ARTIGO TÉCNICO SOBRE O
IPv6 no Brasil

ANATEL

CxSC Telecom
Centro de Segurança Cibernética

Inatel

HUAWEI

PREFÁCIO

Artigo técnico sobre o IPv6 no Brasil

por Agência Nacional de Telecomunicações (Anatel)

Com o avanço das Tecnologias de Informação e Comunicação (TICs), a demanda por conectividade dos usuários dos serviços de telecomunicações também se transformou. No passado, o desejo dos brasileiros era um serviço de voz baseado em um acesso fixo, agora, a demanda migrou para uma conectividade de dados baseada em um acesso móvel ou uma banda larga de alta capacidade.

Não por coincidência, as ações de massificação dos serviços de telecomunicações desempenhadas pela Anatel no decorrer dos anos seguiram o mesmo caminho, iniciando com a ampliação da oferta do STFC (Serviço Telefônico Fixo Comutado), passando pelos primeiros editais de licitação do Serviço Móvel Celular (SMC), que trouxeram obrigações de massificação de voz móvel, seguindo para os editais do Serviço Móvel Pessoal (SMP), que substituiu o SMC, focados em conectividade de dados, onde destacamos o edital do 3G, o primeiro que teve um enfoque da massificação de banda larga móvel, e o mais recente edital do 5G, que trouxe obrigações para os vencedores do certame de implementar redes 5G *Standalone* (totalmente orientada a pacotes).

Ressalta-se, ainda, que para que o usuário usufrua da conectividade de dados, não basta que sua prestadora construa a rede de acesso baseada em fibra ou que a prestadora móvel instale antenas do SMP. É necessário que o dispositivo do usuário seja compatível e que as prestadoras tenham um *core* de rede robusto e conectado com as redes de diversos provedores de conteúdo, tanto nacionais como internacionais, que conjuntamente configuram a Internet. E para que haja comunicação na Internet é obrigatório que todos os agentes envolvidos (dispositivo do usuário, redes de acesso, transporte e provedores de conteúdo) utilizem um endereço IP público e válido, conforme definido nos padrões internacionais.

Contudo, o padrão internacional que definiu o endereço IP utilizado até hoje (IPv4) na Internet não previu o crescimento vertiginoso de seus usuários, sendo que os números disponíveis por fim se esgotaram, o que demandou a criação de um novo padrão, o chamado IPv6, para suportar o crescimento da Internet e os novos requisitos que vem surgindo com as novas tecnologias de vanguarda, como a Internet das Coisas (*Internet of Things* - IoT), Cloud Computing e Realidade Virtual e Aumentada, por exemplo.

A distribuição de endereços IPs no Brasil é de responsabilidade do Comitê Gestor da Internet no Brasil (CGI.br), mas a Anatel, como o regulador do setor de telecomunicações, em 2014, estabeleceu um grupo de trabalho, em conjunto com o CGI.br e as prestadoras de telecomunicações, que teve como objetivo

definir metas para a implantação do IPv6 nas redes de telecomunicações brasileiras, além de mecanismos de transição entre o IPv4 e IPv6 para, com isso, disponibilizar o novo protocolo IP no Brasil e garantir que os usuários brasileiros tenham acesso aos conteúdos disponíveis na Internet, estejam estes armazenados em provedores de conteúdo que usem o IPv4 ou IPv6.

Conforme os dados coletados dispostos neste estudo, a partir de 2015, prazo das principais metas acordadas no GT-IPv6, tivemos um grande crescimento da disponibilidade e uso do IPv6 no país, sendo que hoje o Brasil se encontra em 3° lugar na disponibilização do protocolo na América Latina e em 22° lugar a nível mundial. Ressalta-se, contudo, que o crescimento do IPv6 no país deixou de avançar nos últimos anos uma vez que, apesar das redes da maioria das prestadoras e novos equipamentos dos usuários que fazem a interface com a Internet (celulares e roteadores, por exemplo) têm suporte nativo ao IPv6, percebe-se pelos dados levantados pela Agência que a disponibilidade do novo protocolo junto aos provedores de conteúdo ainda tem muito a avançar e que ações adicionais para fomentar sua adoção são necessárias.

A estagnação do crescimento do IPv6 é preocupante porque, tendo em vista a necessidade do usuário em continuar acessando conteúdos disponíveis apenas no protocolo anterior, em conjunto com o fim dos endereços IPv4 disponíveis, foi necessário a implementação de solução de contorno (o chamado CGNAT-44) que permite o compartilhamento dos endereços IPv4 disponíveis entre os diversos usuários, solução esta que traz impactos na experiência do usuário e nas ações de investigação policial que necessitam identificar de forma única o usuário.

