

GII TDRC

MEMORIA EVALUACIÓN SEMINARIOS

Autor: Antonio Fernández Ares (Basado en: Miguel Ángel López y Revisión Antonio M. Mora)
antares@ugr.es

NOMBRE Y APELLIDOS	Nikita Stetskiy		
ISLA X	8	ISLA Y	10

INSTRUCCIONES:

- No es obligatorio la resolución de todos los ejercicios. Los alumnos podrán elegir los ejercicios a resolver para alcanzar el máximo de calificación.
- No todos los ejercicios tienen la misma puntuación, ni implican el mismo tiempo de resolución. Se recomienda leer todos los ejercicios antes de empezar a resolverlo.
- Debe reemplazar por la respuesta correcta todo texto que aparezca de color rojo. Puede añadir todas las anotaciones e texto adicional que estime conveniente.
- Incluya capturas de pantalla donde aparezca el símbolo de imagen (reemplace dicha imagen por la captura o capturas que necesite). ¹



- Incluya fotografías donde aparezca el símbolo de imagen (reemplace dicha imagen por las fotografías que necesite). Se le pedirá que los ejercicios sean resueltos en papel, y adjunte en la memoria una fotografía de ese folio. Si necesita asesoramiento, consulte con el profesor.

¹ Puede emplear la herramienta recortes en windows para realizar las capturas de pantalla o emplear el atajo WINDOWS+IMPRIMIR_PANTALLA y posteriormente pegar la captura en el documento.

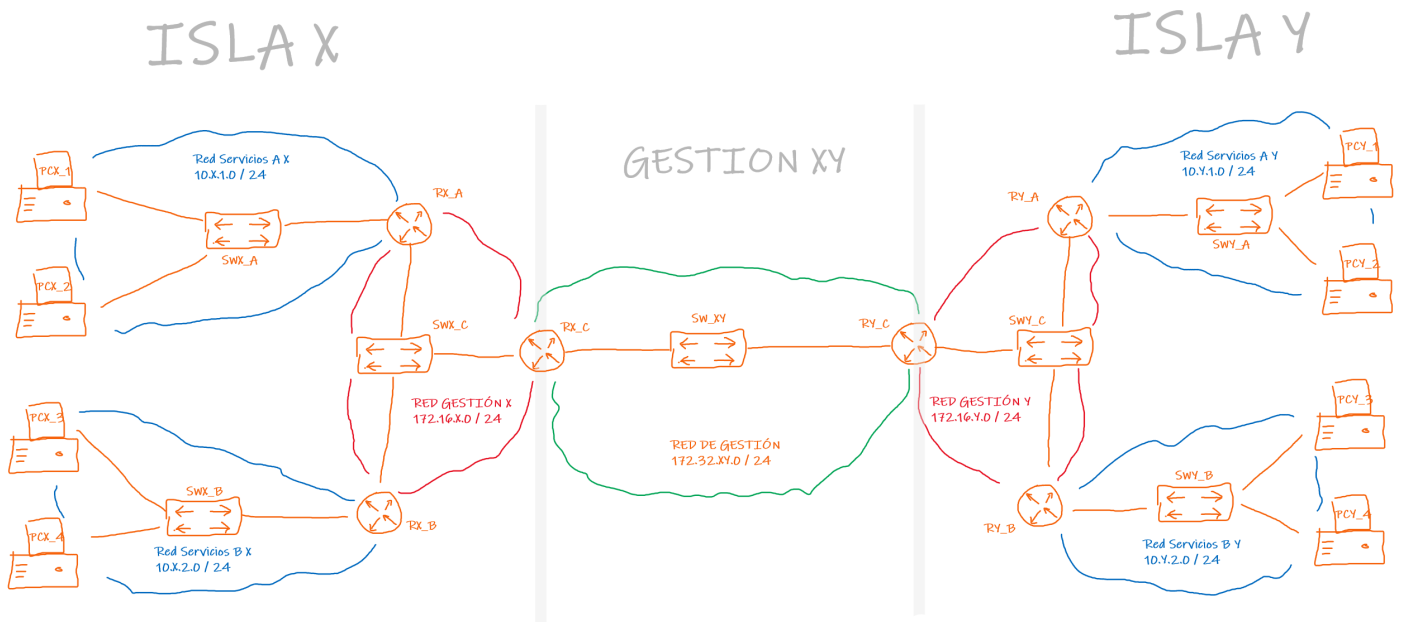
- Puede emplear la herramienta Shutter en linux para realizar las capturas de pantalla.
- Puede emplear el atajo COMANDO+MAYUSCULAS+4+BARRA_ESPACIADORA en MAC para realizar las capturas de pantalla.

EVALUACIÓN:

- La nota de seminarios es de 1.5 puntos sobre el total de la asignatura. Esta nota es la máxima obtenible por tareas desarrolladas en seminarios.
- La asistencia a cada seminario se recompensa con 0.1 puntos sobre el total por cada seminario. Se puede conseguir un máximo de 0.5 puntos por asistencia.
- Esta memoria de prácticas se puntúa sobre un máximo de 1.5 puntos, pero se ofertan ejercicios con un potencial mayor, para que los alumnos elijan los ejercicios a resolver.
- La resolución de más ejercicios, no aumentará la nota de seminarios por encima de los 1.5 puntos, pero aumentará las posibilidades de alcanzar la máxima nota en caso de errar en alguno de los ejercicios.

CONSIDERACIONES PREVIAS:

- Muchas de las preguntas de esta memoria se basan en la topología de red diseñada en el seminario 5, basada en los valores X e Y asignados en el documento disponible en PRADO.



- El NO cumplimiento de la asignación de las islas X e Y será considerado como susceptible plagio, por lo que será abordado según la normativa vigente de la universidad de Granada.
- Adicionalmente, se hará uso de la herramienta TURNITIN² para la detección de posibles plagios en la elaboración de esta memoria.

FORMATO DE ENTREGA:

- Una vez elaborado este documento será convertido a PDF y entregado en PRADO.

² <https://biblioteca.ugr.es/pages/servicios/turnitin>

SEMINARIO 1 – REPASO DIRECCIONAMIENTO IPv4

Ejercicio 1
(0.1 puntos)

Indique la siguiente información para la red Servicios A de la Isla X de la topología diseñada en el seminario 5.

