

# RCOM Projeto 2

---

Autores:

Filipe Reis Almeida (up201708999)

Luís Ricardo Matos Mendes (up201604835)

## Sumário

Este trabalho aborda o desenvolvimento de uma aplicação que descarrega ficheiros de um servidor FTP. Esta aplicação tem de funcionar corretamente nos computadores tux3 e tux2 do laboratório que inicialmente não têm acesso à internet. Para tal, é necessário o setup devido destes computadores para que seja possível o download de um ficheiro de um servidor FTP externo.

## Introdução

O objetivo deste trabalho consiste em produzir uma aplicação cuja funcionalidade é executar a transferência de ficheiros de um servidor FTP e configurar uma network entre os computadores para que a partir destes seja possível o download de um ficheiro de um servidor FTP.

Neste relatório está explicado a nossa implementação da aplicação, a sua arquitetura e forma de lidar com os erros, tal como a configuração da rede, análise dos logs e conclusões retiradas.

## Aplicação download

### Arquitetura da aplicação

A estrutura global da aplicação, no que diz respeito ao envio dos comandos, é semelhante à experiência do telnet no guião da primeira aula.

O primeiro passo é retirar a informação da ligação a partir do link inserido como argumento. O método `validate_and_parse_arguments` valida o número de argumentos inseridos e aloca para a struct `LinkInfo` o username, a password, o hostname e o filePath. Também lida com links sem username e password, nesse caso, o username e password enviados pelos comandos ao servidor ftp são "anonymous" e "1", respetivamente. Também lida com links mal construídos, retornando 1 caso algum elemento não exista ou a sintaxe do link esteja incorreta.

De seguida, com método `get_host` obtém-se a informação do host a partir do node do host fornecido no link. Caso a função `gethostbyname` falhe, o programa retorna erro.

De seguida, o programa abre uma socket TCP e conecta-se ao servidor. Esta socket é usada para o envio do user e da password (método `send_credentials`) e do comando `pasv` (método `switch_passive_mode`). Em ambos estes métodos, caso seja recebido um código de resposta diferente de 2xx e 3xx, o programa retorna com erro.

No `switch_passive_mode`, o programa aguarda por uma resposta com código 230 que contém a string, por exemplo: "Entering Passive Mode (149,20,1,49,65,17)", da qual se retira a nova porta dos dois últimos códigos com a lógica  $65 \times 256 + 17$  (método `get_port`). Como nos métodos anteriores, caso receba um código diferente de 2xx e 3xx, o programa retorna erro. Com a porta recebida pela resposta do modo passivo, abre-se uma nova socket TCP associada ao endereço IP retirado pela `gethostbyname`.

Depois, envia-se o comando retrieve pela socket utilizada para o envio dos comandos e de seguida faz-se a leitura da nova socket criada para a receção do ficheiro (método `receive_and_create_file`). Caso o servidor FTP retorne um código diferente de 1xx no envio do comando `retr`, o programa termina com erro, pois é provável que o ficheiro não exista no servidor. Caso o read da socket FTP falhe, o programa termina com erro. Durante a leitura da socket é feita a escrita dos bytes para o file descriptor do ficheiro criado na raíz do projeto.

Ao terminar, fecha-se as as duas sockets TCP criadas.

## Resultados de um download com sucesso

```
luis@luis-desktop-arch:~/work/rcom/feup-rcom/Trabalho_2$ make clean && make && ./download ftp://ftp.isc.org/isc/ls-lR.gz
rm -f obj/*.o
rm -f download
gcc -Wall -c -Iinclude src/main.c -o obj/main.o
gcc -Wall -c -Iinclude src/auxiliar.c -o obj/auxiliar.o
gcc obj/main.o obj/auxiliar.o -o download

Connecting to server
< Response Code: 220
> user anonymous
< Response Code: 331
> pass 1
< Response Code: 230
> pasv
< Response Code: 230
Entering Passive Mode (149,20,1,49,50,129)
Connecting to server
> retr ls-lR.gz
< Response Code: 150
Finished file Download

luis@luis-desktop-arch:~/work/rcom/feup-rcom/Trabalho_2$
```

## Configuração da network e análise

### Exp 1- Configure an IP Network

Nesta experiência, foram criados novos endereços de ip nas interfaces de rede dos tuxes 3 e 4. Como os ips tinham a mesma mask (172.16.y0.0), era possível estabelecer a ligação entre ambos.

