

Redes y comunicaciones - 1ra fecha (21/06/2022)

Siempre es necesario justificar, las respuestas no debidamente justificadas serán consideradas incorrectas. En los ejercicios de subnetting deberá ser claro tanto el por qué se selecciona una red y como así también se deben dejar expresados los cálculos o explicado el proceso para obtener el resultado.

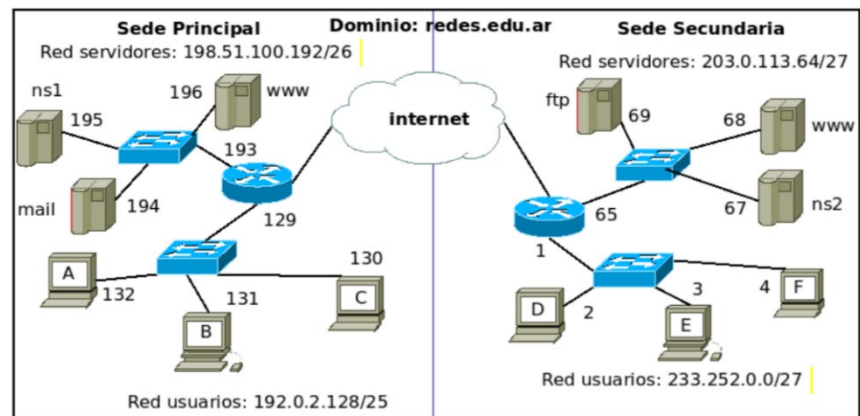
Al comenzar cada ejercicio se suponen todas las tablas vacías (CAM, Caché, ARP).

Para mencionar la dirección MAC de un dispositivo utilice la notación: MAC_dev_iface. Ej.: la MAC de pc-B será MAC_PC-B_ethO.

1. La persona encargada de la organización redes.edu.ar requiere de su servicio de consultoría. Le presenta una explicación con el siguiente diagrama:

REQUISITOS:

- Ambos host WWW comparten un filesystem y solo alojan tres sitios estáticos `www.redes.edu.ar`, `sedeprincipal.redes.edu.ar` y `sedesecundaria.redes.edu.ar`. Debido a la alta demanda es necesario balancear carga entre los servidores.
- El host MAIL es un servidor SMTP utilizado por aplicaciones para enviar correos a los usuarios. No cumple ninguna otra función.
- NS1 y NS2 brindaran respuestas autoritativas para el dominio.
- El personal de IT usa el nombre FTP para acceder a dicho host, pero los usuarios prefieren un nombre más semántico como "sharedfolder".



- a) Liste los registros DNS que debería tener configurado ns1 para cumplir con los requisitos dados.

• <code>redes.edu.ar</code>	NS	<code>ns1.redes.edu.ar</code>
• <code>ns1.redes.edu.ar.</code>	A	<code>198.51.100.195</code>
• <code>redes.edu.ar</code>	NS	<code>ns2.redes.edu.ar</code>
• <code>ns2.redes.edu.ar</code>	A	<code>203.0.113.67</code>
• <code>www.redes.edu.ar</code>	A	<code>196.51.100.196</code>
• <code>www.redes.edu.ar</code>	A	<code>203.0.113.68</code>
• <code>sedeprincipal.redes.edu.ar</code>	CNAME	<code>www.redes.edu.ar</code>
• <code>sedesecundaria.redes.edu.ar</code>	CNAME	<code>www.redes.edu.ar</code>
• <code>ftp.redes.edu.ar</code>	A	<code>203.0.113.69</code>
• <code>sharedfolder.redes.edu.ar</code>	CNAME	<code>ftp.redes.edu.ar</code>
• <code>mail.redes.edu.ar.</code>	A	<code>198.51.100.194</code>

- b) Se desea configurar un nuevo host en la red de usuarios de Sede Principal. Indique todos los valores de red que el técnico de la red debería configurar para que el host pueda conectarse a Internet y a los recursos de la organización.

Se conecta un nuevo usuario PC-G. Su dirección de red será: 192.0.2.133/25. Debe configurar a 192.0.2.129/25 como su gateway por default.

- c) Si un usuario en PC-C ingresa mediante su navegador a `http://www.redes.edu.ar` ¿es posible determinar a qué host llegará esa solicitud?

Debería acceder al más cercano (ns1) por un tema de velocidad. Pero depende de varios factores, como la tabla de ruteo, si ns1 está caído o colapsado de trabajo, etc.