Dirección IP	10.8.1.80 / 24
Clase	A
Publica / Privada	Privada
Máscara	255.255.255.0 = /24
Nº bits de red/host	24/8
Nº de IPs disponibles en la subred	$2^8 - 2$ (reservadas) = 254
Dirección de RED	10.8.1.0 / 24
Dirección de Difusión (Broadcast)	10.8.1.255
Primera IP disponible	10.8.1.1
Última IP disponible	10.8.1.254
Posición de la IP en la subred	Posición 80
¿Qué IP está justo en la mitad +1 de la subred?	10.8.1.128

Ejercicio 2
(0.1 puntos)

Las redes de servicio están sobredimensionadas para el número de host terminales que tienen. Rediseñe la red de Servicios B de la isla Y para que se desperdicien la menor cantidad de direcciones IP. Para ello, emplee VLSM para emplear un tamaño de máscara variable. Adicionalmente, responda a las siguientes cuestiones:

¿Cuántos host terminales tiene la red B de la isla Y?

Contando las interfaces que utilizan los ordenadores tenemos 2, pero si contamos también la del router serían 3.

¿Cuántas direcciones IP necesita dicha red?

Usamos 5 direcciones IP, entre ellas, 2 están reservadas para la red y broadcasting. También usamos 2 para hosts terminales y 1 para la dirección del router. Por lo que necesitamos 8 direcciones IP.

Rellene la siguiente tabla con la información resultante.

IP red	10.10.2.3 / 29
Clase	A
Publica / Privada	Privada
Máscara	255.255.255.248 = /29
Nº bits de red/host	29/3
Nº de IPs disponibles en la subred	$2^3 - 2$ (reservadas) = 6
Dirección de RED	10.10.2.0 / 29
Dirección de Difusión (Broadcast)	10.10.2.7
Primera IP disponible	10.10.2.1
Última IP disponible	10.10.2.6
Posición de la IP en la subred	Posición 3
¿Qué IP está la 2ª en la subred?	10.10.2.2

Ejercicio 3
(0.1 puntos)

Suponga que en la red de gestión (aquella que conecta los routers RX_C y RY_C) se conecta un nuevo dispositivo enrutador (al que denominaremos RZ) que conecta con otra red (Red Z). Se desea configurar los equipos de la red Z para que envíen al router RZ el tráfico perteneciente a las redes de Servicio de las islas X e Y. Se propone emplear el enrutamiento entre dominios sin clase (CIDR) para minimizar la tabla de enrutamiento.

Calcule la dirección de red y máscara que englobando a todos los host de las redes de servicios de las islas X e Y, hacen la red lo más compacta posible. Puede emplear la siguiente tabla como apoyo:

10.10.1.1	0000 1010	0000 10 10	0000 0001	0000 0001
10.10.1.2	0000 1010	0000 10 10	0000 0001	0000 0010
10.10.2.1	0000 1010	0000 10 10	0000 0010	0000 0001
10.10.2.2	0000 1010	0000 10 10	0000 0010	0000 0010
10.8.1.1	0000 1010	0000 10 00	0000 0001	0000 0001
10.8.1.2	0000 1010	0000 10 00	0000 0001	0000 0010
10.8.2.1	0000 1010	0000 10 00	0000 0010	0000 0001
10.8.2.2	0000 1010	0000 10 00	0000 0010	0000 0010

10.8.0.0 / 14	255.252.0.0
---------------	-------------

Para ello he utilizado el protocolo CIDR, el cual permite un uso más eficiente de las direcciones IPv4. Para ello he pasado a binario todas los hosts con el fin de sumarizar. Después he identificado el número de bit n hasta el cual todos los bits de todas los hosts son iguales (los bits contenidos entre este y los bits de host iniciales deben formar un recubrimiento completo). Para obtener el número de la red se dejan los n bits primeros como están y el resto se pone a 0 obteniendo una red X.Y.Z.K. La red será X.Y.Z.K/n

SEMINARIO 2 – HERRAMIENTAS Y UTILIDADES DE DIAGNÓSTICO EN RED

Ejercicio 4 (0.1 puntos)

Explique brevemente cual es la utilidad de la aplicación NMAP. Indique dos ejemplos de uso (indicando los parámetros a emplear y la información que se desea obtener) y ejecútelos contra el equipo scanme.nmap.org.

Podemos ver con la herramienta man la utilidad del comando Nmap también conocido como Network Mapper. Es una herramienta de código abierto muy versátil para los administradores de sistema. Se utiliza para explorar redes, realizar análisis de seguridad, auditoría de red y búsquedas de puertos abiertos en la máquina remota. También analiza en busca de hosts en directo, sistemas operativos, filtros de paquetes y puertos abiertos que se ejecutan en máquinas remotas.

```
NMAP(1)                                [FIXME: manual]                                NMAP(1)

NOMBRE
  nmap - Herramienta de exploración de redes y de sondeo de seguridad /
  puertos

SINOPSIS
  nmap [Tipo de sondeo...] [Opciones] {especificación de objetivo}

DESCRIPCION
  Nmap ("mapeador de redes") es una herramienta de código abierto para
  exploración de red y auditoría de seguridad. Se diseña para
  analizar rápidamente grandes redes, aunque funciona muy bien contra
  equipos individuales. Nmap utiliza paquetes IP "crudos" (A<<raw>>, N.
  del T.) en formas originales para determinar qué equipos se
  encuentran disponibles en una red, qué servicios (nombre y versión
  de la aplicación) ofrecen, qué sistemas operativos (y sus
  versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos
  se están utilizando así como docenas de otras características. Aunque
  generalmente se utiliza Nmap en auditorías de seguridad, muchos
  administradores de redes y sistemas lo encuentran útil para realizar
  tareas rutinarias, como puede ser el inventariado de la red, la
  planificación de actualización de servicios y la monitorización del
  tiempo que los equipos o servicios se mantiene activos.
```

`nmap -v scanme.nmap.org`

Este comando lo que hace es sondear todos los puertos TCP reservados del dicho servidor scanme.nmap.org. Con el modo verboso, la opción -v, se activa el modo detallado.

```
MacBook-Pro-de-Nikita:~ nikitastetskiy$ nmap -v scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-06 14:45 CEST
Initiating Ping Scan at 14:45
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 14:45, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:45
Completed Parallel DNS resolution of 1 host. at 14:45, 0.05s elapsed
Initiating Connect Scan at 14:45
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 13 out of 43 dropped p
robes since last increase.
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 14:45, 27.11s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Not shown: 962 closed ports
PORT      STATE SERVICE
13/tcp    filtered daytime
22/tcp    open  ssh
80/tcp    open  http
255/tcp   filtered unknown
513/tcp   filtered login
990/tcp   filtered ftps
1035/tcp  filtered multidropper
1065/tcp  filtered syscomlan
1096/tcp  filtered cnrprotocol
1187/tcp  filtered alias
1310/tcp  filtered husky
1455/tcp  filtered esl-lm
1594/tcp  filtered sixtrak
1761/tcp  filtered landesk-rc
2144/tcp  filtered lv-ffx
2170/tcp  filtered eyetv
2607/tcp  filtered connection
3551/tcp  filtered apcupsd
3871/tcp  filtered avocent-adsap
4321/tcp  filtered rwhois
5815/tcp  filtered unknown
5825/tcp  filtered unknown
5961/tcp  filtered unknown
5998/tcp  filtered ncd-diag
7100/tcp  filtered font-service
8002/tcp  filtered teradataordbms
8291/tcp  filtered unknown
8654/tcp  filtered unknown
9001/tcp  filtered tor-orport
9929/tcp  open  nping-echo
20031/tcp filtered unknown
24800/tcp filtered unknown
31337/tcp open  Elite
32769/tcp filtered filenet-rpc
32771/tcp filtered sometimes-rpc5
32772/tcp filtered sometimes-rpc7
49156/tcp filtered unknown
62078/tcp filtered iphone-sync

Read data files from: /usr/local/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.96 seconds
```

nmap -sS -O scanme.nmap.org/24

Lo que realiza este comando es lanzar un sondeo de tipo SYN sigiloso. Este comando requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo.

