Universidade do Porto

FEUP Faculdade de Engenharia

LAB 2 – COMPUTER NETWORKS

Gonçalo Ferreira – up201707382
Diogo LANdau – up201603722

MIEEC – Redes de Computadores
dezembro de 2020

ÍNDICE

INTRODUÇÃO

No âmbito da Unidade Curricular de Redes de Computadores, foi-nos proposta a realização da experiência laboratorial 2.

Esta experiência laboratorial é composta por duas partes. A primeira parte tem como objetivo a implementação de um cliente FTP. A segunda parte, dividida em várias experiências, tem como objetivo a realização de uma rede local de computadores.

O objetivo deste projeto é a aplicação num ponto de vista mais prático dos conhecimentos adquiridos ao longo do semestre, para além da utilização de conhecimentos prévios, como a programação em C ou a utilização do Linux.

Porém, devido ao curto semestre e à pandemia que assola o país, o trabalho teve de ser encurtado para apenas as primeiras cinco experiências da segunda parte, não tendo sido realizado o cliente FTP, nem as experiências 6 e 7 da segunda parte.

REDE DE COMPUTADORES

Uma rede de computadores consiste no agrupamento de vários computadores através de ligações de rede físicas (ou sem fios), de forma a estas poderem comunicar entre si. Para a ligação deste conjunto de computadores, a nível de hardware utilizam-se aparelhos externos como switches, nameservers, routers, entre outros, que têm como função encaminhar os dados dos vários computadores na rede para os destinatários corretos.

Esses aparelhos utilizados são apenas interfaces e pequenos computadores programados para realizar o roteamento e encaminhamento dos pacotes de dados, através do protocolo IPv4.

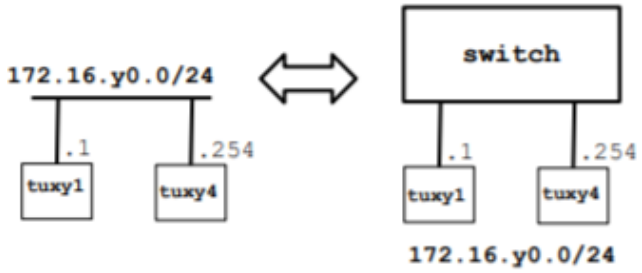
Este protocolo é o mais utilizado pois é o principal da camada de rede da internet. A nível de estrutura, o modelo OSI divide-se em 7 camadas, sendo que estas camadas são níveis de abstração, de organização da rede. São estas a camada física, a de ligação, a de rede, a de transporte, sessão, apresentação e a de aplicação.

Neste trabalho, são exploradas principalmente as vertentes das camadas física, de ligação e de rede, onde utilizando o hardware do laboratório e bibliotecas de Linux Networking criou-se uma rede local.

EXPERIÊNCIA 1

– Configurar uma rede IP

A primeira experiência tem como objetivo criar a rede IP inicial. Para isso, utilizou-se um switch e dois computadores “tuxy3” (substitui o tuxy1 do diagrama) e “tuxy4”, sendo “y“ o número da bancada. Os dois computadores estão ligados entre si pela switch, que implementa o código de encaminhamento através do endereço MAC destino de um pacote.



Para configurar o switch, ligou-se um dos computadores com a ligação porta série à consola do mesmo. Para esta experiência só seria necessário verificar que as portas do switch conectadas a cada dispositivo encontram-se na mesma VLAN.

A configuração de cada dispositivo foi feita usando os comandos presentes no ficheiro config/config_4.sh (linha 1 a 3) e config/config_3.sh (linha 1 a 3).

Para testar a configuração apagou-se a tabela ARP do computador tux3, e iniciou-se uma captura com a aplicação wireshark, e fez-se ping do tux3 para o tux4. O ficheiro de captura é o Lab_1/capturas/ping3_4.pcapng no anexo.

