28 de setiembre de 2022

Redes de Datos 1
1er parcial – 2022
Solución

Esta es una posible solución a las preguntas planteadas. ***Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta de forma suficiente.***

Pregunta 1 (8 puntos)

a) Explique qué se entiende por congestión en una red y por qué es importante controlarla. ¿Pueden existir diferentes niveles o grados de congestión? Justifique su respuesta.

La congestión ocurre cuando se sobrepasa la capacidad de algún elemento en la red, típicamente de algún enlace o la CPU/memoria de algún enrutador de la red. En esos casos, existen más paquetes de los que se puede procesar o que quieren utilizar un mismo enlace, por lo que se utiliza una cola donde almacenarlos temporalmente hasta poder procesarlos. Cuando los paquetes tienen que esperar en esas colas, tardarán más tiempo en llegar a destino e incluso podrían ser descartados en algún enrutador de la red si se supera la capacidad de la cola de atención.
Los paquetes terminan acumulando las demoras ocurridas en cada salto de red a lo largo se su trayecto y los extremos no conocen exactamente dónde ocurre la congestión, solo se percibe el efecto acumulado.

Es importante controlar la congestión porque las demoras mayores a lo esperado en las respuestas a los segmentos TCP o las pérdidas de paquetes (y con ellos el segmento TCP que transporta), generan retransmisiones. Estas se producen porque TCP un protocolo con garantía de entrega y el transmisor retransmitirá cuando considere que la respuesta no va a llegar. Si se generan retransmisiones, se estarán generando aún más paquetes en la red, pudiendo ocurrir que en las colas existan segmentos con la misma información o que directamente no haya mas lugar en estas colas de atención. Esto contribuirá a aumentar la congestión en un proceso de realimentación positiva que podría llevar a que la red deje de funcionar casi por completo, debido a la sobrecarga de muchos nodos. Si analizamos la información que envía el transmisor y la que recibe el receptor, veremos que muchas retransmisiones bajan el ancho de banda efectivo (información nueva por unidad de tiempo), y peor aun si debido a los descartes nunca llegan los reconocimientos. En pocas palabras la congestión no permite una utilización eficiente de los recursos (idealmente las retransmisiones deberían ser pocas), y degrada la percepción de los usuarios.

La congestión puede ser "leve" cuando en un período de tiempo aumentan un poco los tiempos de encolamiento en algún nodo, y por tanto el RTT (tiempo de ida y vuelta de los mensajes), pero sin llegar a generarse pérdidas. Si los transmisores incrementan la tasa de transmisión, la congestión aumenta, y podría suceder que los tiempos de ida y vuelta excedan el temporizador previsto (timeout de retransmisión en TCP) y entonces comiencen a generarse retransmisiones. En este escenario estamos alcanzando congestión "intermedia" donde tendremos RTT altos, varias retransmisiones y algunos pocos descartes porque no hay lugar en las colas de atención. Si los transmisores persisten en intentar enviar más información, la congestión aumenta aún más y en algún enrutador de la red podría alcanzarse la capacidad máxima de la cola de procesamiento, ocurriendo descartes de paquetes. En este escenario es muy probable que los nuevos envíos no lleguen al receptor y estaríamos en un estado de congestión "severa". Cuanto mas esfuerzo realizo en transmitir (y retransmitir), llega cada vez menos información al destino (o reconocimientos al transmisor).

b) Explique en qué componentes de la red puede ocurrir congestión y cómo concretamente impacta en el procesamiento de los paquetes. Explique cómo perciben la congestión los usuarios finales.

Como se mencionó en a) la congestión puede darse en los enrutadores o enlaces de la red, cada enrutador puede tener varias interfaces, si ocurre un evento que dos paquetes quieren salir por una misma interfaz al mismo tiempo, esto no resulta posible. Uno de ellos debe de esperar, para ello se implementaron las colas de procesamiento, que deben de tener capacidad finita, porque los protocolos confiables retransmiten cuando no llegan los reconocimientos. Un consumo elevado de CPU, agrega demora a la tarea de procesar los paquetes en espera. Los paquetes en la cola de atención deben esperar a que se atiendan los paquetes que están antes que ellos, antes de ser enviados al siguiente salto.

Este aumento de los retardos será visto por los usuarios finales o por sus aplicaciones como enlentecimiento de transacciones, lentitud en el refresco de pantallas, demoras en culminar las descargas, interrupción de las conexiones en caso de pérdidas excesivas. Las eventuales retransmisiones que se generen por congestión determinarán una disminución de la tasa efectiva de intercambio de datos.

c) Explique qué medidas usa TCP para detectar la congestión de la red. Explique cómo intervienen los temporizadores dinámicos en esa detección. Nota: no es necesario incluir las fórmulas de cálculo.

