



Todos os datagramas são iguais perante a Rede!

Carlos A. Afonso

**Neutralidade e desagregação de redes:
o exemplo da Inglaterra**

Gustavo Gindre

Todos os datagramas são iguais perante a Rede!

Carlos A. Afonso*

Todas as informações que circulam na Internet são decompostas em pacotes de dados (os datagramas, ou “packets”), que são enviados por um ou mais caminhos ao destino, onde são recompostos para formar o conjunto de dados original – uma mensagem, uma imagem, um documento, ou mesmo um fluxo de vídeo ou voz.

Um “packet sniffer” (farejador de pacotes) atualmente pode ser capaz de recompor integralmente mensagens de e-mail, fluxos de som ou imagem digital, dados de navegação Web, contidos em um gigabyte de dados copiados da Internet em um único segundo. Isso significa que o farejador pode recompor e gravar milhares de mensagens de e-mail, ou ainda uma imensa quantidade de dados trafegados por pessoas que navegam em sítios Web, em um único segundo. Pode ainda reconstituir e gravar milhares de conversações simultâneas de telefonia via Internet (conhecida como “voz sobre IP” ou voIP). Os datagramas são analisados e eventualmente copiados para um banco de dados, e continuam ou não seu caminho – e podem, por exemplo, continuar em um fluxo muito mais lento. Tudo isso é programável por “farejadores” de datagramas e gerenciadores de tráfego (os “traffic shapers”). A menos que os dados não cheguem, nem recipiente nem remetente

saberão de nada. Se for telefonia via Internet, o usuário pode atribuir a voz entrecortada a um eventual tráfego intenso em algum ponto da rede. Em resumo, essas iniciativas são difíceis de detectar por um usuário não especialista ou alguém que não seja particularmente teimoso.

Um gigabyte de dados por segundo significa uma capacidade de transmissão de 10 Gb/s (10 gigabits por segundo, ou um bilhão de caracteres por segundo), fluxo maior que a capacidade somada de todas as espinhas dorsais (infovias principais, ou “backbones”) da Internet da maioria dos países. Um farejador moderno é basicamente um software contido em um microcomputador de alta capacidade -- mas não muito diferente dos computadores domésticos de topo de linha que a garotada mais abastada usa para seus joguinhos. Utilizando a eficácia de sistemas operacionais similares ao UNIX, o farejador trabalha em uma máquina conectada a um ponto estratégico da Internet -- por exemplo, um ponto de troca de tráfego (PTT) entre várias infovias.

Farejadores com essas características são vendidos, por exemplo, pela empresa Narus¹. Uma licença típica de uso custa em torno de US\$50 mil – uma ninharia para a NSA (a Agência Nacional de Segurança dos EUA) e para qualquer operadora

* Carlos A. Afonso é um dos representantes das organizações não governamentais sem fins de lucro no Comitê Gestor da Internet no Brasil (CGI.br) e diretor de planejamento da Rede de Informações para o Terceiro Setor (Rits).

de infovias da Internet. Este “packet sniffer” veio a público porque a Electronic Frontier Foundation (EFF)², a partir de denúncia detalhada de um funcionário da AT&T, move uma ação contra a empresa sobre violação óbvia de privacidade. A AT&T alega que fez isso a pedido do governo dos EUA, mas nunca informou seus milhões de usuários. Segundo a EFF e o funcionário da empresa, a AT&T usa a tecnologia da Narus para a prática de violação de privacidade em massa.

No Brasil, em 2004, a BR Telecom bloqueou o tráfego de datagramas correspondentes a chamadas telefônicas via Internet provenientes de outras empresas de serviços deste tipo, como a Skype e a GVT, por exemplo³. O bloqueio foi suspenso, após denúncia de usuários, no caso do Skype, e por determinação da Anatel, no caso da GVT – afinal, bloquear qualquer datagrama é censurar conteúdo, assunto que, além de violar o direito à liberdade de informação e à privacidade dos dados, extrapola a jurisdição da concessionária de telecomunicações – seria como a concessionária de uma rodovia proibir o tráfego de veículos de cor vermelha ou algo assim. Claro que os advogados da BR Telecom sabiam disso, mas uma concessionária que é um virtual monopólio de um serviço em sua região (uma espécie de “capitania” herdada da privatização das telecomunicações) pode dar-se ao luxo de testar hipóteses na prática – um balão de ensaio para sondar o terreno. Coincidentemente ou não, a BR Telecom é uma das clientes da empresa Narus, como informava até recentemente o próprio sítio Web desta empresa⁴. De qualquer modo, softwares de administração de datagramas são usados rotineiramente pelas operadoras de espionagem para a cobrança de “pedágio” pela passagem de certos tipos de tráfego em seus circuitos.

