

Solución Parcial – 28 de Noviembre de 2014
(ref: src20141128.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: 3 horas. Culminadas las 3 horas, el alumno no podrá modificar de ninguna forma las hojas.
- Justifique todas sus respuestas.

Pregunta 1 (4 puntos)

Suponga dos *hosts* en dos segmentos de red diferentes, separados por un *router* que actúa como su *default gateway* para cada LAN. Desde uno de estos *hosts* se ejecuta un ping con destino el otro *host* el cual llega a destino y es respondido exitosamente. Realice un diagrama que incluya todos los mensajes ARP e ICMP (que incluyan las direcciones MAC e IP de origen y destino), asumiendo que todas las tablas están vacías.

Solución Pregunta 1 (4 puntos)

Asumimos los siguientes datos para la red.

MAC HOST1: 00:00:00:00:00:01
 MAC HOST2: 00:00:00:00:00:02
 MAC ROTER EN RED 1: 00:00:00:00:00:03
 MAC ROTER EN RED 2: 00:00:00:00:00:04
 IP HOST1: 1.1.1.1
 IP HOST2: 2.2.2.1
 ROUTER GW PARA HOST1: 1.1.1.2
 ROUTER GW PARA HOST2: 2.2.2.2

El ping va desde HOST1 a HOST2

MAC ORIGEN	IP ORIG	MAC DESTINO	IP DEST	PROT	COMENTARIO
00:00:00:00:00:01	1.1.1.1	FF:FF:FF:FF:FF:FF	1.1.1.2	ARP REQ UEST	Consulta MAC del ROUTER en su LAN. En realidad la MAC destino de ARP es 00:::, la que es FF:: es en capa dos.
00:00:00:00:00:03	1.1.1.2	00:00:00:00:00:01	1.1.1.1	ARP REPL AY	
00:00:00:00:00:01	1.1.1.1	00:00:00:00:00:03	2.2.2.1	ICMP REQ UEST	El destino en capa 3 es el HOST2, pero en capa 2 es el router.
00:00:00:00:00:04	2.2.2.2	FF:FF:FF:FF:FF:FF	2.2.2.1	ARP REQ UEST	Consulta MAC del HOST2. En realidad la MAC destino de ARP es 00:::, la que es FF:: es en capa dos.
00:00:00:00:00:02	2.2.2.1	00:00:00:00:00:04	2.2.2.2	ARP REPL AY	
00:00:00:00:00:04	1.1.1.1	00:00:00:00:00:02	2.2.2.1	ICMP REQ	

Redes de Computadoras

MAC ORIGEN	IP ORIG	MAC DESTINO	IP DEST	PROT	COMENTARIO
				UEST	
00:00:00:00:00:02	2.2.2.1	00:00:00:00:00:04	1.1.1.1	ICMP REPL AY	Acá ya está cargado en la tabla ARP
00:00:00:00:00:03	2.2.2.1	00:00:00:00:00:01	1.1.1.1	ICMP REPL AY	Acá ya está cargado en la tabla ARP

Pregunta 2 (4 puntos)

Suponga una red compuesta por tres *hosts* conectados al mismo *switch* sin VLANs configuradas y cada uno en un puerto distinto del mismo.

- ¿Cuántos dominios de colisión hay en dicha red?
- ¿Cuántos dominios de *broadcast* hay en dicha red?
- ¿Cambiarían sus respuestas si ahora se reemplaza el *switch* por un *hub*?

Solución Pregunta 2 (4 puntos)

- 3, pues el *switch* genera que cada puerto sea un dominio de colisión independiente.
- Solo uno, pues estamos hablando de la misma VLAN o LAN.
- Para la pregunta a) ahora tendría un solo dominio de colisión.

Pregunta 3 (4 puntos)

Suponga un *switch* con 2 VLANs configuradas, y un *host* conectado a cada una de ellas. A cada *host* se le configura una dirección IP de la subred a la que pertenece, sin *default gateway*.

- Si ejecuta un ping entre los dos *hosts*, ¿cuántos mensajes ARP se generan?
- ¿Qué dispositivos y configuraciones agregaría para que un ping entre los dos *hosts* sea exitoso?
- Luego de ejecutar el ping de la parte anterior, ¿cual es el contenido de la tabla ARP de ambos *hosts*?

Solución Pregunta 3 (4 puntos)

- No se genera ninguno, ya que la red de destino es inalcanzable.
- Agregaría un router, con una interfaz en cada red y una dirección IP en cada una. Finalmente, configuraría la IP del router que está en su LAN como el default gateway de cada PC.
- La tabla ARP del host 1, tendrá el mapeo IP-MAC para la IP del router en su LAN, y lo mismo sucederá con la tabla ARP del host 2.

Pregunta 4 (4 puntos)

Se desea numerar con direcciones IP tres segmentos de red conectados cada uno a una interfaz distinta de un mismo *router*. En cada segmento hay 30, 16 y 8 computadoras

Redes de Computadoras

conectadas respectivamente. Se dispone para ello del prefijo 10.10.10.0/25.