Analisando a captura de pacotes, pode-se verificar que quando o ping é realizado, como a tabela ARP foi apagada antes de iniciar o comando, o computador teve de realizar o protocolo ARP (request), para determinar o endereço MAC do dispositivo destino. Após receção do ARP (reply), o computador já consegue realizar o protocolo ICMP (echo request), que é o que se verifica.

1 – What are the ARP packets and what are they used for?

Os pacotes ARP servem para os computadores numa rede local trocarem entre si informações sobre os endereços MAC dos próprios dispositivos. Numa rede local, para enviar dados para um dispositivo é necessário saber o seu endereço MAC, então ele procura o mesmo endereço através do endereço IP de destino na tabela ARP. Caso essa informação não esteja armazenada na tabela, o computador efetua um ARP request com o IP do dispositivo de destino, e o endereço MAC de destino ff:ff:ff:ff:ff:ff (broadcast MAC). Devido ao broadcast todos os computadores que estejam no mesmo broadcast domain recebem o pacote ARP. O computador na rede local que tiver o endereço IP que está contido no pacote ARP (request), responde com um pacote ARP (reply), com o seu endereço MAC.

2 – What are the MAC and IP addresses of ARP packets and why?

ARP (request):

IP origem: 172.16.40.1 (eth0 tux3)	MAC origem: 00:21:5a:61:2d:72 (eth0 tux3)
IP destino: 172.16.40.254 (eth0 tux4)	MAC destino: ff:ff:ff:ff:ff:ff (MAC broadcast)

Todos os computadores que pertencem à rede local, recebem o ARP request, e apenas o computador com o IP de destino processa e responde o pedido.

ARP (reply):

IP origem: 172.16.40.254 (eth0 tux4)	MAC origem: 00:21:5a:c3:78:70 (eth0 tux4)
IP destino: 172.16.40.1 (eth0 tux3)	MAC destino: 00:21:5a:61:2d:72 (eth0 tux3)

O pacote é direcionado ao computador que originou o pedido, e contém agora o endereço MAC do IP que se procurou inicialmente.

3 – What packets does the ping command generate?

O comando ping gera pacotes ICMP echo request e ICMP echo reply.

4 – What are the MAC and IP addresses of the ping packets?

O ping gerado foi do tux3 para o tux4.

ICMP (echo request):

IP origem 172.16.40.1 (eth0 tux3)	IP destino 172.16.40.254 (eth0 tux4)
MAC origem 00:21:5a:61:2d:72 (eth0 tux3)	MAC destino 00:21:5a:c3:78:70 (eth0 tux4)

ICMP (echo reply):

IP origem 172.16.40.254 (eth0 tux4)	MAC origem 00:21:5a:c3:78:70 (eth0 tux4)
IP destino 172.16.40.1 (eth0 tux3)	MAC destino 00:21:5a:61:2d:72 (eth0 tux3)

5 – How to determine if a receiving Ethernet frame is ARP, IP, ICMP?

O header Ethernet contém a informação relativa ao tipo do pacote. Caso os bytes respetivos ao Type sejam 0x0800 o pacote é referente ao tipo IPv4, caso seja 0x0806, é referente ao tipo ARP.

Dentro do header IPv4, o byte referente ao protocol, indica o tipo do protocolo IPv4, e caso tenha o valor 0x01, é relativo ao protocolo ICMP.

6 – How to determine the length of a receiving frame?

Caso seja um pacote do tipo IPv4, no header, o 3º e 4º byte indicam o tamanho da trama.

