Redes de Computadoras

Segundo Parcial – 27 de noviembre de 2019

(ref: prc20191127.odt)

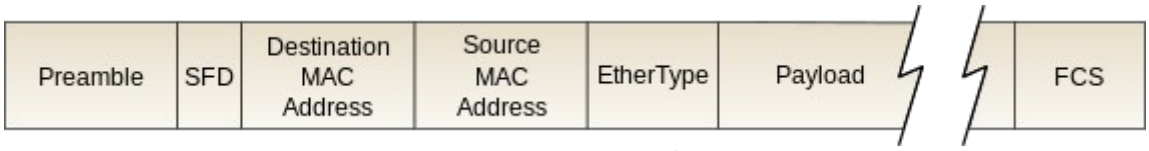
Instrucciones

• Indique su nombre completo y número de cédula en cada hoja.
• Numere todas las hojas e indique en la primera la cantidad total de hojas que entrega.
• Escriba las hojas de un solo lado y utilice una caligrafía claramente legible.
• Comience cada pregunta en una hoja nueva.
• Sólo se responderán dudas de letra. No se responderán dudas de ningún tipo durante los últimos 30 minutos de la prueba.
• La prueba es individual y sin material. Apague su teléfono celular mientras esté en el salón de la prueba.
• Duración: 2 horas. Culminadas las 2 horas, el alumno no podrá modificar de ninguna forma las hojas.
• Justifique todas sus respuestas.

Pregunta 1 (10 puntos)

a) Enumere y describa los campos de la trama Ethernet.
b) Describa el algoritmo de acceso al medio utilizado por Ethernet.
c) Describa el concepto de auto-aprendizaje (*self-learning*) que implementan los switches Ethernet.

Solución
a)



Preamble: 7 bytes con el patrón 10101010 seguido de un byte con el patrón 10101011(SDF). Se utiliza para sincronizar los relojes del receptor y emisor
Addresses: 6 bytes (Destination MAC Addres y Source MAC Address). Cuando una interfaz recibe una trama con Destination MAC Address igual a su dirección MAC o con dirección broadcast (FF-FF-FF-FF-FF-FF), entonces transfiere la trama a la capa de red, en caso contrario lo descarta.
EtherType: indica el portocolo que contiene el **payload** (por ejemplo IP, pero pueden ser otros, por ejemplo., Novell IPX, AppleTalk)
Payload: datos transportados por la trama (correspondientes a protocolos de capas superiores)
FCS: permite que el receptor haga chequeo de errores. En caso de existir errores, la trama se elimina.

b)
Ethernet utiliza **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) . El algoritmo tiene el siguiente comportamiento:
1. Cuando la tarjeta de red (NIC – Network Interface Card) recibe un datagrama de la capa de red, crea una trama.
2. Si la NIC detecta que el canal está disponible, comienza la transmisión de la trama. Si detecta que el canal está ocupado, espera hasta que se libere y entonces transmite la trama.
3. Si la NIC logra transmitir la totalidad de la trama sin detectar otra transmisión (sin colisión), entonces la transmisión se realizó con éxito.
4. Si la NIC detecta otra transmisión mientras se encuentra transimitiendo el frame, entonces aborta el envío y envía una "jam signal" (señal de duración 48 bits que permite informar al resto de los hosts que existió una colisión)
5. Después de abortar el envío la NIC realiza un "exponential backoff", que consiste en sleccionar un K en forma aleatoria, con valores entre {0,1,2,…,2m-

1}, espera K*512 tiempos de bit, y vuelve al paso 2.

c)
El objetivo del self-learning es identificar que dispositivos son alcanzables en cada interfaz del switch, y consiste en construir una tabla con 3 columnas: **<MAC, interfaz, ttl>**.
Cuando se recibe una trama, el dispositivo aprende que la MAC del origen puede ser encontrada en la interfaz de entrada, y esta información es agregada en la tabla del switch. El campo ttl es utilizado para mantener la información durante cierto tiempo y después eliminarla.

