25 de noviembre de 2024

Redes de Datos 1

2do parcial – 2024

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 de forma suficiente.

Pregunta 1 (10 puntos)

En el esquema de red de la Figura 1, R_1 es un enrutador, SW_1 y SW_2 son switches ethernet; y los equipos PC_* son computadoras. Todos los equipos están correctamente configurados y no hay información relevante en ningún caché.

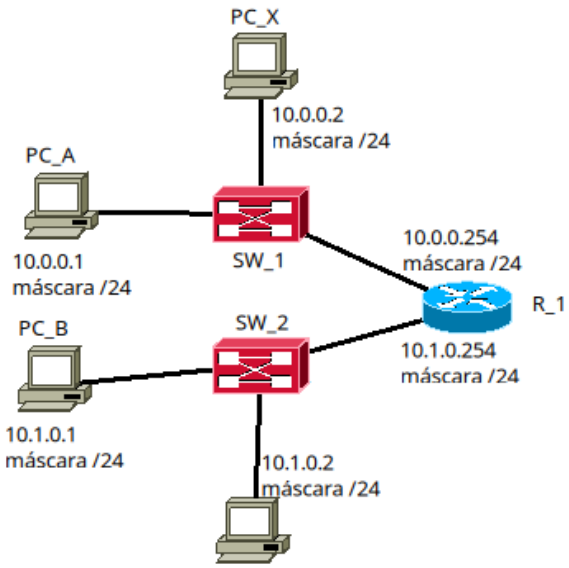

Figura 1

a) Explique por qué se necesita el protocolo ARP en las redes 802.3 (ethernet).

Las comunicaciones entre aplicaciones se inician desde capa de aplicación, solicitando un servicio a capa de transporte, la capa de transporte a la capa de red, y a su vez esta a la capa de enlace.

La separación de responsabilidades entre capas, y el permitir desacoplarse (modificar una capa, "sin" afectar a la otra capa), junto con disponer de un medio compartido en el cual hay varias estaciones escuchando al medio, introduce la necesidad de disponer de direccionamiento diferente, con alcance diferente, dirección de capa 3 global, y dirección de capa 2 local (al medio de acceso compartido). Un ejemplo de la ventaja de esta separación de direccionamiento es que se pudo mantener Ethernet cuando apareció IPv6.

En los casos que tenemos tecnologías de red de acceso compartidas (como lo es IEEE 802.3), necesitamos un identificador de capa de enlace (MAC address) para identificar para qué dispositivo es el mensaje de capa 2. La capa de enlace solo conoce de identificadores de capa de enlace, la capa de red solo conoce identificadores de capa de red. Por lo cual es necesario en un medio compartido que dada la IP destino sea posible identificar a que dispositivos (dirección MAC) direccionar la trama (unidad de intercambio de capa 2).

El protocolo ARP (Address Resolution Protocol) resuelve este "inconveniente" en una red de acceso compartido: dada una dirección IP, obtiene la dirección MAC del dispositivo que tiene dicha dirección IP en capa 3.

***Nota:** Para que esto funcione, implícitamente se está considerando que el segmento de red (la LAN) coincide con la red multiacceso de capa 2 (el dominio de broadcast). Recordar que la consulta ARP se dirige en ethernet/802.3 a la dirección MAC de broadcast ya que debe llegar a todos los dispositivos de la red multiacceso.*

***Nota2:** La existencia de direcciones MAC en redes multiacceso es lo que nos permite también generar varias eficiencias, la primera solo la estación que tiene la MAC de destino procesa la trama (salvo los broadcast que son procesados por todas las estaciones), la segunda es que es la base del algoritmo de backward learning de los switches que permite mejorar las tasas de intercambio entre estaciones.*

***Nota3:** la API de invocación a Ethernet hay que entregarle la MAC destino, no resulta lógico desde el punto de vista de separación de funciones entre capas entregar el paquete con destino a IP_B, la capa 2 tendría que buscar en la tabla de ruteo el next-hop. Si bien queda algo sujeto a la implementación software, lo más razonable es que sea la capa 3 que invoque al API de ARP para obtener la MAC address*

destino, y luego invocar a la API de ethernet con el paquete IP (origen IP_A, destino IP_B) y MAC destino (MAC R_1_1).

b) Explique detalladamente los mensajes ARP intercambiados en el segmento de red de PC_A, cuando PC_A envía un paquete IP a PC_B. Justifique su respuesta.

