



Todas las respuestas se consideran válidas **solo** si están debidamente justificadas.

### Ejercicio 1

Se dispone de un satélite de órbita baja que se encuentra a 2000 km de distancia de la Tierra, que posee una cámara fotográfica que permite capturar y transmitir imágenes con una resolución de 800x600 pixeles a una tasa de 30 imágenes por segundo. El canal de comunicaciones tiene un ancho de banda de 27 MHz y la velocidad de propagación es 300 000 km/s. Para transmitir las imágenes se usa un protocolo Go-back-N con un frame de 4 kb de largo. Se necesita conocer:

- a. La relación señal ruido mínima (expresada en decibeles) para que la comunicación se pueda establecer, si los pixeles se codifican con 24 bits y las imágenes se suponen equiprobables.

Rta:

$$H = \log_2(N) = \log_2((2^{24})^{800 \times 600}) = 24 \times 800 \times 600 = 11520000 \text{ bits/img} = 11,52 \text{ Mb/img}$$

$$C = 30 \text{ img/s} = 345,6 \text{ Mbps}$$

$$SNR = 2^{\frac{C}{B}} - 1 = 2^{\frac{345,6}{27}} - 1 \approx 7130,55$$

$$SNR_{dB} = 10 \log_{10}(7130,55) \text{ dB} \approx 38,53 \text{ dB}$$

- b. La cantidad de frames a secuenciar dado que se está usando un tamaño de ventana que maximiza la eficiencia del protocolo

Rta:

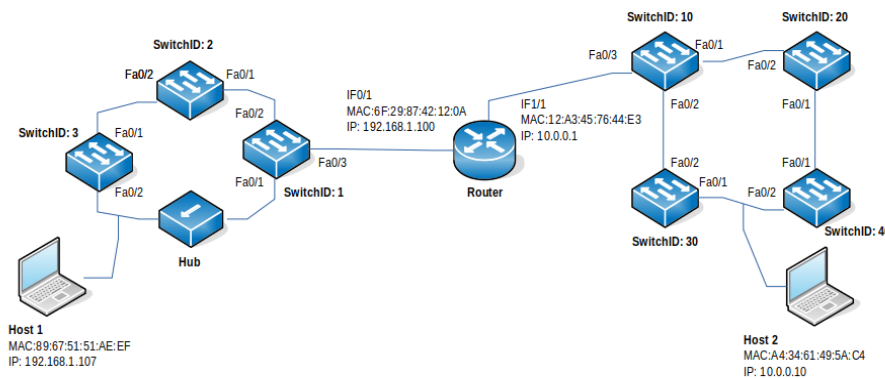
$$Delay = T_{tx} + T_{prop} = 4 \text{ kb} / 3456000 \text{ kbps} + 2000 \text{ km} / 300000 \text{ km/s} \approx 6,678 \text{ ms}$$

$$SWS = V_{tx} * RTT / |Frame| = 345600 \text{ kbps} * 13,356 \text{ ms} / 4000 \text{ bits} = 1153,958 = 1154$$

$$\#Frames \geq SWS + RWS = 1154 + 1 = 1155$$

### Ejercicio 2

En la red de la figura un router separa dos LAN implementadas con switches que tienen un host cada una. En cada LAN, el Spanning Tree Protocol convergió y ya están bloqueadas interfaces según la configuración de SwitchIDs.



- a. Suponiendo que los switches ya aprendieron todas las direcciones MAC, mostrar la tabla de forwarding del switch que queda como root en cada LAN.

Rta:

SwitchID: 1, LAN de la izquierda.

| MAC               | Interfaz |
|-------------------|----------|
| 6F:29:87:42:12:0A | Fa 0/3   |
| 89:67:51:51:AE:EF | Fa 0/1   |

SwitchID: 1, LAN de la derecha.

| MAC               | Interfaz |
|-------------------|----------|
| 12:A3:45:76:44:E3 | Fa 0/3   |
| A4:34:61:49:5A:C4 | Fa 0/2   |

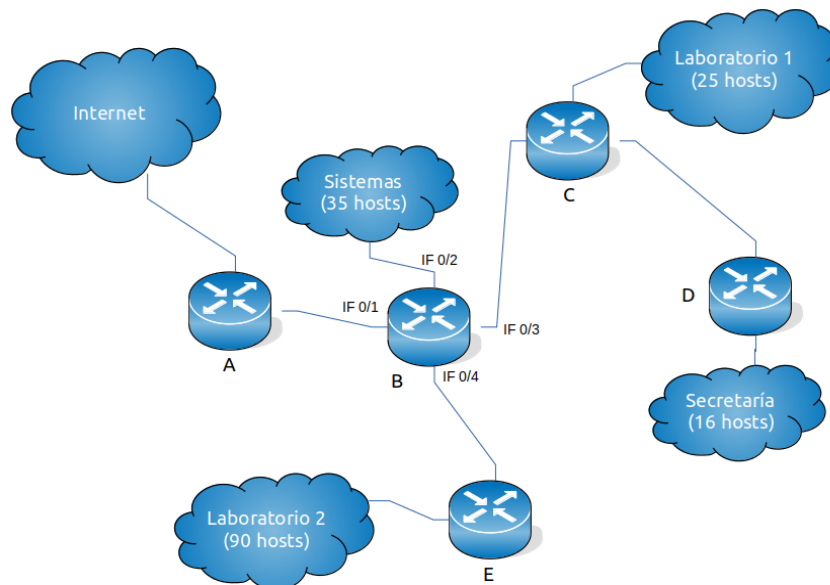
- b. Mostrar una configuración para la tabla de forwarding del router de manera que el Host 1 pueda comunicarse con el Host 2 a nivel IP.

