

## Control 3

### Redes (Pauta)

Plazo de entrega: 22 de noviembre 2022

José M. Piquer

#### P1: TCP AVANZADO

##### 1.1 RTT y retransmisiones físicas

En algunos enlaces físicos (típicamente redes 3G o 4G) la tarjeta de red retransmite y reintenta los envíos muchas veces, generando enlaces con RTTs muy variables (es común que los paquetes demoren entre 300ms y 3000ms cuando la señal no es muy buena). Ni IP ni TCP se enteran de estas retransmisiones, para esos niveles, sólo se percibe como un delay muy cambiante de un paquete a otro.

- a. Explique cómo puede esto afectar el rendimiento de TCP y proponga ideas para mejorarlo en estos casos. *El problema es el cálculo de timeout: al tener tanta varianza, el timeout de TCP tenderá a ser demasiado grande, y las verdaderas pérdidas se retransmitirán muy tarde, generando demoras innecesarias. Si uno piensa que el RTT puede ser hasta 10 veces más grande que el real, ¡puedo demorar una retransmisión 10 veces más de lo necesario! Una posible mejora sería limitar la varianza medida, por ejemplo descartando mediciones absurdas y fuera de rango, o definir una varianza máxima para que no crezca demasiado. De esa forma, el timeout nunca será tan absurdamente grande.*
- b. Analice la alternativa que la tarjeta elimine este comportamiento y no trate de corregir, generando simplemente una pérdida. *¿Sería esto mejor o peor? En general, es mala idea que dos capas de red intenten arreglar el mismo problema. Si IP decidió no arreglar la pérdida y dejarla a transporte, es mala idea que la capa física corrija incluso antes que IP. Pero, en este caso es dudoso: la capa física no está corrigiendo realmente, está retransmitiendo errores de señal y, como vimos en TCP en ventana de congestión, es bueno esconderle a la capa transporte los errores físicos, para que no los confunda con errores por congestión. Seguramente en algunos casos TCP funcionaría mejor si la capa física no retransmitiera, por que tendría el timeout mejor calculado, pero en otros funcionaría peor, por que creería que esos errores son por congestión y achicaría demasiado la ventana de transmisión.*

## 1.2 Números de secuencia

En TCP el número de secuencia cuenta 'bytes' transmitidos. En la Tarea, contamos paquetes enviados. Discuta los pro y contra de ambos esquemas y averigüe por qué en TCP es importante que cuente bytes y no paquetes.

*En general, es mejor contar paquetes, por que así los números de secuencia 'duran' más, y los reciclo menos seguido. Pero, en TCP es importante contar bytes, eso nos permite cambiar el tamaño máximo de segmento (MSS) en la mitad de una conexión (por ejemplo con MTU Path Discovery eso puede suceder) y retransmitir datos que están en la ventana de transmisión segmentados en paquetes de distinto tamaño. Si numero paquetes, esto es imposible, y no puedo cambiar el tamaño de paquetes ya enviados.*

## P2: REDES IP

### 2.1 CIDR

Cuando se inventó CIDR para IPv4, ningún router de Internet lo soportaba. Todo Internet funcionaba con las clases antiguas. De a poco, se fueron actualizando los routers y kernels para soportar CIDR. Pero la transición fue larga. Durante ese período, convivieron routers que entendían CIDR y otros que no. Explique cómo funcionaba esto (o si no era posible) en un router que entiende CIDR y en uno que no, en el caso de estos dos ejemplos:

- a. Agrupar 8 clases C consecutivas en un prefijo común de 21 bits (/21). La idea es manejar ese conjunto de prefijos como si fuera uno solo. *En este caso, basta con que los routers que no saben de CIDR manejen esos 8 prefijos en su tabla de rutas, apuntando todos al mismo router de entrada. Lo malo es que un prefijo CIDR se transforma en 8 prefijos distintos, o sea hace crecer las tablas de rutas, pero funciona. Otro problema es que ese router va a difundir su tabla con esos 8 prefijos separados, y aunque el router receptor de la información entienda CIDR, ya no va a poder juntarlos y seguirá difundiéndolos como 8 prefijos distintos.*
- b. Dividir una clase A en 255 redes consecutivas, con prefijos de 16 bits (/16) (equivalente a 255 'clases B'). La idea es que cada una de estas 255 redes sea independiente y pueda asignarse a cualquier organización y/o lugar del mundo. *Si enviamos información de ruta a un router no CIDR, él entenderá que esta clase A es una sola red. Por lo tanto, no puedo dividir ese prefijo en redes distintas mientras hayan routers que no entiendan CIDR. Este mecanismo se comenzó a utilizar muchos años después, para evitar este problema. Una posible solución habría sido colocar un router único a cargo de ese prefijo clase A, que conociera los destinos a todas esas sub-redes,*

*de modo que él recibiera este tráfico y los distribuyera. Pero, habría que asegurar que el camino desde él a todas esas sub-redes fueran sólo routers CIDR. Esto nunca se hizo así, y se esperó a que no hubiese más routers antiguos en los proveedores de Internet.*

## 2.2 IPv6

Suponga que Ud quiere experimentar con IPv6 en su casa, y quiere armar una red IPv6 pura, pero con conexión a Internet, para poder acceder todos los servicios existentes. Entonces, uno quiere que dentro de la casa se hable IPv6, pero podamos salir al Internet que todavía es IPv4 (y suponga que su proveedor de Internet no le puede proveer IPv6 aún).

