

# Rede de Computadores - Trabalho Prático nº 4

## Protocolo IPv4 - Datagramas *IP* e Fragmentação

William Sousa, Manuel Maciel e Rui Santos

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal  
e-mail: {a61029,a68410,a67656}@alunos.uminho.pt

**Resumo** Neste relatório, iremos propor respostas para as perguntas da ficha de trabalho prática nº 4 que foi realizada no âmbito da unidade curricular de Redes de Computadores, lecionada no ano lectivo 2015/2016 do Mestrado Integrado de Engenharia Informática, portanto, toda a estrutura de perguntas e respostas, presentes neste relatório, irão de encontro ao que foi pedido e/ou fornecido nessa ficha prática. Acreditamos, que as perguntas e respostas aqui apresentadas, de uma forma geral, ajudam a compreensão e análise de muitos conceitos relacionados com as redes de computadores, nomeadamente do nível 3 do modelo OSI[1] (i.e., camada de rede) com especial atenção ao protocolo *IP* que é o principal protocolo de comunicação usado no usado no *Internet protocol suite*[2] para garantir o envio dos *datagrams* através de uma rede *TCP/IP*.

## 1 Introdução

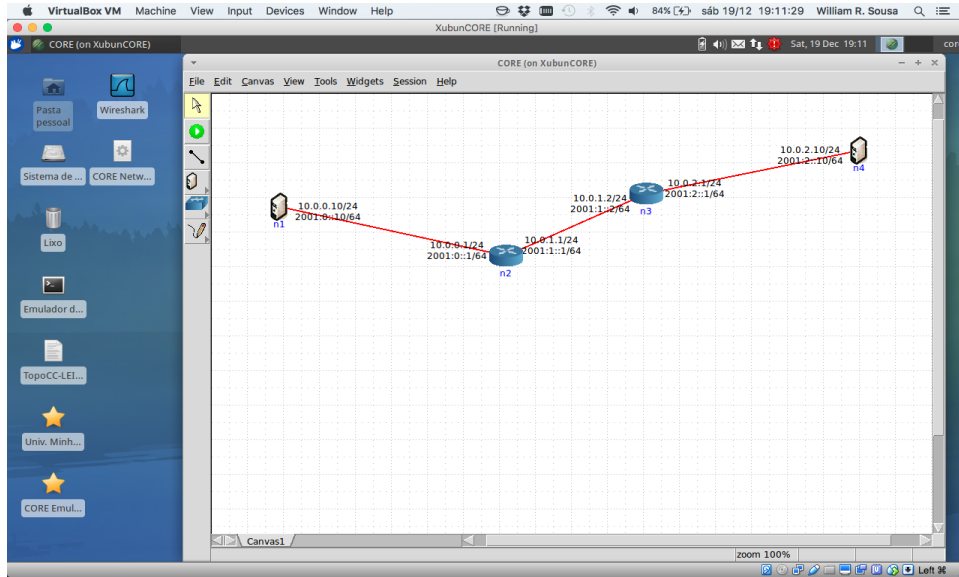
“A camada de rede desempenha um papel central da arquitetura TCP/IP, já que todos os protocolos das camadas superiores assentam na utilização do seu protocolo chave: o *Internet Protocol (IP)*. Como principais funções dessa camada destaca-se o endereçamento e o encaminhamento, essenciais para o funcionamento da Internet.”[4] Vamos abordar ao longo desse relatório sobre os principais aspectos e funções associadas ao protocolo *IP* que são essencialmente a fragmentação, “reasseblagem” de pacotes e o encaminhamento. No entanto, é importante referir que o protocolo *IP* não garante a transferência fiável de pacotes e que funciona em modo de ausência de ligação.

A não garantia da transferência fiável de informação significa que este protocolo não executa quaisquer operações de detecção e recuperação de, eventuais, erros que possam ocorrer no envio dos pacotes, portanto é normal referir que o protocolo *IP* suporta um serviço de entrega de pacotes em modo de melhor esforço (*best effort*).

O modo de funcionamento em ausência de ligação (*connectionless mode*) está relacionado com o facto de não ser mantido qualquer informação de estado acerca do fluxo de datagramas, ou seja, cada pacote *IP* é encaminhado na rede de forma independente dos outros, que o precederam.

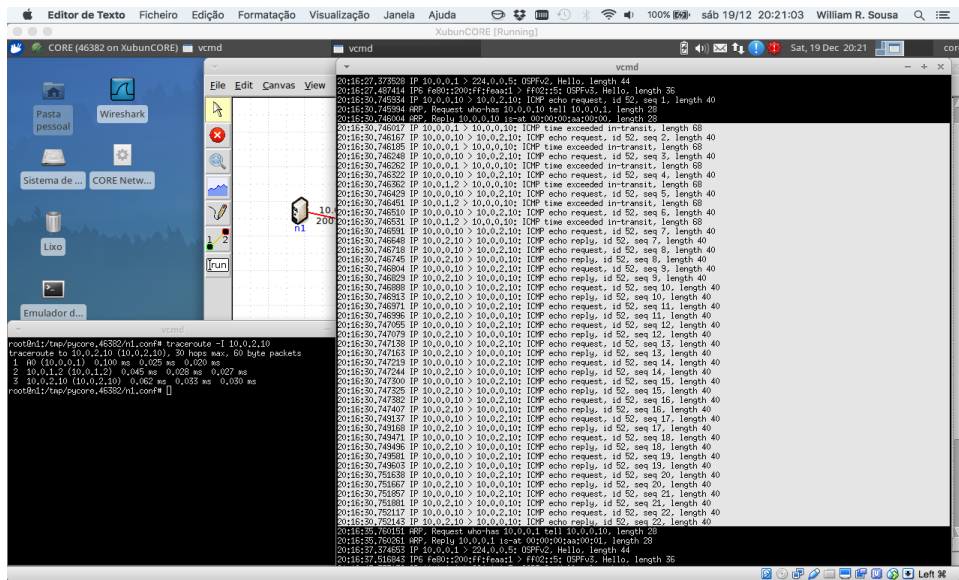
## 2 Captura de tráfego IP

2.1 Prepare uma topologia **CORE** para verificar o comportamento do traceroute. Ligue um host n1 a um router n2; o router n2 a um router n3 que, por sua vez, se liga a um host n4:



Active o **Wireshark** ou o **tcpdump** no nó 1. Numa *shell* de n1, e execute o comando **traceroute -1** para o endereço IP do *host* n4.

