24 de noviembre de 2022

Redes de Datos 1

2º parcial – 2022

Solución

Esta es una posible solución a las preguntas planteadas. ***Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta****.*

Pregunta 1 (10 puntos)

Notas generales:

i. En la figura se indica la dirección IP asignada a cada interfaz de cada equipo.
ii. Sobre cada red se especifica el rango de direcciones correspondiente a esa red.
iii. Asuma que los nombres de las interfaces son de la forma **ethX** donde **X** es el último octeto de la dirección IP de la interfaz. Ej: Si la IP de una interfaz es 10.0.0.**5**, el nombre de la interfaz es **eth5**.
iv. Use el nombre de la interfaz como próximo salto para las redes directamente conectadas.
v. Ninguno de los enrutadores tiene disponible la funcionalidad de NAT/PAT.

a) En la red IP esquematizada en la figura 1 se desea que el tráfico originado en PCa y destinado a las direcciones de la LAN2 pase por el enlace R1-R2, pero que el tráfico originado en PCa y destinado a PCb siga el camino R1-R3-R2.
Escriba las entradas requeridas en las tablas de forwarding de los equipos involucrados para lograrlo. Justifique su respuesta.

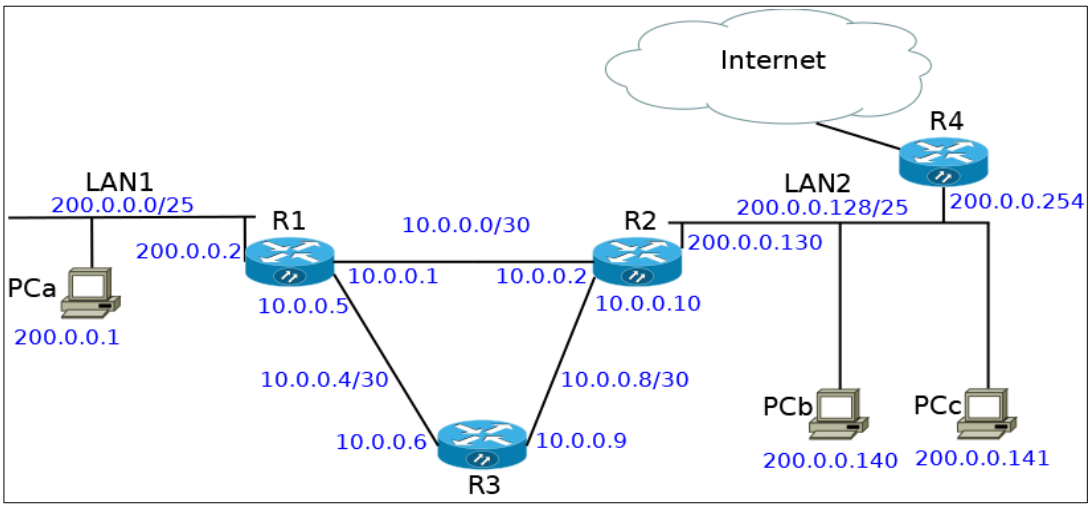

Figura 1

Para que el tráfico pueda transitar desde un origen a un destino, es necesario que en todos los equipos involucrados (origen y enrutadores intermedios) exista una entrada en la tabla de forwarding para alcanzar al destino.
Las tablas de forwarding contendrán dos columnas. La primera contendrá rangos de direcciones destino especificados por su número de red y su máscara, y en la segunda columna se indicará el próximo salto para ese destino.
En base al algoritmo de búsqueda en la tabla de forwarding (longest prefix match), para saber cuál es el mejor próximo salto para una IPx, se recorrerán las entradas de la tabla comenzando por las entradas de largo de máscara mayor (rangos de direcciones más pequeños y por tanto más específicos), siguiendo luego por los rangos de largo de máscara menor (rangos de direcciones más grandes y por tanto más genéricos). Para cada entrada se comparará el resultado de realizar un AND bit a bit entre la dirección a la que se quiere llegar (IPx) y la máscara de la entrada en cuestión. El resultado se comparará con la dirección de red del rango de esa entrada. Si hay una coincidencia (la IPx está incluida en el rango indicado en esa entrada) entonces se encamina el paquete hacia el próximo salto indicado en la tabla y se finaliza la búsqueda. Si no hay coincidencia se continúa el procedimiento con la siguiente entrada de la tabla. Si se llega al final de la tabla, se descarta el paquete y se envía un mensaje ICMP del tipo "network

unreacheable" al originador del paquete que se estaba tratando de caminar (dirección IP de origen del paquete).
Puede existir una ruta por defecto que es válida para cualquier dirección y que se utilizará en caso que ninguna de las entradas de la tabla sirvan para llegar a ese destino. Esta entrada se identifica como 0.0.0.0/0 (número de red 0 y largo de máscara 0), ya que si se aplica el AND bit a bit con una máscara de largo 0 (la máscara tiene cero 1s o sea consiste de 32 bits en 0) a cualquier dirección IP, el resultado será 0 y coincidirá por tanto con el número de red de esa entrada (0.0.0.0).
Otra consideración general es que al configurar una interfaz de cualquier equipo, se debe indicar la dirección IP y la máscara de la interfaz. Con esta información el equipo sabrá qué rango de direcciones tiene directamente conectadas (son alcanzables recurriendo a los servicios de capa 2 sin necesidad de pasar por un enrutador) en esa interfaz y cuál es su propia dirección. Como se indicó en la nota iv) utilizaremos el nombre de la interfaz para poner como próximo salto para las redes directamente conectadas a cada equipo.
Para cumplir los requerimientos solicitados, se pueden poner entradas generales (incluso entradas por defecto) en algunos equipos y entradas más específicas que se evaluarán antes. Una solución posible sería:

