

Redes de Computadores

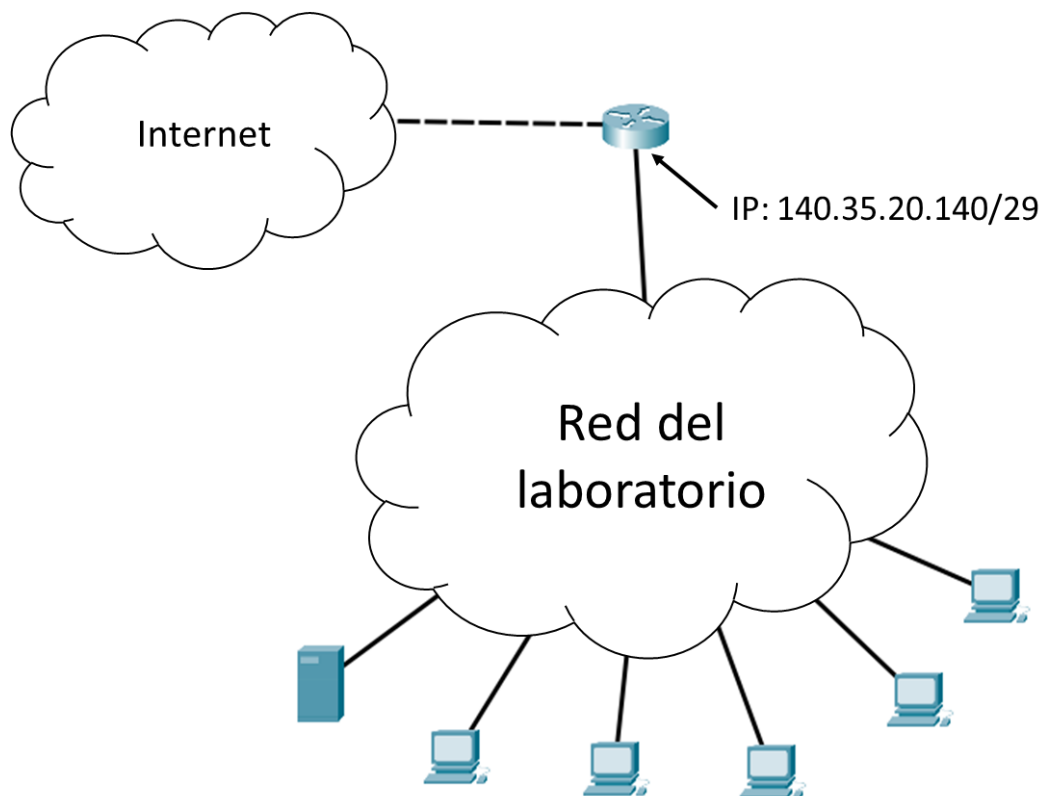
Entregable 2

Nombre: Pelayo Iglesias Manzano

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.

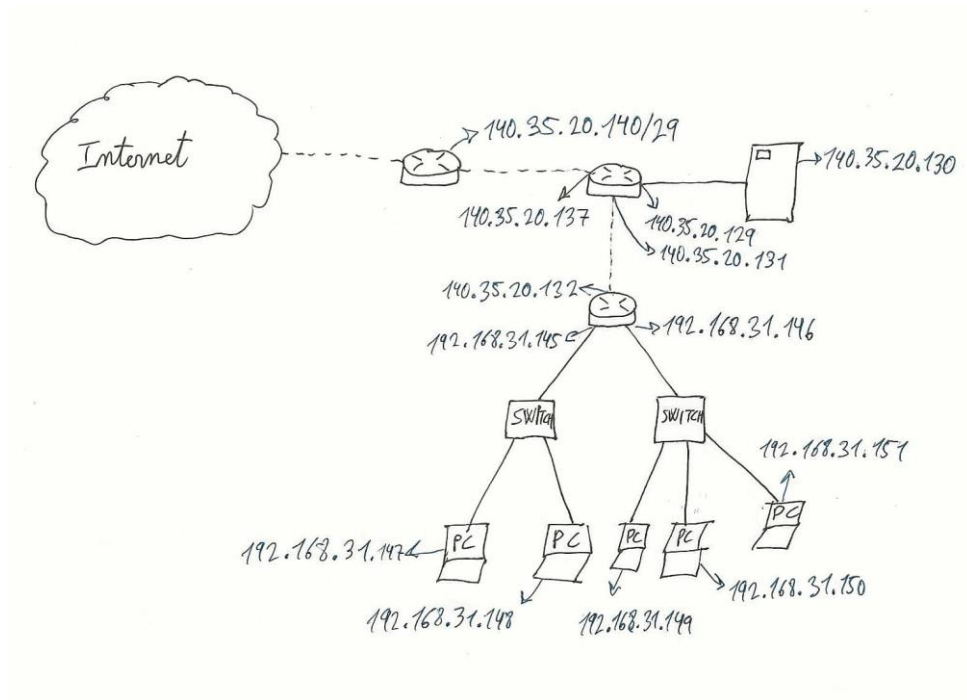
- a) ¿Cómo permite NAT/PAT ampliar el rango de direcciones posibles? Realiza una breve explicación con las diferentes alternativas que permite ampliar este rango. **(1 punto)**