Registe e analise o tráfego **ICMP** enviado por n1 e o tráfego **ICMP** recebido como resposta. Comente os resultados face ao comportamento esperado



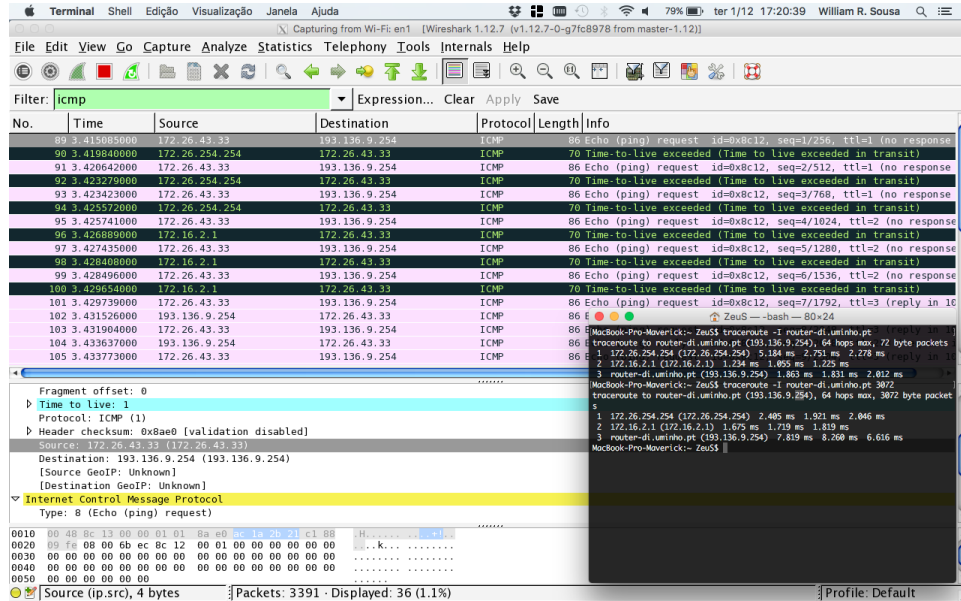
A rotina **traceroute** utiliza pacotes “**ICMP echo request**” para determinar a rota entre a origem e destino. Para além disso, utiliza **TTLs** incrementais a cada envio de três pacotes, utilizando como valor inicial **TTL = 1**. Qualquer *router* que apanhe um pacote com um

$TTL = 1$  “descarta-o” e envia como resposta, ao *destino do pacote* uma mensagem do tipo “*ICMP exceeded in-transit*”. No nosso caso, analisando os *outputs* fornecidos pelo *CORE* temos que os primeiros três pacotes enviados a partir do *host* n1 tem um *time to live (TTL)* igual apenas um salto, logo não conseguem “chegar” ao primeiro router, neste caso o n2; os próximos três pacotes enviados por n1 possuem um *time to live (TTL)* igual a dois saltos, logo conseguem alcançar pelo menos o segundo router da rede, neste caso o n3. Portanto só a partir do 7º pacote enviado por n1, ou seja quando o  $TTL \geq 3$ , e que os pacotes conseguem chegar ao destino pretendido, i.e. ao *host* n4, só nessa altura e que é recebido uma mensagem do tipo *ICMP echo reply*. Relativamente ao *output* fornecido pelo comando *traceroute*, estes referem-se ao tempo que demora aos pacotes a chegar ao destino, também conhecido como *round trip delay time (RTT)*.

**Qual deve ser o valor inicial mínimo do campo *TTL* para alcançar o destino n4? Qual o tempo médio de ida-e-volta (*RTT - round-trip time*) obido?** Tal como referido anteriormente o *TTL* mínimo para que n1 consiga alcançar n4 é de três unidades, ou seja,  $TTL \geq 3$ . Relativamente ao tempo médio de ida-e-volta é fornecido pela seguinte expressão:  $(0.062 + 0.033 + 0.030)/3 = 0.041667ms$ . É de notar que o primeiro tempo *RTT* correspondente, ao primeiro salto de ida-e-volta e pode demorar mais, como é o caso, porque ainda não se sabe quais os endereços *MAC* do destino, e por sua vez pode ter que fazer consultas nas tabelas *ARP*, como é possível ver na imagem acima fornecidas.

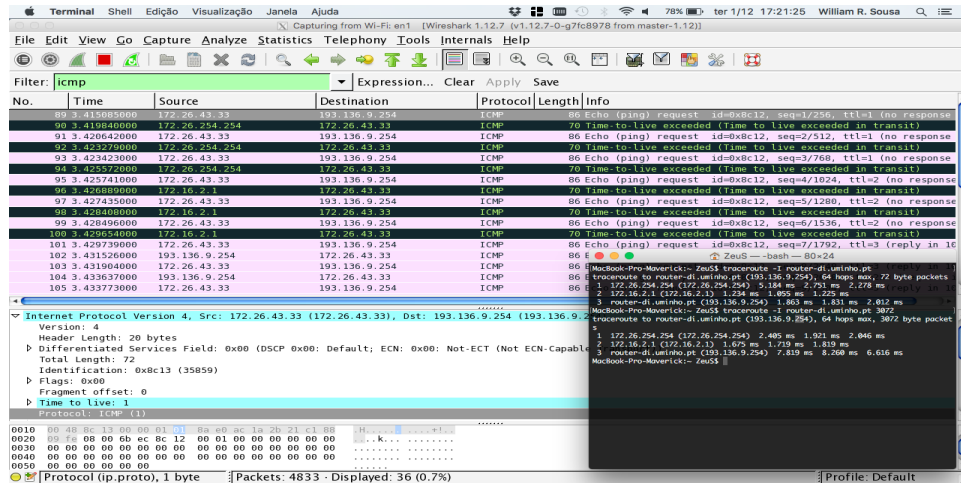
2.2 Pretende-se agora usar o **traceroute** na sua máquina nativa e gerar de datagramas IP de diferentes tamanhos. Exemplo: `%traceroute -I router-di.uminho.pt 2500`

Qual é o endereço IP da interface ativa do seu computador?



