



# Redes de Computadores I

---

Relatório do Redes I 2018/2019

Docentes: Adriano Jorge Cardoso Moreira  
João Rui Magalhães Velho Cunha Galvão



# Elementos do grupo

---

Hugo Machado, A80362

José Bravo, A80132

Nathália Viana, E8801



# Índice

---

Glossário .....	
Introdução .....	
Emulação de LANs Ethernet .....	
Interligação de LANs e redes IP .....	
DHCP .....	
Uso das camadas de rede e transporte por parte das aplicações .....	
Interligação via NAT .....	



## Glossário

---

**ARP (Address Resolution Protocol)** - O ARP estabelece uma ligação entre o endereço físico da placa de rede e o endereço IP. A placa de rede de um PC contém uma tabela onde faz a ligação entre os endereços físicos e lógicos dos computadores da rede. Quando um PC quer comunicar com outro verifica se o computador está presente na rede. Se estiver presente, envia os dados diminuindo o tráfego, caso contrário envia um sinal designado por pedido ARP para determinar o seu endereço.

**DHCP (Dynamic Host Configuration Protocol)** – Protocolo responsável por reduzir a complexidade e morosidade das configurações TCP/IP numa rede. Através deste serviço é possível atribuir, automaticamente, as configurações do protocolo TCP/IP numa rede.

**FTP (File Transfer Protocol)** - Permite a transferência de dados ou ficheiros entre computadores mesmo com sistemas operativos diferentes.

**HTTP (Hypertext Transfer Protocol)** - Protocolo responsável pela troca ou transferência de hipertexto (texto estruturado que utiliza ligações lógicas entre nós)

**ICMP (Internet Control Message Protocol)** – Protocolo responsável para enviar mensagens de resposta de pacotes de informação que não foram entregues corretamente. Deste modo, é enviada uma mensagem ICMP e o pacote de informação não recebido volta a ser enviado.

**IP (Internet Protocol)** – Protocolo responsável por estabelecer o contacto entre os computadores emissor e recetor de maneira a que a informação não se perca na rede.

**TCP (Transmission Control Protocol)** – Protocolo que permite dar segurança à transferência de informação e verificar se a mesma foi bem recebida, caso contrário, volta a enviar essa informação.

**LAN (Local Area Networks)** – Rede local

**NAT (Network Address Translation)** - Protocolo que consiste em reescrever, recorrendo a uma tabela, os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede privada tenha acesso ao exterior (rede pública).



# Introdução

---

No âmbito da Unidade Curricular Redes de Computadores I procedemos ao desenvolvimento deste projeto prático, que tem como objetivo promover a aquisição de competências de redes de computadores com base nas tecnologias Ethernet e TCP/IP.

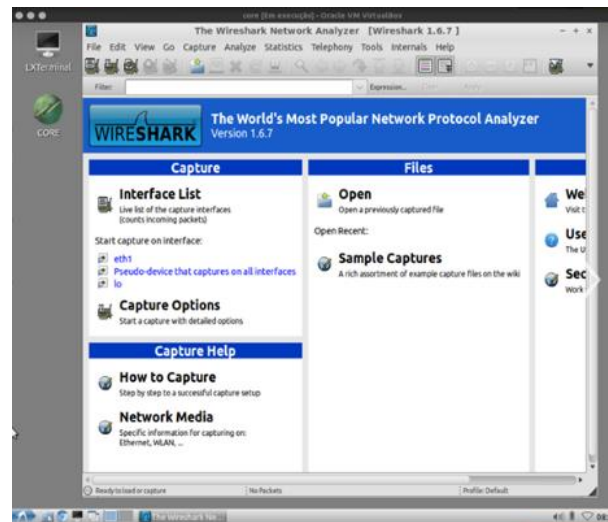
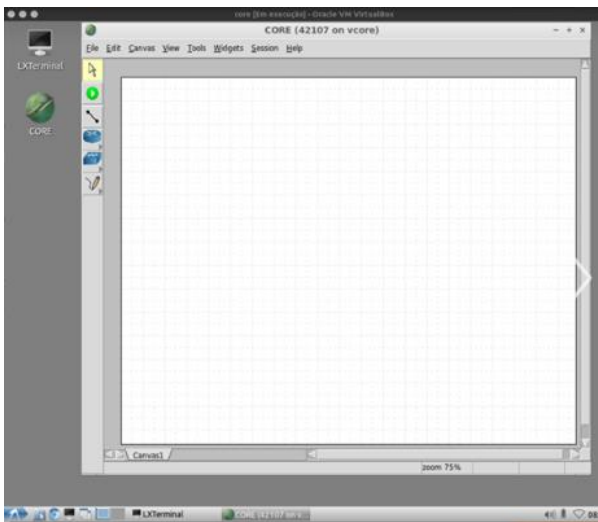
Este relatório relata o desenvolvimento dos problemas propostos pelos docentes, que envolvem a emulação de diferentes redes e a sua interligação.

As ferramentas fundamentais para a realização deste projeto foram, sobretudo, o emulador de redes CORE (utilizado para estabelecer e configurar diferentes topologias de rede) e o Wireshark (utilizado para efetuar testes de conectividade e analisar capturas de tráfego).