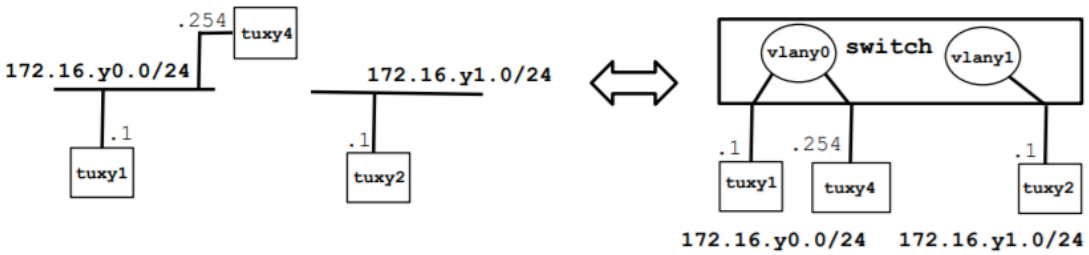
Caso seja o protocolo ARP, o comprimento deste é sempre o mesmo para o protocol type IPv4, e Hardware type Ethernet, tendo 28 bytes de informação.

7 – What is the loopback interface and why is it important?

A interface loopback é uma interface virtual que permite ao computador comunicar consigo (nas duas direções), e é utilizada principalmente para testar se as configurações estão corretas.

EXPERIÊNCIA 2

– Implementar duas LANs virtuais numa switch



Uma VLAN é uma sub-rede que pode agrupar vários dispositivos em LANs diferentes, estando estes ligados ao mesmo dispositivo, o switch. Dentro dele configura-se as portas às suas VLANs respetivas, e qualquer dispositivo que esteja conectado por uma porta fora de uma VLAN, deixa de conseguir comunicar com a rede local especificada. Esta separação de rede ocorre a nível da camada de ligação.

Esta configuração permite melhorar a segurança e a segmentação da rede, pois dá acesso a um maior grau de controlo sobre os dispositivos, e o desempenho de uma rede.

Nesta experiência criou-se duas VLANs. Os computadores tuxy3 e tuxy4 pertencem à primeira VLAN, VLANy0, e um terceiro computador, tuxy2, pertence à VLANy1. As VLANs são implementadas na switch, utilizando o CLI do mesmo através de uma ligação pela porta serie.

No tuxy3, realizou-se o comando ping para o tuxy4 e para o tuxy2 individualmente. Não se teve a possibilidade de capturar esta interação entre os dispositivos, mas o resultado esperado seria o tuxy4 responder com sucesso, e o tuxy2 por não estar na mesma VLAN que o tuxy3, não conseguir responder ao pacote.

De seguida, iniciou-se uma captura nos 3 computadores, e realizou-se um ping broadcast no tux53 na sua sub-rede 172.16.50.255. A captura de pacotes encontra-se em anexo nos ficheiros “Lab_2/capturas/broadcast3_*.pcapng”. Esta captura dá azo a duas observações, mesmo que uma delas não a pretendida. A primeira é que o ping atinge o tux54, mas não consegue chegar ao tux52. A segunda observação, a que não é desejada, é que o computador tux54 estava configurado com a opção de ignorar os ICMP echo ignore broadcasts, não tendo dado resposta ao pacote.

Deu-se inicio à mesma captura novamente, mas desta vez o tux52 fez o ping broadcast para a sua sub-rede 172.16.51.255. Aqui o resultado foi o esperado pois nenhum dos outros computados estava conectado à VLAN deste computador, não tendo sido observado este request em mais nenhum dispositivo. Os ficheiros de captura encontram-se no “Lab_2/capturas/broadcast2_*.pcapng”.

Os ficheiros de captura têm a seguinte sintaxe: “broadcast” para indicar que foi o tipo de ping empregue, “2” ou “3”, para indicar de que computador originou o comando ping, e “*” para indicar de que computador se observa a captura.

1 – How to configure VLANy0?

Os comandos utilizados para configurar a VLAN encontram-se no ficheiro “config/config_VLAN.sh” em anexo.