Indique cuáles de las siguientes opciones de planes de numeración son viables de configurar, y cuáles no:

- a) Asignar los prefijos 10.10.10.0/27, 10.10.10.32/27 y 10.10.10.64/28 respectivamente.
- b) Asignar los prefijos 10.10.10.0/26, 10.10.10.64/27 y 10.10.10.96/28 respectivamente.
- c) Asignar los prefijos 10.10.10.16/27, 10.10.10.48/27 y 10.10.10.0/28 respectivamente.

Solución Pregunta 4 (4 puntos)

En cada segmento se requieren, como mínimo, las siguientes cantidades de direcciones IP a configurar en interfaces distintas, respectivamente: 31 (30 + 1), 17 (16 + 1) y 9 (8 + 1). Por lo tanto, en cada segmento se requieren, como mínimo, las siguientes subredes, respectivamente: /26 ($2^6 = 64$), /27 ($2^5 = 32$) y /28 ($2^4 = 16$).

Analizando cada caso,

El plan de numeración de a) no me permite numerar de manera completa la primera subred, por lo tanto no es viable.

El plan de numeración de b) sí me permite numerar de manera completa cada subred, por lo tanto sí es viable.

El plan de numeración de c) está mal realizado, por lo tanto no es viable.

Justificación:

En la siguiente tabla se identifica en cada fila el último byte y el efecto de la máscara de los prefijos 10.10.10.0/28, 10.10.10.16/27 y 10.10.10.48/27

0	0	0	0	X	X	X	X
0	0	0	1	X	X	X	X
0	0	1	1	X	X	X	X

Para el segundo caso, se presenta una inconsistencia entre el largo de la máscara y la dirección de red. Además, un /27 no es suficiente.

Si el router recibe un paquete destinado, por ejemplo, a la dirección IP 10.10.10.20, al momento de decidir su forwarding, tendrá dos opciones válidas, la de la subred 10.10.10.0/28 y la de la subred 10.10.10.16/27, por lo que la configuración no es correcta.

Algo similar ocurre con el prefijo 10.10.10.48/27.

Pregunta 5 (4 puntos)

- a) Describa el concepto de ventana de congestión en TCP.
- b) ¿Por qué se dice que TCP es un protocolo justo ("fair")? Ilustre con un ejemplo.

Solución Pregunta 5 (4 puntos)

a) La Ventana de Congestión es un *buffer* de almacenamiento del emisor TCP que

Redes de Computadoras

define la cantidad de bytes que se pueden enviar al receptor sin necesidad de recibir un paquete de confirmación ACK, si asumimos que no tenemos la restricción del *buffer* de recepción del receptor TCP. Estrictamente, la cantidad de datos no reconocidos en un emisor TCP no puede superar:

mínimo{Ventana de Congestión, Ventana de Recepción}

b) Se dice que TCP es "*fair*" porque el control de congestión converge para proporcionar la misma cuota de ancho de banda de un enlace cuello de botella a las distintas conexiones TCP que compiten por dicho ancho de banda. Por ejemplo, dos sistemas que inician conexiones TCP por un enlace de capacidad R, van a llegar a un estado de equilibrio donde cada conexión usa R/2 del ancho de banda disponible.

Pregunta 6 (4 puntos)

Describe el concepto de medio compartido, y comente las características del mecanismo *ALOHA con particiones* ("slotted ALOHA"). ¿Cuál es su eficiencia?

Solución Pregunta 6 (4 puntos)

El medio compartido, también llamado enlace de difusión (o *broadcast*), puede tener múltiples emisores y receptores, todos conectados al mismo enlace de difusión compartido. Ejemplos típicos son el medio inalámbrico y la primera versión de *ethernet*. *Slotted ALOHA* es un protocolo de acceso aleatorio, que considera particiones (*slots*) de tiempo fijo en los cuales se puede transmitir una trama. Al inicio de cada *slot*, el emisor que tiene una trama para transmitir lo hace, y detecta si hubo colisiones; si no las hubo, no es necesario retransmitirla, pero si se produjo colisión, el nodo volverá a transmitir en el *slot* siguiente con una determinada probabilidad p , repitiendo el procedimiento hasta lograr transmitir la trama. Este protocolo impone la sincronización entre los nodos participantes. La eficiencia del protocolo se calcula considerando la probabilidad que exactamente un nodo de N posibles tenga éxito transmitiendo su trama, y se llega a la expresión

$N * p * (1-p)^{N-1}$

Si se maximiza para N tendiendo a infinito se obtiene una eficiencia de 1/e, es decir, 37%.

Pregunta 7 (4 puntos)

Discuta las ventajas y desventajas entre utilizar HTTP/1.0 y HTTP/1.1.