A prática de manipulação de datagramas não fica apenas na telefonia voIP. As operadoras têm condições de identificar o tráfego de cópia de arquivos entre duas máquinas na Internet (a base dos sistemas de rede “peer-to-peer” ou P2P, como o Bit Torrent, por exemplo), podendo reduzir o fluxo desses datagramas ou simplesmente descartá-los. Por padrão, a maioria dos serviços Internet é definida por um código simples, contido no cabeçalho de cada datagrama, que define o tipo de serviço (cópia de arquivos, voz sobre IP, transferência de dados, acesso Web, envio ou recepção de emails etc). Esses códigos (ou “portas” de serviço) são definidos pelos organismos que coordenam a infra-estrutura lógica da Internet⁵, mas nada impede que outras portas sejam definidas de comum acordo entre dois usuários para realizarem algum tipo de transferência de dados entre eles. No entanto, como em geral essas portas são as utilizadas em todos os aplicativos da Internet por padrão (se não, para quê defini-las?), isso torna a tarefa de identificar e eventualmente bloquear ou “prejudicar” o tráfego de datagramas mais fácil.

Mais um exemplo: a Telemar (hoje Oi) recentemente decidiu bloquear alguns tipos de serviços em seu acesso de banda larga conhecido como Velox, argumentando que estava censurando conteúdo por razões de segurança, para “proteger os usuários”⁶. Repete-se o caso de uma operadora de infovia que decide, ilegalmente, bloquear conteúdo. Máquinas de usuários conectadas à rede Velox que podem estar funcionando com características de servidor sofrem com frequentes quedas da camada de conexão de banda larga, que é simplesmente reiniciada para mudar o número IP designado pela operadora.

Essas iniciativas de intervenção na camada de conteúdo por parte das operadoras, além de ilegais, dificultam o uso das máquinas dos usuários para uma série de serviços, entre os quais a administração remota de servidores, o teste de serviços antes de ativá-los em um servidor real, além de ser frequentemente orientada a prejudicar a comunicação bilateral que envolve tráfego significativo nos dois sentidos. É como se as operadoras de banda larga nos dissessem: use seu computador como um receptor de TV, não como um comunicador! Mas, se você quiser mesmo usá-lo como um comunicador, então vamos decidir o que você pode e não pode comunicar, e com que eficácia. A lei? Ora, a lei...

Em alguns casos, torna-se óbvia a motivação real – reduzir ao máximo possível a eficácia de serviços de terceiros que possam competir com serviços similares oferecidos pela operadora. O caso mais evidente é telefonia voIP, mas, à medida que nos aproximamos da consolidação da chamada “Web 2.0” (envolvendo muito mais interação entre usuários e serviços de comunicação e informação, bem como um crescente comércio de multimeios sob demanda, como TV sobre IP e outros), acompanhada da concentração de serviços Internet nas mãos de operadoras de infra-estrutura, podemos considerar que estamos apenas no começo de tentativas muito mais agressivas de qualificar (ou desqualificar) a conexão do usuário à Internet como um todo.

Uma operadora de banda larga pode (como já estão fazendo) instalar grandes bases de servidores Web com conectividade praticamente direta para os usuários dessa operadora, e a partir desses servidores oferecer repositórios pagos de música e vídeo, e outros serviços Internet mais tradicionais, de modo que, cada vez mais, o usuário seja induzido a ficar

restrito a esse tráfego e cada vez menos busque o resto da Internet. Quando buscar, poderá ter uma qualidade de tráfego deliberadamente pior. Por exemplo, você conseguiria baixar um CD inteiro do servidor da operadora em 20 minutos, mas levaria um ou dois dias baixando um CD de um sítio Internet fora do âmbito da operadora, mesmo que a banda passante real para este sítio “externo” seja de excelente qualidade e esteja descongestionada. É o que se convencionou chamar de “Internet em camadas” (“tiered Internet”). Essa situação é tão séria que levou o Congresso dos EUA a aprovar, em 2006, legislação que garante a neutralidade da rede contra tratamento discriminatório de tráfego⁷.

A Internet, como uma infovia mundial, foi concebida como um espaço neutro e democrático – toda a concepção da Internet tem como premissa a ausência de qualquer controle centralizado sobre seu conteúdo – apesar de que em países inteiros isso é simplesmente atropelado por seus governos. Os operadores da infovia (em geral, empresas de telecomunicações e de redes de TV a cabo), ao oferecer canais para a Internet, implicitamente assumem esse compromisso – que, de resto, está sacramentado em forma de lei em muitos países.

