

"12 Passos para implementar IPv6 em uma rede de ISP"

Este documento não se destina a ser um resumo técnico abrangente e detalhado de como implantar o IPv6 em uma rede ISP que atualmente tenha IPv4, mas sim um resumo de execução das 12 etapas fundamentais, não incluindo serviços (DNS, web, e-mail, etc.), Para suporte nativo IPv6 e manutenção do IPv4 como um serviço transparente.

1. Quantos clientes (residenciais + corporativo) tem na sua rede e qual é o seu crescimento esperado no curto/médio prazo? Se o total for inferior a 50.000 clientes, recomendamos que solicite ao LACNIC um /32, se você tem entre 50.000 e 100.000 clientes peça um /31, entre 100.000 e 200.000 clientes, um /30, e assim por diante. Se você já tem um /32 e tem acima de 50.000 clientes, solicite ampliação do seu prefixo. Solicite seu prefixo de IPv6 em [Recursos de Numeração](#).
2. Necessita fazer um mapeamento de toda a sua rede, precisa saber quais equipamentos não tem um bom suporte a IPv6, quais devem ser atualizados e quais devem ser substituídos. É importante um relatório muito detalhado, a partir da conexão com seus fornecedores de link (borda) até a as CPEs clientes. Se os fabricantes não lhe dão um bom suporte, avalie a substituição pois o mercado é grande e livre com muitas outras opções.
3. Capacite os profissionais da sua organização com empresas que tenham experiência comprovada na implantação de IPv6 em ISPs. IPv6 não é difícil, mas IPv4 e IPv6 são diferentes e não é tão fácil de "mudar o chip": Você precisa "desaprender" IPv4 para entender bem o IPv6. É conveniente que você contrate o serviço de consultoria em conjunto com o treinamento. Pode parecer excessivo, mas vai economizar uma grande perda de tempo, pois cada vez será mais importante e urgente a transição para o IPv6 e esse tempo vai custar mais na perda de negócios e problemas com IPv4 que o custo de tal treinamento e consultoria.
4. Confirme se seus fornecedores de link tem suporte IPv6, e suba seção BGP com eles. A mesma coisa com CDNs, caches e PTTs. Se os fornecedores atuais não tem suporte, você realmente precisa encontrar outros fornecedores. Esta parte da rede deve ser dual-stack. No pior dos casos, se não houver nenhuma possibilidade de que um ou mais fornecedores de link tenham suporte dual-stack, você pode precisar usar algum túnel, tipicamente 6in4 (protocolo 41, configurado manualmente) ou GRE, mas você deve pensar que isso deve ser temporário.
5. Verifique suas políticas de segurança. Eles devem ser equivalentes às aplicadas com IPv4, mas não filtre o ICMP em IPv6 e outros relacionados que impedem o bom fluxo de tráfego em sua rede. Revise também os filtros para prefixos IPv6 em seus peers BGP, de novo são políticas conceitualmente equivalentes ao que você conhece com IPv4, mas com protocolos diferentes.
6. Configure suporte IPv6 em todos os seus sistemas de monitoramento. IPv6 é tão importante quanto IPv4. Qualquer sistema que permite, tanto de dentro quanto de fora da rede, ver a qualidade do tráfego, quantidade de tráfego, estabilidade do mesmo, visibilidade do seu prefixo, etc., etc., devem estar em igualdade de condições, e IPv4 e IPv6.
7. Agora que você conhece bem as diferenças entre IPv4 e IPv6, esta pronto para desenhar seu plano de numeração, mesmo que boa parte disso possa ter sido feito pela consultoria. Esta é a chave para uma boa implantação do IPv6, é muito diferente do que com IPv4 e definitivamente precisa de um software

como o IPAM (IP Address Management). É impossível gerenciar milhões de IPs com Word ou Excel como você fazia com IPv4.

8. Implante IPv6 em seu core e na sua rede de distribuição. Possivelmente seja suficiente com dual-stack numa primeira fase. Mais tarde talvez você pode eliminar IPv4 dessa parte da rede e tirar proveito desses endereços IPv4 nos locais mais importantes da rede.
9. É aconselhável fazer um piloto em uma parte de sua rede, como de funcionários por ex. Lembre-se que o mínimo em cada LAN ou VLAN é um / 64, a regra de ouro é manter dual-stack em LANs / VLANs (mesmo se eles usam endereços IPv4 privados), o mais aconselhável e prático é usar SLAAC e RDNNs. DHCPv6 é um extra, muitas vezes desnecessário e não suportado por Android por exemplo. Além disso, nesta fase, pode ser interessante inserir um cliente corporativo no piloto, e até mesmo alguns residenciais. Mesmo que nesta etapa seja feito com provisionamento manual.
10. Prepare a sua rede de acesso, e seu sistema de provisionamento. Talvez ele também pode afetar seu sistema de gerenciamento. É necessário estudar qual mecanismo de transição será utilizado. Minha recomendação é 464XLAT¹, pelo menos para os clientes residenciais e redes celulares. É essencial que você tenha um bom suporte dos fabricantes de CPEs. Para provisionar a maneira mais fácil é usar DHCPv6-PD. Estude [BCOP de RIPE](#) sobre como numerar seus clientes.
11. Configure PLAT (NAT64 + DNS64) na sua rede. Não use CGN, vai trazer muitos mais problemas, mais custo (não somente pelo CGN mas também, pelos sistemas de logging). Se você tem uma rede celular, com a implantação de PLAT, e permitindo um APN IPv6-only, você terá tudo funcionando para smartphones e outros dispositivos 3G / LTE. Para Android e Windows, adicione o cliente CLAT, enquanto que no caso de iOS / Apple, use apenas PLAT porque força o suporte IPv6 em todos os aplicativos.
12. Atualize as CPEs. Volte a testar com alguns clientes, uma vez atualizados; isto é mais crítico e mais complexo de todo o processo. Há muitas maneiras de lidar com ele. A partir daqui, você está pronto para ativar IPv6 massivamente (talvez por etapas, regiões, etc.) e realizar a divulgação comercial disso.

Você já tem sua rede preparada para o futuro!

Agora começar a pensar sobre IPv6 e tirar proveito de novos serviços e aplicações, a Internet das coisas é a palavra chave, mas certamente vai encontrar outras vantagens.

Author: Jordi Palet, “The IPv6 Company”

¹ 464XLAT é um dos mecanismos de transição mais modernos (e mais comumente usado, com milhões de usuários em redes 3G / 4G), que tem a vantagem de usar apenas-IPv6 na rede de acesso, que o ISP não requer IPv4 nas mesmas, e ainda fornece endereços privados IPv4 para usuários (através CLAT), de modo que os seus dispositivos e aplicações continuem a funcionar de forma transparente.