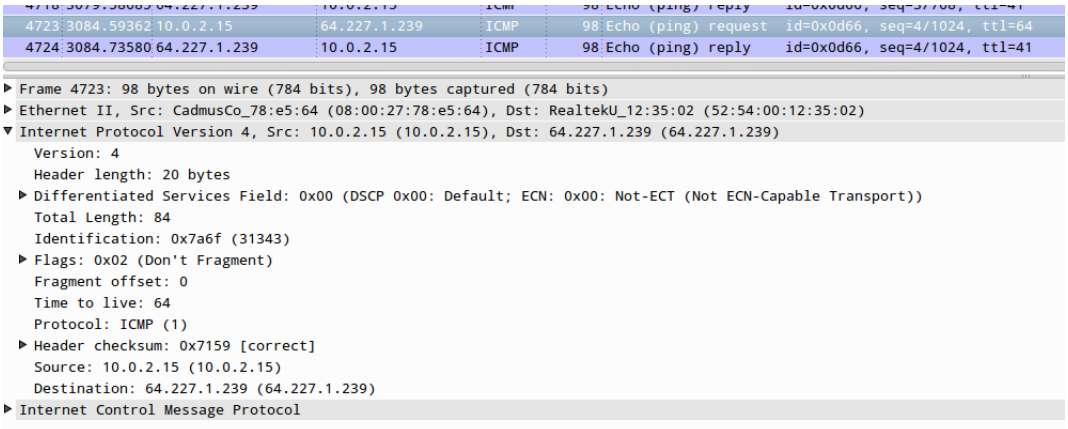


Figura 1: Captura de Tráfego Ping

O protocolo que foi utilizado é o PING. Como o ping trabalha diretamente com a camada de rede, o protocolo de transporte não é aplicável pelo que não existe porta de atendimento nem overhead de transporte.

- **Traceroute:**

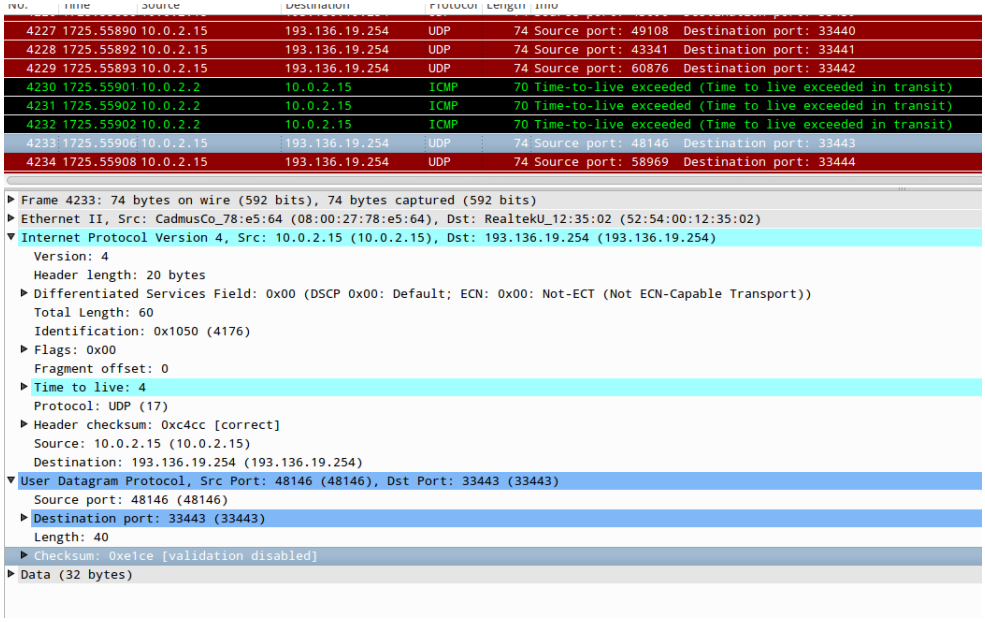


Figura 2: Captura de Tráfego Traceroute

O protocolo de aplicação utilizado foi o TRACEROUTE .Com base na figura 2 podemos observar que o protocolo de transporte é o UDP. A porta de atendimento para a trama é a 33443. Uma vez que o protocolo de transporte é o UDP, possui um cabeçalho de tamanho fixo de 8 bytes,logo o overhead é $(8/40) * 100 = 20\%$