Nombre y Apellido:

Legajo:

- d) **Cuándo cualquiera de los hosts "www" recibe una solicitud, ¿Qué característica del protocolo en cuestión permite determinar qué sitio dentro de los que aloja debe presentar al cliente?**

El header de http permite incluir el nombre del método (por ejemplo, get) y la dirección (/practicas/practica3) para hacer el request correspondiente al host indicado también en los headers (redes.edu.ar).

2. Dada la siguiente salida del comando **ss -nltn** en el host A:

	Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
1.	udp	UNCONN	0	0	0.0.0.0:53	0.0.0.0:*
2.	udp	UNCONN	0	0	0.0.0.0:80	0.0.0.0:*
3.	tcp	LISTEN	0	10	0.0.0.0:5762 1	0.0.0.0:*
4.	tcp	LISTEN	0	128	127.0.0.1:8080	0.0.0.0:*
5.	tcp	LISTEN	0	128	127.0.0.1:17603	0.0.0.0:*
6.	tcp	LISTEN	0	50	0.0.0.0:9 1 00	0.0.0.0:*
7.	tcp	LISTEN	0	40	0.0.0.0:80	0.0.0.0:*
8.	tcp	ESTAB	0	0	192.168.22. 15:53646	38.54.44.72:443
9.	tcp	ESTAB	0	0	127.0.0. 1:17603	127.0.0. 1:9 100
10.	tcp	CLOSE-WAIT	25	0	192. 168.22. 15:56584	151.101.218.137:443
11.	tcp	ESTAB	0	0	192. 168.22. 15:46074	159. 138.208.235:443
12.	tcp	TIME-WAIT	0	0	192. 168.22. 15:46076	159.138.208.235:443
13.	tcp	CLOSE-WAIT	130	0	192.168.22.15:43810	35.186.224.25:443
14.	tcp	ESTAB	0	0	127.0.0. 1:9 100	127.0.0. 1:1760 3

- A. **¿Puede determinar y listar las direcciones IP que tiene asignadas host A?**

Podemos conocer la:

- IP local → 192.168.22.15
- Loopback → 127.0.0.1

- B. **¿A qué fase de la conexión se corresponde el estado de la línea 12? Independientemente de quien inicia esta fase, brinde dos intercambios de mensajes posibles asociados.**

Corresponde a la fase de cierre de 3 vías. Mensajes asociados podrían ser:

- Estando en Time-Wait (es decir, espero que me envíen un FIN), recibo el FIN y envío el ACK para pasar a Close-Wait.
- Estando en Fin-Wait-1 (es decir, envié el FIN y espero que me envíen el ACK) puedo recibir el ACK y pasar a Time-Wait o que se pierda, pasar a Fin-Wait-2 y reenviar el FIN.

- C. **Indique como se vería con TCPDUMP la respuesta a los siguientes paquetes observados en el host A (incluya toda la información posible: direcciones IP, puertos, flags y numeras de secuencia y confirmación):**

a. 192.168.22.20:35794 > <ip_host_A>:80 : Flags [S], seq 110012, ack 0

RTA → <ip_host_A>:80 > 192.168.22.20:35794 : Flags [SA], seq 0, ack 110013

b. 192.168.22.20:35794 > <ip_host_A>:9100 : UDP, length 1024

RTA → Es UDP, no hay respuesta. Salvo un ICMP si hubo un error.

c. 192.168.22.20:33444 > <ip_host_A>:8080 : Flags [S], seq 552201, ack 0

RTA → <ip_host_A>:8080 > 192.168.22.20:33444 : Flags [SA], seq 0, ack 552202

3. Un usuario indica que utilizando un navegador accede a <http://www.redes.edu/hola.txt> y tiene problemas para visualizar el recurso solicitado. Usted se conecta al servidor y obtiene la siguiente captura de tráfico:

172.16.8.16.35794 > 192.168.22.31.80: Flags [S], seq 558012, win 65495, length 0

192.168.22.31.80 > 172.16.8.16.35794: Flags [SA], seq 160879, ack 558012, win 65483, length 0

172.16.8.16.35794 > 192.168.22.31.80: Flags [RA], ack 1, win 404, length 0

- a) **¿En qué protocolo ubicaría el problema? ¿el problema está en el cliente o en el servidor?**

En el protocolo TCP, ocurre que el servidor pone mal el ACK. Envía ack=558012 cuando tendría que haber pedido el 13 (1 más de lo que ha recibido).

Por otro lado, al cliente le envían un mensaje de tamaño 0 y la ventana de congestión se le reduce en 65091 bytes. Raro cuanto menos.