Além disso, diversas melhorias disponíveis no IPv6 e em sua evolução (o IPv6 Enhanced) se tornam disponíveis quando todos os elos da cadeia (usuário, rede e conteúdo) utilizam o novo protocolo, melhorias estas que são importantes para que as novas tecnologias de vanguarda que estão surgindo (como a Realidade Virtual e Aumentada e Internet das Coisas, por exemplo) possam ser utilizadas em sua plenitude e gerar valor para a sociedade.

Dessa forma, o presente estudo busca apresentar um panorama do IPv6 e suas características técnicas, como está a sua adoção no Brasil e no mundo, como este auxilia na adoção das novas tecnologias de vanguarda que estão surgindo e, por fim, sugere possíveis caminhos para aumentar a sua adoção no nosso país, trazendo ainda alguns casos de uso sobre o tema.

ÍNDICE

Capítulo 1

Definição e benefícios do IPv6

Capítulo 2

Desenvolvimento global do IPv6

Capítulo 3

Valor e aplicações do IPv6/IPv6 Enhanced nos setores

Artigo técnico sobre o IPv6 no Brasil

Capítulo 4

Índice de desenvolvimento do IPv6

Capítulo 5

Implantação do IPv6 no Brasil

Capítulo 6

Casos de uso do IPv6 e do IPv6 Enhanced

CAPÍTULO 1 - DEFINIÇÃO E BENEFÍCIOS DO IPv6

1.1 Visão geral das inovações do IPv6 e do IPv6 Enhanced

1.1.1 Visão geral de endereços IP e desenvolvimento de tecnologias de IP

A Internet é uma rede global de conexões que, desde seu surgimento, já passou por várias transformações em seus padrões técnicos de funcionamento. As mudanças refletem a evolução do propósito da rede, que ocorre conforme as inovações tecnológicas vão surgindo e mais usuários têm acesso a ela. Atualmente, a Internet é acessada por mais de 5 bilhões de usuários ao redor do mundo [1], e, como já bem conhecido, cada vez mais dispositivos têm sido conectados a ela para diversos fins, inclusive na indústria. Em 2023, a quantidade de dispositivos conectados à Internet ultrapassou a marca de 15 bilhões e até 2030 esse número deve praticamente dobrar [2]. Assim, ela que começou como uma pequena rede dedicada à pesquisa [3], ao longo do tempo, evoluiu e se expandiu, tornando-se essencial para o desenvolvimento e o progresso das nações.

Para a Internet se desenvolver, foi necessário aprimorar as regras de comunicação dos dados. No início da década de 1980, o padrão TCP/IP (*Transmission Control Protocol/ Internet Protocol*) foi adotado e propiciou o crescimento ordenado da rede [3]. Desde então, o protocolo IP, na sua versão IPv4 [4], se tornou o principal protocolo de rede da Internet e assim permanece até os dias de hoje [5].

Os endereços IP são administrados globalmente pela IANA (*Internet Assigned Numbers Authority*). Ela distribui grandes blocos para os Registros Regionais de Internet [6], que gerenciam os endereços em suas respectivas regiões, alocando-os com base em políticas locais. São cinco registros ao redor do mundo, como mostra a Figura 1.

