

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN (UPCT)
LAB. REDES Y SERVICIOS DE COMUNICACIONES (Ingeniero Técn. de Telecomunicación, Esp. Telemática)

Convocatoria de Junio. Fecha: 19 de Junio de 2006.

Alumno: _____

PROBLEMA 1 (1,6 pts.) – FIGURA 1

El *router* A y el *router* B han sido configurados para implementar la funcionalidad Proxy ARP entre las tres redes físicas *Ethernet* a las que se encuentra conectado. Las tablas caché ARP de los PCs 1, 2, 3, 101, 102, 103 y del *router* C se encuentran inicialmente vacías.

Suponga que durante un cierto tiempo **todos los PCs, y los routers A, B y C** han estado generando y recibiendo tráfico, por lo que las tablas caché ARP de TODOS los dispositivos tienen toda la información completa (han aprendido todas las entradas posibles). Escriba los contenidos de las tablas caché ARP de los dispositivos que se le indica.

Tabla Caché ARP Router C		Tabla Caché ARP PC 1	
Dirección MAC	Dirección IP	Dirección MAC	Dirección IP
00:40:0d:00:00:01	197.1.1.1	00:40:0d:00:00:02	197.1.1.2
00:40:0d:00:00:02	197.1.1.2	00:40:0d:00:00:03	197.1.1.3
00:40:0d:00:00:03	197.1.1.3	00:40:0d:00:00:F1	197.1.1.254
00:40:0d:00:00:E1	197.1.1.101	00:40:0d:00:00:E1	197.1.1.101
00:40:0d:00:00:E1	197.1.1.102	00:40:0d:00:00:E1	197.1.1.102
00:40:0d:00:00:E1	197.1.1.103	00:40:0d:00:00:E1	197.1.1.103
00:40:0d:00:00:E1	197.1.1.253	00:40:0d:00:00:E1	197.1.1.253
00:40:0d:00:00:E1	197.1.1.252	00:40:0d:00:00:E1	197.1.1.252
00:40:0d:00:00:E1	197.1.1.251	00:40:0d:00:00:E1	197.1.1.251
00:40:0d:00:00:E1	197.1.1.250	00:40:0d:00:00:E1	197.1.1.250

Tabla Caché ARP PC 101		Tabla Caché ARP PC 103	
Dirección MAC	Dirección IP	Dirección MAC	Dirección IP
00:40:0d:00:00:D1	197.1.1.1	00:40:0d:00:00:B1	197.1.1.1
00:40:0d:00:00:D1	197.1.1.2	00:40:0d:00:00:B1	197.1.1.2
00:40:0d:00:00:D1	197.1.1.3	00:40:0d:00:00:B1	197.1.1.3
00:40:0d:00:00:D1	197.1.1.254	00:40:0d:00:00:B1	197.1.1.254
00:40:0d:00:00:D1	197.1.1.253	00:40:0d:00:00:B1	197.1.1.253
00:40:0d:00:00:D1	197.1.1.252	00:40:0d:00:00:B1	197.1.1.252
00:40:0d:00:00:A2	197.1.1.102	00:40:0d:00:00:B1	197.1.1.101
00:40:0d:00:00:C1	197.1.1.251	00:40:0d:00:00:B1	197.1.1.102
00:40:0d:00:00:C1	197.1.1.250	00:40:0d:00:00:B1	197.1.1.251
00:40:0d:00:00:C1	197.1.1.103	00:40:0d:00:00:B1	197.1.1.250

PROBLEMA 2 (2 pts.)

Una aplicación A establece una conexión TCP con una aplicación B. El extremo aceptador informa de que el tamaño máximo de segmento que está dispuesto a recibir es de 5000, mientras que el extremo iniciador de la conexión informa que el tamaño máximo de segmento que está dispuesto a recibir es 1460.

