

Prueba

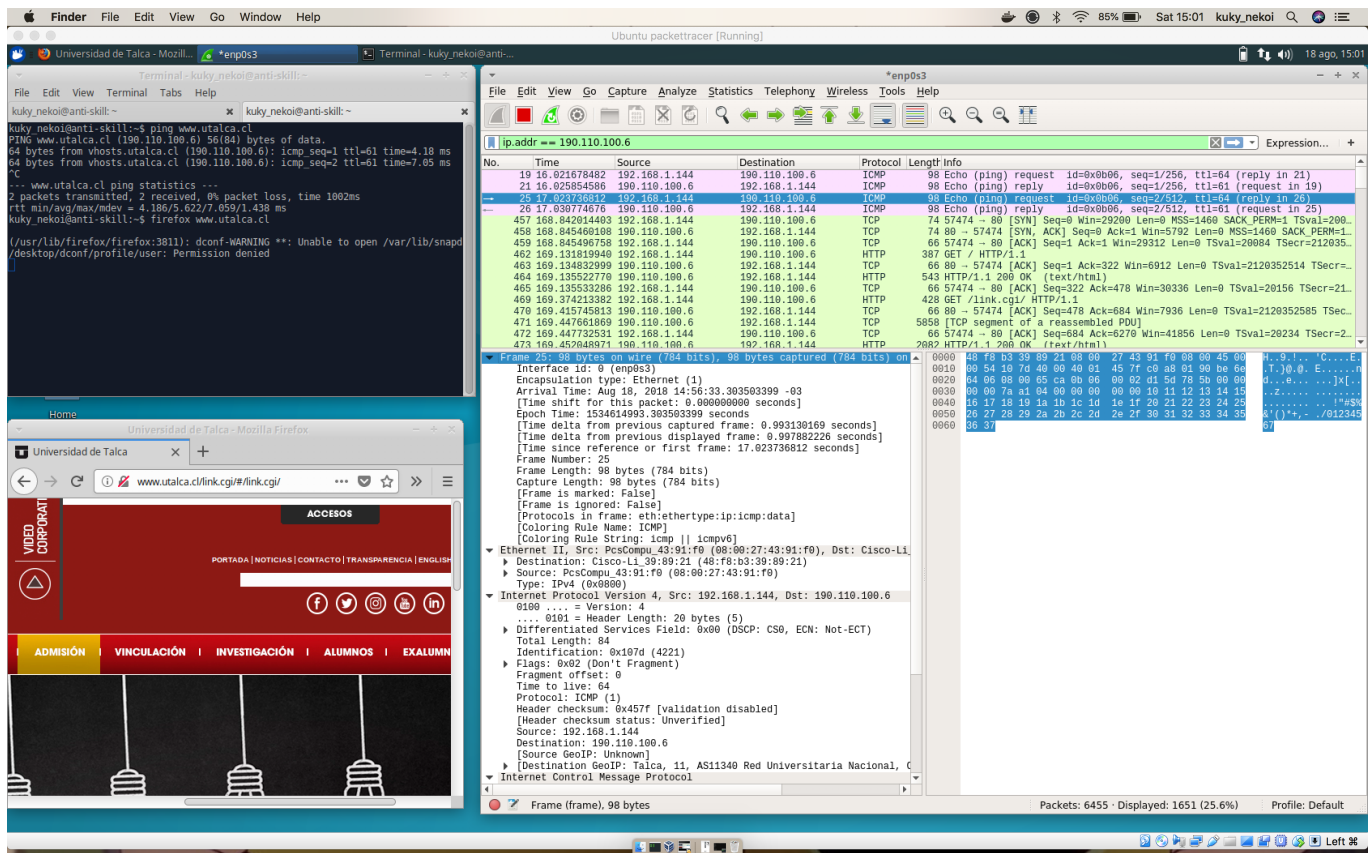
El resto de la prueba fue escrita, por lo que no está en este repositorio.

Pregunta 1

1.a.- Dirección IP de destino

190.110.100.6

1.b.- Compruebe que la dirección es correcta mediante un ping.



1.c.- Dirección IP de la fuente

192.168.1.144

1.d.- ¿Cuál es el host de destino?

www.otalca.cl

1.e.- ¿Qué versión del explorador muestra el paquete? ¿Coincide?

Mozilla 5. Si coincide aproximadamente, de todas maneras es la que manifiesta el cliente.

1.f.- Identifique la porcion hexa del destino, fuente y mac.

The screenshot displays a network traffic analysis setup. On the left, a terminal window shows commands like 'ping www.uta.cl' and 'nmap -sS 190.110.100.6'. In the center, a Firefox browser displays the website 'www.uta.cl'. On the right, the Wireshark network protocol analyzer shows a packet capture of traffic to and from 190.110.100.6. The packet list shows various protocols including ICMP, TCP, and HTTP. The packet details pane shows the structure of an Ethernet II frame, an Internet Protocol Version 4 header, and a Hypertext Transfer Protocol (HTTP) request. The packet bytes pane shows the raw data of the selected packet.

1.g Haga una nueva captura con los sitios www.yahoo.com y www.cisco.com y www.google.com y diga si existen diferencias.

