UNIVERSIDADE LUSÓFONA

Redes de Computadores

DNS e SMTP

Universidade Lusófona de Humanidades e Tecnologias

Licenciatura em Engenharia Informática / Engenharia Informática, Redes e Telecomunicações
Docente: Miguel Tavares, Pedro Sá da Costa

Objetivo do trabalho

A presente ficha é de natureza prática e tem por objetivo explorar alguns aspetos de duas aplicações de grande importância: o DNS e o correio eletrónico.

Domain Name System

O DNS é uma base de dados distribuída contendo informação de mapeamento entre nomes de domínio e informação relativa a esses domínios. É também um protocolo de aplicação que permite a comunicação entre clientes e servidores. O DNS define o processo de interrogação e atualização da base de dados, os mecanismos de replicação da informação entre servidores e a organização da informação na base de dados.

Para compreender o funcionamento do DNS é necessário descrever o serviço nestas duas perspetivas - a comunicação entre clientes e servidores, e o modo como se organiza a informação sob a forma de base de dados distribuída.

Tal como o WWW e o correio eletrónico, o DNS opera com base no modelo cliente-servidor, onde um cliente é qualquer equipamento que necessita de conhecer informação contida no DNS, por exemplo, um endereço IP correspondente a um nome. A um pedido de acesso à informação do DNS, dá-se o nome do 'Query'. Para um computador cliente interrogar um servidor, necessita de um 'Resolver', ou seja, de um conjunto de rotinas ou processo a que uma aplicação do utilizador recorre para obter a tradução do nome em endereço IP e que constitui o verdadeiro cliente do serviço.

Os servidores de nomes ('Name Servers') implementam uma base de dados distribuída, que armazena os registos de correspondência entre nomes e endereços IP, assim como outra informação necessária ao funcionamento ao serviço e à implementação de todas as funcionalidades. A informação relativa aos dados dos domínios designa-se por 'zona' e é armazenada num conjunto de ficheiros referidos como ficheiros de zona, que incluem diversos tipos de 'resource records' (RR). Através destes registos são definidos os mapeamentos entre nomes e endereços, assim como os restantes dados do domínio.

Os RR mais frequentes são:

Tipo de RR	Descrição
SoA	Start of Authority – indica o início de conjunto de dados sobre o qual o servidor tem autoridade.
NS	Name Server – lista os servidores de nomes da zona
A	Address – define uma correspondência entre um nome e endereço
PTR	Pointer Record – define uma correspondência entre um endereço e um nome
CNAME	Canonical Name – indica o nome real (canonical) correspondente a um nome alternativo (alias)

Geralmente, os servidores de nomes são equipamentos com sistema operativo UNIX que executam o software "Berkeley Internet Name Domain" (BIND). As plataformas de servidor Microsoft incluem software que permite a implementação de servidores de nomes.

A comunicação entre clientes e servidores de nomes recorre ao protocolo de aplicação designado por DNS, que utiliza o porto 53 e os protocolos de transporte TCP e UDP. O porto 53, em TCP, é também usado para transferências de ficheiros de dados relativos ao espaço de nomeação (zonas) entre servidores de nomes.

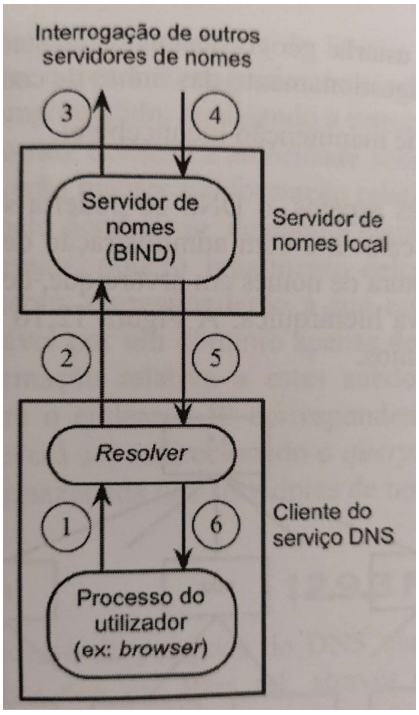

Figura 1: Diálogo entre cliente e servidor de nomes.