Este comando se realiza contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "scanme.nmap.org". Incluso intenta determinar cual es el sistema operativo que se ejecuta en cada máquina que esté encendida.


```
MacBook-Pro-de-Nikita:~ nikitastetskiy$ sudo nmap -sS -O scanme.nmap.org/24
Password:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-06 14:50 CEST
Nmap scan report for li982-4.members.linode.com (45.33.32.4)
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:4.2
OS details: Linux 3.13 or 4.2
Network Distance: 14 hops

Nmap scan report for li982-5.members.linode.com (45.33.32.5)
Host is up (0.18s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8090/tcp  open  opsmessaging
Aggressive OS guesses: HP P2000 G3 NAS device (93%), Linux 2.6.32 (92%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (91%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (91%), Netgear RAIDiator 4.2.21 (Linux 2.6.37) (91%), Linux 3.1 (91%), Linux 3.2 (91%), Netgem N7700 set-top box (91%), Linux 2.6.32 - 3.13 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

Nmap scan report for li982-6.members.linode.com (45.33.32.6)
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
Aggressive OS guesses: Linux 3.13 or 4.2 (94%), Linux 3.10 - 4.11 (94%), HP P2000 G3 NAS device (93%), Linux 3.2 - 4.9 (93%), Linux 2.6.32 - 3.1 (92%), Linux 3.7 (92%), Linux 2.6.32 - 3.13 (91%), Linux 3.0 - 3.2 (91%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (91%), Linux 3.16 - 4.6 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

Nmap scan report for li982-8.members.linode.com (45.33.32.8)
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: storage-misc|general purpose|WAP|broadband router|media device
Running (JUST GUESSING): HP embedded (93%), Linux 2.6.X|3.X (91%), Infomir embedded (91%), Ubiquiti embedded (91%), Ubiquiti AiROS 5.X (91%), Netgem embedded (91%)
OS CPE: cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:infomir:mag-250 cpe:/h:ubnt:airmax_nanostation cpe:/o:ubnt:airos:5.5.9 cpe:/h:netgem:n7700
Aggressive OS guesses: HP P2000 G3 NAS device (93%), Linux 2.6.32 - 3.13 (91%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (91%), Linux 2.6.32 (91%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (91%), Linux 2.6.32 - 3.1 (91%), Infomir MAG-250 set-top box (91%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (91%), Linux 3.7 (91%), Ubiquiti AiROS 5.5.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

Nmap scan report for li982-9.members.linode.com (45.33.32.9)
Host is up (0.18s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
2000/tcp  open  cisco-sccp
Aggressive OS guesses: HP P2000 G3 NAS device (93%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (91%), OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (91%), Linux 2.6.32 (91%), Linux 3.1 (91%), Linux 3.2 (91%), Netgem N7700 set-top box (91%), Linux 2.6.32 - 3.13 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90%), Linux 2.6.18 - 2.6.22 (90%)
No exact OS matches for host (test conditions non-ideal).
```


Ejercicio 5 (0.1 puntos)

Explique brevemente cual es la utilidad de la aplicación TRACEROUTE. Realice un traceroute a un equipo de la universidad de Granada (por ejemplo, el servidor web de www.ugr.es) y a otro que desconozca dónde se sitúa (por ejemplo, el servidor web de cualquier marca, empresa, videojuego que conozca. Intente ser original para evitar coincidencias). Interprete brevemente los resultados obtenidos.

Gracias a la herramienta man la utilidad del comando Traceroute, sabemos que podremos seguir la pista a los paquetes que vienen desde un host, es decir, obtendremos una estadística de la latencia de red de esos paquetes, lo que es una estimación de la distancia a la que están los extremos de la comunicación.

```
TRACEROUTE(8)          BSD System Manager's Manual          TRACEROUTE(8)

NAME
    traceroute -- print the route packets take to network host

SYNOPSIS
    traceroute [-adeFISdNnrvx] [-A as_server] [-f first_ttl] [-g gateway]
               [-i iface] [-M first_ttl] [-m max_ttl] [-P proto] [-p port]
               [-q nqueries] [-s src_addr] [-t tos] [-w waittime]
               [-z pausesecs] host [packetsize]

DESCRIPTION
    The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. traceroute utilizes the IP protocol 'time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

    The only mandatory parameter is the destination host name or IP number. The default probe datagram length is 40 bytes, but this may be increased by specifying a packet size (in bytes) after the destination host name.
```

Esta herramienta utiliza y manipula el parámetro TTL (*Time To Live*) de los paquetes UDP o ICMP para ir descubriendo la ruta que sigue dicho paquete. Incrementando el TTL unidad a unidad, puede determinar la respuesta del paquete en cada uno de los puntos o "saltos" durante su viaje en la red.

En caso de que en alguno de los saltos aparezcan asteriscos continuos, esto indica que la respuesta no fue recibida. Esto ocurre en algunos routers que no emiten mensajes ICMP de TTL expirado.

```
iMac-de-Nikita:~ nikitastetskiy$ traceroute www.ugr.es
traceroute to www.ugr.es (150.214.204.231), 64 hops max, 52 byte packets
 1  www.adsl.vf (192.168.0.1)  2.437 ms  2.261 ms  2.588 ms
 2  * * *
 3  10.183.69.17 (10.183.69.17)  28.898 ms  14.717 ms  5.232 ms
 4  * * *
 5  * * *
 6  rediris.baja.espanix.net (193.149.1.26)  14.901 ms  14.602 ms  14.726 ms
 7  ciemat.ael.cica.rtl.and.red.rediris.es (130.206.245.38)  25.191 ms  26.040 ms  25.807 ms
 8  cica-router.red.rediris.es (130.206.194.2)  26.353 ms  26.899 ms  41.572 ms
 9  xe-2-0-0.granada01.red.cica.es (150.214.231.22)  99.730 ms  30.477 ms  31.522 ms
10  ugr-router.red.cica.es (150.214.231.138)  31.657 ms  33.299 ms  30.157 ms
11  * * *
12  * * *
13  * * *
```

