Relatório de RCOM

Parte 4

O objetivo desta experiência era adicionar à sub-rede a ligação ao router e configura-lo com funcionalidades NAT de forma a estabelecer ligação à Internet. Para este objetivo foi necessário configurar duas interfaces do router: interface gigabitEthernet 0/0 ligada à vlan1 e a interface gigabitEthernet 0/1 ligada à rede exterior da sala.

A partir da consola de configuração para ambas interfaces foi definido o seu endereço IP e mask através do comando <ip adress [ip] [mask]> em que o IP era 172.16.51.254 para a interface 0/0 e 172.16.2.59 com máscara de 24 bits. De seguida, introduziu-se o comando <no shutdown> para que as configurações não fossem perdidas caso o router fosse desligado e finalmente foi definido o ponto de entrada e saída de NAT através do comando <nat inside/outside> sendo aplicados respetivamente à interface 0/0 e interface 0/1.

Após as interfaces estarem configuradas, foi necessário executar os comandos <ip nat pool ovrld 172.16.2.59 172.16.2.59 prefix 24> e <ip nat inside source list 1 pool ovrld overload> para garantir a gama de endereços.

No seguimento, executou-se o comando <acesslist 1 permit ip [max]> sobre ambas sub-redes - 172.16.50.0 e 172.16.51.0 – com o max definido com 0.0.0.255 para criar uma lista de acessos e permissões de pacotes.

Finalmente, definiu-se as rotas através do comando <ip route [dest] [mask] [gw]> de forma a que os pacotes fossem redirecionados para o local correto. Foram adicionadas duas rotas: uma interna através do comando <ip route 0.0.0.0 0.0.0.0 172.16.1.254> para garantir que os pacotes eram enviados para a sub-rede 172.16.51.0 e uma rota externa através do comando <ip route 172.16.50.0 255.255.255.0 172.16.51.253> para garantir que os pacotes enviados para a sub-rede 172.16.50.0 eram redirecionados para o tux54 que estabelece ligação com esta sub-rede.

Adicionalmente foram utilizados os comandos <route add> e <route del> para introduzir e remover, respetivamente, entradas nas listas de reencaminhamento e <traceroute [ip]> para analisar o percurso dos pacotes ao longo da rede.

Através da análise dos resultados conclui-se que o router tem a capacidade de reencaminhar os pacotes para outras sub-redes quando no terminal não está definida a rota e que o a funcionalidade NAT é essencial à visibilidade da sub-rede para o exterior.

Parte 5

Nesta experiência pretendia-se configurar o servidor de DNS para permitir ligação à Internet através da procura de nomes de domínios. Domain Name System (DNS) é responsável por associar e traduzir diversa informação associada aos nomes dos domínios em particular o seu IP.

Para associar o DNS à sub-rede foi necessário modificar o ficheiro /etc/resolv.conf em todas as máquinas. Para tal, editou-se o seu conteúdo de acordo com o formato <search new-page-name [nameserver] [IP-page]>, sendo que *new-page-name* representa o nome da página, e *IP-page* o endereço IP da página.

O conteúdo do ficheiro passou a ser:

“search netlab.fe.up.pt

nameserver 172.16.2.1”

Para testar esta funcionalidade foi feito um ping ao domínio www.reddit.com.

Através da análise dos resultados do Wireshark podemos observar que no início da comunicação, antes do envio/receção de pacotes ICMP (enviados pelo comando <ping [ip]>), foram enviados pacotes DNS para identificar o endereço IP do destino (neste caso reddit.com).

Foi pedido ao DNS que enviasse os atributos do domínio através do pacote 3. Como resposta o servidor enviou o pacote 4 que inclui entre outras informações o endereço IP do destino.

Posteriormente, foi também feito um pedido reverse DNS (rDNS) nos pacotes 7 e 8 que processa o pedido contrário, ou seja, obter o nome domínio a partir do enderenço IP.

Parte 6

Arquitetura:

Idêntico à experiência 5.

Objetivo:

Desenvolver uma aplicação de download com base no protocolo FTP e analisar as características da comunicação tais como as ligações de controlo e dados e as suas fases, os dados transferidos através da ligação de controlo, o mecanismo ARQ e o mecanismo de controlo de congestão.

Análise de resultados:

Ao longo da execução da aplicação são abertos dois canais de comunicação: um de controlo por onde são enviados vários comandos tais como USER, PASV, RETR, etc e um de dados por onde são recebidos os pacotes do ficheiro.

Podemos identificar 3 fases durante a comunicação: estabelecimento de conexão, transferência e terminação de conexão.

A 1ª ocorre logo no inicio da transferência e é caracterizada por um handshake de 3 passos: envio de SYN, reposta de [SYN, ACK] e envio de ACK. Esta fase está visível na sequência dos pacotes 4-6.

A 2ª corresponde ao processo de transferência e é visível durante o envio e reposta de comandos FTP. Durante a transferência do ficheiro tornam-se evidentes várias características do TCP incluindo o mecanismo ARQ quando é pedido a retransmissão de pacotes (ex: pacote 62759).

A 3ª ocorre no fim da transferência e é caracterizada por um handshake de 3 passos: envio de FIN, resposta de [FIN, ACK], envio de ACK. Esta fase está visível na sequência dos pacotes 8754…-8754…(não dá para ver no print).

O mecanismo ARQ no TCP baseia-se numa variante de Go-Back-N utilizando uma janela deslizante, em que são enviados ACKs com um único número de sequência para informar o emissor que os pacotes até esse número foram recebidos com sucesso. Em caso de erro ou perda de pacotes são enviados ACKs duplicados até que o emissor reenvie os pacotes perdidos um de cada vez (assunção otimista). É também utilizado timeout para quando uma resposta não é recebida. Este timeout é adaptativo, calculado dinamicamente de acordo com RTT (Round Trip Time) medido ao longo da transmissão.

Existe ainda a possibilidade de utilizar selective acknowledgements (SACKs).