Como se pode, trivialmente, verificar pela imagem acima fornecida o endereço *IP* da minha interface activa é o 172.26.43.33.

Qual é o valor do campo protocolo? O que identifica?



O valor do protocolo *ICMP* é o 0x01, como se pode verificar com a imagem acima.

**O datagrama IP foi fragmentado? Justifique.** Não poque o offset é 0, logo é o primeiro fragmento do PDU, e o a flag tem valor 0, logo não há mais fragmentos, tornando-o único, ou seja, não foi fragmentado. E é normal que não o seja, pois o `traceroute` envia pacotes por defeito com um valor que não necessita de ser fragmentado.

[illegible]

**Que campos se mantêm constantes? Que campos se devem manter, preferencialmente, constantes? Justifique.** Os campos que se mantêm constantes são: *version, header, length, differentiated services field, protocol, source, destination, flags* e o *more flags*. Os campos que devem, preferencialmente, se manterem constantes são os campos *flags* e o *fragment offset*, pois estes se mudam-se estaríamos, erradamente, a fragmentar o datagrama.

**Observa algum padrão nos valores do campo de Identificação do datagrama IP?** Sim, o valor do campo identificação é incrementado uma unidade a cada novo request.

A seguir (com os pacotes ordenados por endereço destino) encontre a série de respostas *ICMP TTL exceeded* enviadas ao seu computador pelo primeiro router. Qual é o valor dos campos Identificação e *TTL*?

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, Capture, Analyze, Statistics, Tools, and Help. The main display area shows a list of captured packets, with packet 12 selected. The packet details pane on the right shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) reply. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.000000	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
92	0.0272980	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
93	0.0273000	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
94	0.0273020	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
95	0.0273040	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
96	0.0273060	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
97	0.0273080	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
98	0.0273100	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
99	0.0273120	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
100	0.0273140	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
101	0.0273160	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
102	0.0273180	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
103	0.0273200	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
104	0.0273220	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
105	0.0273240	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
106	0.0273260	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
107	0.0273280	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
108	0.0273300	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
109	0.0273320	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
110	0.0273340	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
111	0.0273360	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
112	0.0273380	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
113	0.0273400	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
114	0.0273420	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
115	0.0273440	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
116	0.0273460	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
117	0.0273480	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
118	0.0273500	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
119	0.0273520	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
120	0.0273540	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
121	0.0273560	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
122	0.0273580	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
123	0.0273600	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
124	0.0273620	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
125	0.0273640	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
126	0.0273660	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
127	0.0273680	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
128	0.0273700	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
129	0.0273720	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
130	0.0273740	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
131	0.0273760	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
132	0.0273780	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
133	0.0273800	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
134	0.0273820	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
135	0.0273840	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
136	0.0273860	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
137	0.0273880	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
138	0.0273900	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
139	0.0273920	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
140	0.0273940	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
141	0.0273960	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
142	0.0273980	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
143	0.0274000	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
144	0.0274020	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
145	0.0274040	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
146	0.0274060	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
147	0.0274080	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
148	0.0274100	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
149	0.0274120	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
150	0.0274140	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
151	0.0274160	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
152	0.0274180	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
153	0.0274200	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
154	0.0274220	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
155	0.0274240	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
156	0.0274260	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
157	0.0274280	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
158	0.0274300	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
159	0.0274320	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
160	0.0274340	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
161	0.0274360	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
162	0.0274380	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
163	0.0274400	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
164	0.0274420	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
165	0.0274440	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
166	0.0274460	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
167	0.0274480	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
168	0.0274500	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
169	0.0274520	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
170	0.0274540	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
171	0.0274560	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
172	0.0274580	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
173	0.0274600	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
174	0.0274620	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
175	0.0274640	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
176	0.0274660	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
177	0.0274680	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
178	0.0274700	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
179	0.0274720	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
180	0.0274740	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
181	0.0274760	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
182	0.0274780	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
183	0.0274800	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
184	0.0274820	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
185	0.0274840	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
186	0.0274860	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
187	0.0274880	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
188	0.0274900	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
189	0.0274920	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
190	0.0274940	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
191	0.0274960	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
192	0.0274980	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
193	0.0275000	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
194	0.0275020	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
195	0.0275040	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
196	0.0275060	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
197	0.0275080	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
198	0.0275100	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
199	0.0275120	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
200	0.0275140	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
201	0.0275160	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
202	0.0275180	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
203	0.0275200	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
204	0.0275220	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
205	0.0275240	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
206	0.0275260	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
207	0.0275280	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
208	0.0275300	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
209	0.0275320	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
210	0.0275340	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
211	0.0275360	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
212	0.0275380	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
213	0.0275400	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
214	0.0275420	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
215	0.0275440	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
216	0.0275460	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
217	0.0275480	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
218	0.0275500	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
219	0.0275520	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
220	0.0275540	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
221	0.0275560	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
222	0.0275580	192.168.1.254	192.168.43.53	ICMP	70	Time to live exceeded (Time to Live exceeded in transit)
223	0.0275600	192.168.1.254	19			

The screenshot displays the Wireshark application window. At the top, the title bar reads "Wireshark - [c:\Users\j...]\Applications\Wireshark". The main menu includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony Tools, Internals, and Help. Below the menu is a toolbar with icons for various functions like opening files, capturing packets, and analyzing data. A filter bar at the top shows the selected filter: "[icmp]". The packet list pane on the left contains several entries, with the first one highlighted: No. 0, Time 0.000000000, Source 172.26.254.254, Destination 172.26.43.33, Protocol ICMP, Length 80. The packet details pane on the right shows the expanded fields for the selected packet, including Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) request. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format. The status bar at the very bottom indicates "Identification up(id), 2 bytes | Packets: 29015 | Displayed: 36 of 131 | Load time: 0:00:43 | Profile: Default".

The screenshot shows the Wireshark network protocol analyzer interface. At the top, the title bar indicates the application is running on a Windows machine. The main window is divided into several panes:

- Packet List:** Displays a list of captured packets. Packet 1 is selected, showing it is an Ethernet II, Type 802.3, and MAC Control frame.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header with destination MAC address 02:00:00:00:00:00 and source MAC address 02:00:00:00:00:00. The protocol field is set to 802.3.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The top status bar shows the current session information, including the capture file (capture.pcap), the version of Wireshark (1.12.7), and the source of the capture (from master-1.120).