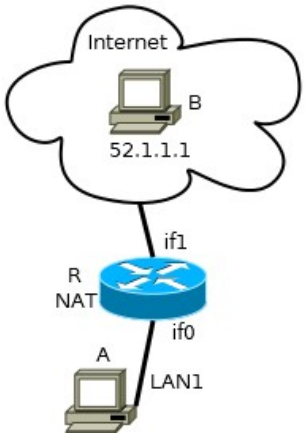
TCP asume que hay congestión cuando no le llegan los reconocimientos de los segmentos a tiempo, asume que los medios físicos actuales son confiables (la tasa de errores en baja) y que no hay pérdidas por otras causas. Esta hipótesis puede no cumplirse en redes donde puede haber mucha interferencia (redes inalámbricas o enlaces distantes con deformación de onda). Para determinar si una respuesta llega o no a tiempo, TCP implementa un temporizador de retransmisión que inicializa con cada segmento que envía. Si ese temporizador expira antes de la llegada del segmento de reconocimiento, TCP asumirá que hay una pérdida (que puede ser en el segmento enviado o en su reconocimiento) debido a congestión.

Como la decisión de si hay o no congestión queda determinada por el valor del temporizador, es importante que se use un valor acorde al tiempo razonable de ida y vuelta en la red, más algún tiempo de guarda o de tolerancia. Como la red puede pasar por diferentes estados (más o menos congestionada), con más o menos equipos intermedios entre dos nodos que quieren intercambiar información, es poco razonable tomar un valor fijo del temporizador. Por este motivo TCP utiliza un temporizador de retransmisión dinámico que va ajustando al comportamiento de la red en cada momento. La idea es medir el tiempo de ida y vuelta de los segmentos (RTT) y construir un estimador estadístico tanto de la media como de la varianza de ese tiempo. En base a esos estimadores se determina el valor del temporizador y por tanto este se ajustará al estado de la red.

En los escenario de congestión severa, no tenemos estimadores de RTT, por la ausencia de ACKs, por lo cual los temporizadores se ajustan con otra estrategia. Formalmente esto ocurre de forma general en ausencia de ningún ACK. En el laboratorio vimos que duplica el último valor de timeout con los re-envíos hasta alcanzar un valor máximo de 120 segundos. Luego re-intenta cada 120 segundos.

Pregunta 2 (10 puntos)

a) Explique por qué fue necesario introducir en IPv4 el mecanismo de traducción de direcciones **NAT/PAT** (Network/Port address translation).
Explique las ventajas y desventajas de usar este mecanismo.



En los comienzos de la red Internet se pensaba en un uso exclusivamente académico de la misma y por tanto utilizada por un grupo reducido de personas o equipos. Las direcciones IP (IPv4) de por si están acotadas al utilizarse un campo de 32 bits en el encabezado del paquete, pero además fueron distribuidas de forma poco eficiente, ya que no se preveía que se terminaran.
Adicionalmente, el uso de máscaras de largo fijo (clases de direcciones), propiciaba un uso poco eficiente de las direcciones.

Con la explosión del uso comercial de internet y aún adoptándose los largos variables de máscara, las direcciones IPv4 empezaron a ser escasas y se entendió que la solución era la creación de un nuevo protocolo IPv6, con mayor espacio de direcciones (128 bits). Sin embargo la definición y adopción de ese nuevo protocolo se sabía que iba a llevar mucho tiempo, principalmente porque algunos equipos no son fáciles de actualizar para soportar ese nuevo protocolo.

Por estos motivos se definió el mecanismo llamado NAT/PAT que contempla el uso de direccionamiento llamado "privado" dentro de las redes y realizar una traducción de las direcciones y puertos cuando esos paquetes tienen que salir a la red "pública". Esto permite seguir usando el mismo protocolo IPv4 y reusar o tener rangos de IPs potencialmente duplicados en diferentes redes del mundo.
El uso de este mecanismo permite que toda una red de una institución sea vista desde el resto de la red con una sola dirección IP. Si antes necesitaba un rango de direcciones para numerar mi red, usando NAT lo puedo hacer con una sola IP pública.
Permite por tanto ahorrar direcciones públicas (las que tienen validez global en la red) y paliar el problema de la escasez de direcciones hasta la completa adopción de IPv6. Esto podría considerarse como que ha resultado en uno de los principales motivos por los cuales la transición a IPv6 se está demorando tanto.