Tabla de PCa		***Comentario***
Destino	***Próximo salto***	
200.0.0.0/25	*eth1*	*Red directamente conectada en la interfaz eth1*
0.0.0.0/0	*200.0.0.2*	*PCa no tiene otras opciones de salida, por lo que puede agregarse una ruta por defecto para llegar a destinos fuera de su red a través de R1.* *También para esta parte podría agregarse una red a la red 200.0.0.128/25 (todas las direcciones de LAN2), utilizando el mismo próximo salto.*

Tabla de R1		***Comentario***
Destino	***Próximo salto***	
200.0.0.140/32	*10.0.0.6*	*Ruta específica para llegar a PCb por el camino R1-R3-R2* *Un rango /32 representa una sola IP y aparecerá el principio de la tabla, por lo que será el camino a usar cuando el destino sea la IP de PCb.*
10.0.0.0/30	*eth1*	*Red directamente conectada en la interfaz eth1*
10.0.0.4/30	*eth5*	*Red directamente conectada en la interfaz eth5*
200.0.0.0/25	*eth2*	*Red directamente conectada en la interfaz eth2*
0.0.0.0/0	*10.0.0.2*	*Para todo el resto del tráfico se usa el camino R1-R2. Esta entrada incluye obviamente el rango de LAN2.* *También para esta parte podría agregarse una red a la red 200.0.0.128/25 (todas las direcciones de LAN2), utilizando el mismo próximo salto.*

Tabla de R3		***Comentario***
Destino	***Próximo salto***	
10.0.0.4/30	*eth6*	*Red directamente conectada en la interfaz eth6*
10.0.0.8/30	*eth9*	*Red directamente conectada en la interfaz eth9*
0.0.0.0/0	*10.0.0.10*	*Para todo el resto del tráfico se envía a R2.* *Esta entrada incluye obviamente el rango de LAN2.* *También para esta parte podría agregarse una red a la red 200.0.0.128/25 (todas las direcciones de LAN2), utilizando el mismo próximo salto .*

Tabla de R2		***Comentario***
Destino	***Próximo salto***	
10.0.0.0/30	*eth2*	*Red directamente conectada en la interfaz eth2*
10.0.0.8/30	*eth10*	*Red directamente conectada en la interfaz eth10*
200.0.0.128/25	*eth130*	*Red directamente conectada en la interfaz eth130*
		Para esta parte no se requiere ninguna ruta adicional.

Con esta configuración de tablas, un paquete originado en PCa y destinado a PCb recorrería el camino R1-R3-R2 (en R1 se envía hacia R3), mientras que un paquete destinado a cualquier otra IP del rango de LAN2, recorrería el camino R1-R2.

Nota: *Rutas de vuelta de PCb a PCa se resolverán en las siguientes partes.*

b) Agregue las entradas requeridas en las tablas de forwarding de los equipos involucrados para que el tráfico originado en los equipos de la LAN2 llegue a PCa.
Teniendo en cuenta solamente lo visto en el curso, ¿es posible forzar los mismos caminos que en la parte a) para el tráfico originado en PCb y PCc y destinado a PCa?. Justifique su respuesta.

De acuerdo a lo visto en el curso,[1] los paquetes se encaminan en base a la dirección IP de destino por lo que cualquier paquete destinado a PCa seguirá el camino que se determine, independientemente de la IP de origen del mismo.
Para que el tráfico de vuelta desde equipos de LAN2 a LAN1 (en particular PCa) pueda encaminarse, se requieren entradas en las tablas de los equipos de LAN2 (en particular PCb y PCc para esta parte) y en los enrutadores involucrados en el camino. Usaremos el camino R2-R1 para el tráfico de vuelta hacia PCa.

Las tablas quedarían entonces:

Tabla de PCb		***Comentario***
Destino	***Próximo salto***	
200.0.0.128/25	*eth140*	*Red directamente conectada en la interfaz eth140*
200.0.0.0/25	*200.0.0.130*	*Ruta hacia la LAN1 a través de R2.* *Para esta parte sería válido agregar una ruta por defecto a R2, pero habría que modificarla para la siguiente parte.*

Tabla de PCc		***Comentario***
Destino	***Próximo salto***	
200.0.0.128/25	*eth141*	*Red directamente conectada en la interfaz eth141*
200.0.0.0/25	*200.0.0.130*	*Ruta hacia la LAN1 a través de R2.* *Para esta parte sería válido agregar una ruta por defecto a R2, pero habría que modificarla para la siguiente parte.*

1 *Los enrutadores comerciales o equipos linux funcionando como enrutadores, pueden implementar funcionalidades extra que permiten realizar encaminamiento diferenciado de los paquetes, agregando otras consideraciones adicionales al encaminamiento típico basado solamente en la IP de destino. Básicamente se implementa teniendo varias tablas de forwarding en el enrutador y eligiendo cuál de ellas se debe consultar. La elección de la tabla a consultar se puede hacer por diferentes criterios, uno de los cuales puede ser la dirección de origen de los paquetes. Con un mecanismo de este estilo, se podría decidir en R2 que si el origen del paquete es la IP de PCb se consulte la tabla de forwarding A en la cual el próximo salto hacia PCa es R3 y si el origen del paquete es la IP de PCc, se consulta la tabla de forwarding B donde el próximo salto para PCa es R1. Esto no fue visto en el curso y por tanto no se esperaba como respuesta.*

