Universidade do Minho
Braga, Portugal

Redes de Computadores TP2

23rd October 2019

1.B. Comportamento esperado, foi feita uma rota entre o servidor s1 e o PC h5 através dos routers r2, r3 e r4, sendo feito um ping com sucesso, e recebida uma reply.

1.C. ttl mínimo = 4

1.D. RTT médio = 0.209 ms

2.

```
/tmp/wireshark_wlp3s0_20191106141346_v1xytK.pcapng 34304 total packets, 34 shown

No.     Time           Source                Destination           Protocol Length Info
     59 16.242882635   172.26.60.248         193.136.9.240         ICMP     74     Echo (ping) request
id=0x0002, seq=1/256, ttl=1 (no response found!)
Frame 59: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
    Interface id: 0 (wlp3s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  6, 2019 14:14:03.293189771 WET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1573049643.293189771 seconds
    [Time delta from previous captured frame: 0.000566051 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 16.242882635 seconds]
    Frame Number: 59
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x95c9 (38345)
    Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x6f6d [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
Internet Control Message Protocol
```

2.A 172.26.60.248

2.B ICMP. Identifica o protocolo de comunicação e encaminhamento dos dados em rede.

2.C Cabeçalho: 20 bytes. Payload: 40 bytes. Tamanho total menos cabeçalho, 60-20=40 bytes

2.D Não, pois o payload length do packet nao supera o MTU(Maximum Transmission Unit).

2.E Identification,TTL, Header Checksum.

/tmp/wireshark_wlp3s0_20191106141346_v1xytK.pcapng 34304 total packets, 34 shown

```
No.     Time           Source                Destination           Protocol Length Info
     65 16.243077670   172.26.60.248         193.136.9.240         ICMP     74     Echo (ping) request
id=0x0002, seq=7/1792, ttl=3 (no response found!)
Frame 65: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x95cf (38351)
    Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 3
    Protocol: ICMP (1)
    Header checksum: 0x6d67 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
Internet Control Message Protocol
```

2.F Identification e TTL vãp incrementando em 1.

2.G TTL= 255. Nao, pois algumas replies tem sources diferentes.

/tmp/wireshark_wlp3s0_20191106141346_v1xytK.pcapng 34304 total packets, 34 shown

```
No.     Time           Source                Destination           Protocol Length Info
     75 16.261136420   172.26.254.254        172.26.60.248         ICMP     70     Time-to-live exceeded
(Time to live exceeded in transit)
Frame 75: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9)
Internet Protocol Version 4, Src: 172.26.254.254, Dst: 172.26.60.248
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x1f4d (8013)
    Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x078c [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.254.254
    Destination: 172.26.60.248
Internet Control Message Protocol
```

3

/tmp/wireshark_wlp3s0_20191106141346_v1xytK.pcapng 34304 total packets, 34 shown

```
No.     Time           Source                Destination           Protocol Length Info
     77 16.278435885   172.16.2.1            172.26.60.248         ICMP     70     Time-to-live exceeded
(Time to live exceeded in transit)
Frame 77: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9)
Internet Protocol Version 4, Src: 172.16.2.1, Dst: 172.26.60.248
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x8ce0 (36064)
    Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
    Header checksum: 0x98c0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.2.1
    Destination: 172.26.60.248
Internet Control Message Protocol
```

3.

/tmp/wireshark_wlp3s0_20191106151919_9UcLZ9.pcapng 298 total packets, 34 shown

```
No.     Time           Source                Destination           Protocol Length Info
     88 2.257340343    172.26.60.248         193.136.9.240         ICMP     1258   Echo (ping) request
id=0x0003, seq=1/256, ttl=1 (no response found!)
Frame 88: 1258 bytes on wire (10064 bits), 1258 bytes captured (10064 bits) on interface 0
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1244
    Identification: 0x5d5d (23901)
    Flags: 0x0172
    ...0 1011 1001 0000 = Fragment offset: 2960
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xa1c7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
    [3 IPv4 Fragments (4184 bytes): #86(1480), #87(1480), #88(1224)]
Internet Control Message Protocol
```

3.A Como o packet é superior ao MTU então tem de ser partido para poder ser enviado.