A comunicação entre o cliente e o servidor está ilustrada na Figura 1. Quando um processo do utilizador, por exemplo um browser, interroga o *resolver* sobre o endereço IP correspondente a um determinado nome (1).

O *resolver* pede esta informação ao servidor de nomes mais próximo, conhecido pela configuração de TCP/IP do cliente (2). Este servidor de nomes, não conhecendo o endereço IP do nome solicitado, interroga outros servidores de nomes (3). O servidor de nomes local, após receber o endereço IP correspondente ao nome solicitado (4), devolve o resultado do *query* ao *resolver* (5). Finalmente, o resolver envia o endereço IP à aplicação do utilizador (6).

Estrutura do espaço de nomeação

É importante descrever o DNS como repositório de informação que contém todas as correspondências entre nomes e endereços IP de todos os computadores na Internet – ou seja, como repositório do "Espaço de Nomeação de Domínios" (*Domain Name Space*).

Além do protocolo de comunicação entre clientes e servidores de nomes, o DNS enquadra também um espaço de nomeação, onde cada dispositivo na rede está associado a um único nome. Este nome pode ser utilizado quer por utilizadores, quer por aplicações para identificar o dispositivo, em alternativa ao respetivo IP.

Este espaço de nomeação constitui um vasto e importante repositório de informação, que define todas as correspondências entre nomes e endereços de dispositivos acessíveis na Internet. Sempre que um equipamento pretende estabelecer uma ligação com outro dispositivo usando o nome, será necessária uma consulta prévia ao espaço de nomeação para obter o endereço IP.

Tendo em conta a dependência de todos os serviços da Internet relativamente ao DNS, o volume de informação a gerir e o número de pedidos de tradução de nomes em endereços, facilmente se poderá concluir que uma implementação simplista baseada num único servidor de nomes seria totalmente inviável.

Para responder a estes aspetos, o DNS só poderia ser implementado como uma base de dados distribuída, escalável e com administração descentralizada, para o que foi necessário desenhar uma estrutura de nomes em árvore que, de algum modo, correspondesse a uma estrutura administrativa hierárquica.

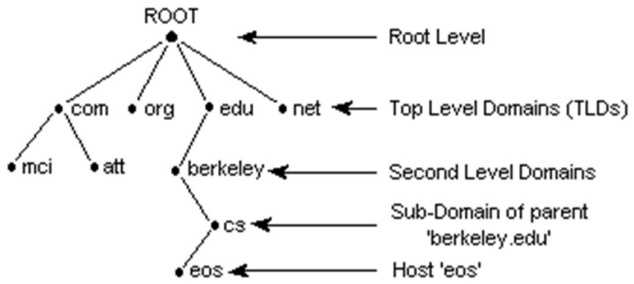

Figura 2: Fragmento do espaço de nomeação de domínios

Cada ramo desta árvore corresponde a um domínio que pode ramificar-se em subdomínios. A cada organização é atribuída autoridade sobre uma parte do espaço de nomeação, ficando responsável pela sua administração, subdivisão e atribuição de nomes dentro desse espaço. A informação relativa a um domínio é armazenada nos respetivos servidores de nomes.

Cada domínio tem um nome único, dependente da sua posição na árvore. O *Fully Qualified Domain Name* (FQDN) de um computador inclui o nome do computador e os nomes de todos os subdomínios até à raiz, separados por ".". No FQDN podem ser utilizados os carateres a-z, A-Z, 0-9, o sinal "-" e "." Como separador entre nomes de domínios. Note-se que não é feita a distinção entre maiúsculas e minúsculas.

O nó de nível mais elevado é a raiz (root domain) e representa-se por ".". Na figura, os domínios *com*, *edu*, *org* são subdomínios da raiz; *att* é subdomínio de *com.* A gestão da raiz do DNS está a cargo de uma autoridade de registo de nomes que delega a responsabilidade

administrativa de partes do espaço de nomeação. Os subdomínios da raiz são designados por domínios de topo (*Top Level Domain – TLD*).