A neutralidade da Internet, como já alertava Lawrence Lessig há cinco anos, significa que os provedores de acesso e de infovias não podem controlar como os usuários utilizam a rede. Não podem censurar datagramas nem discriminar tipos de serviços pelos respectivos conteúdos (seja do cabeçalho ou de qualquer outra parte de qualquer datagrama). Não cabe ao operador de infovia, qualquer que ela seja, decidir se carros vermelhos têm menos prioridade que carros azuis, ou se datagramas de telefonia IP têm menos prioridade que

datagramas de vídeo originados de determinado servidor. Não deveriam (mas fazem isso frequentemente) sequer criar dificuldades para que um pequeno empresário ou usuário doméstico conecte mais de um computador a um mesmo circuito de banda larga.

Foi justamente essa concepção democrática e igualitária, bem como sua prática generalizada à medida que a rede crescia mundialmente, que permitiram a incrível expansão da Internet, bem como a inovação acelerada de seu uso ao longo de poucos anos.

No debate internacional sobre a neutralidade da rede, é frequente ver opiniões procurando enfatizar que muitos dos problemas interpretados como violação da neutralidade são de fato problemas de ordem técnica que ocorrem basicamente no roteamento dos datagramas. De fato, há fragmentação de datagramas maiores, dificuldades ocasionais com as tabelas de roteamento, degradação devido a ataques etc. No entanto, estes problemas não se manifestam de forma regular ou sistemática, ou as empresas de mídia não estariam migrando em massa seus serviços para a Internet. Aqui nos referimos a efeitos no tráfego claramente provocados de maneira regular e sistemática por uma ou mais operadoras de infovia, frequentemente de modo arbitrário, não especificados no contrato entre o usuário da rede e a prestadora dos serviços.

O fato é que, quando um usuário contrata um serviço de banda larga, ele está contratando um serviço Internet de ponta a ponta. Ele quer ter a mesma facilidade de acesso a um sítio Web japonês e um brasileiro, e usar qualquer serviço quando quiser e da forma que quiser. Se no processo cometer

alguma ilegalidade quando ao conteúdo (oferecer conteúdo de pedofilia, ou disseminar conteúdo cuja cópia é protegida por algum contrato de copyright etc), estaríamos na mesma situação de um usuário de uma rodovia transportando em seu carro de uma cidade para outra caixas de material ilegal (cópias piratas, drogas proibidas etc). Seria a concessionária da rodovia a responsável por esse transporte? Não há a mínima dúvida que não, já que esta não tem poder de polícia nem de fiscalização.

O exemplo quer dizer o seguinte: as leis sobre uso ilegal ou inadequado de conteúdo estão acima da Internet, e obedecem às fronteiras nacionais e às convenções internacionais. O que pode ser ilegal em um país pode ser legal em outro (por exemplo, criticar o governo central), mas a operadora da infovia não deveria ter nada com isso (e nunca deveria meter-se nisso por conta própria). As autoridades, quando constatada a violação de uma lei, sim, é que podem exercer seu poder buscando inclusive o auxílio legal da concessionária para localizar a origem de uma infração.

Milton Mueller, renomado pesquisador das políticas públicas para a Internet mundial e coordenador do Projeto de Governança da Internet (ICP) nos EUA⁸, afirma que não é violação da neutralidade da rede o preço diferenciado em função da velocidade de conexão oferecida ao usuário final. Ele tem razão – isso na verdade já ocorre desde o começo da Internet comercial. Quem quer pagar o mínimo possível, usa uma conexão discada por períodos de tempo curtos. Quem quer um serviço mais eficaz, migra, se puder pagar mais, para uma conexão em banda larga; quem quer baixar ou enviar arquivos mais rapidamente, contrata mais banda e paga mais por isso. Mas, em qualquer caso, tanto um como

outro usuário poderão utilizar todos os serviços Internet disponíveis sem que a operadora interfira no fluxo de qualquer datagrama. Como diz Mueller: "A questão real é a discriminação, que pode ser motivada tanto política quanto economicamente... detentores de banda [as operadoras de infovias] não devem bloquear ou tornar mais lento o conteúdo de que não gostam, e não devem bloquear ou interromper serviços... simplesmente porque competem com outros serviços Internet da empresa... seja qual for a garantia de qualidade oferecida para um, ela deve estar disponível para todos os demais"⁹.

Esse é um elemento central para a neutralidade da rede: a infovia não pode censurar ou interferir no tráfego de conteúdo, seja este qual for.