Pregunta 2 (10 puntos)

a) ¿Qué función cumple el protocolo ARP (Address Resolution Protocol) en IPv4? Describa brevemente cómo funciona, y en particular, qué mensajes se intercambian.
b) ¿Qué mecanismo sustituye esta funcionalidad en IPv6? Describa brevemente cómo funciona, y en particular, qué mensajes se intercambian.

Solución

a) El protocolo ARP (Address Resolution Protocol), permite determinar la dirección MAC de una interfaz de red que tiene configurada cierta dirección IP. Cada nodo en la red (ya sea un host o un router) presenta una tabla ARP. Esta tabla contiene registros con los siguientes campos: dirección IP, dirección MAC y TTL (Time to live), para los nodos de la subred a la que pertenece (LAN): **<IP, MAC, TTL>**, donde el TTL indica después de que tiempo es eliminado el registro.

   Ejemplo de funcionamiento:

   • Cuando el host con dirección IP **A** desea enviar un datagrama al host con dirección IP **B**, y la dirección MAC de B no se encuentra en la tabla ARP de A, debe realizar los siguientes pasos:

   • Envía una trama ethernet cuyo payload transporta un mensaje **ARP request** que contiene la dirección IP de B, y las direcciones IP y MAC de A (el emisor). La trama se envía a la dirección de **broadcast** (FF:FF:FF:FF:FF:FF), y por lo tanto es recibida por todos los nodos de la LAN.

   • Cuando B recibe el mensaje **ARP request**, lo responde con un mensaje **ARP response** al equipo A con su dirección MAC. Este mensaje es enviado en forma unicast a la dirección MAC de A.

   • El host A inserta la correspondencia <IP B, MAC B, TTL> en su tabla ARP; esta entrada expira cuando transcurre el tiempo TTL.

b) La funcionalidad equivalente a ARP en IPv6 es implementada como parte del **Neighbor Discovery Protocol** (ND), que provee servicios adicionales a la simple resolución del mapeo IP→MAC. El equivalente a ARP es implementado solamente con el intercambio de mensajes **ND Solicitation** y **ND Response**, equivalentes a ARP request y ARP Response. Cada nodo en la red (ya sea un host o un router) presenta una tabla de vecinos (neighbors). Ésta tabla contiene registros con los siguientes campos: **dirección IP**, **dirección MAC**, **interfaz** y **TTL** (Time to live), para los nodos de su LAN, donde el TTL indica después de cuanto tiempo debe eliminarse el registro. La interfaz

es necesaria para resolver ambigüedades con las direcciones de tipo link local.

Ejemplo de funcionamiento:

- Cuando el host A desea enviar un datagrama al host B, y la dirección MAC de B no se encuentra en la tabla de vecinos, debe realizar los siguientes pasos:

- Envía un mensaje ICMPv6 de tipo Neighbor Solicitation, que en la cabecera IPv6 lleva las siguientes direcciones: la propia en el origen, y la dirección de multicast de todos los nodos del segmento ff02::1 en el campo destino (siendo precisos, ff02::1:ff concatenado con los 3 últimos bytes de la dirección que estamos averiguando). A nivel de la cabecera Ethernet, se coloca como origen la dirección MAC asociada a la dirección por donde se envía el paquete y la dirección MAC correspondiente a la dirección de multicast, (siendo precisos, la MAC 33:33?: concatenado con los 3 últimos bytes de la IPv6 que estamos averiguando). En el payload del mensaje ICMPv6 se coloca la dirección IPv6 que estamos averiguado, así como, la MAC origen. Este mensaje es recibido por todos los nodos de la LAN.

- Cuando B recibe el paquete Neighbor Solicitation, lo contesta con un Neighbor Advertisement, que en la cabecera IPv6 lleva las direcciones IPv6 de ambos hosts, en la cabecera Ethernet van las MAC correspondientes de ambos. El Payload IPv6 es de tipo ICMPv6, indicando la TargetAddress igual a la IPv6 Origen; este mensaje es enviado en forma unicast. El host A graba la correspondencia IP(B),MAC(B) en la tabla ARP hasta que pase el TTL.

Pregunta 3 (5 puntos)

Explique que función cumple y como funciona el mecanismo de *Reverse Path Forwarding* (RPF).