Como já se referiu, um dos objetivos principais do DNS é permitir uma administração descentralizada da informação, o que é conseguido através da **delegação de autoridade**. O domínio raiz delegou a autoridade sobre os domínios *com*, *edu* em organizações que deverão manter a informação relativa a estes domínios. Por sua vez, a entidade responsável pelo domínio *com* delegou à entidade responsável pelo domínio *att* autoridade sobre esse domínio. Esta entidade, se o desejar, poderá igualmente delegar autoridade sobre outros subdomínios que corresponderão à estrutura administrativa. Deste *modo*, uma entidade responsável por um domínio apenas deverá manter referências para os pontos que contém informação relativa a estes subdomínios. Assim, quando um servidor for interrogado sobre o endereço IP correspondente a um determinado nome, saberá informar para onde deverá ser redirecionado o *query*. A informação de delegação de subdomínios é armazenada nos servidores de nomes.

Resolução de Nomes

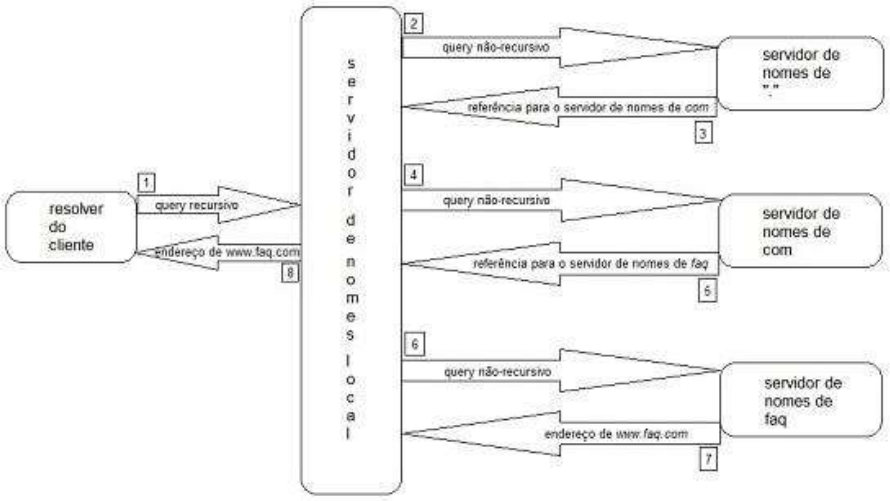

Figura 3: Pesquisa hierárquica do DNS

A Figura 3 ilustra o processo de pesquisa do DNS quando um computador cliente pretende resolver o nome www.faq.com. Para tal, através do *resolver,* solicita-se ao servidor de nomes a execução desta tarefa (1). O servidor de nomes do cliente verifica que www.faq.com não faz parte do seu domínio e interroga o servidor de nomes da raiz (2). Este desconhece o endereço IP do *query* mas tem uma referência para o servidor de nomes do subdomínio *com*, que devolve ao servidor de nomes do cliente (3). Este pode interrogar o servidor de nomes com sobre o endereço IP de www.faq.com (4), e obter uma referência para o servidor de nomes de *faq.com* que devolve ao servidor de nomes local (5). Este interroga finalmente o servidor de *faq.com* (6) que pode resolver o endereço pretendido (7). Termina assim o processo de resolução e o servidor de nomes local devolve ao cliente o endereço IP correspondente ao nome solicitado.

Note-se que o servidor de nomes local (definido na configuração TCP/IP do cliente), após receber um *query* do *resolver* no sistema cliente, executa todo o trabalho de resolução do nome, trabalho este que termina com a devolução do endereço ao *resolver*.

No entanto, os outros servidores não se comportam do mesmo modo. De facto, estes, ao receberem um *query* do servidor de nomes do cliente, limitam-se a responder com uma referência para um outro servidor de nomes que melhor possa responder ao pedido. O servidor de nomes contido nesta referência será, então, interrogado pelo servidor de nomes do cliente.

Diz-se que o servidor de nomes do cliente aceitou um *query recursivo* do *resolver* e formulou *queries não-recursivos* (ou *iterativos*) aos outros servidores de nomes.

Assim, conclui-se que quando um servidor de nomes aceita um *query recursivo* fica obrigado a responder com os dados solicitados (ou com uma mensagem de erro indicando que não conseguiu resolver o pedido) e, deste modo, assumir todo o trabalho de localização no espaço de nomeação da informação solicitada. Quando um servidor de nomes recebe um *query não-recursivo*, apenas responde com a informação de que dispõe, isto é, com uma referência para outro servidor de nomes mais próximo da informação pretendida.

