Redes de Computadores

Entregable 2

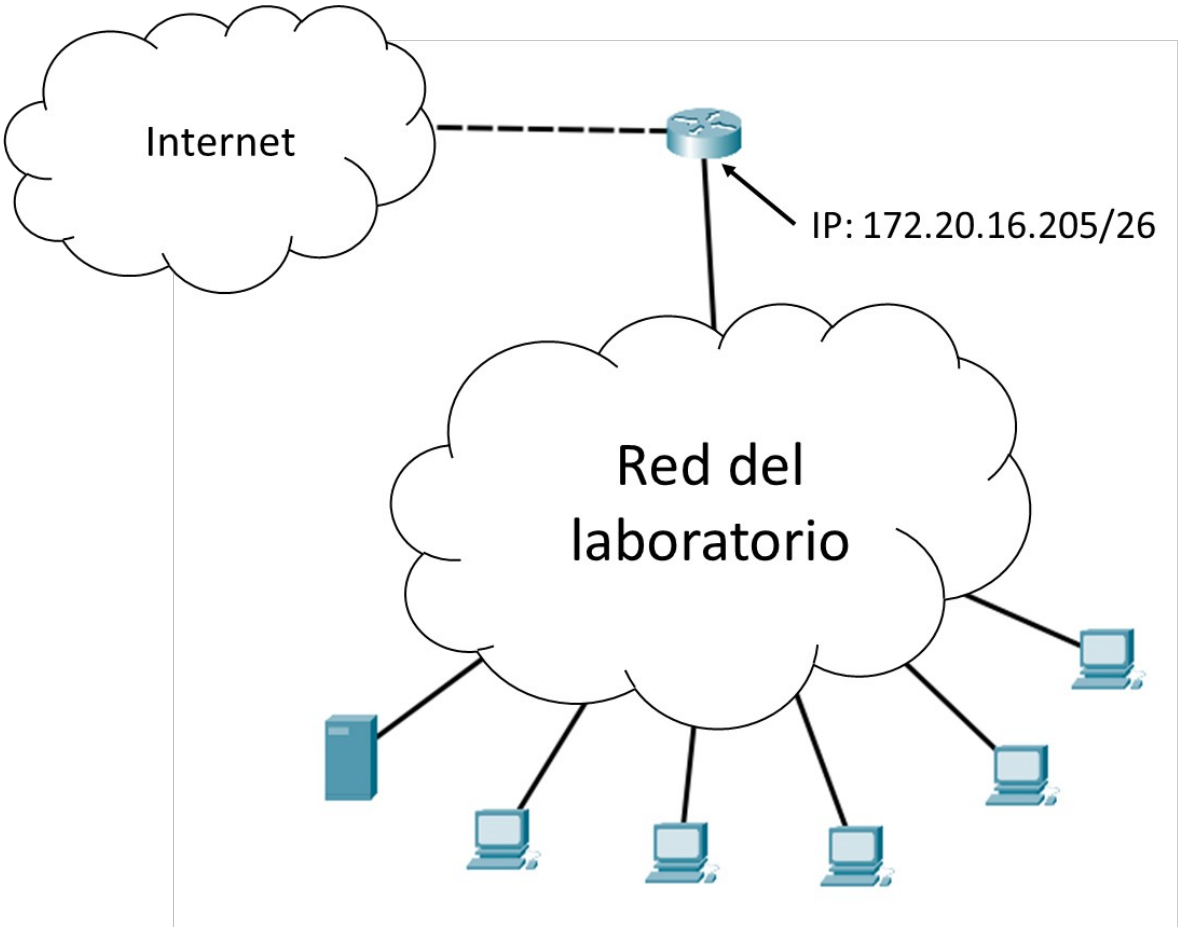
6'15

Nombre: Juan Francisco Mier Montoto

Ejercicio 1 (4 puntos) 1'25

Un grupo de investigación de la universidad está montando su propio laboratorio dentro de la escuela y necesita diseñar el montaje de los equipos que lo compondrán. En dicho laboratorio hay 1 servidor que necesita poder acceder a equipos externos, además de tener acceso a ellos desde el exterior sin habilitar el reenvío de puertos. Se poseen también 5 PCs que necesitan poder comunicarse con el exterior, pero no es necesario que dispongan de una IP pública. Dichos PCs tienen que pertenecer los 5 a la misma subred, pudiendo el servidor formar parte de ella o de una red externa.

