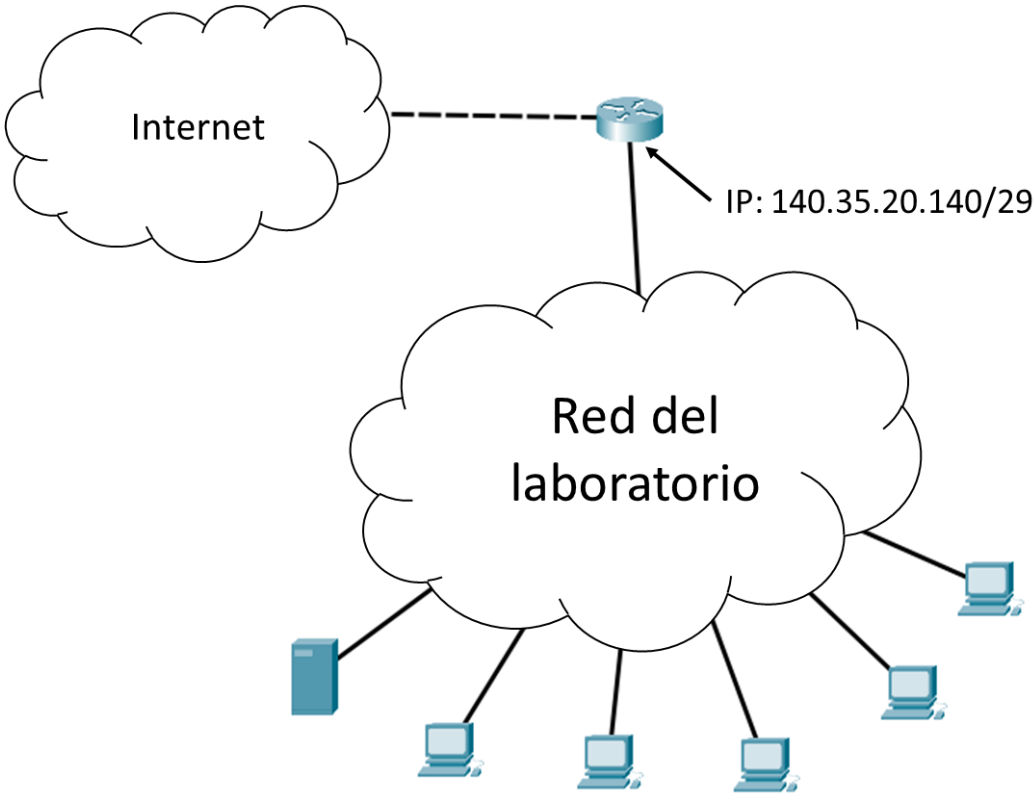
Redes de Computadores
Entregable 2

Nombre: Gustavo Sobrado Aller – UO286277

Ejercicio 1 (3,5 puntos)

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 imprescindible que dispongan de una IP pública. Dichos PCs tienen que pertenecer 2 a la misma subred y los otros 3 a otra subred diferente, pudiendo el servidor formar parte de alguna de ellas o de una red externa.

Tras hablar con el servicio informático nos comunican que se puede utilizar el rango de direcciones públicas 140.35.20.128-140.35.20.135, además de que está libre la dirección 140.35.20.137, pero que solo se puede asignar a un equipo que pertenezca a la red 140.35.20.136/29, la cual ya está asignada a algunos equipos dentro de la escuela. La salida a Internet del laboratorio debe realizarse a través del *router* principal de la escuela, el cual posee la dirección 140.35.20.140/29. 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 192.168.31.144/29 y la técnica NAT/PAT (*Network Address Translation*) estudiada en la asignatura.

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

NAT (Network Address Translation) y PAT (Port Address Translation) son técnicas para superar las limitaciones de direcciones IP públicas en IPv4. Estas técnicas permiten que múltiples dispositivos compartan una o varias direcciones IP públicas para conectarse a Internet.