- **Telnet:**

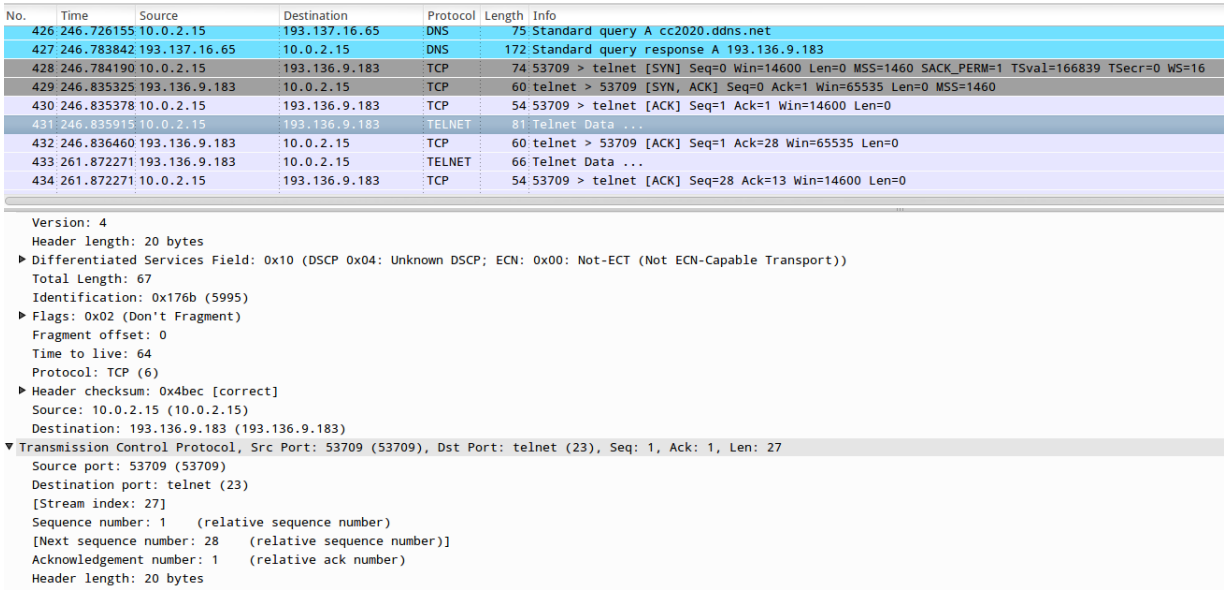


Figura 3: Captura de Tráfego Telnet

O protocolo de aplicação utilizado é o TELNET. O protocolo de transporte é o TCP e a porta de atendimento da trama é a 23. O overhead é $(20/(67-20)) * 100 = 42.5\%$

- **FTP:**

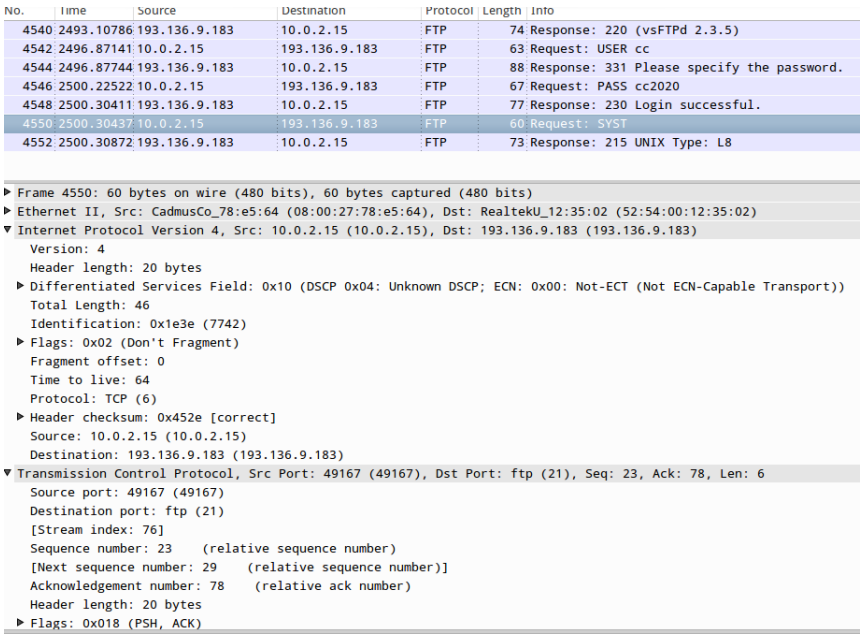


Figura 4: Captura de Tráfego FTP

Na figura 4 verificamos que o protocolo de aplicação utilizado é o FTP. O protocolo de transporte é o TCP e a porta de atendimento da trama é a 21. O overhead é $(20/(46-20)) * 100 = 76.9\%$

