Licenciatura em Engenharia de Telecomunicações e Informática

Redes de Computadores I - Departamento de Sistemas de Informação

Trabalho Prático

Simulação de LANs Ethernet e redes TCP/IP usando o CORE

Tiago Diogo A103665

José Novais A105056

Miguel Machado A103668

3ºano | 1ºSemestre |24/25

Índice

Introdução

No âmbito da unidade curricular de Redes de Computadores I, foi proposto aos alunos sumarizar os conhecimentos obtidos ao longo da UC no formato de um trabalho prático. Para o desenvolvimento deste projeto recorremos à utilização das ferramentas CORE, um emulador de redes, e o Wireshark, uma ferramenta de diagnóstico.

Este projeto é constituído por 5 exercícios que abordam diversos temas da unidade curricular:

1. Emulação de LANs Ethernet - O primeiro exercício propõem emular no CORE uma pequena rede local onde seja possível executar diagnósticos de conectividade, capturas e análise de tráfego

2. Interligação de LANs e redes IP - Neste segundo exercício é pedido a interligação de redes locais Ethernet com recurso a routers para encaminhar todo o tráfego IP entre as diferentes redes.

3. DHCP (Dynamic Host Configuration Protocol) – Nesta terceira parte é pretendido o uso do protocolo DHCP para ativar a configuração dinâmica e automática dos endereços IP numa rede local

4. Uso das camadas de rede e transporte por parte das aplicações – Na quarta parte do projeto é requisitado o instalamento de um servidor HTTP na rede resultante, que se encontra apta para suportar serviços e suportar aplicações de rede

5. Interligação via NAT (Network Address Translator) – Corresponde à fase final do projeto tendo o objetivo de implementar o protocolo NAT de modo a permitir que um computador de uma rede interna (privada) tenha acesso ao exterior.

Ao longo deste trabalho exploramos tecnologias como a Ethernet e TCP/IP, assim como diversos protocolos que suportam as redes.

Assim sendo, neste relatório iremos expressar as nossas conclusões sobre o funcionamento de uma rede.

1. Emulação de LANs Ethernet

a) Construção da topologia

Nesta topologia de rede local são usados 1 Hub(H1) e dois Switches(S1, S2), os dispositivos são Pc´s e estão identificados pelos números 1,2,3,4,5 e 6.

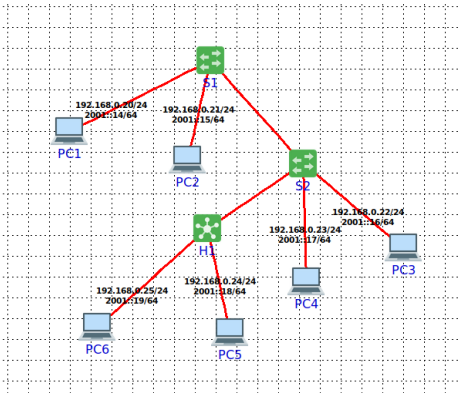


Figura 1– Criação da topologia

b) Testes de Conectividade

Para testar a conectividade foi feito um *ping* entre os computadores PC1 para o PC6 e também do PC3 para o PC1. Este comando PING (em modo execução) testa a conectividade entre os sistemas terminais recorrendo ao ICMP(Internet Control Message Protocol) que envia um pacote(request) para a máquina destino e aguarda uma resposta(reply). Se o destinatário estiver ativo, o emissor receberá uma resposta. Com isto, testamos o envio de pacotes entre os sistemas terminais, assim como a sua chegada. Neste exemplo, confirmamos que existe conectividade entre os sistemas PC1, PC3 e PC6.

```
root@PC1:/tmp/pycore.1/PC1.conf# ping 192.168.0.25
PING 192.168.0.25 (192.168.0.25) 56(84) bytes of data.
64 bytes from 192.168.0.25: icmp_seq=1 ttl=64 time=0.438 ms
64 bytes from 192.168.0.25: icmp_seq=2 ttl=64 time=0.092 ms
64 bytes from 192.168.0.25: icmp_seq=3 ttl=64 time=0.106 ms
64 bytes from 192.168.0.25: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 192.168.0.25: icmp_seq=5 ttl=64 time=0.112 ms
64 bytes from 192.168.0.25: icmp_seq=6 ttl=64 time=0.096 ms
^C
--- 192.168.0.25 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5123ms
rtt min/avg/max/mdev = 0.092/0.157/0.438/0.125 ms
root@PC1:/tmp/pycore.1/PC1.conf#
```

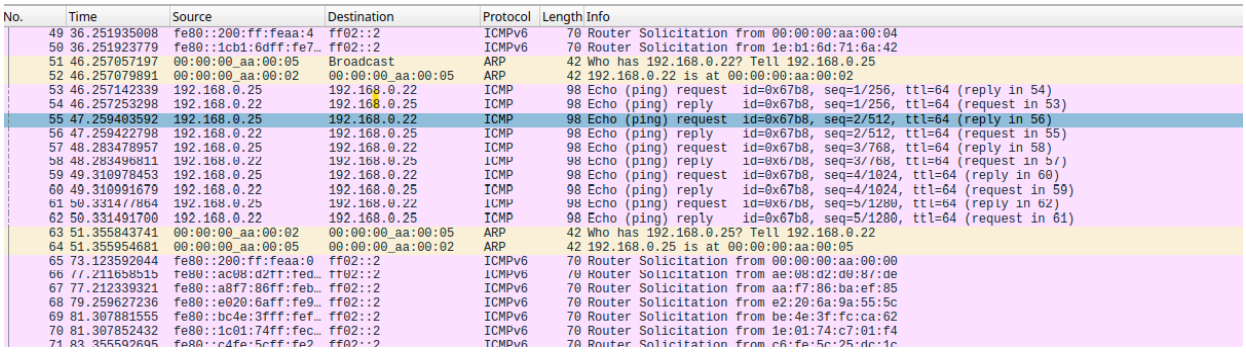
Figura 2- Teste de Conectividade (Ping) do PC1 para PC6

```
root@PC3:/tmp/pycore.1/PC3.conf# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=64 time=0.323 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=64 time=0.073 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=64 time=0.073 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=64 time=0.081 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=64 time=0.078 ms
^C
--- 192.168.0.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.073/0.125/0.323/0.098 ms
root@PC3:/tmp/pycore.1/PC3.conf#
```

Figura 2 1- Teste de Conectividade (Ping) do PC3 para PC1

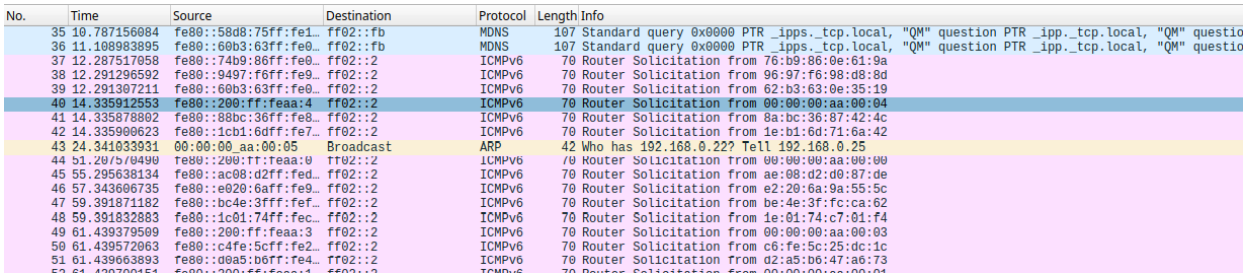
Recorrendo ao Wireshark, foi possível capturar o tráfego entre os PCs PC1 e PC6 nos PCs 3,4 e 5.

