7 de febrero de 2007

Examen de Redes de Datos - Respuesta

Plan 97

Pregunta 1

a) Explique cómo se realiza el encaminamiento (forwarding) de paquetes en una red de datagramas (por ejemplo: IP) y en una red de circuitos virtuales (por ejemplo: ATM o Frame Relay). En particular, indique las tablas que se utilizan, la información que contienen y los algoritmos de encaminamiento (cómo se usan las tablas).

b) Explique brevemente qué función cumplen las tablas de enrutamiento en una red de circuitos virtuales.

c) ¿Cuál de las dos arquitecturas (datagramas o circuitos virtuales) le parece más adecuada para dar servicios de calidad garantizada? Justifique brevemente.

Respuesta a pregunta 1

a) Las principales diferencias entre un tipo de red y otro derivan de la forma en que se encaminan los paquetes (celdas en ATM) en una y otra red.

En una red de datagramas utilizamos la dirección de destino del paquete. Dicha dirección se busca en una tabla de ruteo (elaborada mediante algún algoritmo/protocolo de ruteo) que nos indica cuál es el próximo salto en función de la dirección que trae el paquete. La tabla de ruteo consiste entonces de grupos de direcciones (por ejemplo dir. de red/máscara) y una lista de "salidas" hacia cada grupo presente en la tabla. El algoritmo de encaminamiento usado en IP (*longest prefix match*) recorre las entradas de la tabla aplicando a la dirección destino del paquete que se desea encaminar, la máscara de cada entrada y verificando si el resultado de este and coincide o no con la "dirección de red" de esa entrada. Si no coincide se prueba con la siguiente entrada de la tabla y si coincide se usa la "salida" asociada a esa entrada para encaminar el paquete. La tabla está ordenada de las entradas más específicas (máscaras con más unos) a las menos específicas.

En una red de circuitos virtuales en cambio, el encaminamiento de los paquetes se realiza en base a información local. Cada paquete trae en su encabezado un identificador de alcance local de circuito (previamente establecido), el cual se busca en una tabla que indica por qué interfaz debe salir dicho paquete y con qué nuevo identificador, si este debe cambiar.

b) Las tablas de ruteo sirven para establecer circuitos de manera dinámica. A la hora de crear un nuevo circuito (por pedido de conexión del usuario, por ejemplo), debe elegirse la ruta de manera adecuada y en general reservar recursos sobre la misma, así como definir los identificadores de circuito a utilizar en cada enlace. En esta etapa los routers (switches) deben conocer la topología de la red y tener una tabla que indique qué camino utilizar para llegar a cada destino.

c) Las arquitecturas de circuitos virtuales son más adecuadas para brindar este tipo de servicios debido a que se tiene un mayor control sobre el camino a seguir por un flujo de datos dado, ya que una vez elegido el circuito este se mantendrá así al menos hasta finalizar el servicio. Esto permite por ejemplo reservar recursos para garantizar calidad sobre los paquetes que circulan. También permite manejar las rutas de diferentes flujos de manera de evitar congestiones. En una red de datagramas este tipo de cosas no son posibles ya que cada paquete es encaminado de manera independiente, y en general los paquetes siguen la ruta más corta, lo cual no permite el uso de rutas alternativas.

Pregunta 2

a) Explique con un ejemplo cómo se realiza una consulta recursiva y cómo una iterativa.

b) Supongamos que en la infraestructura de la figura 1, el terminal T1 realiza dos consultas DNS a través de su servidor recursivo local:

- Registro A de web.empresa.com.uy, obteniendo la correspondiente dirección IP.

- Registro A de ftp.empresa.com.uy, recibiendo una respuesta que incluye el mensaje de error con el código NXDOMAIN. Recuerde que, cuando se realizar una búsqueda de DNS por un dominio que no existe, quien realiza la búsqueda recibe un mensaje de error con el código 3 (NXDOMAIN).

En base a esta secuencia de eventos:

i. ¿Qué conclusiones podemos inferir sobre web.empresa.com.uy y ftp.empresa.com.uy? Justifique.

ii. ¿Qué servidor generó el mensaje de error con el código de error NXDOMAIN? Justifique.