Cuando PC_A quiere enviar un paquete a la IP de PC_B, consultará su tabla de forwarding. En este caso, a partir de la figura, la tabla de forwarding de PC_A podría tener las siguientes entradas:

Tabla de PC_A	
Destino	***Próximo salto***
10.0.0.0/24	*Directamente conectada*
0.0.0.0/0	*10.0.0.254 (*)*

(*) Dada la topología de la red, también podría reemplazarse la ruta por defecto indicada en la tabla por una ruta a la única red existente (Destino: 10.1.0.0/24, Próximo salto: 10.0.0.254)

Vamos a suponer los siguientes valores para algunas de las direcciones MAC:
PC_A tiene dirección de capa MAC MAC_A conectado al SW_1
PC_B tiene dirección de capa MAC MAC_B conectado al SW_2
R_1 tiene dirección de capa MAC MAC_R_1_1 conectado a SW_1
R_1 tiene dirección de capa MAC MAC_R_1_2 conectado a SW_2

Los mensajes ARP tienen varios campos que en el escenario de capa 2 802.3/Ethernet y capa 3 IP se mantienen, estos son "Hardware Type", y "Hardware Size" que indican el tipo de hardware de capa 2 y el largo de las direcciones de capa 2; "Protocol Type" y "Protocol Size" que indican el tipo de protocolo de capa 3 y el largo de las direcciones de capa 3. A continuación se agrega una tabla donde figuran los ***campos relevantes de los mensajes ARP que viajan sobre tramas Ethernet (en las observaciones se explicitan estos encabezados):***

		Campos Relevantes de los mensajes ARP					
#	*Genera mensaje*	***tipo de mensaje ARP***	*MAC origen*	*IP origen*	*MAC destino*	*IP destino*	*Observaciones*
1	*PC_A*	*ARP Request*	*MAC_A*	*10.0.0.1*	*0 (en las consultas no se conoce)*	*10.0.0.254*	*- próximo salto para alcanzar a PC_B es 10.0.0.254 - en el encabezado de 802.3/Ethernet el destino es FF:FF:FF:FF:FF:FF - "Who has 10.0.0.254?" - R_1 guarda en el caché de ARP la asociación [10.0.0.1;MAC_A] - Solo R_1 guarda/actualiza en su caché ARP la asociación [10.0.0.1;MAC_A] - El resto de las estaciones no modifican su caché de ARP*
2	*R_1 (conexión a SW_1)*	*ARP Response*	*MAC_R_1_1*	*10.0.0.254*	*MAC_A*	*10.0.0.1*	*- R_1 retorna su dirección MAC en el dominio de bradcast de SW_1. - en el encabezado de 802.3/Ethernet el destino es unicast MAC_A - "10.0.0.254 is at MAC_R_1_1" - PC_A guarda en el caché de ARP [10.0.0.254;MAC_R_1_1]*

Los mensajes que se muestran en la tabla asumen que no hay entradas en los caché ARP de PC_A y de R_1.

En el caso del ejemplo, PC_A usará el algoritmo Longest Prefix Match y encontrará que el destino 10.1.0.1 (IP_B) está incluido en la segunda entrada de la tabla y por tanto deberá entregar el paquete al equipo con IP 10.0.0.254 para que lo haga llegar al destino. Esa IP de R_1, 10.0.0.254, está directamente conectada, por lo que PC_A necesitará conocer su dirección MAC para poder enviarle una trama conteniendo el paquete que desea enviar a B. Como no hay información relevante en el caché de ARP, entonces tendrá que averiguar la MAC de R_1.

