18 de noviembre de 2019

Redes de Datos 1
2º parcial – 2019
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 (8 puntos)

a) Explique las diferencias conceptuales entre las redes de circuitos virtuales y las redes de datagramas.

En las redes de datagramas, cada paquete lleva la dirección de destino, y es encaminado por cada enrutador independientemente de los datagramas anteriores utilizando la información local del mejor próximo salto. No es necesario realizar ninguna acción antes de enviar paquetes a la red.
En las redes de circuitos virtuales, antes de enviar paquetes desde un origen a un destino, se requiere el establecimiento de un circuito virtual (CV). Ese CV determina un camino en la red, por el que van a transitar los paquetes desde el origen al destino.
Se identifican entonces 3 fases en la transmisión de datos en una red de este tipo: fase de establecimiento del CV, fase de uso del CV (los paquetes circulan por el CV) y fase de liberación o corte del CV.
A diferencia de lo que ocurre en las redes de datagramas, los paquetes desde el origen al destino recorrerán siempre el mismo camino, determinado por el CV que utilicen.
La elección del camino se realiza en la función de ruteo de la red, quien determinará el "mejor" camino entre esos puntos.

b) ¿Qué ventajas presentan las redes de circuitos virtuales frente a las redes de datagramas?

Como ventaja de las redes de CVs se puede mencionar que permiten manejar el problema de la congestión con más herramientas que en las redes de datagramas. Esto se debe a que antes de enviar el tráfico es necesario establecer el CV y en ese procedimiento será necesario dialogar con todos los nodos del camino que se desee usar. Si los nodos no tuvieran recursos suficientes al momento de intentar establecer un nuevo CV, podrían rechazar la petición y se intentará buscar otro camino alternativo que permita el establecimiento del CV.
Por otro lado, en la instancia de establecimiento podrían reservarse los recursos necesarios para el nuevo CV, lo que permitiría garantizar calidad de servicio a los caminos en la red. Por ejemplo se podría garantizar a un nuevo CV cierto nivel de retardo máximo o de ancho de banda mínimo.
Esto permitiría ofrecer servicios diferenciados con diferentes calidades o garantías.
Además el sólo hecho de que los paquetes circulen siempre por el mismo camino, contribuirá a que el retardo de extremo a extremo y la variación de retardo de los paquetes, sea más predecible. Este último factor es importante también para algunos servicios sensibles al retardo.
Finalmente las redes de CVs permiten implementar "ingeniería de tráfico", lo que significa que podemos controlar cómo se encamina el tráfico por la red en base a criterios adicionales a la dirección de destino (que es lo que se usa como criterio en las redes de datagramas).
Una ventaja adicional, es que el forwarding de paquetes en estas redes es más rápido, ya que no se requiere una búsqueda en la tabla (como en el algoritmo longest-prefix-match de IP), sino que se realizará un intercambio de identificadores como se explica en la parte d).

c) ¿Qué desventajas presentan las redes de circuitos virtuales frente a las redes de datagramas?

Como desventajas se puede mencionar que al requerir el establecimiento de CVs, la red almacenará (en las tablas de CVs de sus nodos) información de estado de la red, lo que significa que la red se acuerda del camino que deben seguir los paquetes de una comunicación. Por tanto si un nodo se cae, se perderá esa tabla y se "olvidará" de los caminos que pasaban por él. Para poder continuar enviando paquetes, habrá que re-establecer un nuevo CV. Este proceso llevará cierto tiempo durante el cual no podré intercambiar información entre ese origen y destino.
También se requiere la gestión de los CVs (establecimiento y liberación), lo que implica una carga de gestión adicional, así como recursos para almacenar la información de los circuitos establecidos.

En las redes de datagramas, como los paquetes se encaminan uno a uno, de forma independiente de los anteriores, estos problemas no se presentan y en la medida que el ruteo de la red se adapte cuando hay caídas en los nodos, el tráfico podría no enterarse que cambió el camino de origen a destino.

d) Explique qué son y cómo se usan los identificadores de circuito virtual en las redes de circuitos virtuales.

