

Examen – Febrero de 2013

(ref: eirc1302.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.
- 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)).
- Duración: 3 horas. Culminadas las 3 horas el alumno no podrá modificar las hojas a entregar de ninguna forma.
- Justifique todas sus respuestas.

Preguntas Teóricas

Pregunta 1 (10 puntos)

Suponga que debido a un error usted tiene una red con dos *hosts* A y B con direcciones IP IP_A e IP_B pero con la misma dirección MAC MAC_A . A y B pertenecen a la misma subred y están conectadas al mismo *hub*.

- Describe los problemas que pueden aparecer cuando los *hosts* A y B se conecten con otros *hosts* en la misma subred. Analice en particular la incidencia sobre el protocolo ARP.
- Suponga ahora que las máquinas anteriores son colocadas en dos segmentos de red independientes, con dos *routers* intermedios y direcciones IP coherentes con la nueva topología. Describa el intercambio de tramas y paquetes que ocurrirá cuando el *host* A envía un paquete al *host* B.

Nota: A y B están conectadas en subredes Ethernet, y los enlaces entre *routers* son de otra tecnología con direcciones de capa de enlace conocidas. Asuma que las tablas de ARP están inicialmente vacías.

Solución:

a) Dado que a nivel de capa de red las direcciones son diferentes, las tablas de ARP de los *hosts* tendrán dos entradas con la misma MAC para direcciones IP diferentes, no habrá problemas. Como el *hub* entregará TODOS los paquetes a TODOS los *hosts*, no se filtrará tráfico en la red; cuando el clasificador de paquetes de la tarjeta de red reciba paquetes con la MAC_A y entregue a la capa superior, se realizará la clasificación relativa a la capa de red correspondiente al *host* A o B, descartándose los paquetes que recibe A y correspondían a B o viceversa. Por lo tanto, otros *hosts* que se comuniquen con A o B no tendrán problemas. Un problema podría ser que, debido a la cantidad de tráfico que reciba uno de los *hosts*, el otro recibirá una cantidad equivalente de interrupciones, pudiendo generar impacto en su desempeño. Todo lo de más funcionará bien, siempre que los protocolos no tengan en cuenta la información de capa de enlace. Podrá haber problemas con características como autoconfiguración a nivel de IPv6.

b) Dado que los dominios de colisiones son totalmente independientes y que la información de capa de enlace queda circunscripta al mismo, todo funcionará adecuadamente.

En detalle:

Cuando A quiera enviar un paquete a B, verá que pertenece a otra subred, y por lo tanto enviará el paquete al gateway de su subred; para ello deberá descubrir su dirección MAC (utilizando ARP), y una vez que la conozca, puede enviar el paquete al gateway (contenido en una trama con destino la MAC del mismo). El gateway verá que el paquete es destinado a otra subred, y se lo enviará al gateway de la otra subred, utilizando las direcciones de capa de enlace conocidas (por ejemplo, circuitos virtuales de ATM). Cuando el paquete sea recibido por el segundo gateway, deberá descubrir la dirección MAC de B (utilizando ARP), para enviar finalmente el paquete a B, contenido en una trama con destino $MAC_B=MAC_A$.

Pregunta 2 (10 puntos)

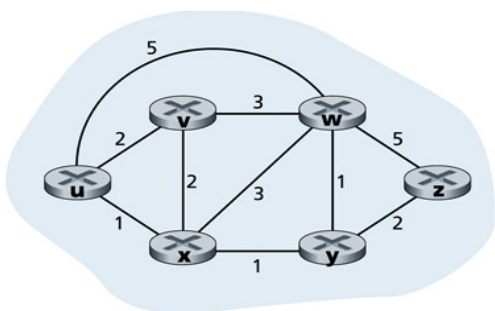
Describa los siguientes componentes de la arquitectura de IP móvil:

- (a) Home Network, Home Agent, Foreign Agent, Correspondent node, Mobile Node, Home Address, Care-of-Address, Mobile Node, Visited Network.
- (b) Explique en que consiste el “routing triangular” en esta arquitectura, que problemas introduce, y proponga soluciones.

Solución:

- a) Ver transparencias 6-3 y 6-4 de <http://eva.fing.edu.uy/mod/resource/view.php?id=6527> (Clase 2 de Redes Inalámbricas y Móviles).
- b) Ver transparencias 6-8 a 6-13 <http://eva.fing.edu.uy/mod/resource/view.php?id=6527> (Clase 2 de Redes Inalámbricas y Móviles).