3.B Flags com more fragments e como fragment offset = 0, é o primeiro fragmento. Tamanho do datagrama é de 1500

/tmp/wireshark_wlp3s0_20191106151919_9UcLZ9.pcapng 298 total packets, 298 shown

```
No.     Time           Source                Destination           Protocol Length Info
     86 2.257321401    172.26.60.248         193.136.9.240         IPv4     1514   Fragmented IP protocol
(proto=ICMP 1, off=0, ID=5d5d) [Reassembled in #88]
Frame 86: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x5d5d (23901)
    Flags: 0x2000, More fragments
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x8239 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
    Reassembled IPv4 in frame: 88
```

3.C. Fragment offset é diferente de 0 logo não é o primeiro. Há mais fragmentos pois apresenta a flag more fragments.

/tmp/wireshark_wlp3s0_20191106151919_9UcLZ9.pcapng 298 total packets, 298 shown

```
No.     Time           Source                Destination           Protocol Length Info
     87 2.257337115    172.26.60.248         193.136.9.240         IPv4     1514   Fragmented IP protocol
(proto=ICMP 1, off=1480, ID=5d5d) [Reassembled in #88]
Frame 87: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x5d5d (23901)
    Flags: 0x20b9, More fragments
    ...0 0101 1100 1000 = Fragment offset: 1480
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x8180 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
    Reassembled IPv4 in frame: 88
```

3.D Foram criados 3 fragmentos.Contém a identificação de todos os fragmentos.

/tmp/wireshark_wlp3s0_20191106151919_9UcLZ9.pcapng 298 total packets, 298 shown

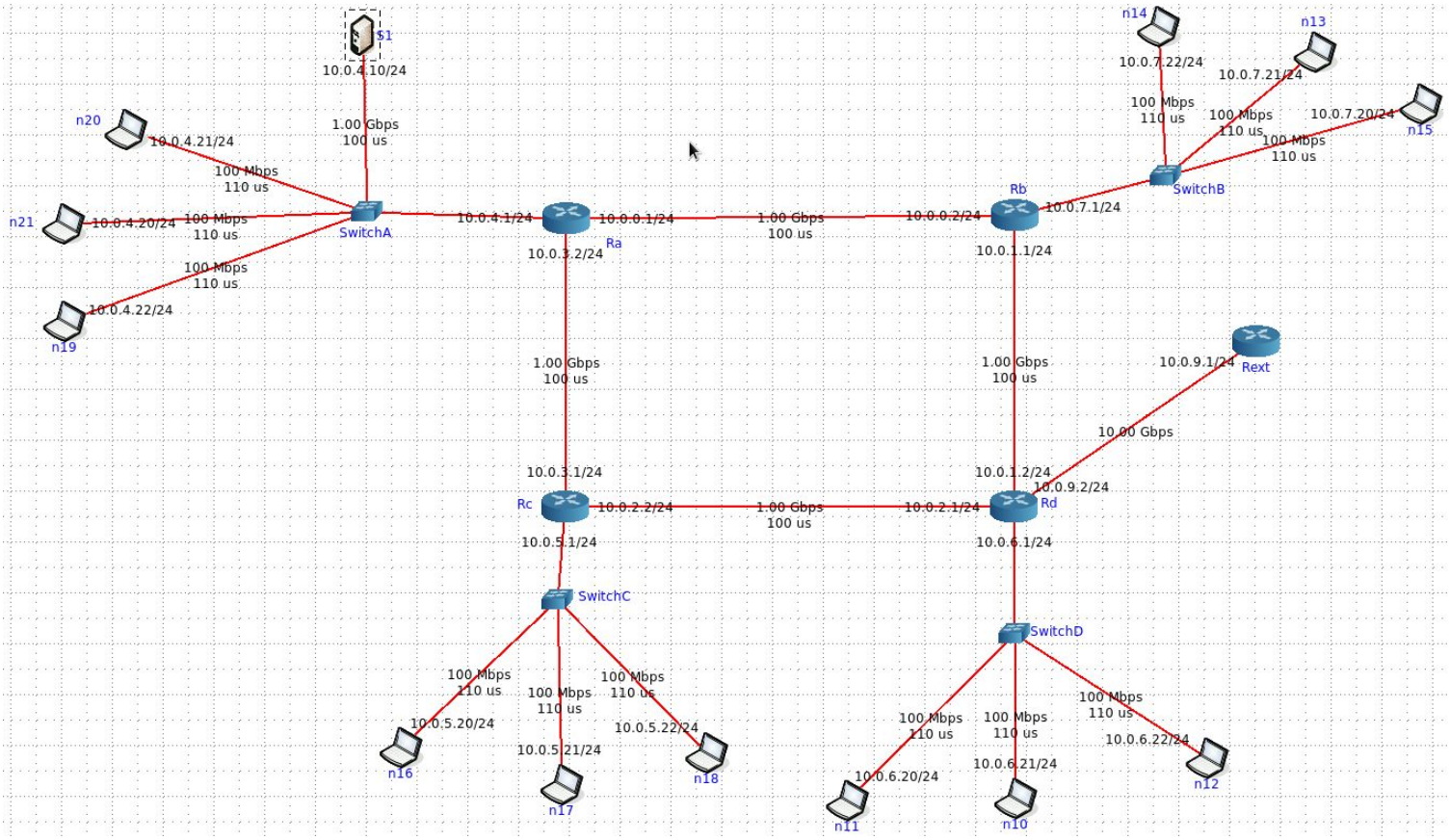
```
No.     Time           Source                Destination           Protocol Length Info
     88 2.257340343    172.26.60.248         193.136.9.240         ICMP     1258   Echo (ping) request
id=0x0003, seq=1/256, ttl=1 (no response found!)
Frame 88: 1258 bytes on wire (10064 bits), 1258 bytes captured (10064 bits) on interface 0
Ethernet II, Src: Azurewav_d2:bb:b9 (28:c2:dd:d2:bb:b9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Internet Protocol Version 4, Src: 172.26.60.248, Dst: 193.136.9.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1244
    Identification: 0x5d5d (23901)
    Flags: 0x0172
    ...0 1011 1001 0000 = Fragment offset: 2960
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xa1c7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.60.248
    Destination: 193.136.9.240
    [3 IPv4 Fragments (4184 bytes): #86(1480), #87(1480), #88(1224)]
        [Frame: 86, payload: 0-1479 (1480 bytes)]
        [Frame: 87, payload: 1480-2959 (1480 bytes)]
        [Frame: 88, payload: 2960-4183 (1224 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 4184]
        [Reassembled IPv4 data: 08008e720003000148494a4b4c4d4e4f5051525354555657…]
Internet Control Message Protocol
```