As atuais implementações de BIND, por defeito, aceitam pedidos recursivos, mas interrogam outros servidores de nomes de forma não-recursiva, para que estes não tenham que suportar um processamento que é da sua responsabilidade.

Os servidores de nomes sujeitos a um elevado número de pedidos, como é o caso dos servidores da raiz do espaço de nomeação de domínios, são configurados de modo a não aceitarem pedidos recursivos, pelo que as suas respostas são baseadas na informação local de que dispõem, geralmente, uma referência para outros servidores de nomes mais próximos da informação solicitada no pedido.

Resolução de endereços

Até aqui apenas foi referida a resolução de nomes de computadores em endereços IP. Contudo, o processo inverso, isto é, a resolução de endereços IP em nomes de computadores, é frequentemente utilizado, não só em mecanismos de autenticação, como também em situações em que pode ter interesse conhecer o nome correspondente a um endereço IP registado num ficheiro de *log*.

Para conseguir uma resolução de endereços em nomes de modo simples e eficaz, foi criado um subdomínio da raiz do espaço de nomeação – “in-addr.arpa”- que é estruturado com os números que constituem os endereços IP.

O domínio “in-addr.arpa” pode ter 254 subdomínios correspondentes aos valores possíveis no primeiro *byte* de um endereço IP. Cada um destes subdomínios pode ter outros 254 subdomínios igualmente correspondentes aos valores dos restantes *bytes* do endereço. Deste modo, é possível incluir todos os endereços IP disponíveis nernet.

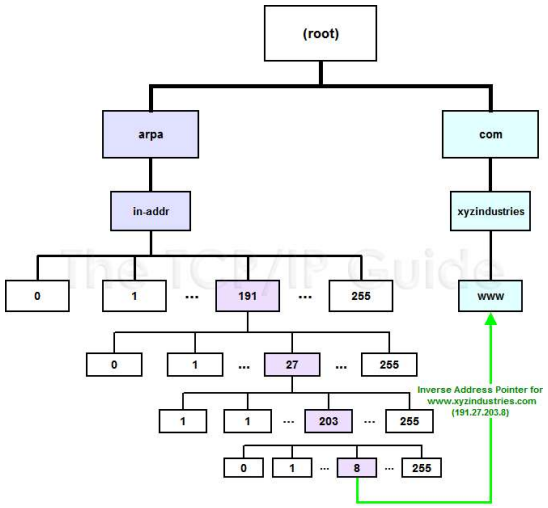

Figura 4: Domínio in-addr.arpa

Considere-se então um computador www.xyzindustries.com com o IP 191.27.203.8. Percorrendo a árvore do mesmo modo que na resolução de nomes em endereços, verifica-se que o FQDN correspondente ao endereço deste computador será *8.203.27.191.in-addr.arpa.*, ou seja, o endereço IP aparece em sentido inverso, com o *byte* menos significativo à direita. O registo no servidor de nomes deverá ser feito neste mesmo sentido. Assim, o servidor de nomes da instituição detentora da rede 191.27.203.8/24 manterá informação relativa à zona *0.203.27.191.in-addr.arpa.*, onde será indicado que, ao domínio *8.203.27.191.in-addr.arpa.* corresponde o nome www.xyzindustriues.com.

Daqui se pode concluir que a informação de mapeamento entre nomes e endereços de IP é de grande importância e é necessário a integridade desta informação.

Serviços adicionais ao DNS

Além da tradução de nomes em endereços IP, um servidor de nomes pode ainda disponibilizar um conjunto de outras funcionalidades de suporte a outras aplicações de rede. Entre estas, devem referir-se a atribuição de nomes alternativos, o encaminhamento e autenticação de correio eletrónico, o balanceamento de carga e o mapeamento de números de telefone (*Telephone Number Mapping* – ENUM).

A atribuição de um nome canónico de um computador a um endereço é feita através de RR do tipo A. Frequentemente, por este nome não ser fácil de se memorizar, necessário atribuir um nome alternativo (alias) a esse computador. Esta funcionalidade pode ser conseguida através de registos do tipo CNAME.