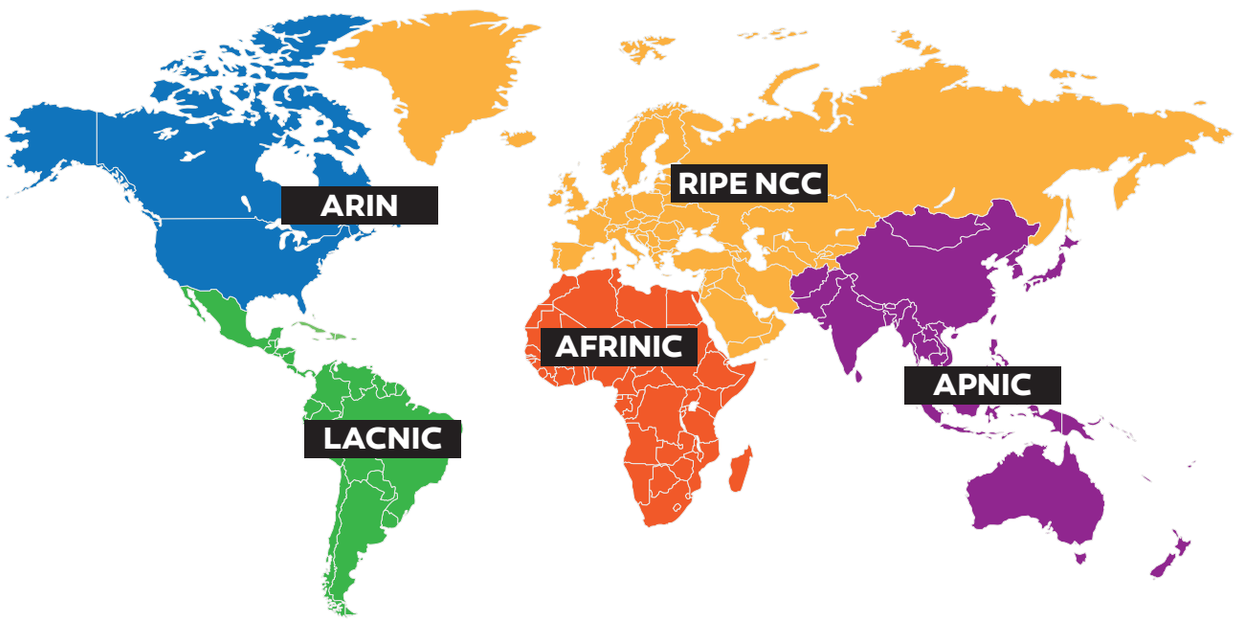

Figura 1 - Distribuição geográfica dos Registros de Internet Regionais (RIR) [6]

O projeto do IPv4, embora robusto, não levou em consideração alguns aspectos importantes para a rede nos dias de hoje, sendo o principal deles a grande demanda de endereços. Ele trabalha com endereços de 32 bits [4], possibilitando identificar cerca de 4,3 bilhões de dispositivos, o que já não é mais suficiente. No início da década de 1990, já havia estudos apontando para o esgotamento dos endereços IPv4 e para problemas devido ao aumento do tamanho da tabela de roteamento [7].

Naquela época, adotou-se algumas medidas paliativas que contribuíram para o uso mais eficiente dos endereços IPv4, atrasando seu esgotamento. Uma das propostas foi o CIDR (*Classless Interdomain Routing*) [8], que extinguiu a segmentação dos endereços em classes. Outra solução foi o DHCP (*Dynamic Host Configuration Protocol*) [9], que permitiu a alocação dinâmica e temporária de endereços para os dispositivos de uma rede. Também foi proposto o mecanismo de NAT (*Network Access Translation*) [10] que, aliado ao conceito de redes privadas [11], permitiu que se compartilhasse um ou mais IPs públicos entre vários elementos de uma rede privada.

Em 1998, surgiu o protocolo IPv6 (IP versão 6), que resolveu o problema de escalabilidade da versão anterior e trouxe vários recursos não contemplados ou não otimizados em seu antecessor [12]. Suas principais vantagens são:

- **Capacidade de endereçamento:** o IPv6 trabalha com endereços de 128 bits [12], resultando em 3,4 x 1038 diferentes combinações. Isso dispensa o uso de NAT na rede e possibilita restabelecer o modelo de comunicação fim-a-fim da Internet.
- **Cabeçalho flexível:** o pacote IPv6 possui um cabeçalho base e cabeçalhos de extensão com funções adicionais que podem ser incluídos após o primeiro formando uma cadeia [12]. Assim, roteadores intermediários não precisam processar essa cadeia completa, aumentando a eficiência na transmissão.
- **Configuração simplificada:** no IPv6, os dispositivos podem se autoconfigurar ao ingressarem em uma rede, através do recurso SLAAC (*Stateless Address Autoconfiguration*) [13]. Isso acelera o provisionamento de novos elementos.
- **Segurança:** o IPv6 possui suporte nativo ao framework IPsec (*IP Security*) [14], que possibilita habilitar mecanismos de autenticação, criptografia e verificação de integridade aos pacotes. Sem a necessidade do uso de NAT, esse recurso pode ser habilitado sem restrições. Além disso, o protocolo possui características que ajudam a evitar alguns tipos de ataques cibernéticos, como o escaneamento de rede.
- **Qualidade de serviço:** o IPv6 provê qualidade de serviço permitindo associar pacotes de um mesmo fluxo e fazer reserva de recurso para priorizá-lo [15].
- **Suporte a melhorias:** os cabeçalhos de extensão do IPv6 podem ser explorados para agregar novas funcionalidades ao protocolo. Isso habilita o desenvolvimento de melhorias contínuas conforme necessário para atender novas demandas.

