



Redes de Computadores (L.EIC025)

Relatório do 2º Trabalho Laboratorial

David dos Santos Ferreir(up202006302)

Henrique Correia Vicente(up202005321)

Dezembro 2022

Introdução

Este segundo projeto da cadeira de Redes de computadores tem como objetivo perceber o funcionamento de uma rede de computadores e saber como configurar a mesma e também entender como se faz aplicação download.

O projeto encontra-se dividido em 3 partes. Cada uma será abordada e explicada neste relatório:

Parte 1 - Aplicação de download: descrição do código que utilizamos para implementar esta aplicação e análise dos testes realizados.

Parte 2 - Configuração da rede: Análise das experiências feitas nas aulas práticas

Parte 3- Conclusão: Resumo sobre o projeto realizado e reflexão sobre os principais objetivos de aprendizagem alcançados.

Parte 1 - Aplicação de download

Esta primeira parte tem como objetivo desenvolver uma aplicação de download capaz de transferir qualquer ficheiro do servidor FTP no modo passivo.

Esta aplicação aceita como argumento um link **ftp://[<user>:<password>@]<host>/<url-path>**.

Arquitetura

O nosso grupo criou a aplicação usando apenas uma função: `main()`. Nesta função, encontra-se a implementação do código para a aplicação do download. Começamos por analisar o link para saber o user, password, host e a path do link onde está o ficheiro. Com a função `gethostbyname(host)`, foi possível saber o host name e o seu ip address respetivo e, a partir disso, conseguimos conectar com o servidor através da função `socket()`. Após a conexão, começamos a enviar comandos para o servidor, bem como as respostas obtidas.

Para prosseguir para o envio do próximo comando, temos que verificar se os códigos estão de acordo com a resposta do servidor, seguindo o RFC 959. A ordem para conseguirmos finalizar o download do ficheiro é:

- Conectar com o servidor e devolver código 220;
- Mandar user para o código ir para a continuação 331;
- Mandar a password e receber o código 230;
- Entrar no modo passivo, receber o código 227 e um IP na forma (a,b,c,d,e,f);

- Ler a resposta do modo passivo, em que obtemos um inteiro $e*256+f$, onde está a porta para a conexão com outro servidor (onde recebemos o documento);
- Enviar o retr para começar o download do ficheiro, ao receber o código 150 o ficheiro começa a ser transferido e guardamos a informação;
- Após a transferência completa e sem erro, é retornado o código 226.

Resultados

A aplicação foi testada com diversos ficheiros de diferentes tamanhos, em modo anônimo e modo não anônimo. É de referir ainda que em caso de erro ou caso não exista um ficheiro, o programa termina.

Parte 2 - Configuração da Rede

Nesta segunda parte, a finalidade trata-se de configurar a rede para permitir a execução ou de uma aplicação, através de duas bridges.

Além disso, foi realizada a configuração do router com a implementação do NAT e, por fim, do DNS.

Experiência 1 - Configurar um IP de rede

Nesta primeira experiência, é pedido para configurar os endereços de IP de dois computadores, tux 3 e tuxy4, de forma a que consigam comunicar entre si. Após configurar as portas eth0, utilizamos o comando ping para verificar a ligação entre os computadores.

O que são os pacotes ARP e para que servem?

O ARP (Address Resolution Protocol) é um protocolo utilizado para mapear endereços da camada de rede (endereços IP) em endereços Ethernet. Desta forma, este serve para encontrar o endereço da camada de ligação associado ao endereço IPv4.

Quais são os endereços MAC e IP dos pacotes ARP e porquê?

Como origem, os pacotes ARP possuem um IP/MAC que já se encontra definido. Os endereços MAC identificam as placas de rede e os endereços IP funcionam como identificadores públicos.

Quais pacotes o comando ping gera?