Busque soluciones posibles y recomiende una, argumentando sus razones para escogerla.

*Hay varias respuestas posibles, yo usaría un tunel IPv6 (Hurricane provee el servicio) que es como una VPN, pero asociada a IPv6. De esa forma, puedo tener toda la red de mi casa con IPv6 y con una salida a Internet por ese tunel, que habría que configurar en el router de salida de la casa.*

## 2.3 Traducción de Direcciones

Hemos visto que usamos ARP o ICMPv6 para traducir direcciones IP a direcciones físicas (MAC Address), una vez que el paquete llega a la red de destino final. ¿Qué pasa en las redes intermedias, entre los routers de Internet por ejemplo? ¿Necesitamos ARP? Si miramos el tráfico de las redes de los proveedores, ¿veremos paquetes ARP o ICMPv6? Explique.

*ARP o ICMPv6 existe en todas las redes que componen el Internet. Siempre necesito traducir direcciones IP a físicas para poder enviar un paquete físico. En la red de un proveedor, por ejemplo, un router tiene un paquete IP que enviar a un destino lejano. En su tabla de rutas encuentra la dirección IP del router siguiente al que se lo debe entregar. Esa dirección IP debe ser traducida la dirección física de la red con la que me conecto con ese router. Por lo tanto, si es una red ethernet, haré ARP (en IPv4) o ICMPv6 (en IPv6) de esa IP para pedir su dirección física. Por lo tanto siempre veremos paquetes de este tipo circulando por todas las redes físicas de Internet.*

## P3: RUTEO

### 3.1 Redes Privadas

Hemos visto que las redes privadas nos han permitido alargar mucho la vida de IPv4, ya que la mayoría de las redes nuevas no requieren más que una IP pública y todo el resto lo manejamos con

redes privadas. Sin embargo, muchos equipos que se conectan a la red privada en nuestras casas (sensores, electrodomésticos, etc), permiten acceso y control desde fuera de mi casa. Por ejemplo, puedo encender mi lavadora o mi aspiradora robot desde cualquier parte de Internet.

- a. Averigüe cómo lo resuelven estos dispositivos y discuta los peligros y funcionalidad que conlleva. *hay dos soluciones más populares: abrir un puerto en el router vía UPnP (que es equivalente a configurar a mano en el router una entrada a mi equipo interno) o usar un sitio en la nube con el que ambos dispositivos conversan (por ejemplo mi app del celular se conecta a una nube pública preguntando por mi aspiradora y mi aspiradora está conectada a ese sitio también). Abrir un puerto siempre es un peligro de seguridad, ya que pueden entrar directo desde Internet a mi dispositivo y abusar algún error de seguridad de él y ahí están dentro de mi casa. Usar la nube es más seguro, pero generalmente hace que si no tengo conexión a Internet mi dispositivo no funciona, incluso dentro de mi casa.*
- b. Averigüe si existe una forma de impedir esto, por ejemplo, que nunca nadie pueda encender mi aspiradora desde fuera de mi casa (pero sí funcione dentro de mi casa). *en el caso de UPnP es fácil: basta configurar mi router para que no acepte ese protocolo. En el caso de la nube es más difícil, debo descubrir la IP del dispositivo, bloquearle a él la salida a Internet y, incluso si eso funciona, es posible que el dispositivo deje de funcionar sin acceso a la nube.*

### 3.2 BGP-4

El 28 de febrero de 2008, Pakistán mató YouTube en el mundo, cuando quería matarlo sólo dentro del país (para detener una ola de protestas internas). Averigüe cómo ocurrió esto y explique por qué BGP-4 no detuvo este desastre a tiempo. Proponga ideas de mejoras que harían más seguro el protocolo. ¿Podría volver a pasar hoy en día?

*El problema de fondo es que BGP-4 no tiene mucha seguridad asociada y los routers tienden a aceptar toda la información que reciben del resto sin validarla mucho. En el caso de Pakistan, el gobierno quería bloquear el acceso a YouTube y comenzó a difundir rutas falsas a los prefijo de red de YouTube para que las redes del país no pudieran salir. Sin embargo, probablemente por error, esas rutas se difundieron a sus proveedores de Internet globales, quienes las aceptaron y propagaron también. En un minuto, casi nadie cercano a Pakistan tenía acceso a YouTube y la red de Pakistan estaba colapsada de paquetes que le llegaban de todas partes. La idea hoy en día es validar qué prefijos de red tienen derecho a difundir qué routers, y que esas entradas vengan firmadas, de modo que no puedan falsificarse. Sin embargo, esta infraestructura es débil aun y probablemente un problema así pueda ocurrir de nuevo.*