- What are the ARP packets and what are they used for?

Os pacotes ARP contêm informações sobre endereços IP e MAC e servem para que um PC seja capaz de mapear endereços IP ao respetivo endereço físico, para depois ser capaz de estabelecer ligações.

- What are the MAC and IP addresses of ARP packets and why?

Se o tux 3 necessitar do MAC address do tux 4, o 3 envia para o 4 um pacote ARP request. Este pacote tem:

- Sender MAC address: MAC do tux 3.
- Sender IP address: IP do tux 3.
- Target MAC address: Não preenchido(00:00:00\_00:00:00 (00:00:00:00:00:00)).
- Target IP address: IP do tux 4.

O 4, ao receber o pacote, guarda o mapeamento dos endereços do 3 e envia um ARP reply:

- Sender MAC address: MAC do tux 4.

- Sender IP address: IP do tux 4.
- Target MAC address: MAC do tux 3.
- Target IP address: IP do tux 3.

Podendo assim o 3 guardar o mapeamento do 4.

- What packets does the ping command generate?

O comando ping usa inicialmente pacotes ARP para mapear os endereços. Posteriormente, são usados pacotes ICMP para a comunicação entre os computadores.

- What are the MAC and IP addresses of the ping packets?

Dando ping do tux 3 para o 4, o ping request tem:

- Sender MAC address: MAC do tux 3.
- Sender IP address: IP do tux 3.
- Target MAC address: MAC do tux 4.
- Target IP address: IP do tux 4.

O ping reply tem:

- Sender MAC address: MAC do tux 4.
- Sender IP address: IP do tux 4.
- Target MAC address: MAC do tux 3.
- Target IP address: IP do tux 3.

## Exp 2 – Implement two virtual LANs in a switch

Nesta experiência foram criadas duas vlans, uma ligada aos tuxes 3 e 4 e outra ao 2. Depois desta experiência, apenas o foi possível estabelecer ligação do 3 com o 4.

- How to configure vlany0?

Para configurar a vlan, apenas é necessário criá-la e atribuir-lhe as portas desejadas.

- configure terminal
- vlan 20
- end

Passos para associar a porta 1 a vlan20

- configure terminal
- interface fastethernet 0/1
- switchport mode access
- switchport access vlan 20
- end

- How many broadcast domains are there?

Existe uma do tux 3 e do tux 4, já que estão na mesma vlan e conseguem estabelecer comunicação um com o outro. A vlan que contém o tux 2 também é um domínio de broadcast.

## Exp 3 – Configure a Router in Linux

Nesta experiência o tux 4 foi configurado como um router. Para além de adicionar o tux 4 a ambas as vlans, foram adicionadas rotas para que ser possível ligar os tuxes 2 e 3.

- What routes are there in the tuxes? What are their meaning?

Tux 2:

- Destination: 172.16.y1.0 Gateway: 172.16.y1.1
- Destination: 172.16.y0.0 Gateway: 172.16.y1.253

Tux 3:

- Destination: 172.16.y0.0 Gateway: 172.16.y0.1
- Destination: 172.16.y1.0 Gateway: 172.16.y1.254

Tux 4:

- Destination: 172.16.y0.0 Gateway: 172.16.y1.254
- Destination: 172.16.y1.0 Gateway: 172.16.y1.253

Todas as rotas com destino 172.16.y0.0 ligam-se à vlan 0 e rotas com destino 172.16.y1.0 ligam-se à vlan 1.

- What ARP messages, and associated MAC addresses, are observed and why?

Tal como já tinha acontecido, quando o ping é iniciado, o tux que recebeu precisa de saber o MAC address de quem o enviou. Para isso, envia um ARP request em modo broadcast e espera pela resposta.

- What ICMP packets are observed and why?

Depois desta experiência, observam-se ping request e ping reply. Isto é possível pois, com as novas rotas, pode estabelecer-se a ligação entre o 2 e o 3.

- What are the IP and MAC addresses associated to ICMP packets and why?

Os endereços associados aos packets os de destino e origem. Por exemplo, nos ping requests do tux 3 para o 2, os de destino são do 2 e os de origem são de 3, mesmo que passe pelo 4.