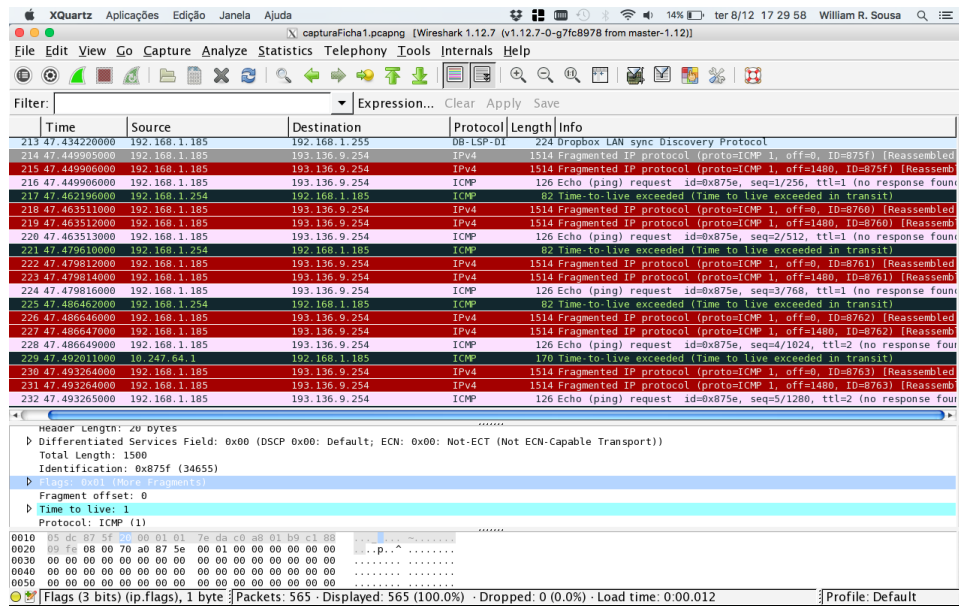
Datagrama 90: identificação é 0x9634 e  $TTL = 255$ .

Datagrama 92: identificação é 0x9635 e  $TTL = 255$

Datagrama 94: identificação éi 0x9636 e  $TTL = 255$

Esses valores permanecem constantes para todas as mensagens de resposta *ICMP TTL exceeded* enviados pelo primeiro router ao seu *host*? Porquê? O campo de identificação muda, pois o pacote não está fragmentado logo os pacotes enviados têm identificadores únicos. O *TTL* permanece constante com valor de 255*hops*.

### 2.3 Pretende-se agora analisar a fragmentação de pacotes IP. Reponha a ordem do tráfego capturado usando a coluna do tempo de captura



Time	Source	Destination	Protocol	Length	Info
213.47.434220000	192.168.1.185	192.168.1.255	DB-LSP-DI	224	Dropbox LAN sync Discovery Protocol
214.47.449050000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=875f) [Reassembled]
215.47.449060000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=875f) [Reassembled]
216.47.449060000	192.168.1.185	193.136.9.254	ICMP	126	Echo (ping) request id=0x875e, seq=1/256, ttl=1 (no response found)
217.47.463190000	192.168.1.254	192.168.1.185	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
218.47.463511000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8760) [Reassembled]
219.47.463512000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8760) [Reassembled]
220.47.463513000	192.168.1.185	193.136.9.254	ICMP	126	Echo (ping) request id=0x875e, seq=2/512, ttl=1 (no response found)
221.47.479610000	192.168.1.254	192.168.1.185	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
222.47.479612000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8761) [Reassembled]
223.47.479614000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8761) [Reassembled]
224.47.479616000	192.168.1.185	193.136.9.254	ICMP	126	Echo (ping) request id=0x875e, seq=3/768, ttl=1 (no response found)
225.47.486462000	192.168.1.254	192.168.1.185	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
226.47.486464000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8762) [Reassembled]
227.47.486467000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8762) [Reassembled]
228.47.486490000	192.168.1.185	193.136.9.254	ICMP	126	Echo (ping) request id=0x875e, seq=4/1024, ttl=2 (no response found)
229.47.493261000	192.168.1.254	192.168.1.185	ICMP	126	Time-to-live exceeded (Time to live exceeded in transit)
230.47.493264000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=8763) [Reassembled]
231.47.493264000	192.168.1.185	193.136.9.254	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8763) [Reassembled]
232.47.493265000	192.168.1.185	193.136.9.254	ICMP	126	Echo (ping) request id=0x875e, seq=5/1280, ttl=2 (no response found)

Header Length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 1500  
Identification: 0x875f (34655)  
Fragment offset: 0  
Time to live: 1  
Protocol: ICMP (1)

0010 05 dc 87 5f 00 01 01 7e da c0 a8 01 b9 c1 88 ...P...  
0020 00 fa 00 00 70 a0 87 5e 00 01 00 00 00 00 00 ...P...  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...P...  
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...P...  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...P...

Flags (3 bits) (ip.flags), 1 byte Packets: 565 - Displayed: 565 (100.0%) - Dropped: 0 (0.0%) - Load time: 0 00.012 Profile: Default

Localize a primeira mensagem *ICMP* depois do tamanho de pacote ter sido definido em 3072bytes. A mensagem foi fragmentada? Porque é que houve (ou não) necessidade de o fazer? A trama em análise na imagem, correspondente ao datagrama 214, indica que houve de facto fragmentação porque apesar do *offset* estar a zero, a *flag more fragments* está activa. Existiu a necessidade de fragmentar o pacote porque o comprimento definido do MTU foi de 3000bytes que excede a capacidade da infraestrutura de rede, que interliga os routers, usada foi a *ethernet* que tem um limite de MTU com 1500bytes.