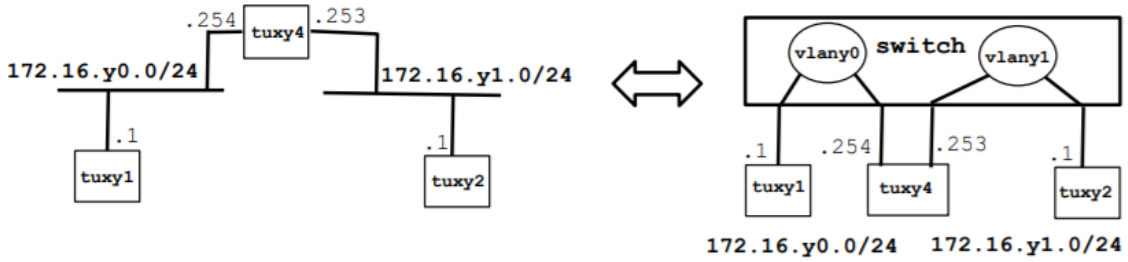
2 – How many broadcast domains are there? How can you conclude it from the logs?

Os domínios de broadcast são 2, um para cada VLAN.

Pelas capturas consegue-se observar que o broadcast feito na VLAN0 não consegue ser capturado pelo dispositivo na VLAN1, e vice-versa.

EXPERIÊNCIA 3

– Configurar um router em Linux



Na experiência 3, o computador tuxy4 foi ligado às duas VLANs e configurado como router, por forma a encaminhar os pacotes através do IP do mesmo. Não foi necessária a configuração das rotas para cada sub-rede pois cada interface de rede já teria sido configurada para cada uma das LANs.

O ficheiro "config/config_4.sh" (linha 1 a 7) descreve os comandos necessários para configurar este dispositivo como router entre as duas VLANs.

Devido à adição do tux4 como router entre a VLAN 0 e 1, tanto o tux2 como o tux3 tiveram de configurar o seu "default gateway" utilizando o IP da interface ethernet do tux4 que se encontrasse na sua VLAN. Ou seja:

- No tux2: route add default gw 172.16.41.253
- No tux3: route add default gw 172.16.40.254

Esta configuração, permite uma ligação entre os três computadores, tux2, tux3 e tux4, podendo agora comunicar entre si, apesar de se encontrarem em VLANs distintas.

O primeiro teste, foi o de verificar se através do tux2, seria possível comunicar com o tux3 e tux4. Para tal, iniciou-se uma captura de pacotes na aplicação wireshark no computador 2, e iniciou-se o comando ping no mesmo, primeiro para o computador 3, e de seguida para o computador 4. Com base nos pedidos e respostas, todos os computadores conseguem comunicar entre si. A captura de pacotes encontra-se no ficheiro "Lab_3/capturas/ping2_3,4,4.pcapng".

Para o próximo teste, as tabelas ARP dos dispositivos tux2, tux3 e tux4 foram apagadas tendo obtido a seguinte sequência de eventos:

1- ARP Request e Reply entre tux2 e tux4
2- ICMP echo request de tux2 para tux3 usando o MAC address do tux4
3- ARP request do tux4 para o tux3
4- Forward do ICMP echo request do tux4 para o tux3.

A captura de pacotes pode ser observada nos ficheiros "ping2_3-4eth0.pcapng" e "ping2_3-4eth1.pcapng". O ficheiro contendo a substring "eth1" nos ficheiros, indica a captura de pacotes pela interface de rede do tux4 que se encontra na rede local do tux2. O outro ficheiro será relativo à captura da interface de rede do tux4 na VLAN do tux3.

1 – What routes are there in the tuxes? What are their meaning?

Rotas de tuxy3:

1. Default gateway caso o IP não pertença à sub-rede deste computador.
2. Rede a que o computador pertence e por que interface deve comunicar caso pretenda comunicar com um IP desta rede.

Rotas de tuxy2:

1. Default gateway caso o IP na pertença à sub-rede deste computador.
2. Rede a que o computador pertence e por que interface deve comunicar caso pretenda comunicar com um IP desta rede.