El mecanismo de NAT tiene la ventaja de ser transparente para los equipos de la red interna ya que las traducciones se hacen el el enrutador de salida.

Para implementar este mecanismo los enrutadores que conectan con la red pública (con internet) tienen que soportar esta nueva funcionalidad, lo que implica cambios en su programación y contar con tablas específicas (tabla de NAT), agregadas a la funcionalidad estándar de un enrutador.

El uso de NAT tiene como resultado que la topología interna de la red se oculta hacia el exterior ya que toda la red sale con una (o unas pocas) direcciones IP. Esto podría considerarse un factor de seguridad que aporta el uso de NAT.

También queda naturalmente impedido el tráfico desde cualquier IP del mundo hacia equipos internos a la institución (ya que estos no tienen una dirección pública en la red). Los accesos deseados, se deben configurar manualmente usando tablas de DNAT (Destination NAT) que permiten mapear un puerto de la IP pública con una IP, puerto de un equipo interno. Esto puede considerarte también un aspecto que contribuye a una mayor seguridad de los equipos internos, ya que solamente serán accesibles aquellos que se dispongan.

Una desventaja que se suele mencionar del NAT es que rompe el principio "end-to-end" de Internet, que indica que los nodos intermedios de la red no deberían modificar los paquetes que pasan por ellos, tratando por igual a todos los paquetes de la red. Este principio no se preserva por este y muchos otros motivos.

b) En el diagrama adjunto, la red **LAN1** usa el rango de direcciones **172.16.0.0/28**. El enrutador **R** brinda conectividad a Internet e implementa NAT/PAT, siendo **200.0.0.1** la IP de su interfaz **if1**. Asigne direcciones a **A** y a la interfaz **if0** de **R.**

Podría asignarse cualquier dirección del rango 172.16.0.0/28 para esos dos equipos o interfaces, exceptuando la dirección de red (172.16.0.0) y la dirección de difusión (172.16.0.15). Se asigna arbitrariamente la dirección 172.16.0.1 a la interfaz if0 del enrutador R, y la dirección 172.16.0.2 al equipo A.

c) Suponga que **A** inicia una conexión TCP al puerto **80** de **B** (IP **52.1.1.1**).
Explique cuál sería el contenido de los campos: IP origen, IP destino, puerto origen, puerto destino; para:
   i. el segmento inicial de esa conexión cuando llega y cuando sale de **R**.
   ii. el segmento de respuesta de **B** cuando llega y cuando sale de **R**.

Las conexiones TCP están identificadas por 4 parámetros (IP de origen, IP de destino, Puerto de origen, Puerto de destino). Cuando A inicia una conexión al puerto 80 de B el sistema operativo elegirá un puerto efímero como puerto de origen, para este ejemplo supondremos que ese puerto es el 5555.
De este modo el paquete que sale de A lo hará con la IP privada y el entutador R hará la modificación o traducción de los campos de interés.
Los segmentos solicitados se muestran en la tabla adjunta.

IP origen	***IP destino***	***Puerto origen***	***Puerto destino***	***Comentarios***
172.16.0.2	*52.1.1.1*	*5555*	*80*	*El equipo A envía un segmento hacia B, usando su IP privada y el puerto efímero indicado*
200.0.0.1	*52.1.1.1*	*7777*	*80*	*El equipo R encamina el segmento hacia B, modificando la IP privada por la IP pública. Además para evitar colisiones en el uso del puerto efímero por dos equipos diferentes de la red, se traduce también el puerto de origen por uno elegido por R (para que no haya colisiones)*
52.1.1.1	*200.0.0.1*	*80*	*7777*	*El segmento regresa desde B hacia la IP pública de R y el puerto desde el que se inició la conexión*
52.1.1.1	*172.16.0.2*	*80*	*5555*	*El equipo R encamina el segmento hacia A, modificando la IP pública por la IP privada correspondiente. Además traduce el puerto.*

d) Explique qué información debe almacenar **R** para implementar el NAT/PAT (use los valores de la parte c)).

Para que R sepa hacia qué IP y puerto interno debe encaminar los paquetes que le llegan, guarda en una tabla de NAT las asociaciones que se utilizaron a la salida de los paquetes.
En el caso del ejemplo el enrutador R debe guardar que la IP interna 172.16.0.2 usando el puerto 5555 fue traducida a la IP 52.1.1.1 y puerto 7777. Consultando esta tabla, cuando regrese el paquete de respuesta, sabrá como traducirlo para que llegue al equipo interno adecuado.

