ANATEL	**INFORME**	**NÚMERO E ORIGEM:** 6/2014 – ORCN/SOR **DATA:** 31/03/2014

1. INTERESSADO

Superintendência de Outorga e Recursos à Prestação - SOR.

2. INTERESSADO

Fabricantes de equipamentos para telecomunicações, concessionárias e autorizadas de serviços de telecomunicações, Organismos de Certificação Designados, Laboratórios de Ensaios e Usuários de Produtos para Telecomunicações.

3. ASSUNTO

Proposta de Consulta Pública de documento que contém a minuta de requisitos técnicos para a certificação de equipamentos para telecomunicações quanto ao suporte ao protocolo IPv6.

4. REFERÊNCIAS

4.1. Lei Geral de Telecomunicações – LGT – Lei 9.472/97;

4.2. Regulamento para Certificação e Homologação de Produtos para Telecomunicações – aprovado pela Resolução n.º 242, de 30 de novembro de 2000;

4.3. Norma para Certificação de Produtos para Telecomunicações – aprovada pela Resolução n.º 323, de 07 de novembro de 2002;

4.4. Regimento Interno da Anatel – aprovado pela Resolução n.º 612, de 29 de abril de 2013; e

4.5. RFC 2460 – Internet Protocol Version 6 (IPv6) Specification.

5. FUNDAMENTAÇÃO

INTRODUÇÃO

5.1. O protocolo IP (*Internet Protocol*) surgiu baseado nas pesquisas e desenvolvimentos do Departamento de Defesa Americano em 1966, através de sua Agência de Pesquisas e Projetos Avançados (ARPA – *Advanced Research Projects Agency*). É um protocolo de camada 3 do Modelo OSI (*Open Systems Interconnect*) responsável por endereçar terminais de comunicação dentro de uma rede WAN (*Wide Area Network*). Ficou muito popular porque é o protocolo utilizado para o transporte de páginas de Internet entre dois terminais em qualquer parte do mundo.

5.2. Atualmente, a versão 4 do protocolo IP (comumente chamada de IPv4) é bastante utilizada nas redes de telecomunicações. Seu projeto prevê 32 bits de endereçamento, o que pode gerar até 4 bilhões de endereços distintos. Embora este número pareça ser suficiente para atender a demanda atual, o que se observa é que já existem regiões onde a quantidade de endereços disponíveis está se esgotando[1]. Isto ocorre porque os endereços IPv4 foram alocados regionalmente de forma ineficiente. Mesmo que fosse corrigida a forma de alocação dos endereços IPv4, eles ainda não seriam suficientes, pois não só computadores hoje têm endereços IPv4, mas qualquer equipamento que se conecte à Internet necessita de um endereço único.

[1] http://www.lacnic.net/pt/web/lacnic/reporte-direcciones-ipv4

5.3. Assim, em 1992 o IETF (*Internet Engineering Task Force*) iniciou estudos para solucionar o problema do esgotamento do protocolo IPv4 e em 1993, por meio da RFC[2] 1550 - *IP: Next Generation (IPng) White Paper Solicitation* – solicitou submissões de pesquisas para a especificação do novo protocolo. Como resultado destas pesquisas e de grupos de trabalhos criados no âmbito do IETF, foi especificada uma nova versão do protocolo, conhecida como a versão 6 do protocolo IP (IPv6). As especificações do protocolo IPv6 foram apresentadas originalmente por meio da RFC 1883 mas, em dezembro de 1998, este documento foi substituído pela RFC 2460, que está atualmente em vigor.

5.4. Desde a época da publicação da RFC 2460 não ocorreram avanços significativos na implementação da última versão do protocolo nas redes. O que se observa é que, atualmente, a transição tem evoluído muito lentamente e, em algumas redes, ainda não há um horizonte definido de atividade nesta área.

5.5. Este documento tem o objetivo de apresentar uma proposta de requisitos para avaliar o suporte de produtos para telecomunicações quanto ao protocolo IPv6. Nesse documento são elencadas as funcionalidades básicas existentes no IPv6. Sob a ótica da Agência, a certificação é uma das formas de estimular a migração do IPv4 para o protocolo IPv6 com menos impacto para operação das redes e com um custo mais baixo, uma vez que o mercado contará com produtos onde o suporte ao IPv6 já foi verificado.

