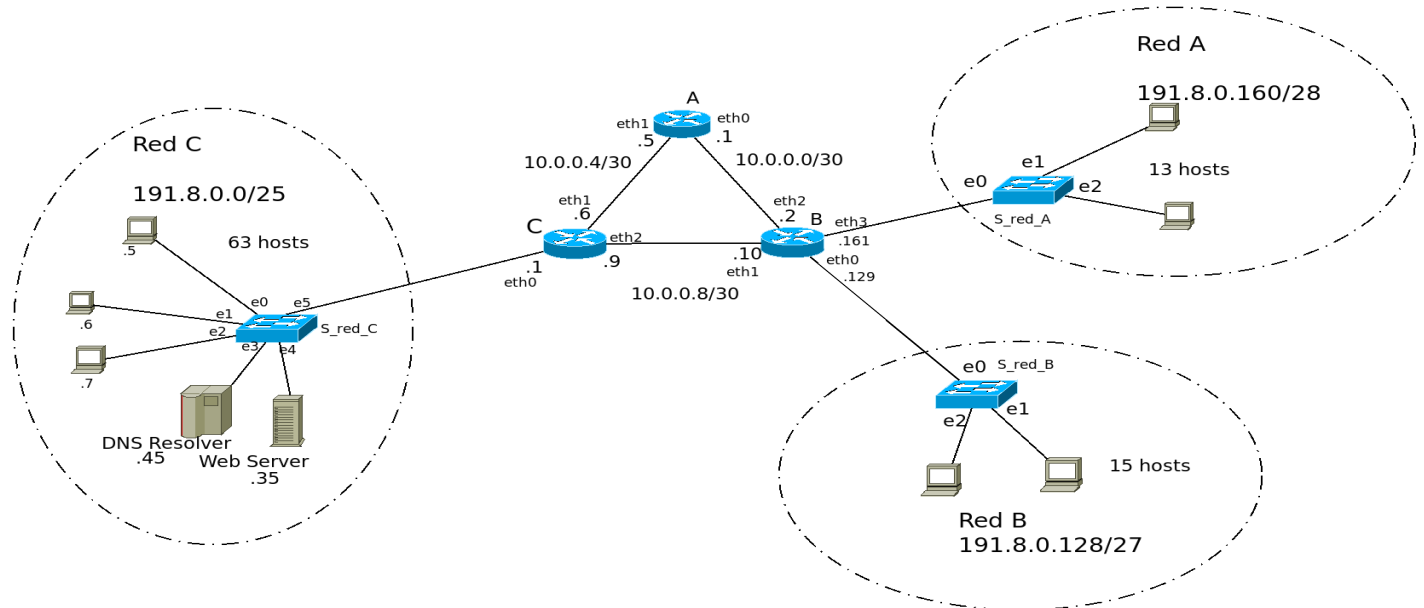


**Redes y comunicaciones - 2da. fecha (06/02/2023)**

Siempre es necesario justificar, las respuestas no debidamente justificadas serán consideradas incorrectas. Considere que todas las tablas cachés están vacías para cada ejercicio.

1) En base a la siguiente topología y la tabla de ruteo del router C, responder:



Router C

Red	Gateway	Máscara	Interface
10.0.0.4	0.0.0.0	255.255.255.252	eth1
10.0.0.8	0.0.0.0	255.255.255.252	eth2
191.8.0.0	0.0.0.0	255.255.255.128	eth0
191.8.0.128	10.0.0.5	255.255.255.224	eth1
191.8.0.160	10.0.0.5	255.255.255.240	eth1
10.0.0.0	10.0.0.5	255.255.255.252	eth1

- IP 161.8.0.5:2323 > 161.8.0.35:80: Flags [S], seq 1363516606, win 512, length 0
- IP 161.8.0.35:80 > 161.8.0.5:2323: Flags [SA], seq 2407054621, ack 1363516610 win 6240, length 0
- IP 161.8.0.165:2836 > 161.8.0.35:80: Flags [S], seq 1273086217, win 512, length 0
- IP 161.8.0.35:80 > 161.8.0.165:2836: Flags [SA], seq 1646827, ack 127308218 win 6240, length 0
- IP 10.0.0.5 > 161.8.0.35: ICMP net 161.8.0.165 unreachable

a) Avisan de un problema de acceso entre los dispositivos y contamos la captura de tráfico realizada en el Web Server. Asumiendo que las IP están correctamente asignadas en los dispositivos de toda la topología, indique qué problemas podrían estar ocurriendo y cuáles serían las soluciones posibles.

