

Universidad Politécnica de Cartagena



Universidad  
Politécnica  
de Cartagena

**INSTRUMENTACIÓN TELEMÁTICA Y  
LABORATORIO DE REDES**  
3º Grado Ingeniería Telemática

**Práctica 3 Sesión 2: Medidas  
desempeño de red y servicios**

Versión 2019/20

**EQUIPO 3**

Profesores:  
Juan Carlos Sánchez Aarnoutse  
Alejandro Martínez Sala

### 3 Comprobación de los equipos de la red

```
sudo nmap -sP 192.168.1.1-255
```

```
sudo nmap -sP 10.1.9.0/24
```

**CUESTIÓN 1:** Anotad los resultados de los equipos. Podéis emplear una captura de pantalla. Si habéis detectado que algún equipo no está, indicadlo.

No hemos detectado ningún error.

### 4 Comprobando puertos y servicios

**CUESTIÓN 2:** Analizando puertos de los servidores desde dentro de la red.

- Escanead los puertos ofrecidos por los servidores 172.16.0.10 y 172.16.1.10. Podéis hacerlo desde dos PCs diferentes, uno para escanear cada servidor.
- Averiguad el SO que corren esos equipos con `-sV -O`  
¿Qué información adicional aparece?  
Que el sistema operativo que corre en esos equipos es Linux.

NMAP 172.16.0.10

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-11-05 10:45 CET
Nmap scan report for 172.16.0.10
Host is up (0.00027s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp    open  ssh?
80/tcp    open  http?
443/tcp   open  https?
990/tcp   open  ftps?
```

NMAP PCC 172.16.1.10

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 09:54 Hora
estándar romance
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:14 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:24 remaining)
Nmap scan report for 172.16.1.10
Host is up (0.0045s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
25/tcp    open  smtp?
```

```
80/tcp    open    http?
110/tcp   open    pop3?
113/tcp   closed  ident
135/tcp   open    msrpc?
143/tcp   open    imap?
443/tcp   open    https?
8008/tcp  open    http
8010/tcp  open    ssl/http-proxy FortiGate Web Filtering Service
```

### **CUESTIÓN 3: Analizando los puertos de los servidores desde fuera de la red.**

- Ejecutad nmap desde PCC contra los servidores 1 y 2. Guardad o anotad los resultados y haced una **breve explicación(en casa)**.

A través de nmap obtenemos el estado de los puertos y el servicio de cada uno.

#### NMAP PCC 172.16.0.10

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 09:54 Hora
estßndar romance
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:14 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:24 remaining)
Nmap scan report for 172.16.1.10
Host is up (0.0045s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
25/tcp    open  smtp?
80/tcp    open  http?
110/tcp   open  pop3?
113/tcp   closed ident
135/tcp   open  msrpc?
143/tcp   open  imap?
443/tcp   open  https?
8008/tcp  open  http
8010/tcp  open  ssl/http-proxy FortiGate Web Filtering Service
```

#### NMAP PCC 172.16.1.10

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 09:54 Hora
estßndar romance
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:14 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 22.22% done; ETC: 10:05 (0:08:24 remaining)
Nmap scan report for 172.16.1.10
Host is up (0.0045s latency).
Not shown: 990 filtered ports
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp?	
25/tcp	open	smtp?	
80/tcp	open	http?	
110/tcp	open	pop3?	
113/tcp	closed	ident	
135/tcp	open	msrpc?	
143/tcp	open	imap?	
443/tcp	open	https?	
8008/tcp	open	http	
8010/tcp	open	ssl/http-proxy	FortiGate Web Filtering Service

#### **CUESTIÓN 4:** Analizando los puertos de todos los equipos de la red.

Ejecutad el script con