Los identificadores de CV son números que identifican a un CV. Tener un único identificador para cada CV sería complicado, ya que requeriría que todos los nodos involucrados en el CV tuvieran ese identificador libre o implicaría realizar un proceso de negociación entre varios nodos para acordar un identificador libre en todos. Por tanto un CV estará identificado por la concatenación de identificadores de CV en cada uno de los tramos que componen el CV. De este modo, si el camino involucra a los nodos A-B-C-D, se realizará una negociación entre A y B para elegir un identificador ID_x, una negociación entre B y C para elegir un identificador ID_y y una negociación entre C y D para elegir un ID_z. El circuito virtual será identificado entonces en cada tramo por un ID diferente.
Para que el tráfico de A a D siga el camino A-B-C-D, cada nodo involucrado realizará un intercambio de etiquetas o identificadores. El tráfico que llegue al nodo B con el identificador ID_x acordado con A, saldrá de B con el identificador ID_y, acordado entre B y C. Del mismo modo, el tráfico que llegue a C con el ID_y, será enviado a D con el identificador ID_z.
Los nodos tendrán tablas de forwarding que reflejen este intercambio de identificadores, por ejemplo el nodo B para este tráfico, tendrá una entrada de la forma:

ID de entrada	**Interfaz de salida**	**ID de salida**
ID_x	If_1	ID_y
….	….	….

Como se mencionó anteriormente, el forwarding es más sencillo y rápido que en las redes de datagramas, porque alcanza con entrar en la tabla con el identificador del paquete que llega (ID_x), intercambiarlo por el que dice la tabla (ID_y) y sacar el paquete por la interfaz de salida adecuada (If_1 en el ejemplo).

Pregunta 2 (9 puntos)

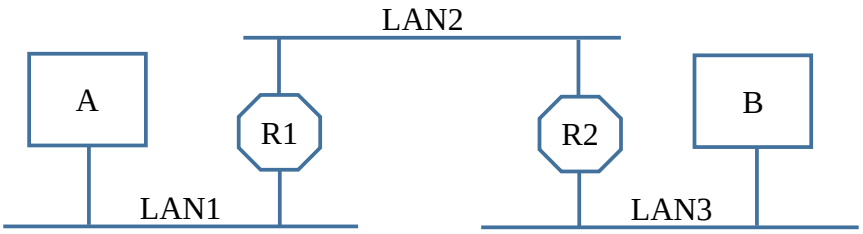
a) Explique el cometido del protocolo ARP (Address Resolution Protocol) y en qué redes se utiliza.

El protocolo ARP tiene como cometido relacionar las direcciones de capa 3 (IP) con las direcciones de capa MAC.
A nivel de capa 3 cuando un equipo X desea enviar información a otro equipo Y, lo que conoce es su dirección de capa 3, por ejemplo la dirección IP de Y. Con esa IP, X buscará en su tabla de forwarding (algoritmo longest-prefix-match) el próximo salto para llegar a Y. Si la IP de Y está en la misma subred que X, entonces X sabrá que para llegar a Y le alcanza con armar una trama y enviarla a través del medio compartido.

Para poder construir esa trama necesitará la dirección de capa MAC de Y (además de otros datos) y el protocolo ARP cumple la función de encontrar la correspondencia entre la IP de Y y la MAC de Y. Es importante destacar que en caso que Y no esté en la misma red que X, X deberá encaminar el paquete hacia el próximo salto indicado en su tabla de forwarding y por tanto necesitará el protocolo ARP para encontrar la MAC de ese próximo salto, no la MAC de Y.

Se utiliza en redes LAN, donde hay capas de enlace de acceso múltiple, es decir aquellas donde por la misma interfaz puedo potencialmente comunicarme con múltiples equipos directamente (en capa 2). Ejemplos actuales de estas redes son las redes 802.3 (Ethernet en todas sus variantes), 802.11 (redes inalámbricas), etc.

b) Determine los mensajes del protocolo ARP intercambiados en los diferentes segmentos de red de la topología de la figura, cuando el equipo A (IP_A) desea enviar un paquete IP al equipo B (IP_B). Para cada mensaje indique su cometido así como los campos relevantes y sus valores. Justifique su respuesta.