Pregunta 3 (3 puntos)

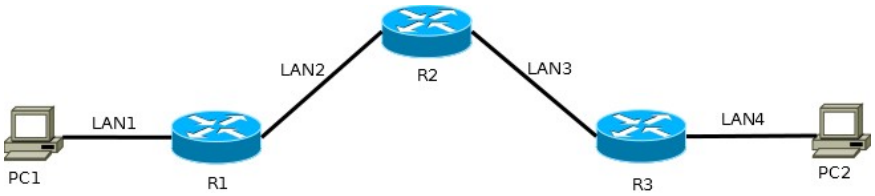
a) Defina los retardos de “propagación”, “serialización o transmisión” y “procesamiento” en una red de datos.

Tiempo o retardo de “propagación” es el tiempo que le lleva a un bit recorrer el largo del enlace hasta llegar al destino. Depende de la velocidad de propagación de la señal en el medio (V) y del largo del medio físico (D), por lo que se calcula como D/V.

Tiempo de “serialización” es el que lleva transmitir todos los bits de un paquete por un enlace. Si el enlace permite transmitir R bits/segundo, transmitir un paquete de L bits tardará L/R segundos.

El tiempo o retardo de “procesamiento” es el tiempo que le lleva a un enrutador examinar el paquete, verificar posibles errores y decidir hacia dónde debe encaminarse el paquete.

b) La red que comunica los equipos PC1 y PC2 está esquematizada en la figura adjunta.
Se considera que:



- La velocidad de transmisión de todos los enlaces LAN es de 1 Gbps (10^9 bits/seg) y tienen 100 metros de longitud
- La velocidad de propagación en el medio es de 200.000 km/s ($2x10^8$ m/s)
- Los enrutadores R1, R2 y R3 introducen un retardo de procesamiento de 1 µs (1 microsegundo)
- Los retardos de encolamiento son despreciables en la red
- El tiempo de procesamiento de los paquetes en PC1 y PC2 es despreciable
- Los paquetes de interés son de 10.000 bits

Calcule el tiempo de ida y vuelta para una transacción consistente en un paquete enviado desde PC1 a PC2 y la correspondiente respuesta desde PC2 a PC1. Se sugiere expresarlo en microsegundos.

El tiempo de ida y vuelta de los paquetes estará dado por la suma de los tiempos de procesamiento, encolamiento, serialización y transmisión en la totalidad del camino de ida y vuelta.

En un enlace de 1Gbps el tiempo de serialización de un paquete de 10000 bits será de 100000/1Gbps segundos o sea $1x10^4$ bits/ 10^9 bits por segundo = 1 $x10^{-5}$ segundos = 10 µs

En un enlace de 100 metros con velocidad de propagación de $2x10^8$ m/s el tiempo de propagación es de $100/2x10^8$ segundos o sea 50 x 10^{-8} segundos = 0,5 x 10^{-6} = 0,5 µs

Por tanto el camino total de ida tendría el siguiente retardo:
- *10 (serialización en PC1) + 0,5 (propagación en LAN1) = 10,5*
- *3 (R1, R2, R3) x (1 (procesamiento) + 10 (serialización) + 0,5 (propagación)) = 34,5*

El tiempo de ida y vuelta será por tanto de: 2 x (10,5+34,5) = 90 µs

c) Sin cambiar la topología (es decir, manteniendo la cantidad de equipos, la longitud de los enlaces y la forma como están conectados), ¿Qué parámetro(s) cambiaría para reducir sustancialmente el retardo total? Justifique su respuesta.

Dado que el retardo que más influye es el de serialización, se podría reducir sustancialmente el retardo total aumentando la velocidad a valores mayores que 1Gbps. La opción de enviar menos bits por paquete (achicar el tamaño del paquete) no es adecuada porque se enviaría menos información y además aumentaría el peso relativo encabezados.

Pregunta 4 (6 puntos)

a) Explique cuál es el cometido principal de la capa de red en el modelo de capas analizado en clase.

La capa de red tiene como cometido principal hacer llegar los paquetes desde origen a destino. Para lograrlo deberá usar los recursos disponibles en la red (enrutadores, enlaces, topología) y en caso de existir más de un camino procurará que los paquetes recorran el "mejor" camino considerando alguna métrica de interés.
Se requerirá un esquema de direccionamiento específico de esta capa para identificar los equipos en la red.
Además la capa de red tiene otras funciones como brindar servicios a la capa de transporte, tarificación.

b) Explique cuáles son las funciones del plano de control y del plano de datos en la capa de red. Explique cómo se vinculan esos planos para cumplir el objetivo explicado en a).