Para averiguar la MAC asociada a 10.0.0.254 envía una trama destinada en ethernet a broadcast (FF:FF:FF:FF:FF:FF) conteniendo una consulta ARP (mensaje #1 de la tabla) preguntando por la MAC

asociada a la IP 10.0.0.254 (e incluyendo su propia asociación MAC_A, IP_A). El switch reenvía esta trama por todas las interfaces (ya que el destino es broadcast). Todos los equipos la reciben, pero solo responde el R_1 porque es el que tiene configurada la IP buscada (10.0.0.254). La respuesta ARP será una trama con MAC de origen la del router (MAC_R_1_1) y MAC de destino la de PC_A (MAC_A). El router guarda en su caché de ARP la correspondencia MAC_A, IP_A. El switch almacena en su tabla de macs la asociación entre la dirección MAC de origen de los mensajes y la interfaz del switch por la que ingresaron (más detalles en Pregunta 2). Cuando PC_A recibe esta respuesta, guarda en su caché de ARP la correspondencia entre MAC_R_1_1 e IP_R_1.

Una vez que PC_A obtuvo la MAC_R_1_1, puede generar la trama para enviar el paquete IP a PC_B. El paquete tendrá como origen IP_A y destino IP_B y la trama ethernet tendrá como origen MAC_A y como destino MAC_R_1_1.

c) Explique qué es el caché de ARP y por qué es útil.

El ARP caché es una tabla de información temporal que almacena las asociaciones de dirección IP a dirección MAC que se fueron obteniendo mediante consultas ARP previas, con una determinada persistencia de tiempo.

IP:MAC:tiempo

Normalmente cuando se intercambia una trama entre dos estaciones es altamente probable que se intercambien más tramas en los próximos segundos, lo cual nuevamente requerirá conocer la dirección MAC de la estación destino asociada a la IP. El caché de ARP permite que las próximas tramas a la misma estación destino, no requieran nuevas consultas ARP, ahorrando el tiempo y recursos de red que insume la consulta.

El tiempo de persistencia de la entrada garantiza dos cosas: la primera es que si se cambia por rotura una placa de red, la estación tendrá otra dirección MAC para la IP de la interfaz, la entrada vigente en los ARP caché expirarán y se actualizará al nuevo valor de MAC; la segunda es que ayuda a que el caché de ARP tenga un "tamaño" (cantidad de entradas) razonable y no insuma mucha memoria.

El caché de ARP es por medio multiacceso, esto quiere decir que cualquier dispositivo que cuente con varias interfaces en redes diferentes, tendrá una tabla por cada interfaz, por lo general se implementa extendiendo una columna adicional que indique el nombre de la interfaz por la cual accede a dicho medio compartido.

IP:MAC:tiempo:interfaz

***Nota:** No todas las entradas del caché ARP se obtienen de forma dinámica (mediante consultas ARP), la asociación de la dirección MAC local a la IP local es fija y no cambia a menos que cambiemos la placa de red o la dirección IP. Existe el concepto de "estado" en la entrada del caché ARP, por ejemplo dinámico (entrada vigente por consulta de ARP), interfaz (interfaz física), estática (asociación forzada por configuración), incompleta (se envió el ARP request pero no se recibió el response), etc.*

***Nota2:** En las tablas de ARP no se actualiza el tiempo de validez por la existencia de tramas intercambiadas que no sean de Protocol-Type ARP.*
Podemos considerar que ARP es una "aplicación" independiente, que solo aprende de lo que se intercambia dentro de los mensajes ARP. Por ejemplo esto justifica el porque en las consultas enviamos la asociación IP, MAC de quién consulta y no solo la IP (la "entidad" ARP no puede ver los encabezados de la trama).
Con este modelo la aplicación ARP no tiene conocimiento de las tramas intercambiadas con Prootocol-Type IP, o cualquiera diferente de ARP.

