2008

¡Todos los Datagramas Son Iguales Ante la Red!

Carlos A. Afonso

Neutralidad y Desagregación de Redes: el Ejemplo de Inglaterra

Gustavo Gindre

rits
nupef rits
IDRC CRDI

¡Todos los Datagramas son Iguales Ante la Red!

Carlos A. Afonso*

Todas las informaciones que circulan por Internet están separadas en paquetes de datos (los datagramas o "packets") que se envían a destino a través de uno o más caminos, donde se recomponen para formar el conjunto original de datos: un mensaje, una imagen, un documento o incluso un flujo de video o voz.

Actualmente un "packet sniffer" es capaz de recomponer integralmente mensajes de correo electrónico, flujos de sonido o imagen digital, datos de navegación web, contenidos en un gigabyte de datos copiados de Internet en un único segundo, lo que significa que el "sniffer" puede recomponer y grabar millares de mensajes de correo electrónico o incluso una inmensa cantidad de datos que trafican las personas que navegan en sitios web, en un único segundo. Puede asimismo reconstituir y grabar millares de conversaciones simultáneas de telefonía vía Internet (conocida como "voz sobre IP" o voIP). Los datagramas se analizan y copian eventualmente en un banco de datos y continúan o no su camino y pueden, por ejemplo, continuar en un flujo mucho más lento. Todo ello es programable a través de sniffers de datagramas y gerenciadores de tráfico (los "traffic shapers"). A menos que los datos no lleguen, ni el destinatario ni tampoco el remitente sabrán de nada. Si fuese telefonía vía Internet, el usuario podría atribuir el efecto de voz entrecortada a un eventual tráfico intenso en algún punto de la red. En resumen, resulta difícil que un usuario no especialista o alguien que no sea particularmente terco logre detectar dichas iniciativas.

Un gigabyte de datos por segundo redunda en una capacidad de transmisión de 10 Gb/s (10 gigabits por segundo o mil millón de caracteres por segundo), flujo mayor que la capacidad sumada de todas las espinas dorsales (principales infovías o "backbones") de Internet en la mayoría de los países. Un sniffer moderno es básicamente un programa o software incorporado a una microcomputadora de alta capacidad pero no muy diferente a las computadoras domésticas de primera línea que la muchachada más acaudalada usa para sus jueguitos. Utilizando la eficacia de sistemas operacionales similares al UNIX, el sniffer trabaja en una computadora conectada a un punto estratégico de Internet, por ejemplo, un punto de intercambio de tráfico (PTT) entre varias infovías.

Sniffers con estas características son vendidos, por ejemplo, por la empresa Narus [1]. Una típica licencia de uso cuesta alrededor de 50 mil dólares norteamericanos, una suma minúscula para la NSA (Agencia Nacional de Seguridad de los Estados Unidos de América) y para cualquier operadora de supercarreteras de Internet. Este packet sniffer pasó a ser conocido pues la Electronic Frontier Foundation (EFF) [2], a raíz de la denuncia detallada de un empleado de la AT&T,

* *Carlos A. Afonso* es uno de los representantes de las organizaciones no gubernamentales sin ánimo de lucro ante el Comité Gestor de Internet en Brasil (CGI.br) y se desempeña como director de planificación de la Red de Informaciones para el Tercer Sector (Rits).

entabla un juicio contra la empresa sobre una violación obvia de privacidad. La AT&T alega que tomó esta medida a solicitud del gobierno de los Estados Unidos (EEUU), pero que nunca informó a sus millones de usuarios. Según la EFF y el empleado de la empresa, la AT&T usa la tecnología de Narus para poner en práctica la violación de privacidad en masa.