3.E Flags e header checksum. As flags permitem identificar quanto do datagrama já foi enviado e se existe mais fragmentos, quando chega ao último fragmento, reconstroi o datagrama.

Parte 2:

1.

a)



b) Públicas porque são endereços de classe A (entre 10.0.0.0 e 10.255.255.255).

c) Os switches não possuem endereços IP porque a função dos mesmos é a de conectar vários elementos a um router, sendo estes apenas uma maneira de melhor organizar as ligações.

d)

PC do departamento A:

```
[n20 n20.conf]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10) 56(84) bytes of data.
64 bytes from 10.0.8.10: icmp_seq=1 ttl=63 time=0.996 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=63 time=0.454 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=63 time=0.455 ms
64 bytes from 10.0.8.10: icmp_seq=4 ttl=63 time=0.455 ms
^C
--- 10.0.8.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.454/0.590/0.996/0.234 ms
```

PC do departamento C:

```
[n16 n16.conf]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10) 56(84) bytes of data.
64 bytes from 10.0.8.10: icmp_seq=1 ttl=62 time=0.871 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=62 time=0.691 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=62 time=0.802 ms
^C
--- 10.0.8.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.691/0.788/0.871/0.074 ms
[n16 n16.conf]#
```

PC do departamento D:

```
[n11 n11.conf]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10) 56(84) bytes of data.
64 bytes from 10.0.8.10: icmp_seq=1 ttl=61 time=1.07 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=61 time=0.899 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=61 time=0.926 ms
^C
--- 10.0.8.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.899/0.965/1.072/0.075 ms
[n11 n11.conf]#
```

PC do departamento B:

```
[n15 n15.conf]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10) 56(84) bytes of data.
64 bytes from 10.0.8.10: icmp_seq=1 ttl=62 time=0.866 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=62 time=0.692 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=62 time=0.686 ms
64 bytes from 10.0.8.10: icmp_seq=4 ttl=62 time=0.869 ms
^C
--- 10.0.8.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.686/0.778/0.869/0.089 ms
```

e)

Teste de conectividade desde router exterior até servidor S1:

```
[Rext Rext.conf]# ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10) 56(84) bytes of data.
64 bytes from 10.0.8.10: icmp_seq=1 ttl=61 time=0.908 ms
64 bytes from 10.0.8.10: icmp_seq=2 ttl=61 time=0.852 ms
64 bytes from 10.0.8.10: icmp_seq=3 ttl=61 time=0.815 ms
^C
--- 10.0.8.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.815/0.858/0.908/0.038 ms
[Rext Rext.conf]# traceroute -I 10.0.8.10
traceroute to 10.0.8.10 (10.0.8.10), 30 hops max, 60 byte packets
 1  10.0.9.2 (10.0.9.2)  0.757 ms  0.669 ms  0.711 ms
 2  10.0.1.1 (10.0.1.1)  0.690 ms  0.670 ms  0.661 ms
 3  10.0.0.1 (10.0.0.1)  0.650 ms  0.643 ms  0.635 ms
 4  10.0.8.10 (10.0.8.10)  5.837 ms  5.844 ms  5.823 ms
[Rext Rext.conf]#
```

Pode se concluir que existe conectividade IP entre o router Rext e o servidor S1.

