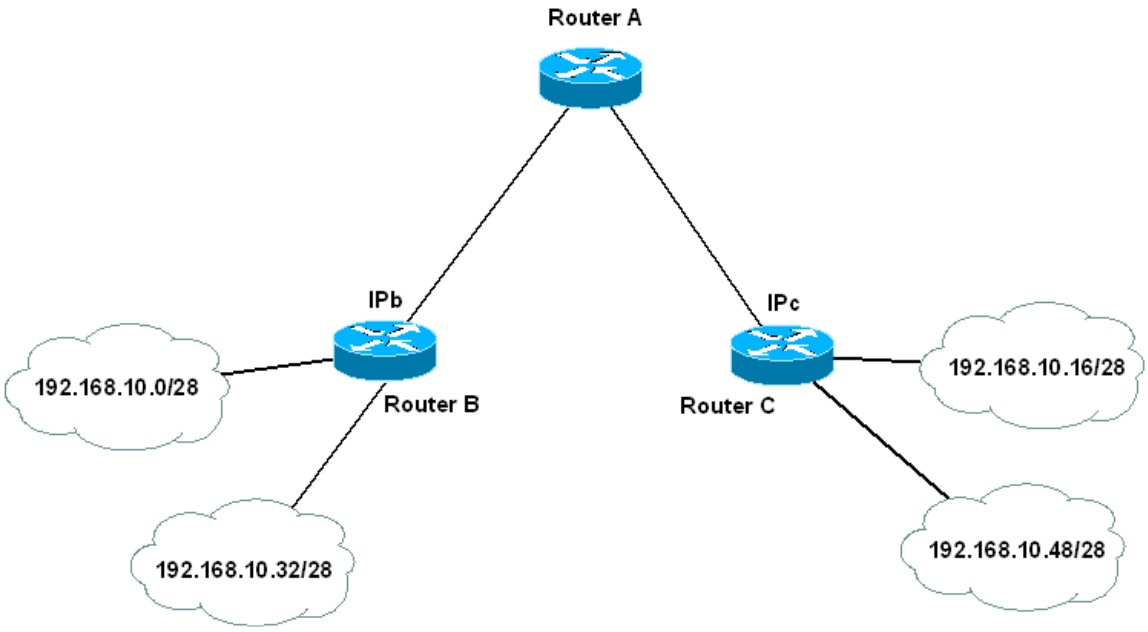
Redes de Datos
1er parcial año 2010

- Las hojas se escriben de un solo lado y preguntas separadas se responden en hojas separadas.
- Letra clara y legible. Respuesta concisa.
- Nombre, número de cédula y número de pregunta en cada hoja.
- Duración del parcial 3 horas. Puntaje total 50 puntos (50% de la suma de parciales)

Pregunta 1 (15 puntos)

a) Indique las funciones involucradas en el encaminamiento de paquetes en una red IP, describiendo brevemente cada una. Indique qué información contienen las tablas de ruteo y cómo se utilizan las mismas.

b) En la siguiente figura indique cómo sería la tabla de ruteo del **Router A** si no se utilizan rutas por defecto.



c) Plantee una solución que permita aplicar ruteo jerárquico de forma de minimizar la cantidad de rutas de la tabla del **Router A** (para esto considere que estas redes pertenecen al mismo proveedor y pueden intercambiarse entre sí).

Respuesta Pregunta 1

a) Las funciones involucradas en el encaminamiento de paquetes son 2, la función de ruteo y la de forwarding.

La función de ruteo se encarga de determinar el contenido de la tabla de ruteo, la cual puede ser estática o dinámica. Para la actualización dinámica se utilizan protocolos de ruteo que, intercambiando información entre los routers de la red y utilizando algoritmos, establecen el contenido de la tabla. Los protocolos de ruteo se encargan de recopilar información de los routers de la red, mientras que los algoritmos deciden en base a la información recogida, el mejor camino para un cierto destino.