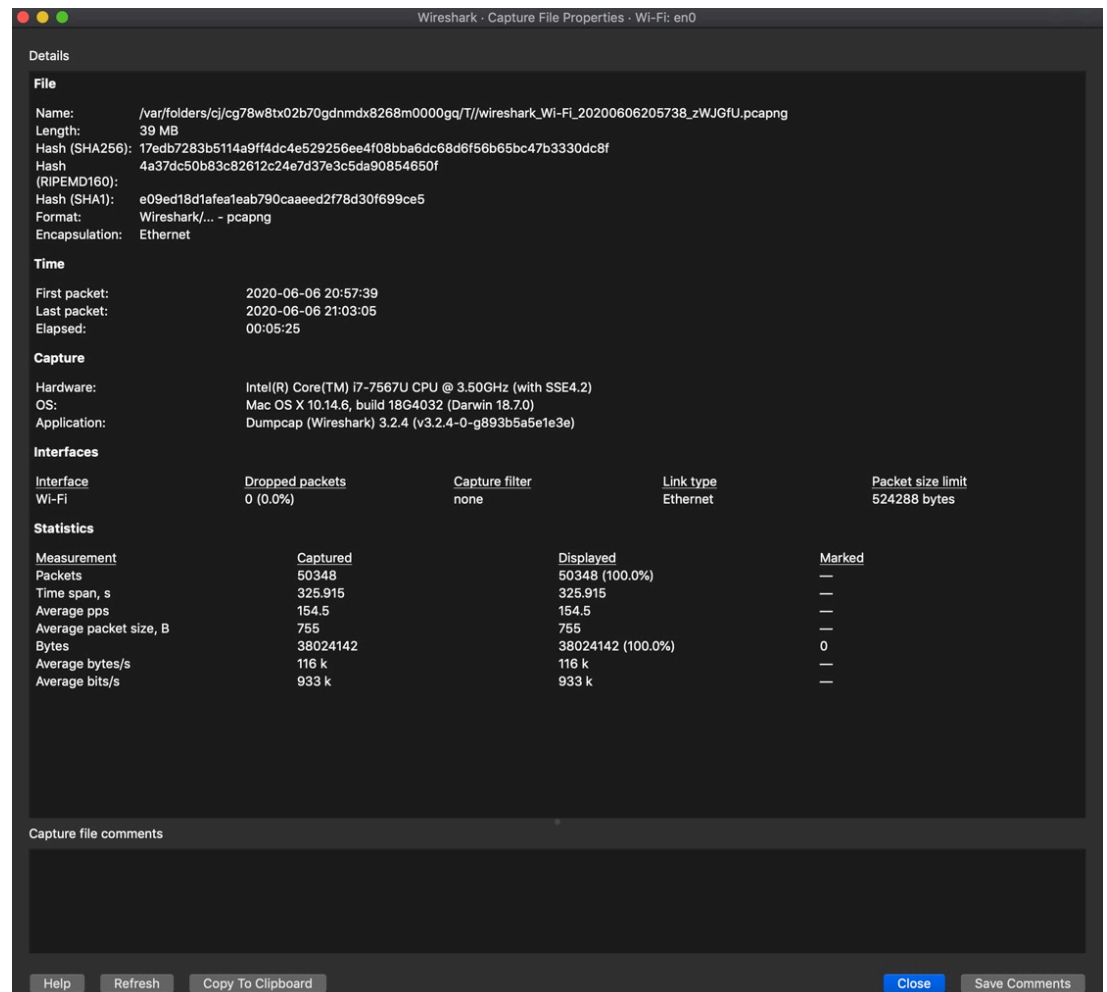
Ahora utilicemos una dirección IP de Yahoo, con la IP 98.139.183.24:

```
iMac-de-Nikita:~ nikitastetskiy$ traceroute 98.139.183.24
traceroute to 98.139.183.24 (98.139.183.24), 64 hops max, 52 byte packets
 1 www.adsl.vf (192.168.0.1) 6.450 ms 3.010 ms 1.834 ms
 2 * * *
 3 10.183.69.17 (10.183.69.17) 5.819 ms 7.283 ms 3.917 ms
 4 172.29.176.113 (172.29.176.113) 4.896 ms * *
 5 * * *
 6 ae7-100-xcr1.mat.cw.net (195.10.44.1) 13.807 ms 12.795 ms 12.489 ms
 7 ae27-xcr2.prp.cw.net (195.2.21.145) 104.237 ms 104.155 ms
 195.2.31.245 (195.2.31.245) 105.759 ms
 8 * * *
 9 et-7-1-0-xcr1.nyh.cw.net (195.2.24.241) 104.143 ms 105.769 ms 104.201 ms
10 ae30-xcr2.nyk.cw.net (195.2.16.134) 104.117 ms
  ae13-xcr2.nyk.cw.net (195.2.25.69) 104.453 ms 104.202 ms
11 nyiix.bas1-m.nyc.yahoo.com (198.32.160.121) 103.894 ms 104.418 ms 109.500 ms
12 ae-1.pat2.bfw.yahoo.com (216.115.111.26) 122.760 ms
  ae-1.pat1.bfw.yahoo.com (216.115.111.28) 114.268 ms
  ae-1.pat2.bfw.yahoo.com (216.115.111.26) 116.404 ms
13 * * *
```

Ejercicio 6 (0.3 puntos)

Empleando Wireshark, capture el tráfico de un equipo doméstico consumiendo tráfico de cualquier aplicación telemática durante al menos 5 minutos (por ejemplo, visualizando streaming, jugando a un videojuego online, teniendo una videoconferencia, asistiendo a una clase online, navegando por internet,...).

a) Muestre un resumen de la información capturada (Capture File Properties)



Wireshark - Capture File Properties - Wi-Fi: en0

Details

File

Name: /var/folders/cj/cg78w8tx02b70gdnmdx8268m0000gq/T/wireshark_Wi-Fi_20200606205738_zWJGfU.pcapng
 Length: 39 MB
 Hash (SHA256): 17edb7283b5114a9ff4dc4e529256ee4f08bba6dc68d6f56b65bc47b3330dc8f
 Hash (RIPEMD160): 4a37dc50b83c82612c24e7d37e3c5da90854650f
 Hash (SHA1): e09ed18d1afea1eab790caeed2f78d30f699ce5
 Format: Wireshark/... - pcapng
 Encapsulation: Ethernet

Time

First packet: 2020-06-06 20:57:39
 Last packet: 2020-06-06 21:03:05
 Elapsed: 00:05:25