2.

a)

Comando executado no router do departamento B:

```
[Rb Rb.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
10.0.2.0        10.0.1.2        255.255.255.0   UG        0 0          0 eth1
10.0.3.0        10.0.0.1        255.255.255.0   UG        0 0          0 eth0
10.0.4.0        10.0.0.1        255.255.255.0   UG        0 0          0 eth0
10.0.5.0        10.0.0.1        255.255.255.0   UG        0 0          0 eth0
10.0.6.0        10.0.1.2        255.255.255.0   UG        0 0          0 eth1
10.0.7.0        0.0.0.0         255.255.255.0   U         0 0          0 eth2
10.0.8.0        10.0.0.1        255.255.255.0   UG        0 0          0 eth0
10.0.9.0        10.0.1.2        255.255.255.0   UG        0 0          0 eth1
[Rb Rb.conf]#
```

Comando executado num PC do departamento B:

```
[n15 n15.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.7.1        0.0.0.0         UG        0 0          0 eth0
10.0.7.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
[n15 n15.conf]#
```

b)

Analisando os processos que estão a correr no Rb (Router do departamento B), obtemos:

```
[Rb Rb.conf]# ps -e
  PID TTY          TIME CMD
    1 ?        00:00:00 vnoded
   54 ?        00:00:00 zebra
   60 ?        00:00:00 ospf6d
   64 ?        00:00:00 ospfd
   81 pts/7    00:00:00 bash
   85 pts/7    00:00:00 ps
[Rb Rb.conf]#
```

Aqui podemos observar que temos dois processos que referem protocolos de encaminhamento dinâmico (OSPF). Conclui-se então que está a ser usado encaminhamento dinâmico.

c)

```
[S1 S1.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.4.1        0.0.0.0         UG        0 0          0 eth0
10.0.4.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
[S1 S1.conf]# route delete default
[S1 S1.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.4.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
[S1 S1.conf]#
```

Executando o comando “route delete default” acontece que deixa de haver ligações default para IPs diferentes de 10.0.8.0, qualquer ligação alternativa não vai ter resposta.

d)

Comandos para adicionar todas as rotas estáticas:

```
[S1 S1.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.4.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
[S1 S1.conf]# route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.1.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.2.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.3.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.4.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.5.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.6.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.7.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.8.0 netmask 255.255.255.0 gw 10.0.4.1
[S1 S1.conf]# route add -net 10.0.9.0 netmask 255.255.255.0 gw 10.0.4.1
```

e)

Utilizando o comando ping verificamos que existe conectividade a todos os departamentos.

Tabela netstat nova:

```
[S1 S1.conf]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.0.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.1.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.2.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.3.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.4.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.4.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.0.5.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.6.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.7.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.8.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
10.0.9.0        10.0.4.1        255.255.255.0   UG        0 0          0 eth0
[S1 S1.conf]#
```

Conclusões:

Com este trabalho ganhamos muita experiência a utilizar e analisar os vários programas indicados, como o CORE, em que ficamos proficientes a fazer topologias de redes e utilizar comandos para simular e testar ligações entre routers, PC's e servidores. Ficamos também familiarizados com o Wireshark de maneira a analisar as mensagens e pedidos enviados entre os vários componentes de uma topologia.

O uso de terminal também foi essencial para a execução dos diferentes comandos indicados no enunciado ('netstat', 'route', 'traceroute', entre outros). Foi necessário verificar a documentação de alguns destes comandos para poder analisar os seus resultados, fizemos isto a partir do uso do comando 'man' no terminal.

Tivemos mais dificuldade na questão 3 devido a não termos interpretado bem o enunciado, mas no resto do trabalho conseguimos fazer o pedido, com a ajuda ocasional do professor.

Em conclusão, este trabalho foi essencial para o nosso desenvolvimento e aprendizagem desta cadeira e na utilização de software de simulação de redes.