Rotas de tuxy4:

1. Sub-rede a que a interface de rede eth0 pertence, e deve ser através da mesma que se deve comunicar caso o IP destino pertença a esta sub-rede.
2. Sub-rede a que a interface de rede eth1 pertence, e deve ser através da mesma que se deve comunicar caso o IP destino pertença a esta sub-rede.

2 – What information does an entry of the forwarding table contain?

Um elemento da tabela contém:

- O IP da sub-rede destino;
- O IP do próximo destino (Gateway);
- Netmask, utilizado para determinar os bits do IP específicos à rede, e os bits específicos ao computador
- Flags, informações específicas sobre a rota;
- Metric, "custo" de cada rota;
- Ref, número de referências – não utilizado;
- Use, contador de pesquisas pela rota;
- Interface de rede.

3 – What ARP messages, and associated MAC addresses, are observed and why?

Segundo o procedimento da experiência 3, observou-se um ARP request do computador 3 a perguntar pelo computador 4, para viabilizar o envio do ICMP echo request para o default gateway da VLAN1, e o segundo ARP request é do computador 4 a perguntar pelo dispositivo 3, para possibilitar o forward do ICMP echo request que o tux4 recebeu do tux2 para o tux3.

4 – What ICMP packets are observed and why?

Há dois pacotes que são observados, um ICMP echo request do tux2 para o tux3, e um ICMP echo reply do tux3 para o tux2.

Para esta comunicação ser possível, ao nível da camada de ligação, o computador 2 deve enviar o pacote inicialmente para o MAC address do tux4, para ser redirecionado através do IP para o tux3.

A captura de pacotes permite verificar que há 4 pacotes ICMP no total entre as duas interfaces de rede do tux4.

1. O pacote ICMP echo request com IP de origem do eth0 do tux2 para o IP de destino do eth0 do tux3, enviado pelo MAC address do eth0 do tux2 para o MAC address do eth1 do tux4.
2. O pacote ICMP echo request com IP de origem do eth0 do tux2 para o IP de destino do eth0 do tux3, enviado pelo MAC address do eth0 do tux4 para o MAC address do eth0 do tux3.
3. O pacote ICMP echo reply com IP de origem do eth0 do tux3 para o IP de destino do eth0 do tux2, enviado pelo MAC address do eth0 do tux3 para o MAC address do eth0 do tux4.
4. O pacote ICMP echo reply com IP de origem do eth0 do tux3 para o IP de destino do eth0 do tux2, enviado pelo MAC address do eth1 do tux4 para o MAC address do eth0 do tux2.

5 – What are the IP and MAC addresses associated to ICMP packets and why?

O endereço IP origem é o endereço IP da interface do computador que inicia o envio do pacote ICMP. O endereço IP destino, é o do computador com que se deseja comunicar.

Quando o computador destino se encontra na mesma sub-rede do computador de origem, verifica-se que o MAC address e o IP address de destino do pacote ping coincidem com os identificadores de um só dispositivo.

No caso do IP destino não estar inserido na sub-rede do computador de origem, o pacote terá de ser encaminhado por um (ou mais) routers ate chegar à sub-rede destino. Devido a isto, quando o computador de origem efetua o ping request, o IP de destino, é o do computador com que se deseja comunicar, mas o endereço MAC destino é o de um gateway. Para melhor descrever esta interação usa-se o exemplo do tux3 fazer o ping request ao tux2. Assim:

tux3-> tux4 -> tux2

O primeiro pacote tem como identificadores:

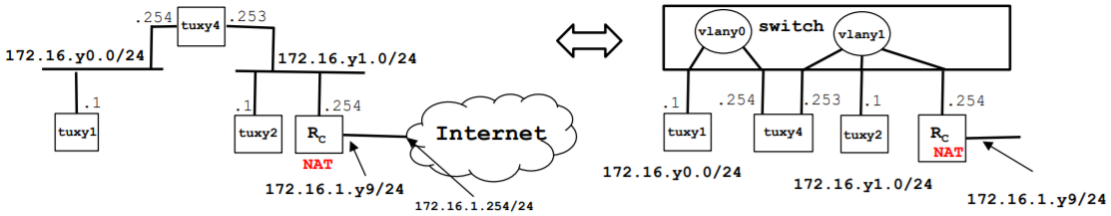
IP source: 172.16.40.1 (eth0 tux3)	MAC source: 00:21:5a:61:2f:d4 (eth0 tux3)
IP destino: 172.16.41.1 (eth0 tux2)	MAC destino: 00:21:5a:5a:7b:ea (eth0 tux4)

O segundo pacote tem como identificadores:

IP source: 172.16.40.1 (eth0 tux3)	MAC source: 00:c0:df:25:1a:f4 (eth1 tux4)
IP destino: 172.16.41.1 (eth0 tux2)	MAC destino: 00:1f:29:d7:45:c4 (eth0 tux2)

EXPERIÊNCIA 4

– Configurar um router comercial e implementar NAT



Foi ligado à rede um router comercial que permite a ligação da rede local à rede do laboratório (e internet).

A configuração do router foi feita com os comandos apresentados no ficheiro "config/config_router.sh" presente no anexo.

A configuração dos computadores para esta aula laboratorial foi feita através dos ficheiros "config/config_2.sh", "config/config_3.sh" e "config/config_4.sh".

Verificou-se que tuxy3 consegue comunicar com todas as interfaces de tuxy4, tuxy2, e Rc utilizando comandos ping.

Após realizar o procedimento indicado no guião da aula laboratorial, realizaram-se dois tipos de ping, um em que o tux2 desativa a opção de ICMP redirect, e outro em que o ICMP redirect volta a ser ativado.

O ICMP_redirect é utilizado por routers para indicar aos computadores host que há uma melhor rota (endereço alternativo como próximo hop) para o IP destino. O router só envia este pacote no caso de:

1. A interface que recebeu o pacote do host é a mesma interface utilizada para o próximo hop.
2. A sub-rede do próximo hop pertence à mesma sub-rede que o host.

Após receção deste pacote, o host redireciona o pacote para o IP indicado pelo router através do pacote ICMP redirect no caso desta definição estar configurada no host.

Antes de se configurar o NAT no router, enviou-se um ping request do tux3 (172.16.40.1) para o router do laboratório (172.16.1.254), observando-se que o pacote consegue chegar ao seu destino, mas devido ao facto do IP source do pacote não ser substituído por um IP da rede do laboratório válido (através do protocolo NAT), o ICMP echo reply não consegue chegar ao computador host que originou o pedido, pois seria enviado para o IP da rede privada 172.16.40.1.

Após configuração do NAT no router, já se conseguiu verificar um ICMP echo request e reply no tux3, pois quando o pacote passa da rede interna para a externa o protocolo NAT troca o IP source do pacote para um IP da sua NAT pool, que será um IP único da rede do laboratório. Aquando do envio do pacote ICMP echo reply, este consegue sempre chegar ao router Rc, pois é o identificador deste na rede do lab.

1 – How to configure a static route in a commercial router?

Para enviar comandos e configurar o router comercial é necessária uma ligação série com o CLI do router através de um dos computadores do laboratório. Acedendo à aplicação do GTKTerm no computador invocam-se os comandos presentes no ficheiro "config/config_router.sh" em anexo.

No ficheiro acima mencionado, os comandos que configuram as rotas estáticas estão presentes nas linha 30 e 31 do mesmo.

2 – What are the paths followed by the packets in the experiments carried out and why?

