Ficha 05 – DHCP e NAT com *routers* Cisco

Ano Letivo de 2019/2020

Cenário de testes

Nesta ficha pretende-se abordar a utilização do Protocolo DHCP (*Dynamic Host Configuration Protocol*), bem como do NAT (*Network Address Translation*), recorrendo para o efeito a um cenário de rede simulado com recurso ao simulador GNS3. A Figura 1 ilustra o cenário de testes a considerar para a execução dos exercícios descritos a seguir.

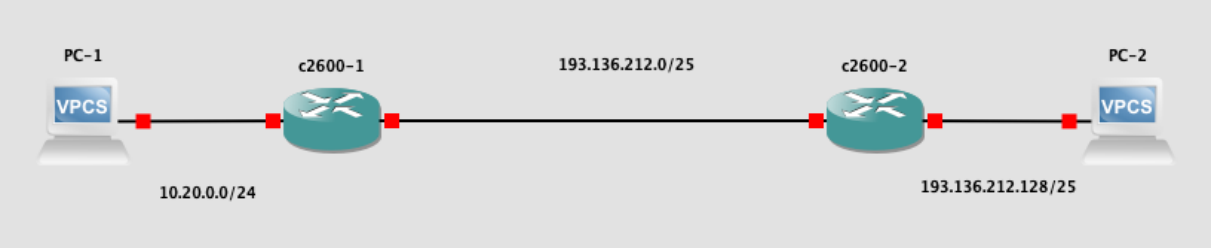

Figura 1 - Cenário experimental da Ficha 5

Configuração do serviço DHCP nos *routers* Cisco

O protocolo DHCP permite que um *host* (computador, qualquer dispositivo ligado à rede) obtenha, de forma dinâmica e automática, a sua configuração de rede a partir de um servidor. Para além do endereço IP, um *host* precisa também da sua máscara de rede, do *gateway* de acesso à Internet e do endereço do servidor de DNS, tudo informação que pode obter com recurso ao DHCP. Para além desta informação de configuração essencial, o DHCP permite enviar mais informação de configuração ao *host*. A Figura 2 ilustra as comunicações utilizadas pelo Protocolo, entre o cliente e o servidor, para obtenção pelo primeiro de uma configuração de rede IP.