PROTOCOLO IPv6 – PRINCIPAIS CARACTERÍSTICAS

5.6. O IPv6, como definido em sua especificação, trouxe novas funcionalidades e características. A seguir, estão descritas as principais características que são importantes para o estudo que fundamentou a proposição em tela:

Versão	Tamanho do Cabeçalho	Tipo de Serviço	Tamanho Total
Identificação		*Rags*	Deslocamento do Fragmento
Tempo de Vida	Protocolo		Soma de Verificação de Cabeçalho
Endereço de Origem			
Endereço de Destino			
Opções + Complementos			

Estrutura do cabeçalho do protocolo IPv6 (Fonte: apostila "curso IPv6 básico" do NIC.br, disponível no endereço http://curso.ipv6.br ou através do e-mail ipv6@nic.br)

Versão	Classe de Tráfego	Identificador de Fluxo
Tamanho dos Dados	Próximo Cabeçalho	Limite de Encaminhamento
Endereço de Origem		
Endereço de Destino		

Estrutura do cabeçalho do protocolo IPv4 (Fonte: apostila "curso IPv6 básico" do NIC.br, disponível no endereço http://curso.ipv6.br ou através do e-mail ipv6@nic.br)

5.6.1. Maior capacidade de endereçamento: no IPv6, o espaço para o endereçamento aumentou de 32 para 128 bits, o que equivale a aproximadamente $3x10^{38}$ endereços IPs (isto é, a título de ilustração, são possíveis aproximadamente $6,7x10^{23}$ endereços

[2] RFC – *Request for Comments*

IP por metro quadrado da superfície terrestre). Além disso, proporciona níveis mais específicos de agregação de endereços e a implementação de mecanismos de autoconfiguração.

5.6.2. Simplificação do formato do cabeçalho: alguns campos do cabeçalho IPv4 foram removidos ou tornaram-se opcionais, com o intuito de reduzir o custo do processamento dos pacotes nos roteadores.

5.6.3. Suporte a cabeçalhos de extensão: as opções não fazem mais parte do cabeçalho base, permitindo um roteamento mais eficaz, limites menos rigorosos em relação ao tamanho e a quantidade de opções, e mais flexibilidade para a introdução de novas opções no futuro.

5.6.4. Capacidade de identificar fluxo de dados: foi adicionado um novo recurso que permite identificar pacotes que pertençam a determinados tráfegos de fluxos, para os quais podem ser requeridos tratamentos especiais.

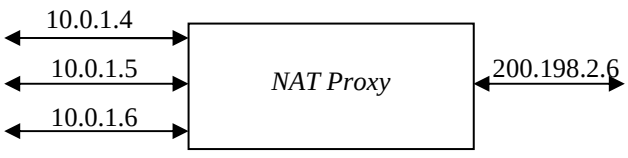
5.6.5. Suporte à autenticação e privacidade: foram especificados cabeçalhos de extensão capazes de fornecer mecanismos de autenticação e garantir a integridade e a confidencialidade dos dados transmitidos.

O PROBLEMA DO ESGOTAMENTO DE ENDEREÇOS IPv4

5.7. Nos últimos anos, os Órgãos Regionais Administradores dos endereços IP (a exemplo do LACNIC – *Latin America and Caribean Internet Register*) vêm alertando sobre a necessidade da migração da versão 4 (IPv4) para a versão 6 (IPv6) do protocolo IP. Este alerta se deve ao fato de que existem poucos recursos disponíveis de endereços IPv4 para distribuição.

5.8. Neste cenário, existem algumas opções possíveis para fazer frente ao grande crescimento das redes e a consequente escassez de endereços:

5.8.1. O uso do NAT (*Network Address Translation*). O NAT tradicional é uma técnica definida pela RFC 3022 - *Traditional IP Network Address Translator* (*Traditional* NAT). O NAT permite que os terminais de uma rede privada possam acessar, transparentemente, terminais em uma rede externa. Ele usa translação entre endereços IP públicos e privados. Endereços IP públicos são aqueles classificados pelo IANA como roteáveis na rede pública. Os endereços IP privados não podem ser roteados nas redes públicas, e foram destinados à comunicação em ambientes IP privados, como em redes locais (RFC 1918 - *Address Allocation for Private Internets*). A translação é feita por meio da correspondência entre um IP válido para um IP privado. Externamente, o terminal destino da comunicação enxergará, como endereço de origem, o IP válido do equipamento que faz o limite entre as redes pública e privada, conforme exemplificado na figura a seguir. Essa técnica tem a grande vantagem de permitir que vários usuários, em uma rede privada, possam utilizar um único endereço IP público para acesso à rede externa. A grande desvantagem desta técnica é a dificuldade da identificação do terminal de origem do tráfego, o que gera uma dificuldade importante para as atividades de investigação de crimes cibernéticos.