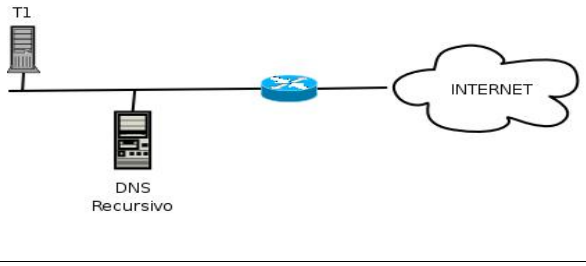


Figura 1

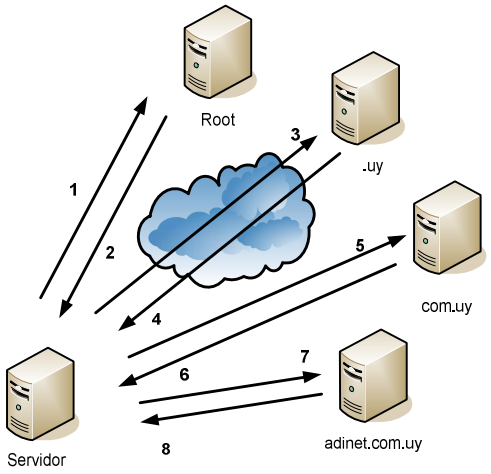
Respuesta a pregunta 2

a)

- **Consulta Iterativa.**

Una consulta iterativa se caracteriza por el hecho de que para poder obtener el resultado final, se necesita realizar varias consultas intermedias. En el peor de los casos es cuando hay que recorrer todo el árbol hasta llegar al servidor de nombres autoritativos del dominio deseado.

Ejemplo: www.adinet.com.uy



1. El servidor pregunta por el registro A de www.adinet.com.uy.
2. Como los root servers no aceptan consultas recursivas. El root server responde con el NS del .uy. (además hay que obtener la dirección IP del servidor)
3. Con la dirección IP del servidor de nombres autoritativo del ".uy", vuelvo a preguntar por el registro A de www.adinet.com.uy.
4. El servidor de nombres autoritativo del ".uy", responde con el NS del "com.uy" (además hay que obtener la direccion IP del servidor)
5. Con la dirección IP del "com.uy", vuelvo a preguntar por el registro A de www.adinet.com.uy.
6. El servidor de nombres autoritativo del "com.uy", responde con el NS del "adinet.com.uy" (además hay que obtener la dirección IP del servidor)
7. Con la dirección IP del servidor de nombres autoritativos del "adinet.com.uy", vuelvo a preguntar por el registro A de www.adinet.com.uy

8. Como esta dentro de la zona de autoridad el servidor tiene que tener la respuesta. La respuesta es la dirección IP buscada.

Observaciones:

- ¿Porque pregunto siempre por www.adinet.com.uy?

Que pasa si el mismo servidor que es autoritativo del “com.uy”, también lo es del dominio “adinet.com.uy”. Realizo una consulta menos.

- Un servidor se dice que no acepta consultas recursivas (o no es recursivo) si para responder la consulta que le realizaron, el no tiene que salir a realizar consultas.

En general se responde con la mejor respuesta posible, como ejemplo veamos que cuando preguntamos al “.uy” responde cual es el servidor de nombres autoritativos del “com.uy”, me acerca al destino deseado. Podría ser que pregunte al autoritativo del “.uy” sobre empresa.com, como no esta en su zona de autoridad nos responde o bien con la lista de autoritativos del “com” o bien con la lista de los root servers.

- La respuesta a una consulta iterativa es normalmente o el resultado final o el registro NS (nombre de una maquina) del siguiente domino a preguntar.

Surge un problema al momento de obtener la dirección IP de ese servidor. Pueden ocurrir dos casos. El primero es que el servidor de nombre este bajo mi dominio, ejemplo cuando le preguntamos al “com.uy” quien es el autoritativo de “adinet.com.uy” y responde “ns1.anteldata.com.uy”. ¿Como obtengo esta dirección IP para poder hacer la consulta via protocolo UDP y puerto destino 53? Normalmente en esto casos además del registro NS se devuelve los registros A asociados a los registros NS, esto se hace para que se pueda continuar la búsqueda. El segundo caso es que el servidor de nombres autoritativo del dominio este bajo otra zona de autoridad, por ejemplo si me responden que el NS de “com.uy” es otro.net. Para poder continuar con la consulta debo obtener el registro A de “otro.net”, esto me implica tener que salir a realizar otras consultas. No es posible que me entreguen la dirección IP de ese servidor de nombres ya que viola la estructura del DNS.