Hay varias formas de lograr esto:

1. **NAT Estática:**
    - Cada dirección IP privada se mapea a una dirección IP pública específica.
    - Útil para servidores o dispositivos que requieren un acceso constante desde el exterior con una dirección fija.
    - **Ventaja:** Fácil de gestionar para dispositivos con requisitos de acceso fijo.
    - **Desventaja:** No ahorra direcciones públicas.
2. **NAT Dinámica:**
    - Se utiliza un conjunto de direcciones IP públicas (pool) para mapear direcciones IP privadas según sea necesario.
    - Cada dispositivo privado obtiene temporalmente una dirección pública del pool durante una conexión activa.
    - **Ventaja:** Aprovecha mejor las direcciones públicas, ya que solo se asignan mientras haya tráfico activo.
    - **Desventaja:** Puede quedarse sin direcciones públicas si el pool es pequeño.
3. **PAT (NAT con traducción de puertos):**
    - Una única dirección IP pública puede ser utilizada por múltiples dispositivos privados, distinguiendo cada conexión mediante números de puerto.
    - **Ventaja:** Muy eficiente, ya que permite que cientos de dispositivos compartan una sola dirección IP pública.
    - **Desventaja:** Complejidad añadida en la gestión de puertos y posibles limitaciones en aplicaciones que dependan de puertos específicos.

Resumen:

- **NAT Estática:** Relación 1 a 1 (privada a pública).
- **NAT Dinámica:** Relación 1 a N, dependiendo de un pool de direcciones públicas.
- **PAT:** Relación muchos a 1, utilizando puertos para distinguir las conexiones.

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. **(2,5 puntos)**

Se buscará una configuración que cumpla las siguientes condiciones:

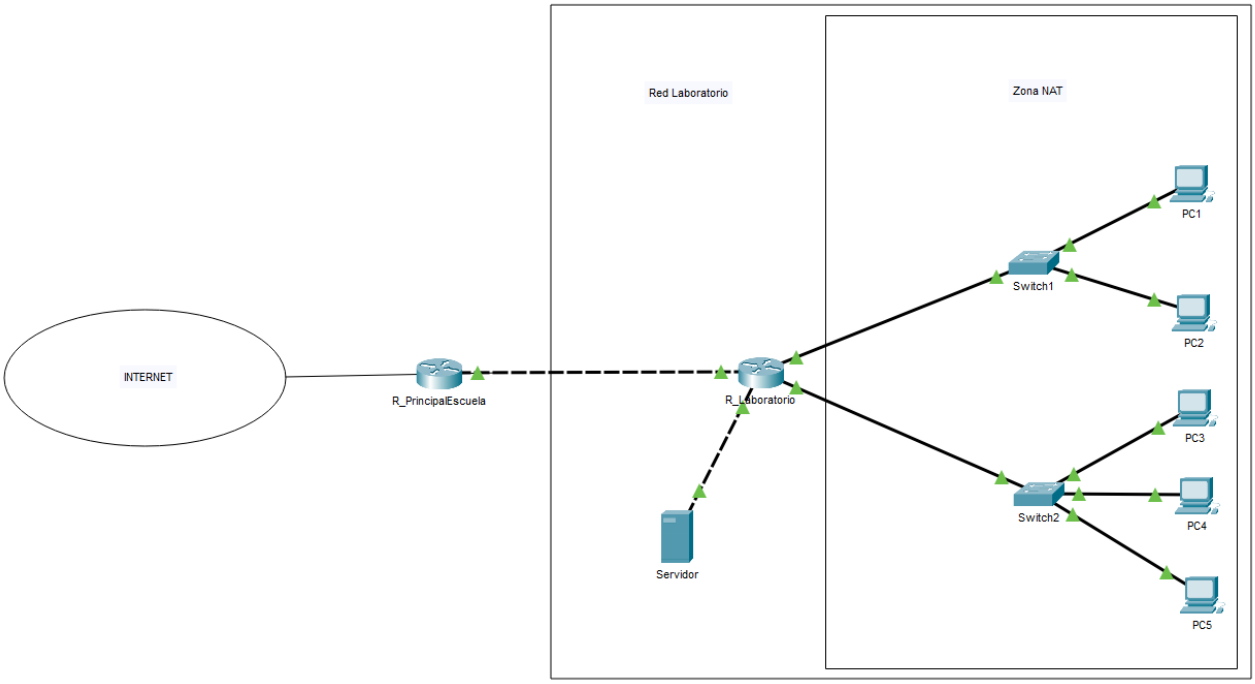
1. Condiciones principales:
   - Servidor: Dirección IP estática y conocida, no afectada por NAT.
   - NAT/PAT: Utilizado para permitir que los PCs accedan a Internet.
   - Direcciones IP permitidas:
     - Públicas: 140.35.20.128 a 140.35.20.135.
     - Privadas: 192.168.31.144/29 (subredes internas).
   - Conexión a Internet: A través del router principal con IP 140.35.20.140/29.
2. División de la red:
   - Servidor: Conectado al router del laboratorio con una IP pública.
   - PCs: Divididos en dos subredes internas gestionadas por NAT.
3. Equipos necesarios:
   - Router del laboratorio: Divide las subredes, implementa NAT y conecta a Internet.
   - Switches (2): Organizan las conexiones para cada subred interna.
   - Servidor: Accesible desde Internet con una IP pública estática.