5.8.2. Obtenção e desenvolvimento de infraestruturas de rede com endereços IPv4 previamente alocados e não utilizados. Nesta alternativa, seria necessário um trabalho de verificação dos endereços não alocados e ressarcimento dos custos pagos pelo detentor dos endereços. Além disso, existe a necessidade de configuração das novas rotas e tabelas de endereçamento.

5.8.3. Desenvolvimento e uso do protocolo IPv6. Como o IPv6 é capaz de endereçar uma quantidade enorme de dispositivos (≈ 3,4 x 10^{38} endereços disponíveis), pesquisadores consideram que seria possível resolver os problemas de endereçamento na Internet pelas próximas décadas.

5.9. A tabela a seguir compara os diferentes cenários, destacando aspectos de cada solução.

	Utilização do NAT	**Endereços IPv4 não utilizados**	**Implementação do IPv6**
Impacto inicial nas configurações das redes	- Poderá requerer dispositivos e equipamentos adicionais. - As configurações da rede deverão ser revistas.	- Os equipamentos existentes poderão ser utilizados. - Algumas configurações poderão necessitar de revisão pelo uso de endereços IPv4 de outras subredes.	- Requer equipamentos adicionais ou diferentes. - Alguns equipamentos poderão ser atualizados. - As configurações das redes deverão ser totalmente atualizadas.
Impacto nos usuários	- Dificuldade para a comunicação direta entre usuários de redes distintas (por exemplo, aplicações VoIP). - Poderá haver problemas na comunicação quando pessoas diferentes utilizem mesmo endereço privado.	- Necessidade de garantir que os registros tenham sido atualizados com a informação do uso de blocos IPv4 de subdomínios diferentes. - Poderá ocorrer falha na transmissão de dados.	- Requer equipamentos adicionais ou diferentes. - Alguns equipamentos poderão ser atualizados. - Não há limitações no uso dos serviços de transmissão de dados.
Impacto nas prestadoras	- É necessário um conhecimento prévio no gerenciamento da rede. - Não é possível afirmar se esta técnica é estável em redes grandes. - Existem problemas de identificação dos usuários e de segurança.	- Com endereços IPv4 móveis (de outros blocos), haverá uma dificuldade de gerenciamento de endereçamento. - Aumenta a complexidade. - Necessitará de roteadores grandes e caros para suportar estas funções.	- Pode ser necessário um treinamento dos técnicos das operadoras para trabalharem com o protocolo IPv6. - Soluções de transição e de interconexão IPv4 e IPv6 necessitam ser utilizadas.
Custos	- Os custos iniciais são relativamente baixos. No entanto, se ocorrer um aumento significativo de usuários, serão necessários grandes investimentos em infraestrutura. - Custos aumentarão devido ao gerenciamento ampliado.	- Custos iniciais baixos. - Custos operacionais significativos de gerenciamento e de transferência dos blocos IPv4.	- Custos iniciais poderão ser significativos. Dependerá dos equipamentos instalados. - Os custos operacionais também serão altos pela necessidade de coexistência das duas versões do protocolo.

Sustentabilidade	- NAT já é utilizado no mundo inteiro. - Seu uso é limitado, principalmente para servidores que necessitam de endereços públicos. - Esta técnica não acomoda demandas de tráfego fim a fim. - É considerada uma solução de curto prazo e de curta duração.	- Medida de curto alcance, pois os endereços não utilizados são limitados. - Usuários antigos, com grandes blocos de endereços, necessitam se engajar nesta técnica. - É uma mudança muito grande na função de gerenciamento e entrega dos pacotes.	- É uma solução de longa duração.

SEGURANÇA DA INFORMAÇÃO

5.10. Segurança da informação é prioridade na sociedade moderna e recebe a atenção cada vez maior no desenvolvimento de políticas públicas e de soluções tecnológicas de ponta.

5.11. A segurança da rede continuará a ser um desafio em ambos os contextos do IPv4 e IPv6. Em relação aos aspectos de segurança de ambas as versões dos protocolos, podem ser destacados os seguintes aspectos:

5.11.1. A interceptação legal e identificação são mais fáceis com o IPv6, na falta de NAT único ou em várias camadas. Isto se deve ao fato de que o protocolo IPv6 não utiliza esquemas de translação entre endereços públicos e privados. Cada usuário deverá possuir um identificador único em todo o mundo.