Pregunta 3 (8 puntos)



Dada la red que se muestra en la figura, muestre la ejecución detallada paso a paso del algoritmo Link-State en el nodo **u** hasta su convergencia.

Utilice una tabla que muestre:

- Paso de la iteración
- Red considerada: (N')
- Distancia al nodo **n**, predecesor para el nodo **n**: $D(n),p(n)$.

Solución:

Sección 4.5.1 del libro, Tabla 4.3 y Figura 4.28.

Pregunta 4 (6 puntos)

- (a) Explique el concepto de longest prefix-match utilizado para el proceso de forwarding.
- (b) Dadas estas entradas en una tabla de forwarding:

Prefijo	Gateway	Interfaz
10.10.10.0/25	1.1.1.1	if0
10.10.10.0/24	2.2.2.2	if1
0.0.0.0/0	3.3.3.3	if2

¿Por qué interfaz será enviado un paquete con destino 10.10.10.129?

Solución:

- (a) “Longest prefix-match” es un algoritmo utilizado para seleccionar una entrada en la tabla de forwarding. Dado que una dirección destino puede coincidir (“match”) más de una entrada en la tabla, se denomina “longest prefix-match” a la entrada más específica, es decir, la que coincide con más bits de la máscara de subred.
- (b) 10.10.10.129 “matchea” con 10.10.10.0/24, pero **no** con 10.10.10.0/25 (que representa direcciones desde 10.10.10.0 a 10.10.10.127), por lo tanto el paquete será enviado por la interfaz **if1**.

Pregunta 5 (6 puntos)

- (a) Mencione ventajas y desventajas de la traducción NAT64, en la que clientes IPv6 se comunican con un dispositivo que realiza la traducción a IPv4.
- (b) Suponga que usted es el administrador/a de una red con direcciones IPv4 públicas. Ahora, necesita expandir la red y su proveedor de servicio solo puede asignarle direcciones IPv6. Justifique cual de las siguientes opciones adoptaría para resolver el problema: i) reenumerar la red con direcciones IPv6 o ii) usar NAT.

Introducción a las Redes de Computador{ae}s y Comunicación de Datos

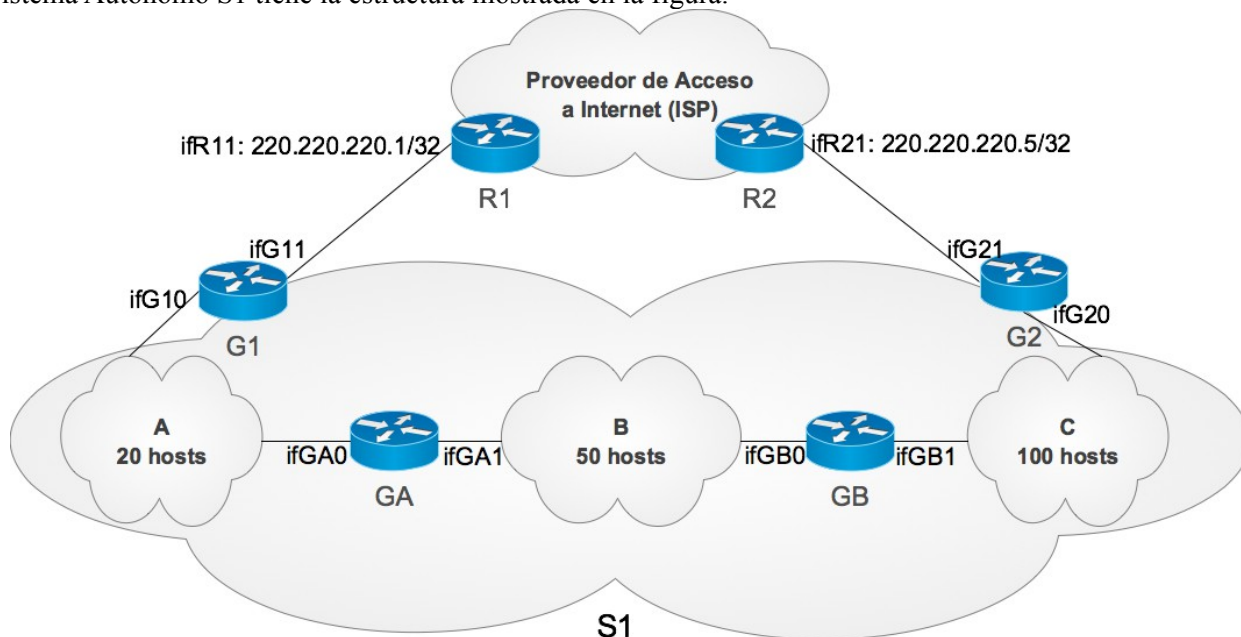
Solución:

- (a) Algunas ventajas: se puede acceder a contenido/servicios de IPv4 sin que se hayan migrado a IPv6 ; El despliegue es muy simple; Se puede eliminar IPv4 de una red interna
Algunas desventajas: Se depende de un único punto de fallos; En caso de requerir traducciones de protocolos avanzadas puede generar un problema de desempeño; no todos los protocolos pueden ser traducidos debido a la forma que utilizan -equivocadamente- información de capas inferiores
- (b) Cualquiera de ambas opciones es viable. Si el número de hosts es relativamente acotado y hay herramientas que puedan ayudar a la re-numeración, como el DHCP, podríamos pensar en reenumerar como una opción, siempre que los protocolos que utilizamos estén portados a IPv6. En caso que el número de hosts sea más amplio, la red mantenga una complejidad bastante grande, especialmente, contando con protocolos que no corran sobre IPv6, se deberá pensar en ampliar el espacio de direcciones sobre IPv4, utilizando rangos de direcciones privadas y compartir mediante NAT algunas direcciones IPv4 públicas a efecto de dar conectividad a los nuevos hosts.

Problemas Prácticos

Problema 1 (30 puntos)

El Sistema Autónomo S1 tiene la estructura mostrada en la figura.



El Proveedor de Acceso a Internet ISP le ha delegado el bloque de direcciones 200.200.200.0/24, y ha asignado para los enlaces las direcciones mostradas en la figura. El administrador de S1 debe cumplir con las siguientes políticas:

- P1) La subred A debe albergar 20 hosts, además de las interfaces correspondientes de los routers G1 y GA.
- P2) La subred B debe albergar 50 hosts, además de las interfaces correspondientes de los routers GA y GB.
- P3) La subred C debe albergar 100 hosts, además de las interfaces correspondientes de los routers G2 y GB.
- P4) Todo el tráfico de salida de la subred A debe utilizar el router G1.
- P5) El tráfico de salida de la subred B hacia el prefijo 15.15.0.0/16 debe utilizar el router G2, y el resto del tráfico de salida debe utilizar el router G1.
- P6) Todo el tráfico de salida de la subred C debe utilizar el router G2.
- P7) Se debe balancear el tráfico de entrada a S1, de forma que aproximadamente la mitad del tráfico ingrese por G1 y la otra mitad ingrese por G2, asumiendo que los todos los *hosts* consumen aproximadamente el mismo tráfico.
- P8) En caso de caída de alguno de los enlaces con el ISP, todo el tráfico debe ingresar por el enlace que sigue activo.

Se pide:

- (a) Asignar prefijos del bloque de direcciones delegado a S1 para cumplir con P1, P2, P3.
- (b) Asigne direcciones IP a todas las interfaces de los routers G1, G2, GA y GB.
- (c) Diseñe las tablas de *forwarding* de los *routers* G1, G2, GA, GB y los *hosts* de las subredes A, B y C para que S1 tenga conectividad completa entre sus subredes e Internet, y se cumplan las políticas P4, P5 y P6. Exprese las tablas con los campos <PREFIJO/BITS DE MÁSCARA>, <GATEWAY>, <INTERFAZ>; para los *hosts* asuma que tienen una sola interfaz denominada *eth0*.
- (d) Exprese los prefijos que deben ser publicados mediante BGP por los *routers* G1 y G2, de forma tal que sean compatibles con su respuesta a la primera pregunta, y que se cumplan las políticas P7 y P8.
- (e) Comente que problema se genera con el tráfico saliente de S1 cuando se cae alguno de los enlaces al ISP, y proponga modificaciones en las tablas de *forwarding* para resolver el caso de caída del enlace G1-R1.

Introducción a las Redes de Computador{ae}s y Comunicación de Datos

Solución:

(a)
S1: 200.200.200.0/24

A: $2^5 \geq 22$
200.200.200.32/27

B: $2^6 \geq 52$
200.200.200.64/26

C: $2^7 \geq 102$
200.200.200.128/25

Obs: hay otras soluciones posibles, lo importante son las máscaras de subred.