Pregunta 2 (10 puntos)

a) Explique detalladamente el funcionamiento de los switches para redes 802.3 (Ethernet).
Incluya en su respuesta al menos los siguientes aspectos:
- En qué capa del modelo actúan
- Qué tablas manejan y cómo las actualizan.
- Qué decisiones y acciones toman ante la recepción de una trama.
- Por qué las entradas de la tabla utilizan temporizadores
- Cómo se utilizan esos temporizadores

La función de los switches Ethernet es interconectar múltiples interfaces Ethernet (posiblemente de distintas velocidades y medios físicos). Esta interconexión es mucho mejor que lo que podría implementarse con un repetidor de capa 1. El switch es un dispositivo de capa 2 (subcapa MAC) por lo que entiende el formato de las tramas. Un switch permite típicamente que varias parejas de equipos se comuniquen entre si simultáneamente y que lo puedan hacer a "velocidad de línea". Esto significa que en un switch con interfaces de 100 Mbps, podría tener tráfico entre dos equipos A y B a 100 Mbps y entre otros dos equipos C y D, también a 100 Mbps simultáneamente. Para esto la velocidad interna del backplane del switch debe tener la capacidad de manejar todas las parejas de equipos simultáneamente a la máxima velocidad de las interfaces.
Para lograr esto, la idea es enviar las tramas solamente a la interfaz donde se encuentra el equipo destino de la trama, evitando reenviar tramas innecesariamente a otros equipos conectados al switch, lo que a su vez requiere saber qué equipo está conectado a cada interfaz.
Para saber qué equipo (que dirección MAC) está conectada a cada interfaz sin necesidad de intervención administrativa para configurarlo, los switches Ethernet utilizan la función de autoaprendizaje para crear una tabla que asocia cada dirección MAC con la interfaz donde está conectada (tabla de direcciones MAC). El switch aprende estas asociaciones a partir de analizar la dirección MAC de origen de las tramas recibidas por cada interfaz. Las entradas en la tabla de macs, tienen un tiempo de vida, para que la tabla solamente mantenga los equipos activos, eliminándose de forma automática las entradas inactivas.

El procesamiento que realiza un switch cuando recibe una trama es:

i. Verifica la suma de comprobación (opcional) y descarta la trama si no es válida.
ii. Si la dirección MAC de origen de la trama no está presente en la tabla, se agrega asociándola con la interfaz de ingreso y se establece un tiempo de validez.
iii. Si la dirección MAC de origen ya está en la tabla, se actualiza el tiempo de validez y se actualiza la interfaz si fuera necesario (el equipo podría haberse cambiado de interfaz por un administrador).
iv. Si la dirección MAC de destino es una dirección "unicast" (es de un equipo) y ya está incluida en la tabla de macs, el switch sabe en qué interfaz está conectado el destino y envía la trama solamente por esa interfaz de salida. En caso que la interfaz de salida coincida con la de entrada, se descarta la trama.
v. Si la dirección MAC de destino es una dirección "unicast" (es de un equipo) y no está includa en la tabla de macs, el switch no sabe en qué interfaz está conectado el destino y por tanto envía la trama por todas sus interfaces excepto por la que ingresó.
vi. Si la dirección MAC de destino es broadcast (FF:FF:FF:FF:FF:FF) entonces la trama se reenvía por todos las interfaces del switch, excepto por la que ingresó.
vii. Si la dirección MAC de destino es multicast, el procedimiento puede variar entre switches, pero generalmente implica el reenvío por los todos los puertos restantes.

Si el switch tiene la capacidad de implementar VLANs (Virtual LANs), la tabla de macs incluye el número de VLAN de cada interfaz, de modo que la difusión de tramas se limite a los puertos correspondientes a cada VLAN.

Pregunta 3 (7 puntos)

Considere la descripción de la red de la Figura 1 del primer párrafo de la Pregunta 1.
Suponga que todos los equipos se acaban de iniciar y por tanto no tienen información previa almacenada.
Suponga que PC_A envía un paquete IP a PC_B y que PC_B le responde con un paquete que llega a PC_A.
Nota: Si respondió las Preguntas 1 y 2, no es necesario repetir las explicaciones detalladas.

a) Explique si los equipos PC_X y PC_Y reciben tramas de las que se intercambian en la red a raíz de ese paquete enviado. En caso que reciben alguna trama, debe justificarse cuál o cuáles de ellos reciben cuáles tramas.