(1,5 pts) Escriba el contenido de los campos de la cabecera TCP vacíos que aparecen en la tabla, en la siguiente secuencia de intercambio de segmentos, suponiendo que no existe pérdida ni desorden en la entrega, salvo en las ocasiones que se indica lo contrario.

P _{origen}	P _{destino}	Seq. Number	ACK	Options	Comentarios
4000	3000	6000	---	MSS=1460	Petición de inicio de conexión
3000	4000	1000	6001	MSS=5000	2º mensaje de inicio de conexión
4000	3000	6001	1001		3º mensaje de inicio de conexión
4000	3000	6001	1001		A envía 300 bytes de datos nuevos (segmento perdido)
4000	3000	6301	1001		A envía 400 bytes de datos nuevos
3000	4000	1001	6001 (pos. fallo ventana)		B envía 100 bytes de datos nuevos
4000	3000	6701	1101		A envía 100 bytes de datos nuevos (segmento perdido)
3000	4000	1101	6001		B envía 300 bytes de datos nuevos (segmento perdido)
4000	3000	6001	1101		A reenvía 300 bytes de datos de 1º segmento perdido (recibido)
3000	4000	1101	6701		B reenvía 300 bytes de datos de 1º segmento perdido (recibido)
4000	3000	6701	1401		A envía segmento de 1000 bytes de datos nuevos

(0,5 pts) Suponga que los mecanismos de control de congestión no afectan en este ejemplo al tamaño de la ventana de transmisión. Suponga que en el extremo A, el tamaño inicial de su ventana de transmisión no varía durante la transmisión de los segmentos. Suponga lo mismo en el extremo B.

¿Cuál es el tamaño mínimo de la ventana de transmisión que tiene el extremo A? (es decir, tal que si su tamaño hubiera sido menor, esta secuencia de segmentos no se podría haber producido).

1000 bytes

PROBLEMA 3 (1 pto.) – FIGURA 2

Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todos los nodos implementan la técnica de split horizon simple con inversión de ruta (*poisoned reverse*). Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- Todos los enlaces punto a punto son anónimos.
- Si considera que algún mensaje no se produce o está vacío, debe indicarlo explícitamente con la palabra “vacío” en la tabla.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.

Mensaje Response generado por A por su interfaz ppp0 (0,25 pts.)	
Ruta	Número de saltos
200.1.1.0	1
200.1.2.0	16
200.1.3.0	16
200.1.4.0	16
200.1.5.0	16

Mensaje Response generado por B por su interfaz ppp1 (0,25 pts.)	
Ruta	Número de saltos
200.1.1.0	16
200.1.2.0	1
200.1.3.0	2
200.1.4.0	3
200.1.5.0	2

Mensaje Response generado por C por su interfaz ppp0 (0,25 pts.)	
Ruta	Número de saltos
200.1.1.0	16
200.1.2.0	16
200.1.3.0	1
200.1.4.0	16
200.1.5.0	16

Mensaje Response generado por E por su interfaz ppp0 (0,25 pts.)	
Ruta	Número de saltos
200.1.1.0	16
200.1.2.0	16
200.1.3.0	16
200.1.4.0	2
200.1.5.0	1

PROBLEMA 4 (2,4 pts.) – FIGURA 3

La figura inferior muestra la red de una empresa dedicada a servicios de consultoría IP:

- La única conexión al exterior de la red es a través del *router* A, que implementa la funcionalidad de *Masquerading* (NAPT), con red interna 192.168.4.0/255.255.255.0, y dirección externa 212.128.100.1.
- El conjunto de PCs 1..100 y el PC ADM se encuentran conectados directamente en la red general interna.
- La red incluye un conjunto de servidores públicos, con dirección IP pública de Internet. Estos servidores deben ser accesibles desde el exterior y desde el interior de la empresa.
- La empresa dispone de 3 servidores en una red interna, **oculta a la red general interna a través del router C**. Las conexiones originadas en estos servidores deben ser enmascaradas. Los siguientes servicios ofrecidos por los servidores, deben ser accesibles (únicamente a la red general interna):
 - Servidor 1: implementa dos servicios en los puertos 22 y 143, que deben ser accesibles desde la red general interna en los puertos 2222 y 143 respectivamente.
 - Servidor 2: implementa dos servicios en los puertos 22 y 80, que deben ser accesibles desde la red general interna en los puertos 2223 y 80 respectivamente.
 - Servidor 3: implementa dos servicios en los puertos 22 y 21, que deben ser accesibles desde la red general interna en los puertos 2224 y 21 respectivamente.