c) Testes de Conectividade



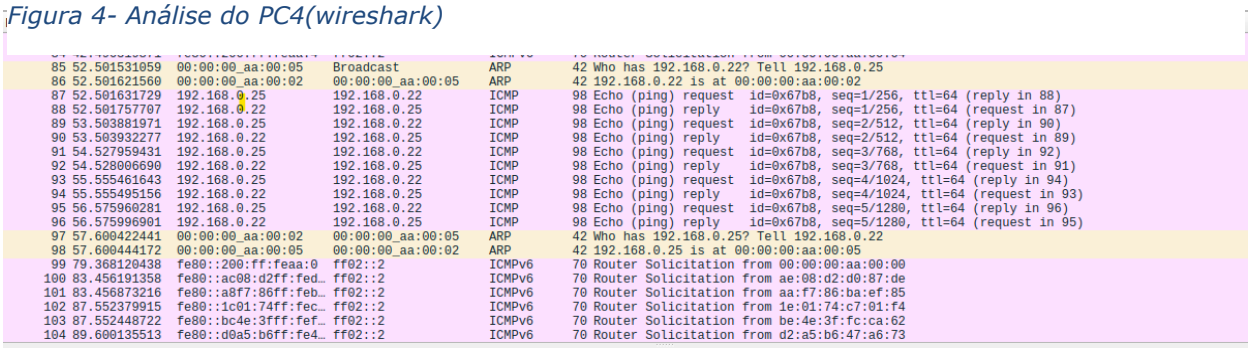
No.	Time	Source	Destination	Protocol	Length	Info
49	36.251935008	fe80::200:ff:feaa:4	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:04
50	36.251923779	fe80::1cb1:6dff:fe7…	ff02::2	ICMPv6	70	Router Solicitation from 1e:b1:6d:71:6a:42
51	46.257057197	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 192.168.0.22? Tell 192.168.0.25
52	46.257079891	00:00:00_aa:00:02	00:00:00_aa:00:05	ARP	42	192.168.0.22 is at 00:00:00:aa:00:02
53	46.257142339	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=1/256, ttl=64 (reply in 54)
54	46.257253298	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=1/256, ttl=64 (request in 53)
55	47.259403592	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=2/512, ttl=64 (reply in 56)
56	47.259422798	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=2/512, ttl=64 (request in 55)
57	48.283478957	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=3/768, ttl=64 (reply in 58)
58	48.283496811	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=3/768, ttl=64 (request in 57)
59	49.310978453	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=4/1024, ttl=64 (reply in 60)
60	49.310991679	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=4/1024, ttl=64 (request in 59)
61	50.3314778…	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=5/1280, ttl=64 (reply in 62)
62	50.331491700	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=5/1280, ttl=64 (request in 61)
63	51.355843741	00:00:00_aa:00:02	00:00:00_aa:00:05	ARP	42	Who has 192.168.0.25? Tell 192.168.0.22
64	51.355954681	00:00:00_aa:00:05	00:00:00_aa:00:02	ARP	42	192.168.0.25 is at 00:00:00:aa:00:05
65	73.123592044	fe80::200:ff:feaa:0	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
66	77.211658515	fe80::ac08:d2ff:fed…	ff02::2	ICMPv6	70	Router Solicitation from ae:08:d2:d0:87:de
67	77.212339321	fe80::a8f7:86ff:feb…	ff02::2	ICMPv6	70	Router Solicitation from aa:f7:86:ba:ef:85
68	79.259627236	fe80::e020:6aff:fe9…	ff02::2	ICMPv6	70	Router Solicitation from e2:20:6a:9a:55:5c
69	81.307881555	fe80::bc4e:3fff:fef…	ff02::2	ICMPv6	70	Router Solicitation from be:4e:3f:fc:ca:62
70	81.307852432	fe80::1c01:74ff:fec…	ff02::2	ICMPv6	70	Router Solicitation from 1e:01:74:c7:01:f4
71	83.355592695	fe80::c4fe:5cff:fe2…	ff02::2	ICMPv6	70	Router Solicitation from c6:fe:5c:25:dc:1c

Figura 3- Análise do PC3(wireshark)



No.	Time	Source	Destination	Protocol	Length	Info
35	10.787156084	fe80::58d8:75ff:fe1…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" questio
36	11.108983895	fe80::60b3:63ff:fe0…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" questio
37	12.287517058	fe80::74b9:86ff:fe0…	ff02::2	ICMPv6	70	Router Solicitation from 76:b9:86:0e:61:9a
38	12.291296592	fe80::9497:f6ff:fe9…	ff02::2	ICMPv6	70	Router Solicitation from 96:97:f6:98:d8:8d
39	12.291307211	fe80::60b3:63ff:fe0…	ff02::2	ICMPv6	70	Router Solicitation from 62:b3:63:0e:35:19
40	14.335912553	fe80::200:ff:feaa:4	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:04
41	14.335878802	fe80::88bc:36ff:fe8…	ff02::2	ICMPv6	70	Router Solicitation from 8a:bc:36:87:42:4c
42	14.335900623	fe80::1cb1:6dff:fe7…	ff02::2	ICMPv6	70	Router Solicitation from 1e:b1:6d:71:6a:42
43	24.341033931	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 192.168.0.22? Tell 192.168.0.25
44	51.207570490	fe80::200:ff:feaa:0	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
45	55.295638134	fe80::ac08:d2ff:fed…	ff02::2	ICMPv6	70	Router Solicitation from ae:08:d2:d0:87:de
46	57.343606735	fe80::e020:6aff:fe9…	ff02::2	ICMPv6	70	Router Solicitation from e2:20:6a:9a:55:5c
47	59.391871182	fe80::bc4e:3fff:fef…	ff02::2	ICMPv6	70	Router Solicitation from be:4e:3f:fc:ca:62
48	59.391832883	fe80::1c01:74ff:fec…	ff02::2	ICMPv6	70	Router Solicitation from 1e:01:74:c7:01:f4
49	61.439379509	fe80::200:ff:feaa:3	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:03
50	61.439572063	fe80::c4fe:5cff:fe2…	ff02::2	ICMPv6	70	Router Solicitation from c6:fe:5c:25:dc:1c
51	61.439663893	fe80::d0a5:b6ff:fe4…	ff02::2	ICMPv6	70	Router Solicitation from d2:a5:b6:47:a6:73

Figura 4- Análise do PC4(wireshark)



85	52.501531059	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 192.168.0.22? Tell 192.168.0.25
86	52.501621560	00:00:00_aa:00:02	00:00:00_aa:00:05	ARP	42	192.168.0.22 is at 00:00:00:aa:00:02
87	52.501631729	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=1/256, ttl=64 (reply in 88)
88	52.501757707	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=1/256, ttl=64 (request in 87)
89	53.503881971	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=2/512, ttl=64 (reply in 90)
90	53.503932277	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=2/512, ttl=64 (request in 89)
91	54.527959431	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=3/768, ttl=64 (reply in 92)
92	54.528006690	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=3/768, ttl=64 (request in 91)
93	55.555461643	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=4/1024, ttl=64 (reply in 94)
94	55.555495156	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=4/1024, ttl=64 (request in 93)
95	56.575960281	192.168.0.25	192.168.0.22	ICMP	98	Echo (ping) request id=0x67b8, seq=5/1280, ttl=64 (reply in 96)
96	56.575996901	192.168.0.22	192.168.0.25	ICMP	98	Echo (ping) reply id=0x67b8, seq=5/1280, ttl=64 (request in 95)
97	57.600422441	00:00:00_aa:00:02	00:00:00_aa:00:05	ARP	42	Who has 192.168.0.25? Tell 192.168.0.22
98	57.600444172	00:00:00_aa:00:05	00:00:00_aa:00:02	ARP	42	192.168.0.25 is at 00:00:00:aa:00:05
99	79.368120438	fe80::200:ff:feaa:0	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
100	83.456191358	fe80::ac08:d2ff:fed…	ff02::2	ICMPv6	70	Router Solicitation from ae:08:d2:d0:87:de
101	83.456873216	fe80::a8f7:86ff:feb…	ff02::2	ICMPv6	70	Router Solicitation from aa:f7:86:ba:ef:85
102	87.552379915	fe80::1c01:74ff:fec…	ff02::2	ICMPv6	70	Router Solicitation from 1e:01:74:c7:01:f4
103	87.552448722	fe80::bc4e:3fff:fef…	ff02::2	ICMPv6	70	Router Solicitation from be:4e:3f:fc:ca:62
104	89.600135513	fe80::d0a5:b6ff:fe4…	ff02::2	ICMPv6	70	Router Solicitation from d2:a5:b6:47:a6:73

Figura 5- Análise do PC5(wireshark)

Desse modo, foi possível perceber o funcionamento dos SWITCHEs e HUBs assim como dos protocolos utilizados (ARP e ICMP).

Primeiramente é enviado um ARP Request a partir do PC6, para se fazer a pergunta "quem tem este ip?", que vai ter ao HUB(H1) e este envia em broadcast para todos os que lhe estão ligados o ARP Request.
O PC5 recebe esse ARP Request e o Switch(S2) também o recebe, e como o Switch está a receber em Broadcast, este envia também para todos, sendo estes o PC3, PC4 e Switch(S1).
Como foi enviado por Broadcast pelo S2, tanto o PC3 como o PC4 vão receber o ARP Request.
O PC3 é o que tem o IP que o PC6 quer saber quem tem, vai responder com um ARP Reply, para dizer que é ele que tem o IP e envia também o seu endereço MAC.
Como o Switch já sabe onde está o PC6, a partir do primeiro ARP, já só vai enviar para o local de onde recebeu o ARP, pelo que o PC4 já não vai receber

o ARP Reply enviado pelo PC3.
Ao chegar ao HUB(H1) ele vai enviar para todos, pois os HUBS não "aprendem" como os Switchs, pelo que o PC5 vai receber o ARP Reply enviado pelo PC3 com destino para o PC6, e o próprio PC6 também vai receber o ARP Reply.
Quem recebeu o ARP Reply também vai receber os pings entre as duas máquinas (PC6 e PC3).
Desta maneira percebemos o detalhe do funcionamento dos HUBs e dos SWITCHs.
No fim do Ping o PC3 envia um ARP Request para o PC6, e o PC6 um ARP Reply, só os PC3, PC5 e PC6 é que vão receber estes ARPs.
Desta maneira também percebemos o funcionamento dos protocolos ARP e ICMP.

O ICMP(Internet Control Message Protocol) é um protocolo que permite gerir problemas na transmissão de dados e é usado pelos sistemas terminais e encaminhadores para trocarem informação do nível de rede.

2. Interligação de Redes

a) Construção da Topologia Requisitada

Tal como pedido no enunciado, criamos a topologia com pelo menos 6 routers (R1, R2, R3, R4, R5, R6) diretamente ligados às respectivas redes com o R6 de interligação entre routers. As cinco redes (A, B, C, D, E) foram criadas com base em dois Switchs e um Hub, com 6 PCs terminais em cada uma, á semelhança do exercício 1.