Por otro lado, la función de forwarding se encarga de encaminar los paquetes consultando a la tabla de ruteo, la cual se realiza paquete a paquete. Las entradas en la tabla de ruteo se ordenan desde aquellas con máscaras más largas (más 1's) hacia las que tienen máscaras más cortas (menos 1's). Las máscaras más largas indican redes más pequeñas y por lo tanto son entradas más específicas. La función de forwarding decide en base al contenido de la tabla de ruteo, el próximo salto de cada paquete. Para esto utiliza el algoritmo *longest prefix match*. Dado un destino, se recorre la tabla haciendo un AND con las máscaras de cada entrada y determinando si el prefijo coincide. Si es así, se elige la entrada (se encamina el paquete al próximo salto) y si no, se compara con la siguiente. Si no se encuentra ninguna coincidencia, se descarta el paquete.

b) Tabla de ruteo de A:

Nombre	RED	Próximo salto
Red 1	192.168.10.0/28	IPb
Red 2	192.168.10.32/28	IPb
Red 3	192.168.10.16/28	Ipc
Red 4	192.168.10.48/28	IPc

c) Una posibilidad para la asignación de los rangos a las diferentes subredes, que permita la aplicación del ruteo jerárquico, es la de intercambiar los rangos pertenecientes a la Red 2 con la Red 3. De esta manera, las direcciones que van desde la 192.168.10.0 a la 192.168.10.31 quedarán detrás del Router B mientras que las demás quedarán detrás del Router C. La tabla de ruteo de A sería entonces:

RED	Próximo salto
192.168.10.0/27	IPb
192.168.10.32/27	IPc

Pregunta 2 **(10 puntos)**

a) Explique las diferencias entre un protocolo **orientado a conexión** y uno **no orientado a conexión**. Explique y ejemplifique en qué aplicaciones es más apropiado utilizar uno u otro tipo de protocolos.

b) ¿Por qué es necesario realizar **control de flujo**? ¿Es lo mismo que **control de congestión**? Justifique.

Respuesta Pregunta 2 **(10 puntos)**

a) En los protocolos orientados a conexión previo a cualquier intercambio de datos, se debe establecer una conexión, una vez que está establecida la conexión recién podemos comenzar a enviar datos. Finalizado el envío de datos se procede a finalizar la conexión. Como contraposición, un protocolo no orientado a conexión, realiza el intercambio de datos sin necesidad de establecer previamente una conexión.

El establecimiento de una conexión, puede implicar reserva de recursos para poder cumplir con la tarea. No necesariamente el establecimiento de una conexión implica que las unidadades de datos viajen por un mismo camino. Por ejemplo, en el caso de un protocolo de capa de transporte, como esta capa es de extremo a extremo, no conoce el camino de las unidadades de datos por la red, que es determinado por la capa de red. De todas formas, existen reservas de recursos (en TCP serían los buffers de recepción y transmisión) en ambos extremos y se acuerdan parámetros generales de la conexión (por ejemplo SACK y Window Scale en TCP).

Es interesante destacar que porque el protocolo sea orientado a conexión no implica que sea confiable, es decir, es posible tener pérdida de información. Normalmente la confiabilidad se termina implementando utilizando ventanas deslizantes, números de secuencia y reconocimientos. En los protocolos no orientados a conexión, no hay reserva de recursos (previos) en ningún

momento. Tampoco hay necesariamente unicidad de camino y por tanto diferentes unidades de datos de una misma comunicación pueden tomar diferentes caminos (pasar por diferentes equipos intermedios o en diferente orden) hasta llegar al destino. No habiendo reservas de recursos y garantías de qué camino tomar hasta el destino, es más difícil poder garantizar cotas para el retardo de ida y vuelta, y variaciones del mismo.

Si estamos en el contexto de capa de transporte orientada a conexión o no orientada a conexión, y además capa de transporte confiable o no confiable, las combinaciones que tienen mayor interés son: protocolo confiable orientado a conexión y protocolo no confiable no orientado a conexión. En este contexto, un protocolo confiable orientado a conexión (como TCP), es lo aconsejable cuando lo que prima es que la información llegue correctamente y no importa el tiempo que lleve (las posibles perdidas requerirán retransmisiones). Para aplicaciones como la voz, en donde si no llegan las muestras antes del instante en que las tengo que presentar al oyente, no tiene sentido que se retransmitan mas tarde la información faltante, es preferible concentrarse en información nueva. En estos casos es preferible usar un protocolo no confiable no orientado a conexión (como UDP).