Dispositivo/Interfaz	Dirección IP	Máscara de Subred	Comentarios
Router principal (Escuela)	140.35.20.140	255.255.255.248 (/29)	Conexión a Internet
Router laboratorio (hacia Escuela)	140.35.20.129	255.255.255.248 (/29)	Conexión al router principal
Router laboratorio (hacia servidor)	140.35.20.130	255.255.255.248 (/29)	Interfaz dedicada al servidor
Router laboratorio (hacia Subred 1)	192.168.31.145	255.255.255.248 (/29)	Gateway para Subred 1
Router laboratorio (hacia Subred 2)	192.168.31.153	255.255.255.248 (/29)	Gateway para Subred 2
Servidor	140.35.20.130	255.255.255.248 (/29)	Dirección estática conocida
PC1 (Subred 1)	192.168.31.146	255.255.255.248 (/29)	
PC2 (Subred 1)	192.168.31.147	255.255.255.248 (/29)	

Dispositivo/Interfaz	Dirección IP	Máscara de Subred	Comentarios
PC3 (Subred 2)	192.168.31.154	255.255.255.248 (/29)	
PC4 (Subred 2)	192.168.31.155	255.255.255.248 (/29)	
PC5 (Subred 2)	192.168.31.156	255.255.255.248 (/29)	

- Subred 1: Utiliza el rango 192.168.31.144/29 para dos PCs conectados al Switch 1.
- Subred 2: Utiliza el rango 192.168.31.152/29 para tres PCs conectados al Switch 2.
- Servidor: Tiene una IP pública estática (140.35.20.130) accesible desde Internet.
- NAT/PAT: Implementado en el router laboratorio para las subredes privadas.

A continuación se presenta un esquema en Cisco Packet Tracer de como seria el esquema:



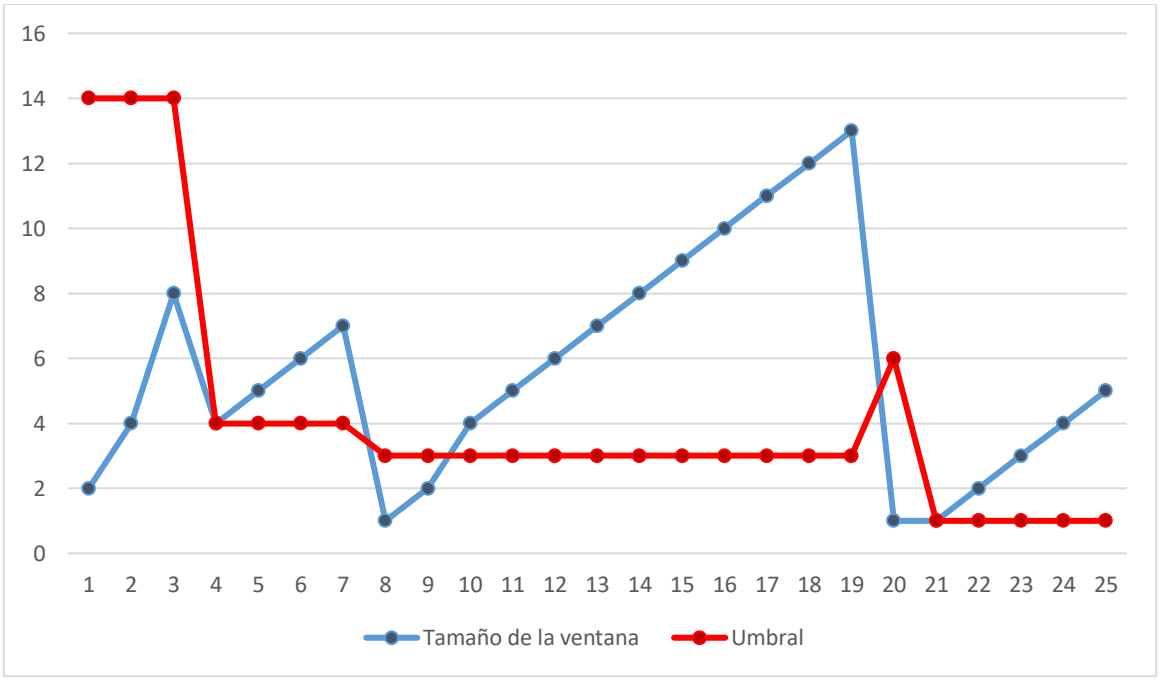
Ejercicio 2 (1 punto)

