Redes de Computadoras

Solución - Examen – 19 de diciembre 2016

(ref: solredes20161219.odt)

Instrucciones

- **Indique su nombre completo y número de cédula en cada hoja.**
- **Numere todas las hojas e indique la cantidad total de hojas que entrega en la primera.**
- **Escriba las hojas de un solo lado y utilice una caligrafía claramente legible.**
- **Comience cada pregunta teórica y cada ejercicio en una hoja nueva.**
- **Sólo se responderán dudas de letra. No se responderán dudas de ningún tipo los últimos 30 minutos del examen.**
- **El examen es individual y sin material. Apague su teléfono celular mientras esté en el salón del examen.**
- **Es obligatorio responder correctamente al menos 15 puntos en las preguntas teóricas y 20 de los problemas prácticos. Los puntos ganados en el curso se suman a los puntos de teórico.**
- **El puntaje mínimo de aprobación es de 60 puntos.**
- **Para todos los ejercicios, si es necesario, puede suponer que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).**
- **Justifique todas sus respuestas.**
- **Duración: 3 horas. Culminadas las 3 horas el alumno no podrá modificar las hojas a entregar de ninguna forma.**

Preguntas Teóricas

Pregunta 1 (7 puntos)

a) ¿Por qué el servicio DNS no está implementado de manera centralizada?
b) Explique el formato de los *Resource Records* (RR).
c) Brinde y explique dos ejemplos de *Resource Records*.

Solución

a) Sería un único punto de falla.
El volumen de tráfico en ese único punto sería enorme.
La operación y mantenimiento de una base de datos centralizada con millones de registros sería inviable.

b) NOMBRE TTL TIPO VALOR

c)

```
www.fing.edu.uy.        551   IN    A     164.73.32.5
fing.edu.uy.            1502  IN    MX    0           smtp.fing.edu.uy.
```

Son dos registros de la clase Internet (IN).
Primer registro:

```
NOMBRE:     www.fing.edu.uy
TTL:        551
TIPO:       A
VALOR:      164.73.32.5
```

Brinda la correspondencia nombre - dirección IP
Segundo registro:

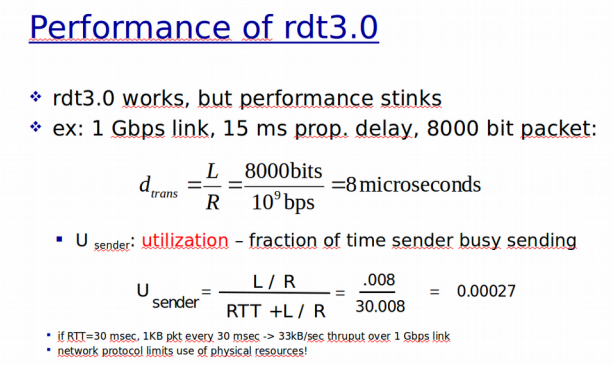
```
NOMBRE:     fing.edu.uy
TTL:        1502
TIPO:       MX
      Preferencia: 0
VALOR:      smtp.fing.edu.uy
```

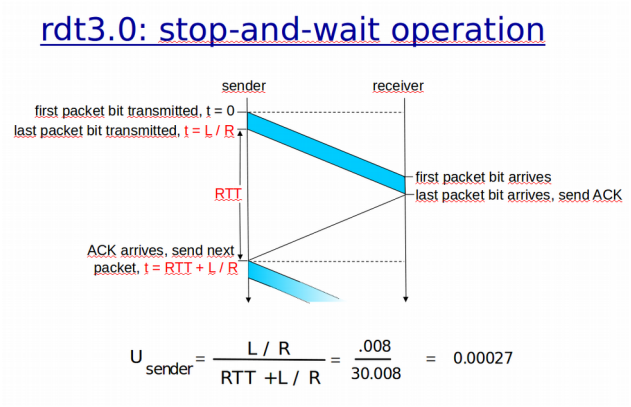
Brinda el nombre de un servidor de correo para el dominio fing.edu.uy. De existir más de un registro MX para un mismo dominio, la primera opción será la de menor valor de preferencia.

Pregunta 2 (5 puntos)

Analice el rendimiento (*performance*) del protocolo `rdt3.0` para un enlace de `1Gbps`, `15ms` de retardo de propagación y RTT de `30ms`, considerando paquetes de `1.000 bytes`.

Solución





Pregunta 3 (10 puntos)

a) Defina los términos “dominio de broadcast” y “dominio de colisión” en el contexto de redes ethernet. En qué caso estos conceptos coinciden?
b) En un contexto de medio compartido, describa al menos dos técnicas de acceso al medio. Haga énfasis en sus diferencias, explicándolas detalladamente.