O debate recente (acirrado a partir de 2005) em torno de uma legislação sobre a neutralidade da Internet nos EUA tem sido estimulado em boa parte por iniciativas das grandes operadoras de infovias de cobrar valores adicionais para conectar grandes fornecedores de conteúdo e garantir que a banda utilizada funcione com eficácia. Para entender por que essa cobrança adicional é injustificada, é preciso compreender como a rede física que interconecta os dispositivos da Internet está organizada em termos comerciais. Há uma "cadeia alimentar" de conexão, que começa no usuário na ponta e termina nas grandes operadoras de espinhas dorsais. No topo dessa cadeia estão as grandes operadoras de espinhas dorsais da Europa, da Ásia, e sobretudo dos EUA (entre as quais a AT&T, Qwest, Verizon/MCI e outras), que controlam o mercado (e o preço) das conexões Internet mundialmente. Qualquer conexão à Internet envolve o pagamento

respectivo a um provedor local ou a uma operadora local de banda larga, que por sua vez paga a uma grande operadora nacional ou regional de espinha dorsal, e esta paga a uma das grandes operadoras mundiais de infovias. Em outras palavras, qualquer conexão à Internet já está sendo paga. O que as grandes operadoras estão propondo pode ser caracterizado como um caso claro de dupla cobrança pelo mesmo serviço.

Daqui emerge um outro elemento central para a neutralidade da rede – não se pode penalizar ninguém por "usar demais" a sua conexão. Se um fornecedor de conteúdo tem grande sucesso e contratou uma banda de determinada capacidade com uma operadora, é responsabilidade da operadora garantir essa banda, só isso. Não interessa à operadora se a banda contratada vai ser efetivamente utilizada ou não. Se for, a operadora que se prepare para isso e honre o contrato.

Os diretores de nossas empresas de telecomunicações e operadoras de cabo podem ficar nervosos com isso, mas não podem tornar-se censores de conteúdo nem exigirem um "pedágio" adicional que penalize os fornecedores de conteúdo, só porque usam efetivamente a banda que contrataram. E muito menos meter o bedelho nos serviços de conteúdo Internet que seus usuários utilizam aqui ou no exterior.

Todos os datagramas são iguais perante a Rede!

Neutralidade e desagregação de redes: o exemplo da Inglaterra

Gustavo Gindre**

A melhor forma de garantir a neutralidade de redes parece ser o caminho trilhado pelo Reino Unido e que já vem sendo estudado por vários outros países da União Européia (como Suécia, Itália e Holanda, por exemplo): a “desagregação de redes”.

Nesse caso, a operadora de telecomunicações é obrigada a dividir-se em duas unidades diferentes. Uma fica de posse da infra-estrutura, mas não pode vender seus serviços para usuários finais, sejam eles pessoas físicas ou jurídicas. A outra unidade passa a ter que contratar a rede para prover seus serviços. E a grande novidade é que a unidade responsável pela infra-estrutura é obrigada a disponibilizar a sua rede para qualquer outra empresa que queira contratá-la para vender serviços.

No modelo atual no Brasil, a empresa, que ao mesmo tempo é a dona da infra-estrutura e aquela que vende os serviços, tende a desrespeitar a neutralidade de redes para evitar que

surjam concorrentes aos seus serviços. Nesse novo modelo, ao contrário, a dona da infra-estrutura passa a ter todo o interesse em permitir que sejam criadas novas empresas de serviços que queiram contratar a sua rede. De uma hora para outra, a infra-estrutura deixa de ser um virtual monopólio para se tornar uma commodity.

No Reino Unido as redes da British Telecom (BT) foram desmembradas em uma empresa específica (Open Reach) que passa a ter como clientes tanto a própria BT quanto qualquer outro provedor de serviços na internet. E uma série de regras de conduta obriga a Open Reach a dar tratamento isonômico a todos os contratantes, evitando que ela beneficie os serviços oferecidos pela British Telecom em detrimento dos demais.

O processo foi responsável por um aumento considerável na penetração dos acessos em banda larga.

** Gustavo Gindre é pesquisador do NUPEF, membro do Coletivo Intervezes e também um dos representantes das organizações não governamentais sem fins de lucro no CGI.br.

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 maio de 2004 (citado no serviço de cclipping do Ministério da Justiça, <http://www.mj.gov.br/DPDC/clipping/2004/maio/060504.htm>).

Em novembro de 2004 vários fóruns de usuários Skype denunciaram o bloqueio deste serviço na rede de banda larga da BR Telecom – o bloqueio foi rapidamente suspenso depois das denúncias (ver, por exemplo, <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 - São as “**portas lógicas**” definidas por consenso a partir de documentos normativos

(RFCs) discutidos no âmbito da Internet Engineering Task Force (IETF, <http://www.ietf.org>).

6 - Ver “**Telemar, Alô?**”, O Globo, 29 de maio de 2006

(<http://oglobo.globo.com/jornal/suplementos/informaticaetc/247699478.asp>).

7 - Ver, por exemplo, “**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** ao portal OPPI da Rits

(http://www.oppi.org.br/apc-aa-foinclusao/foinclusao/busca_results.shtml?x=1199&slice_id=b086b923a61775308cc750e201fe2eed).