O comando ping gera pacotes ARP, com o objetivo de obter os endereços MAC e, assim, gerar pacotes ICMP (Internet Control Message Protocol). Assim, podemos testar a conectividade entre o tuxy3 e o tuxy4.

Quais são os endereços MAC e IP dos pacotes de ping?

Na tabela, encontram-se os endereços dos pacotes ping. Verificou-se que os pacotes ICMP utilizam os endereços MAC adquiridos pelo protocolo ARP.

Como determinar se uma Ethernet frame de recebimento é ARP, IP, ICMP?

Para diferenciar os pacotes ARP, IP e ICMP, é necessário analisar o cabeçalho da trama Ethernet. Por exemplo, se o valor for 0x0806 corresponde às tramas do tipo ARP e, caso seja 0x0800, representa um pacote de tipo IP, sendo possível analisar o IP header. Por sua vez, se o valor for 1, estamos presente um protocolo do tipo ICMP.

Como determinar o comprimento de uma frame de recepção?

Para determinar o tamanho de uma trama, verificamos os pacotes IP, pois estes possuem informação sobre o seu tamanho.

O que é a interface de loopback e por que ela é importante?

A interface de rede virtual loopback comporta-se como um canal de comunicação e realiza testes de conectividade de 10 em 10 segundos, para verificar a ligação. Este procedimento é importante, uma vez que permite que dois computadores se comuniquem entre si, através da configuração dos endereços IP.

Experiência 2 - Configurar duas Bridges virtuais

Nesta experiência o objetivo será configurar duas bridges no switch, uma chamada bridgey0 e outra bridgey1. Bridge é um dispositivo de rede de computadores que cria uma única rede agregada a partir de várias redes de comunicação ou segmentos de rede.

Como configurar a Bridgey0?

Para configurar a bridge, começamos por criar a mesma e estabelecer ligações físicas entre as portas do switch e os computadores, que tencionamos fazer parte desta.

Para isso, são utilizados os seguintes comandos no GtkTerm do tux a configurar:

```
/interface bridge remove bridge20  
/interface bridge remove bridge21
```

```
/interface bridge add name=bridge20  
/interface bridge add name=bridge21
```

```
/interface bridge port remove [find interface eth6)
```

```
/interface bridge port add bridge=bridge20 interface=eth0  
/interface bridge port add bridge=bridge21 interface=eth1
```

Quantos domínios de broadcast existem? Como podemos concluir isso a partir dos logs?

Quando configuramos as Bridge's, invocamos o comando ping a partir de ambos os tuxes. Através dos logs, analisamos que o tuxy4 obteve resposta ao ping broadcast a partir do tuxy3, mas que o tux 2 não recebeu nenhuma resposta.

Experiência 3 - Configurar router in Linux (Lab)

Nesta experiência, aplica-se a configuração ao testada na experiência anterior e testa-se a mesma em ambiente laboratório, para fazer esta experiência precisamos antes de tudo usar dois comandos: o **primeiro** para ativar o encaminhamento do ip no computador do router, neste caso o tuxy4. O **segundo** para desativar o ICMP para ignorar os broadcasts.

Enable IP forwarding on tux14
echo 1 > /proc/sys/net/ipv4/ip-forward

O passo seguinte passo por adicionar rotas para conseguirmos passar a informação do tuxy2 para tuxy3 para isso vamos usar os **seguintes comandos**:

Add route to 172.16.11.0/24 on tux13 (route -n)

route add default gw 172.16.Y0.254

Add route to 172.16.10.0/24 on tux12 (route -n)

route add default gw 172.16.Y1.253

Que rotas existem nos tuxes? Quais são os seus significados?

Na tabela abaixo, encontram-se as rotas existentes em cada tux, sendo que o destino de cada rota diz respeito ao alcance desta.