Tabla de R2		***Comentario***
Destino	***Próximo salto***	
10.0.0.0/30	*eth2*	*Red directamente conectada en la interfaz eth2 (parte a)*
10.0.0.8/30	*eth10*	*Red directamente conectada en la interfaz eth10 (parte a)*
200.0.0.128/25	*eth130*	*Red directamente conectada en la interfaz eth130 (parte a)*
200.0.0.0/25	*10.0.0.1*	*Se requiere que R2 sepa cómo llegar a LAN1.*

No se requiere agregar nada en la tabla de R3 porque decidimos usar el camino R1-R2 para el tráfico de vuelta.

c) Para posibilitar la conexión de la red a Internet se contrata un nuevo enlace con un proveedor. Para implementarlo, el proveedor entrega el enrutador R4 configurado correctamente y, de acuerdo a los datos que Ud. le proporcionó, configura la interfaz que se conectará a la LAN2 con la dirección IP 200.0.0.254 (y máscara /25). El proveedor desconoce la topología interna de la red.
Manteniendo las entradas en las tablas de forwarding de las partes a) y b), agregue las entradas necesarias en los equipos involucrados para posibilitar el tráfico bidireccional de los equipos PCa, PCb y PCc a Internet. Justifique su respuesta.

Para llegar a Internet se requieren rutas por defecto, de modo que se puedan encaminar paquetes hacia cualquier dirección destino. Además se requerirán rutas para los paquetes de vuelta.
Con la solución propuesta, PCa, R1 y R3 ya tienen rutas por defecto (R3 no se estaría usando para encaminar tráfico desde o hacia internet).
Resta agregar entradas en R2, PCb y PCc, por lo que las nuevas tablas de esos equipos quedarían:

Tabla de PCb		***Comentario***
Destino	***Próximo salto***	
200.0.0.128/25	*eth140*	*Red directamente conectada en la interfaz eth140 (parte b)*
200.0.0.0/25	*200.0.0.130*	*Ruta hacia la LAN1 a través de R2 (parte b)*
0.0.0.0/0	*200.0.0.254*	*Ruta por defecto a R4.*

Tabla de PCc		***Comentario***
Destino	***Próximo salto***	
200.0.0.128/25	*eth141*	*Red directamente conectada en la interfaz eth141 (parte b)*
200.0.0.0/25	*200.0.0.130*	*Ruta hacia la LAN1 a través de R2. (parte b)*
0.0.0.0/0	*200.0.0.254*	*Ruta por defecto a R4.*

Tabla de R2		***Comentario***
Destino	***Próximo salto***	
10.0.0.0/30	*eth2*	*Red directamente conectada en la interfaz eth2 (parte a)*
10.0.0.8/30	*eth10*	*Red directamente conectada en la interfaz eth10 (parte a)*
200.0.0.128/25	*eth130*	*Red directamente conectada en la interfaz eth130 (parte a)*
200.0.0.0/25	*10.0.0.1*	*Se requiere que R2 sepa cómo llegar a LAN1. (parte b)*
0.0.0.0/0	*200.0.0.254*	*Ruta por defecto a R4.*

También será necesario que los paquetes que llegan desde Internet a la red a través de R4 (paquetes destinados a las direcciones de LAN1 y LAN2) sean encaminados correctamente. La LAN2 está directamente conectada a R4, por lo que contará con esa entrada en su tabla, pero no sabrá cómo llegar a LAN1. Para eso deberemos agregar una entrada en R4. La tabla de R4 sería entonces:

Tabla de R4		*Comentario*
Destino	***Próximo salto***	
Sin datos	*Sin datos*	*Red directamente conectada en la interfaz a Internet (interfaz WAN).* *No se dieron los datos en la letra.*
200.0.0.128/25	*eth254*	*Red directamente conectada en la interfaz eth254 (configurada por el proveedor)*
200.0.0.0/25	*200.0.0.130*	*Se requiere que R4 sepa cómo llegar a LAN1.*
0.0.0.0/0	*Sin datos*	*Ruta por defecto hacia un equipo del proveedor.* *No se dieron los datos en la letra.*

Con estas entradas tendremos tráfico saliente a cualquier dirección y también entrante.

d) Observe que las direcciones de las LAN1 y LAN2 son direcciones públicas, pero que las de los enlaces R1-R2, R1-R3 y R2-R3 son direcciones privadas. ¿Qué ventajas, desventajas o limitaciones identifica en esa configuración? Justifique su respuesta.

Para encaminar los paquetes solamente hace falta conocer el próximo salto, por lo que no hay inconveniente en que las direcciones de los enlaces entre enrutadores sean privadas. Las direcciones origen y destino de los paquetes no se modifican en tránsito.
Esta configuración permite ahorrar direcciones públicas.

La limitación que aparece es cuando el origen o destino de los paquetes es una IP de una interfaz de un enrutador. Por ejemplo, si desde la consola de R1 hago un ping a la IP 200.0.0.140, la dirección origen del paquete creado por R1 será normalmente la IP 10.0.0.5, ya que es la IP de la interfaz por la que ese paquete saldría de R1. Ese paquete llegaría sin problema a PCb ya que el encaminamiento se hace en base a la IP de destino. Pero el paquete de vuelta, según las tablas que se crearon en las partes anteriores, se encaminaría por R4 hacia Internet o se descartaría (ya que normalmente las conexiones a Internet se configuran para descartar paquetes destinados a direcciones de rangos privados). Para resolver este caso, se podría agregar en R4 una ruta para llegar a las redes 10.0.0.x a través de R2.
Observe que en algún interno, podría funcionar, por ejemplo un ping de R2 a PCa funcionaría.
En general comunicaciones a equipos de Internet no van a ser posibles cuando el origen sea una dirección privada, un escenario simple es pensar en un traceroute desde internet a PCa. También esta configuración podría verse como una ventaja en cuanto a la seguridad, ya que nunca desde afuera de la red podrán llegar a una dirección 10.0.0.x.