LAN2
A
R1
R2
B
LAN1
LAN3

LAN	MAC origen	MAC destino	Contenido especificando el cometido del mensaje y los campos más relevantes
LAN1	*MAC_A*	*FF:FF:FF:FF:FF:FF*	*El equipo A observa en su tabla de forwarding que el próximo salto para llegar a IP_B es R1.* *El mensaje de ARP para encontrar la MAC asociada a la IP_R1_LAN1 se envía en una trama destinada a la dirección de broadcast de la red (para que todos los equipos de la red la procesen).* *El mensaje pregunta ¿quién tiene configurada la IP_R1_LAN1?* *En la pregunta también se indica la correspondencia del originador (IP_A, MAC_A) ya que seguramente el destinatario de la consulta (en este caso R1) necesitará comunicarse con A y para ello necesitará la MAC_A.*
LAN1	*MAC_R1_LAN1*	*MAC_A*	*De todos los potenciales equipos que comparten el medio, R1 será el que conteste el mensaje ARP del paso anterior, ya que él tiene configurada la IP_R1_LAN1 por la que se está consultando.* *Esta respuesta va destinada a nivel de capa MAC a la MAC_A, obtenida de la consulta ARP anterior. De este modo ya no se involucra al resto de los equipos.* *La respuesta será de la forma: la IP_R1_LAN1 se corresponde con la MAC_R1_LAN1.*
LAN1	*MAC_A*	*MAC_R1_LAN1*	*Ahora que A averiguó con ARP la MAC_R1_LAN1 puede enviar la información que desea a B a través de R1.* *Enviará por tanto una trama ethernet con MAC de origen MAC_A y MAC de destino MAC_R1_LAN1, conteniendo el paquete IP con dirección IP de origen IP_A y dirección IP de destino IP_B.* *La pregunta solamente requería los mensajes ARP, pero para mejorar la explicación se incluye en la tabla.*
LAN2	*MAC_R1_LAN2*	*FF:FF:FF:FF:FF:FF*	*Cuando la trama anterior llega a R1 (está destinada a su MAC_R1_LAN1), será procesada y enviada a su capa de red para ser procesada. Como R1 es un enrutador, aceptará paquetes que van a otras IPs (en este caso IP_B) además de las propias. Para saber cómo encaminar ese paquete hacia IP_B consultará su tabla de forwarding, obteniendo que el próximo salto es IP_R2_LAN2 que está directamente conectado con R1.* *Del mismo modo que A, R1 tendrá que averiguar entonces la dirección MAC asociada a la IP_R2_LAN2.* *Entonces (como en el primer mensaje ARP), R1 consulta por la MAC_R2_LAN2, en un mensaje de pregunta ¿quién tiene configurada la IP_R2_LAN2?* *En la pregunta también se indica la correspondencia del originador (IP_R1_LAN2, MAC_R1_LAN2).*
LAN2	*MAC_R2_LAN2*	*MAC_R1_LAN2*	*En la LAN2 contestará R2, reconociendo su dirección IP_R2_LAN2 en el mensaje de ARP.* *Este mensaje se dirigirá a la MAC_R1_LAN2, obtenida a partir del mensaje anterior, y tendrá la correspondencia (IP_R2_LAN2, MAC_R2_LAN2).*
LAN2	*MAC_R1_LAN2*	*MAC_R2_LAN2*	*Ahora que R1 averiguó la MAC_R2_LAN2 puede enviar la información que desea a B a través de R2.* *Enviará por tanto una trama ethernet con MAC de origen MAC_R1_LAN2 y MAC de destino MAC_R2_LAN2, conteniendo el paquete IP con dirección IP de origen IP_A y dirección IP de destino IP_B.* *La pregunta solamente requería los mensajes ARP, pero para mejorar la explicación se incluye en la tabla.*
LAN3	*MAC_R2_LAN3*	*FF:FF:FF:FF:FF:FF*	*Del mismo modo que se explicó para R1, ahora R2 necesita averiguar la MAC_B para poder encaminar el paquete a IP_B.* *Entonces, R2 consulta la MAC_B, mediante un mensaje ARP destinado a broadcast, consultando ¿quién tiene configurada la IP_B?* *En la pregunta también se indica la correspondencia del originador (IP_R2_LAN3, MAC_R2_LAN3).*
LAN3	*MAC_B*	*MAC_R2_LAN3*	*El equipo B identifica su dirección IP, y contesta con su correspondencia (IP_B, MAC_B) en un mensaje ARP dirigido a MAC_R2_LAN3, con la correspondencia (IP_B, MAC_B)*
LAN3	*MAC_R2_LAN3*	*MAC_B*	*Ahora que R2 averiguó la MAC_B puede enviar la información que desea a B.* *Enviará por tanto una trama ethernet con MAC de origen MAC_R2_LAN3 y MAC de destino MAC_B, conteniendo el paquete IP con dirección IP de origen IP_A y dirección IP de destino IP_B* *La pregunta solamente requería los mensajes ARP, pero para mejorar la explicación se incluye en la tabla.*