## Fase 1 – Instalação e familiarização

---

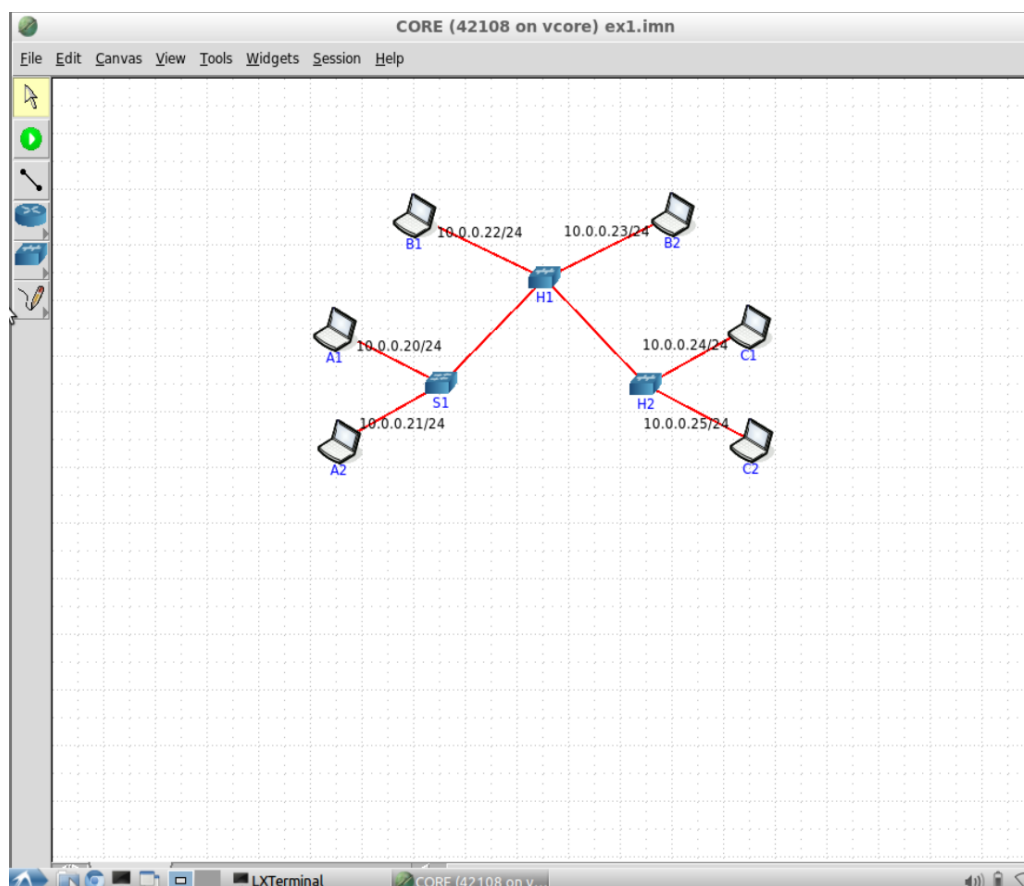
Nesta primeira fase começamos por instalar a Virtual Box, a virtual box do CORE e o Wireshark. Na Virtual Box instala-mos também as ferramentas pedidas no Anexo A, os servidores FTP e HTTP, retificámos as permissões para a captura de tráfego a partir do CORE.



## Fase 2- Emulação de LANs Ethernet

Neste primeiro exercício temos como objetivo emular uma pequena rede local (LAN), utilizando a interface gráfica do CORE.

Neste exercício foi nos pedido para construir uma rede local usando dois hubs (h1, h2) e um switch (s1) com a topologia indicada na figura do enunciado. Também nos foi proposto que cada switch ou hub tivesse no mínimo dois computadores ligados e organizado pelas letras A,B e C. Na configuração desta rede desativamos os endereços IPv6 e os endereços IPv4 deixámos ficar os atribuidos automaticamente, conforme nos foi pedido .



*Figura 1- Topologia pedida com os componentes pedidos*

Após a construção da rede local testamos a conectividade através do comando ping entre os computadores A1 e C2, com o Wireshark a capturar tráfego da placa de rede conforme ilustrado nas figuras 2 e 3.