- **TFTP:**

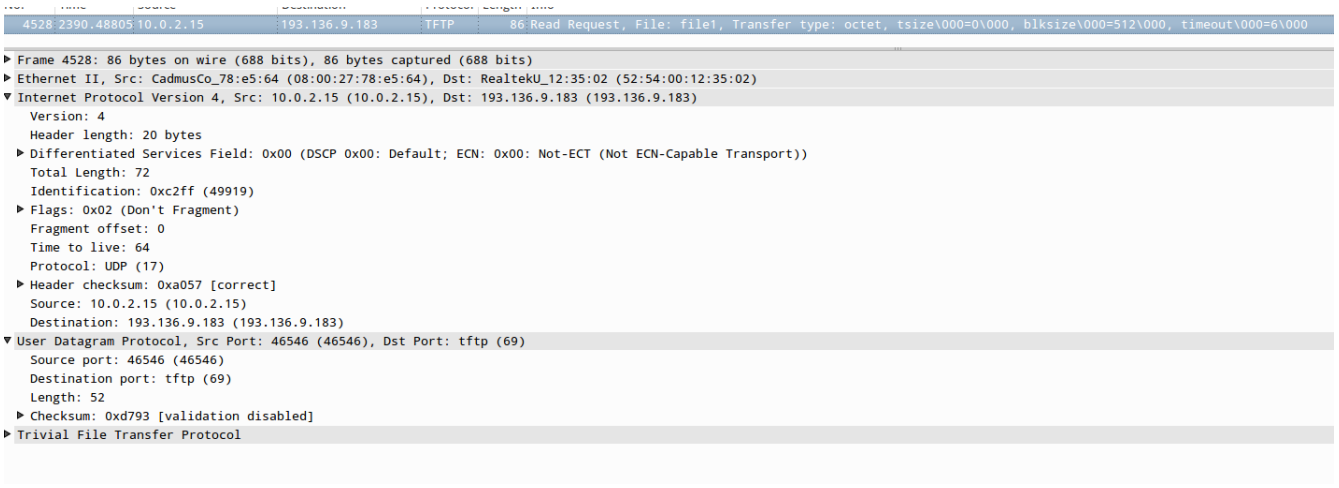


Figura 5: Captura de Tráfego TFTP

Como podemos visualizar na figura 5, o protocolo de aplicação é o TFTP. O protocolo de transporte é o UDP que tem cabeçalho de tamanho fixo de 8

bytes como foi dito anteriormente. A porta de atendimento da trama é a 69. O overhead é $(8/52) * 100 = 15.4$