Pregunta 2 (6 puntos)

a) ¿Por qué no se usan las direcciones IP como identificadores en la subcapa MAC (en reemplazo de las direcciones Ethernet)? Justifique su respuesta.

Para explicar la necesidad de dos direcciones distintas, vale la pena recordar el porqué del modelo de capas. En el modelo de capas se busca independizar funcionalidades, lo que permite a capas superiores abstraerse de lo que sucede en capas inferiores, haciendo uso únicamente de las primitivas de servicio que les brindan las capas subyacentes. Por lo tanto, capas distintas tienen objetivos distintos.

La capa de enlace tiene como objetivo asegurarse que la información llega correctamente de un "extremo del cable a otro". Se puede decir que la capa de enlace tiene funcionalidad local, en rigor, solo le importa la comunicación entre dos máquinas adyacentes físicamente.
La capa de enlace no tiene conocimiento alguno de la capa de red, por lo tanto, se necesita para que se realice la comunicación correctamente, identificar cada computadora que esté compartiendo el medio de forma unívoca.

La dirección de capa de red, o dirección IP, es un identificador mediante el cual nos aseguramos que todas las computadoras puedan encontrarse entre sí a escala global, independientemente de cómo están conectadas físicamente.

En resumen, las direcciones MAC tienen como cometido identificar entidades de forma local e independiza a la capa de enlace del direccionamiento utilizado en protocolos de capa de red. En cambio, las direcciones de capa de red tienen validez global.

b) ¿Cuál es el objetivo de la funcionalidad conocida como VLANs (Virtual LANs)?. Justifique su respuesta.

Las redes de área local como Ethernet presentan la ventaja de permitir la comunicación directa entre equipos a nivel de capa 2, pero esto en muchos casos es también una desventaja, por ejemplo:

- *Falta de segregación de tráfico puede generar problemas de seguridad.*
- *Tráfico de broadcast y tramas a destinos aún no aprendidos se inundan a toda la red, disminuyendo la performance.*

En muchas redes es entonces necesario o conveniente organizarla en varias subredes IP, interconectadas por dispositivos de capa 3 o superior, para aislar conjuntos de equipos con distintos requerimientos (seguridad, performance, etc).
Se presenta entonces el problema de separar las distintas redes Ethernet. Una posibilidad es utilizar un switch por red, pero con esto tenemos un uso ineficiente de los switches, a lo que se le agrega dificultades de gestión si se quiere mover un equipo de un grupo a otro, ya que se debe cablear nuevamente hacia otro switch. Queremos utilizar entonces un mismo switch para conexión de redes distintas.

Las VLAN's logran separar lógicamente una misma infraestructura física en múltiples LAN's virtuales. Para lograr esto, un switch que pueda implementar VLAN's realiza un mapeo VLAN-Puerto, separando el conjunto de puertos físicos en uno o varios grupos aislados entre si. De esta forma cada equipo conectado a un puerto solamente comparte el medio de difusión con equipo conectados a puertos de la misma VLAN. Con esto se logra:

- *Seguridad: correctamente implementado, los equipos de una VLAN no pueden comunicarse con los de otra sin pasar por un dispositivo de capa 3 (enrutador)*
- *Eficiencia: los paquetes broadcast de una VLAN no llegan a otras*
- *Flexibilidad: los puertos pueden asignarse a distintas VLANs según conveniencia sin necesidad de recableados.*

c) ¿Qué modificaciones en el formato de trama 802.3 fueron necesarios al estandarizar las VLAN (protocolo 802.1Q)? ¿Quiénes deben implementar estas modificaciones? Justifique su respuesta.

El protocolo 802.1q permite a los switches extender el encabezado de capa de enlace agregando información de forma tal que distintos switches puedan distinguir a qué VLAN pertenece cada trama.
Para lograr esto, algunos puertos del switch se configuran para utilizar 802.1Q (puertos "trunk"), opcionalmente indicando las VLANs permitidas. A la hora de decidir por dónde reenviar una determinada trama el switch considerará que ese puerto pertenece a todas las VLANs permitidas. Suponiendo que el puerto "trunk" está conectado con otro switch, el switch receptor analiza la información extra agregada en cada trama de forma tal de identificar a qué VLAN pertenece y posteriormente reenviar las tramas solamente por los puertos asociados a dicha VLAN.

Pregunta 3 (10 puntos)

Los equipos A, B, C y D se encuentran conectados como se indica en la figura, mediante dos switches Ethernet transparentes. Suponga que todos los equipos están correctamente configurados y acaban de encenderse, por lo que no tienen ninguna información en las tablas dinámicas involucradas.

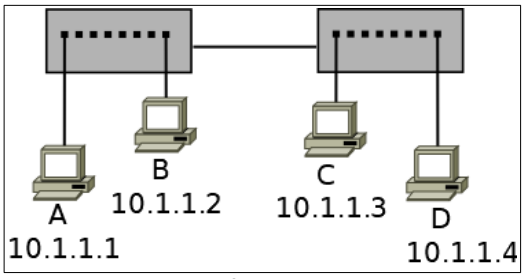

Figura 2

a) ¿Qué sucede cuando en A se ejecuta el comando "ping -c 1 10.1.1.3" ?. Recordar que este comando envía un mensaje ICMP del tipo "echo request" a la IP de C. Suponga que C recibe y responde el mensaje (con un ICMP "echo reply").
Explique detalladamente qué decisiones se toman y qué acciones se realizan en A; ¿qué protocolos están involucrados y qué tramas se envían y reciben por la interfaz de red de A? Justifique su respuesta.
Detalle los campos relevantes de las tramas (direcciones, protocolos, cometido del mensaje).