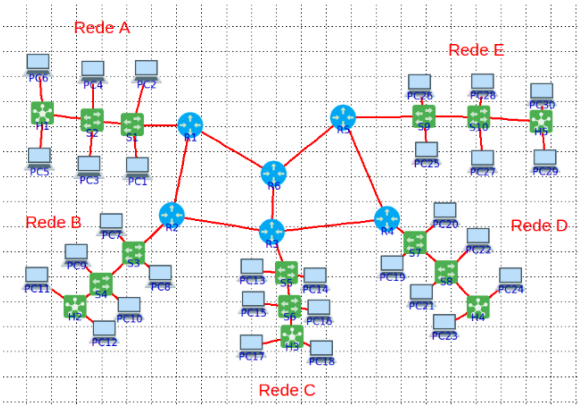


Figura 6-Estrutura da rede

b) Esquema de endereçamento

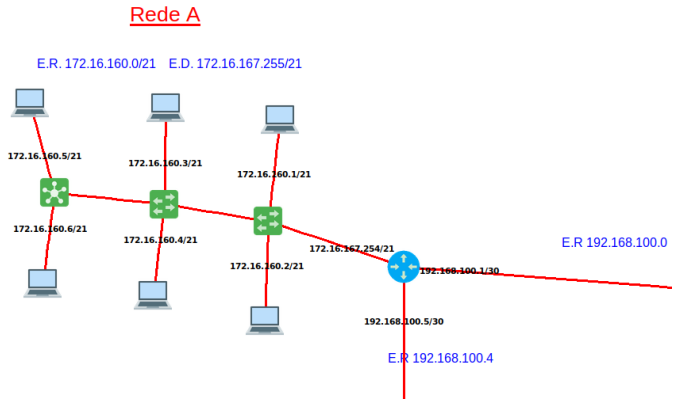


Figura 8- Estrutura e endereços rede A

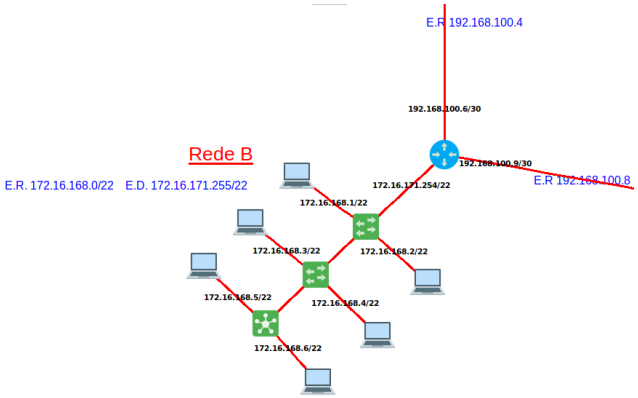


Figura 7-Estrutura e endereços rede B

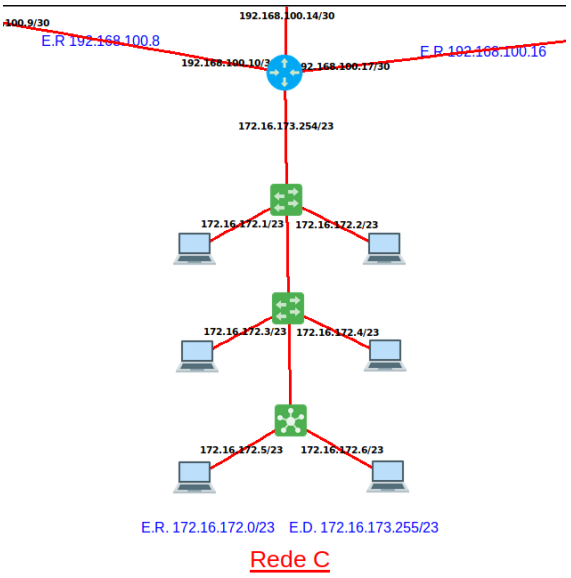


Figura 9-Estrutura e endereços rede C

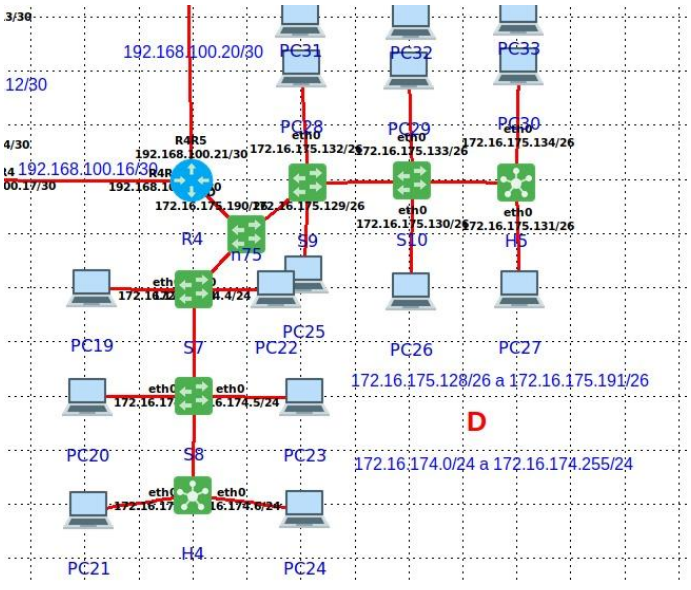


Figura 10-Estrutura e endereços rede D

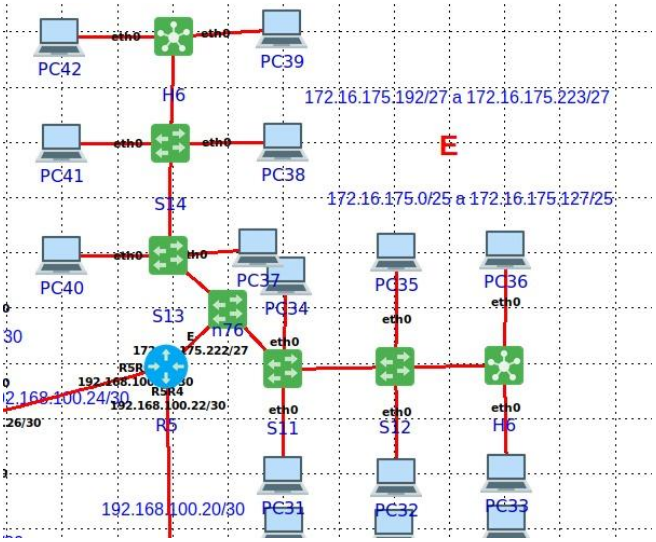


Figura 11-Estrutura e endereços rede E

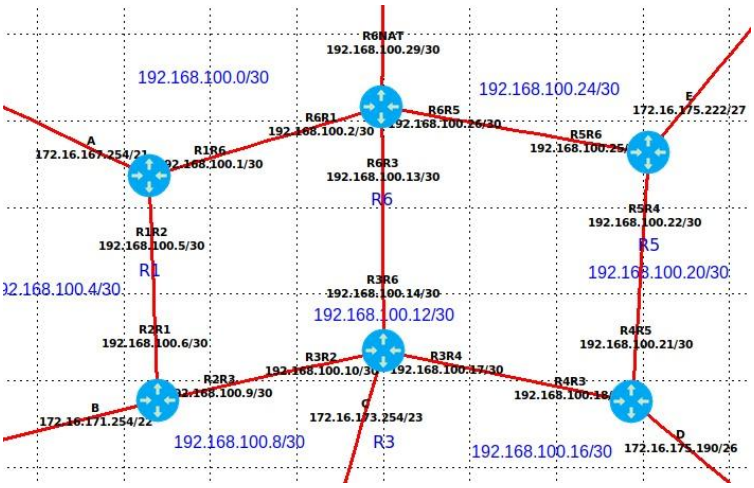


Figura 12-Estrutura e endereços dos routers

ID Rede	Endereço de Rede	Endereço de Difusão	Máscara	Endereços Válidos
A	172.16.160.0	172.16.167.255	255.255.248.0/21	De 172.16.160.1 a 172.16.167.254
B	172.16.168.0	172.16.171.255	255.255.252.0/22	De 172.16.168.1 a 172.16.171.254
C	172.16.172.0	172.16.173.255	255.255.254.0/23	De 172.16.172.1 a 172.16.173.254
D1	172.16.174.0	172.16.174.255	255.255.255.0/24	De 172.16.174.1 a 172.16.174.254
D1	172.16.175.0	172.16.175.127	255.255.255.128/25	De 172.16.175.1 a 172.16.175.126
D2	172.16.175.178	172.16.175.191	255.255.255.192/26	De 172.16.175.179 a 172.16.175.191
E2	172.16.175.192	172.16.175.223	255.255.255.224/27	De 172.16.175.193 a 172.16.175.222
NAT	192.168.200.0	192.16.200.55	255.255.255.0/24	De 192.168.200.1 a 192.16.200.54

Tabela 1- Tabela de Endereçamento

ID Rede	Endereço de Rede	Endereço de Difusão	Máscara	Endereços Válidos
R1 – R6	192.168.100.0	192.168.100.3	255.255.255.252/30	De 192.168.100.1 a 192.168.100.2
R1 – R2	192.168.100.4	192.168.100.7	255.255.255.252/30	De 192.168.100.5 a 192.168.100.6
R2 – R3	192.168.100.8	192.168.100.11	255.255.255.252/30	De 192.168.100.9 a 192.168.100.10
R3 – R6	192.168.100.12	192.168.100.15	255.255.255.252/30	De 192.168.100.13 a 192.168.100.14
R3 – R4	192.168.100.16	192.168.100.19	255.255.255.252/30	De 192.168.100.17 a 192.168.100.19
R4 – R5	192.168.100.20	192.168.100.23	255.255.255.252/30	De 192.168.100.21 a 192.168.100.22
R5 – R6	192.168.100.24	192.168.100.27	255.255.255.252/30	De 192.168.100.25 a 192.168.100.26
R6 – R7	192.168.100.28	192.168.100.31	255.255.255.252/30	De 192.168.200.29 a 192.16.200.30