A transição entre os protocolos IPv4 e IPv6 foi projetada para que acontecesse gradualmente. Para isso, inicialmente, propôs-se a operação em pilha dupla [16]. Assim, haveria uma migração natural do tráfego da rede para o novo protocolo e seu antecessor poderia ser desativado ao final desse processo. Entretanto, isso não ocorreu na velocidade que se esperava e os endereços IPv4 se esgotaram completamente antes da transição se completar [17]. Por isso, foi necessário adotar técnicas auxiliares de transição.

As técnicas de transição podem utilizar mecanismos de tunelamento ou de tradução para integrar dispositivos e redes IPv6 a uma Internet predominantemente IPv4. Elas agregam mais complexidade à rede, mas são necessárias enquanto o IPv4 estiver ativo na Internet. E, para sobrevida desse protocolo, criou-se ainda um mecanismo que realiza NAT nos provedores de

acesso, conhecida como NAT444 ou CGNAT-44 (*Carrier Grade NAT-44*) [18]. Assim, passou-se a ter um duplo NAT e, para isso, foi reservada uma faixa de endereços para ser usada somente na estrutura do provedor [19], como ilustra a Figura 2.

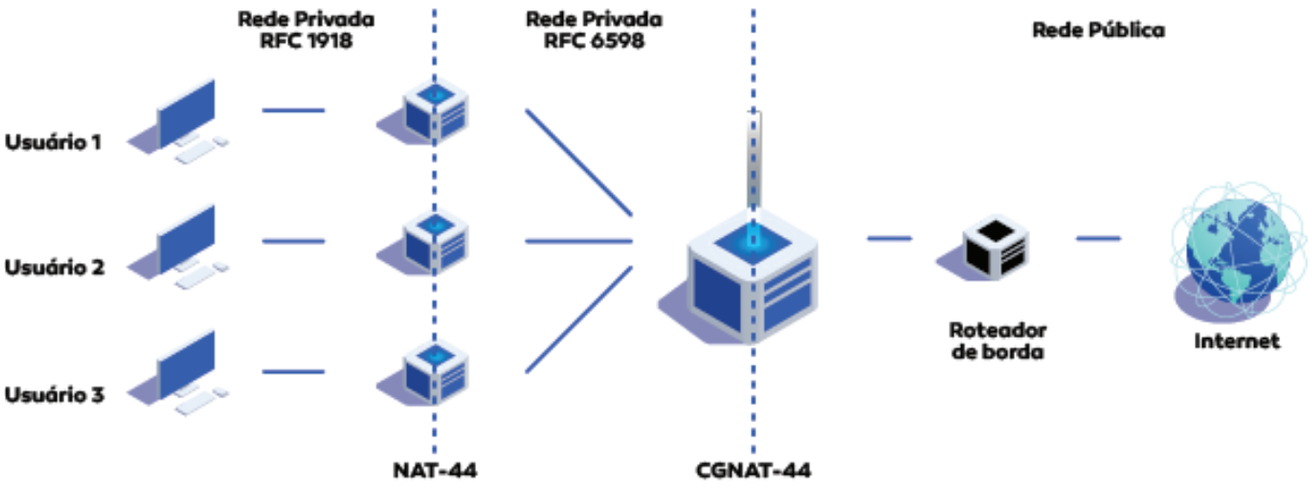

Figura 2 - Arquitetura de rede utilizando CGNAT-44

Essa não consiste em uma técnica de transição entre os protocolos, pois seu objetivo é compartilhar endereços IPv4 públicos entre usuários e não exige a implementação do IPv6. Por isso, é importante mencionar que seu uso isolado não é recomendado, pois ela apenas adia o problema se não for empregada em conjunto com o IPv6. Desde 2012, recomenda-se que todos os dispositivos IP possuam suporte ao IPv6 [20].

1.1.2 Necessidade de transição e evolução do IPv6

Com o advento de inovações tecnológicas como as redes 5G, a IoT e a computação em nuvem, surgem cenários complexos que demandam requisitos de conectividade avançados. Essas exigências vão além de se resolver a questão da falta de endereços IPv4, mas impõem o desenvolvimento de novas funcionalidades para o protocolo IP. Isso intensificou a necessidade de se concluir a transição entre os protocolos, pois o IPv6 permite extensões e melhorias devido à sua flexibilidade. O IPv4 possui limitações que não só irão restringir o desenvolvimento tecnológico, mas também gerarão impactos econômicos e sociais se não for superado.

