Universidade de Coimbra
Faculdade de Ciências e Tecnologia

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

TRABALHO PRÁTICO

Sistema de *messaging*

Ano Letivo de 2020/21

1 Objetivos

O objetivo deste trabalho prático é implementar um sistema de troca de mensagens entre utilizadores, recorrendo a diversas técnicas de comunicação e com recurso aos protocolos da pilha protocolar TCP/IP. A aplicação irá utilizar comunicações TCP e UDP, bem como as técnicas de comunicação e de endereçamento IP necessárias ao suporte dos requisitos de comunicação da aplicação, descritos a seguir. O trabalho compreenderá duas fases, avaliadas separadamente. Na primeira fase o foco incidirá na configuração do cenário da Rede de comunicação de suporte à aplicação. Na segunda fase, o alvo da avaliação será sobre a aplicação distribuída a desenvolver, para suportar o sistema de *messaging*.

2 Cenário de Rede

A Figura 1 ilustra a Rede de comunicação a configurar, para suportar a aplicação a desenvolver no trabalho. Para suportar as comunicações UDP e TCP da aplicação, a aplicação fará uso de uma rede com 3 *routers*, que deverão ser configurados para suportar as necessárias operações de encaminhamento, bem como de NAT (Network Address Translation).

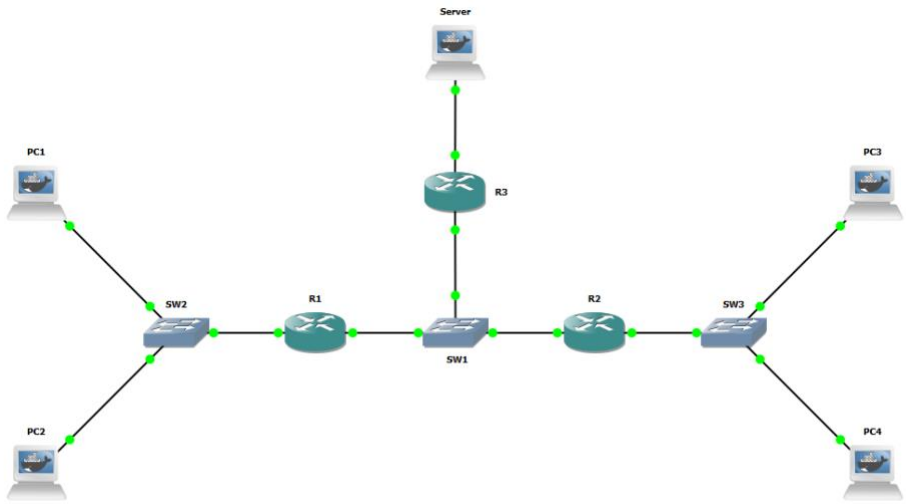

Figura 1 - Rede de comunicação de suporte à aplicação

O trabalho compreende duas fases de implementação e avaliação, com os seguintes objetivos:

- **Meta 1**: implementação do cenário de rede com recurso ao GNS3, com todas as configurações necessárias ao suporte do encaminhamento entre redes, bem como de NAT (SNAT e DNAT, funcionalidades descritas mais à frente no enunciado).

- **Meta 2 (entrega final)**: funcionalidades da aplicação distribuída de *messaging*, nas suas componentes servidor e cliente.

A seguir descrevem-se os requisitos a ter em conta na implementação do cenário da rede de comunicação de suporte à aplicação, com recurso ao GNS3.

3 Rede de comunicação de suporte à aplicação

Tal como a Figura 1 ilustra, o cenário de rede faz uso de 3 *routers* e 3 *switches*. Os equipamentos devem ser configurados de forma a garantir que os clientes (PCs) conseguem comunicar entre si, bem como com o servidor. **Os PCs (clientes e servidor) deverão utilizar Linux, recorrendo à imagem criada em docker e já disponível no GNS3 na VM fornecida aos alunos**.

Ao nível do endereçamento IP, deverá ter em conta os seguintes requisitos:

- Utilize a Rede 10.90.0.0/24 para endereçar a rede do servidor. No cenário, esta rede funcionará como rede DMZ (demilitarized zone), interligada com as restantes redes do cenário através do router R3, redes estas a que serão consideradas as redes externas.

- Utilize a Rede IPv4 193.136.212.128/25 para endereçar as várias redes externas do cenário, sendo que no caso da rede que interliga os routers R1, R2 e R3 deverá usar uma rede /29 (máscara 255.255.255.248).