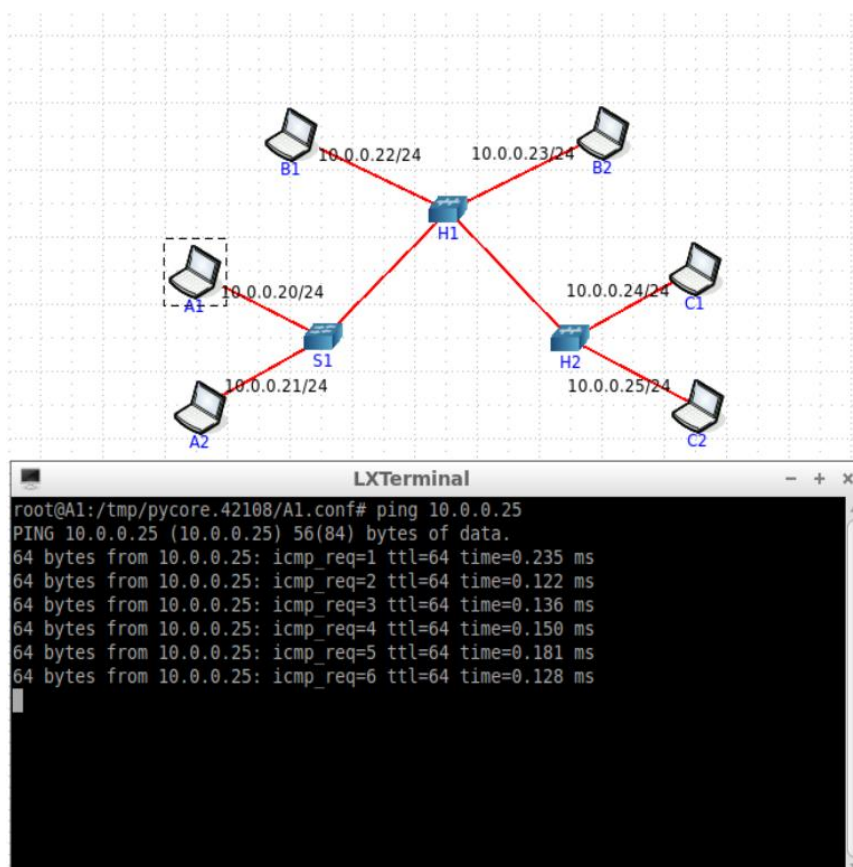


Figura 2-Execução do comando ping

No.	Time	Source	Destination	Protocol	Length	Info
30	14.000133	10.0.0.25	10.0.0.20	ICMP	98	Echo (ping) reply id=...
31	15.000130	10.0.0.20	10.0.0.25	ICMP	98	Echo (ping) request id=...
32	15.000229	10.0.0.25	10.0.0.20	ICMP	98	Echo (ping) reply id=...
33	15.003709	00:00:00_aa:00:05	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.20? Tell...
34	15.003730	00:00:00_aa:00:00	00:00:00_aa:00:05	ARP	42	10.0.0.20 is at 00:00:00...
35	16.000332	10.0.0.20	10.0.0.25	ICMP	98	Echo (ping) request id=...
36	16.000426	10.0.0.25	10.0.0.20	ICMP	98	Echo (ping) reply id=...
37	16.999884	10.0.0.20	10.0.0.25	ICMP	98	Echo (ping) request id=...
38	16.999979	10.0.0.25	10.0.0.20	ICMP	98	Echo (ping) reply id=...
39	17.999947	10.0.0.20	10.0.0.25	ICMP	98	Echo (ping) request id=...
40	18.000043	10.0.0.25	10.0.0.20	ICMP	98	Echo (ping) reply id=...

Figura 3-Captura do protocolo ARP

No Wireshark foram capturados dois protocolos diferentes, o ICMP e o ARP.





## Fase 3- Interligação de LANs e redes IP

Nesta fase construímos uma rede de interligação de redes locais (LAN) e redes de IP, de forma a que seja possível encaminhar tráfego a partir de uma rede para outra rede local diferente.

A topologia pedida é constituída por LANs diferentes (A,B,C,D e E), sendo que cada uma delas está centrada num Hub ou Switch com um mínimo de dois PCs. Para cada uma destas redes deve existir um router distinto com caminhos alternativos.

Foi nos fornecida a gama de endereços 192.168.0.0/24 para a interligação dos routers e a gama 10.9.0.0/23 para as redes locais, sendo que por rede temos um número predefinido de estações.

Rede	Número de estações
A	288
B	59
C	59
D	27
E	11

Figura 4

### Tabelas de Endereçamento

#### Redes Locais

Nome	IP de Rede	Máscara	Gama	IP de Difusão	IP de Router
A1	10.9.0.0	/24	.0.1 - 254	.0.255	.0.1
A2	10.9.1.0	/26	.1.1 - 62	.1.63	.1.1
B	10.9.1.64	/26	.1.65 - 126	.1.127	.1.65
C	10.9.1.128	/26	.1.129 - 190	.1.191	.1.129
D	10.9.1.192	/27	.1.193 - 222	.1.223	.1.193
E	10.9.1.224	/27	.1.225 - 254	.1.255	.1.225



## Sub-redes entre routers

Ligação		
AB	192.168.0.1/30	192.168.0.2/30
AC	192.168.0.5/30	192.168.0.6/30
BD	192.168.0.9/30	192.168.0.10/30
BE	192.168.0.13/30	192.168.0.14/30
CD	192.168.0.17/30	192.168.0.18/30
CE	192.168.0.21/30	192.168.0.22/30
DE	192.168.0.25/30	192.168.0.26/30

## Tabelas de Encaminhamento

As tabelas seguintes têm como função indicar o encaminhamento atribuído aos diferentes routers, sendo que são estes os responsáveis por definir as rotas entre as diferentes topologias.