	Rota para a	Gateway	Rota para a	Gateway
--	-------------	---------	-------------	---------

	bridgey0		bridgey1	
tux2	172.16.y0.0	172.16.y1.253	172.16.y1.0	172.16.y1.1
tux3	172.16.y0.0	172.16.y0.1	172.16.y1.0	172.16.y0.254
tux4	172.16.y0.0	172.16.y0.254	172.16.y1.0	172.16.y1.253

Que informações contém uma entrada da tabela de encaminhamento?

Uma entrada da tabela de encaminhamento possui informações sobre Destination (o destino da rota), Gateway (o IP do próximo ponto a passar pela rota), Metric (o custo de cada rota), Netmask (máscara que determina o ID da rede), Ref (número de referências para a rota), Use (conta as pesquisas pela rota) e Interface (placa de rede disponível pela gateway).

Quais mensagens ARP e endereços MAC associados são observados e porquê?

Se utilizarmos o comando ping, podemos analisar as mensagens ARP, que expõem o pedido de mapeamento do endereço de rede para um endereço físico (MAC). O endereço pedido é o da gateway, uma vez que é para esta que terão de enviar a informação para, de seguida, ela encaminhar para o destino final.

Quais pacotes ICMP são observados e porquê?

Os pacotes ICMP de request e reply são observados entre todos os pares de tuxes, uma vez que foram adicionadas rotas que permitem que todos eles consigam atingir os outros. Se não conseguissem alcançar, os pacotes ICMP não chegariam ao destino.

Quais são os endereços IP e MAC associados aos pacotes ICMP e porquê?

Os endereços IP e MAC do tux de origem e do de destino estão associados aos pacotes ICMP, isto ocorreu quando o tux de destino se tornou alcançável e caso o MAC esteja mapeado.

Experiência 4 - Configurar um Router Comercial e implementar uma NAT

Nesta quarta experiência, passa por estabelecer uma ligação com a rede dos laboratórios e implementar rotas num router comercial, com NAT implementado. Foi também configurado o DNS, para poder aceder a redes externas.

Como configurar uma rota estática num router comercial?

Antes de começar a configuração, é necessário ligar a porta ether1 à porta do router da ether2. De seguida, utiliza-se os seguintes comandos:

```
/ip address add address=172.16.1.29/24 interface=ether1  
/ip address add address=172.16.21.254/24 interface=ether2
```

Quais são os caminhos seguidos pelos pacotes nos experimentos realizados e porquê?

Caso a rota exista, os pacotes usam-na durante a experiência. Se não, os pacotes dirigem-se ao router, a rota por default, este informa que o tux existe e envia as informações pelo mesmo

Como configurar o NAT no router comercial?

Para a configuração do NAT, apenas inserimos, no GtkTerm, os comandos fornecidos.

O que faz o NAT?

O NAT (Network Address Translation) consiste num mecanismo implementado em routers, que trata de substituir os endereços IP locais nos pacotes por um endereço IP público. Assim, possibilita a comunicação entre computadores da rede criada com redes externas.

Experiência 5 - DNS

Nesta quinta experiência, temos como tarefa aprender como configurar o DNS.

Como configurar o serviço DNS num host?

Para configurar o serviço DNS, necessitamos de alterar os parâmetros no ficheiro resolv.config, em todos os hosts da rede criada.

Depois de termos o DNS configurado, os pacotes relativos ao DNS nos logs já estarão disponíveis.

Que pacotes são trocados pelo DNS e que informações são transportadas?

Quanto aos pacotes, o host trata de enviar um pacote, que tem associado um hostname, para o servidor, sendo que o servidor responde com um pacote que contém o endereço IP pretendido.

Exp 6 – TCP connections

Nesta experiência, o objetivo foi a observação do funcionamento e comportamento do protocolo TCP, sendo para isso utilizada a aplicação desenvolvida anteriormente.

Principais comandos: Compilação e execução da aplicação criada anteriormente.

Quantas conexões TCP são abertas pelo seu aplicativo ftp?