La siguiente tabla detalla el conjunto de acciones y tramas que se ven en la interfaz de A. Se supone que los equipos no implementan la funcionalidad mencionada de "ARP gratuito".

#	MAC Origen	MAC Destino	IP Origen	IP Destino	Protocolo	Motivo
1				10.1.1.3		A tiene que enviar un paquete a la IP indicada, para lo que debe consultar su tabla de forwarding. Como la IP está en su mismo rango, sabe que es alcanzable sin necesidad de ningún salto intermedio y utiliza el protocolo ARP para averiguar la MAC de C y poder completar los datos de la trama. Antes de hacer la consulta por ARP se fijará si ya tiene la MAC de C en su tabla o caché de ARP, pero como esa tabla está incialmente vacía no la encontrá. A tiene su IP y su MAC, tiene la IP de C, pero desconoce su MAC. El protocolo ARP es el encargado de averiguar ese dato.
2	MAC A	FF::FF (broadcast)			ARP (ARP request MAC de 10.1.1.3)	A envía un mensaje a broadcast (para que llegue a todos los equipos de la LAN) y así obtener la dirección MAC de C. No es un paquete IP, por lo que los campos IP de origen y destino no se completan en la tabla. En el contenido del mensaje de ARP viaja la IP de la que se desea averiguar su MAC, así como la correspondencia IP de A, MAC de A para que se conozca por el destinatario. Todos los equipos de la red reciben este mensaje (está dirigido a FF:..:FF) pero solamente responde el equipo al que va destinada la consulta ARP (equipo C).
3	MAC C	MAC A			ARP (ARP reply 10.1.1.3 y MAC C)	Respuesta unicast (ya no es broadcast, va destinada solo a la MAC A). Se envía dentro del mensaje ARP la correspondencia MAC C, IP C.
4	MAC A	MAC C	10.1.1.1	10.1.1.3	ICMP echo request	A obtuvo la MAC C por lo que tienen todos los datos para crear la trama ethernet que lleva el “paquete” ICMP de echo request.
5	MAC C	MAC A	10.1.1.3	10.1.1.1	ICMP echo reply	C dispone de la MAC A (obtenida de la consulta de ARP del paso 2) y tiene todos los datos para crear la trama ethernet que lleva el “paquete” ICMP de echo reply.

b) Explique cuáles de los equipos (PCs y switches) reciben cada una de las tramas descritas en la parte a), qué información aprenden y de qué forma almacenan esa información. Justifique su respuesta.

Las tramas de la parte a) llegan a los equipos mediante los switches. Los switches transparentes inicialmente no saben qué equipos tienen conectados a sus interfaces, pero a medida que reciben tráfico aprenden, en base a las direcciones MAC de origen y el puerto por el que le llegan las tramas, dónde está conectado cada equipo. Esa información que aprenden la guardan en tablas para posteriormente encaminar las tramas solamente por la interfaz necesaria para llegar al destino, haciendo más eficiente el uso de la red.

Las entradas en la tabla del switch tienen un tiempo de validez para evitar mantener entradas para equipos que abandonan la red o para equipos que no generan tráfico por largos períodos de tiempo.

En la siguiente tabla, el número hace referencia a las tramas de la tabla de la parte a).

	MAC Origen	*MAC Destino*	*PC que ven la trama*	*Switches*	*Motivo*
2	*MAC A*	*FF::FF*	*B,C,D*	*Ambos aprenden por qué puerto alcanzar a **A** (**MAC A**) y guardan cada uno en su tabla de MACs la correspondencia. Esa correspondencia se guarda por un tiempo de vigencia **Ts**.*	*El broadcast de ethernet se debe replicar en todos los puertos de los switches (menos por el que ingresa la trama), ya que debe llegar a todos los equipos.* *Por esto ven la trama B,C y D.*
					*A nivel de ARP, la consulta es por la IP de C por lo que C guardará la correspondencia **IP_A -MAC A** en su cache de ARP (adelantándose a que seguramente la va a necesitar para responder a A). Esta entrada tendrá un tiempo de vida T_A.* *Los demás equipos también ven la consulta (era broadcast) pero solo en caso de tener una entrada previa para **IP_A**, actualizarán la MAC asociada (por si hubiera cambiado). Si no tenían información previa de A (como en este caso porque no había nada en las tablas) ignorarán el mensaje*
3	*MAC C*	*MAC A*	*A*	*Ambos aprenden por que puerto pueden alcanzar a **C** (**MAC C**) y guardan en la tabla de MACs del switch esa correspondencia por un tiempo de vigencia **Ts**.*	*Como los switches ya aprendieron donde se encuentra **A** (del mensaje anterior), dirigen solamente la trama por estos puertos: el link entre switches y la interfaz donde está conectada **A.***
					*A nivel ARP y del mismo modo que lo descrito anteriormente, A almacena en su caché de ARP la correspondencia **IP_C -MAC C** con un tiempo de vida **T_A***
4	*MAC A*	*MAC C*	*C*	*Los switches refrescan la entrada que asocia la interfaz donde está conectada **A** y su **MAC A***	*Como los switches ya aprendieron donde se encuentra **C**, dirigen la trama solamente por los puertos necesarios: el link entre switches y la interfaz donde se conecta **C***
					C** refresca la entrada del caché de ARP asociada a **A.
5	*MAC C*	*MAC A*	*A*	*Los switches refrescan la entrada que asocia la interfaz donde está conectada **C** y su **MAC C***	*Como los switches ya aprendieron donde se encuentra **A**, dirigen la trama solamente por los puertos necesarios: el link entre switches y la interfaz donde se conecta **A**-*
					A** refresca la entrada del caché de ARP asociada a **C.

c) Si al cabo de un tiempo **T**, en A se vuelve a ejecutar el mismo comando, discuta cómo se realizaría el envío de tramas según los valores de los tiempos validez de las entradas en las tablas involucradas.