A sequência de hops ("saltos") do primeiro pacote em ambos os casos da experiência (com ICMP redirect e sem ICMP redirect) é a seguinte:

1. O tux2 identifica que o IP de destino não consta em nenhuma das sub-redes da sua tabela de rotas, e envia o pacote para o seu default gateway, Rc.
2. O Rc tem configurado que o próximo hop para a sub-rede 172.16.40.0/24 deve ser feita usando o router tux4 através do seu endereço 172.16.41.253 na interface de rede eth1, e envia o pacote para este dispositivo.
3. O router Rc envia um pacote ICMP_redirect para o host para indicar que o gateway address 172.16.41.253 deve ser utilizado quando este deseja comunicar com o IP 172.16.40.1;
4. O tux4 reencaminha o pacote para o tux3 que está na sua sub-rede da interface eth0.

No caso do tux2 não ter a opção do ICMP_redirect configurado, o computador não altera as suas configurações, mantendo a mesma sequência de hops previamente mencionado. Mas no caso desta definição estar configurada, os próximos pacotes de ICMP echo request têm a seguinte estrutura:

1. O tux2 envia o ICMP request para o tux4 (172.16.41.253);
2. O tux4 encaminha o pacote para o tux3 (172.16.40.1).

Esta interação pode ser verificada na captura de pacotes feita nos ficheiros "Lab_4/capturas/ping2_3.pcapng" e "Lab_4/capturas/ping2_3_icmp_on.pcapng".

O primeiro ficheiro demonstra o caso da captura ter sido feito sem o tux2 aceitar o ICMP redirect, verificando-se continuamente o router a indicar a rota alternativa através do pacote ICMP redirect.

No segundo ficheiro, já se pode verificar que o ping passa uma vez pelo router, o host tux2 recebe o ICMP redirect, e o próximo ping request já vai diretamente para o tux4.

3 – How to configure NAT in a commercial router?

Para configurar o NAT, na CLI do router, é necessário:

1. Criar uma pool de IPs que serão utilizados para substituir o IP de origem proveniente de um computador da rede interna.
2. Uma lista no router que pode aceder a estes IPs.

3. Acrescentar os IPs da rede interna que pertencem à lista do ponto 2.

Estes passos estão descritos no ficheiro “config/config_router.sh” nas linhas 22 a 27.

4 – What does NAT do?

O NAT é um protocolo que funciona ao nível do router, e que tem como objetivo trocar endereços de IP privados para endereços IP públicos válidos e idealmente únicos na rede externa, e vice-versa.

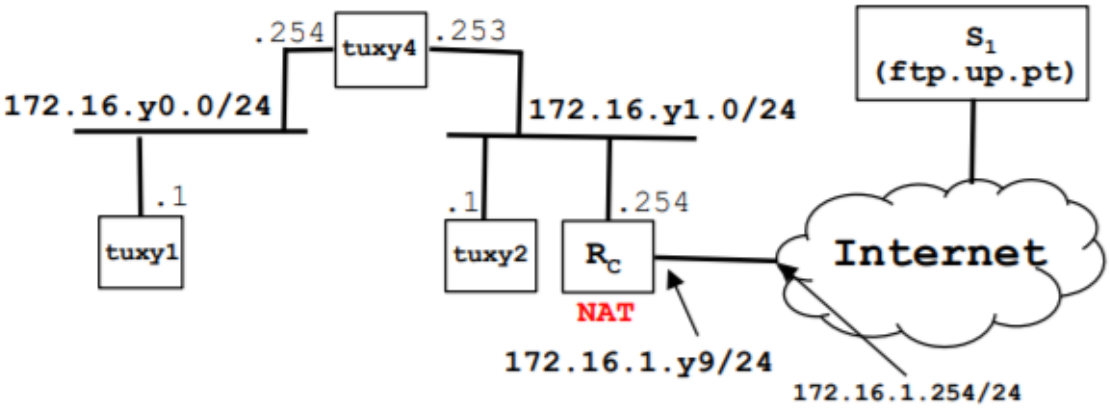
Quando o router recebe um pacote direcionado para uma rede externa, no caso do NAT estar configurado, o IP de origem é substituído por um IP que pertença a uma NAT pool do router, e encaminhado para o IP de destino. Quando o dispositivo de destino responder a este pedido, a resposta é encaminhada para o IP atribuído pelo protocolo NAT, ou seja, para o router, e aquando da chegada do pacote ao router, o IP de destino da resposta é atualizado com o IP do dispositivo que inicializou a comunicação em primeiro lugar.

