**Faculdade de Engenharia da Universidade do Porto**

Uma imagem com texto

Descrição gerada automaticamente

**2º Trabalho Laboratorial**

Relatório

Redes de computadores

Margarida Mesquita Leal – up201906884

Miguel Augusto Marombal Araújo – up201905077

Índice

[1. Introdução 4](#_Toc105526776)

[2. Parte I – Download Application 4](#_Toc105526777)

[2.1. Arquitetura da Aplicação de Download 4](#_Toc105526778)

[2.1.1. Processamento da string de input 4](#_Toc105526779)

[2.2. Resultados 4](#_Toc105526780)

[3. Parte II – Network configuration and analysis 5](#_Toc105526781)

[3.1. Experiência 1 5](#_Toc105526782)

[3.1.1. What are the ARP packet and what are they used for? 5](#_Toc105526783)

[3.1.2. What are the MAC and IP addresses of ARP packets and why? 5](#_Toc105526784)

[3.1.3. What packets does the ping command generate? 6](#_Toc105526785)

[3.1.4. What are the MAC and IP addresses of the ping packets? 6](#_Toc105526786)

[3.1.5. How to determine if a receiving Ethernet frame is ARP, IP, ICMP? 6](#_Toc105526787)

[3.1.6. How to determine the length of a receiving frame? 6](#_Toc105526788)

[3.1.7. What is the loopback and why is it important? 6](#_Toc105526789)

[3.2. Experiência 2 6](#_Toc105526790)

[3.2.1. How to configure vlan60? 7](#_Toc105526791)

[3.2.2. How many broadcast domains are there? How can you conclude it from the logs? 7](#_Toc105526792)

[3.3. Experiência 3 7](#_Toc105526793)

[3.3.1. What routes are there in the tuxes? What are their meaning? 7](#_Toc105526794)

[3.3.2. What information does an entry of the forwarding table contain? 8](#_Toc105526795)

[3.3.3. What ARP messages, and associated MAC addresses, are observed and why? (?????) 8](#_Toc105526796)

[3.3.4. What ICMP packets are observed and why? (=?????) 8](#_Toc105526797)

[3.3.5. What are the IP and MAC addresses associated to ICMP packets and why? (?????) 8](#_Toc105526798)

[3.4. Experiência 4 9](#_Toc105526799)

[3.4.1. How to configure a static route in a commercial router? 9](#_Toc105526800)

[3.4.2. What are the paths followed by the packets in the experiments carried out and why? 9](#_Toc105526801)

[3.4.3. How to configure NAT in a commercial router? 9](#_Toc105526802)

[3.4.4. What does NAT do? 9](#_Toc105526803)

[3.5. Experiência 5 (????) 9](#_Toc105526804)

[3.5.1. How to configure the DNS service at an host? 9](#_Toc105526805)

[3.5.2. What packets are exchanged by DNS and what information is transported? 10](#_Toc105526806)

[3.6. Experiência 6 10](#_Toc105526807)

[3.6.1. How many TCP connections are opened by your ftp application? 10](#_Toc105526808)

[3.6.2. In what connection is transported the FTP control information? 10](#_Toc105526809)

[3.6.3. What are the phases of a TCP connection? 10](#_Toc105526810)

[3.6.4. How does the ARQ TCP mechanism work? What are the relevant TCP fields? What relevant information can be observed in the logs? 10](#_Toc105526811)

[3.6.5. How does the TCP congestion control mechanism work? What are the relevant fields. How did the throughput of the data connection evolve along the time? Is it according the TCP congestion control mechanism? 10](#_Toc105526812)

[3.6.6. Is the throughput of a TCP data connections disturbed by the appearance of a second TCP connection? How? 11](#_Toc105526813)

[4. Conclusões 11](#_Toc105526814)

***Sumário***

O trabalho sobre o qual incide este relatório foi realizado no âmbito da unidade curricular Redes de Computadores. O mesmo previa dois objetivos: o desenvolvimento de uma aplicação de download de um cliente FTP e a configuração de uma rede de computadores no laboratório.