5.11.2. Como os novos sistemas operacionais já trazem o suporte ao protocolo IPv6, existe uma possibilidade de falta de segurança nas redes já que os operadores ainda não estão acostumados a trabalhar com a nova versão do protocolo e seus aspectos de segurança.

5.11.3. O protocolo IPsec funciona da mesma maneira entre as duas versões do protocolo IP, mas o IPv6 possui facilidades para o fácil desenvolvimento e uso de aplicações fim a fim seguras.

5.11.4. Como o IPv6 é novo e diferente do IPv4, há um cenário potencial para a criação de novos tipos de ataques baseados em vulnerabilidades ainda não identificadas.

5.11.5. O NAT dificulta a identificação dos usuários e possibilita a realização de ataques cibernéticos sem a identificação da origem.

O PROTOCOLO IP E O SERVIÇO DE TELECOMUNICAÇÕES

5.12. Um assunto que gera muita polêmica é a relação do protocolo IP e os serviços de telecomunicações e a Internet. De fato, no Brasil, a questão é mais polêmica devido à consideração de a Internet ser um serviço de valor adicionado.

5.13. Entretanto, quando se trata o protocolo IP, no âmbito das telecomunicações, trata-se, de fato, das redes de transporte, ou redes de suporte aos serviços de telecomunicações. O protocolo IP é utilizado, hoje, em quase todas as redes de transporte, e transformou-se praticamente no protocolo universal de transporte de informações. Não há como dissociá-lo.

5.14. Assim, a Lei estabelece que à Agência c**ompete tratar de redes de telecomunicações e da fruição dos serviços, o que não exclui os que dependem da utilização do protocolo IP**, segundo o inciso XIV do art. 19 da LGT**.**

CERTIFICAÇÃO DOS PRODUTOS COMO FORMA DE ESTIMULAR O DESENVOLVIMENTO E A UTILIZAÇÃO DO PROTOCOLO IPv6

5.15. Como descrito anteriormente, um dos grandes fatores que dificultam a mudança para o protocolo IPv6 é o custo para esta migração, devido à necessidade de adequação das redes e treinamento de seus operadores. Além do núcleo das redes, os terminais de usuário (modems, telefones smartphones, telefones IP, etc), em sua maioria, ainda não possuem suporte ao protocolo ou não possuem todas as funcionalidades necessárias para operar em um ambiente IPv6.

5.16. Vale ressaltar que, diante da escassez dos recursos de endereços IPv4, algumas operadoras utilizarão o NAT – *Network Address Translation*. Essa solução é paliativa mas, como destacado anteriormente, este tipo de técnica pode dificultar a identificação do usuário de origem, tornando as investigações de crimes cibernéticos mais complexa, e dificultar a utilização de serviços ponto-a-ponto, como o VoIP.

5.17. Para a migração para a versão mais nova do protocolo, alguns requisitos devem ser observados na certificação:

5.17.1. A alteração deve ser gradativa.

5.17.2. Enquanto houver redes com suporte ao IPv4, deve-se garantir a coexistência das duas versões do protocolo na rede. Assim, redes IPv4 devem comunicar-se com as redes IPv6 e vice-versa.

5.17.3. Os equipamentos das redes e dos terminais de usuário, ambos, devem suportar o protocolo IPv6.

5.18. Sobre tais premissas, e considerando-se a experiência brasileira adquirida no processo de certificação de produtos de telecomunicações, a avaliação da conformidade de produtos IPv6 que comporão os núcleos de rede e terminais de usuários é uma decisão adequada para incentivar benefícios da adoção da nova versão do protocolo IP.

5.19. Assim, a inclusão, no processo de certificação dos produtos para telecomunicações, da verificação do suporte ao IPv6 apresentará ganhos à rede de telecomunicações nacional e regional, por exemplo, por meio dos seguintes fatores:

5.19.1. Maior segurança das operadoras de rede para a atualização de sua infraestrutura de transporte, considerando-se que o produto possui certificação com base em "requisitos mínimos" para os protocolos de sinalização, diminuindo, assim, o tempo para a sua aceitação pelas prestadoras.

5.19.2. Maior compatibilidade (interoperabilidade) entre produtos de diferentes fabricantes.

5.19.3. O processo de interconexão entre as redes das operadoras será menos complexo, uma vez que as interfaces e protocolos estarão padronizados.

5.19.4. Os terminais já estarão certificados para o suporte ao IPv6, o que aumentará a interoperabilidade e a possibilidade de oferecer novos serviços.