Dado que la comunicación entre los hosts de la red C con el web server es exitosa, y que el único fallo es red inalcanzable al intentar enviar un paquete hacia la red A, la causa más factible del problema es que el router A tenga mal configurada su tabla de ruteo. Supongo esto porque la tabla de ruteo del router C también es correcta, y este tiene configurado al router A como next-hop para alcanzar la red A.

Hay 2 soluciones:

- La correcta: arreglar la tabla de ruteo del router A para que envíe correctamente los paquetes.
- La "a la que te criaste": cambiar el gateway de la tabla de ruteo de router C de 10.0.0.5 (router A) a 10.0.0.10 (router B).

- b) Asumiendo que la red está funcionando correctamente, sin tener en cuenta lo evaluado en el punto a, indique de qué forma se podría reducir la tabla de ruteo del router C que se visualiza manteniendo el acceso a todas las redes.

La mejor opción sería agregar un default gateway (0.0.0.0) que sea router A y quitar de la tabla las 3 direcciones que tienen a router A como next-hop.

- c) La empresa decidió migrar únicamente los servidores de la Red C a una nueva red, Red D, conectada al router B usando alguna de las redes disponibles teniendo en cuenta que la dirección inicial a partir de la cual se realizó el subnetting es 191.8.0.0/23. Se debe asignar una de las redes libres de forma que se pueda aplicar CIDR en el router A desperdiciando la menor cantidad posible de direcciones y con la capacidad de asignar direcciones IPs como máximo a 14 hosts.
- i) Indique la dirección de red que se asignará detallando el desarrollo para su obtención.

Red D → 16 hosts → 4 bits  
 191.8.0.0/23 → red inicial  
 191.8.0.0000 0000 /25  
 191.8.0.0 /25 → Red C  
 191.8.0.128/25 → Libre  
 ↳ 191.8.0.1000 0000 /27  
 191.8.0.128 /27 → Red B  
 191.8.0.160 /27 → Libre  
 ↳ 191.8.0.1010 0000 /28  
 191.8.0.160 /28 → Red A  
 191.8.0.176 /28 → Red D

- ii) Realice tabla de ruteo del router A de forma que se pueda acceder a todas las redes por el camino más corto, indicando las redes que se simplificaron.

Destination	Mask	Next-Hop	Iface
10.0.0.4	/30	-	Eth1
10.0.0.0	/30	-	Eth0
191.8.0.0	/25	10.0.0.6	Eth1
191.8.0.128	/27	10.0.0.2	Eth0
191.8.0.160	/28	10.0.0.2	Eth0
191.8.0.176	/28	10.0.0.2	Eth0

Destination	Mask	Next-Hop	Iface
10.0.0.4	/30	-	Eth1
10.0.0.0	/30	-	Eth0
191.8.0.0	/25	10.0.0.6	Eth1
191.8.0.128	/26	10.0.0.2	Eth0

2) ¿Cómo quedaría la tabla CAM del switch S\_red\_C luego del intercambio de la captura del webserver? (solo tener en cuenta los mensajes que se muestran en la captura)

S_red_C	
MAC	PORT
MAC_PC-5	E0
MAC_Web-Server	E4
MAC_Router-C_eth0	E5

3) Se desea agregar un servicio de mail para los usuarios de todas las redes. Para asegurarse un buen servicio se agregarán 2 servidores de mail.

- a) Indique todos los registros que se deberán agregar en el servidor de DNS teniendo en cuenta que el dominio es campeones.com y los servidores mailreda.campeones.com (principal) se encuentra en la red D y alt1.mailreda.campeones.com (secundario) en la red A.

campeones.com	5	MX	mailreda.campeones.com
campeones.com	10	MX	alt1.mailreda.campeones.com
mailreda.campeones.com		A	191.8.0.178
alt1.mailreda.campeones.com		A	191.8.0.46

(Podría poner aparte un CNAME para el Pop, pero lo veo más engorroso que beneficioso en este ejercicio)

- b) Al momento que el cliente desea recibir sus mails el servicio deberá cumplir con los siguientes requisitos: no guardar copia de los mails en el servidor por defecto, permitir enviar correos cifrados. Indique cuál es el protocolo elegido.