Router-A	Rede destino	Mascara	Int. de saída	Próx. Nó
A1	10.9.0.0	/24	10.9.0.1	
A2	10.9.1.0	/26	10.9.1.1	
B	10.9.1.64	/26	192.168.0.1	192.168.0.2
C	10.9.1.128	/26	192.168.0.5	192.168.0.6
D	10.9.1.192	/27	192.168.0.1	192.168.0.2
E	10.9.1.224	/27	192.168.0.5	192.168.0.6

Router-B	Rede destino	Mascara	Int. de saída	Próx. Nó
A1	10.9.0.0	/24	192.168.0.2	192.168.0.1
A2	10.9.1.0	/26	192.168.0.2	192.168.0.1
B	10.9.1.64	/26	10.9.1.65	
C	10.9.1.128	/26	192.168.0.2	192.168.0.1
D	10.9.1.192	/27	192.168.0.9	192.168.0.10
E	10.9.1.224	/27	192.168.0.13	192.168.0.14



Router-C	Rede destino	Mascara	Int. de saída	Próx. Nó
A1	10.9.0.0	/24	192.168.0.6	192.168.0.5
A2	10.9.1.0	/26	192.168.0.6	192.168.0.5
B	10.9.1.64	/26	192.168.0.6	192.168.0.5
C	10.9.1.128	/26	10.9.1.129	
D	10.9.1.192	/27	192.168.0.17	192.168.0.18
E	10.9.1.224	/27	192.168.0.21	192.168.0.22

Router-D	Rede destino	Mascara	Int. de saída	Próx. Nó
A1	10.9.0.0	/24	192.168.0.10	192.168.0.9
A2	10.9.1.0	/26	192.168.0.10	192.168.0.9
B	10.9.1.64	/26	192.168.0.10	192.168.0.9
C	10.9.1.128	/26	192.168.0.18	192.168.0.17
D	10.9.1.192	/27	10.9.1.193	
E	10.9.1.224	/27	192.168.0.25	192.168.0.26

Router-E	Rede destino	Mascara	Int. de saída	Próx. Nó
A1	10.9.0.0	/24	192.168.0.22	192.168.0.21
A2	10.9.1.0	/26	192.168.0.22	192.168.0.21
B	10.9.1.64	/26	192.168.0.14	192.168.0.13
C	10.9.1.128	/26	192.168.0.22	192.168.0.21
D	10.9.1.192	/27	192.168.0.26	192.168.0.25
E	10.9.1.224	/27	10.9.1.225	

Nas figuras seguintes estão representadas as configurações efetuadas nos routers A,B,C,D e E, sendo que utilizamos o comando `ip route` para definir as rotas a seguir pelos pacotes de informação.