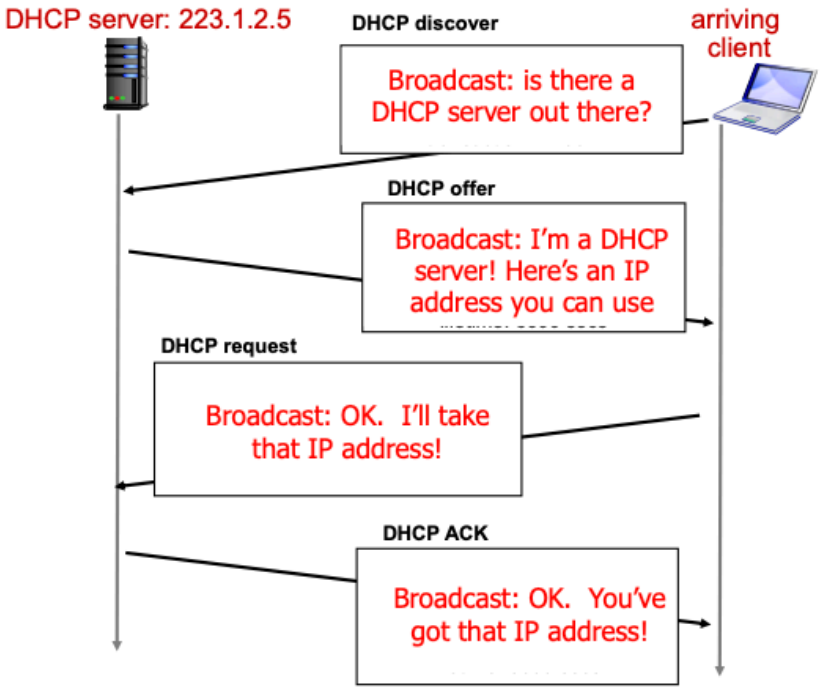

Figura 2 - Comunicações entre um cliente e um servidor DHCP

Os *routers* da Cisco, através do seu sistema IOS (*Cisco Internetwork Operating System*) podem desempenhar a função de servidor DHCP, mesmo que em muitas redes este seja um *host* dedicado. Outra característica essencial do DHCP é a possibilidade de definir um tempo de validade para a informação de configuração atribuída ao *host* (ou cliente DHCP). Esta informação de configuração é designada por *lease* e o período de validade referido por *lease time*. Assim, um cliente que pretenda manter a sua configuração por mais tempo tem que pedir ao servidor uma renovação da *lease*, antes da sua expiração. O exemplo seguinte ilustra a configuração, na sua forma mais simples, do serviço DHCP no Cisco IOS.

```
router# config terminal
router (config)# service dhcp
router (config)# ip dhcp pool IRC
router (dhcp-config)# network 10.16.1.0 255.255.255.0
router (dhcp-config)# default-router 10.16.1.254
router (dhcp-config)# exit
router (config)# ip dhcp excluded-address 10.16.1.1 10.16.1.30
router (config)# ip dhcp excluded-address 10.16.1.220 10.16.1.255
router (config)# end
```

O exemplo anterior ilustra a utilização do comando "ip dhcp pool" para criação de uma *pool* de endereços para atribuição a clientes DHCP. Nesta configuração, e de acordo com o exemplo anterior, os clientes irão receber também o endereço 10.16.1.254 como *default gateway* (o *router*). Vemos ainda a exclusão de duas gamas da *pool* de endereços a atribuir a clientes, com recurso ao comando "ip dhcp excluded-address". Estes endereços excluídos podem, por exemplo, ser reservados para endereçamento estático.

Exercício 1 (preparação de cenário experimental):

Configure o cenário de rede ilustrado na Figura 1. Neste cenário, considere as gamas (redes) de endereços ilustradas. Recorra ao comando "ping" para validar a comunicação entre os VPCS terminais (VPC1 e VPC2).

Nota: nesta fase deverá atribuir endereços estáticos aos VPCS, não iremos ainda usar DHCP. Assim, o VPC1 deverá utilizar o endereço 10.20.0.1 e o VPC2 o endereço 193.136.212.254.

Exercício 2 (configuração do servidor DHCP):

Neste exercício aborda-se a utilização do Protocolo DHCP. Configure o *router* c2600-1 do cenário como servidor DHCP para a rede do VPC1 (gama 10.20.0.0/24), de acordo com os seguintes requisitos:

- Atribuir configurações na rede do VPC1, utilizando para o efeito a gama de endereços do 10.20.0.100 ao 10.20.0.130.
- Na configuração de rede a atribuir pelo servidor DHCP aos clientes deverá constar também o endereço do *router* (*default gateway*) e de um servidor DNS. Considere que o servidor DNS está na rede do VPC1, convencionando um endereço para o efeito.

Nota: no modo de configuração do DHCP, de acordo com o exemplo anterior, recorra ao comando "?" para ver os comandos disponíveis.

Finalmente, valide no VPC1 que consegue obter a configuração da rede por DHCP, recorrendo ao comando "ip dhcp".

Exercício 3 (testes ao funcionamento do protocolo DHCP):

Neste exercício pretendem-se analisar as mensagens utilizadas nas comunicações do Protocolo DHCP, no decurso da atribuição, a um cliente, de uma configuração de rede.

- Force uma nova obtenção de configuração de rede no VPCS, recorrendo ao comando "ip dhcp -d".

- Recorra ao Wireshark para analisar as comunicações utilizadas pelo Protocolo. Que mensagens são utilizadas pelo DHCP e qual será o seu propósito?

- Qual é o *lease time* da *lease* obtida do servidor?

- Altere agora o *lease time* na configuração da *pool* DHCP, que deverá passar a ser de apenas 2 min. Para tal, no modo de configuração da *pool* DHCP, deverá recorrer ao comando *lease*, que aceita a seguinte sintaxe:

```
lease <dias> <horas> <minutos>
```

- Force nova obtenção da configuração de rede pelo VPC1 e valide, novamente com recurso ao Wireshark, que o cliente solicita a sua renovação ao servidor, antes do final do período de validade.