Tras hablar con el servicio informático nos comunican que podremos utilizar el rango de direcciones 172.20.16.184-172.20.16.191, además de que está libre la dirección 172.20.16.220, la cual tiene que utilizar obligatoriamente una máscara de 26 bits. La salida a Internet del laboratorio debe realizarse a través del *router* principal de la escuela, el cual posee la dirección 172.20.16.205/26. En la figura que aparece a continuación, se puede ver un esquema simplificado de toda la información obtenida:



Para resolver el problema anterior, será necesario utilizar como apoyo el rango de direcciones reservadas 10.0.0.192/26 y la técnica NAT (*Network Address Translation*) estudiados en la asignatura.

a) **¿Cómo permite NAT ampliar el rango de direcciones posibles? Realiza una breve explicación con las diferentes alternativas que permite NAT para ampliar este rango.** (1 punto) 0'25

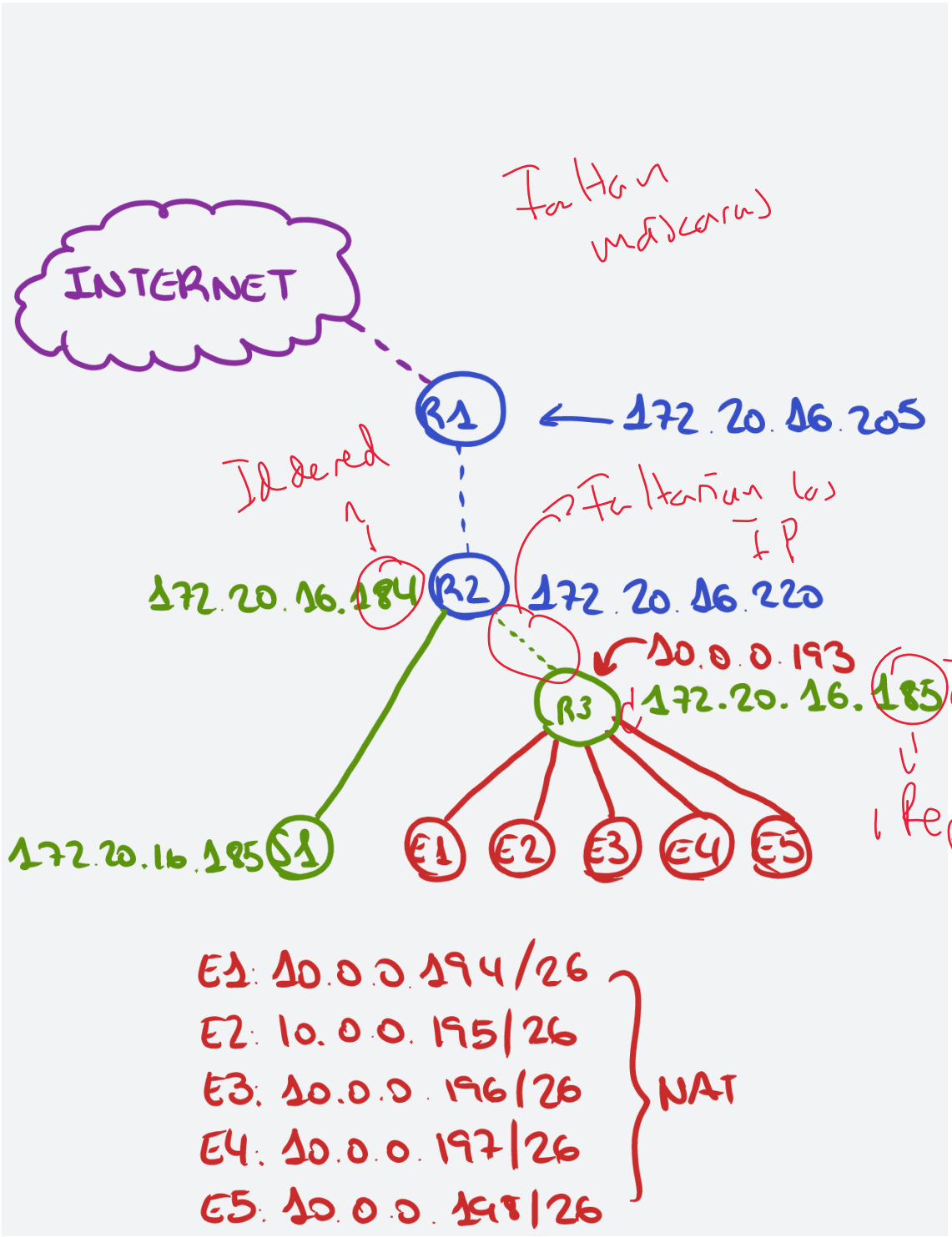
Falta hablar de NAT estát. dinámico ...