Tabela 2- Tabela de Endereçamento

c) Esquema de encaminhamento

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	172.16.167.254	255.255.248.0/21	----------
(B)172.16.168.0	192.168.100.5	255.255.252.0/22	192.168.100.6
(C)172.16.172.0	192.168.100.5	255.255.254.0/23	192.168.100.6
(D1)172.16.174.0	192.168.100.1	255.255.255.0/24	192.168.100.2
(E1)172.16.175.0	192.168.100.1	255.255.255.128/25	192.168.100.2
(D2)172.16.175.128	192.168.100.1	255.255.255.192/26	192.168.100.2
(E2)172.16.175.192	192.168.100.1	255.255.255.224/27	192.168.100.2
(R1 – R6) 192.168.100.0	192.168.100.1	255.255.255.252/30	----------
(R1 - R2) 192.168.100.4	192.168.100.5	255.255.255.252/30	----------
(R2 – R3) 192.168.100.8	192.168.100.5	255.255.255.252/30	192.168.100.6
(R3 – R6) 192.168.100.12	192.168.100.1	255.255.255.252/30	192.168.100.2
(R3 – R4) 192.168.100.16	192.168.100.5	255.255.255.252/30	192.168.100.6
(R4 – R5) 192.168.100.20	192.168.100.1	255.255.255.252/30	192.168.100.2
(R5 – R6) 192.168.100.24	192.168.100.1	255.255.255.252/30	192.168.100.2
(R6 – R7) 192.168.100.28	192.168.100.1	255.255.255.252/30	192.168.100.2
(NAT) 192.168.200.0	192.168.100.1	255.255.255.0/24	192.168.100.2

Tabela 3- Tabela de Encaminhamento Router 1

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.6	255.255.248.0/21	192.168.100.5
(B)172.16.168.0	172.16.171.254	255.255.252.0/22	----------
(C)172.16.172.0	192.168.100.9	255.255.254.0/23	192.168.100.10
(D1)172.16.174.0	192.168.100.9	255.255.255.0/24	192.168.100.10
(E1)172.16.175.0	192.168.100.6	255.255.255.128/25	192.168.100.5
(D2)172.16.175.128	192.168.100.9	255.255.255.192/26	192.168.100.10
(E2)172.16.175.192	192.168.100.6	255.255.255.224/27	192.168.100.5
(R1 – R6) 192.168.100.0	192.168.100.6	255.255.255.252/30	192.168.100.5
(R1 - R2) 192.168.100.4	192.168.100.6	255.255.255.252/30	----------
(R2 – R3) 192.168.100.8	192.168.100.9	255.255.255.252/30	----------
(R3 – R6) 192.168.100.12	192.168.100.9	255.255.255.252/30	192.168.100.10
(R3 – R4) 192.168.100.16	192.168.100.9	255.255.255.252/30	192.168.100.10
(R4 – R5) 192.168.100.20	192.168.100.9	255.255.255.252/30	192.168.100.10
(R5 – R6) 192.168.100.24	192.168.100.9	255.255.255.252/30	192.168.100.10
(R6 – R7) 192.168.100.28	192.168.100.9	255.255.255.252/30	192.168.100.10
(NAT) 192.168.200.0	192.168.100.6	255.255.255.0/24	192.168.100.5

Tabela 4- Tabela de Encaminhamento Router2

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.10	255.255.248.0/21	192.168.100.9
(B)172.16.168.0	192.168.100.10	255.255.252.0/22	192.168.100.9
(C)172.16.172.0	172.16.173.254	255.255.254.0/23	----------
(D1)172.16.174.0	192.168.100.17	255.255.255.0/24	192.168.100.18
(E1)172.16.175.0	192.168.100.14	255.255.255.128/25	192.168.100.13
(D2)172.16.175.128	192.168.100.17	255.255.255.192/26	192.168.100.18
(E2)172.16.175.192	192.168.100.14	255.255.255.224/27	192.168.100.13
(R1 – R6) 192.168.100.0	192.168.100.14	255.255.255.252/30	192.168.100.13
(R1 - R2) 192.168.100.4	192.168.100.10	255.255.255.252/30	192.168.100.9
(R2 – R3) 192.168.100.8	192.168.100.10	255.255.255.252/30	----------
(R3 – R6) 192.168.100.12	192.168.100.14	255.255.255.252/30	----------
(R3 – R4) 192.168.100.16	192.168.100.17	255.255.255.252/30	----------
(R4 – R5) 192.168.100.20	192.168.100.17	255.255.255.252/30	192.168.100.18
(R5 – R6) 192.168.100.24	192.168.100.14	255.255.255.252/30	192.168.100.13
(R6 – R7) 192.168.100.28	192.168.100.14	255.255.255.252/30	192.168.100.13
(NAT) 192.168.200.0	192.168.100.14	255.255.255.0/24	192.168.100.13

Tabela 5- Tabela de encaminhamento Router3

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.18	255.255.248.0/21	192.168.100.17
(B)172.16.168.0	192.168.100.18	255.255.252.0/22	192.168.100.17
(C)172.16.172.0	192.168.100.18	255.255.254.0/23	192.168.100.17
(D1)172.16.174.0	172.16.174.254	255.255.255.0/24	----------
(E1)172.16.175.0	192.168.100.21	255.255.255.128/25	192.168.100.22
(D2)172.16.175.128	172.16.175.190	255.255.255.192/26	----------
(E2)172.16.175.192	192.168.100.21	255.255.255.224/27	192.168.100.22
(R1 – R6) 192.168.100.0	192.168.100.18	255.255.255.252/30	192.168.100.17
(R1 - R2) 192.168.100.4	192.168.100.18	255.255.255.252/30	192.168.100.17
(R2 – R3) 192.168.100.8	192.168.100.18	255.255.255.252/30	192.168.100.17
(R3 – R6) 192.168.100.12	192.168.100.18	255.255.255.252/30	192.168.100.17
(R3 – R4) 192.168.100.16	192.168.100.18	255.255.255.252/30	----------
(R4 – R5) 192.168.100.20	192.168.100.21	255.255.255.252/30	----------
(R5 – R6) 192.168.100.24	192.168.100.21	255.255.255.252/30	192.168.100.22
(R6 – R7) 192.168.100.28	192.168.100.18	255.255.255.252/30	192.168.100.17
(NAT) 192.168.200.0	192.168.100.18	255.255.255.0/24	192.168.100.17

Tabela 6- Tabela de encaminhamento Router4

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.25	255.255.248.0/21	192.168.100.26
(B)172.16.168.0	192.168.100.25	255.255.252.0/22	192.168.100.26
(C)172.16.172.0	192.168.100.25	255.255.254.0/23	192.168.100.26
(D1)172.16.174.0	192.168.100.22	255.255.255.0/24	192.168.100.21
(E1)172.16.175.0	172.16.175.126	255.255.255.128/25	----------
(D2)172.16.175.128	192.168.100.22	255.255.255.192/26	192.168.100.21
(E2)172.16.175.192	172.16.175.222	255.255.255.224/27	----------
(R1 – R6) 192.168.100.0	192.168.100.25	255.255.255.252/30	192.168.100.26
(R1 - R2) 192.168.100.4	192.168.100.25	255.255.255.252/30	192.168.100.26
(R2 – R3) 192.168.100.8	192.168.100.25	255.255.255.252/30	192.168.100.26
(R3 – R6) 192.168.100.12	192.168.100.25	255.255.255.252/30	192.168.100.26
(R3 – R4) 192.168.100.16	192.168.100.22	255.255.255.252/30	192.168.100.21
(R4 – R5) 192.168.100.20	192.168.100.22	255.255.255.252/30	----------
(R5 – R6) 192.168.100.24	192.168.100.25	255.255.255.252/30	----------
(R6 – R7) 192.168.100.28	192.168.100.25	255.255.255.252/30	192.168.100.26
(NAT) 192.168.200.0	192.168.100.25	255.255.255.0/24	192.168.100.26

Tabela 7- Tabela de Encaminhamento Router5

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.2	255.255.248.0/21	192.168.100.1
(B)172.16.168.0	192.168.100.2	255.255.252.0/22	192.168.100.1
(C)172.16.172.0	192.168.100.13	255.255.254.0/23	192.168.100.14
(D1)172.16.174.0	192.168.100.26	255.255.255.0/24	192.168.100.25
(E1)172.16.175.0	192.168.100.26	255.255.255.128/25	192.168.100.25
(D2)172.16.175.128	192.168.100.26	255.255.255.192/26	192.168.100.25
(E2)172.16.175.192	192.168.100.26	255.255.255.224/27	192.168.100.25
(R1 – R6) 192.168.100.0	192.168.100.2	255.255.255.252/30	----------
(R1 - R2) 192.168.100.4	192.168.100.2	255.255.255.252/30	192.168.100.1
(R2 – R3) 192.168.100.8	192.168.100.13	255.255.255.252/30	192.168.100.14
(R3 – R6) 192.168.100.12	192.168.100.13	255.255.255.252/30	----------
(R3 – R4) 192.168.100.16	192.168.100.13	255.255.255.252/30	192.168.100.14
(R4 – R5) 192.168.100.20	192.168.100.26	255.255.255.252/30	192.168.100.25
(R5 – R6) 192.168.100.24	192.168.100.26	255.255.255.252/30	----------
(R6 – R7) 192.168.100.28	192.168.100.29	255.255.255.252/30	----------
(NAT) 192.168.200.0	192.168.100.29	255.255.255.0/24	192.168.100.30