c) ¿Cuál es el contenido de las tablas de ARP en los distintos equipos luego de los intercambios de mensajes detallados en b)? ¿Qué equipos de los que aparecen en el diagrama anterior disponen de dicha tabla?

Cada equipo tendrá las correspondencias intercambiadas dentro de las LANs a las que pertenece.

La tabla del equipo A contendrá:
(IP_R1_LAN1) at MAC_R1_LAN1 on LAN1

La tabla del equipo R1 contendrá:
(IP_A) at MAC_A on LAN1
(IP_R2_LAN2) at MAC_R2_LAN2 on LAN2

La tabla del equipo R2 contendrá:
(IP_R1_LAN2) at MAC_R1_LAN2 on LAN2
(IP_B) at MAC_B on LAN3

La tabla del equipo B contendrá:
(IP_R2_LAN3) at MAC_R2_LAN3 on LAN3

Pregunta 3 (6 puntos)

a) ¿Qué tabla o tablas debe tener un switch Ethernet para cumplir su función? ¿Cómo las utiliza? Justifique su respuesta.

Un switch Ethernet cumple la función de forwarding (en capa 2) de tramas ethernet. Para cumplir con esta función, este cuenta con una tabla que en sus entradas relaciona direcciones MAC con puertos físicos y el tiempo de validez de esta correspondencia. Al expirar el tiempo de validez de una entrada de la tabla, esta se elimina.

Dirección MAC	Puerto	Tiempo
62:FE:F7:11:89:A3	3	9:32
7C:BA:11:E1:55:A1	4	2:40
…..	...	…..

Al recibir una trama, el switch observa la dirección MAC destino de esta y la envía por el puerto correspondiente indicado en su tabla, si la MAC destino está en el mismo puerto por el que ingresó la trama, esta se descarta.

En caso de no contar con esta información en su tabla, o en caso que esta dirección sea la de broadcast, se reenvía la trama por todos los puertos del switch exceptuando aquel por el que recibió la trama. Para direcciones destino de multicast, el procedimiento a emplear depende del switch aunque en general también se inunda por los restantes puertos.

Algunos switches tienen la posibilidad de implementar VLANs, en estos tipos de switches, cada entrada de la tabla mencionada también cuenta con un identificador de VLAN, en estos casos al hacer difusión de una trama se restringe a los puertos pertenecientes a la VLAN por la que llegó.

b) ¿Cómo se obtiene la información necesaria para completar el contenido de esta(s) tabla(s)?

El switch, al recibir una trama,

- *Verifica la suma de comprobación (opcional) y la descarta si es necesario.*
- *Si la dirección MAC de origen no está en su tabla, la agrega en ella asociándola con el puerto por el cual recibió la trama, y le asocia un tiempo de validez.*
- *Si ya cuenta con la dirección MAC de origen en su tabla, actualiza el tiempo de validez y corrige la relación MAC-Puerto en caso de haber cambiado.*

En caso de que ya contara con la entrada en su tabla, actualiza la información sobre esta.

Pregunta 4 (7 puntos)

a) En un switch Ethernet, ¿Qué función cumplen las VLANs (Virtual LANs)?