- Deverá atribuir a todos os equipamentos endereços IP apropriados, na gama da sub-rede convencionada.

Para além da comunicação, o router R3 deverá suportar NAT nos modos SNAT (Source NAT) e DNAT (Destination NAT). Estas duas formas de NAT deverão ser configuradas atendendo ao seguinte:

- O router R3 deverá efetuar SNAT para as comunicações com origem na rede DMZ (rede do servidor) e destinadas às redes externas.

- O router R3 deverá efetuar SNAT nas comunicações com origem nas redes externas e destinadas ao servidor. Ou seja, os clientes deverão poder comunicar com os portos do servidor com recurso a DNAT, sendo que as comunicações com destino ao endereço da interface externa do router R3 (que liga às redes externas) devem ser redirecionadas para o servidor.

A seguir descreve-se o funcionamento dos mecanismos de SNAT e DNAT.

Funcionamento do SNAT (Source NAT) e DNAT (Destination NAT)

O NAT (Network Address Translation) permite mapear endereços IP nas comunicações entre diferentes redes, através da alteração do endereço de origem ou destino no cabeçalho dos pacotes IP, durante a sua passagem por um *router*. Na realidade, o NAT implementa várias técnicas, algumas das quais com designação que varia de fabricante para fabricante. Uma das técnicas mais úteis é a do SNAT (ou Source

NAT), utilizado na prática nas comunicações entre redes com endereços IP privados e a Internet, onde forçosamente se usam endereços IP oficiais. O funcionamento do SNAT é ilustrado na Figura 2.

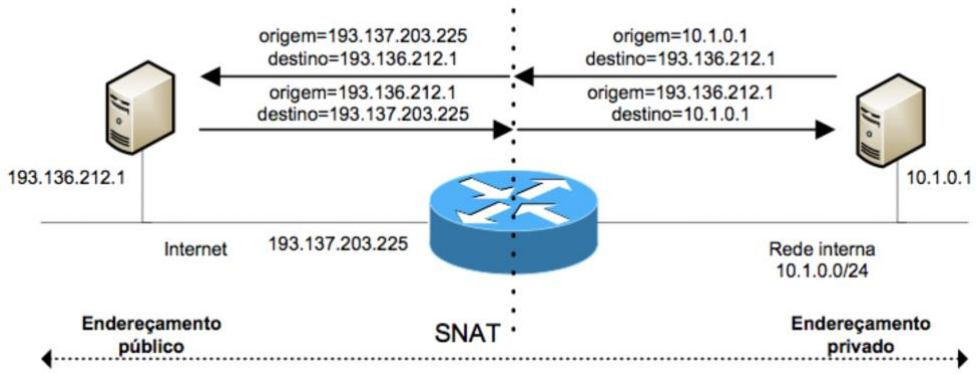

Figura 2 - Funcionamento do NAT (SNAT)

Como é possível ver na Figura 2, neste cenário o NAT utiliza o endereço externo do *router* (neste exemplo o endereço 193.137.203.225) como endereço de origem para as comunicações com origem na rede interna (a rede 10.1.0.0/24). Para este efeito, o NAT recorre a portos diferentes para distinguir as várias comunicações sujeitas a NAT, para as quais armazena a correspondência entre portos internos e externos numa tabela de translação de endereços.

Por sua vez, o DNAT permite a translação do endereço de destino dos pacotes IP. O funcionamento do DNAT encontra-se ilustrado na Figura 3, sendo que no exemplo as comunicações com origem no exterior e destinadas ao endereço de destino 193.137.203.225 (o endereço IP da interface de ligação do router ao exterior) é alterado para o endereço 10.1.0.1, para que a ligação seja efetivamente redirecionada para a máquina da rede interna.

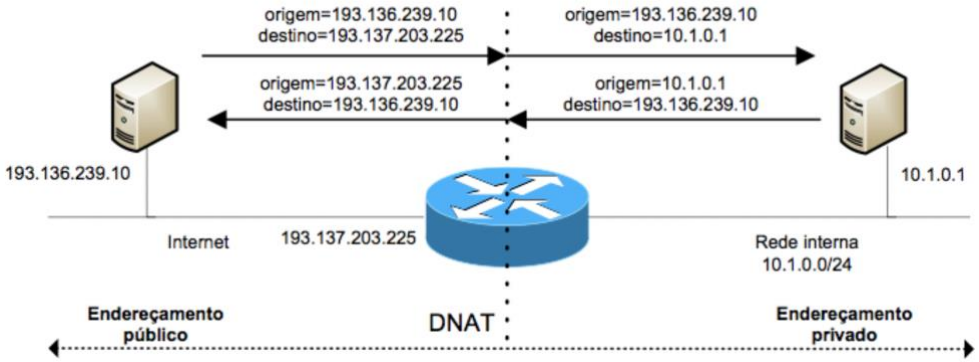

Figura 3 - Funcionamento do DNAT (DNAT)