O campo *owner* do CNAME indica o nome do alias que se quer criar, e o campo RDATA indica o nome canónico, isto é, o nome real do servidor. Neste exemplo, o nome do *host* do servidor FTP em 207.126.127.132 é *ftp.lowewriter.com* (A). A entrada CNAME permite os utilizadores acederem ao servidor *files.lowewriter.com* em vez de *www1.lowewriter.com*.

```
ftp.lowewriter.com.    IN  A      207.126.127.132
files.lowewriter.com.  IN  CNAME  www1.lowewriter.com.
```

Um registo *Pointer* (PTR) é o oposto do RR A. Este registo fornece o nome de domínio totalmente qualificado para um determinado endereço. O campo do *owner* deve especificar o

nome do domínio de pesquisa inversa e o campo RDATA especifica o nome de domínio totalmente qualificado.

```
102.129.71.64.in-addr.arpa. IN  PTR  www.lowewriter.com.
```

O DNS desempenha um papel no encaminhamento de correio eletrónico, permitindo informar os servidores de correio eletrónico sobre a identificação dos servidores (mail exchanger – MX) dos domínios de correio eletrónico para onde devem enviar as suas mensagens. Esta informação está contida em registos MX, através dos quais o administrador de um serviço de correio eletrónico anuncia a identificação dos servidores que podem receber mensagens destinadas a esse domínio.

```
lowewriter.com.    IN  MX  0   mail1.lowewriter.com.
lowewriter.com.    IN  MX  10  mail2.lowewriter.com.
```

Neste exemplo, o domínio *lowewriter.com* tem dois servidores de mail, *mail1.lowewriter.com* e *mail2.lowewriter.com*.

O DNS oferece também um mecanismo de autenticação de correia que pode ser visto como um MX em sentido inverso, cujo objetivo é identificar que servidores estão autorizados enviar mensagens com origem num determinado domínio. Deste modo, antes de aceitar uma mensagem, um servidor de correio eletrónico (MTA) consulta o DNS, para averiguar se o servidor que pretende entregar a mensagem está identificado como origem válida de mensagens desse domínio.

Um registo SOA contém informação administrativo sobre a zona. O SOA contém um ficheiro de zona com todas as entradas de recursos descritos na zona.

A distribuição de carga aplicacional por vários servidores de rede é outra funcionalidade oferecida pelos servidores de nomes que implementam um mecanismo de *load sharing* ou *round-robin*. Este mecanismo baseia-se no mapeamento do mesmo nome em vários endereços IP. Assim, quando um servidor de nomes recebe um pedido de resolução do nemo responde com um dos endereços. No pedido seguinte de resolução desse mesmo nome, o servidor responde com outro endereço na sequência de endereços atribuídos a esse nome. Note-se que se trata de um mecanismo de distribuição de carga e não de balanceamento de carga (*load balancing*), na medida em que o servidor de nomes devolve, de forma determinística, um endereço IP, sem atender à carga atual do computador, cujos serviços são solicitados.

Exercícios

1. **Resolução de nomes e endereços**

O **nslookup** é uma ferramenta, comum ao Windows e ao Linux, utilizada para se obter informações sobre registros de DNS de um determinado domínio, host ou IP. O **nslookup** pode ser utilizado em modo interativo ou em modo não interativo.

O **modo interativo** utiliza-se quando se pretende interrogar o DNS sobre vários equipamentos, ou obter uma lista dos computadores num domínio. A maneira mais simples de utilizar o modo interativo é digitar o comando sem qualquer argumento.

O **modo não interativo** utiliza-se quando se pretende fazer apenas uma única interrogação sobre um dado equipamento.

Com o wireshark a correr, execute os seguintes comandos:

1. Digite o comando “nslookup” e depois digite o endereço www.fca.pt e de seguida introduza o respetivo IP.
2. Em modo não interativo execute o comando “nslookup www.fca.pt” e o comando nslookup <IP>.