Las diferencias son principalmente las direcciones, ya que la mayoría de la comunicación se lleva a cabo entre el equipo y el enrutador, por tanto detalles del hardware son omitidos durante la transmisión. Adicionalmente no se captura el tráfico de las ip de [yahoo.com](http://www.yahoo.com) ni [google.com](http://www.google.com) ya que estas sirven el tráfico a través de balanceadores con diferentes IPs las que son asignadas durante el proceso de descubrimiento del dns. Por

3: Genere un script con tres tareas en un crontab

```
## Crontab definition
```



```
0 8 * * 1-5 /home/kuky_nekoi/shutdown_staging.sh > /var/log/rpi_aws.log
0 20 * * 1-5 /home/kuky_nekoi/poweron_staging.sh > /var/log/rpi_aws.log
```

Shellscript

Both scripts are intended to run on a RPi, in order to shutdown and disconnect bastion servers when people is around office hours

shutdown_staging.sh

```
#!/bin/bash
echo "#####"
echo "Execution time: $(date)"
# stop staging environment
public_ip="$(dig +short myip.opendns.com @resolver1.opendns.com)"
echo $public_ip > /tmp/public_address #this should be replaced with
another directory

# revoke access to bastion
aws eb stop -f
aws ec2 revoke-security-group-ingress --group-name bastion-development --
protocol tcp --port 22 --cidr ${myip}/24
```

poweron_staging.sh

```
echo "#####"
echo "Execution time: $(date)"
#!/bin/bash
# automatic updation of some packages
apt-get update
apt-get upgrade -y

# stop staging environment
public_ip=$(cat /tmp/public_address)

# revoke access to bastion
aws eb stop -f
aws ec2 authorize-security-group-ingress --group-name bastion-development
--protocol tcp --port 22 --cidr ${myip}/24
```

4 packet tracer

El [archivo .pkt](#) contiene la información de la red solicitada. No fue securizado ningun router puesto que el problema era de enrutamiento + argumentos.

Capturas

Interface id: 0 (enp0s3)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 18, 2018 15:07:03.73352961 -03
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1534615623.73352961 seconds
[Time delta from previous captured frame: 0.00116722 seconds]
[Time delta from previous displayed frame: 0.00116722 seconds]
[Time since reference or first frame: 647.45386374 seconds]
Frame Number: 20444
Frame Length: 744 bytes (5952 bits)
Capture Length: 744 bytes (5952 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
▼ Ethernet II, Src: PcsCompu.43:91:f0 (08:00:27:43:91:f0), Dst: PcsCompu.43:91:f0 (08:00:27:43:91:f0)
► Destination: PcsCompu.43:91:f0 (08:00:27:43:91:f0)
► Source: Cisco-Li.39:89:21 (48:f8:b3:39:89:21)
Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 23.41.157.14, Dst: 192.168.1.144
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 798
Identification: 0x9d31 (36145)
► Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x3b7d (validation disabled)
[Header checksum status: Unverified]
Source: 23.41.157.14
Destination: 192.168.1.144
► [Source GeoIP: Cambridge, MA, AS13424 Intercity, United States, 42.36258]
[Destination GeoIP: Mountain View, CA, AS15169 Google Inc., United States]
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 56688, Seq: 1, Ack: 1
► Destination (ip.dst), 4 bytes

Interface id: 0 (enp0s3)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 18, 2018 15:08:05.416762930 -03
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1534615685.416762930 seconds
[Time delta from previous captured frame: 0.00028523 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 709.136996343 seconds]
Frame Number: 27765
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: PcsCompu.43:91:f0 (08:00:27:43:91:f0), Dst: Cisco-Li.39:89:21 (48:f8:b3:39:89:21)
► Destination: Cisco-Li.39:89:21 (48:f8:b3:39:89:21)
► Source: PcsCompu.43:91:f0 (08:00:27:43:91:f0)
Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.1.144, Dst: 64.233.186.103
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xf32a (62250)
► Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x89f5 (validation disabled)
[Header checksum status: Unverified]
Source: 192.168.1.144
Destination: 64.233.186.103
► [Source GeoIP: Unknown]
[Destination GeoIP: Mountain View, CA, AS15169 Google Inc., United States]
▼ Internet Control Message Protocol
► Destination (ip.dst), 4 bytes

captura1 captura1 captura1 captura1 captura1 captura1 captura1 captura1
captura1 captura1 captura1

Configuracion ospf

```
! router 0
enable
configure terminal
router ospf 10
log-adjacency-changes
network 200.33.146.0 0.0.0.3 area 10
network 192.168.1.0 0.0.0.255 area 10
passive-interface gigabitEthernet0/0
passive-interface gigabitEthernet0/1
passive-interface gigabitEthernet0/2
                        redis static subnet

exit
exit
wr
exit

! router 1
enable
configure terminal
router ospf 10
log-adjacency-changes
network 200.33.146.0 0.0.0.3 area 10
network 200.33.147.0 0.0.0.3 area 10
network 172.16.1.0 0.0.0.255 area 10
passive-interface gigabitEthernet0/0
passive-interface gigabitEthernet0/1
passive-interface gigabitEthernet0/2
                        redis static subnet

exit
exit
wr
exit

! router 2
enable
configure terminal
router ospf 10
log-adjacency-changes
network 200.33.147.0 0.0.0.3 area 10
network 10.1.50.0 0.0.0.255 area 10
passive-interface gigabitEthernet0/0
passive-interface gigabitEthernet0/1
passive-interface gigabitEthernet0/2
                        redis static subnet

exit
exit
wr
exit
```

Argumento OSPF

- OSPF es un protocolo que no es privativo, por tanto podemos seguir extendiendo la red con otros productos que no sean CISCO.
- Las definiciones de area y que sea classless permite definir las máscaras solicitadas.
- Es fácil de utilizar.