(b)

G1
ifG10:200.200.200.33/27
ifG11:220.220.220.2/30

G2
ifG20:200.200.200.129/25
ifG21:220.220.220.6/30

GA
ifGA0:200.200.200.34/27
ifGA1:200.200.200.65/26

GB
ifGB0:200.200.200.66/26
ifGB1:200.200.200.130/25

(c)

G1	200.200.200.32/27	DC	ifG10
	200.200.200.0/24	200.200.200.34	ifG10
	0/0	220.220.220.1	ifG11

G2	200.200.200.128/25	DC	ifG20
	200.200.200.0/24	200.200.200.130	ifG20
	0/0	220.220.220.5	ifG21

GA	200.200.200.64/26	DC	ifGA1
	200.200.200.32/27	DC	ifGA0
	200.200.200.128/25	200.200.200.66	ifGA1
	0/0	200.200.200.33	ifGA0

GB	200.200.200.64/26	DC	ifGB0
	200.200.200.128/25	DC	ifGB1
	200.200.200.32/27	200.200.200.65	ifGB0
	0/0	200.200.200.129	ifGB1

Hosts de A	200.200.200.32/27	DC	eth0
	200.200.200.0/24	200.200.200.34	eth0
	0/0	200.200.200.33	eth0

Hosts de C	200.200.200.128/25	DC	eth0
	200.200.200.0/24	200.200.200.130	eth0
	0/0	200.200.200.129	eth0

Hosts de B	200.200.200.64/26	DC	eth0
	200.200.200.128/25	200.200.200.66	eth0
	200.200.200.32/27	200.200.200.65	eth0 !se puede omitir, matchea con 0/0
	15.15.0.0/16	200.200.200.66	eth0
	0/0	200.200.200.65	eth0

(d)

G1 Debe publicar 200.200.200.0/25 y 200.200.200.0/24
G2 Debe publicar 200.200.200.128/25 y 200.200.200.0/24

(e)

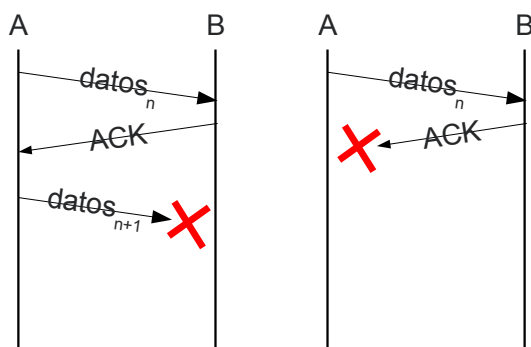
Cambiar los default gateways:

```
G1      0/0      200.200.200.34    ifG10
GA      0/0      200.200.200.66    ifGA1
Hosts de A
0/0      200.200.200.34    eth0
Hosts de B
0/0      200.200.200.66    eth0
```

Problema 2 (30 puntos)

Suponga que la entidad de red A envía **constantemente** mensajes a la entidad de red B (como máximo cada t segundos). Entre ambas existe un canal que puede perder y corromper los mensajes y tiene un retardo máximo de r segundos.