Capture

Hardware: Intel(R) Core(TM) i7-7567U CPU @ 3.50GHz (with SSE4.2)
 OS: Mac OS X 10.14.6, build 18G4032 (Darwin 18.7.0)
 Application: Dumpcap (Wireshark) 3.2.4 (v3.2.4-0-g893b5a5e1e3e)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Wi-Fi	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

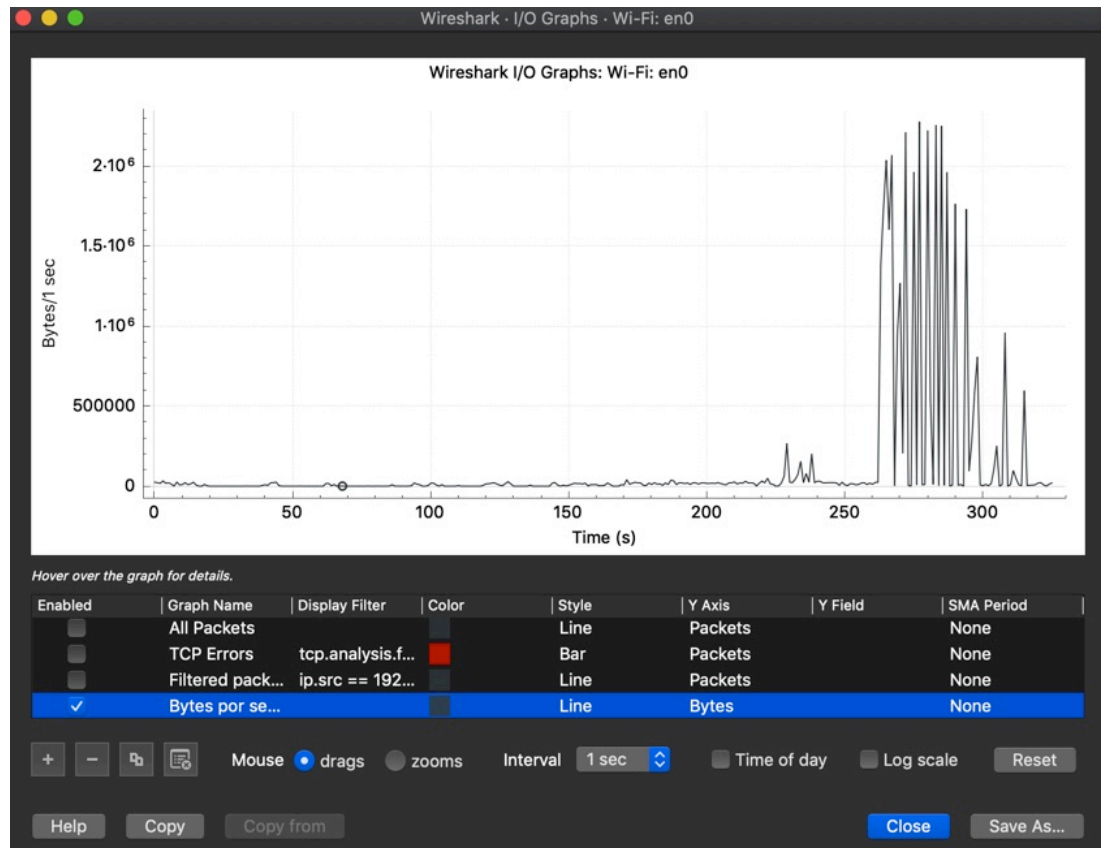
Measurement	Captured	Displayed	Marked
Packets	50348	50348 (100.0%)	—
Time span, s	325.915	325.915	—
Average pps	154.5	154.5	—
Average packet size, B	755	755	—
Bytes	38024142	38024142 (100.0%)	0
Average bytes/s	116 k	116 k	—
Average bits/s	933 k	933 k	—

Capture file comments

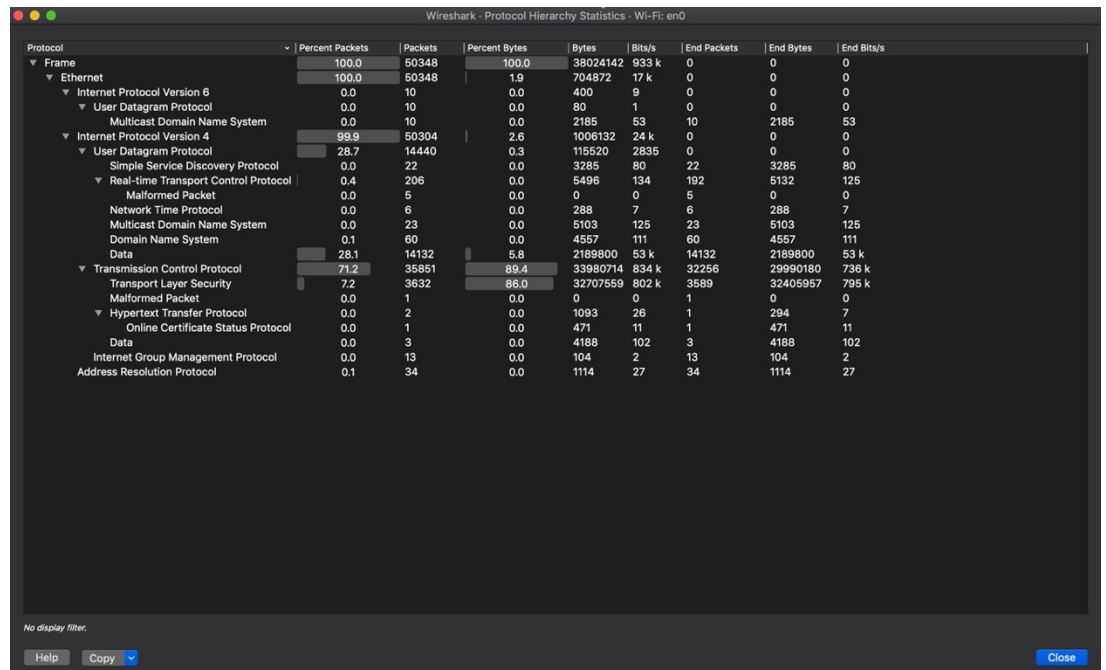
Help Refresh Copy To Clipboard Close Save Comments

b) Represente gráficamente el ancho de banda en bytes por segundo (IO

Graph).