Rta:

| Network        | Next Hop |
|----------------|----------|
| 192.168.1.0/24 | IF 0/1   |
| 10.0.0.0/8     | IF 1/1   |

### Ejercicio 3

En la figura se muestra como están organizados los hosts de un departamento de una universidad mediante routers IP. La universidad dispone del rango IP 200.10.2.0/24 para asignar direcciones IP en todas las interfaces que haga falta. Los routers no usan NAT. En los enlaces punto a punto se puede usar la red privada 10.0.0.0/8. El router A que se conecta con Internet ya tiene la interfaz conectada con el proveedor de servicio y dicha interfaz es configurada y administrada por afuera de la universidad.



- a. Asigne las subredes IP del rango disponible para la universidad, aclarando la dirección de red, de broadcast y máscara de cada subred. *Usar subredes privadas /30 para los enlaces punto a punto entre routers.*

Rta:

Laboratorio 2 - Red: 200.10.2.128/25, Broadcast: 200.10.2.255

Sistemas - Red: 200.10.2.0/26, Broadcast: 200.10.2.63

Laboratorio 1 - Red: 200.10.2.64/27, Broadcast: 200.10.2.95

Secretaría - Red: 200.10.2.96/27, Broadcast: 200.10.2.127

- b. Suponga que la universidad funciona como un sistema de ruteo autónomo que usa el protocolo RIP para distribuir la información. Una vez ya convergidas las tablas, muestre un posible mensaje RIP que el router B le envía a sus vecinos. *No hace falta mostrar el header.* Muestre, además, la tabla de forwarding de B.

Rta:

El router B envía a sus vecinos la información de cuantos routers intermedios hay para llegar a cada subred.

|                 |
|-----------------|
| (Header)        |
| 200.10.2.128    |
| 255.255.255.128 |
| 1               |
| 200.10.2.0      |
| 255.255.255.192 |
| 0               |
| 200.10.2.64     |
| 255.255.255.224 |
| 1               |
| 200.10.2.96     |
| 255.255.255.224 |
| 2               |

| Network         | Next Hop  |
|-----------------|-----------|
| 10.0.0.0/30     | IF 0/1    |
| 200.10.2.0/26   | IF 0/2    |
| 10.0.0.8/30     | IF 0/3    |
| 10.0.0.12/30    | IF 0/4    |
| 200.10.2.128/25 | 10.0.0.13 |
| 200.10.2.64/26  | 10.0.0.9  |
| 0.0.0.0/0       | 10.0.0.1  |

#### Ejercicio 4

Una conexión TCP ya establecida tiene en el transmisor una ventana de congestión en 30 kB y su Ssthresh en 16 KB. Con estos valores, entra en un período *idle*. Luego de este período, el transmisor desea enviar 40 kB de datos. El receptor siempre anuncia una *AdvertisedWindow* de 50 kB.

- a. Suponiendo que no se pierde ningún segmento (Ni de datos ni de ACK) ¿Cuál es el valor de CWND después que llegan todos los ACKs que reconocen datos?

Rta:

| RTT | CWND | RWND | Ssthresh | FlightSize | LBS  |
|-----|------|------|----------|------------|------|
| 1   | 4KB  | 50KB | 16KB     | 4KB        | 4KB  |
| 2   | 8KB  | 50KB | 16KB     | 8KB        | 12KB |
| 3   | 16KB | 50KB | 16KB     | 16KB       | 28KB |
| 4   | 18KB | 50KB | 16KB     | 12KB       | 40KB |

CWND queda en 18KB.

- b. Luego del envío de datos, el host emisor envía un segmento sin datos que tiene sólo el flag FIN prendido. Describir una secuencia válida de envío de segmentos y cambios de estados en ambos extremos de la conexión hasta que se termina de cerrar.

Rta:

El emisor comienza el cierre con el segmento con FIN y pasa a FIN\_WAIT\_1.

El receptor recibe el FIN, envía un FIN+ACK y pasa a CLOSE\_WAIT y después a LAST\_ACK.

El emisor recibe el FIN+ACK, envía un ACK y pasa a TIME\_WAIT.

El receptor recibe el ACK y pasa a CLOSE.

Después de 1 minuto (2 life time segments), el emisor pasa a CLOSE.