*En la parte a) mencionamos que existe un timer **Ts** de tiempo de vida de las entradas en las tablas de los switches en las que se almacena la correspondencia entre las MACs y las interfaces o puertos del switch. En la parte b) mencionamos que existe un timer T_A de tiempo de vida de la asociación MAC a IP en las tablas de ARP en las PCs.*

Asumimos para el análisis que el intercambio de tramas fue rápido y de duración mucho menor que ambos timers, despreciando por tanto esos tiempos.

Analicemos los posibles casos:

Si $Ts < T_A < T$ (o $T_A < Ts < T$): Habrán expirado tanto el cache de ARP y las asociaciones en los switches, por lo tanto se vuelve a reproducir todo el intercambio visto en a) y sus consecuencias detalladas en b).

Si $T < T_A < Ts$ (o $T < Ts < T_A$): Ninguno de los caches habrá expirado por lo que A mantiene la asociación MAC C – IPc, y los switches conocen por que puertos alcanzar a MAC A y MAC C. Por lo que se intercambia directamente el paquete IP, utilizando las MAC aprendida, y el resto de las PCs no ven el intercambio de tramas (que transportan el mensaje ICMP). Observar que tal cual lo explicado en b), ambos timers se refrescan, en las tablas de ARP y en los switches.

*Si $T_A < T < Ts$: Expiró el cache de ARP, pero no las asociaciones de MAC-puerto en los switches. A debe realizar un nuevo ARP Request, el broadcast lo ven todas las PCs (paso 2 de parte a). La respuesta ARP reply de C (que es unicast), solo lo ve A (paso 3 de parte a) ya que los switches aún saben por qué puerto se llega a **A** (y lo refrescan con estos intercambios). Si bien los switches conocían dónde estaban ubicadas las estaciones, el intercambio de tramas es similar al de la parte a). Los switches refrescan las entradas existentes para MAC A y puerto, y MAC C y puerto.*

*Si $Ts < T < T_A$: Expiraron las asociaciones MAC-puerto en las tablas de los switches, pero no las entradas de ARP en los PCs. A dispone de la MAC de C y puede enviar la trama que lleva al ICMP echo request. Al llegar al switch, este aprende que la MAC de A es alcanzable por el puerto que ingresó, pero no conoce el puerto donde está conectada la MAC C. Entonces debe inundar (genera una copia de la trama por todos los puertos del switch, salvo por el puerto que ingresó). Esto hace que B, C y D vean la trama que lleva el ICMP echo request, pero como no se está consultando por sus IPs, ignoran el mensaje ARP. C (para quien sí está dirigido el mensaje ARP) ya dispone de la MAC A para responder con el ICMP echo reply, los switches conocen donde se encuentra la MAC A, por lo que generan una copia solo por dichos puertos (link entre switches y puerto de A), a la vez que aprenden como alcanzar la MAC C (crean la asociación MAC C puerto y tiempo de validez **Ts**)*

Pregunta 4 (8 puntos)

a) Explique el funcionamiento del protocolo de acceso al medio CSMA/CD.

Los protocolos CSMA (Carrier Sense Multiple Access) son protocolos para arbitrar el acceso al medio en canales compartidos y basan su funcionamiento en la posibilidad de las estaciones de detectar si el medio está siendo utilizado por una transmisión (detección de portadora) y actuar acorde a ello, de modo de acotar la probabilidad de colisiones.

Aún cuando se sense el medio antes de intentar transmitir, es posible que ocurran colisiones ya que una estación puede ver el canal libre "más o menos" simultáneamente con otra y ambas pueden decidir comenzar a transmitir en función de los retardos inherentes al canal. Cuando ocurren colisiones, las señales eléctricas correspondientes a ambas tramas se suman en el canal, corrompiéndose los datos enviados por ambas estaciones.

Vimos tres modalidades de los protocolos CSMA, que se describen a continuación:

<u>CSMA persistente-1</u> Este protocolo es el más sencillo de los que implementan detección de portadora. Cada vez que una estación desea transmitir una trama, sensa el canal (detección de portadora).
Si el canal esta libre comienza la transmisión de la trama.
Si está ocupado, entonces permanece sensando el canal y cuando se desocupa, transmite. Se le llama persistente-1, ya que con probabilidad 1 transmite cuando se encuentra el canal libre. Esta característica es la que diferencia las restantes modalidades.

En caso de ocurrir una colisión, la estación espera una cantidad aleatoria de tiempo e intenta nuevamente el proceso indicado.

CSMA no persistente La modalidad no persistente se diferencia de la persistente-1 solamente cuando una estación encuentra el canal ocupado. En lugar de escuchar el canal hasta que la estación que estaba haciendo uso del canal lo libere y comenzar a transmitir de inmediato; espera un tiempo aleatorio y vuelve a sensar el canal, siguiendo el mismo comportamiento luego. De esta manera se obtiene una mejor utilización del canal que en el caso anterior, a costa de un mayor retardo.