c) Obtenga un resumen de los protocolos empleados (Protocol Hierarchy Statistics) e interprete los resultados, indicando los protocolos que conoce.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	50348	100.0	38024142	933 k	0	0	0
Ethernet	100.0	50348	1.9	704872	17 k	0	0	0
Internet Protocol Version 6	0.0	10	0.0	400	9	0	0	0
User Datagram Protocol	0.0	10	0.0	80	1	0	0	0
Multicast Domain Name System	0.0	10	0.0	2185	53	10	2185	53
Internet Protocol Version 4	99.9	50304	2.6	1006132	24 k	0	0	0
User Datagram Protocol	28.7	14440	0.3	115520	2835	0	0	0
Simple Service Discovery Protocol	0.0	22	0.0	3285	80	22	3285	80
Real-time Transport Control Protocol	0.4	206	0.0	5496	134	192	5132	125
Malformed Packet	0.0	5	0.0	0	0	5	0	0
Network Time Protocol	0.0	6	0.0	288	7	6	288	7
Multicast Domain Name System	0.0	23	0.0	5103	125	23	5103	125
Domain Name System	0.1	60	0.0	4557	111	60	4557	111
Data	28.1	14132	5.8	2189800	53 k	14132	2189800	53 k
Transmission Control Protocol	71.2	35851	89.4	33980714	834 k	32256	39980180	736 k
Transport Layer Security	7.2	3632	86.0	32707559	802 k	3589	32405957	795 k
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	0.0	2	0.0	1093	26	1	294	7
Online Certificate Status Protocol	0.0	1	0.0	471	11	1	471	11
Data	0.0	3	0.0	4188	102	3	4188	102
Internet Group Management Protocol	0.0	13	0.0	104	2	13	104	2
Address Resolution Protocol	0.1	34	0.0	1114	27	34	1114	27

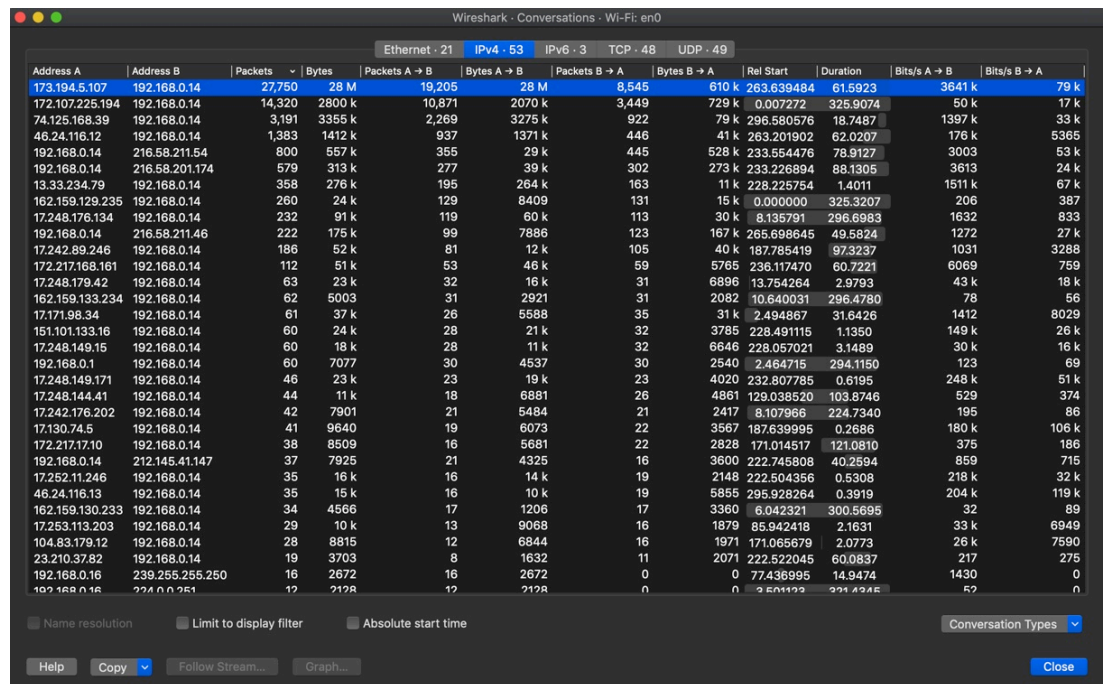
Podemos ver la poca cantidad que hay de paquetes UDP frente a la cantidad de tiempo en comparación con TCP, para UDP he utilizado un servicio de streaming de voz en línea con una aplicación llamada Discord y en los últimos minutos he visto un video en YouTube por eso podemos ver esos picos de paquetes TCP. Aunque UDP se ha utilizado más tiempo, el porcentaje de paquetes es de sólo 28.7 % frente al 71.2 % de TCP.

d) ¿Qué porcentaje del tráfico capturado es TCP y cuánto es UDP? Justifíquelo en función del tipo de aplicación telemática capturada.

Porcentaje tráfico TCP	71.2 %
Porcentaje tráfico UDP	28.7 %

La diferencia es bastante grande, sobre todo cuando vemos el tiempo que se ha empleado para medir las dos plataformas de streaming. Aunque podemos ver que la aplicación de comunicación por voz (voIP) consume muchos menos datos que un video de Youtube a 1080p, algo bastante comprensible. Ya que un video a una calidad tan alta requiere relativamente grandes cantidades de datos. Además de que apenas pierde paquetes.

e) ¿Con qué equipo (por su IP) ha conversado (conversation) mayor cantidad de tráfico (medido en paquetes)? Justifique porque hay varias “pestañas” en la ventana conversaciones. ¿Cuántos Bytes son tráfico A → B y cuanto B → A? ¿Y Bits/s? Identifique su IP y la IP del servidor externo.