Asumiendo que tenemos a TCP y UDP como exponentes de ambas alternativas, es posible utilizar UDP en aplicaciones que transmitan pocos paquetes de datos, por lo cual demoran mas tiempo utilizando TCP por el control de congestión que dispone. También en aplicaciones que involucren un protocolo sencillo de intercambio como un paquete de consulta y un paquete de respuesta, utilizando UDP me ahorro el tener que iniciar la conexión y finalizarla.

b) El objetivo del control de flujo es regular la comunicación entre dos hosts que estén intercambiando datos, mediante mecanismos aplicados a alguno ó ambos hosts. El mismo es necesario para evitar que un transmisor de gran velocidad sature a un receptor de menor capacidad. Si un host transmite a una tasa que el receptor no puede procesar, se comienzan a perder datos y aparecen retransmisiones, lo que empeora aún más la situación. El control de flujo regula el intercambio de datos para evitar lo anterior, llevando a una comunicación lo más eficiente posible.

   Por otro lado, la congestión es la sobrecarga de algún elemento de la red ocasionada por sobreutilización (posiblemente momentánea) de algún recurso, ya sea capacidad disponible en un enlace, capacidad de procesamiento de un equipo, etc.

Pregunta 3 **(10 puntos)**

Dos aplicaciones en las máquinas **A** y **B** intercambian datos utilizando el protocolo TCP.

a) ¿Que funciones cumplen las banderas **FIN**, **ACK**, y **SYN** del encabezado TCP? Realice un diagrama del establecimiento de la conexión TCP indicando cuáles de éstas banderas se utilizan (y de qué manera lo hacen). Indique cómo se utilizan los números de secuencia en el establecimiento de la conexión.

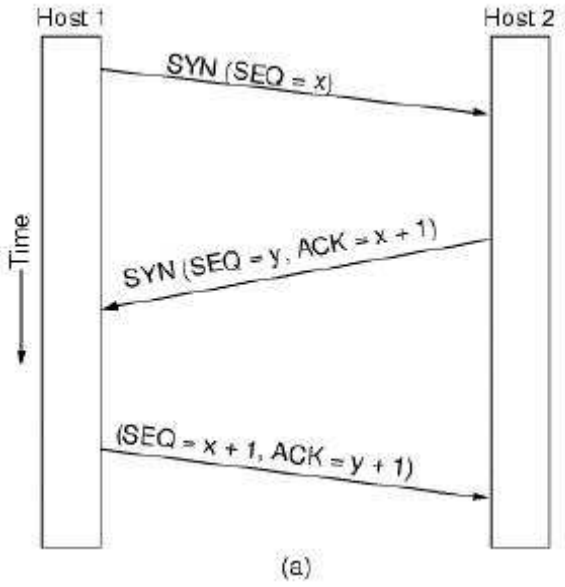
b) Durante el intercambio de datos entre **A** y **B**, luego de establecida la conexión, la máquina **A** no recibe una confirmación de **B** sobre su último envío (llamémosle **copia1** al segmento original), por lo que retransmite el segmento no confirmado (llamémosle **copia2** a la retransmisión). Al cabo de un tiempo, **B** recibe las dos copias del segmento tal como **A** las envió. ¿Tiene alguna forma **B** de detectar que se trata de dos copias de la misma información? Justifique su respuesta.

Respuesta Pregunta 3

a) **Bandera ACK:** Cuando esta bandera se establece en 1, indica que los datos del campo *acuse de recibo* son válidos. Es decir, se utiliza para indicar que el segmento enviado es un reconocimiento de algún paquete recibido. También se utiliza esta bandera durante el establecimiento de conexión, como se verá más adelante.
   Bandera FIN: Este bit se utiliza para liberar una conexión. Cuando un transmisor no tiene más datos para enviar lo enciende. De esta manera el receptor entiende que el transmisor no tiene más datos para enviar y quiere liberar la conexión. Este cierre de conexión es solamente en un sentido, ya que el receptor podría seguir enviando datos al transmisor hasta que él mismo no envíe la bandera FIN encendida.

Bandera SYN: Esta bandera se utiliza para el establecimiento de conexiones. Un host envía las banderas SYN=1 y ACK=0 (connection request) para indicar que desea establecer una conexión. La respuesta a este segmento también utiliza la bandera SYN=1, esta vez junto a ACK=1 (connection accepted).

A continuación se muestra un diagrama del establecimiento de conexión TCP:



En los paquetes intercambiados se utilizan las banderas SYN (paquetes 1 y 2) y la ACK (paquetes 2 y 3). En el primer paquete el Host1 utiliza la bandera SYN=1 indicando que quiere iniciar una conexión, a lo que el host 2 responde también con SYN=1 pero además con ACK=1. Por último el tercer paquete, Host 1 envía solamente ACK=1 para dar por terminado el establecimiento de conexión.