- b) **¿Qué datos del protocolo HTTP llegaron a ser intercambiados?**

Se envió el http request y la respuesta dio un error del servidor (500)

Nombre y Apellido:

Legajo:

4. Utilizando CIDR, indique cuáles de los siguientes bloques pueden ser agrupados y determine el bloque CIDR resultante de dicha sumariación: 113.33.215.0/24, 113.33.216.0/24, 113.33.217.0/24 y 113.33.218.0/23.

Se puede agrupar, ya que hasta el bit número 20 son iguales:

113.33.215.0/24 - 113.33.1101 0111.0/24
113.33.216.0/24 - 113.33.1101 1000.0/24
113.33.217.0/24 - 113.33.1101 1001.0/24
113.33.218.0/23 - 113.33.1101 1010.0/23

CIDR:

113.33.1101 0000.0/20
113.33.208.0/20

5. Utilizando el prefijo de red 13.14.56.0/23, asigne direcciones IP a las siguientes subredes, las cuales tienen los siguientes requerimientos: Red A (117 hosts), Red B (97 hosts), Red C (192 hosts).

Para asignar direcciones IP a las subredes utilizando el método de Subneteo de Longitud de Máscara Variable (VLSM), debemos comenzar con la subred que requiere la mayor cantidad de hosts. Aquí están los pasos:

Red C (192 hosts): Para soportar 192 hosts, necesitamos una subred con al menos 256 direcciones (el siguiente número de potencia de 2). Esto requiere 8 bits para los hosts, dejando 24 bits para la red. La máscara de subred para la Red C es /24. Podemos usar el rango de direcciones 13.14.56.0 a 13.14.56.255 para la Red C.

Red A (117 hosts): Para soportar 117 hosts, necesitamos una subred con al menos 128 direcciones. Esto requiere 7 bits para los hosts, dejando 25 bits para la red. La máscara de subred para la Red A es /25. Como la Red C ya está utilizando las primeras 256 direcciones, podemos usar el rango de direcciones 13.14.57.0 a 13.14.57.127 para la Red A.

Red B (97 hosts): Para soportar 97 hosts, también necesitamos una subred con al menos 128 direcciones. Esto también requiere 7 bits para los hosts, dejando 25 bits para la red. La máscara de subred para la Red B es /25. Como la Red C y la Red A ya están utilizando las primeras 384 direcciones, podemos usar el rango de direcciones 13.14.57.128 a 13.14.57.255 para la Red B.

Por lo tanto, las asignaciones de direcciones IP para las subredes utilizando VLSM son las siguientes:

- Red C: 13.14.56.0/24 (13.14.56.0 a 13.14.56.255)
- Red A: 13.14.57.0/25 (13.14.57.0 a 13.14.57.127)
- Red B: 13.14.57.128/25 (13.14.57.128 a 13.14.57.255)

Es importante tener en cuenta que, en cada subred, la primera dirección se utiliza como dirección de red y la última dirección se utiliza como dirección de difusión, por lo que no se pueden asignar a hosts individuales. Esto deja 254 direcciones disponibles para hosts en la subred C, y 126 direcciones disponibles para hosts en las subredes A y B, que son suficientes para satisfacer los requerimientos de hosts para cada subred.

6. Indique todas las direcciones IPv6 con las que se autoconfigura una PC utilizando EUI-64 considerando que: Tiene la dirección MAC 3c:e5:8d:96:9a:b5. Está conectada a un segmento de red en el que se recibe un Router Advertisement del prefijo 2900:aabb::/64.

3c → 0011 1100

Invierto el 7mo bit → 00111110 → 3E

Agrego FF:FE en el medio 3c:e5:8d:ff:fe:96:9a:b5

Agrego el prefijo 2900:aabb y agrupo de a 16 bits → 2900:aabb::3ce5:8dff:fe96:9ab5

7. Dada la siguiente tabla de rutas: Indique por cuál interfaz se enviarán los siguientes paquetes y en cada uno, la dirección MAC de destino que tendría que usar (suponga que la conoce).

Tabla de rutas IP del núcleo

Destino	Pasarela	Genmask	Indlc	Métrlc	Ref	Uso	Interfaz
0.0.0.0	192.168.0.255	0.0.0.0	UG	600	0		e eth0
172.11.0.0	192.168.0.255	255.255.0.0	u	0	0		e eth0
172.18.0.0	192.168.1.255	255.255.0.0	u	0	0		e eth1
172.19.0.0	192.168.2.255	255.255.0.0	u	0	0		e eth2
172.21.0.0	192.168.2.255	255.255.0.0	u	0	0		e eth2
192.168.0.0	0.0.0.0	255.255.255.0	u	600	0		e eth0
192.168.1.0	0.0.0.0	255.255.255.0	u	600	0		e eth1
192.168.2.0	0.0.0.0	255.255.255.0	u	600	0		e eth2