Como é visível no exemplo, o DNAT permite, desta forma, expor ao exterior serviços que estejam disponíveis em servidores na rede interna (com endereçamento privado), com recurso ao endereço externo do router. A seguir descrevem-se os fundamentos em relação à configuração dos mecanismos de DNAT e SNAT em routers Cisco.

Configuração de SNAT nos *routers* Cisco

Tal como seria de esperar, os routers Cisco suportam a configuração do NAT nos seus vários modos de utilização, entre os quais o SNAT e DNAT (descritos anteriormente). O exemplo seguinte ilustra a configuração do SNAT para translação de endereços da rede 10.5.0.0/24 para a rede externa (193.137.203.0/24), recorrendo para o efeito ao endereço 193.137.203.1, o endereço da interface externa utilizado no modo "overload". O modo "overload" significa que o NAT recorre a diferentes portas para diferenciar as várias ligações.

```
router# config terminal
router(config)# access-list 30 permit 10.5.0.0 0.0.0.255
router(config)# ip nat inside source list 30 interface Ethernet0 overload
router(config)# interface FastEthernet0
router(config-if)# ip address 10.5.0.1 255.255.255.0
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface Ethernet0
router(config-if)# ip address 193.137.203.1 255.255.255.0
router(config-if)# ip nat outside
router(config-if)# end
```

Confirme o exemplo anterior ilustra, as interfaces nas quais o NAT opera são declaradas como "inside" e "outside". A primeira é a interface de ligação à rede interna, na qual é utilizada a gama de endereços privados, sendo a externa a interface "outside". O comando "access-list" permite definir a gama de endereços aos quais a operação de NAT irá aplicar-se, no exemplo a toda a rede 10.5.0.0/24 (de notar a utilização de "0.0.0.255", para identificar a totalidade da gama desta rede).

Configuração de DNAT nos *routers* Cisco

Os routers Cisco suportam igualmente a configuração de NAT no modo DNAT, descrito anteriormente. Neste modo, é necessário identificar as comunicações a sujeitar a DNAT (para as quais o endereço de destino deve ser alterado), para que sejam redirecionadas para o servidor da rede interna. Uma das formas de configurar DNAT nos routers Cisco consiste no redirecionamento de portos específicos, para ligações efetuadas ao IP da interface do router que liga às redes exteriores. Considere o seguinte exemplo, que ilustra esta forma de configuração.

```
router# config terminal
router(config)# ip nat inside source static tcp 10.5.0.200 80 193.137.203.1 80
router(config)# interface FastEthernet0
router(config-if)# ip address 10.5.0.1 255.255.255.0
router(config-if)# ip nat inside
router(config-if)# exit
router(config)# interface Ethernet0
router(config-if)# ip address 193.137.203.1 255.255.255.0
router(config-if)# ip nat outside
router(config-if)# end
```

No exemplo anterior, utiliza-se DNAT para redirecionar ligações efetuadas ao porto 80 do endereço 193.137.203.1 (da interface externa ou 'outside' do router) para o mesmo IP na máquina 10.5.0.200 da rede interna.

4 Funcionalidades da aplicação de *messaging*

Após a configuração da Rede de comunicação de suporte à aplicação, será necessário construir a aplicação de *messaging*, através do desenvolvimento das suas componentes cliente e servidor. Descrevem-se a seguir os modelos de comunicação a suportar e as funcionalidades da aplicação a implementar.

Modelos de comunicação suportados pelo serviço

Para a comunicação entre utilizadores da aplicação, pretende-se que o serviço de *messaging* suporte os seguintes modos de comunicação:

- **Comunicação cliente-servidor**: comunicação entre clientes (utilizadores) com passagem das mensagens pelo servidor.

- **Comunicação P2P**: comunicação direta entre clientes (utilizadores), sendo que neste caso as mensagens não passam pelo servidor.

- **Comunicação em grupo**: caso tenha autorização, um utilizador poderá criar um grupo e enviar uma mensagem que será recebida pelos restantes participantes desse grupo.