#### Ejercicio 5

Un usuario usa POP3 para bajar los mails de su casilla a su computadora. El servicio de POP3 tiene autenticación durante la conexión. En su casilla de mail se encuentra solamente el siguiente mail:

```
To: shepard@n7.com
From: liara@normandy.com
Subject: ME4 Announced!
MIME-Version: 1.0
Content-Type: text/html; charset = "iso-8859-1"
<html> <head></head>
<body>
Mass Effect 4 anunciado!
<br />
<a href="http://bioware.com/virus.php?id=liara@normandy.com">Reserva YA!</a><br />
<br />
<br />
<iframe src="http://masseffect.com" /><br />
</body>
</html>
```

a. ¿Cuántos RTTs se necesitan como mínimo para que el usuario pueda descargar este mail usando POP3?

Rta:

Lo mínimo usando autenticación sería:

1 RTT por establecimiento de conexión

1 RTT por el comando APOP (pueden usar USER y PASS también, eso serían 2 RTTs)

1 RTT por el comando LIST

1 RTT por el comando RETR

b. Suponiendo que la computadora se conecta a la web directamente y que en todas las conexiones se usa HTTP/1.1, detalle los mensajes HTTP (Requests y Responses) que desencadena la apertura del mail en la computadora del usuario. Suponga que bioware.com y masseffect.com ya están resueltos a nivel DNS y dichas IPs son distintas.

Rta:

1) Se envía un GET pidiendo la imagen como el siguiente: GET /header.png HTTP/1.1 Host: bioware.com y vuelve 200 OK con la respuesta

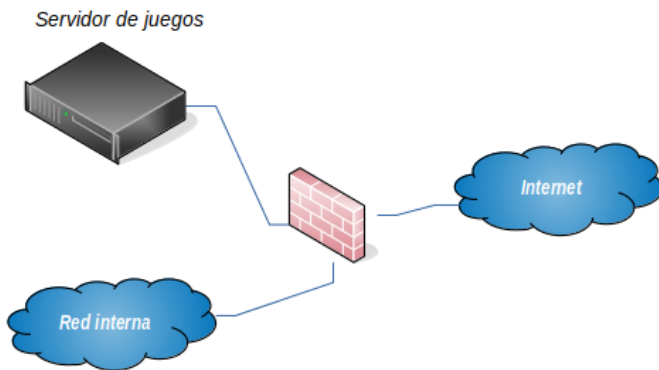
2) Se envía un GET pidiendo la imagen como el siguiente: GET /flyer.png HTTP/1.1 Host: bioware.com y vuelve 200 OK con la respuesta

3) Se envía un GET pidiendo la imagen como el siguiente: GET /footer.png HTTP/1.1 Host: bioware.com y vuelve 200 OK con la respuesta

4) Se envía un GET pidiendo el html como el siguiente: GET / HTTP/1.1 Host: masseffect.com y vuelve 200 OK con la respuesta

## Ejercicio 6

En la figura se muestra como está organizada la red de una universidad en la que se usa una zona demilitarizada de manera de exponer el servidor de juegos a Internet y que la red interna no quede expuesta. El servidor de juegos necesita exponer como puerto entrante el 5000 de UDP y poder conectarse con otros jugadores al puerto 2099 de TCP. Esto tanto para jugadores internos como de Internet. Desde la red interna, los usuarios pueden navegar la web sólo de forma segura, y también pueden realizar consultas DNS a un servidor con IP 8.8.4.4 en Internet.



- a. Muestre las reglas de *firewall statefull* que permitan proteger a la red de la compañía de posibles atacantes en Internet  
Rta:

Regla default: DROP

Una para la salida DNS:  $\langle RedInterna, *, 8.8.4.4, 53, UDP \rangle$

Una para la web segura:  $\langle RedInterna, *, Internet, 443, TCP \rangle$

Una para que se puedan recibir mensajes al UDP 5000 desde Internet:  $\langle Internet, *, GamingServer, 5000, UDP \rangle$

Una para que se puedan enviar mensajes desde TCP 2099 a Internet:  $\langle GamingServer, *, Internet, 2099, TCP \rangle$

Una para que se puedan recibir mensajes a UDP 5000 desde RedInterna:  $\langle RedInterna, *, GamingServer, 5000, UDP \rangle$

Una para que se puedan enviar mensajes desde TCP 2099 a RedInterna:  $\langle GamingServer, *, RedInterna, 2099, TCP \rangle$

- b. Los usuarios necesitan poder autenticarse con garantías de no repudio al servidor de juegos. También es importante garantizar integridad para evitar hacks de superpoderes. Explique qué información tiene que tener el cliente y el servidor para que esto sea posible.

Rta:

Cada cliente debe tener generada una clave pública y su respectiva clave privada. El server debe tener la clave pública de cada cliente autorizado a jugar. Se asume que este intercambio se realizó previamente y de manera segura. Además, cliente y servidor deben ponerse de acuerdo en los algoritmos a usar para implementar firma digital. Una posible combinación es RSA para criptografía asimétrica y SHA-3 para el cálculo de hashes (integridad)