A rede 5G representa uma revolução para as telecomunicações. Ela irá contribuir com a transformação digital de diversos setores, como educação, saúde, comércio, energia, manufatura, agricultura, entretenimento, indústria automotiva e outros. Sua proposta habilita aplicações como realidade virtual e aumentada, streaming de vídeo de altíssima resolução, telepresença, telemedicina, casas inteligentes, carros autônomos, IoT massiva, dentre muitas outras. Para isso, o 5G provê três cenários disruptivos [21]:

- ***Enhanced Mobile Broadband (eMBB):*** rede móvel de altíssima largura de banda.
- ***Massive Machine-Type Communication (mMTC):*** rede com altíssima densidade de conexões.
- ***Ultra-Reliable and Low Latency Communications (URLLC):*** rede de baixíssima latência e altíssima confiabilidade.

Para prover esses cenários de forma eficiente, o 5G agrega muitas inovações tecnológicas que otimizam sua implementação e sua operação. Dentre elas, pode-se citar a *NFV (Network Function Virtualization)* e o fatiamento de rede *(network slicing)* [21]. A primeira implementa as funções

de rede de forma virtualizada e a segunda permite segmentar a infraestrutura da rede de forma a prover diferentes cenários de conectividade.

A IoT habilita serviços avançados por meio da interconexão entre “coisas”, que são dispositivos inteligentes capazes de processar, enviar e receber dados. Sua arquitetura pode ser dividida em quatro camadas tecnológicas [22]: dispositivos, rede, suporte a serviços e aplicações e segurança da informação. Em cada uma há tendências relativas ao desenvolvimento de tecnologias que melhor se adaptem aos requisitos de conectividade e de infraestrutura. A IoT opera em espaços físicos, como residências, cidades, fábricas e campo. Assim, ela será parte importante da transformação digital de diversos setores e contribuirá significativamente com o desenvolvimento econômico dos países.

A computação em nuvem também trouxe um novo paradigma tecnológico. Ela é definida como “um modelo para permitir acesso onipresente, conveniente e sob demanda através da rede a um conjunto compartilhado de recursos de computação configuráveis que podem ser rapidamente provisionados e dispensados com mínimo esforço de gerenciamento ou interação com o provedor de serviços” [23]. Assim, ela reduz as complexidades do gerenciamento e da operação de TI, agregando eficiência, flexibilidade e economia. Os provedores de nuvem devem garantir cinco características principais a seus clientes: autoatendimento sob demanda, amplo acesso à rede, agrupamento de recursos, rápida elasticidade e serviços mensuráveis. Atualmente, cada vez mais recursos computacionais estão migrando para a nuvem, criando uma tendência de convergência entre nuvem e rede. À medida que as aplicações vão migrando para a nuvem, esta se torna o centro da infraestrutura e a rede deve ser pensada e implementada em seu entorno [24].

O protocolo IPv4 irá limitar o pleno funcionamento das redes 5G e das aplicações de IoT devido a seus problemas de escalabilidade e inflexibilidade. O crescente número de dispositivos conectados vai demandar uma grande capacidade de endereçamento e aplicações de IoT com dispositivos de baixo processamento vão requerer protocolos de comunicação adaptados [25]. Outro fator importante que não será atendido efetivamente é a aplicação de segurança na camada de rede [26]. A rede 5G também irá demandar mecanismos avançados para monitoramento, detecção e correção de falhas, além de medição de desempenho de forma eficiente [26].

Da mesma forma, a computação em nuvem também será restringida pela rede IPv4. Os endereços públicos são hoje um recurso escasso que ficará cada vez mais caro e os provedores de nuvem devem repassar o custo a seus clientes [27]. As limitações de implementação de segurança na camada de rede do IPv4 também é um ponto negativo nesse cenário. Além disso, os serviços em nuvem possuem processos dinâmicos que requerem mecanismos ágeis para suportar o provisionamento rápido e a otimização de recursos, além das atividades de monitoramento [24].

O uso de CGNAT-44 no IPv4 se estabeleceu com o esgotamento de seus endereços. A dependência prolongada desse serviço, necessário para o crescimento da rede, leva a uma piora no desempenho das conexões e a um aumento de custo e complexidade [28]. Além disso, há aplicações que requerem baixa latência na comunicação e existem usuários que hospedam serviços, necessitando de um endereço IP único. Nesses casos, o NAT compromete drasticamente a funcionalidade da rede [28].