De acuerdo a lo explicado en la pregunta 1 cuando se envía un paquete de PC_A a PC_B y una respuesta de PC_B a PC_A, se requiere intercambiar las siguientes tramas:

#	LAN	Ethernet Origen	Ethernet Destino	IP origen	IP destino	Cometido
1	de A	MAC_A	FF:FF:FF:FF:FF:FF	-	-	De su tabla de forwarding A sabe que para llegar a B necesita enviar el paquete a 10.0.0.254. A consulta por ARP la MAC de R_1. En el mensaje ARP además va la pareja (MAC_A, IP_A)
2	de A	MAC_R_1_1	MAC_A	-	-	Respuesta ARP de R_1 indicando su MAC_R_1_1
3	de A	MAC_A	MAC_R_1_1	IP_A	IP_B	Envío de paquete IP
4	de B	MAC_R_1_2	FF:FF:FF:FF:FF:FF	-	-	R_1 recibe la trama anterior y ve que es para su MAC, pasa el contenido de la trama a la capa 3 que observa que la dirección del paquete no es para ninguna de sus IPs (es para IP_B). Como es un enrutador, debe enviar el paquete al destino y por tanto consulta su tabla de forwarding para saber cómo enviarlo. De la tabla surge que B está directamente conectado y por tanto debe consultar por ARP cuál es la MAC asociada a IP_B. En el mensaje ARP va su correspondencia (MAC_R_1_2, 10.1.0.254)
5	de B	MAC_B	MAC_R_1_2	-	-	Respuesta ARP de B indicando su MAC_B.
6	de b	MAC_R_1_2	MAC_B	IP_A	IP_B	Envío de paquete IP

De acuerdo a lo explicado en la pregunta 2:

i. *La trama 1 está destinada a broadcast por lo que el SW_1 la hace llegar a R_1 y PC_X. SW_1 aprende la interfaz en que está conectada MAC_A (y lo agrega a su tabla de macs)*
ii. *La trama 2 está destinada a MAC_A y solo la recibe PC_A porque en el paso 1, SW_1 aprendió la interfaz donde está conectado MAC_A. Además SW_1 aprende dónde está conectado R_1. La trama no llega a PC_X.*
iii. *La trama 3 va destinada a MAC_R_1_1. Al recibirla SW_1 refresca el tiempo de validez de la entrada que asocia la interfaz donde se conecta A con MAC_A y del paso anterior sabe dónde está conectado MAC_R_1_1. La trama no llega a PC_X.*
iv. *La trama 4 (idem i), llegará a PC_Y y a PC_B.*
v. *La trama 5 (idem ii), no llegará a PC_Y*
vi. *La trama 6 (idem iii), no llegará a PC_Y*

Observar que los mensajes de broadcast y los mensajes de ARP no se rutean, por lo que obviamente las tramas 1, 2 y 3 no llegan a PC_Y (ni a PC_B) y las tramas 4, 5 y 6 no llegan a PC_X (ni a PC_A).

b) Indique concretamente qué información aprende cada equipo de la red (PCs, Switches, Router) luego de completado el envío del paquete y en qué tabla lo almacena.

#	LAN	Ethernet Origen	Ethernet Destino	IP origen	IP destino	¿Qué se aprende y dónde?
1	de A	MAC_A	FF:FF:FF:FF:FF:FF	-	-	SW_1 aprende a qué interfaz está conectada MAC_A en su tabla de MACs. R_1 aprende la correspondencia MAC_A, IP_A en su tabla de ARP
2	de A	MAC_R_1_1	MAC_A	-	-	SW_1 aprende a qué interfaz está conectada MAC_R_1_1 en su tabla de MACs. A aprende la correspondencia MAC_R_1_1, IP_R_1_LANA en su tabla de ARP
3	de A	MAC_A	MAC_R_1_1	IP_A	IP_B	SW_1 refresca el tiempo de vida de la entrada de MAC_A en su tabla de MACs.
4	de B	MAC_R_1_2	FF:FF:FF:FF:FF:FF	-	-	SW_2 aprende a qué interfaz está conectada MAC_R_1_2 en su tabla de MACs. B aprende la correspondencia MAC_R_1_2, IP_R_1_LANB en su tabla de ARP
5	de B	MAC_B	MAC_R_1_2	-	-	SW_2 aprende a qué interfaz está conectada MAC_B en su tabla de MACs. R_1 aprende la correspondencia MAC_B, IP_B en su tabla de ARP.
6	de b	MAC_R_1_2	MAC_B	IP_A	IP_B	SW_2 refresca el tiempo de vida de la entrada de MAC_B en su tabla de MACs.