Tabela 8- Tabela de Encaminhamento Router6

Rede Destino	Interface de Saída	Máscara	Próximo Nó
(A)172.16.160.0	192.168.100.30	255.255.248.0/21	192.168.100.29
(B)172.16.168.0	192.168.100.30	255.255.252.0/22	192.168.100.29
(C)172.16.172.0	192.168.100.30	255.255.254.0/23	192.168.100.29
(D1)172.16.174.0	192.168.100.30	255.255.255.0/24	192.168.100.29
(E1)172.16.175.0	192.168.100.30	255.255.255.128/25	192.168.100.29
(D2)172.16.175.128	192.168.100.30	255.255.255.192/26	192.168.100.29
(E2)172.16.175.192	192.168.100.30	255.255.255.224/27	192.168.100.29
(R1 – R6) 192.168.100.0	192.168.100.30	255.255.255.252/30	192.168.100.29
(R1 - R2) 192.168.100.4	192.168.100.30	255.255.255.252/30	192.168.100.29
(R2 – R3) 192.168.100.8	192.168.100.30	255.255.255.252/30	192.168.100.29
(R3 – R6) 192.168.100.12	192.168.100.30	255.255.255.252/30	192.168.100.29
(R3 – R4) 192.168.100.16	192.168.100.30	255.255.255.252/30	192.168.100.29
(R4 – R5) 192.168.100.20	192.168.100.30	255.255.255.252/30	192.168.100.29
(R5 – R6) 192.168.100.24	192.168.100.30	255.255.255.252/30	192.168.100.29
(R6 – R7) 192.168.100.28	192.168.100.30	255.255.255.252/30	----------
(NAT) 192.168.200.0	192.168.200.1	255.255.255.0/24	----------

Tabela 9- Tabela de Encaminhamento Router7

d) Desativação do Encaminhamento Dinâmico e configuração do Encaminhamento Estático

Desativamos o encaminhamento dinâmico, desativando os OSPFv2 e OSPFv3, inserimos então as rotas necessárias para garantir conectividade IPv4 entre todas as redes de acordo com as tabelas de encaminhamento anteriores, configurando então a rota estática no zebra de cada Router.

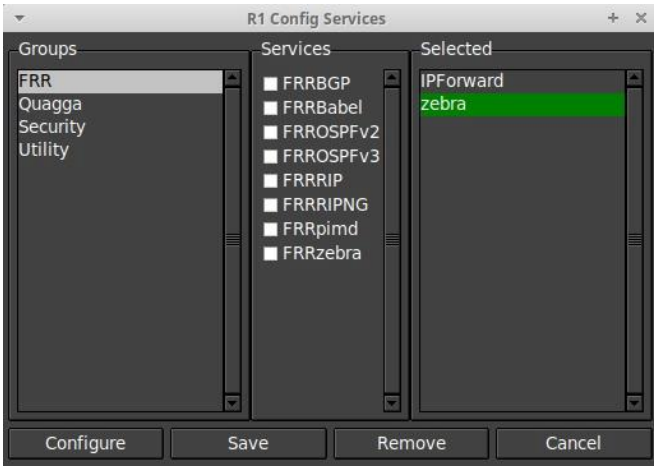


Figura 9- Desativação do Encaminhamento Dinâmico

```
interface R1R6
!
ip address 192.168.100.1/30

interface R1R2
!
ip address 192.168.100.5/30

interface RedeA
!
ip address 172.16.167.254/21

outras rotas
!
ip route 172.16.174.0/24 192.168.100.2
ip route 172.16.175.128/26 192.168.100.2
ip route 172.16.175.0/25 192.168.100.2
ip route 172.16.175.192/27 192.168.100.2
ip route 172.16.168.0/22 192.168.100.6
ip route 172.16.172.0/23 192.168.100.6
```

Figura 10- Configuração router1

```
interface R2R1
!
ip address 192.168.100.6/30

interface R2R3
!
ip address 192.168.100.9/30

interface RedeB
!
ip address 172.16.171.254/22

outras rotas
!
ip route 172.16.160.0/21 192.168.100.5
ip route 172.16.172.0/23 192.168.100.10
ip route 172.16.174.0/24 192.168.100.10
ip route 172.16.175.128/26 192.168.100.10
ip route 172.16.175.0/25 192.168.100.10
ip route 172.16.175.192/27 192.168.100.10
```

Figura 11- Configuração router2

```
interface R3R2
!
ip address 192.168.100.10/30

interface R3R6
!
ip address 192.168.100.14/30

interface R3R4
!
ip address 192.168.100.17/30

interface RedeC
!
ip route 172.16.172.0/23 172.16.173.254

!outras
ip route 172.16.160.0/21 192.168.100.9
ip route 172.16.168.0/22 192.168.100.9
ip route 172.16.175.0/25 192.168.100.13
ip route 172.16.175.192/27 192.168.100.13
ip route 172.16.174.0/24 192.168.100.18
ip route 172.16.175.128/26 192.168.100.18
```

Figura 13-Configuração router3

```
interface R4R3
!
ip address 192.168.100.18/30

interface R4R5
!
ip address 192.168.100.21/30

interface D
!
ip address 172.16.174.254/24
ip address 172.16.175.190/26

outras
!
ip route 192.168.100.0/30 192.168.100.17
ip route 192.168.100.4/30 192.168.100.17
ip route 192.168.100.8/30 192.168.100.17
ip route 192.168.100.12/30 192.168.100.17
ip route 192.168.100.24/30 192.168.100.22
ip route 192.168.100.28/30 192.168.100.17
ip route 172.16.160.0/21 192.168.100.17
ip route 172.16.168.0/22 192.168.100.17
ip route 172.16.172.0/23 192.168.100.17
ip route 172.16.175.0/25 192.168.100.22
ip route 172.16.175.192/27 192.168.100.22
ip route 192.168.200.0/24 192.168.100.17
```

Figura 12-Configuração router4

```
interface R5R4
!
ip address 192.168.100.22/30

interface R5R6
!
ip address 192.168.100.25/30

interface E
!
ip address 172.16.175.126/25
ip address 172.16.175.222/27

outras
!
ip route 192.168.100.0/30 192.168.100.26
ip route 192.168.100.4/30 192.168.100.26
ip route 192.168.100.8/30 192.168.100.26
ip route 192.168.100.12/30 192.168.100.26
ip route 192.168.100.16/30 192.168.100.21
ip route 192.168.100.28/30 192.168.100.26
ip route 172.16.160.0/21 192.168.100.26
ip route 172.16.168.0/22 192.168.100.26
ip route 172.16.172.0/23 192.168.100.26
ip route 172.16.174.0/24 192.168.100.21
ip route 172.16.175.128/26 192.168.100.21
ip route 192.168.200.0/24 192.168.100.26
```

Figura 14-Configuração router5

```
interface R6R1
!
ip address 192.168.100.2/30

interface R6R3
!
ip address 192.168.100.13/30

interface R6R5
!
ip address 192.168.100.25/30

!outras
ip route 172.16.160.0/21 192.168.100.1
ip route 172.16.168.0/22 192.168.100.1
ip route 172.16.172.0/23 192.168.100.14
ip route 172.16.174.0/24 192.168.100.26
ip route 172.16.175.128/26 192.168.100.26
ip route 172.16.175.0/25 192.168.100.26
ip route 172.16.175.192/27 192.168.100.26
```

Figura 15-Configuração router6

e) Teste da conectividade entre todas as redes

Depois de todas as configurações passamos a testar a conectividade entre as diferentes redes com os comandos ping e traceroute.

```
root@PC1:/tmp/pycore.1/PC1.conf# ping 172.16.168.1
PING 172.16.168.1 (172.16.168.1) 56(84) bytes of data.
64 bytes from 172.16.168.1: icmp_seq=1 ttl=62 time=0.488 ms
^C
--- 172.16.168.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.488/0.488/0.488/0.000 ms
root@PC1:/tmp/pycore.1/PC1.conf# traceroute 172.16.168.1
traceroute to 172.16.168.1 (172.16.168.1), 30 hops max, 60 byte packets
 1  172.16.167.254 (172.16.167.254)  0.073 ms  0.022 ms  0.025 ms
 2  192.168.100.6 (192.168.100.6)  0.041 ms  0.027 ms  0.028 ms
 3  172.16.168.1 (172.16.168.1)  0.060 ms  0.041 ms  0.057 ms
root@PC1:/tmp/pycore.1/PC1.conf#
```

Figura 19-Teste de conectividade A-B

```
root@PC1:/tmp/pycore.1/PC1.conf# ping 172.16.172.1
PING 172.16.172.1 (172.16.172.1) 56(84) bytes of data.
64 bytes from 172.16.172.1: icmp_seq=1 ttl=61 time=0.321 ms
64 bytes from 172.16.172.1: icmp_seq=2 ttl=61 time=0.227 ms
^C
--- 172.16.172.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1016ms
rtt min/avg/max/mdev = 0.227/0.274/0.321/0.047 ms
root@PC1:/tmp/pycore.1/PC1.conf# traceroute 172.16.172.1
traceroute to 172.16.172.1 (172.16.172.1), 30 hops max, 60 byte packets
 1  172.16.167.254 (172.16.167.254)  1.161 ms  1.086 ms  1.048 ms
 2  192.168.100.6 (192.168.100.6)  1.010 ms  0.957 ms  0.912 ms
 3  192.168.100.10 (192.168.100.10)  0.859 ms  0.799 ms  0.749 ms
 4  172.16.172.1 (172.16.172.1)  0.700 ms  0.623 ms  0.560 ms
root@PC1:/tmp/pycore.1/PC1.conf#
```