Note-se que nestes exercícios a resposta do servidor de nomes é precedida de *Non-authoritative answer*:, o que pode sugerir uma informação pouco exata. Esta é a forma do servidor de nomes indicar que obteve a informação interrogando outros servidores de nomes e não a partir de dados armazenados localmente.

3. Desligue o wireshark e analise o pedido e a resposta da *query* realizada. Indique o tipo e a classe de pedido foi realizado?
4. Liste as entradas do www.fca.pt com o comando “host -a www.fca.pt”.
5. Utilize o comando ‘dig’ (comando alternativo ao nslookup mas que tem o mesmo objetivo) para resolver o nome www.google.pt. Identifique o servidor de nomes que é interrogado e verifique que consta da configuração de TCP/IP do equipamento que está a ser utilizado. Analise a resposta e verifique a utilização do DNS para a atribuição de nomes alternativos e distribuição de carga.

6. Tipos de registos de DNS e servidores de nomes

Além de nomes e endereços a resolver, o ‘nslookup’ pode receber diversas opções que permitem especificar o tipo de registos DNS pretendido ou o servidor de nomes a interrogar. Em modo não interativo, o tipo de registos é especificado com a opção “-type”. Além disso, um servidor de nomes alternativo pode ser especificado como último parâmetro da linha de comandos do ‘nslookup’. Ligue o wireshark e execute os comandos:

1. Utilize o **nslookup** em modo interativo e não interativo para identificar o servidor de nomes do domínio da universidade (nslookup -type=ns ulusofona.pt); identifique o endereço IP dos servidores de correio eletrónico que servem esses domínios.
2. Utilize o **nslookup** em modo interativo e não interativo para identificar o servidor de mail da universidade (nslookup -type=mx ulusofona.pt); identifique o endereço IP dos servidores de correio eletrónico que servem esses domínios (nslookup ASPMX2.GOOGLEMAIL.COM.)

SMTP

O SMTP é o protocolo utilizado para transferir mensagens entre servidores de correio eletrónico. O correio eletrónico assenta sobre o protocolo SMTP, sendo uma das principais aplicações da Internet. Em SMTP, tal como outros protocolos, a troca de comandos protocolares entre cliente e servidor é feita em ASCII sobre uma ligação TCP/IP. Assim,
As mensagens transportadas por SMTP apenas podem conter carateres ASCII com 7 *bits*, vulgarmente designadas com *plain text*. Assim, para permitir a transmissão de mensagens multimédia ou de caracteres ASCII com 8 *bits*, será necessária uma codificação da mensagem para ASCII com 7 *bits* antes da transmissão e a consequente descodificação após a receção.

Dentro do processo SMTP, as mensagens são reencaminhadas de computador para computador via servidores SMTP. Os códigos de respostas dos servidores SMTP indicam o que aconteceu às mensagens.

Os códigos de respostas mais importantes são os seguintes.

250 – essa resposta do servidor SMTP simplesmente significa que tudo correu bem e sua mensagem foi entregue ao servidor destinatário.
421 – sua mensagem foi adiada temporariamente pelo servidor destinatário. Isso geralmente é um resultado de muitas conexões em um curto período de tempo ou muitas mensagens.
450 – sua mensagem não foi entregue porque a outra caixa de correio do usuário não estava disponível. Isso pode acontecer se a caixa de correio estiver bloqueada ou não for roteável.
451 – essa resposta é enviada quando a mensagem simplesmente falhou. Muitas vezes isso não é causado por você, mas sim por causa de um problema de servidor extremo.
452 – esse tipo de resposta é enviado de volta quando não há armazenamento de sistema suficiente para enviar a mensagem. Sua mensagem é adiada até que o armazenamento seja aberto e ele pode ser entregue.
530 – Problema de autenticação
550 – a mensagem falhou porque a caixa de correio do outro usuário não está disponível ou porque o servidor de destinatário rejeitou sua mensagem.
551 – a caixa de correio que sua mensagem foi destinada não existe no servidor destinatário.
552 – a caixa de correio que sua mensagem foi enviada não tem armazenamento suficiente para aceitar sua mensagem.
553 – a mensagem não foi entregue porque o nome da caixa de correio que você enviou não existe.
554 – esta é uma resposta de falha de mensagem muito vaga que pode se referir a qualquer número de problemas ou no seu final ou com o servidor destinatário.