São abertas duas conexões TCP pela aplicação, uma quando se entra em contacto com o servidor e através da qual se envia e recebe comandos para preparar a transferência do cheiro, e outra para fazer a transferência do cheiro em si.

Em que conexão é transportada a informação de controle do FTP??

O controlo de informação é transportado na primeira conexão TCP (na que trata do envio e receção de comandos).

Quais são as fases de uma conexão TCP?

Numa conexão TCP, primeiro estabelece-se a conexão, depois ocorre a troca de dados, e depois a conexão é encerrada, havendo assim três fases.

Como funciona o mecanismo ARQ TCP? Quais são os campos TCP relevantes? Quais informações relevantes podem ser observadas nos logs?

O mecanismo ARQ TCP funciona através do método da janela deslizante, que consiste no controle de erros na transmissão de dados. Para este efeito, são utilizados números de confirmação, que indicam o correto recebimento da trama, tamanho da janela, que indica a gama de pacotes recebidos, e uma sequência de números, que é o número do pacote a ser enviado.

Como funciona o mecanismo de controle de congestionamento do TCP? Quais são os campos relevantes. Como evoluiu o throughput da conexão de dados ao longo do tempo?

O mecanismo de controlo de congestão do TCP tem como base os ACKs recebidos na transmissão de pacotes. Estes são o source clock da transmissão. É utilizada uma nova variável/valor por conexão, denominada **CongestionWindow**, de modo a regular o tamanho da janela deslizante de transmissão de pacotes tendo em conta a congestão da conexão. Este valor é regulado, incrementando se a congestão da rede diminui e decrementa se a congestão da rede aumenta. Isto é normalmente feito incrementando **CongestionWindow** por 1, a cada RTT (round trip time). Quando se deteta que um pacote é perdido (normalmente isso é detetado quando ocorre um timeout, ou quando se recebe 3 ACKs duplicados), o valor de CongestionWindow passa para metade. O bitrate da conexão será aproximadamente igual a **CongestionWindow**.

No início da conexão, pode também haver uma fase de início lento, que serve para, de modo a delimitar um limite que é depois utilizado numa fase posterior de congestion avoidance. Foi registado que, quando o primeiro download, no tuxy1, começou, a taxa de transmissão aumentou rapidamente, tendo depois chegado a um pico alguns segundos depois. Após o início do segundo download, no tuxy2, a taxa de transmissão no tuxy1 diminuiu rapidamente e a do tuxy2 aumentou também rapidamente, e passado alguns "altos e baixos", o throughput estabilizou relativamente num nível mais baixo do que era anteriormente, antes do segundo download ter começado.

Está de acordo com o mecanismo de controle de congestionamento do TCP?

As mudanças referidas anteriormente fazem sentido e estão de acordo com o mecanismo de controlo de congestão do TCP, uma vez que quando circulavam na rede menos pacotes (apenas um download a ser feito), o bitrate para a conexão do tuxy1 é mais alto do que quando os dois downloads estavam a ser feitos ao mesmo tempo, o que aumenta o congestionamento da rede. É possível observar um gráfico que demonstra o que foi explicado, nos anexos.

A taxa de transferência de uma conexão de dados TCP é perturbada pelo aparecimento de uma segunda conexão TCP? Quanto?

Sim. A taxa de transmissão de pacotes da conexão TCP que já estava iniciada diminui, uma vez que a outra conexão foi atribuída uma capacidade para a transmissão de pacotes na mesma, de modo a que a taxa de transferência seja distribuída de igual forma para cada ligação.

Parte 3 - Conclusão

Após este projeto realizado conseguimos fazer a conexão à internet no tuxy3, tal como era pedido. Os objetivos propostos deste projeto foram cumpridos, sendo que permitiram perceber como funcionam as transferências por FTP e o próprio protocolo. Além disso, foram consolidados os conceitos referentes às funcionalidades dos equipamentos de redes e o seu funcionamento.