Uma Visão Geral das Soluções para Uso de IPv6

Andrey Vedana Andreoli, Liane Tarouco

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil
{andrey,liane}@penta.ufrgs.br

Resumo. *Este artigo tem por objetivo apresentar um breve relato sobre algumas das principais soluções para uso de IPv6 e interoperabilidade com IPv4, discutidas pelo IETF e em redes experimentais ao redor do Mundo. Trata-se do início de um estudo inicialmente teórico que visa esclarecer os pontos fortes, as limitações e contextos onde cada solução pode ser melhor aplicada. Tais resultados têm fornecido subsídios para testes de implementações em uma rede de testes, que na medida do possível têm sido transportados para ambientes de produção.*

1. Introdução

Como conseqüência do vasto crescimento da Internet, algumas limitações têm se apresentado na versão atual do Internet Protocol, conhecido como IPv4. A principal das limitações envolve o espaço de endereçamento, atualmente com 32 bits. Com a explosão de dispositivos conectados à Internet, o total de endereços unívocos que podem ser utilizados no IPv4 tem se tornado limitado e isso clamou por uma nova tecnologia [COM01]. Os objetivos desta nova tecnologia seriam de aumentar o espaço de endereçamento, oferecer novos recursos para as aplicações que tem surgido e para melhoras na infra-estrutura de rede.

Em 1994, iniciou-se o estudo pelo IETF de uma nova versão do protocolo IP, que surgiu a partir de 1995 através da RFC 1883 [DEE95]. A nova versão do protocolo IP foi intitulada IPng – IP Next Generation.

Em diversos aspectos o protocolo IPv6 [DEE98] assume as mesmas funcionalidades que fizeram o sucesso do IPv4 [ISI81]. Por trata-se de uma inovação que estará incorporada nos diversos níveis da Internet, sua entrada deve ser gradual e capaz de manter a interoperabilidade com o atual IPv4.

A área de roteamento - como sendo o nível mais baixo onde o IPv6 atua - exerce um papel importante e essencial, já que através deste nível operam os demais níveis da Internet, a citar: gerência e segurança de redes, além do desenvolvimento de aplicações.

A área de roteamento representa um conjunto vasto de recursos, formando então a chamada infra-estrutura de rede responsável pelo funcionamento do IPv6. Inicialmente, devido à situação que grande parte dos equipamentos de rede não tinha suporte nativo a IPv6, tornou-se comum a utilização de túneis, fazendo com que o tráfego IPv6 fosse roteado sobre redes IPv4 de forma transparente. No entanto, tal flexibilidade implicava em overhead e ainda na ineficácia do cálculo dos melhores caminhos para determinadas redes IPv6.

A primeira utilização de IPv6 em túneis de maior abrangência surgiu em 1996, chamada de 6Bone [BON04], sendo definida pelo IETF como uma rede de testes, para prover conectividade IPv6 a redes interessadas e contribuir para sua expansão. A adesão a este projeto foi muito grande pelo motivo de ser uma forma simples de uma rede possuir conectividade IPv6 sem adquirir novos equipamentos, permitindo testes com novas aplicações e a experimentação do IPv6 na prática.

A partir daí, diversos recursos tem surgido, além do enfoque de uso de IPv6 não ser mais apenas para validação da tecnologia, mas de uso em produção e sendo objeto de pesquisa para muitas redes experimentais como: Europa com a 6NET [NET04b], Estados Unidos com a Internet2 [INT04], além da iniciativa da Rede Nacional de Pesquisa no Brasil [RNP04].

1. Recursos para IPv6 atuais

Tendo ciência do tamanho da mudança que o IPv6 inclui sobre o IPv4, já que se trata do protocolo/tecnologia básico para a operação da Internet, é esperado que à médio/longo prazo o uso de IPv6 seja fortemente atrelado ao funcionamento em harmonia com o IPv4. Isto tem se revelado como uma das principais preocupações dos grupos de trabalho do IETF, como o V6 Operations [6OP04], e também nas discussões em redes experimentais.