En Brasil, en 2004, la BR Telecom bloqueó el tráfico de datagramas correspondientes a llamadas telefónicas vía Internet provenientes de otras empresas de servicios de este tipo, como por ejemplo Skype y GVT [3]. El bloqueo fue suspendido, posterior a una denuncia hecha por usuarios, en el caso de Skype y por determinación de la Anatel, en el caso de GVT; al final, bloquear cualquier datagrama es censurar contenido, asunto que, además de violar el derecho a la libertad de información y a la privacidad de los datos, extrapola la jurisdicción de la concesionaria de telecomunicaciones. Sería como si la concesionaria de una carretera prohibiese el tránsito de vehículos de color rojo o algo semejante. Por supuesto que los abogados de la BR Telecom estaban al tanto de eso pero una concesionaria que es un virtual monopolio de un servicio en su región (una especie de "capitanía" heredada de la privatización de las telecomunicaciones) puede darse el lujo de probar hipótesis en la práctica, un tubo de ensayo para tantear el terreno. Por coincidencia o no, la BR Telecom es una de las clientes de la empresa Narus, como informaba hasta hace poco el propio sitio web de la empresa [4]. De cualquier modo, los softwares de administración de datagramas son usados de manera rutinaria por las operadoras de espinas dorsales para cobrar "peaje" debido a la transmisión de ciertos tipos de tráfico en sus circuitos.

La práctica de manipulación de datagramas no se restrinje tan solo a la telefonía voIP. Las operadoras tienen la potestad de identificar tráfico de copia de archivos entre dos computadoras en Internet (la base de los sistemas de red "peer-to-peer" o P2P, como el Bit Torrent, por ejemplo) pudiendo disminuir el flujo de estos datagramas o sencillamente descartarlos. Por principio, la mayoría de los servicios en Internet está definida por un código simple, que viene en el encabezado de cada datagrama, el cual define el tipo de servicio (copia de archivos, voz sobre IP, transferencia de datos, acceso web, envío o recepción de correos electrónicos, etc). Los organismos que coordinan la infraestructura lógica de Internet [5] definen estos códigos (o "puertas de servicio") pero nada evita que otras puertas se definan de común acuerdo entre dos usuarios para realizar algún tipo de transferencia de datos entre ellos. Sin embargo, como en general dichas puertas se utilizan en todas las aplicaciones de Internet por patrón (sino ¿para qué definirlas?), esto hace que la tarea de identificar y eventualmente bloquear o "perjudicar" el tráfico de datagramas sea más fácil.

Otro ejemplo más: la Telemar (actualmente llamada Oi) recientemente decidió bloquear algunos tipos de servicios en su acceso de banda ancha conocido como Velox, aduciendo que estaba censurando contenido por razones de seguridad, para "proteger a los usuarios" [6]. Se repite este caso con una operadora de infovía que decide, ilegalmente, bloquear contenido. Las computadoras de usuarios conectadas a la red Velox que pueden estar funcionando con características de servidor sufren de reiteradas bajas de la capa de conexión de banda ancha, que es simplemente reiniciada para cambiar el número IP designado por la operadora.

Estas iniciativas de intervención en la capa de contenido por parte de las operadoras, además de ilegales, dificultan el uso de las computadoras de los usuarios con respecto a una serie de servicios, entre los cuales se encuentran la administración remota de servidores, la prueba de los servicios antes de activarlos en un servidor real, además de que suele estar dirigida a perjudicar la comunicación bilateral que implica tráfico significativo en ambos sentidos. Es como si las operadoras de banda ancha nos dijesen: use su computadora como un receptor de TV ¡no como un comunicador! Pero si usted quiere de hecho usarla como un comunicador, entonces vamos a escoger aquello que tiene permiso para comunicar y lo que no y con qué eficacia. ¿La ley? Bueno, la ley...

En algunos casos sale a relucir la motivación real: reducir al máximo posible la eficacia de los servicios de terceros que puedan competir con los servicios que la operadora ofrezca. El caso más evidente es el de la telefonía voIP aunque, a medida que nos acercamos a la consolidación de la llamada "Web 2.0" (involucrando mucha más interacción entre usuarios y servicios de comunicación e información, así como un creciente comercio de multimedios bajo demanda, como TV sobre IP y otros), seguida de la concentración de los servicios de Internet en manos de las operadoras de infraestructura, podemos considerar que estamos viendo apenas los primeros atisbos de intentos mucho más agresivos de calificar (o descalificar) la conexión de los usuarios a Internet como un todo.