- **Browser/HTTP:**

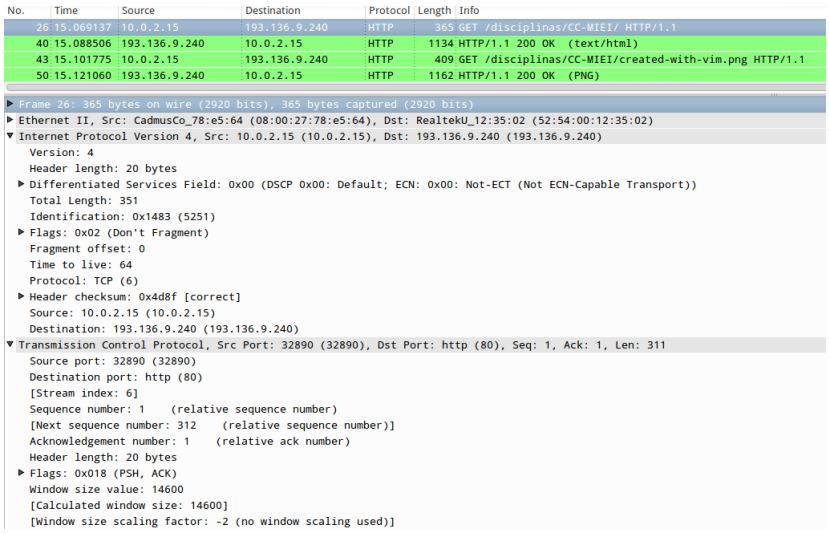


Figura 6: Captura de Tráfego HTTP

Como podemos observar na figura 6, o protocolo de aplicação é o HTTP. O protocolo de transporte utilizado é o TCP e a porta de atendimento é a 80. De acordo com os dados da figura, o overhead é $(20/(351 - 20)) * 100 = 6\%$

- **nslookup:**

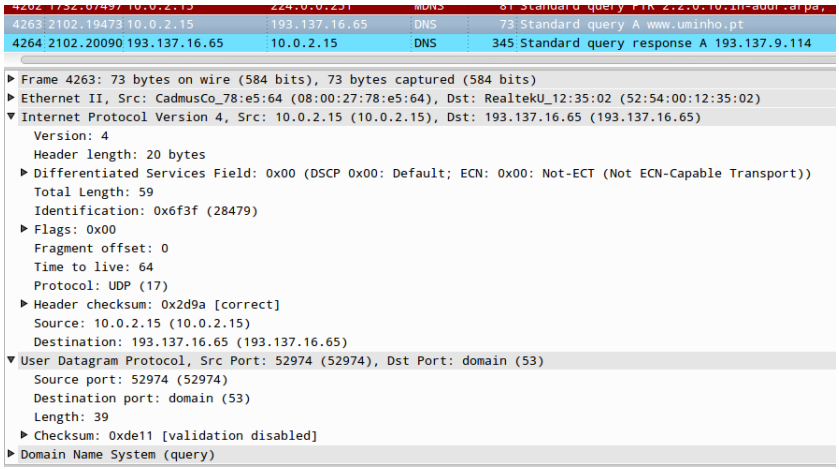


Figura 7: Captura de Tráfego DNS

Como podemos observar na figura 7, o protocolo de aplicação utilizado é o DNS. O protocolo de transporte utilizado é o UDP e a porta de atendimento da trama é a 53. O overhead é $(8/39) * 100 = 20.5\%$

- **SSH:**

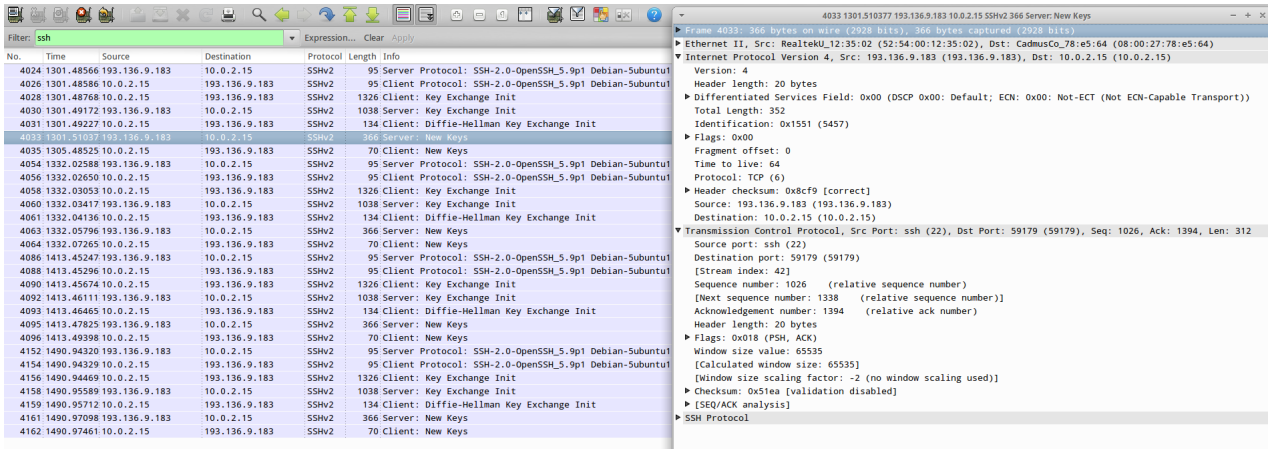


Figura 8: Captura de Tráfego SSH

Como podemos verificar na figura 8 o protocolo de aplicação utilizado é o SSH. O protocolo de transporte é o TCP e a porta de atendimento da trama é a 22. O overhead é $(20/(352-20)) * 100 = 6\%$