No final das aulas reservadas para o trabalho os requisitos foram cumpridos pelo que o mesmo foi concluído com sucesso sendo capaz de transferir um ficheiro sem erros numa rede de computadores configurada pelo grupo como pretendido, no processo foram desenvolvidas capacidades quer de interpretação quer de implementação no domínio de Redes de Computadores.

# Introdução

O trabalho desenvolvido foi dividido em duas partes. Na primeira, foi desenvolvida uma **aplicação de *download*** capaz de transferir um ficheiro alojada num servidor, garantindo todas as comunicações necessárias com este. Já na segunda parte do trabalho, foi **configurada progressivamente uma rede de computadores**, analisando passo-a-passo o comportamento da rede em cada uma das experiências.

Com este relatório pretende-se analisar e interpretar o desenvolvimento do trabalho em cada uma das partes (implementação da aplicação de download e configuração da rede de computadores). Para além disso, o presente relatório visa clarificar as estratégias de implementação e desenvolvimento do trabalho fornecendo uma justificação clara das decisões tomada para a realização do mesmo.

Para garantir uma estrutura organizada o relatório segue divido de forma coerente com as duas partes do trabalho:

* Parte 1 – Download Application:

- Explicação da arquitetura utilizada

- Exposição dos resultados obtidos com a aplicação

* Parte 2 – Configuração e Analise de uma rede de computadores, seguindo a ordem cronológica das experiências realizadas no laboratório (experiência 1 a 4), dando resposta às questões fornecidas pelo guião em cada uma das experiências.

# Parte I – Download Application

## Arquitetura da Aplicação de Download

Eia que arquitetura

### Processamento da string de input

Processei bue

## Resultados

Ui que resultados top

# Parte II – Network configuration and analysis

Na segunda parte do trabalho propunha-se a configuração e posterior análise de uma rede de computador num processo progressivo e dividido em quatro experiências. Neste capítulo cada uma das quatro experiências será analisada individualmente. Respondendo, em cada caso, ao leque de questões disponibilizadas no guião cuja resposta serve de base para a compreensão dos tópicos mais pertinentes e fundamentais para perceber a experiência em questão.

## Experiência 1

Na experiência 1 propunha-se a criação de uma rede onde os tux3 e tux4 se ligavam. Para tal, ligou-se o tux3 (eth0) e o tux4 (eth0) ao switch de modo que ambos pudessem comunicar entre si.

### What are the ARP packet and what are they used for?

Os pacotes ARP (*Address Resolution Protocol*) são pacotes utilizados para fazer mapeamento de um endereço de rede a um endereço físico. Este protocolo surge da necessidade de identificar o endereço físico de um dispositivo cuja única informação que temos de momento é o seu endereço IP.

Para descobrir o endereço MAC correspondente ao endereço IP do dispositivo com que se pretende comunicar é enviado em Broadcast um pacote ARP que contém o endereço IP do dispositivo para o qual se pretende comunicar e esperasse uma resposta com o endereço MAC correspondente.

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

Os pacotes ARP contêm o endereço MAC e IP de quem os enviou bem como o endereço IP do destinatário. FIGURAS

Cada pacote ARP contém informação acerca do endereço MAC e IP de quem o enviou e acerca de do endereço MAC e IP do seu destinatário. Os exemplos abaixo, retirados dos pacotes ARP presentes nos logs desta experiência nas linhas 7 e 8, demonstram isso mesmo.

Inicialmente (imagem da esquerda), o pacote ARP enviado pelo tux3 quando fazemos ping 172.16.50.254 tem como endereço MAC e IP do *sender* os do tux3 (emissor) e como endereço IP do *target* o do tux4 (recetor), sendo que o endereço MAC do *target* se encontra a 00:00:00\_00:00:00 uma vez que é essa a informação que queremos obter.

De facto, na imagem da direita vemos o pacote ARP enviado como resposta ao inicial e vemos que este já contem o endereço MAC do *sender* e do *target*.

### What packets does the ping command generate?

O comando ping gera pacotes ICMP (*Internet Control Message Protocol*), sendo os mesmos usados para transferir mensagens de controlo entre endereços IP.