Una operadora de banda ancha puede (como ya lo está haciendo) instalar grandes bases de servidores web con conectividad prácticamente directa para los usuarios de esta operadora y, a partir de estos servidores, ofrecer repositorios pagos de música y video, así como de otros servicios de Internet más tradicionales de modo que, cada vez más, los usuarios se verán inducidos a permanecer acotados a este tráfico, a buscar cada vez menos en el resto de Internet y a que, cuando se acometan a hacerlo, tener una calidad de tráfico deliberadamente peor. Por ejemplo, usted lograría descargar un CD entero del servidor de la operadora en 20 minutos pero llevaría de uno a dos días bajando un CD de un sitio de Internet fuera del ámbito de la operadora, aunque la banda pasante real a este sitio "externo" sea de excelente calidad y esté descongestionada. Es lo que se ha acordado en denominar "Internet en capas" ("tiered Internet"). Esta situación es tan seria que llevó a que el Congreso Norteamericano aprobase la promulgación de una ley en 2006 que garantiza la neutralidad de la red contra tratamiento discriminatorio de tráfico [7].

Internet, como una infovía mundial, fue ideada como un espacio neutro y democrático – toda la concepción de Internet tiene como premisa la ausencia de cualquier control centralizado sobre su contenido – pese a que en países enteros esto se vea sencillamente atropellado por los respectivos gobiernos. Los operadores de la infovía (en general, empresas de telecomunicaciones y de redes de TV por cable) al ofrecer canales para Internet, implícitamente se pliegan a este compromiso que, por otro lado, está sacramentado bajo la forma de ley en muchos países.

La neutralidad de Internet, como ya lo advertía Lawrence Lessig hace cinco años, significa que los proveedores de acceso y de infovías no puedan controlar la manera como los usuarios utilizan la red. No pueden censurar datagramas ni discriminar tipos de servicios por sus respectivos contenidos (sea del encabezado o de cualquier otra parte de un datagrama).

No le incumbe al operador de la infovía, cualquiera que fuere, decidir si los carros rojos tienen menos prioridad que los de color azul, ni si los datagramas de telefonía IP tienen menos prioridad que los datagramas de video originados en determinado servidor. No deberían (aunque suelen hacerlo) ni siquiera crear dificultades para que un pequeño empresario o usuario doméstico conecte más de una computadora a un mismo circuito de banda ancha.

Fue justamente esta concepción democrática e igualitaria, al igual que su práctica generalizada al paso que la red crecía mundialmente, las que permitieron la increíble expansión de Internet, así como la innovación acelerada del uso de la misma a lo largo de pocos años.

En el debate internacional sobre la neutralidad de la red suelen verse opiniones que tratan de enfatizar el hecho de que gran parte de los problemas interpretados como violación de la neutralidad son en realidad problemas de tinte técnico que ocurren básicamente en el ruteo de los datagramas. De hecho, hay una fragmentación de los datagramas mayores, dificultades ocasionales con las tablillas de ruteo, degradación debido a ataques, etc. Sin embargo, estos problemas no se manifiestan de forma regular ni sistemática, si no las empresas de medios no estarían migrando en masa sus servicios a Internet. Aquí nos referimos a los efectos sobre el tráfico claramente causados de manera regular y sistemática por una o más operadoras de infovía, en general de modo arbitrario, no estipulados en el contrato firmado entre el usuario de la red y la prestadora de los servicios.
En verdad, cuando un usuario contrata un servicio de banda ancha, está contratando un servicio de Internet de extremo a extremo, de cara a tener la misma facilidad de acceso a un sitio web japonés y a otro brasileño, además de usar cualquier servicio cuando lo desee y de la forma como lo desee. Si en el proceso comete alguna ilegalidad respecto del contenido (ofrecer contenido de pedofilia o diseminar contenido cuya copia está protegida por algún contrato de derechos de autor, etc) estaríamos en la misma situación de un usuario que viaja por una carretera y transporta en su carro, de una ciudad a otras, cajas de material ilegal (copias piratas, drogas prohibidas, etc). ¿Sería la concesionaria de la carretera a la que le cabría la responsabilidad de este transporte? Sin asomo de duda la respuesta es no, ya que ésta no tiene poder policíaco ni de fiscalización.