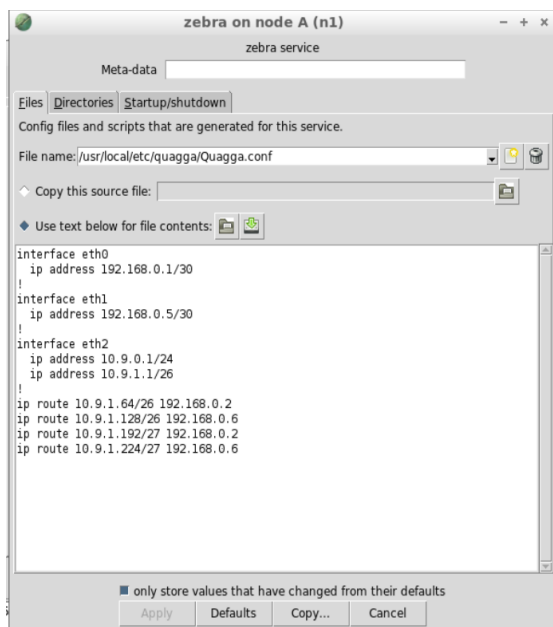


Figura 6- Configuração do zebra do router A

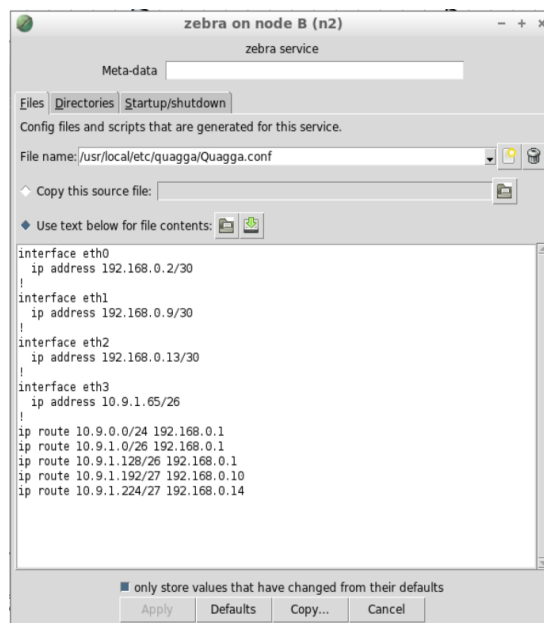


Figura 5- Configuração do zebra do router B

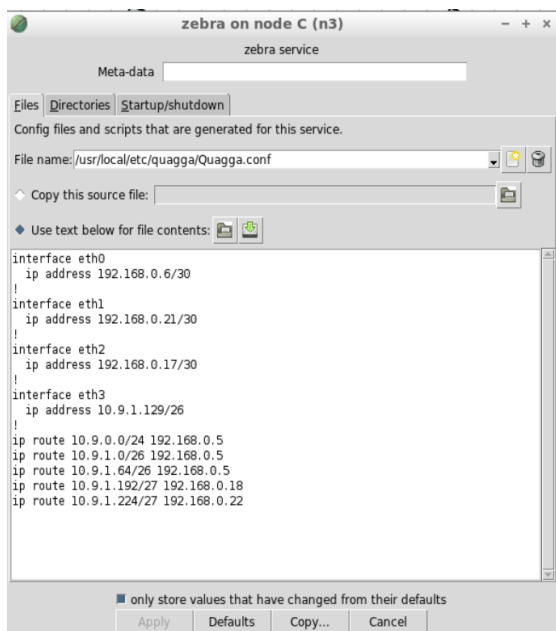


Figura 7-Configuração do zebra do router C

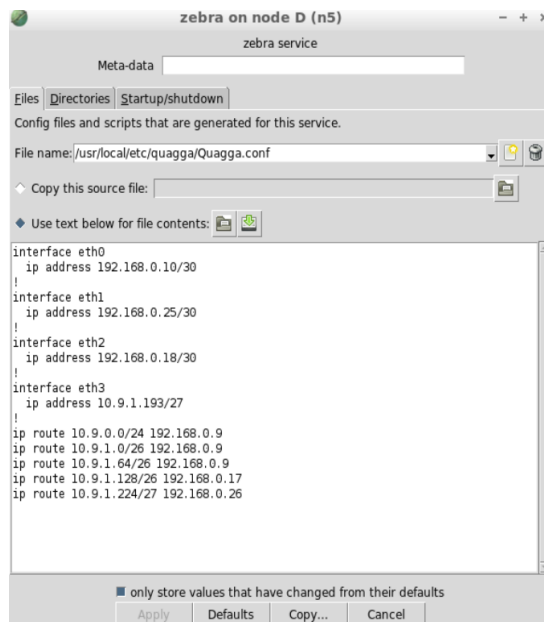


Figura 8-Configuração do zebra do router D

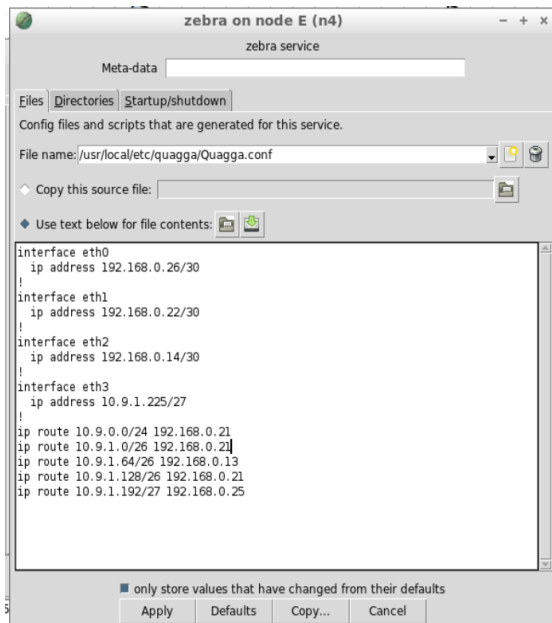


Figura 9-Configuração do zebra do router  
E

De modo a testar a conectividade entre as redes, recorreremos aos comandos ping e traceroute, conforme ilustrado nas figuras seguintes.

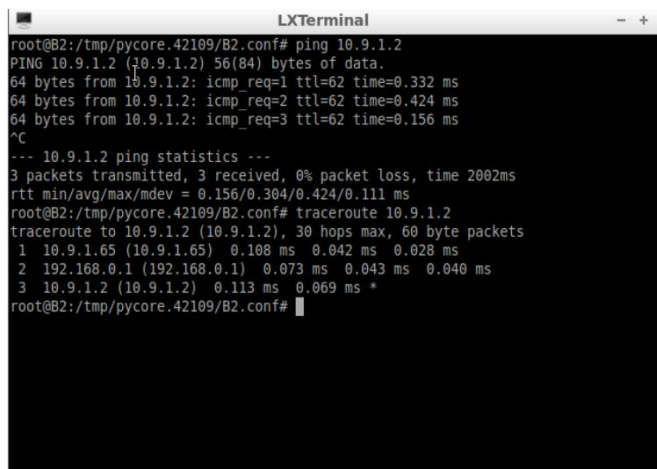


Figura 8- Ping e Traceroute do PC B2 para  
o PC A21

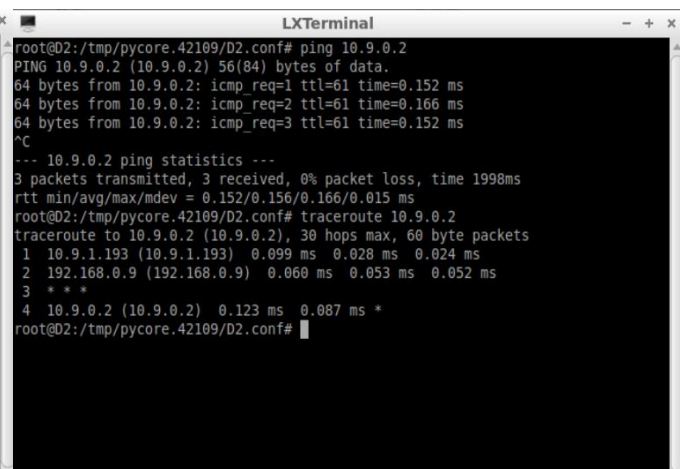


Figura 7- Ping e Traceroute do PC D2 para o  
PC A11

## Fase 4 - DHCP

Nesta fase recorreremos ao protocolo DHCP para configurar os elementos da rede de forma automática e dinâmica. Desta forma tivemos que colocar um servidor na Rede Local B, nesse servidor ativámos o protocolo DHCP e nos PCs da rede ativámos o protocolo DHCP Client.