O serviço de NAT também traz problemas relacionados à segurança. Um deles é a dificuldade de rastreamento de atividades maliciosas [29]. No caso de um ataque cibernético, é mais complexo identificar sua origem, pois um endereço IP leva a vários usuários, podendo inclusive inviabilizar uma investigação judicial. Outra limitação do serviço é a impossibilidade de se implementar o IPsec em conexões fim-a-fim [30].

Permanecer no IPv4 significa, portanto, limitar o avanço tecnológico e isso irá gerar impactos na economia dos países, pois o desenvolvimento de negócios digitais será cada vez mais prejudicado. Além disso, haverá uma ampliação no gap de distribuição de endereços IP já existente, inclusive na relação per capita dos países [31], aumentando a desigualdade digital. O IPv6 não só resolve as limitações técnicas do IPv4, mas viabiliza outras inovações necessárias no protocolo para o progresso tecnológico, favorecendo o crescimento da economia digital e a promoção de uma Internet mais acessível para todos.

1.2 Arquitetura de evolução do IPv6 Enhanced

A evolução do protocolo IPv6 está acontecendo no sentido de se ter uma rede IP inteligente que suporte as inovações presentes nessa nova era tecnológica. Em 2021, o ETSI (E*uropean Telecommunications Standards Institute*) criou um ISG (*Industry Specification Group*) chamado IPv6 *Enhanced Innovation* (IPE) que reúne vários players da indústria para discutir sobre a evolução do IPv6 [32] . Dentre as atividades do grupo está o desenvolvimento de novas funcionalidades para o protocolo e o IPE pontua que as inovações no IPv6 devem ocorrer continuamente em seis dimensões [24]:

• **Conectividade ubíqua:** os usuários devem conseguir acessar serviços hospedados em diversas localidades, escolhendo dinamicamente a nuvem e o SLA desejado.
• **Largura de banda elevada:** aplicações comerciais de alto desempenho demandam uma infraestrutura de rede com altíssima taxa de transmissão de dados.
• **Qualidade determinística:** alguns serviços nas indústrias precisam de redes que garantam SLAs rigorosos, como baixíssimo jitter e baixíssima perda de pacotes.
• **Baixa latência:** algumas aplicações não toleram atraso na comunicação, como, por exemplo, cenários de IoT e realidade virtual e aumentada.
• **Automação:** as redes devem ser provisionadas rapidamente e serem capazes de detectar e corrigir falhas em pouco tempo para reduzir o impacto nos serviços. Com o aumento de escala e de complexidade da rede, é necessário implementar um novo nível de inteligência e automação nos processos.
• **Segurança:** com a evolução da rede e dos serviços ofertados deve-se aumentar os cuidados com a segurança e isso inclui o desenvolvimento contínuo de tecnologias que atuem na detecção e resposta a ameaças, como a inteligência artificial (IA).

As melhorias no protocolo IPv6, em geral, fazem uso de suas extensões, sem alterações em seu cabeçalho. Assim, elas não impactam a conectividade de uma rede padrão IPv6. A evolução do protocolo IPv6 envolve as inovações descritas a seguir.

1.2.1 SRv6

O SRv6 (*Segment Routing over IPv6*) é um protocolo de suporte ao IP que atua no plano de encaminhamento do IPv6 provendo recursos de programabilidade [33] [34]. Ele elimina a necessidade de alguns protocolos tradicionais, como o LDP (*Label Distribution Protocol*) e o RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) [35]. Assim, ele agrega mais inteligência e simplicidade ao roteamento dos pacotes, atuando melhor frente às demandas de conectividade que estão por vir.

No domínio SRv6, a rede é dividida em trechos denominados segmentos. O trajeto dos pacotes consiste em uma sequência de segmentos definida pelo nó de origem em uma lista que é inserida em um cabeçalho de extensão do pacote IPv6 [33]. Assim, o processo de roteamento dos pacotes se assemelha a um vôo composto de escalas, em que as escalas correspondem aos segmentos.

Ao comprar uma passagem para um determinado destino, o passageiro sabe desde o início os trechos que percorrerá até o fim da viagem.

A programabilidade de rede oferecida pelo SRv6 possui três dimensões [35]. A primeira é a possibilidade de se prover o caminho mais adequado para um fluxo de dados a partir da combinação de segmentos. A segunda é a definição de funções a serem executadas durante o encaminhamento dos pacotes. E a terceira é um campo existente no cabeçalho para funções opcionais. Esse conjunto agrega inteligência ao processo de roteamento, contribuindo para o provisionamento rápido de recursos em resposta às solicitações de clientes e atendimento dos SLAs contratados nos provedores.