0.1.2 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. (Nota: a transferência por FTP envolve mais que uma conexão FTP, nomeadamente uma de controlo [ftp] e outra de dados [ftp-data]. Faça o diagrama apenas para a conexão de transferência de dados do ficheiro mais pequeno)

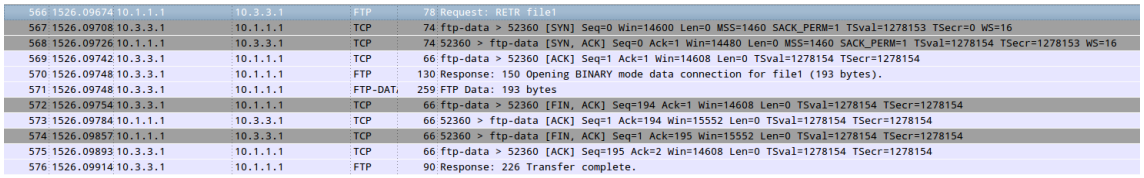


Figura 9: Captura de transferência via ftp

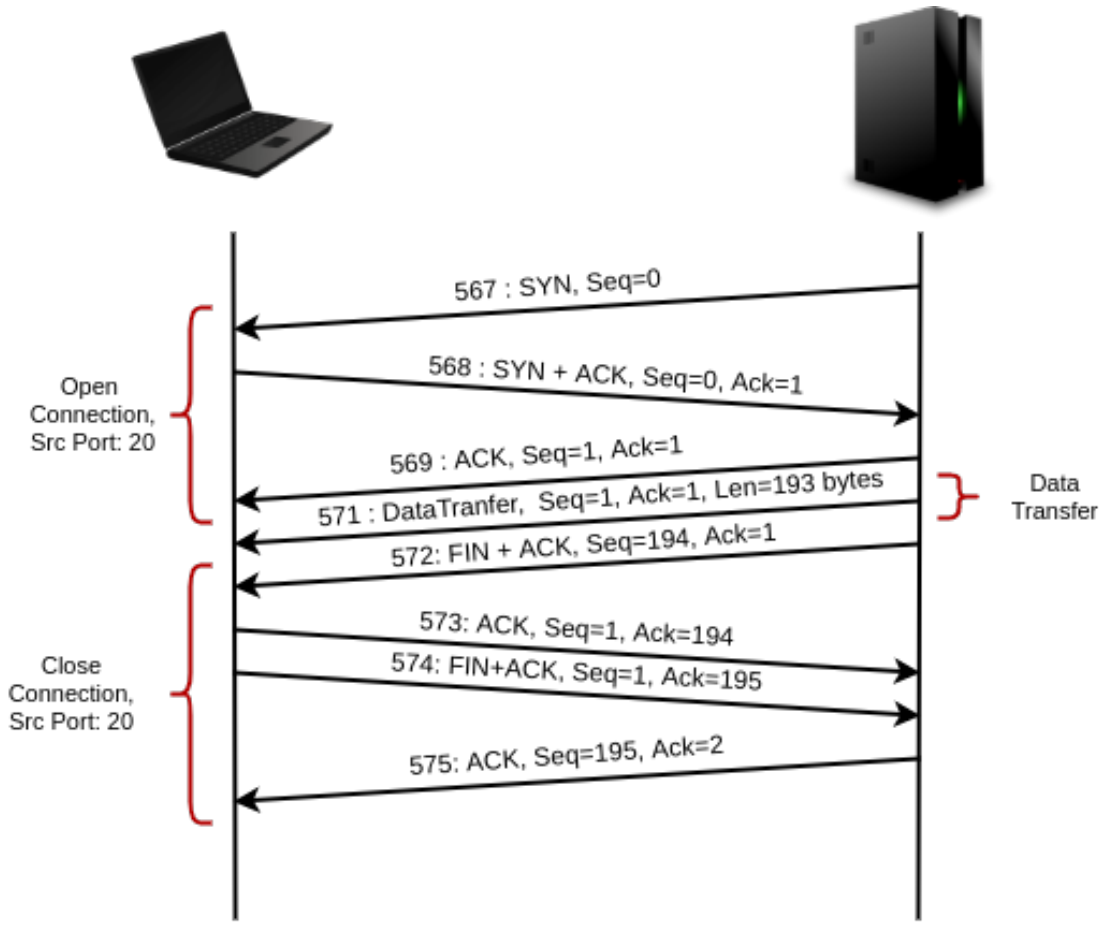


Figura 10: Diagrama Temporal ftp

Primeiramente, o servidor começa a conexão através da porta 20, enviando um pacote SYN cujo número de sequência é 0. O cliente responde com um SYN+ACK. De seguida, o servidor envia um ACK de volta ao cliente. Depois de enviar os dados pretendidos, o servidor inicia a fase de encerramento de conexão, que é constituída por quatro etapas. A flag FIN indica que se pretende terminar a conexão, ficando à espera de uma resposta ACK. Podemos verificar isso através do diagrama temporal apresentado, tendo este sido construído com base na captura de tráfego observada na Figura 9.

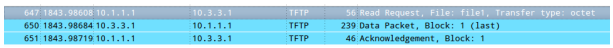


Figura 11: Captura de transferência via tftp

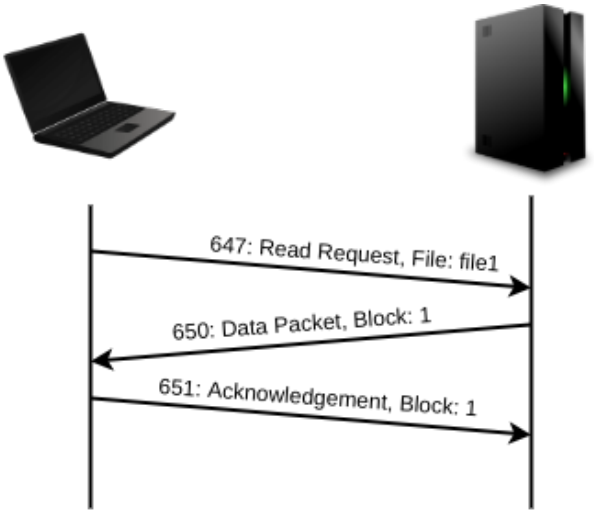


Figura 12: Diagrama temporal tftp

O cliente envia um Read Request para o servidor que irá conter diversas informações,entre as quais o nome do ficheiro. O servidor irá responder com um pacote de dados. Após a receção dos dados por parte do cliente, este irá enviar um pacote ACK.

0.1.3 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;