La técnica NAT/PAT permite ampliar el rango de direcciones posibles haciendo que múltiples dispositivos en una red privada compartan una sola dirección IP pública. Para esto se pueden utilizar:

- **NAT estático:** se asigna una dirección IP pública a una dirección IP privada única de manera estática y permanente, lo que permite asociar una a una las direcciones IP públicas y privadas.
- **NAT dinámico:** utiliza un grupo de direcciones IP públicas disponibles. Cuando un dispositivo con IP privada solicite el acceso a Internet, se le asigna de forma dinámica una dirección IP pública disponible dentro del rango.
- **PAT:** traduce las direcciones IP y los números de puerto asociados con las direcciones IP. Cada dispositivo de una red privada tiene una dirección IP pública, pero se diferencian por los números de puerto únicos asociados a cada conexión.

- 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)**

Añadiremos 2 routers y 2 switches para poder realizar la configuración. Un router servirá para comunicar los 2 switches que conectan los PCs de cada subred. Para la primera subred tendremos 2 PCs y para la segunda 3 PCs. Otro router tendrá conectado el servidor y conectará el router nombrado anteriormente con el principal.



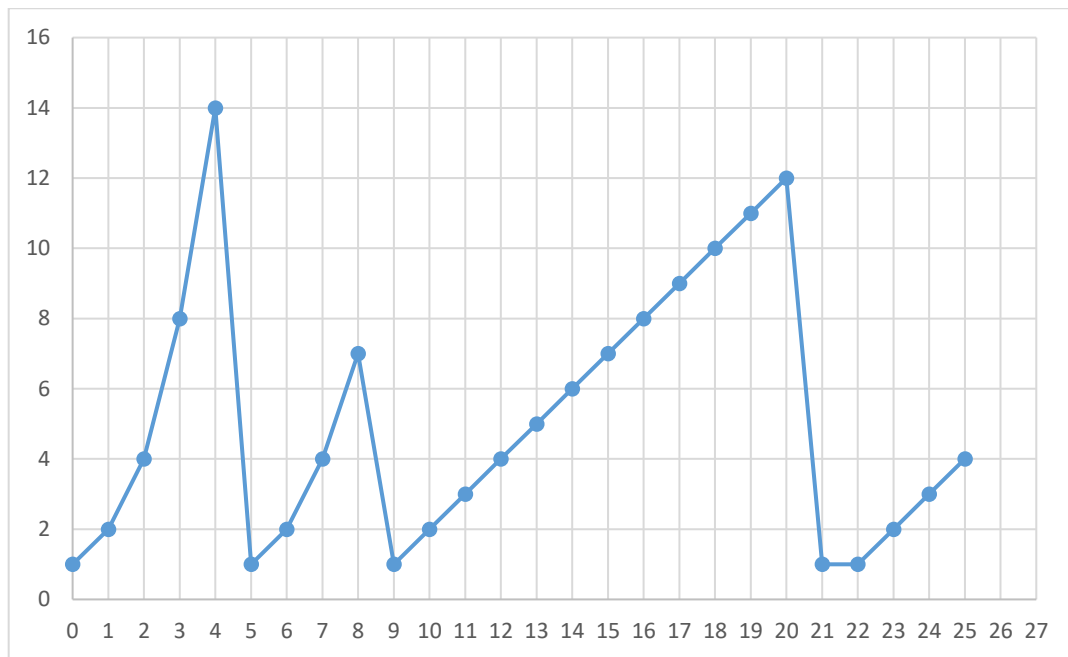
Ejercicio 2 (1 punto)

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:



Después de la primera pérdida, el umbral pasa de 14 a 7. Tras la segunda, pasa de 7 a 3. En la tercera pasa de 12 a 6. Por último, pasa de 6 a 3 nuevamente.

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)**

Filtro: (ip.src == 156.35.233.143 && ip.dst == 192.168.1.14) || (ip.src == 192.168.1.14 && ip.dst == 156.35.233.143). Mi dirección IP es 192.168.1.14 y mi MAC es a8:b1:3b:73:f8:b5.

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

La dirección IP de la web de la universidad es 156.35.233.143 y sólo sabemos la MAC del router, no de la universidad.

- 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)**

Para saber cuántas conexiones TCP se establecen con la página web de la Universidad he usado este filtro: tcp.flags.syn == 1 && ip.dst == 156.35.233.143, y el resultado ha sido 2. Para saber los cierres de conexión: tcp.flags.fin == 1 && ip.dst == 156.35.233.143, y ha habido 0. Se consultan los parámetros SYN y FIN, respectivamente.

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

Petición al puerto 443 y contestación al 60972.

- 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)**

- 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 TCP parte los mensajes en segmentos antes de enviarlos y los reensambla otra vez cuando llegan al receptor.

Con el filtro: tcp.segment, podemos ver los mensajes partidos y reensamblados. Si pulsamos sobre cada mensaje nos indica los segmentos reensamblados.

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)**

He realizado un ping a otro dispositivo de mi red local.

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

He sincronizado manualmente la hora en mi ordenador.

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

He renovado la dirección IP de la interfaz con: ipconfig/renew.

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

He consultado el dominio www.google.es con el comando nslookup.

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

He realizado un ping a un dominio, en este caso Google, con la IP pública 8.8.8.8.