CSMA persistente-p Esta modalidad se aplica solamente a canales ranurados, es decir, en los que las estaciones solamente pueden transmitir en instantes determinados de tiempo (o ranuras). El funcionamiento es similar a la modalidad persistente-1, salvo que cuando una estación está lista para transmitir y observa que el canal esta en reposo, transmite con probabilidad p y espera a la siguiente ranura con una probabilidad 1-p. En la siguiente ranura vuelve a sensar el canal y repite el proceso. De esta forma continúa hasta que logra transmitir la trama.

El protocolo CSMA/CD agrega a los anteriores la detección de colisión (Colission detection, CD). Esta detección se realiza escuchando el canal mientras se transmite y comparando lo que se recibe con lo que se transmite. Si se recibe lo mismo que se transmite, entonces no hay colisiones.

***Nota:** Sin entrar en los detalles de bajo nivel, la detección de portadora hace referencia a que la codificación del bit 0 o el bit 1 en señales eléctricas, fuerza a que el nivel medio de señal en el canal es diferente de cero (o solo ruido). De esta forma midiendo determinado nivel eléctrico, podemos detectar si hay una estación transmitiendo.*

b) Fundamente la necesidad de estandarizar un tamaño mínimo de trama.

*El largo mínimo de trama es necesario porque puede suceder que la estación **A** vea el canal libre y comience a transmitir pero por los retardos de propagación del canal, en otro punto del medio compartido, otra estación **B** aún vea el canal libre y también comience a transmitir. En este caso habría una colisión y para que **A** pueda detectarla deberá permanecer leyendo el canal y comparando con lo que está enviando. Si **A** parara de transmitir antes, no sabría si la señal que le llega de **B** es de una estación lejana que colisionó con su trama o de una estación cercana que comenzó a transmitir en cuanto A se detuvo.*

*De forma intuitiva se necesita que la estación **A** transmita un tiempo suficiente para garantizar que la información de la trama llegue hasta la estación mas lejana **B**, y si hay una colisión, **A** se entere antes de finalizar la transmisión. Por lo tanto, se necesita que en el peor caso **A** transmita al menos el tiempo necesario para que la señal de **A** llegue a **B** más el tiempo en que la señal de **B** llegue a **A**, y este tiempo multiplicado por la velocidad de transmisión en bits/s nos da la longitud mínima de trama (en bits). Este tiempo depende de la distancia máxima admitida entre cualquier par de estaciones (peor caso de separación entre **A** y **B**) y la velocidad de propagación de la señal electromagnética por el medio elegido. O sea **L** (bits)=**V** (bps) * **T** (s), siendo **V** la velocidad en bps y **T** el tiempo de ida y vuelta entre las estaciones más lejanas.*

Según la norma 802.3, en una LAN a 10 Mbps con una distancia máxima entre estaciones de 2500 metros y 4 repetidores, el tiempo de ida y vuelta (incluyendo la propagación en el cable y los retardos introducidos por los repetidores), se considera alrededor de 50 μsec en el peor caso. Por lo tanto el tamaño mínimo de trama será de $10 \times 10^{6} \times 50 \times 10^{-6} = 500$ bits, por lo que se toma agregando cierto margen de seguridad 512 bits = 64 bytes como tamaño mínimo de trama.

c) A lo largo de los años se han ido incrementando las velocidades de los estándares de Ethernet de 10 Mbps, a 100 Mbps, 1 Gbps y más. ¿Fue necesario modificar el tamaño mínimo de trama? Justifique su respuesta.

*En base al cálculo del tamaño mínimo de trama explicado en b), si no se cambian los parámetros físicos de la red, **T** no cambiará (definido por la propagación electromagnética), por lo que al aumentarse **V**, aumentaría en la misma proporción el largo mínimo de trama. Para evitar esto, lo que cambió en las normas al aumentar la velocidad de transmisión, es la disminución de la distancia máxima admitida entre cualquier par de estaciones en el medio compartido (implica disminuir **T**).*

Pregunta 5 (8 puntos)

a) Explique las principales diferencias vistas en el curso entre un algoritmo de cifrado simétrico y un algoritmo de clave pública.

	Cifrado Simétrico	***Clave pública***
Claves utilizadas	*Clave compartida.* *Los interlocutores comparten la misma clave.*	*Cada entidad genera dos claves relacionadas, (dependientes del algoritmo), tales que la clave privada no puede deducirse de la clave pública (seguridad computacional).* *Clave pública que se puede distribuir, clave privada debe mantenerse en secreto.*
No repudio (verificación por terceros)	*Imposible ya que al menos transmisor y receptor poseen la clave compartida y pueden generar mensaje cifrado.*	*Un mensaje firmado puede ser verificado por terceros ya que solo quien tiene la clave privada puede haber firmado (tiene validez legal, dependiendo que la clave pública haya sido registrada en una CA) .*
Intercambio de claves	*Se deben de poner de acuerdo entre las partes. Cualquiera que obtenga la clave puede cifrar y descifrar mensajes, por lo que debe realizarse mediante mecanismo seguro.*	*Solo se comparte la clave pública, y no requiere cuidados especiales de seguridad para compartir.* *Se requiere algún mecanismo para asociar la clave pública con la entidad a quien pertenece si el intercambio es por medios no seguros, por ejemplo utilizando el sistema de PKI (una autoridad certificadora firma un certificado asociando la clave pública con una identidad)*
Cifrado/descifrado	*Algoritmo de cifrado y descifrado utilizan la misma clave*	*Lo que se cifra con la clave privada puede descifrarse solamente con la clave pública, mientras que lo cifrado con la clave pública se descifra con la clave privada*
Firmas Digitales	*En el curso no vimos mecanismos, existen algunos pero a través de un tercero confiable por todas las partes (equivalente a un "escribano")*	*Si se gestionó las claves con una CA (Certificate Authority), y se tiene firmada la clave publica. Se puede utilizar el procedimiento de firma digital y cuenta con validez legal.*
Velocidad o necesidades de cálculo	*Más simple, menores requerimientos computacionales, por este motivo son más rápidos.*	*Mayor requerimiento de computo, por las operaciones matemáticas que conllevan (aritmética con números grandes), típicamente cientos o miles de veces más lentos que los simétricos utilizando recursos de cómputo similares.*