- **Consulta recursiva.**

Una consulta recursiva es aquella consulta en la cual el servidor de nombre sale a consultar y obtener el resultado por nosotros. Debemos aclara la diferencia entre consulta recursiva y un servidor que acepte consultas recursivas.

Un servidor acepta consultas recursivas, si en el caso de que hagamos la consulta recursiva, sale a obtener los resultados intermedios y nos responde el resultado final directamente.

Ejemplo www.adinet.com.uy , responde con 200.40.30.218.

Un servidor recursivo, al cual no le realizan la consulta de forma recursiva responde lo mejor que pueda basándose en la información de su cache o desde sus archivos de zona. La respuesta dependerá de lo que ya este en su cache.

Ejemplo a www.adinet.com.uy, puede responder con: los root servers, los NS e IP del “.uy”, los NS e IP del “com.uy”, los NS e IP del “adinet.com.uy” o el A de www.adinet.com.uy. Dependerá de que es lo que se encuentre en el cache. La diferencia se encuentra en que el valor de TTL que se retorna es diferente.

Un servidor que no es recursivo, solo responde sobre los registros sobre los cuales es autoritativo, independientemente de cómo se realice la consulta.

Observaciones:

- Formalmente la recursividad de una consulta esta dada por un flag en el encabezado de DNS en la capa de aplicación. Un servidor utiliza otra flag para avisarle al originador de la consulta si acepta o no consultas recursivas.

- Un servidor autoritativo utiliza un flan del encabezado de DNS para avisar que el es autoritativo del registro. Las respuestas que se contestan desde un cache de DNS (normalmente cuando le consulto a un servidor que acepta consultas recursivas), no tienen prendido este flag. Si bien obtengo una respuesta se que no es el origen mas confiable.

b)

i. Dado que T1 realiza la consulta por web.empresa.com.uy y recibe la respuesta del registro A, podemos concluir que existe el dominio empresa.com.uy y también existe un servidor autoritativo para dicha zona, la cual es delegada desde la zona ".com.uy". Además se concluye que el registro ftp.empresa.com.uy no existe, es decir no fue generado en el dominio empresa.com.uy.

ii. Quien responde con el código NXDOMAIN es el servidor autoritativo de la zona empresa.com.uy.

Pregunta 3

Una empresa *E1* necesita conectar su red privada con la red de otra empresa *E2*. Para realizar dicha conexión deciden implementar lo que se conoce como red privada virtual (VPN).

Una VPN es una red IP privada y segura transportada sobre la red de un proveedor. Dicha red contratada garantiza confidencialidad, autenticidad e integridad y desde el punto de vista de los enrutadores (*RE1* y *RE2*) se ve como un enlace punto a punto con las direcciones marcadas en la figura 2.

a) Al implementar la VPN el administrador de la red de E1 nota que ambas redes, la de E1 y la de E2, utilizan el rango de direcciones IP privadas 192.168.1.0/24 y ninguna de las empresas esta dispuesta a realizar una renumeración. ¿Qué problema presenta la interconexión de las dos redes? Proponga una posible solución al problema.

b) Muestre como funciona la solución que propuso en la parte b) cuando se realiza una consulta desde m1 (192.168.1.1) a la base de datos BD (192.168.1.2).

Figura 2

Respuesta a pregunta 3

a) El problema que presenta es que ambas subredes utilizan el mismo espacio de direcciones, con lo que no sería posible distinguir paquetes dirigidos a una y otra subred.

b) Se propone como solución implementar NAT puro en ambos routers; RE1 y RE2. Consiste en que en cada router REi se traduzcan las direcciones de la LAN Ei en otras direcciones que no generen conflicto con la subred de la otra empresa. La comunicación dentro de cada LAN continuará siendo igual (se utiliza el rango de direcciones IP original) con lo que no sería necesaria ningún tipo de configuración en las PCs de cada LAN. Cuando una PC se intente comunicar con otra de la otra LAN el router/nat se encargará de cambiar la dirección de origen por otra dirección única en la VPN. Así mismo cuando llegue información desde fuera de la LAN a algún terminal de la LAN el router/nat realizará el cambio inverso.