La función del plano de control es determinar los mejores caminos para los paquetes entre un origen y un destino, es decir, implementa la función el ruteo. Para definir los mejores caminos se utiliza una representación de la red como un grafo con nodos, enlaces y costos en los enlaces; y se utilizan algoritmos de ruteo para determinar los mejores caminos en función de su costo. Los algoritmos pueden ejecutarse periódicamente para adaptarse a los cambios del estado de la red. En la arquitectura tradicional, los enrutadores pueden implementar protocolos de ruteo dinámico mediante los cuales intercambian información del estado de la red. A partir de la información recolectada aplican luego un algoritmo para encontrar los mejores caminos. Típicamente los cambios de la red y por tanto de los mejores caminos se realizan en intervalos de tiempo del orden de minutos.
En la arquitectura SDN la función de ruteo se implementa a nivel del controlador de forma centralizada a partir del conocimiento global de la topología de la red.

Los caminos elegidos por el plano de control, se plasman en tablas de forwarding en los enrutadores de la red, ya que cada enrutador debe saber qué hacer con los paquetes que van a un cierto destino. En una red que usa protocolo IP, las tablas asocian rangos de direcciones (red/máscara) con las direcciones IP del próximo enrutador (o próximo salto) más adecuado para las direcciones destino pertenecientes a ese rango. En las redes de CV se usan tablas con la identificación de los CVs establecidos y los conmutadores hacen el swapping de los identificadores.

La función de el plano de datos es la de encaminar los paquetes usando la tabla creada por la función de ruteo. En el caso de IP (datagramas), para cada paquete que recibe un enrutador se debe hacer una búsqueda en la tabla de forwarding para determinar cómo encaminar el paquete. En el caso de CVs la tabla se indexa por los identificadores de CV de entrada, haciendo más simple el forwarding.

Complementando lo explicado anteriormente, simplificadamente se podría decir que la función de ruteo crea o escribe las tablas de forwarding (encaminamiento) y la función de encaminamiento usa o lee esas tablas para saber cómo encaminar cada paquete.

c) Compare las funciones del plano de control y del plano de datos en las arquitecturas de red de datagramas y de circuitos virtuales. Compare ventajas y desventajas de ambas arquitecturas.

En ambas arquitecturas se requiere un plano de control con características similares que aplique algoritmos para determinar los mejores caminos para los paquetes, dada la topología y costo de los enlaces. En la arquitectura de circuitos virtuales (CV), el camino que se elije (circuito virtual) se utiliza para todos los paquetes. En la arquitectura de datagramas, como los paquetes se encaminan de forma independiente de los anteriores, podría suceder que se modifique el camino durante una comunicación y por tanto que paquetes que van hacia el mismo destino recorran diferentes caminos.

En la arquitectura de circuitos virtuales, los paquetes se encaminan en función de la tabla de circuitos virtuales. Esa tabla contiene la información de los circuitos virtuales establecidos asociando un identificador de circuito virtual de entrada con un identificador de circuito virtual de salida. Las entradas de la tabla se crean cuando se establece un nuevo circuito virtual. En esta arquitectura, los enrutadores o conmutadores, cuando reciben un paquete por una interfaz, ingresan en la tabla de CVs usando como índice la interfaz y el identificador de CV del paquete; y obtienen los datos para hacer el encaminamiento del paquete (la interfaz de salida y el identificador de CV de salida).

En la arquitectura de datagramas el encaminamiento se realiza paquete a paquete realizando una búsqueda en la tabla de forwarding.

Las arquitecturas pueden compararse en diferentes aspectos como se indica en la siguiente tabla:

	Datagramas	**Circuitos Virtuales**
Establecimiento previo de un camino para enviar los paquetes	No. Cada paquete se encamina de forma independiente.	Si. Antes de enviar paquetes se requiere establecer un circuito virtual que será utilizado para todos los paquetes de ese flujo.
Dirección para forwarding o encaminamiento de los paquetes	Se necesita la dirección del destino final ya que cada paquete se encamina de forma independiente.	Como los paquetes requieren un CV previamente establecido, luego solo alcanza con la identificador del CV (de cada tramo) para encaminarlo. Es importante notar que el identificador de CV (que tiene alcance local y solo se necesita para distinguir circuitos establecidos) podría tener menos bits que una dirección de alcance global. Esto podría ahorrar bits en los encabezados.
La red almacena el estado de los flujos?	No. Cada paquete se encamina de forma independiente.	Si. El estado de los CVs establecidos se plasma en la tabla de CVs.
Encaminamiento de paquetes	Se busca en la tabla de forwarding la mejor entrada para la dirección del paquete a encaminar.	Se consulta la tabla de CV (no es una búsqueda, es una tabla de doble entrada) y por tanto más rápida que la búsqueda en datagramas.
Fallas en los enrutadores	Afectan solamente a los paquetes en tránsito, ya que si se usa algún mecanismo de ruteo dinámico, la red podría encontrar un mejor camino en la nueva topología (donde se sacan los enlaces o nodos caidos), actualizar las tablas de forwarding y que los siguientes paquetes tomen una ruta alternativa para seguir llegando al destino. Podría haber pérdida de algunos paquetes, pero la comunicación podría seguir su curso.	Cuando se cae un enrutador, se cortan los CVs establecidos porque se borra la tabla de CVs. Como el tráfico requiere un camino previamente establecido, será necesario volver a establecer el CV para poder retomar la comunicación. Si bien hay mecanismos rápidos para el re-establecimiento de CVs, es posible que sean igual más lentos que en el caso de datagramas.
Control de Congestión	Difícil. No hay muchas herramientas en una red de datagramas para saber si hay congestión en la red. Por eso en la arquitectura TCP/IP, se le asigna a la capa de transporte tratar de controlar la congestión.	En este caso es posible, porque al momento de establecer un nuevo CV, los enrutadores podrían rechazar el establecimiento si están congestionados y habrá que recurrir a otros caminos (no congestionados) para establecer el CV.
Calidad de Servicio	Difícil. Tampoco hay muchas herramientas en estas redes para brindar calidad de servicio. Los paquetes se encaminan de acuerdo a su dirección de destino.	En esta arquitectura se pueden reservar recursos al momento de establecer el CV de acuerdo a los requerimientos del flujo. También se pueden establecer caminos diferentes para diferentes tipos de tráfico o de clientes de la red.

Pregunta 5 (10 puntos)

a) Explique para qué sirven y cómo se utilizan los registros tipo **A** y **MX** en el **DNS**.

El registro A asocia una etiqueta o nombre de dominio con una dirección IPv4. Sirve para poder identificar los equipos con nombres más fáciles de recordar e interpretar por los humanos. Por ejemplo el equipo ampere.fing.edu.uy tiene asociado un registro A cuyo valor es 164.73.38.2.

El registro MX asocia una etiqueta o nombre de dominio con el nombre del servidor de correo electrónico encargado de recibir correos para ese dominio. Por ejemplo fing.edu.uy tiene asociado un registro MX de valor smtp.fing.edu.uy. Una particularidad de los registros MX es que tiene asociado un valor de prioridad ya que por redundancia puede haber más de un servidor de correo que atienda a un dominio. Este

registro se usa cuando un servidor tiene que enviar un correo a una dirección particular. Por ejemplo si un servidor tiene que entregar un correo a la dirección info@fing.edu.uy, tendrá que consuiltar al DNS por el registro MX asociado a fing.edu.uy para saber cuál es el servidor al que conectarse para entregar el mail. Como el valor del registro MX es un nombre, habrá que consultar posteriormente (si la información no viene como glue-record) el registro A asociado a ese nombre, para obtener la IP a la cual conectarse.

b) Un servidor de correo en Australia tiene configurado como servidor DNS local recursivo el equipo con dirección IP **IPau** y necesita enviar un correo a la dirección **info@fic.edu.uy**.
Explique detalladamente cómo se realiza la búsqueda en el DNS indicando todos los mensajes en los que participa el servidor DNS local recursivo **IPau**.
Considere que:
- no hay información relevante en ningún cache
- los servidores de primer nivel (TLDs) no responden consultas recursivas
- el servidor de nombres de edu.uy también **es autoritativo** de **fic.edu.uy**
- el servidor de nombres de edu.uy **no es autoritativo** para **fing.edu.uy**
- el tiempo de vida de todos los registros involucrados es de **1 hora**

Se recomienda:
- Utilizar nombres y direcciones IP de fantasía para identificar los equipos (IPns1, ns1.dominio).
- Ilustrar con un diagrama la secuencia de consultas y respuestas.
- Completar una tabla con la secuencia de consultas y respuestas. Para una respuesta completa, se sugiere usar el siguiente formato para la tabla:

Secuencia	**Equipo Origen**	**Equipo Destino**	**Consulta o Respuesta**	**Observaciones**
1	Nombre fantasía 1	Nombre fantasía 2	Cuál es el valor del registro Z?	Explicación…