Se tiene un algoritmo de control de congestión TCP Tahoe, con un umbral de tamaño de ventana al inicio de 14. Tras el ciclo 4, se reciben 5 ACKs duplicados. Después del ciclo 8 salta un temporizador RTO para reenviar un paquete. Tras el ciclo 9, se reciben de forma consecutiva 2 ACKs repetidos. Por último, tras el ciclo 20, salta un temporizador RTO y en el ciclo 21 se reciben 3 ACKs duplicados.

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

Nota: Puedes editar la gráfica inferior en Word con botón derecho -> modificar datos, o generar tu propia gráfica con un gestor de hojas de cálculo tipo Excel y pegar la gráfica aquí.

Respuesta:

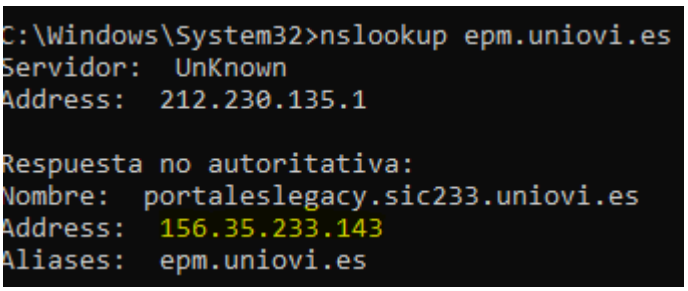


El umbral comienza siendo 14. Cada vez que hay un temporizador RTO o al menos tres ACKs duplicados, el umbral se divide por la mitad del tamaño actual de la ventana. Después de cada pérdida, el tamaño de la ventana se reinicia a 1 y vuelve a crecer de manera exponencial hasta alcanzar el umbral, pasando luego a un crecimiento lineal.

Ejercicio 3 (3 puntos)

Utilizando Wireshark realiza una captura de cómo tu ordenador obtiene la página web de la Escuela Politécnica de Mieres (https://epm.uniovi.es/). 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.

a) La nota de esta cuestión se corresponde a la captura completa y a la siguiente pregunta: ¿Qué filtro has empleado para aislar el tráfico entre la web de la universidad y tu PC? ¿Cuál es tu dirección IP y tu MAC? **(0,75 puntos)**



Después de obtener la dirección IP del servidor de la universidad con un simple nslookup (se podría hacer con peticiones DNS pero eso generaría más tráfico y habría que buscarlo a ojo), se pueden filtrar las direcciones IP mediante:

$$\text{ip.src} == 156.35.233.143 \;||\; \text{ip.dst} == 156.35.233.143$$

Mi dirección IP es 192.168.1.130 y mi dirección MAC es 2c:f0:5d:89:45:58

b) ¿Cuál es la dirección IP de la web de la universidad? ¿Y su dirección MAC? **(0,25 puntos)**

Como he respondido antes, la IP de la web de universidad es 156.35.233.143. La dirección MAC del servidor de la página no se observa directamente, ya que el tráfico pasa a través de enrutadores u otros dispositivos y no se conecta directamente a mi PC. No se puede capturar directamente a menos que esté en la misma red local que el servidor (lo cual no aplica aquí). Sólo puedo identificar su dirección IP.

c) ¿Cuántas conexiones TCP se establecen con la página web de la Universidad? ¿Y cierres de conexión? ¿Qué parámetros tienes que consultar para responder a lo anterior? En caso de no haber ninguna conexión, ¿a qué se debe? **(0,75 puntos)**

- Filtro para conexiones TCP abiertas:
  - Filtra los paquetes SYN para identificar el inicio de las conexiones TCP:

$$tcp.flags.syn == 1$$

Se establece 1 conexión TCP única con la página web de la Universidad. Esta conexión se identificó agrupando por las combinaciones únicas de dirección de origen, dirección de destino y puerto de destino.