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, bajando performance*

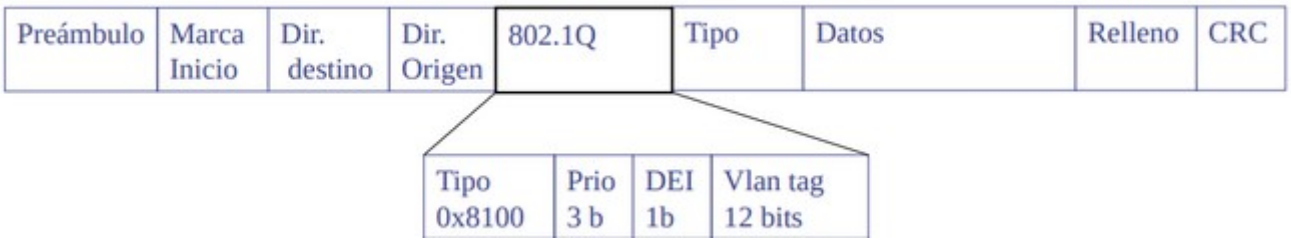
En muchas redes es entonces necesario o conveniente organizarla en varias subredes IP, interconectadas por dispositivos de capa 3 o superior, para aislar conjuntos de equipos con distintos requerimientos (seguridad, performance, etc).
Se presenta entonces el problema de separar las distintas redes Ethernet. 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 host 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, pero sin los problemas que tendríamos con switches standard.

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 host conectado a un puerto solo comparte el mismo medio de difusión con hosts 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*
- *Eficiencia: los paquetes broadcast de una VLAN no llegan a otras*
- *Flexibilidad: los puertos pueden asignarse a distintas vlans según conveniencia*

b) El protocolo 802.1Q modifica el formato de la trama Ethernet cuando se interconectan switches que manejan VLANs. ¿Qué información es necesario agregar a las tramas en este protocolo? 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.
La información agregada a cada trama es la siguiente:



Se agregan 4 bytes de los cuales:

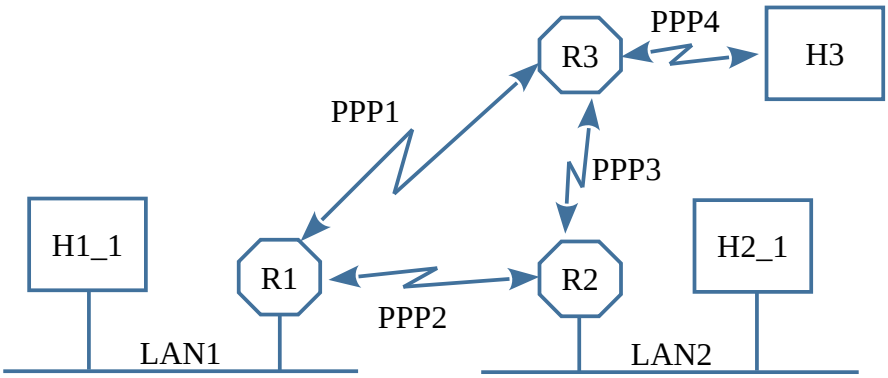
- *2 bytes para indicar que la trama es una trama con VLAN*
- *3 bits para asignar hasta 8 valores de prioridad a las tramas,*
- *1 bite DEI (Drop eligible indicator) el cual permite indicar si tramas deben ser descartadas en caso de congestión. Usualmente no utilizado*
- *12 bits asignados como identificador de la VLAN.*

c) Las computadoras conectadas a un switch que maneja VLANs, ¿deben implementar 802.1Q? Justifique su respuesta.

No es necesario implementar dicho protocolo, dado que el principal objetivo del mismo es la interconexión entre switches que manejen VLAN.
Los puertos donde se conectan las computadoras se configuran perteneciendo estáticamente a una VLAN X (puertos “acceso” o “untagged”). Todas las tramas recibidas por ese puerto (sin encabezado 802.1Q) se tratarán como pertenecientes a la vlan X, y solo se enviarán hacia ese puerto tramas pertenecientes a la vlan X

Pregunta 5 (9 puntos)

En el diagrama de la figura se necesita asignar direcciones IP a todas las subredes involucradas (incluyendo los enlaces punto a punto, PPP*). De acuerdo al dimensionamiento realizado, en la LAN1 se piensa instalar 8 computadoras (H1_*) y en la LAN2, 28 computadoras (H2_*). Los equipos R* son enrutadores.



Se dispone del rango de direcciones 10.10.0.0/**L**, siendo **L** el largo del prefijo.

a) Determine el mayor valor de **L** que permita cumplir los requerimientos. Justifique su respuesta.