NAT permite el acceso de múltiples dispositivos en una red local al exterior a través de una sola dirección IP pública mediante enrutamiento de puertos. NAT funciona gracias a modificaciones en los puertos y las direcciones de origen y destino de los paquetes manejados por el router de la red, que los cambia dependiendo del equipo de origen o de destino respectivamente. Esto permite que todos los paquetes de utilice NAT tengan la dirección de destino del router, en lugar del equipo original. Del mismo modo, al no estar representados por una dirección individual cada equipo, el router reenvía las peticiones pertinentes a cada equipo guiándose por el puerto y modificando cada paquete.

b) **¿Qué equipos (*hubs*, *switchs* o *routers*) serán necesarios para poder realizar una configuración de red que permita cumplir todos los requisitos mencionados al principio del ejercicio? Explica por qué es necesario cada equipo extra a la hora de realizar la configuración y haz un esquema en el que se conecten todos los PCs y servidores a los equipos propuestos, además de asignar las direcciones IPs (utiliza NAT/PAT si es necesario) correspondientes a todas las interfaces utilizadas.** (3 puntos)

Se utilizan dos routers: uno "maestro" que controla toda la red del laboratorio y se comunica con Internet (R2) y otro "esclavo" (R3) que se utiliza como puente NAT para los cinco equipos. De esta manera, el servidor está conectado con el router R2 y tiene conexión directa a Internet sin reenvío de puertos y los equipos tienen direcciones locales que se reenvían a través del router R2 gracias a NAT. De esta manera, se pueden diferenciar cuatro "niveles", representados cada uno en un color diferente en el esquema inferior. Se utilizan solo las IPs asignadas.