Solución

En el contexto de enrutamiento broadcast o multicast, Reverse Path Forwarding (RPF) es un mecanismo de inundación (flooding) controlado, que permite determinar por qué enlaces se va a reenviar un mensaje de difusión. Cuando un nodo recibe un mensaje desde una fuente, lo reenviará por todos sus enlaces excepto por donde llegó, solo si dicho enlace está en el camino unicast más corto desde el nodo a la fuente; en otro caso, descartará el mensaje, implementando inundación controlada, como se dijo anteriormente.

Pregunta 4 (10 puntos)

a) Suponga que un paquete IP ingresa a un router y que la respuesta del mismo es un ICMP Network unreachable, ¿a qué se debe?

b) Suponga que un paquete IP ingresa a un router y que la respuesta del mismo es un ICMP Host unreachable, ¿a qué se debe?

c) Suponga que un paquete con IP destino 192.168.1.64 ingresa a un router, cuya tabla contiene los siguientes prefijos: 192.168.0.0/23, 192.168.1.0/26 y 192.168.1.0/24. Muestre una simulación de ejecución paso a paso del LPM para ese escenario.

Solución

a) Se debe a que la dirección IP de destino no corresponde a ninguna de las direcciones IP configuradas en alguna interfaz del router, y tampoco hay coincidencia con ninguna de las entradas de la tabla de forwarding al realizar el LPM.

b) Se debe a que si bien la IP de destino corresponde a un prefijo de red que es alcanzable de acuerdo al contenido de la tabla de forwarding, luego al realizar el intento de enviar ese paquete no se encuentra el host de destino, por ejemplo porque no se logra resolver el ARP.

c) IP DEST=11000000 10101000 00000001 01000000

Paso 1) Enmascaro red destino y comparo con IP destino enmascarada (en ambos casos me quedo con los 23 bits mas significativos)

11000000 10101000 0000000 << Fila 1 enmascarada

11000000 10101000 0000000 << IP destino enmascarada

Hay coincidencia, y tomo por ahora que es la mejor con el prefijo de largo 23.

Paso 2) Enmascaro red destino y comparo con IP destino enmascarada (en ambos casos me quedo con los 26 bits mas significativos)

11000000 10101000 00000001 0**0** << Fila 2 enmascarada

11000000 10101000 00000001 0**1** << IP destino enmascarada

Difieren en el último bit, no hay coincidencia.

Paso 3) Enmascaro red destino y comparo con IP destino enmascarada (en ambos casos me quedo con los 24 bits mas significativos)

11000000 10101000 00000001 << Fila 3 enmascarada

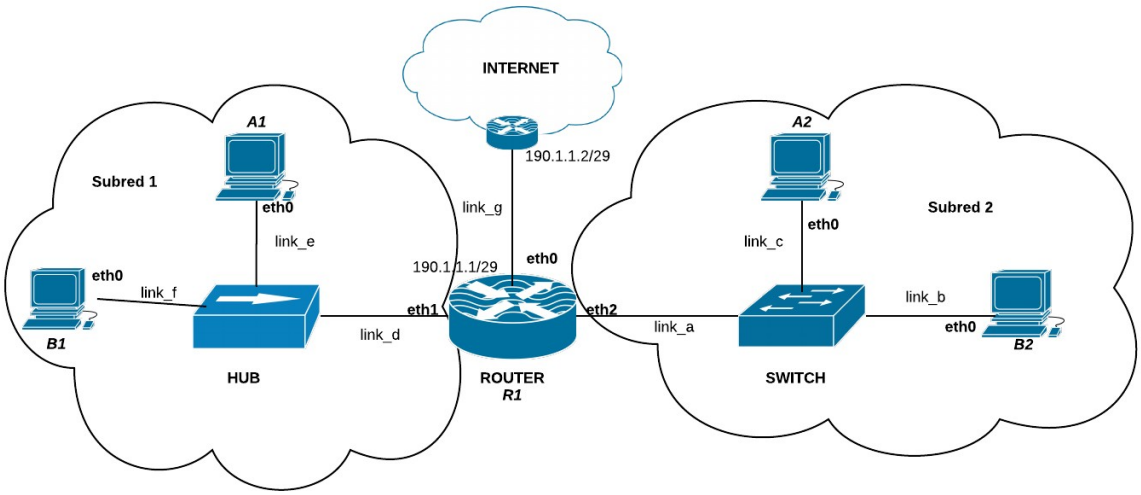
11000000 10101000 00000001 << IP destino enmascarada

Hay match, entonces comparo el largo de la máscara actual (24) con el que tenía actualmente (23), de manera que lo actualizo.