O SRv6 não requer que todos os nós de trânsito sejam capazes de processá-lo. Os equipamentos que não suportem o protocolo podem encaminhar os pacotes normalmente processando somente o cabeçalho base IPv6 [33], possibilitando sua adoção gradual.

1.2.2 Fatiamento de rede

O fatiamento de rede é um recurso que permite a criação de múltiplas redes lógicas em uma mesma infraestrutura física e sua aplicação em redes que seguem padrões do IETF, incluindo a tecnologia IP, está sendo discutida [36]. Nesse modelo, cada fatia de rede pode ser definida de forma flexível, variando sua topologia lógica, requisitos de conectividade, nível de segurança e de confiabilidade e, assim, atender a especificações de diferentes serviços e usuários. Isso aumenta a capacidade de monetização dos provedores e facilita a transformação digital.

Um exemplo de aplicação desse recurso é em redes elétricas inteligentes ou *smart grids*, onde há diferentes serviços que possuem diferentes requisitos de conectividade. Por exemplo, sistemas de proteção e controle requerem baixa latência, já sistemas de inspeção por vídeo necessitam de alta taxa de dados, e medidores inteligentes formam um cenário de conexões massivas. Assim, o fatiamento de rede pode ser usado para direcionar os recursos próprios para cada serviço, otimizando o uso da rede.

1.2.3 IFIT

IFIT (*In-situ Flow Information Telemetry*) é um framework em construção que propõe aplicar técnicas de telemetria *on-path* para coletar e relacionar informações de medição para monitoramento de desempenho e detecção de falhas da rede [37]. Nesse modelo, a coleta de dados é feita a partir do tráfego real dos serviços, sem a necessidade do uso de pacotes de teste, permitindo a obtenção de informações mais detalhadas e mais assertivas do plano de dados. Assim, ele melhora significativamente a eficiência das atividades de O&M (operação e manutenção), ajudando a garantir os SLAs contratados e estabelecendo uma base sólida para O&M inteligente, se alinhando aos desafios da era do 5G, da IoT e da computação em nuvem.

1.2.4 APN6

APN6 (*Application-aware IPv6 Networking*) é um recurso em desenvolvimento que visa tornar a rede consciente das aplicações que trafegam por ela [38]. As aplicações são distinguidas com base em atributos APN (*Application-aware*) adicionados ao cabeçalho dos pacotes IPv6, o que possibilita o emprego de políticas diferenciadas para cada uma. Ele pode ser combinado com outras tecnologias, como SRv6, fatiamento de rede e IFIT, permitindo a implementação de serviços de rede de granularidade fina e atividades de O&M precisas e contribuindo para atender aos requisitos de conectividade das aplicações e garantir os SLAs. Assim, consiste em um importante recurso frente aos desafios de inteligência das redes do futuro.

1.3 Desafios de segurança na transição e evolução do IPv6

O IPv6 é um protocolo que se difere em muitos aspectos de sua versão anterior, o IPv4. Contudo, é importante salientar que existem diferenças substanciais tanto em características bem conhecidas do IPv4 quanto em recursos completamente novos no IPv6 e esses novos aspectos também trazem novos desafios de segurança cibernética. A Figura 3 ilustra, de forma não exaustiva, alguns aspectos de cibersegurança do IPv6 e compara, também de forma não exaustiva, com os aspectos do IPv4. Pode-se perceber que alguns aspectos de segurança são similares entre os protocolos, alguns pontos são mais bem endereçados pelo IPv6 e há novos desafios aparecendo juntamente com o IPv6.

