

Redes – Control 3

José M. Piquer - 2 hrs - Pauta

15 de diciembre de 2013

Pregunta 1 (TCP)

Parte I

Considere el algoritmo de Sliding Window con Go-Back-N. Si existe desorden de paquetes en la red, ¿puede fallar el protocolo?

El protocolo resiste desorden en la red ya que numera los paquetes, y puede re-ordenarlos en la recepción. Sin embargo, al re-utilizar los números de secuencia, siempre es posible que se inyecte un paquete duplicado y antiguo erróneamente si el delay es tan grande que consumimos todos los números de secuencia y dimos la vuelta mientras llegaba. Esto nos lleva a limitar los delays a una cota superior y a agrandar lo más posible el tiempo que toma dar vuelta el número de secuencia.

Parte II

Explique por qué es bueno que en TCP se utilice el número de bytes transmitidos en los números de secuencia, en vez de números de paquetes.

La gran ventaja es que permite modificar los tamaños de los paquetes mientras están en la ventana de envío. Esto se usa para MTU path discovery por ejemplo.

Parte III

Explique por qué durante la fase de conexión de TCP es más probable que haya fallas que después, una vez que ya estamos conectados y transmitiendo datos.

Durante la fase de conexión no tenemos suficiente información aun de los parámetros de esta conexión: tamaño de la ventana, RTT, etc. Por lo tanto debemos usar timeouts fijos y número de retransmisiones pre-definidos. Eso hace que somos mucho más frágiles a fallas y tengamos que abortar una conexión que, una vez establecida, podría funcionar impecable.

Pregunta 2 (Ruteo)

Parte I

Ud es el ingeniero a cargo de diseñar la red futura del campus Beauchef, que incluye 12 departamentos, muchas salas de clases, salas de eventos, etc. Digamos que se piensa tener unos 5.000 puntos de red. Hay dos viejos ingenieros del CEC, uno recomienda usar RIP para el ruteo, el otro recomienda usar OSPF.

Explique qué decisión tomaría Ud y por qué.

RIP, en sus versiones más modernas, es un buen protocolo de ruteo a pequeña escala y tiene la gracia que es autoconfigurable y no requiere mucha coordinación ni administración central. OSPF es más óptimo, pero requiere una configuración bien diseñada, administrada, en una red más o menos estable, pero de mayor tamaño. Yo propondría más bien RIP en la facultad, por su des-centralización en la administración (departamentos), tamaño aun manejable, es una red de campus donde todos los enlaces son muy parecidos, locales y sin una topología compleja. También podría defenderse OSPF al configurar una troncal de campus (área 0) y suponer que todo router que conecta a la central queda en manos del CEC y cada área asignada a un departamento la administra un personaje local, y así encontramos rutas óptimas en cada red.

Parte II

Explique por qué no se usa OSPF o RIP para el ruteo en el Internet global. ¿Qué tiene BGP-4 que ellos no tienen?

Escalabilidad: la factorización del problema al usar Sistemas Autónomos para rutear en vez de prefijos de red es la clave que me permite rutear a escala global. Resultaría imposible intercambiar tablas caminos de prefijos a nivel central de la red, cuando andan cerca de ser medio millón.

Parte III

En una corporación ultra-segura, se descubre que un usuario ha estado entrando a su cuenta desde fuera de la red. El administrador de sistemas dice que eso es imposible, ya que él solo deja entrar los puertos 25 y 80 (mail y web) en el firewall de acceso.

¿Qué puede estar pasando?

Aunque esté todo perfecto en la configuración del firewall, no podemos garantizar que los puertos 25 y 80 sean solo mail. Basta instalar un servidor de login escuchando en uno de esos puertos en cualquier computador accesible desde Internet y tenemos acceso remoto.

Pregunta 3 (DNS)

Parte I

Explique por qué Anycast ayuda a que el DNS funcione mejor.

Me permite instalar muchos servidores de nombres, en diversas partes del mundo, usando la misma dirección IP. Si BGP-4 hace bien su trabajo de llevarme por las rutas más cercanas, siempre encontraré la copia más cercana, dando tiempos de respuesta mejores, mayor tolerancia a fallas y un buen soporte a ataques de denegación de servicio distribuidos, ya que reparte el tráfico entre los servidores y no permite que se agrupe en uno solo.

Parte II

En el DNS existe un conflicto de autoridad: en el servidor de .CL, por ejemplo, se requiere listar los servidores de nombres de uchile.cl, para delegar ese dominio a esos servidores de nombres, y esa lista es la que se le envía a todos los que buscan nombres en ese dominio. Pero, en uchile.cl también se listan los servidores de nombres oficiales de uchile.cl, puesto que ellos son los encargados de esa zona, y saben quienes son los servidores primario y secundarios.

A veces existen inconsistencias entre ambas listas, al modificarse por separado. Si Ud tiene que escribir un servidor de nombres, a quién le creería más, ¿a .cl o a uchile.cl ?

¿Qué pasa si las listas son totalmente incompatibles y ningún servidor de nombres figura en ambos al mismo tiempo?

El que tiene información más al día y creíble es uchile.cl, hay que creerle siempre a él. El problema es que el primero que me dice quien es el creíble, es justamente .CL. Si en algún momento las listas divergen por completo, no lograré resolver nombres en uchile.cl, siendo un desastre mayor.

Parte III

Explique por qué el campo Expire del SOA se recomienda ponerlo muy alto (tipo un mes).

Ese campo indica cuanto tiempo debe recordar un secundario la zona que obtuvo de su primario, cuando logra contactarlo nunca más. Es importante que sea mucho tiempo, así puedo corregir la conectividad o volver a subir un primario sin perder el dominio.