1

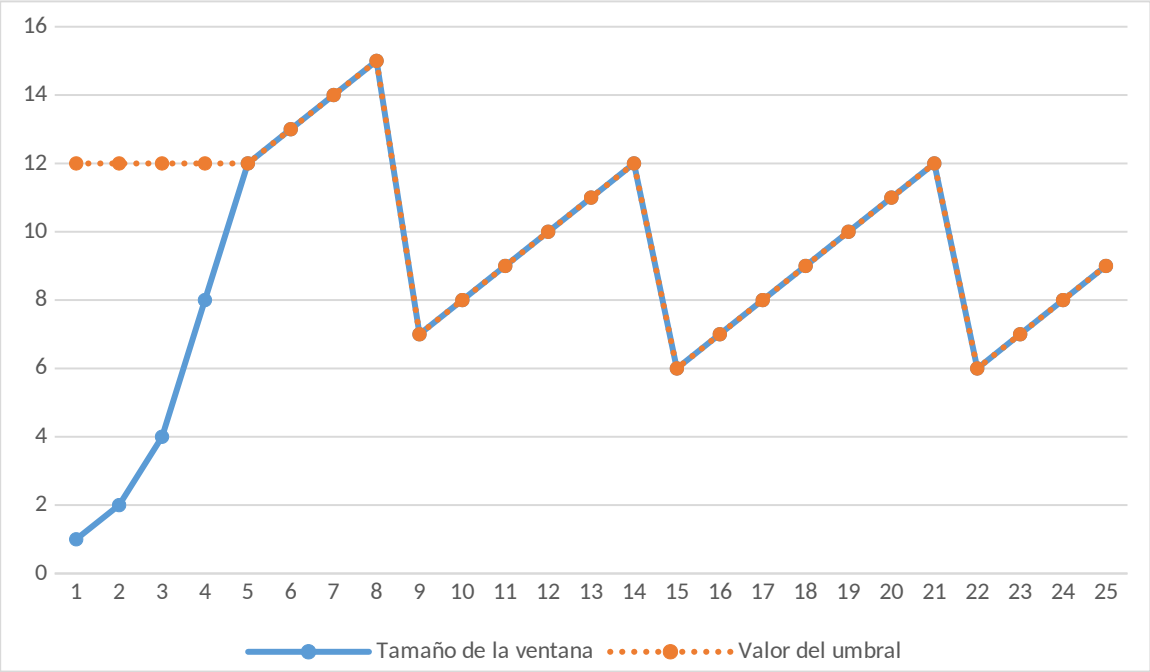

INTERNET
R1
172.20.16.205
Ordered
172.20.16.184
R2
172.20.16.220
10.0.0.193
R3
172.20.16.185
Repetida
172.20.16.185
E1
E2
E3
E4
E5
E1: 10.0.0.194/26
E2: 10.0.0.195/26
E3: 10.0.0.196/26
E4: 10.0.0.197/26
E5: 10.0.0.198/26
NAT

Ejercicio 2 (1 punto)

Tenemos un algoritmo de control de congestión TCP Reno, con un umbral de tamaño de ventana al inicio de 12. Tras el ciclo 8, se reciben 3 ACKs duplicados. Después del ciclo 14 salta un temporizador RTO para reenviar un paquete. Tras el ciclo 19, se reciben de forma consecutiva 2 ACKs repetidos. Por último, tras el ciclo 21, se vuelven a recibir 4 ACKs repetidos.

Dibuje hasta el ciclo 25, la gráfica asociada al tamaño de ventana, e indique cuáles son los diferentes umbrales cuando se produce una pérdida.

Respuesta:



El umbral comienza siendo 12 y luego (debido a que se está utilizando Reno) permanece igual durante el resto del ejercicio. Cada vez que hay un temporizador o al menos tres ACKs repetidos, se parte a la mitad tanto el tamaño de la ventana como el umbral, por lo que nunca va a tener crecimiento exponencial tras el primero.

Ejercicio 3 (2,5 puntos) 1'4

Utilizando Wireshark realiza una captura de cómo tu ordenador obtiene la página web de la Universidad de Valladolid (https://www.uva.es/). Para realizar esta captura es aconsejable tener cerradas todas las aplicaciones que puedan generar tráfico en segundo plano, además de utilizar un navegador diferente al que emplees habitualmente, para evitar que la página se cargue desde la memoria del ordenador en lugar de descargarse de Internet. Dicha captura deberá ser filtrada mediante los comandos adecuados y exportada mediante la instrucción *File/Export Specified Packets…* de tal forma que en ella únicamente quede el tráfico intercambiado entre el ordenador original y la web de la universidad en un archivo de formato *.pcap*. El resultado obtenido deberá ser subido a la entrega habilitada en el campus virtual con el nombre UoXXXXXX_Captura_WUniv.pcap. Además de la captura, será necesario contestar a las cuestiones que se plantean a continuación.