Los números de secuencia juegan un papel muy importante en el establecimiento de conexión TCP, permitiendo asegurar que se establece una única conexión y evitando que paquetes duplicados o perdidos generen problemas al establecimiento.

La gestión de los números de secuencia durante el establecimiento es la siguiente: Cuando el Host 1 va a enviar el primer segmento genera un número de secuencia propio a partir de su reloj interno, y siguiendo algunas reglas en su elección para asegurarse que ese número no este en uso en la red. Dicho número lo envía en el primer segmento del establecimiento. A continuación Host 2 genera de la misma manera su propio número de secuencia, independiente del de Host 1, que envía en el segundo segmento intercambiado. A su vez, en dicho segmento Host 2 reconoce el número de secuencia de Host 1, indicando cual es el siguiente número que espera recibir. Por último en la tercer etapa del establecimiento Host 1reconoce el número de secuencia de Host 2.

b) B es capaz de detectar que se trata de un duplicado, ya que ambos segmentos tienen igual número de secuencia. B va a aceptar el primero que reciba, y luego descartará el segundo, al ver que tiene unnúmero de secuencia menor al que esta esperando.

Pregunta 4 **(15 puntos)**

a) Explique la función de al menos 4 tipos de registros del servidor de nombres (DNS).

- SOA (Inicio de Autoridad): Nombre del servidor primario de dominio, tiempos de vida, correo del administrador.
- A (Dirección IP): Mapea un nombre hacia una dirección IP.
- MX (Manejo de correo): Nombre de máquina u otro dominio que recibe correo para este dominio.
- NS (Servidor de nombres): Nombre de una máquina servidor de nombres para este dominio.

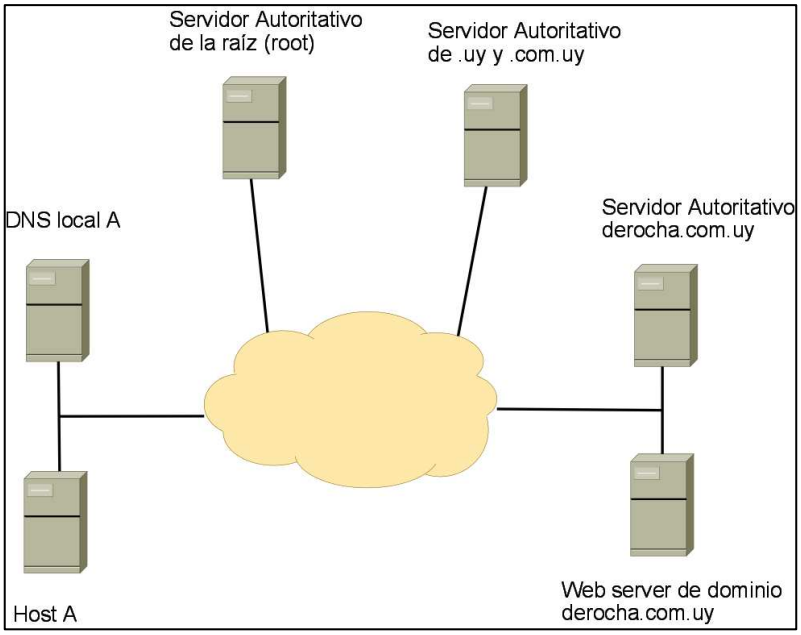
- CNAME (Nombre canónico): Permite crear un alias al nombre de máquina.
- PTR (Puntero): Mapea dirección IP hacia nombre de máquina.

b) En el esquema de la figura, considere que el **Host A** tiene configurado como servidor local recursivo al **DNS local A** y que el resto de los servidores de DNS involucrados no responden consultas recursivas.

Tomando como referencia dicho esquema, describa la totalidad de consultas DNS que ocurren cuando un navegador del **Host A** intenta acceder a la página web **www.derocha.com.uy**. Indique:

- El orden en que se realizan
- Los registros involucrados
- Las respuestas correspondientes

Nota: Al inicio no existe información relevante en el cache de ninguno de los servidores DNS involucrados.