	SFTP	FTP	TFTP	HTTP
Uso da camada de transporte	Protocolo TCP	Protocolo TCP	Protocolo UDP	Protocolo TCP
Eficiência na Transferência	A eficiência é comprometida pela fiabilidade da transferência de dados.	Fiável, levando a um maior overhead.	Como não se responsabiliza por entregar os dados, apresenta um overhead menor.	Apresenta grande eficiência. Como usa pipelining é bastante rápido o que o torna uma escolha ideal.
Complexidade	É muito complexo devido ao facto de apresentar muitas funcionalidades.	Como garante segurança na transferência de dados, é complexo.	O protocolo de transporte é o UDP e as funcionalidades presentes são mais pequenas. Deste modo, é uma versão simplificada do FTP	Pouco complexo.
Segurança	Como recorre à autenticação e encriptação dos dados, é seguro.	Apesar de utilizar autenticação, é pouco seguro uma vez que a informação não é encriptada, mas sim passada como texto.	É pouco seguro, uma vez que não fornece mecanismos de autenticação ou encriptação dos dados.	É pouco seguro pois apenas recorre à autenticação, não utilizando encriptação dos dados. É vulnerável a ataques "man-in-the-middle", o que permite a atacantes o acesso a contas e informações confidenciais.

0.1.4 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).

Tal como podemos observar na figura que apresentamos a seguir, foi realizado um ping na LAN3 onde 10% dos pacotes foram perdidos e um pacote foi duplicado. Isto acontece devido à existência de problemas a nível de rede.