Como no hay mas entradas en la tabla, me quedo con la Fila 3, que tiene el largo de máscara mas largo, de manera que el tráfico se debería reenviar por el next-hop que indique la tabla en su Fila 3.

Problema 1 (15 puntos)

Considere la topología de la siguiente figura:



Se pide:

a) Identifique todos los dominos de broadcast y de colisión.
b) Numere todas las subredes utilizando direcciones IPv4 privadas. Debe considerar que la subred 1 debería alojar hasta 30 hosts y la subred 2 hasta 125 hosts. La asignación debe ajustarse estrictamente a estas necesidades.
c) Asigne IPs a todas las interfaces del diagrama que así lo requieran. Asigne direcciones MAC para A1 y A2.
d) Escriba las tablas de forwarding para R1, A1 y A2 de manera que haya conectividad total.
e) Describa las condiciones y configuraciones necesarias que se deben realizar en la en la red actual para que los hosts A2 y B2 puedan pertenecer a subredes diferentes sin ser movidos de su ubicación actual y sin necesidad de nuevo hardware.
Tenga en cuenta que el router R1 tiene solo tres interfaces físicas.

Solución

a)

Dominios de broadcast: Subred 1, Subred 2 y enlace router-internet.

Dominios de colisión: toda la subred 1, cada enlace del switch en la Subred 2, y el enlace router-internet.

b)

La subred 1 debe soportar hasta 30 hosts. Si a esto le sumamos la interfaz del router R1 y las direcciones de red y broadcast, son necesarias 33 direcciones. Por lo tanto voy a necesitar un prefijo /26 que me permite tener 64 direcciones.

La subred 2 debe soportar hasta 125 hosts, mas la dirección del router R1 y la dirección de red y broadcast. Es decir, necesito 128 direcciones. Por lo tanto, con un prefijo /25 es suficiente.

Numero la subred 1 con el prefijo 192.168.1.0/26 y la subred 2 con el prefijo 192.168.1.128/25

c)

Subred 1

A1 – 192.168.1.2

B1 – 192.168.1.3

R1-eth1 – 192.168.1.1

Subred 2

A2 – 192.168.1.130

B2 – 192.168.1.131

R1-eth2 – 192.168.1.129

MAC A1 – 00:00:00:00:00:01

MAC A2 – 00:00:00:00:00:02

d)

Tabla A1

Prefijo/Máscara	**Next-Hop**	**Interfaz**
192.168.1.0/26	Directamente conectado	eth0
Default (0.0.0.0/0)	192.168.1.1	eth0

Tabla A2

Prefijo/Máscara	**Next-Hop**	**Interfaz**
192.168.1.128/25	Directamente conectado	eth0
Default (0.0.0.0/0)	192.168.1.129	eth0

Tabla R1

Prefijo/Máscara	**Next-Hop**	**Interfaz**
192.168.1.0/26	Directamente conectado	eth1
192.168.1.128/25	Directamente conectado	eth2
190.1.1.0/29	Directamente conectado	eth0
default (0.0.0.0/0)	190.1.1.2	eth0

e)

Para que A2 y B2 pertenezcan a subredes diferentes es necesario configurar VLANs diferentes para cada host.
Para esto es condición necesaria que tanto el Router R1 como el switch soporten la configuración de VLANs.
En el switch se deben configurar dos VLANs, VLAN A y VLAN B.
La interfaz que conecta el link_c se agrega a la VLAN A y la interfaz que

conecta el link_b se agrega a la VLAN B.
Luego el enlace link_a se debe configurar como trunk. Para esto se deben definir dos interfaces virtuales en la interfaz física eth2 del router. Se configurarán las interfaces eth2.A y eth2.B las cuales cada una pertenecerán a la VLAN A y B respectivamente.