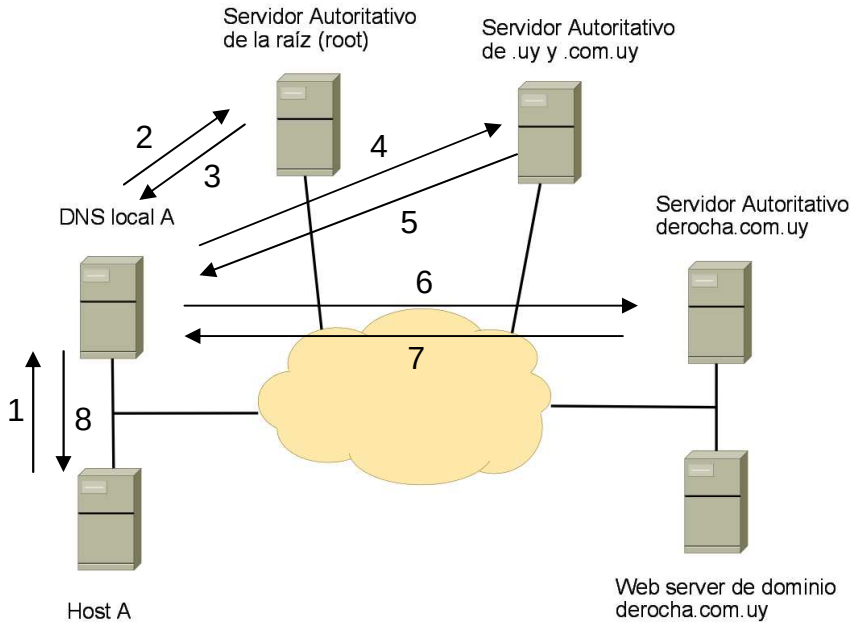


Respuesta Pregunta 4

a)

- SOA (Inicio de Autoridad): Nombre del servidor primario de dominio, tiempos de vida, correo del administrador.
- A (Dirección IP): Mapea un nombre hacia una dirección IP.
- MX (Manejo de correo): Nombre de máquina u otro dominio que recibe correo para este dominio.
- NS (Servidor de nombres): Nombre de una máquina servidor de nombres para este dominio.
- CNAME (Nombre canónico): Permite crear un alias al nombre de máquina.
- PTR (Puntero): Mapea dirección IP hacia nombre de máquina.

b)



1. Consulta por “derocha.com.uy A”?
Como el DNS local A es recursivo, el DNS local A sale a obtener la respuesta.

2. Consulta por “derocha.com.uy A”?

3. uy NS nombre1
Como los servidores de la raíz no son recursivos, se devuelve la mejor respuesta que se tenga, que es justamente quien es el servidor de nombre autoritativo por el dominio “uy”, en principio los root server no tienen porque conocer que el servidor autoritativo del “uy” es el mismo que del “com.uy”.
Nota 1: de alguna forma se debe de obtener la dirección IP del servidor autoritativo del “uy”, no alcanza con el nombre para poder continuar la búsqueda.

4. Consulta por “derocha.com.uy A”?

5. com.uy NS nombre2
Como el servidor autoritativo del “uy” no es recursivo, se devuelve la mejor respuesta que se tenga, dado que el autoritativo del “uy” es también autoritativo del “com.uy”, la respuesta es el servidor de nombre autoritativo del dominio “derocha.com.uy”.
Nota 2: de alguna forma se debe obtener la dirección IP del servidor autoritativo de “derocha.com.uy” para poder continuar la búsqueda.

6. Consulta por “derocha.com.uy A”?

7. derocha.com.uy A nombre3

8. derocha.com.uy A nombre3
Nota 3: de alguna forma para poder realizar la conexión se debe obtener la dirección IP del servidor nombre3.

Aclaración sobre notas Nota 1, Nota 2 y Nota 3: Para poder continuar la búsqueda, hay que obtener las respectivas direcciones IP de los servidores involucrados en los registros NS y A (nombre1, nombre2 y nombre3) de las respuestas 3, 5, 7. Estas direcciones IP pueden venir adjuntas en las respuestas, en la parte de “Additional Section” de las mismas. En caso de no venir adjuntas las direcciones IP en las respuestas, esto desencadena nuevas consultas (iniciadas por el servidor recursivo DNS local A) para poder obtener los registros A (dirección IP) de los servidores nombre1, nombre2 y nombre 3.