c) Imagine que la información aprendida por los switches tiene una validez (tiempo de vida) de 300 segundos (5 minutos) y la información aprendida por los restantes equipos tiene una validez de 600 segundos (10 minutos).
Explique en cada uno de los siguientes escenarios si los equipos PC_X y PC_Y reciben tramas relacionadas con un segundo paquete enviado por PC_A a PC_B si:

i. El segundo paquete de PC_A a PC_B se envía 1 minuto después de enviado el primero
ii. El segundo paquete de PC_A a PC_B se envía 6 minutos después de enviado el primero

En el caso i. los tiempos de vida de todas las tablas aún no expiraron, por lo que el envío solo pasa por los equipos involucrados y no hay mensajes de ARP. PC_X y PC_Y no ven ninguno de los intercambios. Las tramas en este caso serían solamente las del paquete IP enviado en cada tramo:

#	LAN	Ethernet Origen	Ethernet Destino	IP origen	IP destino	Cometido
1	de A	MAC_A	MAC_R_1_1	IP_A	IP_B	Envío de paquete IP. SW_1 sabe dónde está MAC_R_1_1 y re-envía la trama solo a R_1. PC_X no la recibe.
2	de B	MAC_R_1_2	MAC_B	IP_A	IP_B	Envío de paquete IP. SW_2 sabe dónde está MAC_B y re-envía la trama solo a B. PC_Y no la recibe.

En el caso ii. cuando se envía el segundo paquete las tablas de ARP no expiraron por lo que no es necesario intercambiar mensajes de ARP. Pero como las tablas de MAC de los switches expiraron, no sabrán en qué interfaz están las MACs destino y deberán inundar las tramas por todas la interfaces (excepto la de entrada).

#	LAN	Ethernet Origen	Ethernet Destino	IP origen	IP destino	Cometido
1	de A	MAC_A	MAC_R_1_1	IP_A	IP_B	Envío de paquete IP. SW_1 no sabe dónde está MAC_R_1_1 y re-envía por todas las interfaces menos por la de entrada. PC_X recibe la trama, pero la ignora porque no está destinada a su MAC. Obviamente R_1 también la recibe y la procesa porque está destinada a una de sus MACs.
2	de b	MAC_R_1_2	MAC_B	IP_A	IP_B	Envío de paquete IP. SW_2 no sabe dónde está MAC_B y re-envía por todas las interfaces menos por la de entrada. PC_Y recibe la trama, pero la ignora porque no está destinada a su MAC.

Pregunta 4 (7 puntos)

Considere la red de la Figura 2 donde todas las tablas de forwarding están bien configuradas, excepto la de A indicada en la Tabla 1.
Un ping desde A logra acceder a todos los destinos, salvo a dirección de la interfaz 2 del Router 3 (if2, R_3).