Solución Pregunta 7 (4 puntos)

Algunas son:

	HTTP 1.0	HTTP 1.1
Ventajas	<ul style="list-style-type: none">• Fácil implementación• Soporte generalizado• Abundantes implementaciones	<ul style="list-style-type: none">• Optimizado para páginas con muchos objetos• Soporte en navegadores modernos
Desventajas	<ul style="list-style-type: none">• Overhead por slow-start en	<ul style="list-style-type: none">• Implementación compleja

Redes de Computadoras

	HTTP 1.0	HTTP 1.1
	<ul style="list-style-type: none">• páginas complejas• No soporta modernos requerimientos de sistemas	<ul style="list-style-type: none">• No se debe dejar de soportar 1.0 por más que se implemente

Pregunta 8 (4 puntos)

Sean las siguientes respuestas a la misma consulta DNS, realizadas a diferentes servidores:

consulta 1

```
dig www.fing.edu.uy @127.0.0.1

; <<>> DiG 9.8.4-P2 <<>> www.fing.edu.uy @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21887
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
www.fing.edu.uy.                IN      A

;; ANSWER SECTION:
www.fing.edu.uy.                1200    IN      A      164.73.32.5

;; AUTHORITY SECTION:
fing.edu.uy.                    600     IN      NS     ns.fing.edu.uy.
fing.edu.uy.                    600     IN      NS     ns2.fing.edu.uy.
fing.edu.uy.                    600     IN      NS     seciu.edu.uy.

;; ADDITIONAL SECTION:
ns.fing.edu.uy.                 600     IN      A      164.73.32.2
ns2.fing.edu.uy.               600     IN      A      164.73.32.4
seciu.edu.uy.                  600     IN      A      164.73.128.5
seciu.edu.uy.                  21554   IN      AAAA   2001:1328:6::5

;; Query time: 299 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 25 08:26:44 2014
;; MSG SIZE rcvd: 180
```

consulta 2

```
dig www.fing.edu.uy @164.73.32.2

; <<>> DiG 9.8.4-P2 <<>> www.fing.edu.uy @164.73.32.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36715
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 2
```

Redes de Computadoras

```
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.fing.edu.uy.                IN      A

;; ANSWER SECTION:
www.fing.edu.uy.                1200   IN      A      164.73.32.5

;; AUTHORITY SECTION:
fing.edu.uy.                    1200   IN      NS     ns.fing.edu.uy.
fing.edu.uy.                    1200   IN      NS     seciu.edu.uy.
fing.edu.uy.                    1200   IN      NS     ns2.fing.edu.uy.

;; ADDITIONAL SECTION:
ns.fing.edu.uy.                 1200   IN      A      164.73.32.2
ns2.fing.edu.uy.                1200   IN      A      164.73.32.4

;; Query time: 24 msec
;; SERVER: 164.73.32.2#53(164.73.32.2)
;; WHEN: Tue Nov 25 08:27:53 2014
;; MSG SIZE rcvd: 136
```

¿Cuál de las respuestas es autoritativa y cuál no?

Solución Pregunta 8 (4 puntos)

La respuesta autoritativa es la segunda, y puede verse por:

- está presente el flag AA (Authoritative Answer)
- el NS al que se consulta es uno de los autoritativos, dado en la sección adicional

Pregunta 9 (4 puntos)

¿Cuál es la relación entre los protocolos de enrutamiento de una red y la tabla de *forwarding* de un router cualquiera de dicha red?

Solución Pregunta 9 (4 puntos)

El *forwarding* o reenvío refiere a la acción local de un enrutador de decidir por qué interfaz de salida enviar un paquete que se recibe en una interfaz de entrada, mientras que el *routing* o enrutamiento refiere al proceso distribuido que realiza la red en su conjunto para determinar los caminos de extremo a extremo. Los protocolos de enrutamiento se ejecutan en cada nodo, y determinar caminos de menor costo a otros nodos en base a la información propia y la que le proporcionan sus vecinos. Una vez decididos los caminos de menor costo, estas decisiones se implementan localmente en cada enrutador mediante una tabla de correspondencia entre prefijos de entrada e interfaces de salida.

Pregunta 10 (4 puntos)

En el marco de la transición hacia IPv6:

- a) Describa los mecanismos de "tunneling" que pueden utilizarse.
- b) Comente los cambios con respecto a IPv4 en las opciones de fragmentación y reensamblado.

Solución Pregunta 10 (4 puntos)

a) La tunelización consiste en tomar el datagrama IPv6 completo como el campo de datos de un datagrama IPv4, el cual se envía normalmente por una red IPv4, permitiendo recuperar el datagrama IPv6 original en el receptor. El concepto se puede aplicar a múltiples protocolos "tunelizados" por otros. El mecanismo más simple es el descrito, normalmente denominado **6in4**; el mecanismo **6to4** es similar pero permite usar servidores de pasarela o *relays*. Entre otras posibilidades, se puede implementar la tunelización con transporte UDP, denominado **Teredo**; en este caso se facilita la tunelización a través de un *router* NAT.

b) IPv6 solamente implementa fragmentación end-to-end, no en los routers intermedios; los datagramas cuya MTU exceda las posibilidades de un medio a lo largo del camino, serán descartados.