O protocolo baseia-se na tabela NAT que permite identificar o IP privado e a porta de comunicação, através do IP público e a porta de comunicação do router no pacote que chega ao router.

EXPERIÊNCIA 5

– DNS

Nesta experiência foi configurado o serviço DNS nos tuxy1, tuxy4, tuxy2. Um servidor DNS constitui um dos nós de uma base de dados distribuída que traduz os hostnames a endereços IP.



1 – How to configure the DNS service at a host?

O serviço DNS é configurado modificando o ficheiro /etc/resolv.conf. Neste ficheiro deve-se acrescentar em lista de prioridade uma linha com "nameserver 172.16.1.2", sendo o IP apresentado o do servidor DNS.

Após introduzir um hostname (ex. google.com), é feito um DNS query ao nameserver estabelecido no ficheiro, e o servidor tenta resolver o hostname para um endereço IP. Caso este seja bem sucedido, é retornado o IP do servidor do mesmo hostname ao dispositivo que iniciou o DNS query.

2 – What packets are exchanged by DNS and what information is transported.

São enviados pacotes DNS cuja estrutura é:

- Header, contém a descrição do tipo de pacote;
- Queries, contém o hostname;
- Answers, para um pacote de resposta contém o endereço IP associado ao hostname.

Primeiro, é enviado um pacote DNS (query) com um pedido de endereço IP através de um hostname, e a seguir o servidor responde com um pacote DNS (response) contendo o hostname e o respetivo endereço IP.

CONCLUSÕES

Este trabalho foi extremamente interessante para a nossa aprendizagem de redes de computadores, pois permitiu que aplicássemos o conhecimento adquirido ao longo das aulas. As capturas de pacotes são muito relevantes neste aspeto pois confirmam todos os aspetos teóricos sobre os protocolos de rede.

Infelizmente, devido às restrições temporais não foi possível continuar a desenvolver e terminar as experiências, nem desenvolver a aplicação ftp.

Este trabalho permitiu constatar todos os factos sobre o funcionamento básico de uma rede:

- A interligação das várias camadas, aumentando o nível de abstração e complexidade do software gradualmente;
- A necessidade dos endereços físicos (MAC) e os endereços do protocolo da internet;
- A existência de vários domínios de colisão;
- A necessidade de uma switch para o agrupamento de vários computadores, criando uma rede;
- A necessidade do estabelecimento de rotas entre os vários dispositivos da rede para a transmissão eficiente dos dados;
- A importância das redes locais virtuais, para o agrupamento virtual de dispositivos que estão ligados ao mesmo dispositivo, o switch;
- A necessidade da descoberta automática de rotas entre os vários computadores de uma rede, para esta ser flexível;
- A necessidade do protocolo ICMP para diagnóstico e controlo de uma rede;
- A importância do NAT e de um router comercial para o estabelecimento da ligação entre a nossa rede local e outras redes;
- A importância do DNS para obter os endereços associados aos hostnames automaticamente.

REFERÊNCIAS

Imagens retiradas do guião do Lab2.

Hiperligações:

IP Packet header: https://flylib.com/books/en/2.298.1.25/1/

DNS: https://accedian.com/blog/dns-query-main-types/

ARP: https://en.wikipedia.org/wiki/Address_Resolution_Protocol

ICMP redirect: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

NAT: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg.html

https://tldp.org/HOWTO/NET3-4-HOWTO.html

Todas as hiperligações foram consultadas a 23 de dez. de 2020.