

2º Trabalho Laboratorial

Computer Networks

**Grupo G04T12**

João António Maricato Malva - UP202006605

Martim Raúl da Rocha Henriques - UP202004421

Redes de Computadores, 22/23

[Parte 1 - Aplicação de Download 3](#_Toc122554796)

[Parte 2 - Análise e Configuração da Rede 4](#_Toc122554797)

[Exp 1 - Configuração do IP 4](#_Toc122554798)

[Exp 2 - Implementação de 2 bridges num switch 5](#_Toc122554799)

[Exp 4 - Configuração de um Router e implementação da NAT 6](#_Toc122554800)

[Exp 5 - DNS 6](#_Toc122554801)

[Exp 6 - Conexões TCP 7](#_Toc122554802)

[Conclusão 7](#_Toc122554803)

# Parte 1 - Aplicação de Download

A aplicação de download de ficheiros (FTP) utiliza a biblioteca padrão do sistema para se conectar a um servidor FTP e fazer o download de um ficheiro específico. A estrutura geral da aplicação é a seguinte:

1. O programa começa lendo o URL do ficheiro a descarregar como argumento da linha de comando.
2. O URL é dividido em duas partes: o caminho do URL e o caminho do ficheiro no servidor. O caminho do URL é dividido em três partes: utilizador, palavra-passe e host.
3. O programa então tenta se ligar ao servidor FTP especificado no URL, utilizando o endereço IP do host e a porta padrão de FTP (21). Se a ligação for bem-sucedida, o programa envia o comando USER e a palavra-passe para o servidor.
4. Se a autenticação for bem-sucedida, o programa envia o comando PASV para solicitar ao servidor um modo passivo de transferência de dados. Em seguida, o programa envia o comando RETR para solicitar o ficheiro especificado no caminho do ficheiro.
5. O servidor começa a enviar o ficheiro para o cliente, que o armazena num ficheiro local. Quando o ficheiro é totalmente transferido, o programa envia o comando QUIT para encerrar a ligação com o servidor.
6. O programa termina a execução e exibe uma mensagem de sucesso ou de falha para o utilizador, dependendo do resultado da transferência de ficheiro.

O download de um ficheiro de um servidor FTP é um processo que envolve a conexão a um servidor FTP, autenticação com o nome de utilizador e palavra-passe, navegação pelos diretórios do servidor para encontrar o ficheiro desejado e, finalmente, transferir o arquivo para o computador local.

# Parte 2 - Análise e Configuração da Rede

## Exp 1 - Configuração do IP

Esta experiência tem como objetivo dar a conhecer aos estudantes o ambiente de configuração e análise de rede, percebendo melhor os conceitos de IP, MAC e ARP.

Ao usar o Wireshark para inspecionar pacotes ARP, foi possível identificar a relação entre os endereços de origem e de destino, bem como constatar que o endereço MAC de destino contém o valor 0.0.0.0 no envio de um pacote ARP request e que esse valor é substituído pelo verdadeiro endereço MAC na recepção do pacote ARP response. Isso nos permitiu entender que o ARP é usado para descobrir o endereço MAC correspondente a um determinado endereço IP.

T Também foi possível estudar a relação entre o utilitário ping e o Internet Control Message Protocol (ICMP) e verificar a função desse protocolo no diagnóstico de possíveis erros na rede. Além disso, conseguimos reconhecer os diferentes valores no campo EtherType das tramas Ethernet, que permitem distinguir entre os diferentes protocolos e entender a ligação entre o tamanho do cabeçalho, dos dados e de verificação da trama e o tamanho total da trama.

Por fim, foi possível compreender a finalidade da interface loopback e observar sua utilidade na detecção de erros de configuração da rede e na comunicação entre dois processos de um mesmo dispositivo.

Em resumo, esta experiência nos permitiu entender melhor os conceitos de IP, MAC e ARP e como esses protocolos são usados para permitir que dispositivos se comuniquem uns com os outros em uma rede.