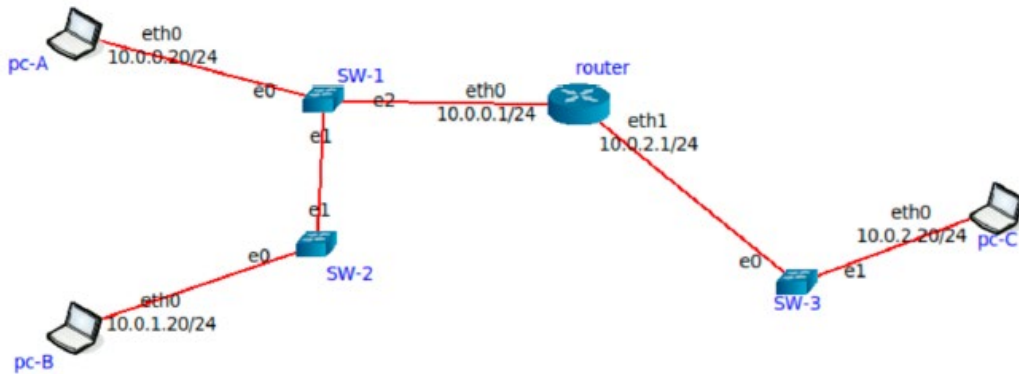
	IP oriaen	IP destino	Protocolo	Port Origen	Port Destino
Paquete 1 -----	172.17.0.34	140.23.40.78	TCP	3250	80
Paquete 2 -----	172.17.0.34	172.21.0.2	UDP	5353	53
Paquete 3 -----	192.168.1.52	192.168.2.24	ICMP		

- Paquete 1 → eth0 porque va al default → MAC_192.168.0.255 (default gateway)
- Paquete 2 → eth2 porque matchea con 172.21.0.0 mask 255.255.0.0 → MAC_192.168.2.255
- Paquete 3 → eth2 porque matchea con 192.168.2.0 mask 255.255.255.0 → MAC_0.0.0.0

Nombre y Apellido:
(algún dispositivo directamente conectado)

Legajo:

8. Considerando la siguiente topología y luego de que pc-A hace un ping exitoso a pc-C:



A. Complete la información del ARP request que realiza pc-A. Incluya la información de los protocolos ethernet y ARP.

Pc-A le pide la MAC al router, del que conoce su IP. Manda un broadcast.

MAC origen	MAC destino	ARP Packet	
pc-A_eth0	FF:FF:FF:FF:FF:FF	MAC origen: pc_A_eth0 IP origen: 10.0.0.20/24	MAC destino: ??? IP destino: 10.0.0.1/24

El router le contesta.

MAC origen	MAC destino	ARP Packet	
router_eth0	pc-A_eth0	MAC origen: router_eth0 IP origen: 10.0.0.1/24	MAC destino: pc-A_eth0 IP destino: 10.0.0.20/24

pc-A le pide la MAC de pc-C al router.

MAC origen	MAC destino	ARP Packet	
pc-A_eth0	router_eth0	MAC origen: pc-A_eth0 IP origen: 10.0.0.20/24	MAC destino: ??? IP destino: 10.0.2.20/24

El router desarma el ARP packet, le pone su información y le pregunta a la red (broadcast) dónde está el dispositivo con IP 10.0.2.20.

MAC origen	MAC destino	ARP Packet	
router_eth0	FF:FF:FF:FF:FF:FF	MAC origen: router_eth0 IP origen: 10.0.0.1/24	MAC destino: ??? IP destino: 10.0.2.20/24

Pc-C responde al router con su MAC.

MAC origen	MAC destino	ARP Packet	
pc-C_eth0	router_eth0	MAC origen: pc-C_eth0 IP origen: 10.0.2.20/24	MAC destino: router_eth0 IP destino: 10.0.0.1/24

Nombre y Apellido:

Legajo:

- B. Indique cómo quedan las tablas CAM de los dispositivos que están en el mismo segmento de broadcast que pc-A.**

SW-1
E0: PC-A
E2: Router

SW-2
E1: PC-A

- C. Si en pc-B hubiesen estado capturando tráfico en la interfaz eth0, ¿que hubiesen escuchado? Para cada paquete capturado, indique el protocolo y si se trata de un requerimiento o una respuesta.**

Hubiera escuchado el requerimiento de PC_A al router, dado que era un broadcast.

Habría visto un paquete IP con el protocolo ICMP del tipo echo request de PC_A hacia PC_C.