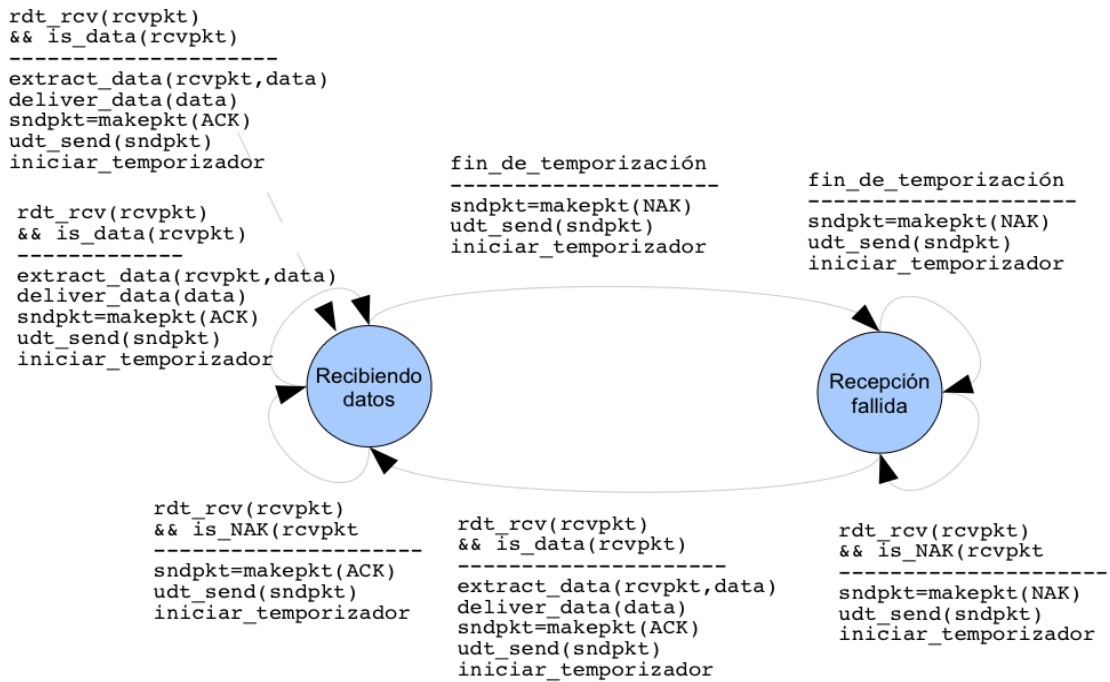
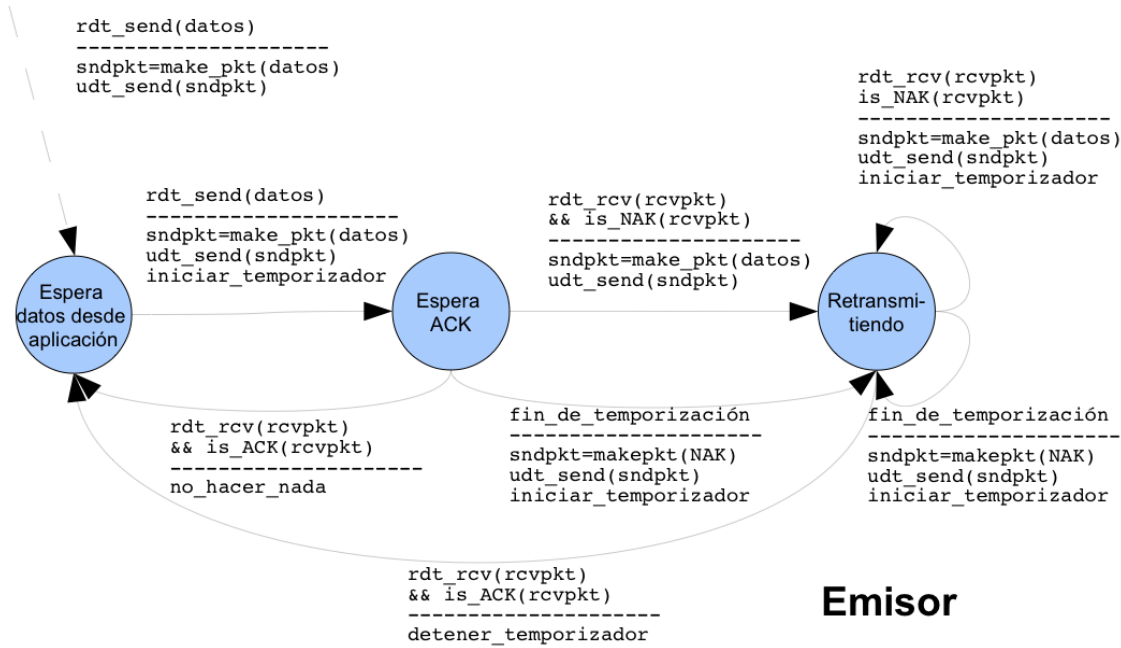
- a) Diseñe un protocolo de transferencia fiable de mensajes entre A y B que sea *stop-and-wait*, que utilice mensajes ACK y NACK (pueden usarse tanto desde el receptor como desde el emisor), y **no** utilice números de secuencia para los mensajes. Especifique las máquinas de estado de el emisor y el receptor, pudiendo utilizar las primitivas del protocolo *rdt 3.0*, por ejemplo, *udt_enviar*, *rdt_enviar*, *rdt_recibir* y aquellas que usted considere necesarias describiendo brevemente su funcionamiento.
- b) Complete los siguientes diagramas con los mensajes tal como los enviaría el protocolo diseñado en la parte a) luego de la pérdida del mensaje indicado con una cruz.



Introducción a las Redes de Computador{ae}s y Comunicación de Datos

Solución:

a)
 Obs: esta solución no considera los paquetes corruptos explícitamente. Se puede asumir que no llegaron y las máquinas de estado son las mismas que las mostradas.



b)