Imprima o primeiro fragmento do datagrama *IP* segmentado. Que informação no cabeçalho indica que o datagrama foi fragmentado? Que informação no cabeçalho *IP* indica que se trata do primeiro fragmento? Qual é o tamanho deste datagrama *IP*? A informação que indica se o datagrama foi fragmentado é o par *fragmentation flag* que está a um, indicando que o datagrama deve ser fragmentado e o *offset* que indica em que posição do pacote esse datagrama se refere, neste caso o *offset* está a 0 o que indica que se trata do primeiro datagrama do pacote fragmentado. O tamanho do datagrama é de 1480 bytes que é o limite do MTU (1500 bytes) menos o *overhead* (20 bytes).

Time	Source	Destination	Protocol	Length	Info
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=0, len=1480) [Fragmented]
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=1480, len=1480) [Fragmented]
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=2960, len=1480) [Fragmented]

Imprima o segundo fragmento do datagrama *IP* original. Que informação do cabeçalho *IP* indica que não se trata do 1º fragmento? Há mais fragmentos? O que nos permite afirmar isso? Não se trata do 1º pacote pois o *offset* não é 0. Ainda, existe pelo menos mais um fragmento pois a *flag more fragments* está a 1.

Time	Source	Destination	Protocol	Length	Info
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=0, len=1480) [Fragmented]
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=1480, len=1480) [Fragmented]
213.47.234.208	192.168.1.185	192.168.1.254	IPV4	1480	Fragmented IP protocol (protocol=1, offset=2960, len=1480) [Fragmented]

Quantos fragmentos foram criados a partir do datagrama original? Como se detecta o último fragmento correspondente ao datagrama original? Foram criados, a partir do datagrama original, três fragmentos. O último fragmento correspondente verifica-se quando a *flag more fragments* é zero. E no datagrama original é feito uma “reassemblagem”, neste caso no terceiro datagrama, do datagrama original.



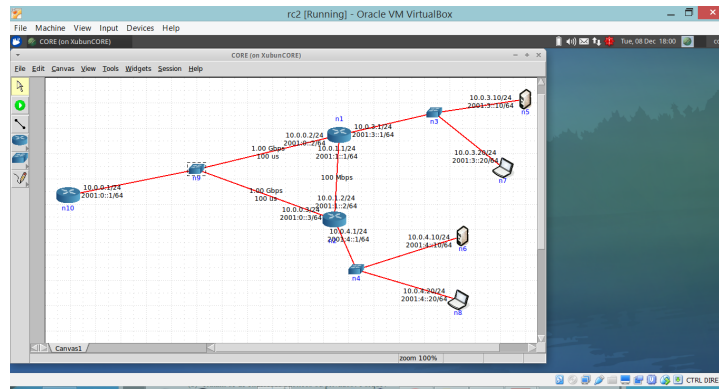
[illegible]

**Indique, resumindo, os campos que mudam no cabeçalho *IP* entre os diferentes fragmentos, e verifique a forma como essa informação permite reconstruir o datagrama original.** Os campos que alteram no cabeçalho *IP* são os campos: *more fragments* e *fragment offset*. Para se obter o datagrama original (“reassemblagem”) basta consultar esses dois campos, tal como explicado anteriormente, pois conseguimos sempre identificar qual o primeiro e o último fragmento (e consequentemente os intermédios) e com o auxílio do campo *offset* a sua posição relativa ao datagrama original.

### 3 Endereçamento e Encaminhamento IP

#### 3.1 Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.

Indique que endereços IP e máscaras de rede foram atribuídos automaticamente pelo CORE a cada equipamento. (Pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento).



Como os endereços IP são /24 a máscara de rede correspondente é o 255.255.255.0.

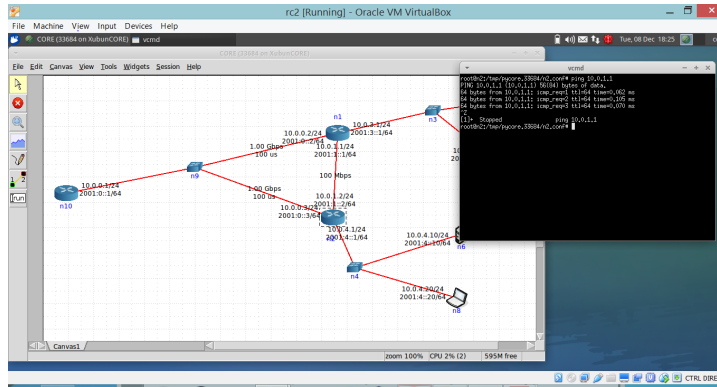
Equipamento	Endereço IP	Rede	Máscara de Rede
Router Saída (n10)	10.0.0.1	10.0.0.0	255.255.255.0
Router Departamento X (n1)	10.0.0.2	10.0.0.0	255.255.255.0
Router Departamento X (n1)	10.0.1.1	10.0.1.0	255.255.255.0
Router Departamento X (n1)	10.0.3.1	10.0.3.0	255.255.255.0
Router Departamento Y (n2)	10.0.0.3	10.0.0.0	255.255.255.0
Router Departamento Y (n2)	10.0.1.2	10.0.1.0	255.255.255.0
Router Departamento Y (n2)	10.0.4.1	10.0.4.0	255.255.255.0
Host Departamento X (n5)	10.0.3.10	10.0.3.0	255.255.255.0
PC Departamento X (n7)	10.0.03.20	10.0.3.0	255.255.255.0
Host Departamento Y (n6)	10.0.4.10	10.0.4.0	255.255.255.0
PC Departamento Y (n8)	10.0.4.20	10.0.4.0	255.255.255.0

**Tratam-se de endereços públicos ou privados? Porquê?** São endereços privados, pois estão dentro dos blocos atribuídos para intranets privadas, ou seja, sem conectividade IP global. Não devem, portanto, ser visíveis e não são encaminhadas para a Internet. Estes blocos são os seguintes [192.168.0.0; 192.168.255.255], [172.16.0.0; 172.16.255.255], [10.0.0.0; 10.255.255.255]. Como os endereços IP atribuídos na rede estão dentro da gama [10.0.0.0; 10.255.255.255] podemos afirmar que são endereços privados.