```
./ ScaneaTodo.sh
```

- Anotad los resultados o volcad la salida en un archivo añadiendo al final del comando `>archivo.txt`.
- **Analizad los resultados en casa. Añadid el listado obtenido al informe de prácticas.**

ScaneaTodo.sh realiza un escaneado de todos los puertos de nuestra red como podemos ver en el listado adjunto.

## 5 Analizando tráfico

#### **CUESTIÓN 5:** Analizando el ancho de banda que nos queda.

Vamos a probar el ancho de banda que nos ofrecería de **subida**.

- Abrid un terminal de Windows (botón de inicio, teclead cmd).
- Id al directorio en el que se encuentra iperf tecleando `cd c:/iperf3`
- Ejecutar una instancia del servidor iperf3.
  - o `iperf3 -s`
- Ejecutad un cliente iperf3 tcp contra ese servidor desde PCA o PCB. No olvidéis indicarle el puerto.
  - o `iperf3 -c DIRECCIÓN_IP`
- Realizad la medida varias veces dado que las condiciones de tráfico variarán en función del instante en el que se realiza (tened en cuenta que es posible que otros compañeros también estén generando tráfico, dependiendo de su ritmo de avance en la práctica). Incluso podéis lanzar dos conexiones simultáneas desde PCA y PCB.
- Anotad los resultados.

```
-----
Server listening on 5201
-----
```

```
Accepted connection from 192.168.10.31, port 37228
```

```
[ 5] local 192.168.20.31 port 5201 connected to 192.168.10.31 port 37230
```

[ ID]	Interval		Transfer	Bandwidth
[ 5]	0.00-1.00	sec	105 MBytes	883 Mbits/sec
[ 5]	1.00-2.00	sec	110 MBytes	923 Mbits/sec
[ 5]	2.00-3.00	sec	110 MBytes	919 Mbits/sec
[ 5]	3.00-4.00	sec	109 MBytes	918 Mbits/sec
[ 5]	4.00-5.00	sec	110 MBytes	919 Mbits/sec
[ 5]	5.00-6.00	sec	110 MBytes	920 Mbits/sec
[ 5]	6.00-7.00	sec	110 MBytes	921 Mbits/sec
[ 5]	7.00-8.00	sec	106 MBytes	889 Mbits/sec
[ 5]	8.00-9.00	sec	110 MBytes	919 Mbits/sec
[ 5]	9.00-10.00	sec	109 MBytes	911 Mbits/sec
[ 5]	10.00-10.04	sec	4.29 MBytes	922 Mbits/sec

[ ID]	Interval		Transfer	Bandwidth	Retr	
[ 5]	0.00-10.04	sec	1.07 GBytes	913 Mbits/sec	610	

sender

[ 5]	0.00-10.04	sec	1.07 GBytes	912 Mbits/sec		
------	------------	-----	-------------	---------------	--	--

receiver

```
-----
Server listening on 5201
-----
```

```
-----
Server listening on 5201
-----
```

Vamos a probar ahora el ancho de banda de **bajada (quizás no sea posible, en ese caso, averiguad el motivo)**.

- Ejecutad un servidor iperf3 tcp en PCA o PCB.