Figura 18-Teste de conectividade A-C

```
root@PC1:/tmp/pycore.1/PC1.conf# ping 172.16.174.1
PING 172.16.174.1 (172.16.174.1) 56(84) bytes of data.
64 bytes from 172.16.174.1: icmp_seq=1 ttl=60 time=0.585 ms
^C
--- 172.16.174.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.585/0.585/0.585/0.000 ms
root@PC1:/tmp/pycore.1/PC1.conf# traceroute 172.16.174.1
traceroute to 172.16.174.1 (172.16.174.1), 30 hops max, 60 byte packets
 1  172.16.167.254 (172.16.167.254)  1.826 ms  1.738 ms  1.700 ms
 2  192.168.100.2 (192.168.100.2)  1.338 ms  1.234 ms  1.187 ms
 3  192.168.100.25 (192.168.100.25)  1.145 ms  1.043 ms  0.995 ms
 4  192.168.100.18 (192.168.100.18)  0.946 ms  0.701 ms  0.632 ms
 5  172.16.174.1 (172.16.174.1)  0.520 ms  0.421 ms  0.345 ms
root@PC1:/tmp/pycore.1/PC1.conf#
```

Figura 17-Teste de conectividade A-D

```
root@PC1:/tmp/pycore.1/PC1.conf# ping 172.16.175.199
PING 172.16.175.199 (172.16.175.199) 56(84) bytes of data.
64 bytes from 172.16.175.199: icmp_seq=1 ttl=61 time=1.47 ms
^C
--- 172.16.175.199 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.468/1.468/1.468/0.000 ms
root@PC1:/tmp/pycore.1/PC1.conf# traceroute 172.16.175.199
traceroute to 172.16.175.199 (172.16.175.199), 30 hops max, 60 byte packets
 1  172.16.167.254 (172.16.167.254)  1.415 ms  1.329 ms  1.292 ms
 2  192.168.100.2 (192.168.100.2)  1.257 ms  1.199 ms  1.157 ms
 3  192.168.100.25 (192.168.100.25)  1.107 ms  1.038 ms  0.984 ms
 4  172.16.175.199 (172.16.175.199)  0.937 ms  0.731 ms  0.621 ms
root@PC1:/tmp/pycore.1/PC1.conf#
```

Figura 16-Teste de conectividade A-E

```
root@PC7:/tmp/pycore.1/PC7.conf# ping 172.16.172.1
PING 172.16.172.1 (172.16.172.1) 56(84) bytes of data.
64 bytes from 172.16.172.1: icmp_seq=1 ttl=62 time=0.212 ms
^C
--- 172.16.172.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.212/0.212/0.212/0.000 ms
root@PC7:/tmp/pycore.1/PC7.conf# traceroute 172.16.172.1
traceroute to 172.16.172.1 (172.16.172.1), 30 hops max, 60 byte packets
 1  172.16.171.254 (172.16.171.254)  1.516 ms  1.401 ms  1.343 ms
 2  192.168.100.10 (192.168.100.10)  1.277 ms  1.089 ms  1.016 ms
 3  172.16.172.1 (172.16.172.1)  0.961 ms  0.824 ms  0.745 ms
root@PC7:/tmp/pycore.1/PC7.conf#
```

Figura 25-Teste de conectividade B-C

```
root@PC7:/tmp/pycore.1/PC7.conf# ping 172.16.174.1
PING 172.16.174.1 (172.16.174.1) 56(84) bytes of data.
64 bytes from 172.16.174.1: icmp_seq=1 ttl=61 time=0.190 ms
64 bytes from 172.16.174.1: icmp_seq=2 ttl=61 time=0.174 ms
^C
--- 172.16.174.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.174/0.182/0.190/0.008 ms
root@PC7:/tmp/pycore.1/PC7.conf# traceroute 172.16.174.1
traceroute to 172.16.174.1 (172.16.174.1), 30 hops max, 60 byte packets
 1  172.16.171.254 (172.16.171.254)  0.087 ms  0.023 ms  0.021 ms
 2  192.168.100.10 (192.168.100.10)  0.042 ms  0.028 ms  0.028 ms
 3  192.168.100.18 (192.168.100.18)  0.191 ms  0.080 ms  0.038 ms
 4  172.16.174.1 (172.16.174.1)  0.083 ms  0.058 ms  0.055 ms
root@PC7:/tmp/pycore.1/PC7.conf#
```

Figura 24-Teste de conectividade B-D

```
root@PC7:/tmp/pycore.1/PC7.conf# ping 172.16.175.199
PING 172.16.175.199 (172.16.175.199) 56(84) bytes of data.
64 bytes from 172.16.175.199: icmp_seq=1 ttl=60 time=0.254 ms
^C
--- 172.16.175.199 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.254/0.254/0.254/0.000 ms
root@PC7:/tmp/pycore.1/PC7.conf# traceroute 172.16.175.199
traceroute to 172.16.175.199 (172.16.175.199), 30 hops max, 60 byte packets
 1  172.16.171.254 (172.16.171.254)  1.300 ms  1.219 ms  1.185 ms
 2  192.168.100.5 (192.168.100.5)  1.154 ms  1.101 ms  1.011 ms
 3  192.168.100.2 (192.168.100.2)  0.959 ms  0.901 ms  0.853 ms
 4  192.168.100.25 (192.168.100.25)  0.802 ms  0.736 ms  0.678 ms
 5  172.16.175.199 (172.16.175.199)  0.622 ms  0.451 ms  0.359 ms
root@PC7:/tmp/pycore.1/PC7.conf#
```

Figura 23-Teste de conectividade B-E

```
root@PC13:/tmp/pycore.1/PC13.conf# ping 172.16.174.1
PING 172.16.174.1 (172.16.174.1) 56(84) bytes of data.
64 bytes from 172.16.174.1: icmp_seq=1 ttl=62 time=0.845 ms
^C
--- 172.16.174.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.845/0.845/0.845/0.000 ms
root@PC13:/tmp/pycore.1/PC13.conf# traceroute 172.16.174.1
traceroute to 172.16.174.1 (172.16.174.1), 30 hops max, 60 byte packets
 1  172.16.173.254 (172.16.173.254)  2.281 ms  0.270 ms  0.025 ms
 2  192.168.100.18 (192.168.100.18)  0.040 ms  0.028 ms  0.026 ms
 3  172.16.174.1 (172.16.174.1)  0.072 ms  0.046 ms  0.047 ms
root@PC13:/tmp/pycore.1/PC13.conf#
```

Figura 22-Teste de conectividade C-D

```
root@PC13:/tmp/pycore.1/PC13.conf# ping 172.16.175.199
PING 172.16.175.199 (172.16.175.199) 56(84) bytes of data.
64 bytes from 172.16.175.199: icmp_seq=1 ttl=61 time=0.348 ms
^C
--- 172.16.175.199 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.348/0.348/0.348/0.000 ms
root@PC13:/tmp/pycore.1/PC13.conf# traceroute 172.16.175.199
traceroute to 172.16.175.199 (172.16.175.199), 30 hops max, 60 byte packets
 1  172.16.173.254 (172.16.173.254)  1.301 ms  1.218 ms  1.181 ms
 2  192.168.100.13 (192.168.100.13)  1.145 ms  1.085 ms  1.032 ms
 3  192.168.100.25 (192.168.100.25)  0.980 ms  0.920 ms  0.867 ms
 4  172.16.175.199 (172.16.175.199)  0.767 ms  0.630 ms  0.540 ms
root@PC13:/tmp/pycore.1/PC13.conf#
```

Figura 21-Teste de conectividade C-E

```
root@PC19:/tmp/pycore.1/PC19.conf# ping 172.16.175.199
PING 172.16.175.199 (172.16.175.199) 56(84) bytes of data.
64 bytes from 172.16.175.199: icmp_seq=1 ttl=62 time=0.629 ms
^C
--- 172.16.175.199 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.629/0.629/0.629/0.000 ms
root@PC19:/tmp/pycore.1/PC19.conf# traceroute 172.16.175.199
traceroute to 172.16.175.199 (172.16.175.199), 30 hops max, 60 byte packets
 1  172.16.174.254 (172.16.174.254)  1.807 ms  1.713 ms  1.326 ms
 2  192.168.100.22 (192.168.100.22)  1.258 ms  1.190 ms  1.140 ms
 3  172.16.175.199 (172.16.175.199)  1.093 ms  0.963 ms  0.855 ms
root@PC19:/tmp/pycore.1/PC19.conf#
```

Figura 20-Teste de conectividade D-E

3. DHCP – Dynamic Host Configuration Protocol

Ativar a configuração automática dos endereços IP na rede local E recorrendo ao protocolo DHCP.

a) Download e instalação no host o DHCP

No terminal inserimos o código `sudo apt-get install isc-dhcp-server`, como pedido no enunciado.