O ARP (Address Resolution Protocol) é um protocolo de camada de rede que permite a uma máquina descobrir o endereço MAC de outra máquina a partir do seu endereço IP. Isso é necessário porque as máquinas na rede usam endereços MAC para se comunicarem entre si na camada de ligação de dados, enquanto que os endereços IP são usados na camada de rede. Quando uma máquina quer enviar um pacote para outra máquina, ela precisa saber o endereço MAC da máquina de destino para poder enviar o pacote corretamente. Para descobrir o endereço MAC, a máquina envia um pacote ARP request, que é um pacote especial contendo o endereço IP da máquina de destino e um endereço MAC de destino especial conhecido como "0.0.0.0". Quando o pacote ARP request é recebido pela máquina de destino, ela responde com um pacote ARP response, que contém o seu próprio endereço MAC. A máquina que enviou o pacote ARP request então armazena o endereço MAC da máquina de destino em sua tabela ARP para uso futuro e pode enviar pacotes diretamente para a máquina de destino usando o endereço MAC.

O ping é usado para testar a conectividade entre duas máquinas na rede. Ele envia pacotes ICMP (Internet Control Message Protocol) para a máquina de destino e aguarda uma resposta. Se a máquina de destino responder, isso significa que ela está conectada e a conexão na rede está funcionando corretamente. Se a máquina de destino não responder, isso pode ser um indicativo de um problema na rede ou na configuração das máquinas.

As tramas Ethernet são quadros de dados que são enviados entre máquinas na rede. Elas têm um cabeçalho de 14 bytes que inclui informações como o endereço MAC de origem e de destino e o EtherType, que indica qual protocolo os dados no quadro seguem. A parte dos dados da trama pode ter tamanho variável, dependendo do protocolo específico, e há também um campo de verificação de 4 bytes no final da trama.

A interface de loopback é uma interface virtual usada para comunicação entre dois processos em uma mesma máquina. Ela é usada como uma forma de testar a configuração de rede de uma máquina, pois qualquer tráfego enviado para ela é imediatamente reenviado de volta para a stack de rede como se fosse tráfego proveniente do exterior. Isso permite que os processos na máquina possam se comunicar entre si como se estivessem em redes diferentes, o que é útil para testes e depuração.

## Exp 2 - Implementação de 2 bridges num switch

Para configurar a bridgeY0, é necessário seguir os seguintes passos:

* Conectar as portas de rede dos dispositivos que você deseja incluir na bridgeY0 a uma porta da switch.
* Acessar a interface de configuração da switch através do terminal.
* Criar uma nova bridgeY0.
* Adicionar as portas da switch que você deseja incluir na bridgeY0 a ela.
* Atribuir endereços IP e sub-rede à bridgeY0.

Há dois broadcast domains na rede. Isso pode ser concluído a partir dos logs, observando que os pings broadcast só são respondidos entre os tuxY3 e tuxY4, que estão no mesmo domínio de transmissão. O tuxY2, que está em outro domínio de transmissão, não responde aos pings broadcast.

Exp 3 - Configuração de um Router em Linux

As rotas nos tuxs são as rotas estáticas que foram configuradas para permitir a comunicação entre as bridges. As rotas permitem que os pacotes de dados sejam encaminhados para o destino correto através do router (tuxY4). As rotas contêm informações sobre o prefixo de destino e a máscara de sub-rede, bem como o endereço de próximo salto (gateway) a ser usado para chegar ao destino.

A tabela de encaminhamento contém entradas que especificam para onde os pacotes devem ser encaminhados, dependendo do endereço de destino. Cada entrada contém o endereço de destino, a máscara de sub-rede, o endereço de próximo salto e a interface de saída a ser usada para enviar o pacote.

As mensagens ARP (Address Resolution Protocol) são observadas quando os dispositivos precisam resolver o endereço MAC de outro dispositivo na rede. Essas mensagens são enviadas para obter o endereço MAC de um determinado endereço IP. Os endereços MAC associados a essas mensagens são os endereços MAC dos dispositivos que estão sendo buscados.

Os pacotes ICMP (Internet Control Message Protocol) são observados quando os dispositivos precisam enviar mensagens de controle, como ping ou traceroute. Os pacotes ICMP são enviados para testar a conectividade ou para rastrear o caminho de um pacote de dados através da rede. Os endereços IP e MAC associados a esses pacotes são os endereços dos dispositivos que estão enviando e recebendo os pacotes.