La consulta DNS se inicia desde el servidor de correo en Australia, que es el que quiere enviar un correo a la dirección info@fic.edu.uy. Para necesitará averiguar el registro MX asociado al nombre de dominio fic.edu.uy. Se presenta a continuación el procedimiento de la búsqueda:

#	***Origen***	***Destino***	***Consulta/Respuesta***	***Observaciones***
1	*IPServidor*	*IPau*	*¿Registro MX asociado a fic.edu.uy?*	*El servidor de correo consulta a su servidor DNS local.*
2	*IPau*	*IPRoot1*	*¿Registro MX asociado a fic.edu.uy?*	*El servidor DNS local no tiene información en el cache, por lo que debe "salir" a buscarla. Esto se debe a que es un servidor recursivo (se hace cargo de la búsqueda y responde a IPServidor solo cuando consigue la información deseada). Inicia la búsqueda en un servidor raíz del que debe disponer la IP.*
3	*IPRoot1*	*IPau*	*Registro NS asociado a .uy es ns.uy* *Registro A asociado a .uy es IP_NSUY*	*El servidor raíz no tiene la información por la que le consultan. Como los servidores raiz no realizan búsquedas recursivas, responde con la mejor información de la que dispone. Devuelve el servidor de nombres autoritativo de .uy, y agrega el glue record para informar también la dirección IP de ese servidor de nombres.*
4	*IPau*	*IP_NSUY*	*¿Registro MX asociado a fic.edu.uy?*	*Las consultas siempre son por el registro final. Se consulta al servidor de nombres autoritativo de .uy.*

#	Origen	Destino	Consulta/Respuesta	Observaciones
5	IP_NSUY	IPau	Registro NS asociado a .edu.uy es ns.edu.uy. Registro A asociado a ns.edu.uy es IP_NSEDUUY	El servidor de nombres autoritativo de .uy no tiene la información por la que le consultan. Según la letra es un TLD y no responde consultas de forma recursiva.
6	IPau	IP_NSEDUUY	¿Registro MX asociado a fic.edu.uy?	
7	IP_NSEDUUY	IPau	Registro MX asociado a fic.edu.uy es correo.fic.edu.uy Registro A asociado a correo.fic.edu.uy es IP_CORREOFIC	El servidor de nombres autoritativo de .edu.uy es también autoritativo de fic.edu.uy por lo que responde la información solicitada.
8	IPau	IPServidor	Registro MX asociado a fic.edu.uy es correo.fic.edu.uy Registro A asociado a correo.fic.edu.uy es IP_CORREOFIC	Respuesta a la consulta 1 de la tabla

c) Luego de 15 minutos de enviado exitosamente el correo de la parte b), el mismo servidor necesita enviar un correo a la dirección **redes@fing.edu.uy**. Explique detalladamente las consultas involucradas en este caso, utilizando el mismo formato de tabla que en la parte b). Justifique su respuesta.

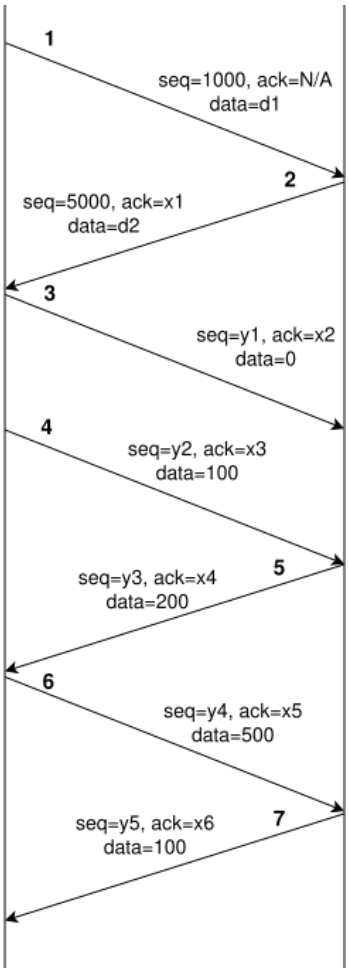
Dado que el TTL (time to live) de los registros es de 1 hora, todos los registros involucrados en la secuencia de pasos presentada en la parte b) siguen siendo válidos 15 minutos después de que hayan sido solicitados y podrán reutilizarse para resolver la nueva consulta.
En este caso el correo debe ser entregado al servidor de fing por lo que la consulta se realizará del siguiente modo:

#	Origen	Destino	Consulta/Respuesta	Observaciones
1	IPServidor	IPau	¿Registro MX asociado a fing.edu.uy?	El servidor de correo consulta a su servidor DNS local.
2	IPau	IP_NSEDUUY	¿Registro MX asociado a fing.edu.uy?	El servidor DNS local tiene en su caché que el servidor de nombres de edu.uy es ns.edu.uy y sabe su IP, por lo que hace la consulta directamente.
3	IP_NSEDUUY	IPau	Registro NS asociado a fing.edu.uy es ns.fing.edu.uy Registro A asociado a ns.fing.edu.uy es IP_NSFING	Como no es autoritativo de fing.edu.uy, le devuelve el registro NS correspondiente a fing.edu.uy y como glue-record el registro A asociado a ese nombre.
4	IPau	IP_NSFING	¿Registro MX asociado a fing.edu.uy?	
5	IP_NSFING	IPau	Registro MX asociado a fing.edu.uy es smtp.fing.edu.uy Registro A asociado a smtp.fing.edu.uy es IP_CORREOFING	El servidor de nombres autoritativo de fing.edu.uy responde la información solicitada.
6	IPau	IPServidor	Registro MX asociado a fing.edu.uy es smtp.fing.edu.uy Registro A asociado a smtp.fing.edu.uy es IP_CORREOFING	Respuesta a la consulta 1 de la tabla

Pregunta 6 (6 puntos)

a) Explique qué función cumplen los números de secuencia y reconocimiento presentes en el encabezado del protocolo TCP.

TCP garantiza un flujo de bytes confiable entre transmisor y receptor. Para garantizar eso debe tener la certeza que cada byte enviado fue recibido correctamente. Además necesita garantizar el orden de los bytes. Si no se recibe la confirmación deberá reenviar los datos hasta asegurarse que lleguen correctamente a destino. Las retransmisiones pueden generar que los datos lleguen duplicados al destino y los números de secuencia sirven también para detectar esos eventuales duplicados.
En un segmento pueden viajar varios bytes de datos, por lo que el campo número de secuencia de un segmento indica el índice del primer byte del campo de datos. Si se envian 10 bytes en un segmento con número de secuencia N, entonces los bytes enviados corresponderán con (N, N+1, N+2, … N+9).
Los números de reconocimiento indican cuál es el próximo número de secuencia esperado, lo que indicará que hasta el número anterior todo llegó correctamente. Esto quiere decir que los números de reconocimiento son acumulativos.
Cada extremo de la conexión elige un número de secuencia inicial a partir del cual numera los bytes enviados. El otro extremo usa esa secuencia en los números de reconocimiento que genera a esos envíos.



b) El diagrama de la figura adjunta representa una secuencia de intercambios que ocurren al inicio de una conexión TCP.
Para cada segmento se indica el valor de algunos campos: **seq** (número de secuencia), **ack** (número de reconocimiento), **data** (largo del campo de datos).
   i. Explique cuál es el valor de las banderas SYN y ACK para cada segmento del diagrama.
   ii. Complete el valor del largo de los campos de datos (**data**) en los segmentos 1 y 2 (**d1** y **d2** respectivamente).
   iii. Complete el valor de los campos **seq**: **y1, y2, y3, y4, y5**.
   iv. Complete el valor de los campos **ack**: **x1, x2, x3, x4, x5, x6**.
   Justifique su respuesta.

i. *Las banderas SYN estarán encendidas (SYN=1) únicamente en los primeros dos segmentos (1 y 2) ya que se usan en el establecimiento de la conexión. En el segmento 1, el transmisor expresa su intención de establecer una comunicación TCP con el receptor. Dado que el receptor acepta esa conexión responde en el segmento 2 con SYN=1.*
La bandera ACK (que indica que el campo de número de reconocimiento tiene un valor válido) estará encendida (ACK=1) en todos los segmentos de una conexión TCP, exceptuando el primero donde aún no hay nada para reconocer. Esto es así porque siempre se va a indicar qué es lo próximo que se espera recibir (aunque ya se lo hayamos dicho al otro extremo, es gratis repetirlo y nos cubrimos de algún reconocimiento anterior perdido)

ii. En el establecimiento de conexión no se envían datos por lo que d1 y d2 son 0.

iii. *El inicio de conexión TCP consume un número de secuencia (aunque no se envíen datos). Los números de secuencia posteriores se incrementarán en función de la cantidad de datos reconocidos.*

y1	*1001*
y2	*1001*
y3	*5001*
y4	*1101*
y5	*5201*

iv. *Los números de reconocimiento indican el número del próximo byte esperado.*

x1	*1001*
x2	*5001*
x3	*5001*
x4	*1101*
x5	*5201*
x6	*1601*