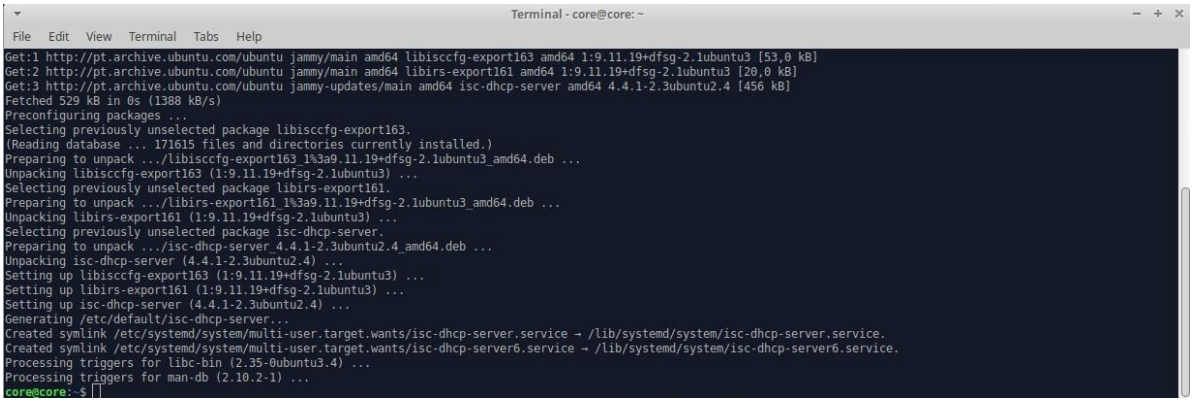


Figura 26- Download e Instalação DHCP

b) Alteração da Configuração da rede E

```
# auto-generated by DHCP service (utility.py)
# NOTE: move these option lines into the desired pool { } block(s) below
#option domain-name "test.com";
#option domain-name-servers 10.0.0.1;
#option routers 10.0.0.1;

log-facility local6;

default-lease-time 600;
max-lease-time 7200;

ddns-update-style none;

subnet 172.16.175.0 netmask 255.255.255.128 {
  pool {
    range 172.16.175.1 172.16.175.124;
    default-lease-time 600;
    option routers 172.16.175.126;
  }
}
```

Figura 30- Configuração do servidor DCHP1

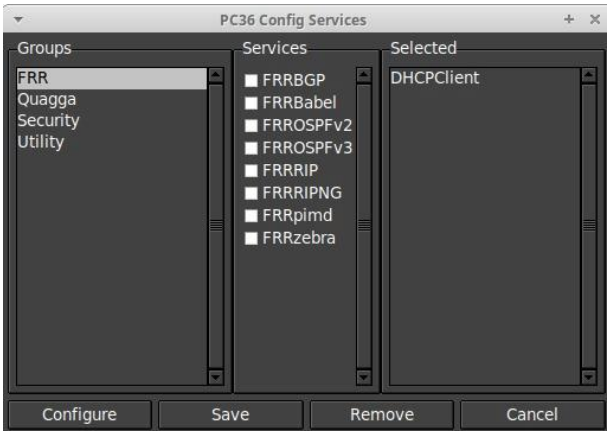


Figura 29- Serviços do PC31

```
# auto-generated by DHCP service (utility.py)
# NOTE: move these option lines into the desired pool { } block(s) below
#option domain-name "test.com";
#option domain-name-servers 10.0.0.1;
#option routers 10.0.0.1;

log-facility local6;

default-lease-time 600;
max-lease-time 7200;

ddns-update-style none;

subnet 172.16.175.192 netmask 255.255.255.224 {
  pool {
    range 172.16.175.193 172.16.175.220;
    default-lease-time 600;
    option routers 172.16.175.222;
  }
}
```

Figura 28- Configuração do servidor DHCP2

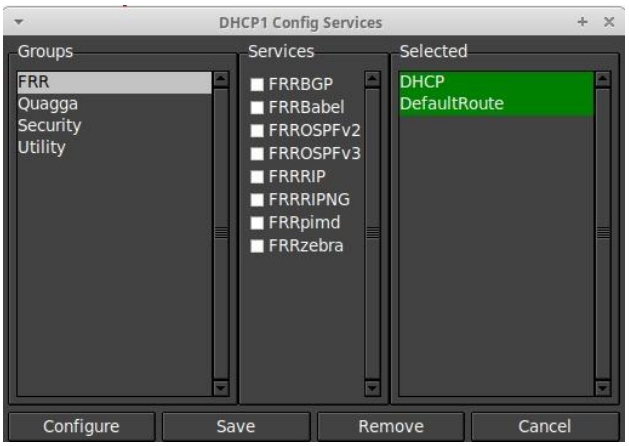


Figura 27- Serviços do router5

c) Captura de Pacotes

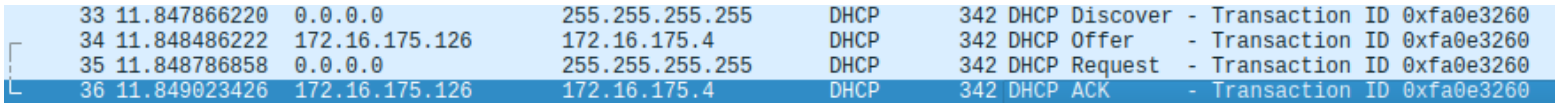


Figura 32- Análise do protocolo DHCP

Utilizámos dois servidores DHCP(DHCP1 e DHCP2) um para cada rede(E1 e E2).
Na figura podemos confirmar o protocolo DHCP.
Primeiro o cliente envia um DHCP Discover para o servidor, sendo o source 0.0.0.0, porque não foi atribuído nenhum IP ao cliente.
O servidor responde com um DHCP Offer, a "oferecer" um IP ao cliente, o cliente envia de seguida um DHCP Request, para reservar esse IP para ele mesmo, enviando em Broadcast para que todos tenham conhecimento dessa reserva.
Por fim o servidor envia um DHCP ACK para confirmar a atribuição do IP ao cliente.
Após a atribuição do IP conseguimos ter conexão com o resto da topologia.
O DHCP fornece a máscara da rede, o IP do server DHCP e endereço IP do Default Gateway.

4. Uso das camadas de rede e transporte por parte das aplicações

a) Ativação de um servidor HTTP e teste

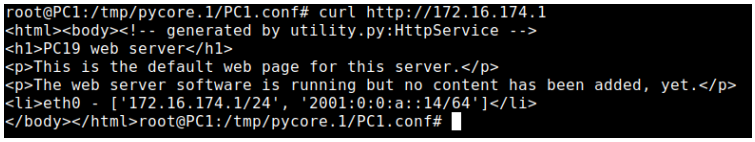


Figura 37- Mensagem que aparece no PC1 da rede A com o curl

Figura 36- Mensagem que aparece no PC7 da rede B com o curl

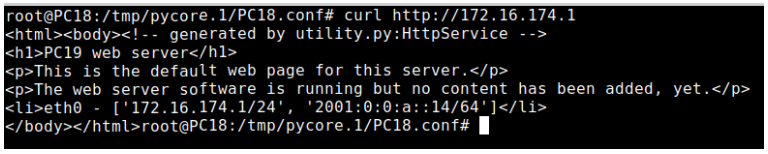


Figura 35- Mensagem que aparece no PC18 da rede C com o curl

Figura 34- Mensagem que aparece no PC27 da rede D2 com o curl

Figura 33- Mensagem que aparece no PC38 da rede E2 com o curl

b) Captura de Pacotes

25	1.736218485	172.16.160.1	172.16.174.1	TCP	74 40616 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3196397104 TSecr=0 WS=128
26	1.736236479	172.16.174.1	172.16.160.1	TCP	74 80 → 40616 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=750129259 TSecr=3…
27	1.736330858	172.16.160.1	172.16.174.1	TCP	66 40616 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3196397105 TSecr=750129259
28	1.736395119	172.16.160.1	172.16.174.1	HTTP	142 GET / HTTP/1.1
29	1.736427761	172.16.174.1	172.16.160.1	TCP	66 80 → 40616 [ACK] Seq=1 Ack=77 Win=65152 Len=0 TSval=750129260 TSecr=3196397105
30	1.737113215	172.16.174.1	172.16.160.1	HTTP	554 HTTP/1.1 200 OK
31	1.737232881	172.16.160.1	172.16.174.1	TCP	66 40616 → 80 [ACK] Seq=77 Ack=489 Win=64128 Len=0 TSval=3196397105 TSecr=750129260
32	1.737755099	172.16.160.1	172.16.174.1	TCP	66 40616 → 80 [FIN, ACK] Seq=77 Ack=489 Win=64128 Len=0 TSval=3196397106 TSecr=750129260
33	1.737953511	172.16.174.1	172.16.160.1	TCP	66 80 → 40616 [FIN, ACK] Seq=489 Ack=78 Win=65152 Len=0 TSval=750129261 TSecr=3196397106
34	1.738006501	172.16.160.1	172.16.174.1	TCP	66 40616 → 80 [ACK] Seq=78 Ack=490 Win=64128 Len=0 TSval=3196397106 TSecr=750129261

Figura 38- Análise dos protocolos HTTP e TCP (Wireshark) (PC1)

Como podemos analisar a partir do Wireshark, existe comunicação com base nos protocolos TCP e HTTP.
Os primeiros 3 pacotes são de conexão:
Um synchronize "SYN" enviado pelo PC1.

Um acknowledge "SYN,ACK", o PC19(Onde está o servidor HTTP) aceita a conexão e inicia o processo de conexão.

Por fim um "ACK", o PC1 confirma a conexão.
A seguir ao HTTP "GET" o PC19 confirma que recebeu o pacote.
Depois de enviar o pacote requisitado pelo PC1, com o "OK" do HTTP, o PC1 envia um "ACK" para confirmar que recebeu a reposta do "GET".

Os últimos 3 servem para terminar a conexão:
Um "FIN,ACK" enviado pelo PC1 para informar o término da conexão.
Um "FIN,ACK" enviado pelo PC19 para também terminar a conexão.
Por fim o PC1 envia o "ACK" para confirmar que recebeu a mensagem.