Solución

a) Un “dominio de broadcast” ethernet es el conjunto de sistemas alcanzables mediante un mensaje de broadcast, es decir, cuando la dirección de destino es “todos 1” (FF:…:FF). El dominio de broadcast constituye una red de área local, y típicamente se corresponde con el concepto de “subred” en capa 3, donde todos los sistemas comparten el mismo prefijo de red. Un “dominio de colisión” es un concepto físico, y está constituído por aquellos sistemas que comparten el medio y por lo tanto pueden colisionar tramas al intentar transmitir. En redes constituídas exclusivamente por “hubs” ambos conceptos coinciden.

b) “Carrier Sense Multiple Access” con detección de colisiones (CSMA/CD) es utilizado en redes ethernet, y especifica la forma de enviar tramas al medio compartido, el mecanismo de detección de colisiones, y el algoritmo de reintento cuando se detecta una colisión (backoff exponencial).
“Aloha” es una técnica de acceso al medio inalámbrico, donde cada nodo transmite una trama cuando está disponible, y si detecta colisiones, intenta trasmitirla nuevamente con cierta probabilidad p.
Estas dos técnicas se usan en medios diferentes (cableado vs. Inalámbrico), y difieren en el mecanismo de reintento, que determina que la eficiencia de los protocolos sea muy distinta.

Pregunta 3 (redes anteriores) (10 puntos)

Describa los conceptos Exploración (*Scanning*) Pasiva y Exploración Activa de la tecnología 802.11 o WiFi.

Solución

El proceso de scanning de 802.11 o WiFi -recorriendo todos los canales disponibles- es el que permite a las estaciones (STAs) conocer los APs/SSIDs disponibles a los efectos que se pueda decidir con cuál de ellos se intentará la Asociación (trama Association Request -destinada a la MAC del AP seleccionado-, y trama Association Response -destinada a la MAC de la STA que envió la trama previa-).

Las dos modalidades de scanning disponibles son: Pasivo y Activo.

En el Pasivo, la STA “escucha” y procesa las tramas Beacon -destinadas al broadcast- emitidas periódicamente por el AP y decide con cual de ellos iniciar la Asociación o presenta la información a quién decidirá.

En el Activo, la STA genera una trama Probe Request -destinada al broadcast- que motivará a los APs que la procesen a que generen una trama Probe Response -destinada a la MAC de la STA que envió la trama previa- que contendrá, a los efectos de la Asociación, la misma información que la trama Beacon.

Pregunta 4 (8 puntos)

Explique y compare las técnicas de "Reverse Path Forwarding" y "flooding controlado por número de secuencia" que se pueden utilizar para determinar el forwarding en redes multicast/broadcast.

Solución

La técnica de "Reverse Path Forwarding" (RPF) especifica que cuando se recibe un paquete de difusión, se reenviará a todas las interfaces del nodo (excepto la interfaz de entrada) solo si el paquete arribó desde un origen que está en el caminio unicast de costo mínimo desde la interfaz de entrada, y en caso contrario, se descartará.
La técnica de "flooding controlado por número de secuencia" especifica que cuando se recibe un paquete de difusión, se reenviará a todas las interfaces del nodo (excepto la interfaz de entrada) solo si el paquete no se había recibido antes, y para esto se marcan los paquetes recibidos con un número de secuencia. En caso de paquete repetido, se descartará.
Ambas técnicas implementan el "flooding" o inundación controlada; RPF es una técnica liviana que solo necesita comprobar la tabla de forwarding del nodo, mientras que la otra técnica exige mantener estado, y consecuentemente es más costosa.

Pregunta 5 (10 puntos)

Describa el algoritmo "link state" utilizado para determinar los caminos de menor costo desde un origen a todos los destinos en una red, y explique por qué determina un árbol de cubrimiento mínimo. Es un algoritmo distribuido o centralizado?

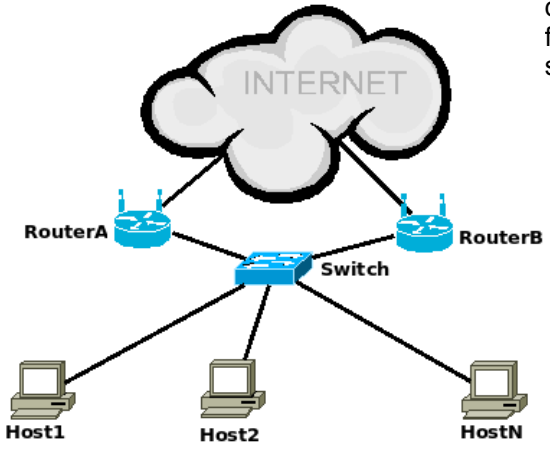
Solución

El algoritmo link-state utilizado es Dijkstra. Determina los caminos de menor costo sin ciclos desde cada nodo hacia los demás, es decir, un árbol de cubrimiento mínimo. Es un algoritmo distribuido, ya que cada nodo corre su instancia, alimentándose de la información intercambiada con los otros nodos, sin que exista una instancia de coordinación.