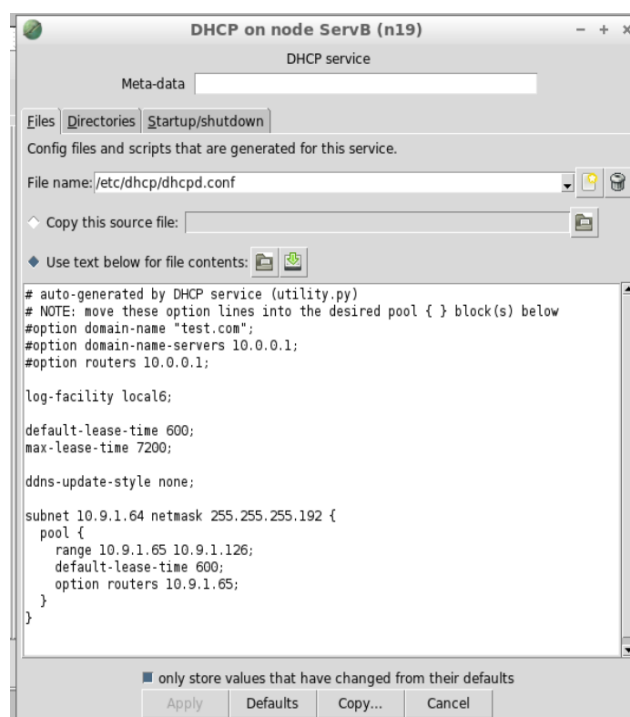


Figura 12- Configuração do servidor DHCP da rede local B

Nesta configuração introduzimos a sub-rede que o servidor DHCP pertence e a sua mascara (/26 ou 255.255.255.192), de seguida em *range* está a gama de endereços de que podem ser atribuídos, e no ultimo parametro *option routers* o IP do Router dessa mesma rede.

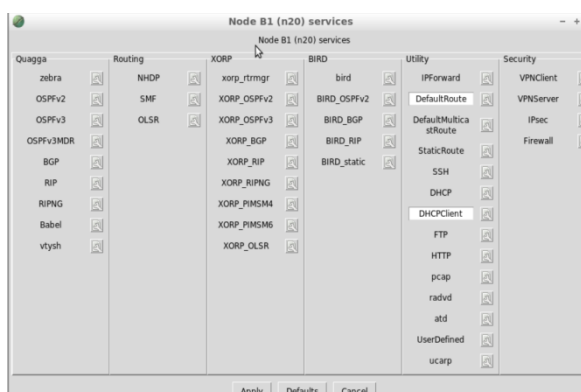


Figura 13- Ativação do DHCP Client nos PCs da rede local B



Para verificar se o DHCP está bem configurado, ligamos o Wireshark no início de sessão no CORE, para confirmar se os endereços estavam a ser atribuídos com sucesso aos PCs da rede local.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.229451	00:00:00_aa:00:1d	Broadcast	ARP	42	Who has 10.9.1.68? Tell 10.9.1.66
7	0.239550	10.9.1.66	10.9.1.68	DHCP	342	DHCP Offer - Transaction ID 0x7704dd24
8	0.240303	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x7704dd24
9	0.249451	00:00:00_aa:00:1d	Broadcast	ARP	42	Who has 10.9.1.67? Tell 10.9.1.66
10	0.250684	10.9.1.66	10.9.1.68	DHCP	342	DHCP ACK - Transaction ID 0x7704dd24
11	0.259295	00:00:00_aa:00:1d	Broadcast	ARP	42	Who has 10.9.1.69? Tell 10.9.1.66
12	0.259402	10.9.1.66	10.9.1.67	DHCP	342	DHCP Offer - Transaction ID 0x5d356779
13	0.259832	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5d356779
14	0.261018	10.9.1.66	10.9.1.67	DHCP	342	DHCP ACK - Transaction ID 0x5d356779
15	0.269385	10.9.1.66	10.9.1.69	DHCP	342	DHCP Offer - Transaction ID 0x3f65394f
16	0.269662	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3f65394f
17	0.271396	10.9.1.66	10.9.1.69	DHCP	342	DHCP ACK - Transaction ID 0x3f65394f

Figura 9-Captura dos protocolos DHCP no servidor DHCP

Como pudemos verificar, os IPs foram atribuídos com sucesso. Podemos verificar também que existem três pedidos diferentes dentro de um protocolo DHCP, para a atribuição de IPs.