Em resumo, três fluentes têm se apresentado no que tange a esta forma de convivência. Cada uma delas possui características básicas que a diferenciam completamente quanto à infra-estrutura e a forma de acesso IPv4/IPv6. Cada uma será apresentada a seguir:

2.1 Dual Stack

A primeira delas é chamada de "Dual Stack" [GIL00], que se trata de uma integração da pilha IPv6 em sistemas operacionais e equipamentos de rede com a pilha IPv4. Neste caso, o mesmo nodo passa a ter a possibilidade de acesso tanto via IPv4 como IPv6. Inclusive, neste mesmo nodo, algumas aplicações podem usar a pilha que desejarem. Em contrapartida, é necessário que a infra-estrutura nesse caso também seja dual stack, ou seja, que forneça tanto conectividade IPv4, quanto IPv6. Grande parte dos sistemas operacionais de hoje oferecem suporte a este recurso, a citar: Windows XP, FreeBSD, Linux, entre outros. Em equipamentos de rede como roteadores e switch/routers, a realidade também é muito semelhante, visto que já existem diversas implementações de protocolos de roteamento IPv6, a citar: RIPng [MAL97], OSPFv3 [COL99] e MP-BGP [BAT00] além dos tradicionais protocolos de roteamento IPv4.

2.2 Tunelamento

O recurso de tunelamento oferece a possibilidade de acesso IPv6 sobre redes IPv4, ou seja, mesmo não tendo infra-estrutura com suporte ao IPv6, os pacotes são encapsulados sobre IPv4. Trata-se de uma forma amplamente empregada no passado, que visa superar diversos problemas com equipamentos de rede antigos, sem suporte ao IPv6.

A seguir são apresentados alguns recursos/soluções de tunelamento:

2.2.1 IPv6-over-IPv4

Trata-se da forma mais elementar de tunelamento que encapsula os pacotes IPv6 em pacotes IPv4. Definido em [GIL00], trata-se de uma forma de tunelamento ponto a ponto, onde o nodo que encapsula deve explicitamente ser configurado com o IP do nodo destino do túnel. Caso entre o nodo inicial ou final do túnel haja uma firewall, deve ser configurado para permitir pacotes IPv4 entre os nodos cujos códigos de protocolos sejam 41 (IPv6) e 58 (ICMPv6). Para os nodos intermediários ao túnel, o tráfego IPv6 será visto simplesmente como tráfego IPv4, obviamente.

2.2.2 Tunnel Broker

Como forma mais automática ao modelo anterior, surge a abordagem de Tunnel Broker, definida em [DUR01]. Tal abordagem prevê uma forma automática onde um host dual-stack situado em uma rede IPv4-only tem a necessidade de conectividade IPv6. Neste caso, o host dual stack acessa um servidor que fornece algum nível de autenticação, retornando um script que estabeleça uma conexão entre o host e o Túnel Broker Tunnel Server, fornecendo assim uma forma de um tunelamento IPv6 automática. Tal prática pode envolver hosts ou gateways de redes dentro de uma instituição, já que esta é de certa forma automática e depende apenas de planejamento.

Nada impede a disponibilização de Tunnel Broker Servers remotos, mas no ponto de vista de roteamento esta opção pode ser inviável pelo delay que fornece em seu acesso. Neste ponto existe uma iniciativa chamada de Freenet6 [FRE04], que fornece uma espécie de Tunnel Broker Server público no Canadá, com a facilidade de estabelecimento de túneis a partir de qualquer rede, em qualquer país do Mundo. Tal recurso foi testado e de fato pode ser visto como a forma mais eficaz de acesso experimental a rede IPv6 mundial.

2.2.3 6to4

Definida em [CAR01], esta forma de tunelamento é considerada uma das mais triviais, visto que sua configuração é mínima e o bloco de endereçamento é automático, baseado no endereço IPv4 dos nodos envolvidos. O prefixo base, alocado pelo IANA é o 2002::/16, que é complementado pelo endereço IPv4 do nodo, na forma de 2002:IPVADDRESS::/48, resultando em um bloco /48 da mesma forma que os prefixos de produção 2001::/16. Neste caso, na comunicação entre nodos 6to4, o destino é roteado de acordo com o endereço IPv4 envolvido no bloco 6to4 a ser alcançado. Dessa forma, nenhum protocolo de roteamento IPv6 necessita ser utilizado, visto que o pacote será roteado via IPv4.

Na comunicação com hosts que não sejam 6to4, surge a necessidade então de uma entidade "relay", que possa fazer a ligação entre as redes 6to4 e as redes IPv6 nativas, tendo uma interface em cada uma destas redes. Neste caso a entidade relay deve fazer uso de protocolos de roteamento IPv6 para exportar o prefixo da rede 6to4 para a rede de produção (2001::/16) e vice-versa. A localização destes relays públicos é feita através do recurso de anycast, conforme [HUI01].