b) ¿Por qué razón práctica usualmente se evita cifrar grandes volúmenes de datos con los algoritmos de clave pública? Justifique su respuesta.

El cifrado/descifrado con algoritmos de clave pública es computacionalmente mucho mas costoso que la misma operación con algoritmos de cifrado simétricos con igual nivel de seguridad.

Si tomamos como ejemplo RSA, el cifrado (y descifrado) tienen la forma $c = m^e \bmod n$ *(c-mensaje cifrado, m-mensaje original, (n,e) – clave), realizar estas cuentas con enteros de miles de bits requiere una cantidad considerable de recursos computacionales.*

c) Explique el mecanismo para realizar una firma digital visto en el curso. Indique qué clave o claves debe conocer el receptor para poder validar la firma. Explique por qué no es posible falsificar una firma sin ser detectado.

*El mecanismo que vimos durante el curso utiliza 2 funciones, una función $E_{ke}(x)$, cifrado de clave pública dependiente de una clave, y una función de hash seguro **H**(x). Para realizar la firma, se calcula $E_{ke}(H(M))$, donde **M** es el mensaje a firmar, y **Ke** es la clave privada de quien firma. El receptor recibe M y $E_{ke}(H(M))$ (firma).*

*Partiendo de $\mathbf{M_2}$ (mensaje recibido) y $\mathbf{E_{ke}(H(M)^*)}$, para verificar la firma se precisa la clave pública de quien firma, **Kp**. Quien quiere verificar la firma descifra $E_{ke}(H(M)^*)$, obteniendo el hash **H(M)***, y calcula el hash del mensaje M_2 recibido, $\mathbf{H(M_2)}$. Si $\mathbf{H(M)^*}=\mathbf{H(M_2)}$ asume que el mensaje fue firmado por quien dispone de la clave privada **Ke** correspondiente a la clave pública **Kp**.*

El principal objetivo de una firma es garantizar el origen del mensaje (quién lo firmó) y su integridad (que el mensaje recibido es el mismo que fue firmado). Esto debe poderse verificar por terceros.

*El origen del mensaje se garantiza por el algoritmo de clave pública, donde no es computacionalmente posible encontrar la clave privada a partir de la pública, ni cifrar un mensaje que se descifre correctamente con la clave pública sin conocer la clave privada. En este sentido, falsificar una firma implicaría encontrar, sin conocer la clave **Ke**, un bloque **B** tal que al descifrarlo con **Kp** me diera el mismo valor que **H(M)**.*
Otra opción sería reutilizar una firma de un mensaje existente $E_{ke}(H(M))$ para un nuevo mensaje M', pero esto implicaría encontrar otro mensaje tal que $\mathbf{H(M')}=\mathbf{H(M)}$, lo cual no es posible si la función de hash H es resistente a las colisiones.

*Este procedimiento entonces nos garantiza que quien "firmó" el mensaje posee la clave privada correspondiente a la clave pública **Kp**.*

*Precisamos entonces estar seguros de la pertenencia de **Kp** a la entidad que firma. Por ejemplo mediante un certificado de clave pública, de una entidad certificadora en la que confíe, que relacione la identidad con la clave pública correspondiente.*

d) ¿Qué sucedería con el punto anterior si el algoritmo de hash (MD, resumen) utilizado no fuera resistente a las colisiones? Justifique su respuesta.

*La resistencia a colisiones (tanto débil como fuerte) es una propiedad necesaria en los hashes seguros, que implica que sea computacionalmente inviable encontrar dos mensajes **M**, $\mathbf{M_2}$ tales que $\mathbf{H(M)} = \mathbf{H(M_2)}$.*

*De no poseer resistencia débil a colisiones, dado un mensaje **M** firmado por una entidad A, el atacante puede generar un mensaje $\mathbf{M_2}$ (beneficioso para el atacante), donde $\mathbf{H(M_2)} = \mathbf{H(M)}$ por lo que $\mathbf{E_{ke}(H(M))} = \mathbf{E_{ke}(H(M_2))}$, lo cual permite entregarle a un tercero B $\mathbf{M_2}$, $\mathbf{E_{ke}(H(M))}$. Al verificar B la firma del mensaje, no detectará la sustitución del mensaje original.*

*De no poseer resistencia fuerte a colisiones el atacante precisará manipular tanto el mensaje que Alice quiere enviar como el que el atacante pretende sustituir, es decir que solo podremos atacar la firma realizada por una entidad que firma datos generados por otros. Una vez que disponemos de dos mensajes **M** y $\mathbf{M_2}$ donde $\mathbf{H(M_2)} = \mathbf{H(M)}$, y Alice firma uno de ellos, podemos realizar la misma sustitución de un mensaje por otro sin ser detectado.*