```
Server listening on 5201
```

```
Accepted connection from 192.168.5.100, port 47640
```

```
[ 5] local 192.168.5.104 port 5201 connected to 192.168.5.100 port 47642
```

[ ID]	Interval		Transfer	Bandwidth
[ 5]	0.00-1.00	sec	2.14 MBytes	18.0 Mbits/sec
[ 5]	1.00-2.00	sec	2.22 MBytes	18.6 Mbits/sec
[ 5]	2.00-3.00	sec	2.99 MBytes	25.1 Mbits/sec
[ 5]	3.00-4.00	sec	3.77 MBytes	31.7 Mbits/sec
[ 5]	4.00-5.00	sec	5.44 MBytes	45.6 Mbits/sec
[ 5]	5.00-6.00	sec	5.32 MBytes	44.6 Mbits/sec
[ 5]	6.00-7.00	sec	5.39 MBytes	45.2 Mbits/sec
[ 5]	7.00-8.00	sec	5.27 MBytes	44.2 Mbits/sec
[ 5]	8.00-9.00	sec	5.45 MBytes	45.7 Mbits/sec
[ 5]	9.00-10.00	sec	5.41 MBytes	45.4 Mbits/sec
[ 5]	10.00-10.02	sec	127 KBytes	44.1 Mbits/sec

[ ID]	Interval		Transfer	Bandwidth
-------	----------	--	----------	-----------

[ 5]	0.00-10.02	sec	0.00 Bytes	0.00 bits/sec	sender
[ 5]	0.00-10.02	sec	43.5 MBytes	36.4 Mb/s	receiver

- Ejecutad un cliente iperf3 tcp contra ese equipo desde el PCC situado en Internet.

-----  
Server listening on 5201  
-----

Accepted connection from 192.168.5.100, port 56824

[ 5] local 192.168.5.104 port 5201 connected to 192.168.5.100 port 56826

[ ID] Interval Transfer Bandwidth

[ 5] 0.00-1.00 sec 5.38 MBytes 45.1 Mb/s

[ 5] 1.00-2.00 sec 5.25 MBytes 44.0 Mb/s

[ 5] 2.00-3.00 sec 5.12 MBytes 43.0 Mb/s

[ 5] 3.00-4.00 sec 5.25 MBytes 44.0 Mb/s

[ 5] 4.00-5.00 sec 5.25 MBytes 44.0 Mb/s

[ 5] 5.00-6.00 sec 5.50 MBytes 46.2 Mb/s

[ 5] 6.00-7.00 sec 5.38 MBytes 45.1 Mb/s

[ 5] 7.00-8.00 sec 5.38 MBytes 45.1 Mb/s

[ 5] 8.00-9.00 sec 5.50 MBytes 46.2 Mb/s

[ 5] 9.00-10.00 sec 5.50 MBytes 46.1 Mb/s

[ 5] 10.00-10.04 sec 128 KBytes 24.2 Mb/s

-----  
[ ID] Interval Transfer Bandwidth

[ 5] 0.00-10.04 sec 53.6 MBytes 44.8 Mb/s

[ 5] 0.00-10.04 sec 0.00 Bytes 0.00 bits/sec

sender

receiver

**En casa:**

**¿Os parece que los datos son estables en el tiempo (valores similares en todas las medidas)? ¿Creéis que son razonables los valores obtenidos?**

Sí son estables en el tiempo, y también creemos que son razonables los valores obtenidos debido a que al ser TCP el ancho de banda es repartido en un 50% aproximadamente para cliente y servidor.