## Exp 4 – Configure a Commercial Router and Implement NAT

Nesta experiência foi adicionado um router à vlan 1. Desta forma o tux 2 e o tux 4 ligam-se diretamente ao router e o 3 tem de passar primeiro pelo 4. Depois da configuração do NAT, foi possível a ligação do tux 2 e 3 com o router do outro laboratório.

- How to configure a static route in a commercial router?

Para que o router conseguisse chegar ao tux 3 através do 4, foi adicionada uma rota ao router com o comando: `ip route 172.16.y0.0 255.255.255.0 172.16.y1.253`, de maneira a poder chegar à vlan 1.

- What are the paths followed by the packets in the experiments carried out and why?

O tux 3, para chegar ao router, tem de se ligar primeiro ao 4. Para o tux 2 chegar ao 3, liga-se ao 4, pois tem uma route definida, ligando-se depois ao 3. Se essa route for removida, o 2 redireciona automaticamente para o router, que depois redireciona para o tux 4 e o 4 para o 3. As restantes ligações são feitas dentro da mesma vlan, podendo ligar-se diretamente.

- What does NAT do?

O NAT permite comunicações para o exterior da rede, fazendo-as sempre com mesmo IP. Permite assim uma maior segurança para os dispositivos conectados a essa rede.

## Exp 5 – DNS

Nesta experiência foi definido o DNS e testada a ligação à internet em todos os tuxes.

- How to configure the DNS service at an host?

O DNS é configurado usando o ficheiro resolv.conf, definindo o nome do servidor e o endereço IP.

- What packets are exchanged by DNS and what information is transported?

Quando é fornecido um hostname, o é necessário enviar um pedido ao servidor para que seja retornado o endereço de IP. Por isso, os pacotes de DNS são para executar esse pedido e enviar a respetiva resposta com o endereço.

## Exp 6 – TCP connections

Nesta experiência foi usado a nossa aplicação de download, com a ligação à internet criada nas experiências.

- How many TCP connections are opened by your ftp application? In what connection is transported the FTP control information?

São abertas duas conexões TCP. Uma para transmitir comandos FTP e receber as respetivas respostas. Depois do envio do comando do modo passivo é aberta outra porta cujo número é obtido pelo cálculo dos bytes de resposta ao comando pasv. Esta socket serve para a receção de pacotes do ficheiro e envio das respostas.

- What are the phases of a TCP connection?

O protocolo TCP tem 3 fases:

- Estabelecimento da conexão
- Envio de pacotes de informação
- Encerramento da conexão

- How does the ARQ TCP mechanism work? What are the relevant TCP fields?

- O ARQ consiste num sistema em que depois do servidor enviar um packet de informação, espera que o recetor retorne um packet de acknowledgment, tentando reenviar a informação ao fim de um timeout até a um determinado número de tentativas.

- Is the throughput of a TCP data connections disturbed by the appearance of a second TCP connection? How?

- Embora o download continue a funcionar sem erros, a velocidade do mesmo diminui, uma vez que a taxa de transferência passa a estar distribuída pelas duas ligações.