- *ARP* - O *ARP* é lançado em *Broadcast*, ou seja para todos os endereços da rede, com um pedido de configurações DHCP.
- *DHCP Offer* – Neste pacote é enviado as configurações de rede para o cliente DHCP.
- *DHCP Request* – Aqui o cliente DHCP responde em *Broadcast* que aceita a proposta do pacote anterior.
- *DHCP ACK* – Resposta por parte do servidor, em que confirma a atribuição do IP do cliente.

## Fase 5- Uso das camadas de rede e transporte por parte das aplicações

Nesta fase foi nos proposto para inserir na rede local C um servidor HTTP e testá-lo.

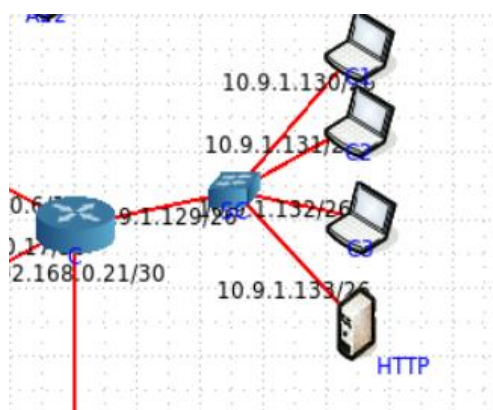


Figura 14-Implementação do servidor HTTP

As figuras seguintes representam as configurações efetuadas no servidor HTTP (Figura 15), sendo que na Figura 16 está representada a execução do comando `wget -S` que permitiu analisar se o servidor HTTP estava a responder de acordo com o esperado. A Figura 17 é a representação das capturas de tráfego na rede ilustrando o estabelecimento de uma conexão TCP como também o pedido HTTP.



Figura 10- Configuração do servidor HTTP



```

LXTerminal
root@B1:/tmp/pycore.42110/B1.conf# wget -S 10.9.1.133/26
--2018-12-28 11:13:40-- http://10.9.1.133/26
Connecting to 10.9.1.133:80... connected.
HTTP request sent, awaiting response...
HTTP/1.1 404 Not Found
Date: Fri, 28 Dec 2018 19:13:41 GMT
Server: Apache/2.2.22 (Ubuntu)
Content-Length: 276
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
2018-12-28 11:13:40 ERROR 404: Not Found.

root@B1:/tmp/pycore.42110/B1.conf#

```

*Figura 11-Comando wget -S para o IP do servidor HTTP*

Capturing from n28.eth0.218 [Wireshark 1.6.7]

Time	Source	Destination	Protocol	Length	Info
1 0.000000	10.9.1.68	10.9.1.133	TCP	74	43895 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SAC
2 0.000044	10.9.1.133	10.9.1.68	TCP	74	http > 43895 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 M
3 0.000139	10.9.1.68	10.9.1.133	TCP	66	43895 > http [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=
4 0.001119	10.9.1.68	10.9.1.133	HTTP	178	GET /26 HTTP/1.1
5 0.001151	10.9.1.133	10.9.1.68	TCP	66	http > 43895 [ACK] Seq=1 Ack=113 Win=14480 Len=0 TSva
6 0.002411	10.9.1.133	10.9.1.68	HTTP	559	HTTP/1.1 404 Not Found (text/html)
7 0.002665	10.9.1.68	10.9.1.133	TCP	66	43895 > http [ACK] Seq=113 Ack=494 Win=15680 Len=0 TS
8 0.004578	10.9.1.68	10.9.1.133	TCP	66	43895 > http [FIN, ACK] Seq=113 Ack=494 Win=15680 Len
9 0.004653	10.9.1.133	10.9.1.68	TCP	66	http > 43895 [FIN, ACK] Seq=494 Ack=114 Win=14480 Len
10 0.004746	10.9.1.68	10.9.1.133	TCP	66	43895 > http [ACK] Seq=114 Ack=495 Win=15680 Len=0 TS
11 5.001346	00:00:00_aa:00:15	00:00:00_aa:00:22	ARP	42	Who has 10.9.1.133? Tell 10.9.1.129
12 5.001315	00:00:00_aa:00:22	00:00:00_aa:00:15	ARP	42	Who has 10.9.1.129? Tell 10.9.1.133
13 5.001374	00:00:00_aa:00:22	00:00:00_aa:00:15	ARP	42	10.9.1.133 is at 00:00:00_aa:00:22
14 5.001401	00:00:00_aa:00:15	00:00:00_aa:00:22	ARP	42	10.9.1.129 is at 00:00:00_aa:00:15

*Figura 12-Captura dos protocolos HTTP no Wireshark*

# Interligação via NAT (Network Address Translator)

Nesta última fase tínhamos como objetivo acrescentar uma rede local privada á topologia anterior, sendo que os endereços utilizados nesta rede são da gama 192.168.1.0/24 . Decidimos ligar esta nova rede privada ao switch da rede local D, utilizando para tal o router NAT.