### **CUESTIÓN 6: Analizando el ancho de banda entre dos equipos de la red.**

**En casa:**

**¿OS parece que los datos son estables en el tiempo (valores similares en todas las medidas)? ¿Creéis que son razonables los valores obtenidos? ¿Hay diferencia entre la medida realizada entre los equipos internos y la realizada con el equipo externo? ¿A qué creéis que es debido?**

Sí, como en el apartado anterior. Podría existir diferencia aunque nosotros no tenemos debido a que no se ha congestionado la red durante nuestra sesión.

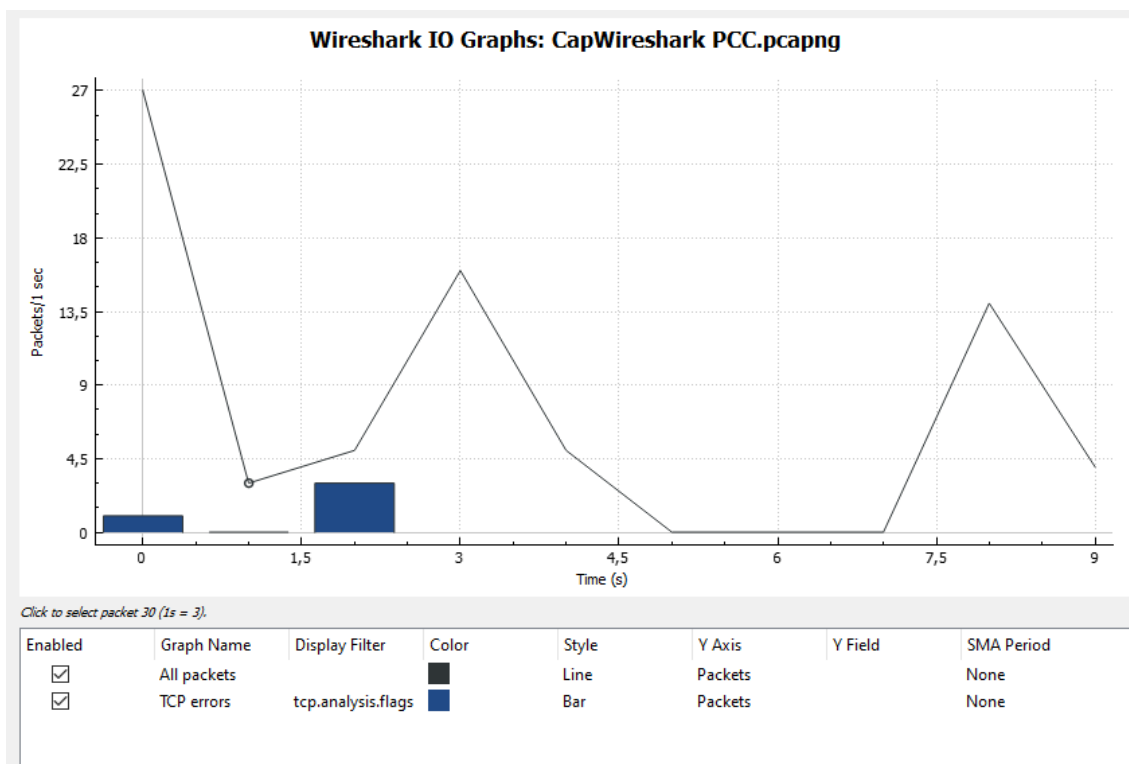
**CUESTIÓN 7:** Estadísticas y gráficas con Wireshark. (SUUUUUIIIIIIIT)

- Detened las capturas de *wireshark* y analizad los resultados:
  - o Id al menú *statistics->Conversations*. Wireshark, mostrará varias pestañas seleccionables con los datos de las “conversaciones” capturadas. Describid brevemente qué tipo de información estáis viendo y para qué creéis que podría ser útil.

La información obtenida muestra la cantidad de paquetes, bytes, el tiempo de inicio de la conversación, la duración y los bits/s que van desde origen -> destino, destino->origen en relación con la pestaña en la que te encuentres siendo la pestaña Ethernet la que te relaciona según las MAC origen y destino, IPv4 las IP origen y destino y TCP y UDP(según el protocolo de transporte escogido) el puerto origen y destino.

Podría ser útil para ver el ancho de banda tanto de transmisión como de recepción (bits/s).

- Id al menú *statistics->IO Graphics*. Wireshark mostrará una gráfica. Guardadla.



## Anexo I

Empleando un editor de texto (puedes emplear *vim* desde consola o alguno con entorno gráfico que proporcione la distribución de Linux empleada como *gedit*) teclead el siguiente código y guárdadlo con el nombre PingComprueba.sh

```
#!/bin/bash

# Programa para comprobar equipos activo

#$1 es el primer argumento, se invocará el programa tecleando

# en una consola ./PingComprueba.sh n

# siendo n el número máximo de equipos a comprobar

for ((i = 1; i <= $1; i++))
do
    echo "probando ping a 192.168.10."$i
    ping -c 2 192.168.10.$i
done
```

Cámbiadle los permisos de archivo para que se pueda ejecutar

```
chmod 755 PingComprueba.sh
```

Se ejecuta tecleando en un terminal

```
./PingComprueba.sh
```