Problemas Prácticos

Problema 1 (30 puntos)

En la red de la figura se desea implementar un servicio de redundancia de capa de red para la salida a Internet, donde solo un router estará activo y el otro lo sustituye en caso de fallas del enlace a Internet del mismo. Se propone que funcione de la siguiente manera:



- los routers *A* y *B* utilizan una dirección IP y MAC virtual, la que debe ser asignada al router que se encuentre *activo* (solamente uno está activo a la vez).
- Los equipos Host1..HostN, se encuentran configurados con un *default gateway* que es al IP virtual mencionada en el punto anterior.
- El router que se encuentra *activo* envía mensajes de *keepalive* al otro router (por UDP a una dirección multicast conocida por ambos routers). Cuando el router *no activo* deje de recibirlos por un período de tiempo X, considerará que el router no está operativo, debiendo entrar él en operación (tomando la IP/MAC virtual).
- Cada router además tiene configurada una IP y MAC fija (conocida por el otro router) que le permite conectividad con el otro router (A o B).

Se cuenta con una variable booleana *enlace_activo*, que indica si el enlace del router con internet se encuentra funcionando. En caso de fallas, la variable pasará a FALSE, volviendo a TRUE cuando el enlace se restablezca.
Ademas existen primitivas que permiten configurar/desconfigurar una dirección IP y MAC adicional a una interface:

- *set(IP_address,MAC_address,interface)*
- *unset(IP_address,MAC_address,interface)*

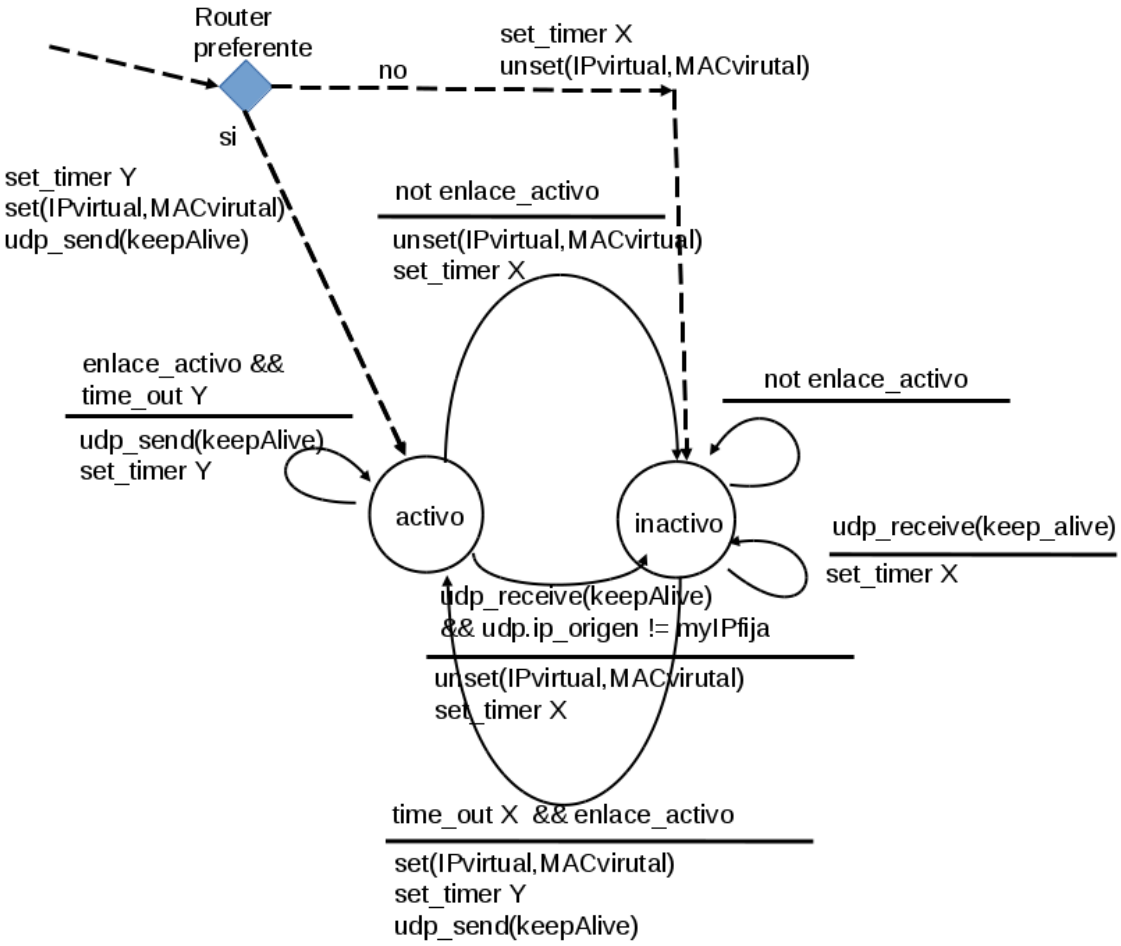
Por último se cuenta con las primitivas para el manejo de timers, así como *udp_send()* y *udp_receive()* para el manejo de UDP.