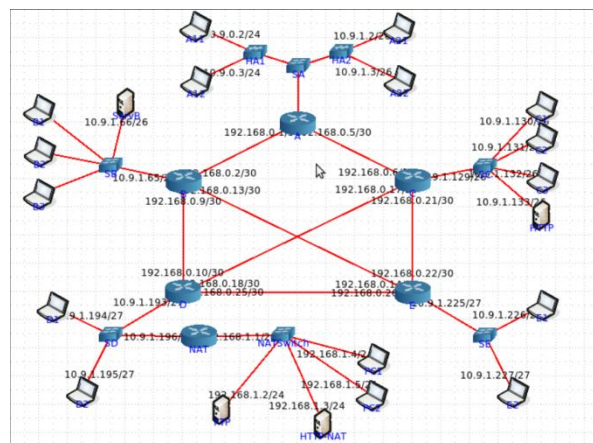


Figura da topologia completa com a rede privada NAT

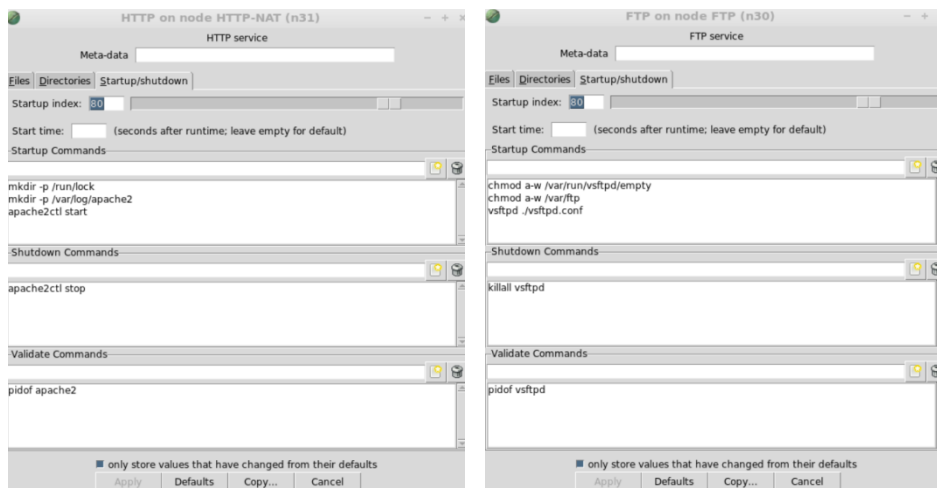
Configuração do router *NAT*, com os seus encaminhamentos para a outras redes.

```

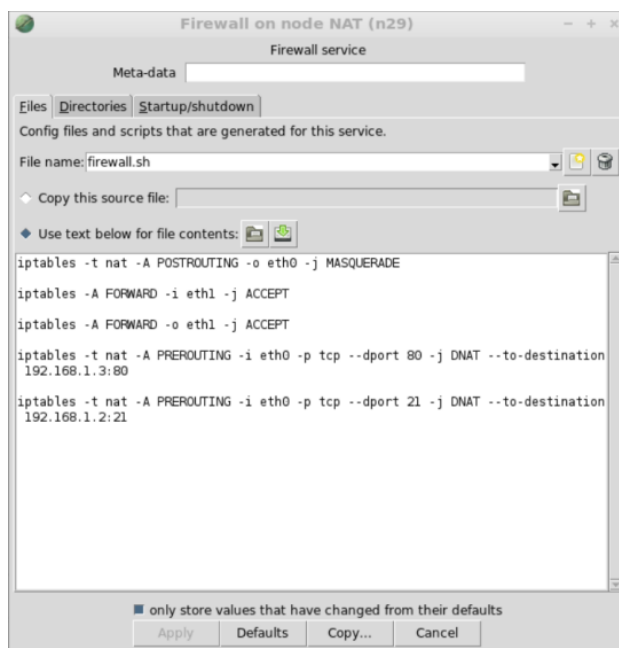
zebra on node NAT (n29)
zebra service
Meta-data
Files Directories Startup/shutdown
Config files and scripts that are generated for this service.
File name: /usr/local/etc/quagga/Quagga.conf
Copy this source file:
Use text below for file contents:
interface eth0
ip address 10.9.1.196/27
!
interface eth1
ip address 192.168.1.1/24
!
ip route 10.9.0.0/24 10.9.1.193
ip route 10.9.1.0/26 10.9.1.193
ip route 10.9.1.64/26 10.9.1.193
ip route 10.9.1.128/26 10.9.1.193
ip route 10.9.1.224/27 10.9.1.193
!
ip forwarding

```

## Configuração dos servidores HTTP e FTP.



Por fim configuramos a *firewall* do router *NAT*, através de *ip tables*, que introduz um novo encaminhamento no router *NAT*.



O primeiro comando, faz com que os elementos da rede privado possam comunicar com as outras redes.

Os dois seguintes comandos, deixam que os elementos da rede local a qual a rede privada está intergada comuniquem.

E os dois ultimos comandos disponibilizam os servidores HTTP e FTP para as redes locais externas.



## Conclusão

---

Este trabalho prático foi fundamental na familiarização com as ferramentas de simulação de redes bem como o Wireshark no diagnóstico e análise de tráfego. Toda esta ambientalização foi-se tornando mais fácil com o decorrer do desenvolvimento do projeto. Relativamente às diferentes configurações e topologias de redes, conseguimos compreender os protocolos associados bem como as suas funções. Em suma, a realização deste trabalho foi essencial para transpor para uma componente mais prática e real, todos os conceitos e temas abordados no decorrer do semestre nas aulas da UC Redes de Computadores I.