Nota: Si por razones de privacidad no se desea subir la captura *pcap* a la entrega del campus, las respuestas a todas las cuestiones deberán adjuntar capturas de pantalla con la información sensible tapada, pero donde se pueda observar claramente cómo se ha obtenido la respuesta.

a) **La nota de esta cuestión se corresponde a la pregunta además de a la captura completa, ya sea en formato .pcap o subiendo una o varias capturas de pantalla con todos los paquetes ¿Qué filtro has empleado para aislar el tráfico entre la web de la universidad y tu PC?** (0.5 puntos)

La captura no viene filtrada 0'25

Después de obtener la dirección IP del servidor de la universidad con las peticiones DNS, se pueden filtrar las direcciones IP mediante el siguiente filtro: `ip.src == 157.88.25.8 || ip.dst == 157.88.25.8`.

b) **¿Cuál es la dirección IP de la web de la universidad? ¿Y su dirección MAC?** (0.5 puntos)

0'2

Como indicado en la pregunta anterior, la IP de la universidad es “157.88.25.8”. Gracias a la primera petición TCP a la página web, podemos comprobar que la dirección MAC es “52:54:00:12:35:02”.

c) **¿Cuántas conexiones TCP se establecen con la página web de la Universidad? ¿Y cierres de conexión? ¿Por qué lo sabes?** (0.5 puntos)

Después de filtrar todas las peticiones TCP y acceder a las estadísticas generales, se puede observar que hay 3834 peticiones TCP hacia y desde la página web:

Tienes que mirar el bit SYN

Hardware:	AMD Ryzen 9 5900X 12-Core Processor (with SSE4.2)
OS:	Linux 4.15.0-20-generic
Application:	Dumpcap (Wireshark) 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
enp0s8	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	3995	3834 (96.0%)	—
Time span, s	3.253	2.706	—
Average pps	1228.0	1417.1	—

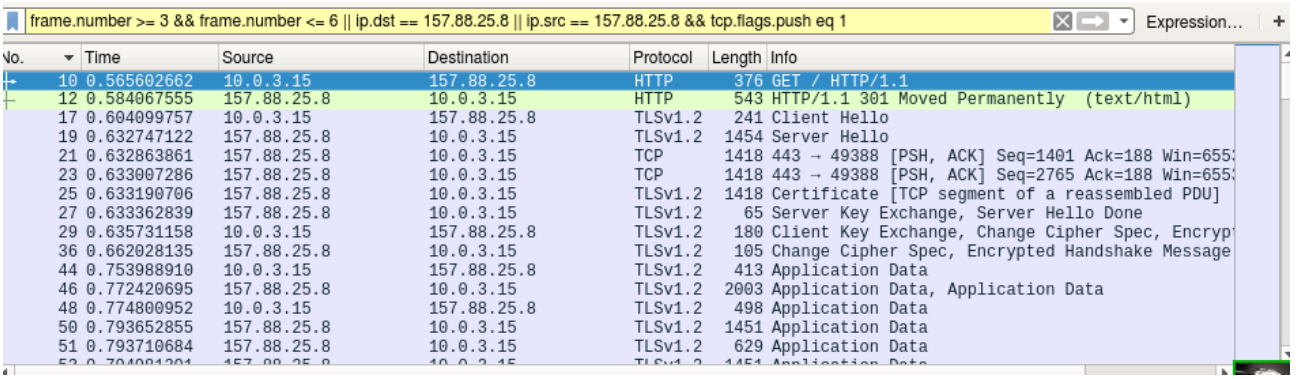
De igual manera, al filtrar por los paquetes TCP que contengan la flag FIN a 1 se pueden observar los paquetes TCP de cierre de conexión (`tcp.flags.fin eq 1`). No se encuentra ningún paquete de este tipo.