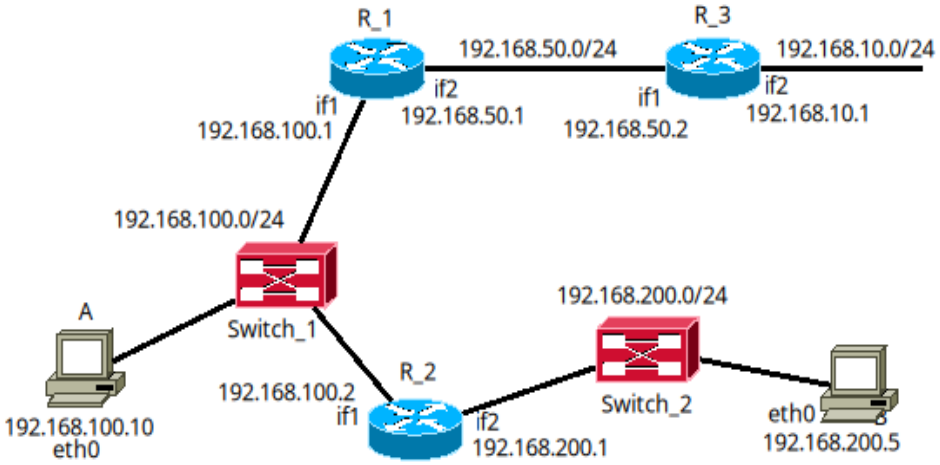

Figura 2

Destino	Máscara	Próximo salto
192.168.100.0	24	Directamente conectada en eth0
192.168.50.0	24	192.168.100.1
192.168.200.0	24	192.168.100.2
192.168.10.0	24	192.168.50.2

Tabla 1: tabla de forwarding de A

a) Explicar cuál es el error en la tabla de forwarding de A que impide la conectividad con la red 192.168.10.0/24 y proponer una corrección que logre conectividad con todos los destinos.

El error es que la IP del próximo salto asociada al rango 192.168.10.0/24 (192.168.50.2 según la tabla) no está directamente conectada al equipo A. En efecto, el próximo salto en una tabla siempre tiene que ser una dirección accesible directamente, esto permite asegurar que el salto es alcanzable, y que su dirección MAC asociada va a poder ser encontrada por los mecanismos típicos de ARP. Notar que en un caso real típicamente no podríamos configurar una tabla así ya que el sistema operativo no nos permitiría (obtendríamos un error).

Para corregir el error debería modificarse la entrada poniendo como próximo salto la dirección IP 192.168.100.1.

b) Una vez corregida la tabla de forwarding de A de acuerdo a la respuesta realizada en la parte a), ¿es posible agregar o sumarizar (ver Nota) en una sola entrada las dos entradas que indican las rutas para los destinos 192.168.50.0/24 y 192.168.10.0/24 manteniendo la conectividad con los restantes destinos?
Si es posible, indique cómo quedaría la entrada sumarizada teniendo en cuenta que el rango resultante sea el más pequeño posible. Si no es posible la sumarización, explique por qué.

La tabla de A corregida en la parte (a) quedaría:

Destino	***Máscara***	***Próximo salto***
192.168.100.0	*24*	*Directamente conectada en eth0*
192.168.50.0	*24*	*192.168.100.1*
192.168.200.0	*24*	*192.168.100.2*
192.168.10.0	*24*	*192.168.100.1*

Como se observa en la nueva tabla hay dos entradas que tienen el mismo próximo salto y por tanto es posible sumarizarlas, para esto se debe encontrar el rango más pequeño que contenga esos dos rangos. Para eso hay que analizar el tercer byte de ambas redes /24.
Para la red 192.168.50.0/24 el tercer byte (50) expresado en binario es: 00110010
Para la red 192.168.10.0/24 el tercer byte (10) expresado en binario es: 00001010
Por tanto un rango que incluya esos dos rangos tendría máscara /18 ya que a partir del bit 19 ya tienen diferencias.
La nueva tabla con la entrada sumarizada y ordenada por largo de máscara quedaría:

Destino	***Máscara***	***Próximo salto***
192.168.100.0	*24*	*Directamente conectada en eth0*
192.168.200.0	*24*	*192.168.100.2*
192.168.0.0	*18*	*192.168.100.1*

Con esta tabla, todos los destinos continúan siendo alcanzables.
El inconveniente que presenta es que además de los rangos 192.168.50.0/24 y 192.168.10.0/24, hay más rangos incluidos en el /18 y por tanto si se envían paquetes a direcciones de esos rangos extra, van a llegar a R_1 (y eventualmente R_3, dependiendo de la tabla de R_1), donde no habrá rutas a esas direcciones y los paquetes serán descartados más adelante cuando se podrían haber descartado en A.

c) En lugar del cambio indicado en la parte b), alguien propone sustituir la entrada correspondiente a estas dos redes por una ruta por defecto (d*estino 0.0.0.0/0, próximo salto 192.168.100.1)*. El resto de las entradas de la tabla se mantienen igual. Explicar si con esa solución se tiene conectividad con todos los destinos o no. ¿Si esa solución es adecuada, qué desventajas presenta?. Justifique su respuesta.