El ejemplo quiere decir lo siguiente: las leyes sobre el uso ilegal o inadecuado de contenido están por encima de Internet y obedecen a las fronteras nacionales y a las convenciones internacionales. Lo que puede ser ilegal en un país puede ser legal en otro (por ejemplo, criticar al gobierno central) pero la operadora de la infovía no debería inmiscuírse en eso (y nunca debería meterse en eso por su cuenta). Las autoridades, cuando se constata la violación de una ley, sí son las que pueden ejercer su poder inclusive buscando el amparo legal de la concesionaria para localizar el lugar donde se origina la infracción.

Milton Mueller, renombrado investigador de políticas públicas para Internet mundial y coordinador del Proyecto de Gobernabilidad de Internet (IGP) en EEUU [8], afirma que no es una violación de la neutralidad de la red el precio diferenciado en función de la velocidad de conexión que se le ofrece al usuario final. Él está en lo cierto pues esto en verdad ya ocurre desde el comienzo de la Internet comercial. El que desee pagar lo menos posible, usa una conexión discada

por períodos cortos de tiempo. Aquel que escoja un servicio más eficaz migra, si puede pagar más, a una conexión de banda ancha; quien quiera descargar o enviar archivos más rápidamente, contrata más banda y paga más por ello. Pero, bajo cualquier situación, tanto un usuario como el otro podrán utilizar todos los servicios de Internet disponibles sin que la operadora interfiera en el flujo de ningún datagrama. Como afirma Mueller: "El tema en realidad es la discriminación, que puede ser motivada tanto política cuanto económicamente... quienes detentan la banda [las operadoras de infovías] no deben bloquear ni enlentecer el contenido que no les plazca ni tampoco deben bloquear ni interrumpir los servicios... simplemente porque compiten con otros servicios de Internet de la empresa... sea cual fuere la garantía de calidad ofrecida a uno, ésta debe estar disponible a todos los demás" [9].

Este es un elemento central para la neutralidad de la red: la infovía no puede censurar ni interferir en el tráfico de contenido, independiente del que se trate.

El debate reciente (exacerbado desde el año 2005 en adelante) en relación a una ley sobre la neutralidad de Internet en EEUU ha sido estimulado en gran parte por iniciativas de las grandes operadoras de infovías de cobrar montos adicionales para conectar grandes proveedores de contenido y asegurar que la banda utilizada funcione con eficacia. Para entender el motivo por el cual el cobro de este monto adicional no tiene asidero, se hace menester comprender cómo la red física que interconecta los dispositivos de Internet está organizada en términos comerciales. Hay una "cadena alimentaria" de conexión, que comienza con el usuario en el extremo y termina en las grandes operadoras de espinas dorsales. En la cima de esta cadena se encuentran las grandes operadoras de espinas dorsales de Europa, de Asia y, sobre todo, de EEUU (entre las cuales están AT&T, Qwest, Verizon/MCI y otras) que controlan el mercado (y el precio) de las conexiones a Internet a nivel mundial. Cualquier conexión a Internet implica el pago respectivo a un proveedor local o a una operadora local de banda ancha que, por su lado, le paga a una gran operadora nacional o regional de espina dorsal y esta le paga a una de las grandes operadoras mundiales de infovías. En otras palabras, cualquier conexión a Internet ya está siendo paga. Lo que las grandes operadoras están postulando puede caracterizarse como un caso claro de doble cobro por el mismo servicio prestado.

De aquí emerge otro elemento central para la neutralidad de la red: no se puede acusar a nadie por "usar demasiado" su conexión. Si un proveedor de contenido tiene un gran éxito y contrata una banda de una cierta capacidad de una operadora, es responsabilidad de la operadora garantizar esa banda, eso es todo. No debe importarle a la operadora si la banda contratada va a ser efectivamente utilizada o no. Si así fuese, la operadora que se prepare para ello y que cumpla el contrato.

