

IPv6: Mais endereços, menos segurança?

Segurança em Redes, Mestrado de Engenharia Informática
Universidade do Minho

Miguel Craveiro Martins de Almeida

4 de Julho de 2009

Existe de facto uma resistência muito grande à implementação massiva do IPv6 na Internet. Se a motivação fosse apenas a simplificação do protocolo e dos seus cabeçalhos, o mais certo seria que o IPv6 nunca chegasse a ser implementado. No entanto, a aproximação do fim do espaço de endereçamento do IPv4 não deixa dúvidas de que mais cedo ou mais tarde a massificação do IPv6 acabará por acontecer. As suas imensas vantagens convencem, mas não se estará a regredir em alguns aspectos, nomeadamente na segurança? Vejamos...

A estrutura fixa do IPv4 não permite a implementação de opções de segurança, já que, para se manter de compatibilidade, não podem ser introduzidos novos campos no cabeçalho. Por este motivo, foi entretanto desenvolvida uma versão alternativa do IP que oferece garantias de autenticação, integridade, confidencialidade e de não repúdio - o IPsec - mas a sua configuração é algo complexa e foi desenhada para cenários *router-to-router*. Por outro lado, a versão IPv6 apresenta cabeçalhos mais simples, mas prevê extensões (*header extensions*), onde podem ser incorporadas de forma nativa todas as opções de segurança que o IPsec já apresentava [4, 1, 2] (AH, ESP, etc). Desta forma, a sua utilização fim-a-fim torna-se simples, permitindo que seja implementada em muitas situações que até então teriam de garantir a segurança em camadas superiores da pilha protocolar. Um ponto a favor do IPv6.

Poderá a gigantesca dimensão do espaço de endereçamento complicar o trabalho às aplicações de *scanning*? Estima-se que os 2^{32} endereços IPv4 esgotem por volta de 2012 [6]. Se cada um dos *hosts* que actualmente utiliza IPv4 passar a utilizar IPv6, o espaço por eles ocupado pode ser desprezado, dada a dimensão do espaço IPv6 (2^{128} endereços). Se a sua alocação for uniformemente distribuída por este espaço, o *scanning* por um IP disponível é de facto um problema intratável. No entanto, na prática, acabarão por ser distribuídos por várias gamas bem definidas pela IANA (entidade responsável pela alocação das gamas de endereços IP pelo mundo), voltando a aproximar-se ao IPv4 em termos de segurança.

Apesar de continuar a existir um sistema de DHCP para o IPv6, na sua falta o sistema operativo pode gerar para si mesmo um IPv6 de forma automática [3]. Um dos métodos consiste na adaptação do endereço físico da placa de rede (*MAC Address*) ao formato

EUI-64 [5], pronto a transformar directamente num IPv6. Já que este endereço físico é único no mundo (ou deveria ser) em princípio será o suficiente para se conseguir gerar de forma automática um IP válido e também único no mundo. No entanto, colocam-se questões de falta de privacidade, já que se torna possível identificar fisicamente um dispositivo através do seu IP. Para além disso, implicaria o anúncio de cada IP individual através dos protocolos de *routing* dinâmico. Por estes motivos, prevê-se que este método venha a ser utilizado apenas em ligações locais (*link local*), tal como já acontecia com os IPs do tipo 169.254.0.0/16 do IPv4 quando não existe um servidor DHCP na rede.

Com o IPv4 as redes privadas encontravam-se, de certa forma, escondidas pelo NAT (*Network Address Translation*). Esse conceito deixa de existir com o aparecimento do IPv6. A possibilidade de atribuição de $5,6 * 10^{28}$ de IPs a cada habitante do globo¹ permite que tudo possa ter um IP acessível de qualquer ponto da Internet. É realmente muito cómodo saber-se que as aplicações que não funcionam por trás de NAT (ou que exigem configurações como *port forwarding*, NAT-Traversal ou UPnP) passem a poder funcionar sem ser necessária a configuração do *router* ou a utilização de mecanismos daquele género. Por outro lado, o facto de haver endereçamento directo para o IP da nossa impressora ou até mesmo aos X10 que controlam as luzes e as portas da nossa casa não apresentará por si uma grande vulnerabilidade?

Em IPv4, a *firewall* num *router* com NAT pode ser um elemento dispensável, bastando que não exista mapeamento de portas para o interior e que o próprio *router* não disponibilize serviços para o exterior. Desta forma, a rede privada encontra-se escondida por natureza. Com IPv6, o papel da *firewall* no *router* passa a ser crucial[1], dado que toda a rede privada passa a estar visível do exterior. Naturalmente que se pode filtrar tudo o que entra, mas volta-se novamente à situação de limitar a utilização dos serviços dos clientes internos. Alternativamente, pode instalar-se a *firewall* em cada um dos equipamentos de rede, mas e se não estivermos a falar de computadores, mas sim das impressoras ou das luzes X10? Torna-se obrigatório que estes equipamentos sejam bem configurados para que só possam ser acedidos do interior. Aquilo que até então era simples - ligar uma impressora *plug & play* à rede e começar a imprimir - pode deixar de o ser.

É importante ter-se a noção de que, na verdade, o que a NAT oferece acaba por ser uma segurança aparente. Muitas vezes, o utilizador deposita toda a sua confiança neste mecanismo, chegando até a desactivar as *firewalls* dos computadores no interior da rede e até a deixar serviços críticos como a partilha de ficheiros completamente desprotegida e sem *password* (afinal de contas ninguém fecha à chave as portas dentro da sua própria casa, a partir do momento que a porta da entrada está fechada). Então e se existir um *trojan* instalado por *ad-ware*, alojado num dos computadores da rede? Se este estabelecer uma ligação para o exterior, permite que um intruso passe a ter acesso a qualquer serviço supostamente disponibilizado apenas para o interior da rede, sem que ninguém desconfie ou repare. Tendo em conta estas situações, o peso acrescido que o IPv6 vem trazer às *firewalls* pode indirectamente acabar por proteger melhor as redes privadas (ou que o tentavam ser). O difícil será mesmo encontrar-se o equilíbrio entre o *plug & play* e a segurança.

¹Enquanto que o IPv4 é capaz de endereçar cerca de $4,2 * 10^9$ endereços, os 128 bits do IPv6 permitem por volta de $3,4 * 10^{38}$ endereços IP. Por volta de $5,6 * 10^{28}$ por habitante.

O IPv6, que aparentava ser menos seguro por ser acessível a partir de qualquer ponto da rede, não tem necessariamente de o ser. Já que as *extension headers* tornam a encriptação e autenticação tão acessíveis, pode dizer-se que a segurança do IPv6 estará, de facto, na combinação destes cabeçalhos com uma boa configuração das *firewalls* [1].

Referências

- [1] U. Ellermann, "IPv6 and Firewalls", 1996
- [2] R. Atkinson, "Security for the Internet Protocol", 1995
- [3] C. Perkins, J. Bound "DHCP for IPv6", 1998
- [4] S. Kent, R. Atkinson "Security Architecture for the Internet Protocol", 1998 [RFC-2401]
- [5] S. Thomson, T. Narten "IPv6 Stateless Address Autoconfiguration", 1998 [RFC-2462]
- [6] IPv4 Address Report (auto-generated) <http://www.potaroo.net/tools/ipv4/>