Dado que no hay que guardar los mails en el servidor, la única opción que tenemos es utilizar el protocolo Pop con la opción de no guardar los mails en el servidor una vez descargados.

Por otro lado, para enviar mails cifrados, además del protocolo SMTP, necesitamos cifrarlo con SSL u otro método de cifrado.

4) Teniendo en cuenta la tabla de ruteo y captura que se muestran en el punto 1, y asumiendo que desde el router B se accede a la Red C por router C, indique qué evento/s de la captura producirán tráfico ARP entre los routers B y C y cuáles serían los ARP Request (indicar datos de Ethernet y ARP) enviados.

El Syn enviado desde la red A hacia la red C produciría tráfico ARP entre los routers B y C.

MAC origen	MAC destino	ARP packet	
MAC_routerB_eth1	FF:FF:FF:FF:FF:FF	MAC origen: MAC_router-B_eth1 IP origen: 10.0.0.10	MAC destino: ??? IP destino: 10.0.0.9

5) En base a la siguiente salida de un comando ejecutado en PC-A, seleccione las opciones verdaderas.

Proto	Dirección local	Dirección remota	State
udp	127.0.0.1:53	0.0.0.0:*	
tcp	0.0.0.0:25	0.0.0.0:*	Listen
tcp	127.0.0.1:143	0.0.0.0:*	Listen
tcp	127.0.0.1:110	0.0.0.0:*	Listen
tcp	0.0.0.0:993	0.0.0.0:*	Listen
tcp	127.0.0.1:25	127.0.0.1:31866	Established
tcp	127.0.0.1:31866	127.0.0.1:25	Established
tcp	202.1.2.2:17236	21.2.6.6:443	Established
tcp	202.1.2.2:32232	21.2.6.6:443	Established
tcp	202.1.2.2:25	21.2.6.6:8273	Established
tcp	202.1.2.2:15647	21.2.6.6:110	Established

- I. Si otra PC en la red de PC-A envía un segmento a PC-A con el flag SYN y puerto destino 110, recibirá como respuesta un RST/ACK. → Verdadero, pues solo está escuchando la interfaz de loopback
- II. La PC-A tiene establecida una conexión IMAP. → Falso
- III. La PC-A tiene establecida una conexión POP. → Verdadero, tiene una conexión con POP en el puerto remoto 110
- IV. Hay un total de 6 conexiones TCP establecidas. → Falso, son 5. Porque 2 son las interfaces de loopback conectadas entre si
- V. La PC-A tiene la IP 127.0.0.1 → Depende a qué se refiere la afirmación. No es la IP de la pc, pero tenerla la tiene. Todas las computadoras tienen la dirección de loopback
- VI. La PC-A tiene la IP 21.2.6.6. → Falso. Es la IP remota

6) En base a la salida completa, seleccione una o más de una respuesta correcta:

```
HTTP/1.1 200 OK
Date: Mon, 03 May 2021 02:25:12 GMT
Server: Apache
Last-Modified: Thu, 27 Apr 2017 13:43:00 GMT
Accept-Ranges: bytes
Content-Length: 430
X-XSS-Protection: 0;
Content-Type: text/html
```

- I. Se utilizó el método HEAD para realizar la consulta. → Verdadero
- II. Si la consulta hubiese llevado la cabecera "If-Modified-Since: Thu, 29 Apr 2017 17:31:00 GMT" el servidor habría respondido con el código "HTTP/1.1 304 Not Modified". → Verdadero
- III. Tiene un total de 8 cabeceras. → Son 7
- IV. Se utilizó el método GET para realizar la consulta. → Usa el HEAD
- V. La respuesta incluye el recurso solicitado. → Verdadero
- VI. El servidor solo devolvió los encabezados de la página. → Verdadero

7) Indique cuáles de las siguientes opciones son correctas en relación a IPv6.

- I. La dirección ff00::4437:39ff:fe65:f518 es una dirección IPv6 válida para asignar a un servidor web que deba ser accesible en Internet. → Es una dirección multicast
- II. La dirección ::/128 hace referencia a la máquina local (localhost). → No, al default (0.0.0.0)
- III. El checksum en IPv6 permite detectar errores en un paquete. → IPv6 quitó el checksum
- IV. El protocolo Neighbour Discovery requiere ICMPv6 para funcionar. → Verdadero
- V. Es posible comunicar dos redes IPv6 por medio de una red IPv4. → Verdadero