5. Interligação via NAT (Network Address Translator)

a)Adição de uma rede privada através de um router NAT

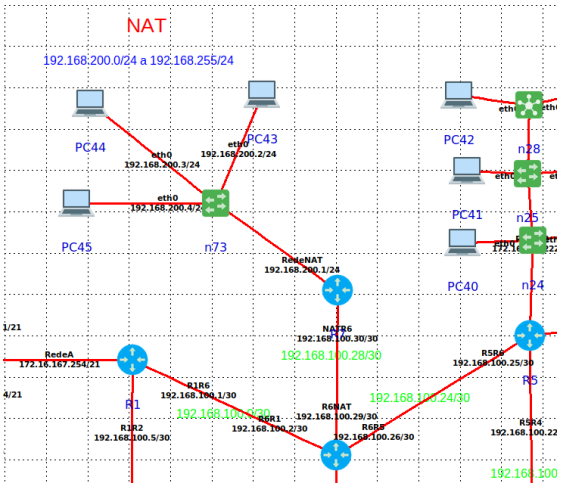


Figura 39- Estrutura redeNAT

b)Configuração do router NAT

Procedemos então à configuração do Router NAT, primeiramente ativamos o serviço NAT onde implementamos os comandos necessários para o seu funcionamento, além disso é necessário configurar o seu esquema de endereçamento para garantir acesso às restantes redes, sem que estas possam acessar a rede interna.

```
#!/bin/sh
# generated by security.py
# NAT out the first interface by default

iptables -t nat -A POSTROUTING -o NATR6 -j MASQUERADE
iptables -A FORWARD -i NATR6 -o NAT -m state --state RELATED,ESTABLISHED -j ACCE
PT

iptables -t nat -A PREROUTING -i NATR6 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.200.3 --dport 21 -j ACCEPT

iptables -t nat -A PREROUTING -i NATR6 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.200.4 --dport 80 -j ACCEPT

iptables -A FORWARD -i NATR6 -j DROP

# iptables -t nat -A POSTROUTING -o NAT -j MASQUERADE
# iptables -A FORWARD -i NAT -m state --state RELATED,ESTABLISHED -j ACCEPT
# iptables -A FORWARD -i NAT -j DROP
```

Figura 42-Configuração NAT

```
 7 5.398567022   192.168.100.30   172.16.160.1     ICMP    98 Echo (ping) request  id=0x249a, seq=1/256, ttl=61 (reply in 8)
 8 5.398613208   172.16.160.1     192.168.100.30   ICMP    98 Echo (ping) reply    id=0x249a, seq=1/256, ttl=64 (request in 7)
 9 6.419808374   192.168.100.30   172.16.160.1     ICMP    98 Echo (ping) request  id=0x249a, seq=2/512, ttl=61 (reply in 10)
10 6.419846536   172.16.160.1     192.168.100.30   ICMP    98 Echo (ping) reply    id=0x249a, seq=2/512, ttl=64 (request in 9)
```

Figura 41- Análise wireshark (ping PC43 para PC1) visão da RedeA

```
24 12.770262328  192.168.200.2    172.16.160.1     ICMP    98 Echo (ping) request  id=0x249a, seq=1/256, ttl=64 (reply in 25)
25 12.770382223  172.16.160.1     192.168.200.2    ICMP    98 Echo (ping) reply    id=0x249a, seq=1/256, ttl=61 (request in 24)
26 13.791513629  192.168.200.2    172.16.160.1     ICMP    98 Echo (ping) request  id=0x249a, seq=2/512, ttl=64 (reply in 27)
27 13.791605531  172.16.160.1     192.168.200.2    ICMP    98 Echo (ping) reply    id=0x249a, seq=2/512, ttl=61 (request in 26)
```

Figura 40-Análise wireshark(ping PC43 para PC1) visão da RedeNAT

c) Criação de servidores HTTP e FTP

Com a rede privada totalmente operacional podemos, tal como fizemos anteriormente, aplicar alguns serviços à mesma, para isso iremos configurar um servidor HTTP e FTP dentro da nossa rede. Para podermos usar o serviço FTP foi necessário executar o comando sudo apt-get install vsftpd para a instalação do mesmo.
Configurámos então os dois serviços nos respetivos *PCs*.

```
#!/bin/sh
# generated by security.py
# NAT out the first interface by default

iptables -t nat -A POSTROUTING -o NATR6 -j MASQUERADE
iptables -A FORWARD -i NATR6 -o NAT -m state --state RELATED,ESTABLISHED -j ACCE
PT

iptables -t nat -A PREROUTING -i NATR6 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.200.3 --dport 21 -j ACCEPT

iptables -t nat -A PREROUTING -i NATR6 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.200.4 --dport 80 -j ACCEPT

iptables -A FORWARD -i NATR6 -j DROP

# iptables -t nat -A POSTROUTING -o NAT -j MASQUERADE
# iptables -A FORWARD -i NAT -m state --state RELATED,ESTABLISHED -j ACCEPT
# iptables -A FORWARD -i NAT -j DROP
```

Figura 43- Configurações NAT no router7

Além de implementar e configurar os serviços, é necessário alterar a configuração do Router NAT para que o mesmo saiba quando a comunicação, por iniciativa da rede local, é para os serviços deixe passar.
Iniciamos então os testes e capturas de tráfego dos serviços implementados.

5	5.503852725	172.16.160.1	192.168.200.3	TCP	74 47368 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=1282597245 TSecr=0 WS=4
6	5.503867663	192.168.200.3	172.16.160.1	TCP	74 21 → 47368 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=225371546 TS…
7	5.503927987	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1282597246 TSecr=225371546
8	5.506434805	192.168.200.3	172.16.160.1	FTP	76 Response: 500 OOPS:
9	5.506563398	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [ACK] Seq=1 Ack=11 Win=65536 Len=0 TSval=1282597248 TSecr=225371548
10	5.506578227	192.168.200.3	172.16.160.1	FTP	124 Response: vsftpd: refusing to run with writable root inside chroot()
11	5.506610047	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [ACK] Seq=1 Ack=69 Win=65536 Len=0 TSval=1282597248 TSecr=225371548
12	5.506618082	192.168.200.3	172.16.160.1	FTP	68 Response:
13	5.506646336	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [ACK] Seq=1 Ack=71 Win=65536 Len=0 TSval=1282597248 TSecr=225371548
14	5.506902373	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [FIN, ACK] Seq=1 Ack=71 Win=65536 Len=0 TSval=1282597249 TSecr=225371548
15	5.507173523	192.168.200.3	172.16.160.1	TCP	66 21 → 47368 [FIN, ACK] Seq=71 Ack=2 Win=65280 Len=0 TSval=225371549 TSecr=1282597249
16	5.507224639	172.16.160.1	192.168.200.3	TCP	66 47368 → 21 [ACK] Seq=2 Ack=72 Win=65536 Len=0 TSval=1282597249 TSecr=225371549

Figura 45- Análise de protocolos no Servidor FTP rede privada

1	0.000000000	172.16.160.1	192.168.200.4	TCP	74 38244 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=14499756 TSecr=0 WS=128
2	0.000016942	192.168.200.4	172.16.160.1	TCP	74 80 → 38244 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2521789232 TSecr=…
3	0.000074010	172.16.160.1	192.168.200.4	TCP	66 38244 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=14499756 TSecr=2521789232
4	0.000119065	172.16.160.1	192.168.200.4	HTTP	143 GET / HTTP/1.1
5	0.000132370	192.168.200.4	172.16.160.1	TCP	66 80 → 38244 [ACK] Seq=1 Ack=78 Win=65152 Len=0 TSval=2521789233 TSecr=14499757
6	0.000985290	192.168.200.4	172.16.160.1	HTTP	556 HTTP/1.1 200 OK
7	0.001228279	172.16.160.1	192.168.200.4	TCP	66 38244 → 80 [ACK] Seq=78 Ack=491 Win=64128 Len=0 TSval=14499757 TSecr=2521789233
8	0.001295979	172.16.160.1	192.168.200.4	TCP	66 38244 → 80 [FIN, ACK] Seq=78 Ack=491 Win=64128 Len=0 TSval=14499758 TSecr=2521789233
9	0.001449958	192.168.200.4	172.16.160.1	TCP	66 80 → 38244 [FIN, ACK] Seq=491 Ack=79 Win=65152 Len=0 TSval=2521789234 TSecr=14499758
10	0.001497218	172.16.160.1	192.168.200.4	TCP	66 38244 → 80 [ACK] Seq=79 Ack=492 Win=64128 Len=0 TSval=14499758 TSecr=2521789234

Figura 44- Análise de protocolos no Servidor HTTP rede privada

Conclusão

Durante a realização deste trabalho de grupo, proposto pela equipa docente, tivemos a oportunidade de colocar em prática os conceitos lecionados nas aulas de Redes de Computadores I.

No decorrer deste projeto foi possível abordar várias componentes da Unidade Curricular, tais como, a criação de topologias, cálculo e endereçamento de IP para diferentes redes e respetivas interligações, assim como a emulação de redes onde foi possível realizar diagnósticos de conectividade, captura e análise de tráfego de rede, assim como diferentes protocolos tais como DHCP, HTTP, TCP e NAT.

Com os diversos pontos conseguimos aprofundar e aplicar os nossos conhecimentos, servindo como um complemento para os ensinamentos previamente adquiridos.

Concluindo, consideramos ter cumprido com sucesso todos os objetivos do trabalho, assim como os objetivos da unidade curricular de Redes de Computadores I, adquirindo o conhecimento e perceção do funcionamento de uma rede assim como problemas que possam surgir e solução para os resolver.