- Filtro para cierres de conexiones TCP:
    - Busca paquetes con banderas FIN para identificar cierres:

$$tcp.flags.fin == 1$$

No hay ningún cierre de conexión, muchas aplicaciones y servicios web (como HTTPS) mantienen conexiones abiertas utilizando la técnica Keep-Alive, lo que evita cerrar las conexiones inmediatamente después de completar una transferencia de datos.

d) ¿A qué puerto se realiza la petición para obtener la página web? ¿A qué puerto/s se contesta? **(0,25 puntos)**

La petición para obtener la página web de la universidad se realiza al puerto 443, que es el puerto estándar para conexiones HTTPS. El servidor responde a los puertos efímeros asignados dinámicamente por mi equipo. En este caso, los puertos utilizados por mi equipo como origen son 50492, 50493, 50494, 50495, 50496, y 50497, cada uno correspondiente a una conexión TCP única.

e) Indica el número de mensaje que le asigna *Wireshark* a los últimos 4 paquetes que contengan tráfico *http* o *https* en la captura. ¿Cuál es el tamaño en el nivel de aplicación de dichos mensajes? ¿Coincide con el tamaño que muestra *Wireshark*? **(0,5 puntos)**

En la captura de tráfico, los últimos 4 paquetes que contienen tráfico HTTPS corresponden a los números **7020**, **7021**, **7023**, y **7026** según el orden asignado por Wireshark. El tamaño total de estos paquetes, mostrado en la columna **Length**, es de **1499 bytes**, **1467 bytes**, **1355 bytes**, y **199 bytes**, respectivamente. Este tamaño incluye todas las capas del paquete, desde la física hasta la de aplicación. En el caso de HTTPS, los datos están cifrados, por lo que el tamaño en el nivel de aplicación no puede determinarse directamente sin descifrar el contenido. Sin embargo, el tamaño total mostrado en Wireshark coincide con los datos observados para la transferencia en la capa de transporte (TLS). Esto indica que los paquetes contienen datos de aplicación encapsulados dentro del protocolo TLS.

f) ¿Parte o reensambla el protocolo de transporte los mensajes que recibe del nivel de aplicación? Señala algún mensaje de ejemplo si lo hace e indica por qué lo sabes. **(0,5 puntos)**

El protocolo de transporte (TCP) parte los mensajes grandes del nivel de aplicación en segmentos más pequeños, y los reensambla en el destino. En esta captura, podemos observar ejemplos como los paquetes consecutivos 7020 y 7021, que forman parte de un mensaje HTTPS más grande. Esto se deduce porque el tamaño de los paquetes coincide con el MSS, y Wireshark marca el reensamblaje cuando ocurre.

Ejercicio 4 (2,5 puntos)

Utiliza Wireshark para realizar capturas de tráfico de los protocolos indicados a continuación. El resultado obtenido deberá ser subido a la entrega habilitada en el campus virtual, con el nombre "Protocolo_*nombreprotocolo*.pcap". Además de la captura, será necesario especificar en el presente documento **qué tráfico has generado con tu equipo para obtener la captura** de cada uno de los protocolos.

a) Protocolo ARP. **(0,5 puntos)**

Abro una terminal en Windows y realizo una conexión a una dirección IP de la red local, en este caso a mi móvil conectado por WIFI:

$$ping\ 192.168.1.133$$

Se genera tráfico de solicitudes ARP (Who has...) y respuestas ARP (is at...).

b) Protocolo NTP. **(0,5 puntos)**

En Windows para generar tráfico NTP basta con activar y desactivar la sincronización de hora con un servidor NTP desde la configuración de Fecha y Hora.

Se genera tráfico de solicitudes de sincronización de hora y respuestas de servidores NTP.

c) Protocolo DHCP. **(0,5 puntos)**

Para generar este tipo de tráfico, basta con desconectarse y volver a conectarse a la red para cambiar la dirección IP de nuestro dispositivo y así solicitar la asignación de una nueva IP. También puede hacerse con estos comandos:

$$ipconfig\ /release$$

$$ipconfig\ /renew$$

Se genera tráfico de peticiones DHCP (DHCP Release, DHCP Discover, DHCP Request) y respuestas del servidor (DHCP Offer, DHCP ACK).

d) Protocolo DNS. **(0,5 puntos)**

La forma más sencilla de generar este tipo de tráfico es resolviendo dominios con la herramienta nslookup, la cual utilizamos anteriormente.

Podemos resolver un dominio cualquiera desde la terminal:

$$nslookup\ google.com$$

Se genera tráfico de consultas DNS (Standard query) y respuestas (Standard query response).

e) Protocolo ICMP **(0,5 puntos)**

Para este protocolo podemos realizar un ping a cualquier dirección IP, por ejemplo:

$$ping\ 8.8.8.8$$

La dirección 8.8.8.8 corresponde a uno de los servidores DNS públicos de Google.

Se genera tráfico de solicitudes de eco (Echo request) y respuestas de eco (Echo reply).