De facto, quando fazemos ping 172.16.50.254 no tux3 vemos que estes pacotes são enviados logo a seguir a obtermos o endereço MAC de destino (pacotes ARP). Contudo, salienta-se que o facto de nesta experiência isto ter acontecido (o envio de pacotes ARP previamente ao envio de pacotes ICMP) deve-se ao facto de o tux3 não conter na sua *ARP table* informação acerca do endereço MAC do 4. Assim sendo, se repetíssemos o ping 172.16.50.254 no tux3 apenas iremos capturar pacotes ICMP, dado já obtemos anteriormente o endereço MAC correspondente ao IP de destino.

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

Os endereços MAC e IP presentes nos pacotes ICMP são relativos quer ao dispositivo que está a realizar o ping quer ao destinatário do mesmo.

Nesta experiência ao realizar um ping do tux4 (com o endereço IP 172.16.60.254) a partir do tux3 (identificado pelo endereço IP 172.16.60.1) os endereços de origem e destino IP e MAC dos pacotes ICMP gerados vão ser os dos tuxs em questão, tux3 e tux4 respetivamente. De seguida expomos informação relativa à análise de um pacote ICMP de pedido e outro de resposta capturados nesta experiência.

### How to determine if a receiving Ethernet frame is ARP, IP, ICMP?

O tipo da trama Ethernet recebida é determinado analisando o cabeçalho presente na mesma, campo “EtherType”. Um valor de 0x0806 neste campo representa uma trama do tipo ARP e um valor de 0x0800 representa uma trama do tipo IP. Pode-se ainda verificar se estamos perante uma trama do tipo ICMP, caso se trate de uma trama IP e o seu cabeçalho contenha o valor 0x01 no campo respetivo ao protocolo.

Figuras

### How to determine the length of a receiving frame?

O comprimento de uma trama está presente na mesma e, nesta experiência, foi obtido usado o *wireshark*. Na figura podemos ver um exemplo retirado desta experiência.

### What is the loopback and why is it important?

*Loopback* é uma interface de rede virtual utilizada para realizar testes de diagnóstico (espaçados de 10 segundos). Esta interface permite ter um endereço de IP no router que está sempre ativo, não se sujeitando a uma interface física.

figura

## Experiência 2

Na experiência 2 propunha-se a configuração no switch de duas VLAN’s (LAN’s virtuais), Vlan60 e Vlan61. Para o efeito, foi ligado o tux3 (eth0) e o tux4 (eth0) à VLAN60 e o tux2 (eth0) e tux4 (eth1) à Vlan61.

### How to configure vlan60?

Configurar a vlan 60 exige ligar fisicamente a carta de rede eth0 do tux3 e a carta de rede eth1 do tux4 ao *switch.* Para esta experiência ligaremos a carta de rede eth0 do tux3 à porta 3 do *switch* e a carta de rede eth1 do tux4 à porta 4.

Depois, ligou-se através da porta série o *switch* ao tux4 para que o mesmo possa ser configurado através deste tux e executou-se os seguintes códigos no terminal da posta série.

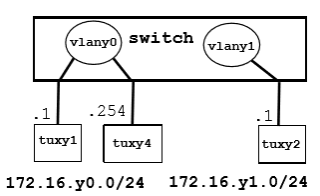
* configure terminal
* vlan 60
* end
* configure terminal
* interface fastethernet 0/(2/3) (‘2’ para a porta 2 do *switch* ‘3’ para a porta 3)
* switchport mode access
* switchport access vlan 60
* end

### How many broadcast domains are there? How can you conclude it from the logs?

Na rede configurada durante esta experiência existiam duas sub-redes distintas, ou seja, dois domínios de Broadcast também eles distintos. Estas duas sub-redes são consequência da criação das duas vlan’s (vlan60 e vlan61).

Verificou-se também que fazendo ping Broadcast (ping -b 172.16.60.255) no tux3 este recebe uma resposta apenas do tux4 (172.16.60.254) e, fazendo ping Broadcast no tux2 (ping -b 172.16.61.255) este não recebe resposta de nenhum dos restantes tux’s (está isolado na vlan na qual foi configurado)

Desta forma, os tux’s 3 e 4 estão num domínio de Broadcast diferente do domínio onde se encontra o tux2, conforme era previsto.