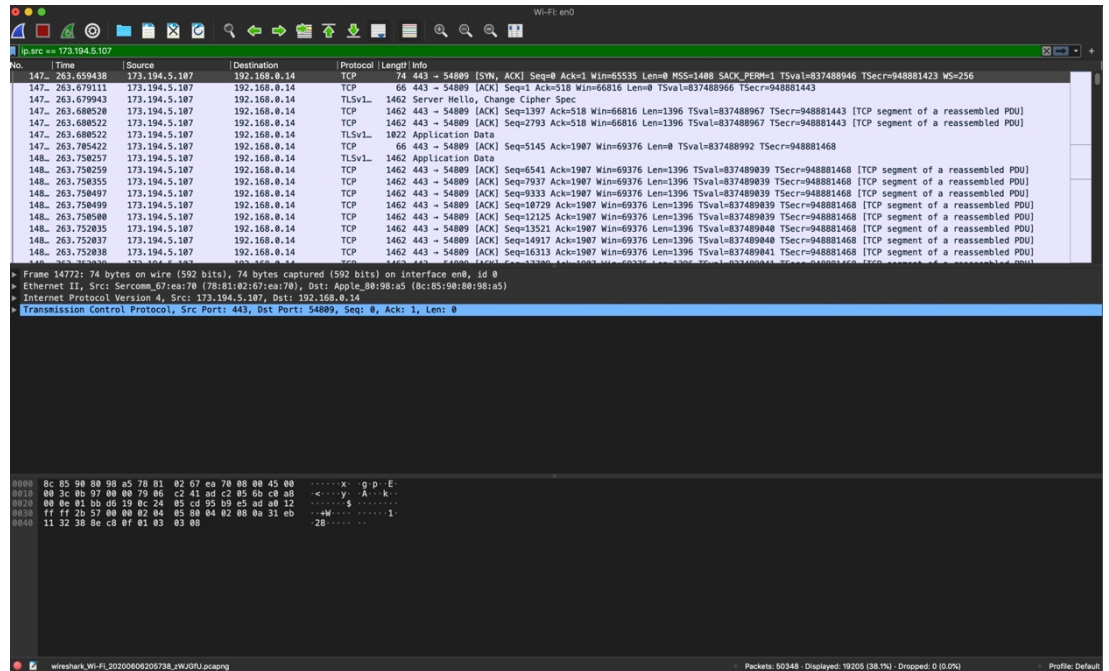


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
173.194.5.107	192.168.0.14	27,750	28 M	19,205	28 M	8,545	610 k	263.639484	61.5923	3641 k	79 k
172.107.225.194	192.168.0.14	14,320	2800 k	10,871	2070 k	3,449	729 k	0.007272	325.9074	50 k	17 k
74.125.168.39	192.168.0.14	3,191	3355 k	2,269	3275 k	922	79 k	296.580576	18.7487	1397 k	33 k
46.24.116.12	192.168.0.14	1,383	1412 k	937	1371 k	446	41 k	263.201902	62.0207	176 k	5365
192.168.0.14	216.58.211.54	800	557 k	355	29 k	445	528 k	233.554476	78.9127	3003	53 k
192.168.0.14	216.58.201.174	579	313 k	277	39 k	302	273 k	233.226894	88.1305	3613	24 k
13.33.234.79	192.168.0.14	358	276 k	195	264 k	163	11 k	228.225754	1.4011	1511 k	67 k
162.159.129.235	192.168.0.14	260	24 k	129	8409	131	15 k	0.000000	325.3207	206	387
172.48.176.134	192.168.0.14	232	91 k	119	60 k	113	30 k	8.135791	296.6983	1632	833
192.168.0.14	216.58.211.46	222	175 k	99	7886	123	167 k	265.698645	49.5824	1272	27 k
172.42.89.246	192.168.0.14	186	52 k	81	12 k	105	40 k	187.785419	97.3237	1031	3288
172.217.168.161	192.168.0.14	112	51 k	53	46 k	59	5765	236.117470	60.7221	6069	759
172.48.179.42	192.168.0.14	63	23 k	32	16 k	31	6896	13.754264	2.9793	43 k	18 k
162.159.133.234	192.168.0.14	62	5003	31	2921	31	2082	10.640031	296.4780	78	56
171.171.98.34	192.168.0.14	61	37 k	26	5588	35	31 k	2.494867	31.6426	1412	8029
151.101.133.16	192.168.0.14	60	24 k	28	21 k	32	3785	228.491115	1.1350	149 k	26 k
172.48.149.15	192.168.0.14	60	18 k	28	11 k	32	6646	228.057021	3.1489	30 k	16 k
192.168.0.1	192.168.0.14	60	7077	30	4537	30	2540	2.464715	294.1150	123	69
172.48.149.171	192.168.0.14	46	23 k	23	19 k	23	4020	232.807785	0.6195	248 k	51 k
172.48.144.41	192.168.0.14	44	11 k	18	6881	26	4861	129.038520	103.8746	529	374
172.42.176.202	192.168.0.14	42	7901	21	5484	21	2417	8.107966	224.7340	195	86
17.130.74.5	192.168.0.14	41	9640	19	6073	22	3567	187.639995	0.2686	180 k	106 k
172.217.17.10	192.168.0.14	38	8509	16	5681	22	2828	171.014517	121.0810	375	186
192.168.0.14	212.145.41.147	37	7925	21	4325	16	3600	222.745808	40.2694	859	715
172.82.11.246	192.168.0.14	35	16 k	16	14 k	19	2148	222.504356	0.5308	218 k	32 k
46.24.116.13	192.168.0.14	35	15 k	16	10 k	19	5855	295.928264	0.3910	204 k	119 k
162.159.130.233	192.168.0.14	34	4566	17	1206	17	3360	6.042321	300.5695	32	89
172.53.113.203	192.168.0.14	29	10 k	13	8068	16	1879	85.942418	2.1631	33 k	6849
104.83.179.12	192.168.0.14	28	8815	12	6844	16	1971	171.065679	2.0773	26 k	7590
23.210.37.82	192.168.0.14	19	3703	8	1632	11	2071	222.522045	60.0837	217	275
192.168.0.16	239.255.255.250	16	2672	16	2672	0	0	77.436995	14.9474	1430	0
192.168.0.16	224.0.0.251	12	2128	12	2128	0	0	2.501122	291.4245	52	0

Ha conversado más con 173.194.5.107, en el cual ha tenido más de 27 mil paquetes. Podemos ver varias pestañas debido a que existen paquetes que funcionan por distintas capas OSI, es decir, en mi caso Ethernet, IPv4, IPv6, TCP y UDP. Podemos ver que de A → B son 28 M y 3641 k (bits/s), en cambio de B → sólo 610 k y 79 k k (bits/s).

IP del equipo doméstico	192.168.0.14 - B
IP del servidor	173.194.5.107 - A

f) Filtre los paquetes para mostrar aquellos que hayan sido enviados por la IP del servidor del apartado anterior



g) Represente nuevamente el ancho de banda en bytes por segundo, pero únicamente de los paquetes filtrados anteriormente.



SEMINARIO 2 – COMANDOS CISCO

Ejercicio 7 (0.15 Puntos)

Defina los comandos y pasos necesarios para realizar la siguiente configuración en un router CISCO:

- **Cambiar el hostname del router a LANISTER**

Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname LANISTER

LANISTER(config)#exit

- **Cambiar el password de acceso administrativo**

Router>enable

Router#config t

LANISTER(config)#enable secret STARK

LANISTER(config)#exit

- **Deshabilitar las búsquedas DNS**

Router>enable

Router#config t

LANISTER(config)#no ip domain-lookup

LANISTER(config)#exit

Habilitar la IP 192.168.12.100 / 23 a la interfaz gigabytethernet 0/1

Router>enable

Router#config t

LANISTER(config)#interface gigabitethernet 0/1

LANISTER(config-if)#ip address 192.168.12.100 255.255.254.0

LANISTER(config-if)#no shutdown

LANISTER(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

LANISTER(config-if)#exit

Ejercicio 8 (0.15 Puntos)

Al ejecutar los siguientes comandos en un router CISCO está obteniendo los siguientes mensajes de error. Indique para cada uno de los errores porque está ocurriendo, que se pretendía obtener con el comando y que acciones tendría que emprender para que el comando funcione correctamente.