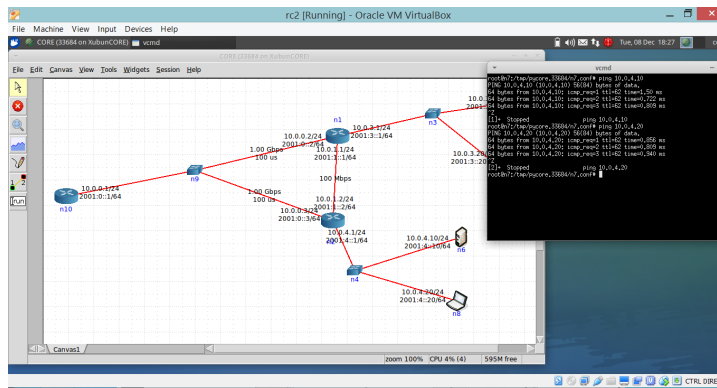
**Porque razão não é atribuído um endereço aos switches?** Não são atribuídos endereços IP aos switches, pois estes são apenas comutadores de rede que operam ao nível físico e a cada porta está associado um domínio de colisão diferente, ou seja, não trata de um alternado de canais segundo uma lógica qualquer implementada, por outras palavras não encaminha nenhum datagrama na rede.

Usando o comando **ping** certifique-se que existe conectividade total entre os sistemas em ligados em rede (basta certificar a conectividade para uma interface de cada rede).

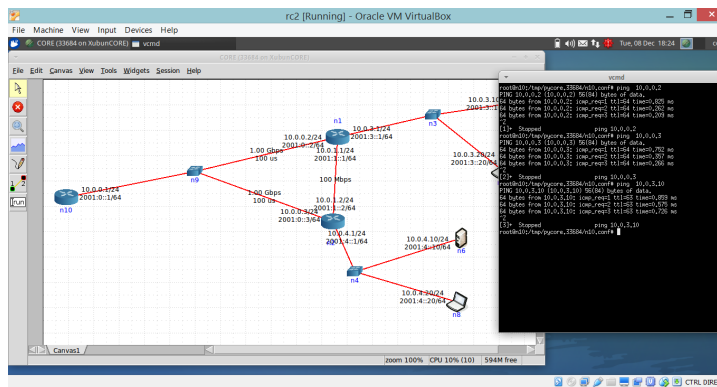
Ping a partir de n2:



Ping a partir de n7:

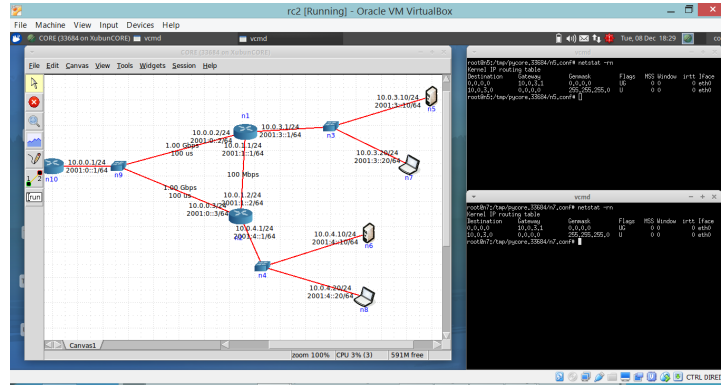


Ping a partir de n10:



### 3.2 Para o router e um laptop de um dos departamentos:

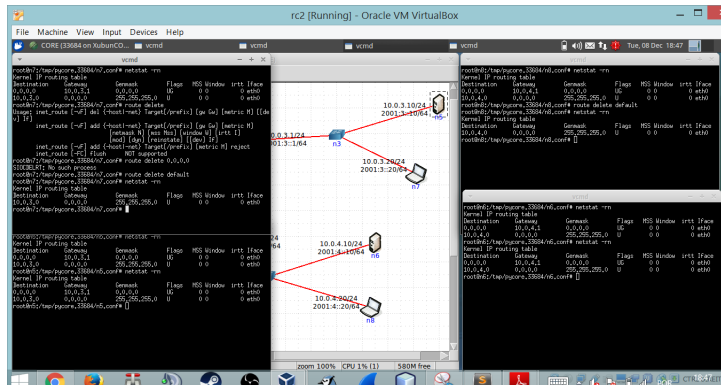
Execute o comando `netstat -rn` por forma a poder consultar a tabela de encaminhamento *unicast (IPv4)*. Inclua no seu relatório as tabelas de encaminhamento obtidas; interprete as várias entradas de cada tabela. Se necessário, consulte o manul respectivo (`man netstat`).



*Destination* corresponde ao destino, *Gateway* é o endereço do proximo salto a ser usado para chegar ao destino, *Genmask* indica a máscara de rede e a *flag* indica, neste caso, que o endereçamento *IP* é dinâmico, *mss* e *windows* indicam tamanhos para conexões *TCP*, neste caso ilimitadas, o *irtt* (*inicial round trip time*) é uma estimativa e por fim o *Iface* é a porta a ser usada.[3]

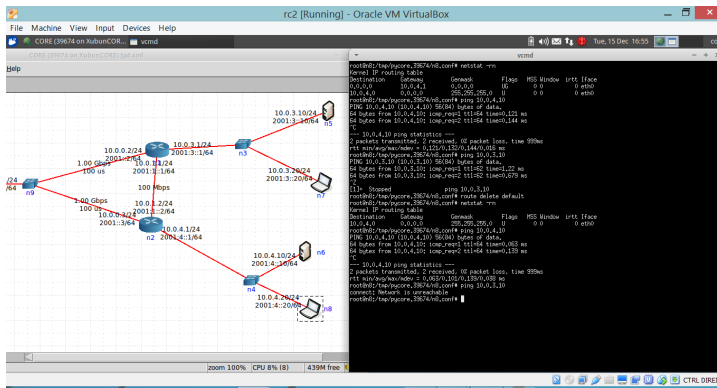
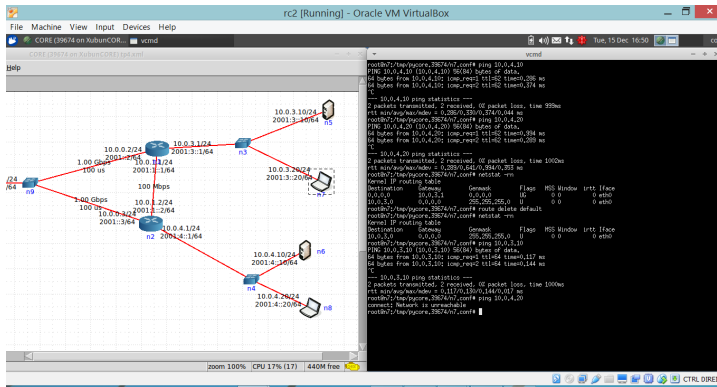
Diga, justificando, se está a ser usado encaminhamento estático ou dinâmico O endereçamento é dinâmico, pois a *flag* é U; se fosse estático teria o valor S.

Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou default) deve ser retirada das tabelas de encaminhamento dos *laptops* de cada departamento. Use o comando `route delete` para o efeito. Como é afectada a conectividade *IP* para cada um dos servidores. Justifique. Ao ser removida a rota por defeito eliminamos a possibilidade de encaminhar pacotes para qualquer rede que não esteja na tabela de encaminhamento, dessa forma, eliminamos por exemplo a possibilidade de conexão com o exterior através da Internet.

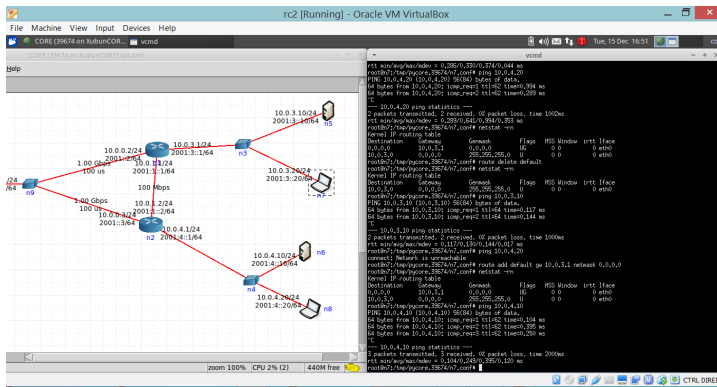


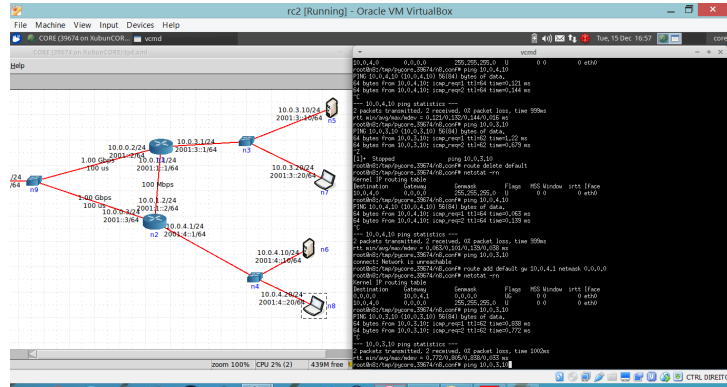
Adicione as rotas estáticas necessárias para repor a conectividade entre os departamentos. Utilize para o efeito o comando `route add`. Registe o comando completo que usou. Teste a nova política de encaminhamento garantido que ambos os servidores estão acessíveis, utilizando para o efeito o comando `ping`. Inclua as novas tabelas de encaminhamento dos *laptops* O comando utilizado foi o `route add -net 10.0.1.0 gw 10.0.0.1 netmask 255.255.5.255 dev eth0` que adicionou a rota estática para a sub-rede 10.0.1.0 utilizando como destino no salto (*gateway*) o endereço 10.0.0.1.

*Laptop n7 e n8 antes de adicionar rota estática*



*Laptop n7 e n8 após rota estática e teste de conectividade*

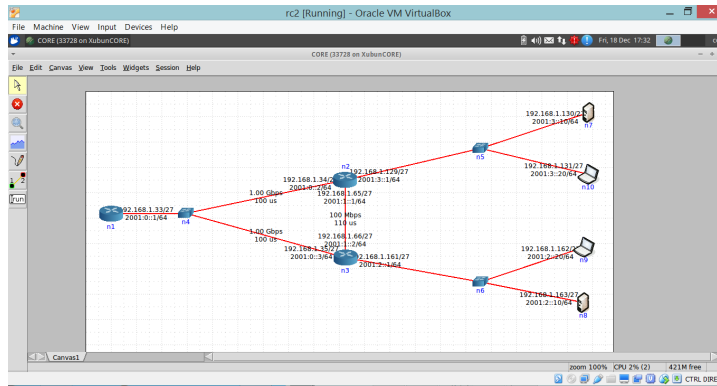




**Que conclui face à actual conectividade externa e interna na empresa?** A topologia da rede, após todas as alterações efectuadas, corresponde a uma rede fechada, ou seja, não possui conectividade com o exterior, portanto como a infraestrutura de rede da empresa, possui conectividade pelo menos interna, então corresponde a uma intranet.

## 4 Definição de Sub-redes

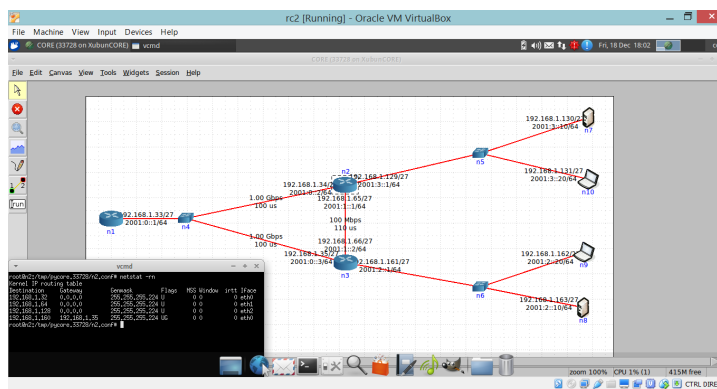
- 4.1 Assumindo que dispõe apenas de um único endereço de rede *IP* classe C 192.168.1.0/24, defina um novo esquema de endereçamento para as redes dos departamentos (mantendo a rede de core inalterada) e atribua endereços às interfaces dos vários sistemas envolvidos. Deve justificar as opções usadas.