Cada cliente deve inicialmente autenticar-se perante o servidor, recorrendo para tal ao seu *username* e *password*, sendo que estas credenciais devem ter sido previamente registadas no servidor pelo administrador do serviço.

Após a autenticação bem sucedida, o cliente recebe do servidor informação acerca das formas de comunicação que está autorizado a utilizar. Ao selecionar a forma de comunicação pretendida (de entre as que está autorizado a utilizar), o cliente solicita ao servidor a informação necessária ao envio da mensagem, tal como descrito mais adiante.

Funcionalidades suportadas pelo servidor

O servidor será responsável pelas seguintes funcionalidades de suporte ao serviço de *messaging*:

- Validação do registo dos clientes através de *username* e *password*, sendo que um utilizador deve ter sido previamente registado no serviço.

- Após a autenticação, enviar ao cliente informação sobre os modos de comunicação que ele está autorizado a utilizar.

- Receber do cliente o pedido para início de uma nova comunicação, de entre as autorizadas ao cliente:

    - Comunicação cliente-servidor: neste caso permite **enviar a mensagem ao utilizador de destino**.

    - Comunicação P2P: devolve ao cliente o **IP e porto UDP do cliente associado ao utilizador de destino**, portanto ao qual o cliente deve enviar diretamente a mensagem.

    - Comunicação em grupo: devolve ao cliente o **endereço multicast** que este deverá utilizar para enviar a mensagem aos restantes utilizadores registados no grupo.

- Fazer o *forwarding* (a troca) das mensagens entre clientes, trocadas em comunicações entre utilizadores com passagem pelo servidor.

O programa servidor deverá ser executado na linha de comandos do Linux recorrendo à seguinte sintaxe:

`server {porto clientes} {porto config} {ficheiro de registos}`

O **`porto clientes`** é o porto UDP utilizado pelos clientes para comunicarem com o servidor, sendo de notar que o endereço de destino que os clientes devem usar é o da interface externa do router R3, tal como descrito anteriormente para o DNAT. É através de comunicações com este porto do servidor que os clientes se autenticam e obtêm a informação necessária às comunicações suportadas pelos serviços autorizados ao cliente.

O **`porto config`** deverá permitir ligações TCP ao servidor para administração através de uma CLI (command line interface), que deverá disponibilizar os seguintes comandos:

- LIST: permite ao administrador listar a informação sobre os clientes registados no serviço (ver formato na tabela seguinte)
- ADD <User-id> <IP> <Password> <Cliente-Servidor> <P2P> <Grupo>: permite ao administrador adicionar um novo utilizador ao serviço.
- DEL <User-id>: permite ao administrador apagar um utilizador do serviço.
- QUIT: permite terminar a sessão (CLI) com o porto de administração do serviço;

O **`ficheiro de registos`** permite manter informação sobre os clientes registados (previamente autorizados) no serviço de *messaging*, na forma de uma linha por cliente do serviço. Apresenta-se a seguir um exemplo da informação que deverá ser armazenada neste ficheiro:

`User-id`	**`IP`**	**`Password`**	**`Cliente-Servidor`**	**`P2P`**	**`Grupo`**
jmanuel	193.136.212.129	privatepass	yes	no	yes

Na informação anterior, o **`IP`** é o endereço autorizado pelo servidor para que o cliente identificado pelo **`User-id`** e pela **`Password`** comunique com o servidor e solicite a utilização do serviço de messaging.

Funcionalidades suportadas pelo cliente

O cliente será responsável pelas seguintes funcionalidades no serviço de *messaging*:

- O cliente deverá solicitar inicialmente ao utilizador o seu *username* e *password*, que deverá enviar ao servidor para se autenticar no serviço de *messaging*. Tal como descrito anteriormente, o registo no servidor destas credenciais é obrigatório, para que o cliente possa comunicar com outros utilizadores.
- Após autenticação do utilizador, o cliente deverá receber do servidor informação sobre as comunicações que está autorizado a utilizar no serviço de *messaging*.
- O cliente deve receber do utilizador o pedido de início de uma comunicação (de entre as autorizadas), comunicando com o servidor para o efeito:
    - Se o utilizador usar o cliente para enviar uma mensagem através do servidor o cliente deve enviar a mensagem ao servidor, juntamente com a indicação do User-id de destino.
    - Se o utilizador pretender comunicar diretamente (P2P) com outro utilizador do serviço, deve pedir ao servidor o endereço e porto UDP do cliente de destino.