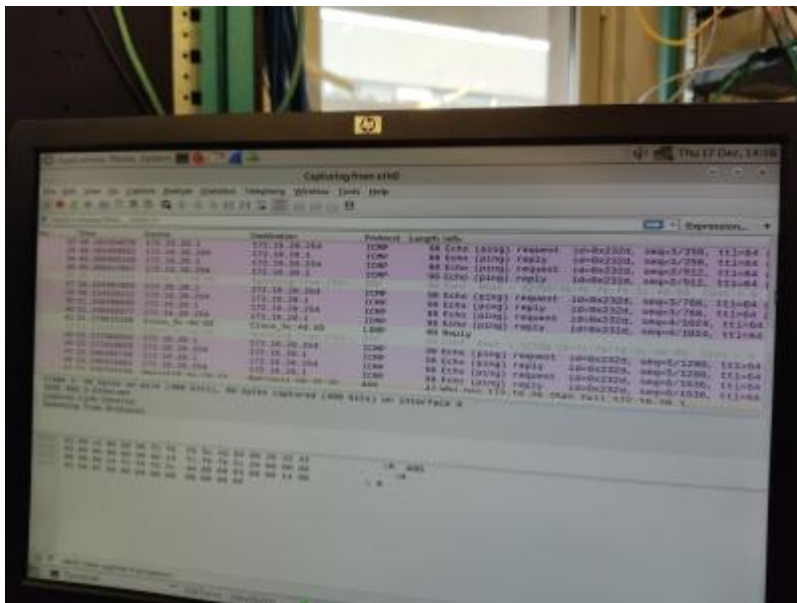
## Conclusões

Depois deste trabalho ficamos com uma melhor noção de como as conexões entre computadores são estabelecidas assim como melhor conhecimento do funcionamento geral da internet. Conceitos como ping, router, IP e MAC addresses, TCP, masks, ARQ, DNS, alguns que já conhecíamos, tornaram-se agora mais claros.

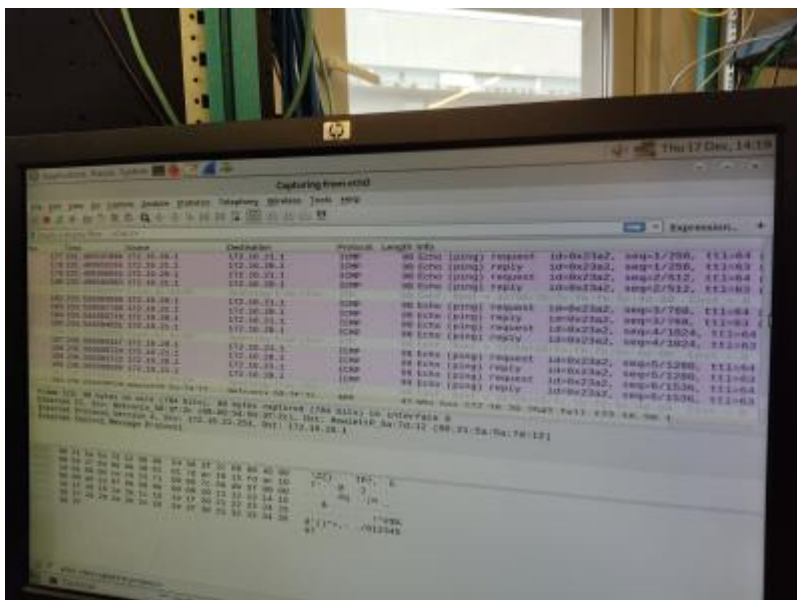
## Anexos

O código está como pasta zip junto com a entrega do relatório.