## Experiência 3

Na experiência 3 propunha-se a configuração e análise de um *router* em Linux.

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

**No tux1:**

* **172.16.61.0/24 via 172.16.60.254 dev eth0** – Esta rota tem como significado que qualquer comunicação com a vlan 61 será feita recorrendo ao tux4 como intermediário.
* **172.16.60.0/24 dev eth0** – significa que o tux1 está conectado à sub-rede 172.16.60.0/24 através da interface eth0.

**No tux2:**

* **172.16.60.0/24 via 172.16.61.253 dev eth0** - Esta rota tem como significado que qualquer comunicação com a vlan 60 será feita recorrendo ao tux4 como intermediário.
* **172.16.61.0/24 dev eth0** – significa que o tux2 está conectado à sub-rede 172.16.61.0/24 através da interface eth0

**No tux4:**

* **172.16.60/24 dev eth0** – significa que o tux4 está conectado à sub-rede 172.16.60.0/24 através da interface eth0
* **172.16.61.0/24 dev eth1** – significa que o tux4 está conectado à sub-rede 172.16.61.0/24 através da interface eth1

### What information does an entry of the forwarding table contain?

Na tabela de forwarding está presente a seguinte informação:

* **Destination**: indica o endereço de IP de destino de um determinado pacote
* **Gateway**: indica o endereço de IP do próximo local por onde deve passar a rota
* **Netmask**: indica a máscara de rede correspondente à rede de destino, esta informação associada ao endereço de destino permite determinar o ID da rede de destino
* **Flags**: indica informações sobre a rota (como, por exemplo, a sua disponibilidade)
* **Metric**: indica o custo de cada rota
* **Ref**: indica o número de vezes que a rota foi referenciada para estabelecer uma ligação
* **Use**: indica o número de vezes que a rota foi vista
* **Interface**: indica o nome da interface localmente utilizada pela rota

### What ARP messages, and associated MAC addresses, are observed and why? (?????)

Ao realizar um *ping* do tux1 para o tux2 este *ping* é redirecionado através do tux4. O tux 1 envia um *ARP packet* de modo a obter o endereço físico (MAC) do tux4 e, posteriormente, o tux4 envia também um pacote ARP para conhecer o endereço físico do tux2.

### What ICMP packets are observed and why? (=?????)

Exemplo

### What are the IP and MAC addresses associated to ICMP packets and why? (?????)

Os endereços IP e MAC associados com os pacotes ICMP são os endereços IP e MAC dos tux’s de origem e destino. EXEMPLO

## Experiência 4

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

Uma rota estática num router comercial é configurada acedendo á consola do mesmo e, no caso do *router* CISCO presente no laboratório onde decorreram as aulas, utilizando a seguinte lista de comandos:

* Configure terminal
* ip route [endereço ip da rota de destino] [máscara] [IP gateway]
* exit

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

O tux4 representa o router padrão para o tux1, por sua vez o *router* comercial representa o *router* padrão para o tux2 e 4. Qualquer ligação entre a vlan60 e vlan61 foi, então, realizada tendo o tux4 como intermediário (como já anteriormente acontecera). Já tentativas de ligação à rede do laboratório (172.16.1.0/24) foram redirecionadas para o *router* comercial, tal como se esperava, visto ser este o *router* padrão entre qualquer um dos tux’s da vlan 61.

### How to configure NAT in a commercial router?

Também tendo como referência o *router* utilizado nas aulas laboratoriais, o NAT foi configurado utilizando os seguintes comandos (fornecidos no guião do trabalho em questão):

* Ip nat pool ovrld 172.16.1.69 172.16.1.69 prefix 24
* Ip nat inside source list 1 pool ovrld overload
* Access-list 1 permit 172.16.60.0 0.0.0.7
* Access-list 1 permit 172.16.61.0 0.0.0.7

### What does NAT do?

O NAT (*Network Address Translation*) é responsável pela tradução de endereços privados (não globalmente únicos) de uma rede interna para endereços públicos.

Deste modo, o NAT é útil para a função de segurança, visto que, numa determinada rede privada, apenas é necessário um endereço de IP público para conectar os restantes. Escondendo, assim, todo o restante da rede privada.