Os endereços IP e MAC associados a pacotes ICMP são os endereços dos dispositivos que estão enviando e recebendo os pacotes. O endereço IP é usado para identificar o dispositivo na rede e o endereço MAC é usado para identificar o dispositivo na camada de enlace de dados (que lida com a comunicação entre dispositivos na mesma rede física).

## Exp 4 - Configuração de um Router e implementação da NAT

Para configurar uma rota estática em um router comercial, é necessário acessar o prompt de comando do router. Esse comando permite adicionar uma rota específica à tabela de encaminhamento do router.

Os pacotes seguem os caminhos especificados pelas rotas configuradas no router. No caso da experiência descrita, os pacotes provenientes do tux3 são encaminhados para o tux4, que os encaminha para o router e os pacotes provenientes do router e do tux2 são encaminhados para o tux3. Esses caminhos são escolhidos pelo router de acordo com as rotas especificadas para cada endereço de destino.

NAT (Network Address Translation) é um mecanismo que permite que os dispositivos da rede privada usem endereços IP públicos para se comunicar com o exterior. Isso é útil porque a gama de endereços IP públicos é muito maior do que a gama de endereços IP privados, o que permite que mais dispositivos se conectem à Internet. O NAT também ajuda a proteger a rede privada, pois oculta os endereços IP privados dos dispositivos e os substitui por endereços IP públicos.

## Exp 5 - DNS

Para configurar o serviço DNS em um host, é necessário editar o arquivo de configuração /etc/resolv.conf.

Os pacotes DNS são utilizados para resolver nomes em endereços IP. Quando um host quer se comunicar com outro host usando um nome, como [www.google.com](http://www.google.com/), ele envia um pacote DNS solicitando o endereço IP correspondente. O servidor DNS envia de volta um pacote com o endereço IP, permitindo que o host inicial se comunique com o host de destino. Os pacotes DNS usam o protocolo UDP para serem transmitidos, o que os torna rápidos, mas não confiáveis, já que não há confirmação de recebimento. Os pacotes DNS transportam informações como o nome solicitado, o endereço IP correspondente e o tipo de registro.

## Exp 6 - Conexões TCP

O protocolo FTP utiliza duas ligações entre o cliente e o servidor: uma ligação de comando para enviar comandos e receber respostas e uma ligação de dados para transferir ficheiros. Tanto a ligação de comando como a ligação de dados são implementadas através da mesma ligação TCP, usando o mesmo socket.

No protocolo FTP, as informações de controlo (ou seja, comandos e respostas) são transmitidas através da ligação de comando. A ligação de comando é usada para estabelecer a ligação, fazer login e trocar comandos e respostas FTP entre o cliente e o servidor.

Uma ligação TCP passa pelas seguintes fases:

* Configuração da ligação
* Transferência de dados
* Terminação da ligação

ARQ (Automatic Repeat reQuest, ou Pedido de Repetição Automática) é um mecanismo utilizado pelo TCP para garantir a transmissão fiável de dados através de uma rede instável. Funciona adicionando um número de sequência a cada segmento TCP e exigindo que o lado receptor envie uma mensagem de confirmação (ACK) de volta para o remetente para cada segmento recebido.

O TCP utiliza um mecanismo de controlo de congestão para ajustar a velocidade com que envia dados para a rede em resposta a alterações nas condições da rede. O objetivo do controlo de congestão é evitar a sobrecarga da rede e garantir que todos os dispositivos na rede tenham uma parte justa da largura de banda disponível.

Quando existem múltiplas ligações TCP a competir pelos mesmos recursos de rede, o mecanismo de controlo de congestão TCP trabalha para garantir que cada ligação receba uma parte justa da largura de banda disponível. A janela de congestão e o limiar de arranque lento são ajustados com base nas mensagens de confirmação recebidas pelo receptor e nas condições da rede.

# Conclusão

Em conclusão, este projeto foi uma oportunidade valiosa para compreender os conceitos teóricos relacionados com o protocolo FTP, a programação de sockets e a configuração de uma rede de computadores. A implementação de uma aplicação de transferência usando o protocolo FTP foi um desafio, mas as experiências realizadas nas aulas foram úteis para compreender os mecanismos que regem a organização de redes e sub-redes e o encaminhamento de pacotes de uma forma mais prática. Esta compreensão foi fundamental para solidificar os conhecimentos adquiridos e preparar-nos para futuros desafios.