Pings do tux23 para 172.16.20.254

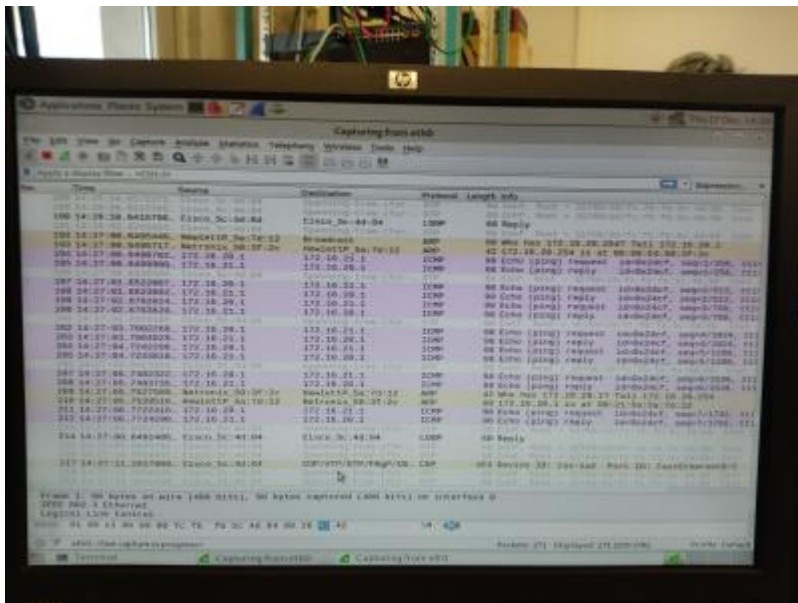


Pings do tux23 para 172.16.21.1

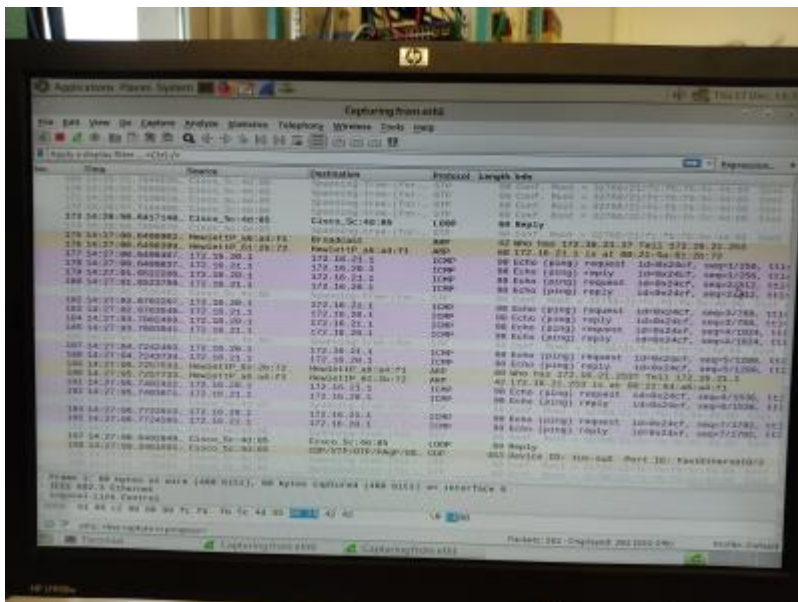




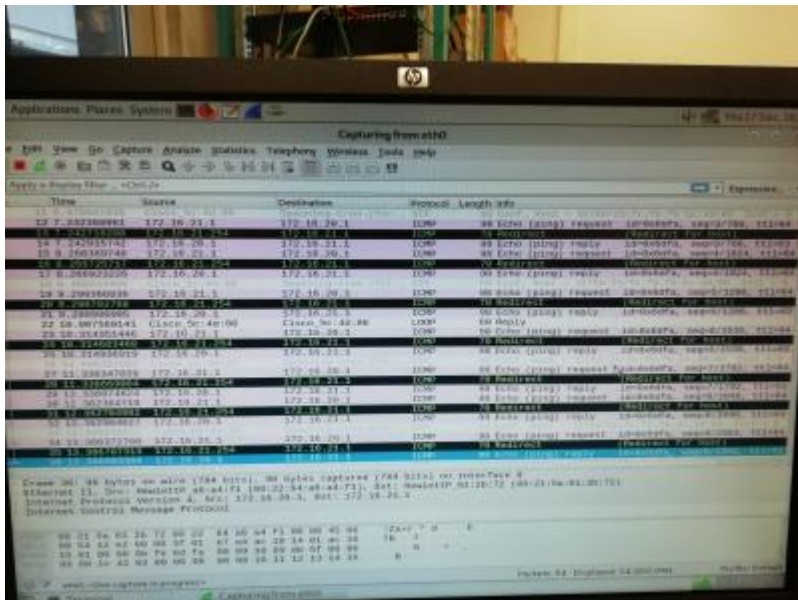
## Pings do tux23 para tux22 no tux24 eth0



## Pings do tux23 para tux24 no tux24 eth1



## Ping tux22 para tux23 sem route para 172.16.20.0



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telescope, Windows, Tools, and Help. The toolbar contains icons for common actions like opening files, saving, and capturing. The status bar at the bottom indicates the current capture source is 'eth0' and shows the capture rate as '0.00 MB/s'.

The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 100 is selected, which is a NetBIOS session setup request from 192.168.1.100 to 192.168.1.1.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and the NetBIOS session setup request structure, including fields like session ID, session type, and session name.
- Packet Bytes:** Displays the raw hexadecimal and ASCII data of the selected packet.

The selected packet (100) is a NetBIOS session setup request. The details pane shows the following structure:

- Ethernet II, Src: Realtek-80-00-00-00-00-00, Dst: 192.168.1.1
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
- NetBIOS session setup request, Src: 192.168.1.100, Dst: 192.168.1.1
- Session ID: 100
- Session type: 1
- Session name: 192.168.1.100

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and the NetBIOS session setup request structure.

[illegible]