NAT (Network Address Translation) e SNAT (Source NAT)

O NAT (*Network Address Translation*) permite remapear 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), utilizada nas comunicações entre redes com endereços IP privados e a Internet, onde forçosamente se usam endereços IP oficiais. Tal como é possível ver no cenário da Figura 1, é nestas condições que se encontram as comunicações entre a rede do VPC1 (onde é utilizada a gama privada 10.20.0.0/24) e as restantes redes do cenário.

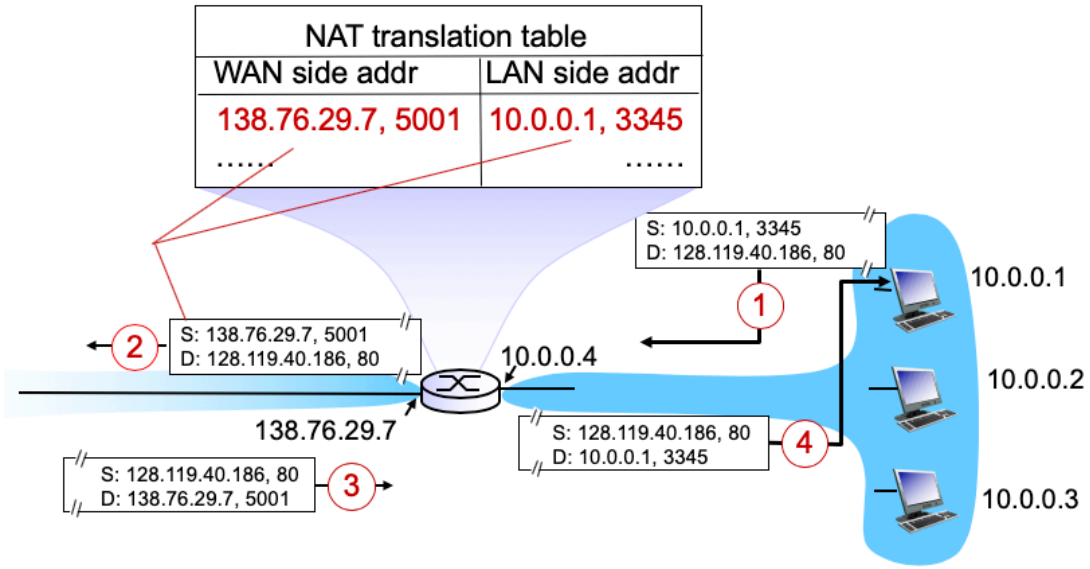

Figura 3 – Funcionamento do NAT (SNAT)

Como é possível ver na Figura 3, neste cenário o NAT utiliza o endereço externo do *router* (neste exemplo o endereço 138.76.29.7) como endereço de origem para as comunicações com origem na rede interna, recorrendo 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.

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 (descrito 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), usando para o efeito o endereço 193.137.203.1, correspondente ao endereço da interface externa utilizado no modo "*overload*" e recorrendo a portas para diferenciar as várias ligações, tal como descrito anteriormente.

Conforme o exemplo seguinte 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).

```
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
```

Exercício 4 (configuração de source NAT):

Neste exercício aborda-se a utilização do NAT, mais propriamente na sua vertente SNAT (*Source* NAT). Configure o *router* c2600-1 do cenário para alteração (translação) do endereço de origem nas comunicações com origem na rede do VPC1 e destinadas às outras redes do cenário.

Após a aplicação da configuração de NAT deverá testar, a partir do VPC1, as comunicações para a rede do VPC2, em particular para a interface de ligação do *router* c2600-2 a esta rede. Assim, deverá fazer um "ping" no VPC1, para a interface interna do *router* c2600-2. Neste *router*, poderá recorrer ao comando seguinte para visualizar na consola os pacotes ICMP trocados no "ping":

```
router# debug ip icmp
```

Os resultados deverão ser semelhantes ao exemplo seguinte, no qual é possível confirmar (marcado a *bold*) o endereço de origem do "ping", que deverá ser o da interface externa do *router* c2600-1:

```
*Nov 30 03:00:33.422: IP: s=193.136.212.1 (Ethernet0/0), d=193.136.212.129, len 84, rcvd 4
*Nov 30 03:00:33.422: ICMP: echo reply sent, src 193.136.212.129, dst 193.136.212.1
*Nov 30 03:00:33.422: IP: s=193.136.212.129 (local), d=193.136.212.1 (Ethernet0/0), len 84
```