La solución de una ruta por defecto también es válida, con la misma salvedad o desventaja comentada en la parte b). Los paquetes originados por A y destinados a cualquier destino inexistente en esta red, llegarán a R_1 que deberá procesarlos y eventualmente descartarlos, cuando se podrían haber descartado en A.

Notar que la ruta por defecto incluye todos los destinos, y en particular por lo tanto el destino 192.168.200.0/24. Para alcanzar dicho destino el próximo salto es 192.168.100.2 y no 192.168.100.1, como el indicado en la ruta por defecto. Sin embargo, esto no genera problemas de conectividad ya que el algoritmo utilizado para buscar en la tabla es el conocido como "longest prefix match" , es decir que para buscar la entrada correspondiente a un cierto destino en la tabla primero se consideran los prefijos más largos (con máscara más grande). Teniendo en cuenta esto se buscan coincidencias de cada línea (teniendo en cuenta destino y máscara) y la IP destino indicada en el paquete. No hay riesgos por lo tanto de que un paquete dirigido a la red 192.168.200.0/24 sea dirigido al próximo salto 192.168.100.1 ya que la primera entrada que coincidirá en la búsqueda es aquella con destino 192.200.0/24 y no la ruta por defecto.

Nota: "Agregar" o "sumarizar" en este contexto significa definir un rango de direcciones que comprenda dos o más rangos de menor tamaño.

Pregunta 5 (8 puntos)

En la criptografía asimétrica o de clave pública:

a) ¿Cuál es el cometido de un certificado digital de clave pública? ¿Cuál es la principal información que se obtiene de un certificado de clave pública?

El principal cometido de los certificados de clave pública es la certificación de la relación entre una clave pública y una identidad (por ejemplo nombre, URL, dirección de correo u otros).
Un certificado es emitido por una Autoridad de Certificación (CA), la cual asegura que la clave pública pertenece a la entidad cuya identidad se indica en el certificado. La CA es la encargada de verificar esta información (que la identidad es correcta, que posee la clave privada correspondiente a la clave pública, etc.), y firma el certificado con su clave privada (de la CA) para garantizar la integridad de la información distribuida.
La principal información que se obtiene es justamente esta relación entre la clave pública y la identidad. Esto permite la distribución confiable de claves públicas.
El certificado incluye otra información útil, como el período de validez del certificado, usos permitidos para la clave pública, algoritmo para el cual es válida la clave pública, etc.

b) ¿Cómo se valida un certificado de clave pública? ¿Qué información se necesita para poder validarlo?

Los certificados de clave pública deben estar firmados por la autoridad de certificación. Para validar el certificado se valida esta firma, en caso de ser correcta nos garantiza (dentro de lo que es seguridad computacional) que la autoridad de certificación es la entidad que firmó el certificado y que la información incluida en el mismo no fue modificada. Entonces si confiamos en esa autoridad de certificación, aceptaremos la información como válida.
Para poder validar el certificado se requiere la clave pública de la Autoridad de Certificación que emitió el certificado

c) Al intentar ingresar a una página web el navegador indica que existe un problema de seguridad al validar el certificado. Indique qué problemas puede haber tenido al intentar validar el certificado.

Debemos validar tanto el certificado como la información contenida en él. Entonces algunos posibles problemas que pueden surgir al momento de validar el certificado son:
- *Imposibilidad de validar la firma del certificado, por no poseer la clave pública correspondiente a la CA. Esto indica que fue firmado por una CA en la cual no confiamos*
- *Error al validar la firma. Esto nos indica que el contenido del certificado puede haber sido manipulado y por tanto no se puede confiar en esta información*
- *Diferencia entre el nombre de la entidad con la que nos estamos conectando y el nombre que figura en el certificado. Esto podría indicar que no nos estamos conectando al sitio correcto (por ejemplo un phishing), o un error del administrador del sitio*
- *La fecha actual no se encuentra dentro del período de validez del certificado*
- *El certificado se encuentra en una lista de revocación (este problema no se discutió en clase en 2024)*
- *Otras validaciones que fallan (usos admitidos no incluyen la aplicación en uso, algoritmos no seguros...)*