Nota: Si al rellenar una tabla, cree que debe estar vacía, debe indicarlo claramente con la palabra “vacía”.

1. (0,25 pts.) Indique el contenido de la tabla de configuración de puertos visibles del *router* A.

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)
(vacía)	(vacía)	(vacía)

2. (0,25 pts.) Indique el contenido de la tabla de configuración de puertos visibles del *router* C.

Tabla de puertos visibles		
IP servidor interno	Puerto servidor interno	Puerto público (externo)
192.168.3.1	22	2222
192.168.3.1	143	143
192.168.3.2	22	2223
192.168.3.2	80	80
192.168.3.3	22	2224
192.168.3.3	21	21

3. (0,25 pts.) Indique razonadamente si el *router* B debe implementar la funcionalidad NAPT.

No, implementa la funcionalidad NAPT. Hace las funciones normales de router, ya que únicamente está conectada a una red que es visible, y no tiene que hacer traducción de direcciones.

4. (1 pts.) Escriba la tabla de encaminamiento de los dispositivos que se le indica.

Tabla encaminamiento router B			
Dirección	Máscara	Interfaz de salida	Gateway
200.1.1.0	255.255.255.0	eth1	---
192.168.4.0	255.255.255.0	eth0	---
0.0.0.0	0.0.0.0	eth0	192.168.4.254

Tabla encaminamiento router A			
Dirección	Máscara	Interfaz de salida	Gateway
192.168.4.0	255.255.255.0	eth0	---
200.1.1.0	255.255.255.0	eth0	192.168.4.253
0.0.0.0	0.0.0.0	ppp0	---

Tabla encaminamiento PC ADM			
Dirección	Máscara	Interfaz de salida	Gateway
192.168.4.0	255.255.255.0	eth0	---
200.1.1.0	255.255.255.0	eth0	192.168.4.253
0.0.0.0	0.0.0.0	eth0	192.168.4.254

Tabla encaminamiento router C			
Dirección	Máscara	Interfaz de salida	Gateway
192.168.3.0	255.255.255.0	eth1	---
192.168.4.0	255.255.255.0	eth0	---
200.1.1.0	255.255.255.0	eth0	192.168.4.253
0.0.0.0	0.0.0.0	eth0	192.168.4.254

5. (0,65 pts.) El PC ADM abre una conexión SSH para configurar remotamente el servidor 2 (que tiene el servidor SSH en su puerto 22). El puerto origen efímero que emplea el PC ADM es el 3000. Durante esta conexión SSH, la tabla de conexiones enmascaradas del router C tiene los siguientes valores:

IP interna	Puerto Máquina interna	Puerto Externo
192.168.3.1	2000	61001
192.168.3.2	2223	61002

Rellene las siguientes tablas describiendo la traducción de direcciones y puertos que sufren los segmentos de la conexión TCP a la que pertenece la conexión SSH. Fíjese bien en lo que se le pide en la columna de la izquierda al escribir su respuesta.

Datagramas de la conexión TCP	IP origen	Puerto TCP origen	IP destino	Puerto TCP destino
PC ADM → Router C	192.168.4.200	3000	192.168.4.252	2223
Router C → Serv 2	192.168.4.200	3000	192.168.3.2	22
Serv 2 → Router C	192.168.3.2	22	192.168.4.200	3000
Router C → PC ADM	192.168.4.252	2223	192.168.4.200	3000