DA PROPOSTA DE REQUISITOS PARA A CERTIFICAÇÃO DE PRODUTOS QUANTO AO SUPORTE AO PROTOCOLO IPv6

5.20. Para facilitar a implementação da nova versão do protocolo nos serviços de telecomunicações, a Gerência de Certificação e Numeração propõe incluir, numa primeira fase, a avaliação da conformidade de produtos destinados ao uso do público em geral, por meio de requisitos que verifiquem a existência de suporte do produto ao protocolo IPv6.

5.21. A proposta de requisitos está desenhada considerando-se 4 (quatro) possíveis funcionalidades/ambientes de utilização do protocolo: função de *host*, função de roteamento, terminal com interface destinada aos serviços móveis e terminal com interfaces para os serviços de acesso condicionado.

5.22. As funções de *host* e de roteamento estão especificadas na RFC 6434 – *IPv6 Node Requirements*. Um roteador é o nó (ou equipamento) que envia pacotes IPv6 que não são endereçados para ele mesmo. Um *host* (ou terminal) é o equipamento que não têm funções de roteamento.

5.23. As outras duas funções são necessárias em face do ambiente de utilização do produto e dos padrões que especificam as funcionalidades para o protocolo IPv6. No caso dos terminais com interface para os serviços móveis, a RFC 7066 descreve um conjunto de funcionalidades oriundas dos padrões do 3GPP (*Third Generation Partnership Project*). Já os terminais com interfaces para sistemas de TV por assinatura (Serviço de Acesso Condicionado) são especificados pelos padrões da *Cable Labs*.

5.24. A construção dos requisitos levou em conta vários documentos disponíveis que especificam perfis de operação para o protocolo IPv6.

5.25. A proposta da ORCN é seguir os perfis desenhados pelo IETF por meio de RFCs, para os terminais com funções de *host*, roteador e terminais com interfaces para os serviços móveis. Já para os terminais com interfaces para sistemas de TV por assinatura, a proposição é seguir o perfil especificado pela *Cable Labs*.

5.26. Portanto, a proposta de requisitos pode ser sumarizada conforme a seguir:

5.26.1. Produtos com função de *host*: RFC 6434 e RFC 6334 – *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite.*

5.26.2. Produtos com função de roteador: RFC 7084 – *Basic Requirements for IPv6 Customer Edge Routers* – e RFC 6333 – *Dual-Stack Lite Broadband Deployments Follwing IPv4 Exhaustion.*

5.26.3. Produtos com interface aérea destinada aos Serviços Móveis: RFC 7066 – *IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts*.

5.26.4. Produtos com interface para os Serviços de Acesso Condicionado: CM-SP-eRouter-I10-130808 – *Data-Over-Cable Service Interface Specifications. IPv4 and IPv6 eRouter Specification.*

6. PROPOSIÇÃO

6.1. Diante do exposto e, em decorrência da competência legal da Anatel, no tocante à expedição de normas e padrões que assegurem a operação integrada e a interconexão entre as redes, abrangendo inclusive os equipamentos terminais, torna-se fundamental que a Agência estimule o processo de implementação do protocolo IPv6 nas redes e em quaisquer equipamentos de telecomunicações.

6.2. Pretende-se, com esta proposição, obter da sociedade subsídios para a construção de requisitos técnicos mínimos que permitam avaliar o suporte ao protocolo IPv6 nos equipamentos terminais.

6.3. Nesse sentido, a Gerência de Certificação e Numeração submete à deliberação superior este Informe com vistas à apreciação pelo Superintendente de Outorga e Recursos à Prestação e consequente aprovação de proposta de consulta pública, com prazo de duração de 60 dias, em conformidade com o Art. 59 do Regimento Interno da Anatel, aprovado pela Resolução n.º 612, de 29 de abril de 2013.

7. RELAÇÃO DE ANEXOS

7.1. Proposta de Requisitos Técnicos para avaliar o suporte dos produtos destinados ao público em geral com relação ao protocolo IPv6.

7.2. Proposta de Consulta Pública.

7.3. Texto resumo explicando o objeto da consulta pública.

ASSINATURAS	
Responsável pelo órgão elaborador	**Responsável pelo órgão emissor**
(original assinado por) Davison Gonzaga da Silva Coordenador de Regulamentação Técnica – ORCN1	*(original assinado por)* Marcos de Souza Oliveira Gerente de Certificação e Numeração

DESPACHO ORDINATÓRIO (Superintendente)	**Data**
De acordo com a proposição. Submeta-se à Consulta Pública. *(original assinado por)* Marconi Thomaz de Souza Maya Superintendente de Outorga e Recursos à Prestação - SOR	31/03/2014