Los directores de nuestras empresas de telecomunicaciones y las operadoras de cable pueden estar agitados por eso pero no pueden volverse censuradores de contenido ni tampoco exigir un "peaje" adicional que perjudique a los proveedores de contenido, solo porque usan efectivamente la banda que contrataron. Y mucho menos entrometerse en los servicios de contenido de Internet que sus usuarios utilizan aquí o en el exterior.

Todos os datagramas são iguais perante a Rede!

Neutralidad y Desagregación de Redes: el Ejemplo de Inglaterra

Gustavo Gindre**

La mejor forma de garantizar la neutralidad de las redes parece ser el camino recorrido por el Reino Unido que está siendo estudiado también por otros países de la Unión Europea (como Suecia, Italia y Holanda, por ejemplo): la "desagregación de redes".

En este caso, la operadora de telecomunicaciones está obligada a dividirse en dos unidades diferentes. Una se queda con la infraestructura pero no puede vender sus servicios a usuarios finales, sean estos particulares o empresas. La otra unidad tiene que comenzar a contratar la red para proveer sus servicios. La gran novedad es que la unidad a cargo de la infraestructura está obligada a disponibilizar su red para cualquier otra empresa que quiera contratarla para vender servicios.

En el modelo actual en Brasil, la empresa, que al mismo tiempo es la dueña de la infraestructura y aquella que vende los servicios, tiende a desdeñar la neutralidad de redes para evitar que surjan competidores para sus servicios. Bajo este nuevo modelo, al contrario, la dueña de la infraestructura está interesada en permitir que se implanten nuevas empresas de servicios que quieran contratar su red. Repentinamente, la infraestructura deja de ser un virtual monopolio para volverse un *commodity*.

En el Reino Unido las redes de la British Telecom (BT) fueron desmembradas en una empresa específica (Open Reach) que tiene como clientes tanto a la propia BT como a cualquier otro proveedor de servicios en Internet. Y una serie de reglas de conducta obliga a Open Reach a dar tratamiento isonómico a todos los contratantes, evitando que favorezca los servicios ofrecidos por la British Telecom en detrimento de los demás.

Al proceso le cupo un aumento considerable respecto de la penetración de los accesos de banda ancha.

** *Gustavo Gindre* es investigador del NUPEF, miembro del Colectivo Intervozes y también es uno de los representantes de las organizaciones no gubernamentales sin ánimo de lucro en el CGI.br.

Referências

1 - Robert Poe, "**The Ultimate Net Monitoring Tool**",
Wired (http://www.wired.com/science/discoveries/news/2006/05/70914).

2 - Ver **http://www.eff.org**.

3 - Ver "**Decon apura se empresa cometeu crime contra consumidores**",
Consultor Jurídico, 6 de mayo de 2004 (citado en el servicio de clipping del
Ministerio de Justicia, http://www.mj.gov.br/DPDC/clipping/2004/maio/060504.htm).
En el mes de noviembre de 2004 varios foros de usuarios Skype denunciaron el bloqueo de este servicio
en la red de banda ancha de la BR Telecom y el bloqueo fue rápidamente suspendido luego de las denuncias
(ver, por ejemplo, http://forum.skype.com/lofiversion/index.php/t10669.html).

4 - Ver "**Narus, IBM Help Brasil Telecom Capture IP Services Revenue**",
VOIP Magazine (http://www.voip-magazine.com/content/view/1982).

5 - Son las "**puertas lógicas**" definidas por consenso en base a documentos normativos
(RFCs) discutidos en el ámbito de la Internet Engineering Task Force (IETF, http://www.ietf.org).

6 - Ver "**Telemar, Alô?**", O Globo, 29 de mayo de 2006
(http://oglobo.globo.com/jornal/suplementos/informaticaetc/247699478.asp).

7 - Ver, por ejemplo, "**What's Happening in Congress?**", Save the Internet
(http://www.savetheinternet.com/=faq#congress).

8 - Ver **http://www.internetgovernance.org**.

9 - **Entrevista de Milton Mueller** al portal OPPI de la Rits
(http://www.oppi.org.br/apc-aa-infoinclusao/infoinclusao/busca_results.shtml?
x=1199&slice_id=b086b923a617753o8cc750e201fe2eed).