- Se o utilizador pretender criar um grupo, o cliente deve enviar ao servidor o pedido de criação do novo grupo, sendo que o servidor deve confirmar e devolver o endereço *multicast* a utilizar para as comunicações neste grupo. Desta forma, todos os clientes cujos utilizadores pretendam comunicar nesse grupo deverão contactar o servidor para obter o endereço multicast a usar.

O programa cliente deverá ser executado na linha de comandos do Linux recorrendo à seguinte sintaxe:

```
cliente {endereço do servidor} {porto}
```

As comunicações entre o cliente e o servidor deverão utilizar UDP. Na sintaxe anterior, o **`endereço do servidor`** deverá ser o endereço da interface externa do router R3 uma vez que, tal como descrito anteriormente, este router deverá estar configurado para redirecionar a comunicação para o servidor na rede DMZ. O **`porto`** é o porto UDP no qual o servidor recebe pedidos dos clientes.

À semelhança do servidor, o cliente deverá disponibilizar uma CLI (command line interface) ao utilizador da aplicação. De notar que neste caso não é necessário que a CLI esteja disponível por ligação a um porto específico, bastando que a aplicação cliente interaja com o utilizador através da consola. Os comandos a suportar para implementar as funcionalidades descritas anteriormente ficam ao critério do aluno.

5 Testes

A aplicação **netcat** (**nc**) poderá ser bastante útil para efetuar testes ao cenário da rede de comunicação, bem como ao nível da própria aplicação. A seguir descreve-se de que forma esta aplicação pode ser usada para testar uma comunicação UDP ou TCP entre dois hosts. O **nc** pode ser usado diretamente na linha de comandos do Linux, portanto nos clientes e no servidor do cenário de comunicação. Para utilizar o **netcat** como **servidor** deverá utilizar a seguinte sintaxe:

```
nc -v -l {porto}          # Escuta num porto TCP
nc -v -u -l {porto}       # Escuta num porto UDP
```

Para utilizar o **netcat** como **cliente** deverá utilizar a seguinte sintaxe:

```
nc -v {IP do servidor} {porto}       # Ligação TCP ao servidor
nc -v -u {IP do servidor} {porto}    # Comunicação UDP com o servidor
```

O **netcat** permite testar a comunicação entre um cliente e um servidor, sendo particularmente útil nos testes ao endereçamento com SNAT e DNAT, funcionalidades descritas anteriormente. Após o estabelecimento da comunicação entre o cliente e o servidor, para testar se a ligação está a funcionar corretamente basta escrever num dos terminais (cliente ou servidor), sendo que o texto introduzido deverá ser enviado e mostrado no outro terminal.

6 Entrega do trabalho

- Realização do trabalho: Trabalho individual ou em grupos de dois alunos.
- A entrega decorre em duas metas, com os seguintes objetivos e datas a ter em atenção:

- **Meta 1**: implementação do cenário de rede com recurso ao GNS3, com todas as configurações necessárias ao suporte do encaminhamento entre redes, bem como de NAT (SNAT e DNAT):

  Entrega do relatório por *upload* no Inforestudante, com no máximo 2 páginas, descrevendo as configurações efetuadas e os testes efetuados para as validar:
  - **Data limite de entrega: 18 de Abril de 2021.**
  - **Defesas na semana de 19 de Abril 2021.**

- **Meta 2**: a entrega final consistirá do relatório final do trabalho, e dos ficheiros com o código fonte em C da aplicação desenvolvida:

  - **Data limite de entrega do relatório final por *upload* no Inforestudante: dia 23 de Maio de 2021.**
  - **Defesas na semana de 24 de Maio 2021.**

Notas importantes:

- Na realização do trabalho deverá recorrer à **linguagem de programação C**.

- O relatório final deve ser sucinto (no máximo 4 páginas A4), no formato PDF (não serão aceites outros formatos). No relatório deve explicar as opções tomadas na construção da solução e o modo de funcionamento.

- Crie um arquivo no formato ZIP (não serão aceites outros formatos) com todos os ficheiros do trabalho:

  - Todos os ficheiros fonte e de configuração necessários.
  - Não inclua quaisquer ficheiros não necessários para a compilação ou execução do programa (ex. diretórios ou ficheiros de sistemas de controlo de versões)
  - Não serão admitidas entregas por e-mail.

- As defesas (meta1 e final) do trabalho são obrigatórias para todos os elementos do grupo.

- Todos os trabalhos serão escrutinados para deteção de cópias de código.