d) ¿A qué puerto se realiza la petición para obtener la página web? ¿A qué puerto/s se contesta? (0.5 puntos)

El puerto del servidor de UVA es el puerto 80, puerto estándar en las conexiones a servidores web. En este caso, el puerto local en el que se responden las peticiones es el 54080. Para los paquetes seguros, el puerto es el estándar, 443, mientras que el puerto local es 49388.

e) ¿Hay algún segmento TCP que contenga el bit PUSH a 1? ¿Detectas en la captura alguna característica o patrón común en todos estos mensajes? ¿Por qué crees que puede ocurrir? (0.5 puntos)

Sí, hay varios paquetes TCP con esa flag a 1:



Son paquetes que manda el servidor con datos. Debido a que es bastante información, seguramente se traten de imágenes u otros contenidos multimedia presentes en la página web final.

Ejercicio 4 (2,5 puntos) 2'5

Utiliza Wireshark para realizar capturas de tráfico de diferentes protocolos. Para realizar esta captura es aconsejable tener cerradas todas las aplicaciones que puedan generar tráfico en segundo plano. Dichas capturas deberán ser filtradas mediante los comandos adecuados y exportadas mediante la instrucción *File/Export Specified Packets…* de tal forma que en ellas únicamente quede el tráfico intercambiado entre el ordenador original y el equipo de destino en un archivo de formato *.pcap*. El resultado obtenido deberá ser subido a la entrega habilitada en el campus virtual, con el nombre "Protocolo_*nombreprotocolo*.tcap". Además de la captura, será necesario especificar en el presente documento **cómo se ha hecho para obtener la captura** de cada uno de los protocolos.

Nota: Si por razones de privacidad no se desean subir las capturas *pcap* a la entrega del campus, las respuestas a todas las cuestiones deberán adjuntar capturas de pantalla con la información sensible tapada, pero donde se pueda observar claramente la captura obtenida.

a) Protocolo ARP. **(0.5 puntos)**

✓ Para obtener paquetes ARP se ha enviado un ping entre la máquina virtual con Wireshark y otra máquina virtual de la asignatura con conexión entre sí. De todas formas, se pueden generar estas peticiones al visitar cualquier página por primera vez.

b) Protocolo NTP. **(0.5 puntos)**

Se pueden obtener peticiones NTP al reiniciar la fecha o activar la sincronización con servidores universales de tiempo.

c) Protocolo DHCP. **(0.5 puntos)**

Se pueden obtener peticiones DHCP mediante el comando "dhcpcd5 -N enp0s8", un cliente de DHCP que se puede instalar fácilmente en Linux.

```
redes@Lubuntu:~$ sudo dhcpcd5 -N enp0s8
[sudo] password for redes:
sending commands to master dhcpcd process
redes@Lubuntu:~$ ps awux | grep dhcp
root       652  0.0  0.0   4972  2076 ?        Ss   21:26   0:00 /sbin/dhcpcd
root       799  0.0  0.0  25988  6284 ?        S    21:26   0:00 /sbin/dhclient
```

d) Protocolo DNS. **(0.5 puntos)**

Al igual que con ARP, se pueden obtener este tipo de peticiones de manera muy sencilla, simplemente visitando URLs que no estén ya en alguna caché. En este caso, se han obtenido peticiones utilizando el comando "nslookup".

e) Protocolo de correo electrónico (SMTP, POP3, IMAP…). **(0.5 puntos)**

Se pueden conseguir peticiones de tipo SMTP conectándose mediante TELNET a algún servidor SMTP. En este caso se utiliza gmail con el puerto "587".

```
redes@Lubuntu:~/Escritorio$ telnet smtp.gmail.com 587
Trying 64.233.166.108...
Connected to smtp.gmail.com.
Escape character is '^]'.
220 smtp.gmail.com ESMTP c17-20020a7bc851000000b003b49bd61b19sm9997523wml.15 - g
smtp
```