1. Funcionamento básico do SMTP

Neste exercício vamos usar o comando telnet dirigida o porto tcp/25 de servidores de correio eletrónico para desempenhar o papel de um cliente SMTP e verificar a operação do protocolo e a inexistência de mecanismos para autenticar os endereços de origem e de destino. Para tal, o docente tem que vos dar o IP do servidor de e-mail (por exemplo postfix) que tem a correr.

1. É possível enviar um e-mail forjado através da ferramenta **telnet** para o porto 25 do servidor SMTP. Execute os comandos abaixo descritos, enquanto o wireshark está a correr. Verifique que a mensagem é igualmente enviada e identifique o código devolvido pelo servidor SMTP;

$ telnet <IP do servidor de mail> <porto>
EHLO <domínio>
MAIL FROM: rementente@origem.pt
RCPT TO: destinatario@destino.com
DATA
Subject: teste
Boa tarde
.
QUIT

2. Repita o exercício usando email inexistente e indique o código devolvido pelo protocolo SMTP

   telnet <IP do servidor de mail> <porto>
   EHLO <domínio>
   MAIL FROM: remetente@origem.pt
   RCPT TO: nonexistant@destino.com

3. Repita o exercício usando email inexistente no emissor, e um email correcto no recetor.
   telnet <IP do servidor de mail> <porto>
   EHLO <domínio>
   MAIL FROM: nonexistant@origem.pt
   RCPT TO: existant@destino.com

Cabeçalhos MIME

Nesta subseção pretende-se explorar e compreender a utilização do protocolo SMTP, que apenas pode transmitir carateres ASCII 7 bits, para transmitir imagens, música ou filmes, que incluem carateres ASCII 8 bits.

O cabeçalho MIME permite que os User Agents (UA), por exemplo o cliente de email, interpretem o conteúdo de mensagem ASCII 8 bits codificadas em ASCII 7 bits para transmissão por SMTP.

1. Envie uma mensagem tipo email com o 'charset=UTF-8' para o email destinatário

```
From: My Self <me@you.com>
To: A secret list <pcosta@rc2019.pt>
Subject: A simple test
Mime-Version: 1.0;
Content-Type: text/html; charset="UTF-8";
Content-Transfer-Encoding: 7bit;

<html>
<head><meta charset="UTF-8"></head>
<body>
<h2>É um link importante.</h2>
Aqui está o <a href="http://www.ulusofona.pt">link </a>
</body>
</html>
```

A codificação e descodificação de mensagens é efetuada utilizando a codificação BASE64. Para tal, recorre-se ao **openssl**, uma vez que está disponível em todos os SOs.

Para converter um ficheiro em BASE64 pode utilizar-se o comando da seguinte forma:

```
$ openssl base64 -in ficheiro-a-converter.txt -out ficheiro-convertido.b64
```

A operação de descodificação para o seu formato original pode ser feita utilizando o seguinte comando:

```
$ openssl base64 -d -in ficheiro-convertido.b64 -out original.txt
```

Os UA automatizam a codificação de mensagens e respetiva descodificação com base aos cabeçalhos MIME 'Content-Type' e 'Content-Transfer-Encoding'. Como o nome indica, o primeiro indica ao UA de destino o tipo de conteúdo incluído na mensagem, enquanto o segundo identifica o tipo de codificação utilizada para permitir a transmissão ASCII 7bits utilizando o SMTP.

1. Escreva um ficheiro de mensagens com carateres acentuados; converta a mensagem em BASE64.

Na página do moodle encontra-se o ficheiro *SendFileEmail.java* que vai ser usado para enviar o ficheiro codificado. Faça *download* do ficheiro SendFileEmail.java e do *javax.mail.jar*. Coloque ambos os ficheiros na mesmo diretoria.

Utilize os seguintes comandos para compilar e executar o programa:

```
javac -cp javax.mail.jar SendFileEmail.java
java -cp javax.mail.jar:. SendFileEmail <smtp host> <from> <to> <ficheiro>
```

1. Envie o email usando a classe java.
2. O docente irá mostrar o ficheiro enviado e irá descodificar a mensagem para verificar que o anexo foi enviado com sucesso.