Red	***Requerimientos***	***Mayor m que cumple el requerimiento (/m)***	***Comentario***
LAN 1	*8 + 1*	*/28*	
LAN 2	*28 + 1*	*/27*	
PPP1	*2*	*/30*	*Puede agregarse en un rango /28*
PPP2	*2*	*/30*	
PPP3	*2*	*/30*	
PPP4	*2*	*/30*	

Para cada una de las redes se considera las máscaras mas largas (o la menor cantidad de hosts) para cumplir con los requerimientos. Se requiere como mínimo una red /26 para cumplir con todos los requerimientos.

Se utiliza la red 10.10.0.0/26

b) Realice una asignación de direcciones adecuada a los requerimientos, justificando detalladamente el procedimiento realizado, así como los rangos que asignaría a cada una de las subredes.

Utilizando la tabla creada en la parte a)

- *Para cada requerimiento de red se busca la potencia de 2 más cercana que cumpla con los requerimientos (tomando en cuenta la pérdida de la dirección IP de red y la dirección de broadcast).*

  *Por ejemplo LAN1, 8 computadoras y un enrutador, 9 <= $2^{(32-m)} - 2$ => **m = 28***
  *Por ejemplo LAN2, 28 computadoras y un enrutador, 29 <= $2^{(32-m)} - 2$ => **m = 27***
  *Por ejemplo PPP#, dos enrutadores, 2 <= $2^{(32-m)} - 2$ => **m = 30***

- *Utilizando el rango 10.10.0.0/26, primero se divide en dos subredes /27, la primera se asigna a la LAN2 (10.10.0.0/27), la segunda mitad se divide en dos subredes /28, la primera se asigna a la LAN1 (10.10.0.32/28).*

  La segunda red /28 se subdivide primero en dos /29, y luego cada una en dos subredes /30
  ***Paso 1:** 10.10.0.48/28 en 10.10.0.48/29 y 10.10.0.56/29.*
  ***Paso 2:** 10.10.0.48/29 en 10.10.0.48/30 y 10.10.0.52/30*
  10.10.0.56/29 en 10.10.0.56/30 y 10.10.0.60/30

Host	*Asignación de Direcciones*	*Máscara*
R1_LAN1	*10.10.0.33*	*/28*
*H1_**	*10.10.0.{34 …. 46}*	*/28*
R1_PPP1	*10.10.0.49*	*/30*
R1_PPP2	*10.10.0.53*	*/30*
R2_LAN2	*10.10.0.1*	*/27*
*H2_**	*10.10.0.{2 … 30}*	
R2_PPP2	*10.10.0.54*	*/30*
R2_PPP3	*10.10.0.57*	*/30*
R3_PPP1	*10.10.0.50*	*/30*
R3_PPP3	*10.10.0.58*	*/30*
R3_PPP4	*10.10.0.61*	*/30*
H3	*10.10.0.62*	*/30*

c) Para el enrutador R3, complete la tabla de forwarding para que todos los destinos sean alcanzables.

Destino	*Próximo salto*	*Comentario*
10.10.0.48/30	*direct*	*Las entradas directamente conectadas se crean cuando se configura la dirección IP y máscara de cada una de las interfaces.*
10.10.0.56/30	*direct*	*Idem comentario anterior*
10.10.0.60/30	*direct*	*Idem comentario anterior*
10.10.0.0/27	*10.10.0.57*	*R2_PPP3*
10.10.0.32/28	*10.10.0.49*	*R1_PPP1*
10.10.0.52/30	*10.10.0.57*	*R2_PPP3*
10.10.0.52/30	*10.10.0.49*	*R1_PPP1*

Dependiendo del enrutador es posible que acepte mas de un next-hop, y se realice balanceo por flujo. En caso de solo aceptar un solo next-hop, cualquiera de los dos entradas para 10.10.0.52/30 es una respuesta válida.

Pregunta 6 (6 puntos)

a) Describa el procedimiento analizado en clase para realizar una firma digital de un documento utilizando un algoritmo de clave pública y un algoritmo de hash (resumen).

El mecanismo que vimos 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.
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 firmado, $H(M_2)$. Si $H(M)^*=H(M_2)$ asume que el mensaje fue firmado por quien dispone de la clave privada Ke correspondiente a la clave pública Kp*

b) ¿Qué propiedades tiene el procedimiento anterior? ¿Cómo se garantiza la seguridad del procedimiento?

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 H(M')=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.