Se pide:

a) Implemente la máquina de estados del router (la misma para A y B), que permite implementar el servicio de redundancia descripto. Puede asumir que los puertos UDP son conocidos, y que se cuenta con los timers necesarios. La solución debe cuidar que los routers no estén en el mismo estado simultaneamente.
b) ¿Analice como se comporta la solución propuesta para los casos de tráfico entrante y saliente de la red?
c) Al cambiar de router la IP y MAC, ¿que cambios se generan en el switch y los PCs para que ahora el tráfico llegue al nuevo router activo en lugar de al viejo?

Solución

a) La solución propuesta supone que existe un criterio inicial Router_preferente, que indica al comienzo de las dos máquinas estará como activo y cual como inactivo.



Los keepalive se envían a la dirección de Multicast conocida, por lo que para determinar si ambos equipos se encuentran en estado activo, cuando llega un keepalive que corresponde a una IP origen diferente a la propia, indica que hay otro equipo activo, y pasa a pasivo.

En caso de encontrarse los dos equipos inactivos, como ninguno envía keepalives, entonces el primero que supere el timeout X pasará a activo, dejando un equipo en activo y otro en inactivo.

El equipo activo envía keepalives cada Y y el X chequea cada X. Para el correcto funcionamiento se debe cumplir Y < X.

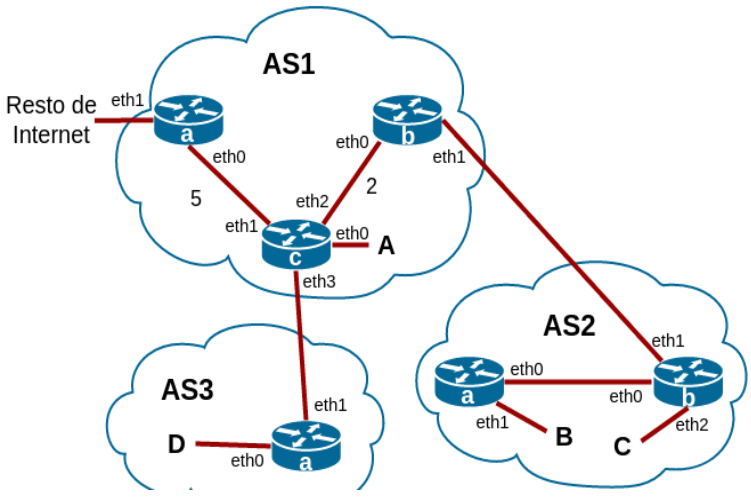
b) Para el tráfico entrante, el cambio de router no modifica nada, dado que todo el tráfico que ingrese por la interfaz conectada a internet en el router inactivo, debería ser dirigido a la LAN. Todas las consideraciones realizadas, deben conjugarse con las políticas de ruteo realizadas en Internet, que podrán involucrar acceso por un router o por los dos.

Para el tráfico saliente, el ruteo esta definido por el default gateway de los HostN, que es la IP virtual, por lo que la ruta de salida será por el router activo.

c) En el caso de cambio de router, asignando la IP/MAC virtual a el otro router, incialmente el switch no conocerá el cambio, por lo que seguirá enviando por el puerto del router que estaba antes activo. Cuando el router que pasó a ser activo envíe un frame con MAC virtual, o cuando se realice una consulta ARP, el switch notará el cambio de puerto de la MAC, e iniciará a enviar por el puerto del router que pasó a activo.

Problema 2 (30 puntos)

Considere la red de la figura.