## Experiência 5 (????)

Na experiência 5 proponha-se a configuração e análise do DNS (*Domain Name System*) em todos os tux’x. Um servidor DNS tem como responsabilidade armazenar os endereços IP públicos associados aos respetivos *hostnames*. É, então, utilizado para traduzir os *hostnames* para os respetivos endereços IP. No caso particular do nosso trabalho foi utilizado o servidor DNS **netlab.fe.up.pt**

### How to configure the DNS service at an host?

A configuração do servidor DNS implica alterar o ficheiro resolv.conf, presente em /etc. Este ficheiro deve passar a conter respetivamente:

* **Search netlab.fe.up.pt**
* **Nameserver 172.16.2.1**

Onde, netlab.fe.up.pt indica o nome do servidor DNS, enquanto que 172.16.2.1 indica o endereço de IP do servidor DNS em questão.

Após a realização desta mesma experiência passa a ser possível aceder à internet nos tux’s.

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

??????

## Experiência 6

Na experiência 6 propunha-se observar e analisar o comportamento do protocolo TCP, recorrendo, para tal, à aplicação desenvolvida na parte 1 do trabalho (já previamente analisada e explicada detalhadamente na parte 1 deste guião).

### How many TCP connections are opened by your ftp application?

A aplicação por nós desenvolvida abre duas ligações TCP, uma de controlo que permite enviar os comandos FTP ao servidor e receber as respetivas respostas, e outra de dados, para receber os dados do servidor.

### In what connection is transported the FTP control information?

????

### What are the phases of a TCP connection?

Uma ligação TCP pode ser divida em **3 fases.** Sendo as mesmas:

1. Estabelecimento da ligação;
2. Troca de dados;
3. Encerramento da ligação.

### How does the ARQ TCP mechanism work? What are the relevant TCP fields? What relevant information can be observed in the logs?

O protocolo TCP utiliza o mecanismo ARQ do tipo **Go-Back-N**, utilizando mensagens de confirmação (ACKs) para reconhecer quais as tramas que foram enviadas corretamente e qual é o número de sequência esperado.

### How does the TCP congestion control mechanism work? What are the relevant fields. How did the throughput of the data connection evolve along the time? Is it according the TCP congestion control mechanism?

O protocolo TCP utiliza uma janela de congestão de modo a limitar o número de bytes que podem ser enviados a cada instante. O tamanho desta janela deve ser determinado e para tal é utilizada uma estimativa resultante da análise da congestão da ligação. É para tal mecanismo implementado o algoritmo AIMD (*Additive Increase/Multiplicative Decrease*) de modo que o tamanho da janela aumente linearmente com a diminuição da congestão e que diminuía exponencialmente quando uma congestão é verificada.

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

O aparecimento de uma segunda ligação TCP pode provocar uma queda na taxa de transmissão uma vez que a taxa é distribuída de igual forma para cada ligação

Wireshark ????

# Conclusões

A realização do trabalho proposto permitiu em ambas as partes consolidar os conhecimentos teóricos acerca do protocolo FTP (*File Transfer Protocol*) e das caraterísticas de uma rede de computadores e também ganhar destreza e conhecimento prático acerca do hardware utilizado para configurar a rede de computadores no laboratório nomeadamente o *Router* e o *Switch*.

No final do mesmo, consideramos benéfico para o desenvolvimento das nossas capacidades no âmbito da unidade curricular a realização deste trabalho que foi concluído com sucesso visto que cumpriu os requisitos previamente proposto.

Contudo, numa eventual continuação do trabalho, ou caso o tempo para realizar o mesmo fosse maior, seria possível organizar o código da aplicação de download num conjunto maior de ficheiros de modo a aumentar a sua organização separando as funções em ficheiros segundo a sua funcionalidade sem que, deste modo, se aumentasse desnecessariamente a complexidade da arquitetura do mesmo (por exemplo, as funções relativas ao DNS estarem num ficheiro isolado e dedicado apenas a estas). Quanto à segunda parte do trabalho seria interessante realizar um conjunto de funções *bash* para automatizar todo o processo de configuração da rede.

Anexo 1 – Logs

Anexo 2 – Código Fonte

Anexo 3 – Códigos de Configuração