Para estes problemas de rede, os protocolos de transporte UDP e TCP têm formas diferentes de reagir. O protocolo TCP tem mecanismos de deteção e recuperação, para quando houver uma perda de pacote este seja retransmitido, garantindo que todos os pacotes são entregues, ao contrário do UDP que não dispõe desses mecanismos. Caso haja perda de pacotes, são os protocolos que correm em cima do UDP que poderão corrigir e identificar estes erros.

Posto isto, no caso do host Alfa, apresentado na figura seguinte, os pacotes podem ser recuperados pois podem ser reenviados devido ao protocolo TCP.

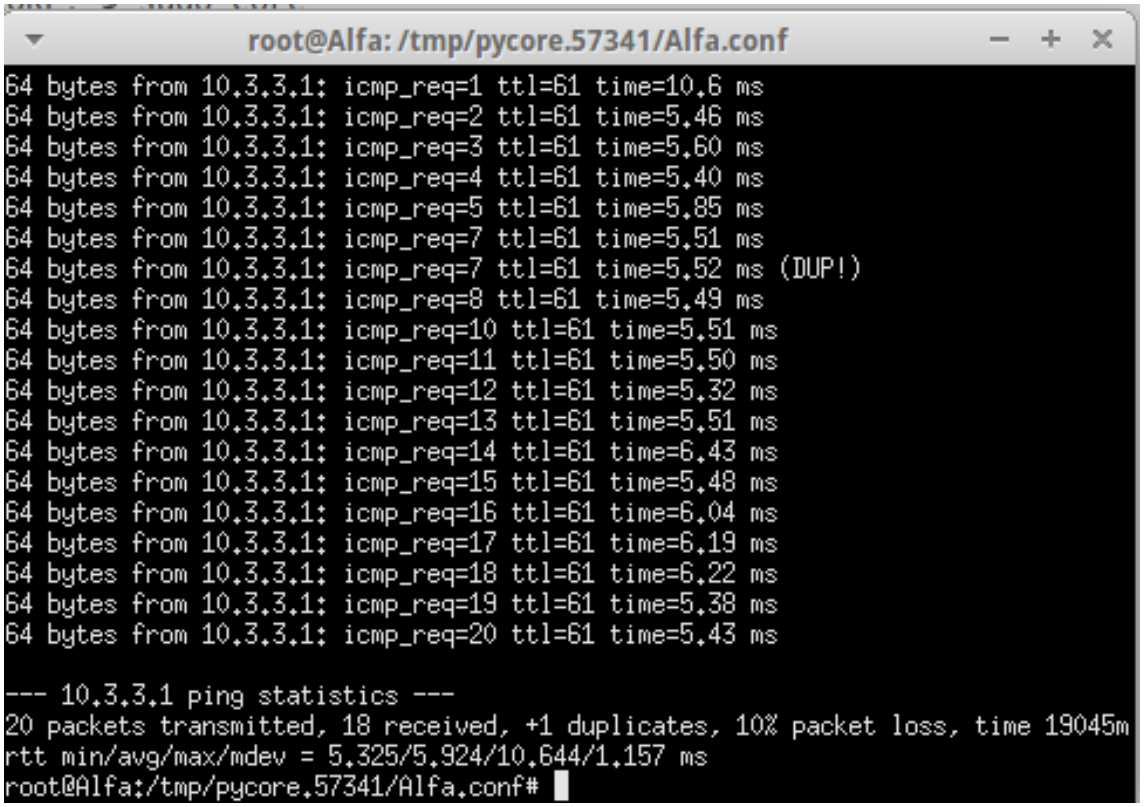


Figura 13: Ping

0.2 Conclusões

Com este trabalho estudámos o modo como as várias aplicações recorrem aos serviços da camada inferior. Para isso foram considerados os diversos protocolos de aplicação e transporte, portas de atendimento e o overhead associado ao transporte.

Começámos por realizar a instalação, configuração e utilização de serviços de transferência de ficheiros.Deste modo, foi transferido um mesmo ficheiro com recurso a quatro serviços diferentes SFTP,FTP,TFTP e HTTP. Foi realizado um diagrama temporal para o FTP e TFTP com a identificação das fases de estabelecimento de conexão, transferência de dados e fim de conexão. Posteriormente, foram analisadas as características de cada um.Por último, observámos o modo como o TCP e o UDP lidam com a perda e duplicação de pacotes.

Em suma, este trabalho permitiu-nos consolidar os conhecimentos acerca da camada de transporte.