Las subredes A, B, C y D tienen los siguientes prefijos asignados:

A) 122.0.0.0/8
B) 200.128.0.0/9
C) 200.64.0.0/10
D) 123.0.0.0/8

Se pide:

i. Asignar entradas a las tablas de forwarding de todos los routers para que haya conectividad total (inter e intra-AS), sin considerar los enlaces punto a punto entre routers. Cada tabla debe tener la menor cantidad posible de entradas. Asigne el valor "n/a" cuando no conozca la puerta de enlace. No puede asumir que las subredes mencionadas tienen un único dominio de broadcast.

ii. Se sabe que los costos en los enlaces punto a punto de los routers de AS1 son los que muestra la figura de arriba, y que corre un algoritmo vector-distancia. Ejecútelo para mostrar cómo recalcula los caminos más cortos entre los routers representados (sin tener en cuenta la subred A) al agregarse un enlace de costo 1 entre los routers a y b.

iii. Suponga que se desea enviar un segmento TCP desde la IP 122.0.10.20 a la IP 123.128.10.10. El MTU del enlace en la interfaz eth0 del router AS1c es de 4352 bytes, mientras el del enlace entre AS1 y AS3 es de 1500 bytes. El campo *length* del datagrama tiene el valor 4000, y los cabezales IP y TCP tienen el tamaño mínimo posible. Explique detalladamente (indicando el valor de los campos *length*, *ID*, *fragflag* y *offset* de los cabezales IP) qué ocurre para que el paquete pueda llegar a destino, asumiendo que el resto de los enlaces del camino tienen MTU de 4352 bytes.

Solución

i)

AS1a:

Prefijo	Enlace	Next hop
122.0.0.0/7	eth0	AS1c:eth1
200.128.0.0/9	eth0	AS1c:eth1
200.64.0.0/10	eth0	AS1c:eth1
default	eth1	n/a

AS1b:

Prefijo	Enlace	Next hop
200.128.0.0/9	eth1	AS2b:eth1
200.64.0.0/10	eth1	AS2b:eth1
default	eth0	AS1c:eth2

AS1c:

Prefijo	Enlace	Next hop
122.0.0.0/8	eth0	n/a
123.0.0.0/8	eth3	AS3a:eth1
200.128.0.0/9	eth2	AS1b:eth0
200.64.0.0/10	eth2	AS1b:eth0
default	eth1	AS1a:eth0

AS2a:

Prefijo	Enlace	Next hop
200.128.0.0/9	eth1	n/a
default	eth0	AS2b:eth0

AS2b:

Prefijo	Enlace	Next hop
200.128.0.0/9	eth0	AS2a:eth0
200.64.0.0/10	eth2	n/a
default	eth1	AS1b:eth1

AS3a:

Prefijo	Enlace	Next hop
123.0.0.0/8	eth0	n/a
default	eth1	AS1c:eth3

ii)

Antes del enlace nuevo:

Router a

	a	b	c
a	0	7	5
c	5	2	0

Router b

	a	b	c
b	7	0	2
c	5	2	0

Router c

	a	b	c
a	0	7	5
b	7	0	2
c	5	2	0

Nuevos costos a partir del enlace nuevo (aún sin intercambiar vectores-distancia)

Router a

	a	b	c
a	0	1	5
b	-	-	-
c	5	2	0

Router b

	a	b	c
a	-	-	-
b	1	0	2
c	5	2	0

Router c

	a	b	c
a	0	7	5
b	7	0	2
c	5	2	0

Intercambio de vectores:

Router a

	a	b	c
a	0	1	3
b	1	0	2
c	5	2	0

	a	b	c
a	0	1	3
b	1	0	2
c	3	2	0

Router b

	a	b	c
a	0	1	5
b	1	0	2
c	5	2	0

	a	b	c
a	0	1	3
b	1	0	2
c	3	2	0

Router c

	a	b	c
a	0	1	5
b	1	0	2
c	3	2	0

	a	b	c
a	0	1	3
b	1	0	2
c	3	2	0

iii)

El datagrama tiene 4000 bytes en total, de los cuales 20 son de cabezales IP, por lo que se deben fragmentar 3980 bytes de datos. Cada nuevo datagrama podrá ocupar 1500 bytes en total. Descontando 20 bytes de cabezales IP por datagrama, se debe dividir el original en tres: dos de 1480 bytes y uno de 1020 bytes. Se tiene entonces que en el enlace inter-ASs deben colocarse tres datagramas, con los siguientes valores:

ID	Length	Fragflag	Offset
Idem al original	1500	1	0
Idem al original	1500	1	185
Idem al original	1040	0	370

Los datagramas serán reenviados a través de los enlaces restantes sin fragmentarse nuevamente, y al llegar al host destino se reensamblarán.