2.2.4 DSTM

O recurso de Dual Stack Transition Mechanism (DSTM) [BUN02] tem como foco redes IPv6-only, ou seja, que possuem infra-estrutura com suporte apenas a IPv6. Neste

caso, a solução atua como forma de manter o acesso a partir de hosts IPv6 a aplicações sobre IPv4 ou ainda pela necessidade de acesso a algum host/serviço IPv4 pela Internet.

Na comunicação entre nodos IPv6, a solução nada precisa fazer já que a infra-estrutura é IPv6 nativa. No caso de acesso IPv4, duas entidades DSTM entram em ação:

- DSTM Server – Faz o controle de endereços IPv4, recebendo e gerenciando os pedidos de conexões IPv4 ao DSTM client, que é o host que IPv6 que deseja fazer o acesso com destino a IPv4.

- DSTM Gateway – Fornece conectividade IPv4, tendo pelo menos uma de suas interfaces sobre IPv4, além de uma interface na rede IPv6.

Em termos de implementação, atualmente ambas as entidades podem ser utilizadas no mesmo host.

Assim sendo, o DSTM client que deseja fazer a conexão sobre IPv4 envia seu pedido ao DSTM Server, que processa e retorna as seguintes informações ao requisitante:

- O IP da família v4 alocado para a conexão;

- O tempo em que o endereço será alocado;

- Os IPs que serão usados para o túnel até o DSTM gateway;

Com posse destas informações, o DSTM client tem plenas condições de obter conectividade IPv4, em posse de um endereço v4 global.

2.3 Tradução

O recurso de tradução envolve cenários onde hosts IPv6-only consigam se comunicar com hosts IPv4-only e vice-versa. Serão apresentadas duas formas conhecidas envolvendo este recurso:

2.3.1 NAT-PT

Da mesma forma que o recurso de NAT é utilizado hoje no IPv4, o Network Address Translation with Protocol Translation (NAT-PT)[TSI00] oferece uma forma de tradução de um pacote IPv4 em um pacote IPv6 semanticamente equivalente. Uma analogia a esta forma pode ser feita lembrando novamente do NAT IPv4 que converte um pacote IPv4 com endereço privado para um pacote equivalente com endereço global.

Através deste recurso surge a possibilidade de manter uma rede com serviços em IPv4, tendo conectividade através da tradução dos pacotes a qualquer rede da Internet sobre IPv6.

2.3.2 ALG

O recurso de Application Layer Gateway (ALG) oferece recursos muito semelhantes ao NAT-PT, mas possui uma diferença muito sutil. Ao invés de fazer a conversão entre pacotes para torná-los semanticamente equivalentes, o ALG recebe as conexões de seus clientes que são feitas diretamente a ele e em caso necessário, abre uma nova conexão ao destino. Uma analogia a esta solução pode ser feita a proxies web, que usam essa mesma filosofia.

Um exemplo de aplicação é que um servidor ALG receba conexões IPv4 de uma rede IPv4-only e ao observar que a conexão é destinada a uma rede IPv6, abrir uma nova conexão a partir de sua interface IPv6, fazendo o mesmo processo no retorno deste acesso.

3 Conclusões

Tratando-se dos principais recursos disponíveis para uso de IPv6 em conjunto com IPv4, cada um destes apresenta pontos fortes, deficiências e contextos que possam ser melhor explorados. A primeira abordagem, envolvendo o uso de "dual stack" continua sendo a alternativa mais aconselhável nos casos onde há possibilidade de uso de intra-estrutura IPv6, ou seja, que haja disponibilidade de equipamentos de redes e hosts com suporte a IPv6. Dessa forma poderão ser agregados serviços sobre IPv6 sem prejudicar o funcionamento de serviços IPv4. Ao mesmo tempo, surge a necessidade de proteção a partir de redes IPv6, visto que surge a possibilidade de hosts dual stack serem atacados pela pilha IPv6. Essa característica deve ser muito bem analisada, pois pode comprometer o plano de segurança sobre IPv4.

Na existência de equipamentos de rede sem suporte ao IPv6 e por conseqüência, sem infra-estrutura com suporte nativo ao IPv6, a opção de túneis pode ser muito bem vista. É muito comum encontrarmos equipamentos de redes antigos ou sem possibilidade de upgrade, forçando então ao uso apenas em IPv4. Nestes casos, a opção de túneis pode mapear redes inteiras ou pequenos segmentos, fornecendo acesso IPv6 sobre a infra-estrutura IPv4. Quanto as opções de túneis, dependendo da realidade de cada rede, uma opção diferente de tunelamento pode ser melhor empregada, necessitando de um estudo específico. Como limitações desta opção, pode-se citar o risco do roteamento não percorrer os melhores caminhos, pois em um túnel que percorre três hops de distancia, para o protocolo de roteamento que usa este túnel a distância é de apenas um hop. Outro fator importante nessa abordagem é o overhead introduzido pelo processamento no encapsulamento. A opção de DSTM, que foca em uma rede IPv6 nativa como base, mas para a atual realidade ainda é uma opção distante, já que é baseada no uso em massa de IPv6, tendo o intuito de garantir operabilidade com entidades IPv4.