- a) Se obtiene el siguiente error:

```
Router(config)#show ip interface brief
      ^
% Invalid input detected at '^' marker.
```

Este comando Muestra un breve resumen de la información y del estado de una dirección IP, agrupandolas por la interfaz, la dirección IP, el estado, método de enrutamiento y el protocolo. El error esta en que no reconoce el comando en el modo configuración por lo que para solucionarlo tendríamos que salirnos del modo (config), con el comando "exit" y poner el comando de nuevo.

- b) Se obtiene el siguiente error:

```
Router(config)#ip address 192.168.12.2 255.255.255.0
      ^
% Invalid input detected at '^' marker.
```

Este comando asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz. De nuevo estamos en la configuración inadecuada para este comando, es decir, estamos en (config) y no en (config-if), para entrar en esta configuración debemos introducir la interfaz donde queramos asignar la dirección ip, mediante el comando "interface <interfaz x/x>".

- c) Se obtiene el siguiente error:

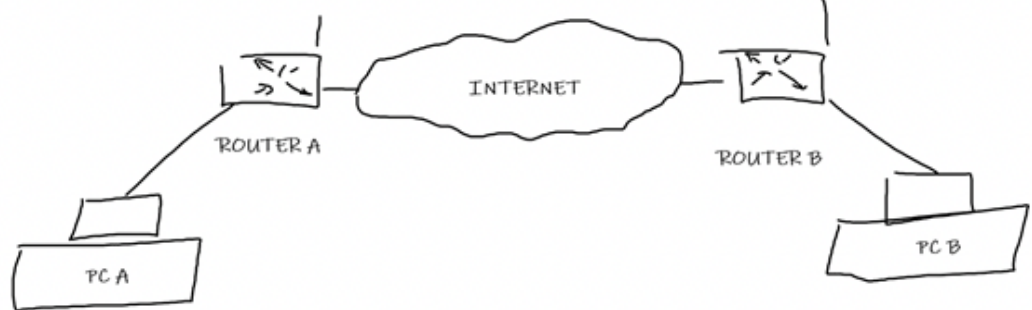
```
Router(config-if)#ip address 192.310.12.2 255.255.255.0
      ^
% Invalid input detected at '^' marker.
```

De nuevo este comando asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz, podemos ver que la ip introducida está mal ya que se sale del rango de ip de la máscara, la cuales son 255 y hemos introducido 310. Para solucionarlo solo deberíamos introducir una ip válida como puede ser 192.31.12.2 en vez de la otra.

SEMINARIO 3 – FUNDAMENTOS PARA LA PUESTA EN MARCHA DE UN SERVICIO TELEMÁTICO EN INTERNET

Ejercicio 9 (0.2 puntos)

Partiendo de la topología de red de la figura anterior, exponga que problemas nos encontraremos para intentar comunicar el PC A con el PC B. Para cada uno de estos problemas, indique que mecanismos o tecnología podemos emplear para solventarlo.



Como estamos en el seminario 3, entiendo que esta enfocado a la práctica que tuvimos que realizar. Por lo que los problemas que podrían surgir son:

- Los servicios o aplicaciones deberán ser accesibles, por lo que tendremos que contar con una ip fija. Estos ordenadores lo más probable es que no la tengan, por lo que para solucionarlo se tendría que usar el servicio DDNS como noip.com para poder usar una IP pública.
- Tampoco tendrán abiertos los puertos necesarios para poder acceder a sus servicios, por lo que se deberán abrir mediante su proveedor correspondiente o mediante la terminal.
- Otro problema es que para tener un servicio propiamente hecho, tenemos que tener instalada la propia aplicación que vayamos a usar.
- Por lo que todas las configuraciones anteriormente dichas tienen que estar bien realizadas, con sus IPs y puertos correspondientes.
- Finalmente, todo tiene que ser coherente, los PCs y los Routers funcionando y claramente los cables conectados entre sus interfaces correspondientes.

SEMINARIO 4 – PROTOCOLO ETHERNET

Ejercicio 10 (0.25 Puntos)

En seminarios hemos estudiado los mecanismos de detección de colisiones en CSMA /CD pero no se ha profundizado en ningún algoritmo de resolución o postergación de colisiones. Realice una pequeña investigación para descubrir los métodos que son habitualmente empleados como algoritmos para el cálculo de tiempo de postergación en CSMA / CD. Explique brevemente uno de ellos con un ejemplo en papel.

<EXPLICACIÓN, INCLUYENDO LAS REFERENCIAS DEBIDAMENTE DOCUMENTADAS>



SEMINARIO 4 – MEDIOS FÍSICOS PARA LA TRANSMISIÓN DE DATOS

Ejercicio 11 (0.15 Puntos)

Una fibra óptica tiene una dispersión modal de 2500 MHzKm. Se quiere usar para un enlace entre dos edificios de un parque tecnológico separados 500 metros.

- ¿De qué ancho de banda se dispondrá en MHz como máximo?
- Suponiendo que se usa una codificación con 16 niveles. ¿Cuántos Mbps se podrán alcanzar en ausencia de ruido?
- Alguien propuso instalar fibra monomodo, pero se rechazó por las altas pérdida de inserción. Explique por qué las pérdidas de inserción afectan más a la fibra monomodo que a la multimodo.

<DEBERA RESOLVER EN PAPEL ESTE EJERCICIO E INCLUIR UNA FOTOGRAFÍA DEL MISMO EN LA MEMORIA DE PRÁCTICAS>



Ejercicio 12 (0.2 Puntos)

Realice una pequeña investigación en su domicilio, para averiguar que medios físicos se están empleando en su conexión a internet. Para ello, le va a tocar mirar detrás del router y/o averiguar el modelo. Indique los tipos de cableado, tecnología en la que se basan y cualquier otro detalle que averigüe.

Además, como dispone de una red inalámbrica, averigüe que versión de WiFi está empleando, el canal de transmisión, las tecnologías de seguridad y emparejado empleados.

(EN EL CASO DE NO TENER INTERNET EN EL DOMICILIO, CONTACTE CON EL PROFESOR PARA QUE LE OFREZCA UNA ALTERNATIVA A ESTE EJERCICIO)

<PUEDEN INCLUIR FOTOGRAFÍAS DE LOS MEDIOS FÍSICOS Y CAPTURAS>



SEMINARIO 5 – INTRODUCCIÓN A LA HERRAMIENTA PACKET TRACER

Ejercicio 13 (0.1 Puntos)

Me han encantado las cuestiones y la herramienta. He respondido a las cuestiones en este enlace:

<https://www.youtube.com/watch?v=G1bRujko-A>