Por ejemplo, un posible mapeo podría ser que en RE1 se traduzca cada dirección 192.168.1.x/24 (Dirección de la LAN E1) en 10.0.1.x/24. y en RE2 cada dirección 192.168.1.z/24 (dirección de la LAN E2) se traduzca en 10.0.2.z/24.

Con esta solución las PCs de la red E1 accederían a las de E2, mediante direcciones 10.0.2.z/24 (y viceversa), y serían los routers quien se encargaría de realizar los cambios correspondientes para que esta configuración sea transparente a ambas redes y posibilitar la comunicación.

b) A continuación se describen todos los eventos en el orden que ocurren:

1. m1 (192.168.1.1) envía su consulta a BD (m1 conoce a BD con la dirección 10.0.2.2). Para ello, los paquetes a enviar tendrán como dirección de origen 192.168.1.1 y como dirección de destino 10.0.2.2.
2. Cuando la consulta llega a RE1, éste cambia la dirección IP de origen, 192.168.1.1 por 10.0.1.1 y reenvía los paquetes correspondientes a la consulta a RE2. RE1 conserva en una tabla la asociación 192.168.1.1< ->10.0.1.1.

3. Cuando los paquetes llegan a RE2 éste mira su tabla de NAT y realiza el cambio en la dirección de destino (10.0.2.2 por 192.168.2.2) y lo reenvía a la LAN de E2.
4. La consulta llega a BD correctamente. Para BD enviar la respuesta a m1, envía los paquetes con su dirección origen (192.168.1.2) y de destino la que conoce de m1 (10.0.1.1).
5. Cuando los paquetes llegan a RE2, éste realiza el NAT sustituyendo la dirección de origen 192.168.1.2 por 10.0.2.2 y guarda esta asociación en una tabla. Los paquetes son entonces reenviados a RE1.
6. Al llegar a RE1 éste observa la dirección de destino de cada paquete y en función de su tabla de NAT realiza la traducción cambiando 10.0.1.1 por la verdadera dirección de m1, 192.168.1.1. RE1 reenvía los paquetes a la LAN E1.
7. Los paquetes que componen la respuesta de BD llegan a m1 correctamente completándose la comunicación.

Pregunta 4

a) Explicar la utilidad del modelo de capas.

b) ¿Por qué algunas capas repiten funciones ya instrumentadas en capas inferiores?

c) ¿Qué parte del paquete se utiliza para calcular la suma de verificación en IP? ¿por qué se hace así y qué asegura esto?

d) ¿Qué parte del segmento se utiliza para calcular la suma de verificación en TCP? ¿qué asegura esto?

Respuesta a pregunta 4

a) El modelo en capas permite simplificar el diseño y la implementación de las redes de datos. Dicha simplificación se logra mediante la división en distintos niveles de abstracción y la independencia entre dichos niveles. Cada capa o nivel, realiza un conjunto de funciones que ofrecen servicios a la capa superior. La implementación de cada una de esas funciones es transparente para las otras capas por lo que mediante una correcta definición de las interfaces entre las capas se logra una verdadera independencia. Dicho modelo permite diseñar e implementar considerando que la comunicación se da entre cada capa correspondiente a cada entidad de red, aunque el flujo real de datos se da en sentido vertical y no horizontal.

Por más información Ver. Tanembaum, Redes de Computadoras, 4ta Edición Capitulo 1 Sección 1.3.

b) Hay funciones que competen a todas las capas, ejemplos de esto son el control de errores, control de flujo, direccionamiento, seguridad. Cada capa realizará lo que está dentro del alcance de ese nivel, contribuyendo a la función general. Por ejemplo, el control de flujo se realiza en distintas capas para poder controlar punto a punto (capa de enlace de datos) y extremo a extremo (capa de transporte). Algo similar ocurre con el control de errores, debe estar presente en las distintas capas porque cada capa realiza un control sobre lo que le compete a esa capa y no a las otras.

c) Se calcula sobre el encabezado IP. El encabezado IP contiene información sobre las direcciones IP de origen y destino, por lo que realizar control de error sobre éste asegura que se pueda encaminar correctamente dicho paquete. No realiza control de errores sobre la carga útil del paquete porque garantizar la integridad de los datos no es función de esta capa.

d) La suma de verificación se realiza sobre el encabezado de la TPDU, los datos y el pseudo encabezado. Esto permite agregar confiabilidad al servicio de transporte, permitiendo que en recepción se pueda verificar si se introdujeron errores en la transmisión de los datos.