A opção de tradução pode ser vista em contextos onde existe de alguma forma conectividade IPv6 na infra-estrutura, mas que alguns segmentos ou alguns serviços legados apenas permitem o uso sobre IPv4. Tal realidade pode ser aplicada a estações de trabalho antigas ou mesmo sistemas legados. Como limitações podemos incluir o overhead que acaba sendo semelhante ao processamento no encapsulamento nos túneis. No caso da solução com NAT-PT, todos os problemas enfrentados com o NAT também ser transportados para a realidade em IPv6, merecendo um estudo mais aprofundado.

4 Trabalhos Futuros

Como trabalhos futuros espera-se analisar mais profundamente cada abordagem, além de elaborar testes de suas implementações em uma rede experimental com sistemas BSD e Linux, além de roteadores Cisco, com o intuito de avaliar a operação de cada das soluções. A partir desse patamar de testes, será possível obter resultados mais concretos sobre cada solução, além de possibilitar que as melhores soluções sejam implantadas de

forma segura e gradativa em instituições da Rede Tche e na Rede Metropolitana de Porto Alegre (Metropoa).

Referências Bibliográficas

[6OP04] **V6 Operations Working Group on IETF** - http://www.ietf.org/html.charters/v6ops-charter.html - Acesso em Junho de 2004

[BAT00] T. Bates, Y. Rekhter, R. Chandra, D. Katz - **Multiprotocol Extensions for BGP-4** – RFC 2858 – IETF – Junho de 2000

[BON04] **Site do Projeto 6Bone** – www.6bone.net - Acesso em Janeiro de 2004

[BUN02] Bund, Toutain, Medina et al - **Dual Stack Transition Mechanism (DSTM)**

Internet Draft ; draft-etf-ngtrans-dstm-08.txt July 2002

[CAR01] B. Carpenter - **Connection of IPv6 Domains via IPv4 Clouds** - RFC 3056 - IETF - Fevereiro de 2001

[COL99] R. Coltun, D. Ferguson, J. Moy - **OSPF for IPv6** – RFC 2740 – IETF – Dezembro de 1999

[COM01] Douglas Comer – **Redes de Computadores e Internet** – Pág.265-275 – Porto Alegre – Bookman – 2001.

[DEE95] S. Deering, R. Hinden - **Internet Protocol, Version 6 (IPv6) Specification** - RFC 1883 – IETF – Dezembro de 1995

[DEE98] S. Deering, R. Hinden - **Internet Protocol, Version 6 (IPv6) Specification** – RFC 2460 – IETF – Dezembro de 1998

[DUR01] A. Durand, P. Fasano, D. Lento - **IPv6 Tunnel Broker** - RFC 3053 - IETF - Janeiro de 2001

[FRE04] **Freenet6 Project** – www.freenet6.org – On Line – Acesso em Junho de 2004

[GIL04] R. Gilligan, E. Nordmark - **Transition Mechanisms for IPv6 Hosts and Routers** - RFC 2893 - IETF - Agosto de 2000

[HUI01] C. Huitema - **An Anycast Prefix for 6to4 Relay Routers** - RFC 3068 - IETF - Junho de 2001

[INT04] **Projeto Internet2** – www.internet2.edu - Acesso em Janeiro de 2004

[ISI81] Information Sciences Institute/ University of Southern California - **Internet Protocol** - RFC 791 – IETF - Setembro de 1981

[MAL97] G. Malkin, R. Minnear - **RIPng for IPv6** – RFC 2080 – IETF – Janeiro de 1997

[NET04b] **Projeto 6NET da Rede Géant** – www.6net.org - Acesso em Janeiro de 2004

[RNP04] **Projeto IPV6 da RNP** – www.rnp.br/ipv6 - Acesso em Janeiro de 2004

[TSI00] G. Tsirtsis, P. Srisuresh - **Network Address Translation - Protocol Translation (NAT-PT)** - RFC 2766 - IETF - Fevereiro de 2000