Foi fornecido um prefixo de rede *IP* classe C correspondente a 192.168.1.0/24, logo temos  $32 - 24 = 8\text{bits}$  para codificar a atribuição de endereços *IP*. Para além disso dispomos de 4 redes internas distintas na nossa infraestrutura. Para proceder à atribuição de endereços *IP* temos que conseguir identificar inequivocamente as redes internas, logo necessitamos de pelo menos 3 bits para esse efeito. Portanto, temos 3bits para identificar as sub-redes e 5bits para hosts/interfaces.

Como existem dois endereços reservados em cada rede a gama de valores, tanto das sub-redes como dos respectivos hosts/interfaces não varia num intervalo contínuo. Deste modo as gamas de endereços possíveis para hosts/interfaces são : [192.168.1.33; 192.168.1.63] [192.168.1.65; 192.168.1.95] [192.168.1.97; 192.168.1.127] [192.168.1.129; 192.168.1.159] [192.168.1.161; 192.168.1.191] [192.168.1.193; 192.168.1.223], em que as sub-redes possíveis utilizando 192.168.1.0/27 são 192.168.1.32 ; 192.168.1.64; 192.168.1.96; 192.168.1.128; 192.168.1.160; 192.168.1.192.

- 4.2 Qual a máscara de rede que usou (em formato decimal)?



A máscara a ser utilizar é a 255.255.255.224.

- 4.3 Com base no novo endereçamento, será possível ao encaminhador de saída anunciar um único prefixo de rede que agregue as redes dos departamentos?

Obviamente, uma vez que o endereço das redes de departamento são aquelas com o prefixo superior a 192.168.1.128/24.

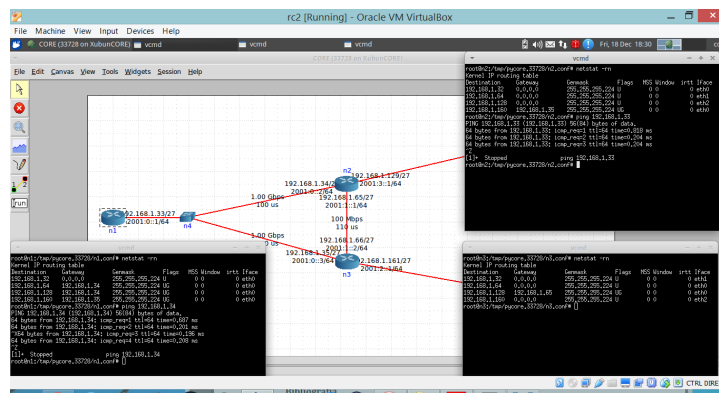
#### 4.4 Que prefixo de rede pode ser anunciado para o exterior?

O prefixo 192.168.1.0/24.

#### 4.5 Quantos *host* pode interligar em cada departamento?

Estamos a utilizar 5 *bits* para representar hosts/interfaces, no entanto os endereços correspondentes aos bits todos nulos ou todos a 1 estão reservados para identificar qualquer host e broadcast respectivamente; como tal restam  $2^5 - 2 = 30$ .

#### 4.6 Garanta que conectividade *IP* entre as várias redes da filial é mantida.



## 5 Conclusão

Neste relatório que foi realizado com o intuito de propor respostas as perguntas apresentadas na ficha prática nº 4, no âmbito da unidade curricular de Redes de Computadores, acreditamos ter respondido de forma clara e bem fundamentada as questões aqui apresentadas, em que um dos principais objectivos era consolidar os conhecimentos teóricos relativos a camada de rede, nomeadamente o protocolo *IPv4*.

Utilizamos, tal como nas fichas práticas anteriores, o analisador de tráfego *Wireshark* para analisar os datagramas *IP*, focando-se essencialmente no seu cabeçalho e na possível fragmentação dos datagramas. Utilizámos também o *CORE* para poder virtualmente administrar e gerir uma rede e estudar de forma mais aprofundada a atribuição e o encaminhamento de endereços *IP*.

De uma forma geral, na primeira parte do relatório nos apercebemos das funções essenciais do protocolo *IP*, que são essenciais para o funcionamento da Internet que essencialmente, mas não só, funciona sobre o *TCP*. E numa segunda parte, estudamos como a atribuição de endereços pode, ou não, influenciar a conectividade e funcionamento, nomeadamente dos endereços *IP* a anunciar para o exterior de forma agregada, caso seja adoptada uma política “inteligente” de atribuição de endereços, sendo possível tirar partido do *supernetting*.

Na primeira parte do relatório, utilizando o analisador de tráfego *Wireshark*, analisamos as mensagens *ICMP* (*Internet Control Menssagem Protocol*) que servem de protocolo diagnóstico ao nível da rede, mais precisamente informa com base nos valores *TTL* se um pacote, foi ou não, entregue ao destino. Para além disso, conseguimos ao longo da ficha consolidar os conhecimentos que tínhamos sobre os campos relativos ao cabeçalho *IPv4* e o seu respectivo *overhead*. Por fim, conseguimos compreender que dado os limites que



podem existir numa infraestruturas de rede, pode ou não, ser necessário fragmentar um pacote e proceder a sua respectiva “reassemblagem” no destino, estudamos como é possível e de que forma garantimos que entregamos o datagrama original no destino depois de fragmentado (com auxílio dos campos *more fragments* e *offset*).

Na segunda parte ao utilizar o *CORE* para consolidar os conceitos relativos ao encaminhamento e endereçamento *IP*. No caso do endereçamento, estudamos qual os papéis das máscaras de rede na resolução de endereços *IP*, como identificamos e quais as diferenças entre endereçamento estático e dinâmico, por fim em que medida e como podemos atribuir os endereços de forma a criar e tirar partido do *subnetting* na estruturação da rede, de acordo com os requisitos do administrador, para que possa ser otimizado, caso seja necessário, através de rotas o funcionamento da rede.

## Referências

1. Wikipedia : OSI Model [https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model) (19/12/2015)
2. Wikipedia: Internet protocol suite: [https://en.wikipedia.org/wiki/Internet\\_protocol\\_suite](https://en.wikipedia.org/wiki/Internet_protocol_suite) (19/12/2015)
3. Route Table: <http://www.cyberciti.biz/faq/what-is-a-routing-table/> (19/12/2015)
4. TCP/IP Teoria e Prática - Fernando Boa Vida, Mário Bernardes - Fernando Boa Vida, Mário Bernardes. ISBN: 978-972-722-745-7