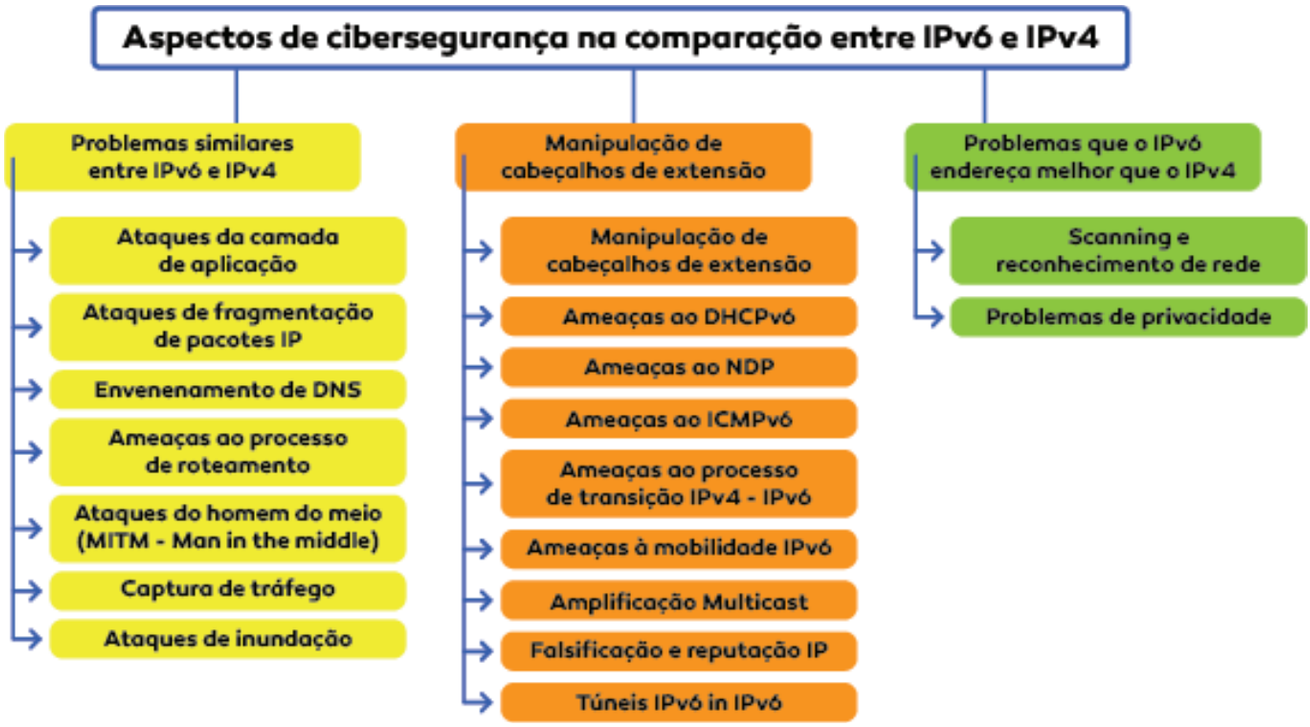

Figura 3 - Aspectos de cibersegurança na comparação entre IPv6 e IPv4

1.3.1 Principais aspectos de segurança similares entre IPv4 e IPv6

Como é bem conhecido, os protocolos IP (versão 4 ou 6) atuam na camada de rede do modelo TCP/IP. Assim, alguns ataques direcionados às outras camadas afetam de forma similar as duas versões do protocolo IP. Esse item apresenta, de forma não exaustiva, alguns ataques que atingem de forma similar tanto o IPv4 quanto o IPv6.

Dentre vários tipos de ataques da camada de aplicação pode-se destacar os que visam aplicações HTTP (*HyperText Transport Protocol*). Em geral, os pacotes de dados dessas aplicações não são examinados do ponto de vista de segurança e é comum serem usados como vetores de ataques, afetando do mesmo modo tanto o protocolo IPv4 quanto o IPv6. O serviço de resolução de nomes da Internet (*DNS – Domain Name System*) também pode ser vetor de vários ataques que atingem ambos os protocolos de forma similar. Ataques DoS que utilizam o DNS, sequestro e envenenamento do DNS podem causar interrupções e redirecionar o tráfego de dados para sites maliciosos nas redes IPs.

A fragmentação de pacotes está presente tanto no IPv4 quanto no IPv6, embora com algumas diferenças. Sendo assim, os ataques de fragmentação IP podem atingir de forma similar ambas as versões do protocolo. Alguns equipamentos de rede fazem uma inspeção rigorosa do

primeiro fragmento do pacote, mas permitem que os demais passem sem o mesmo rigor. Assim, alguns ataques usam a fragmentação IP para se desviarem de dispositivos de segurança, como *firewalls* e até mesmo alguns IDS (*Intrusion Detection System*), dividindo-se aleatoriamente em fragmentos de pacotes IPs.

Os ataques de interceptação, conhecidos como MITM (*Man-in-the-Middle*) também atingem de forma similar o IPv4 e o IPv6. Basicamente, esse ataque explora a inexistência ou falhas de autenticação em sistemas e, portanto, as contramedidas para ele passam por processos de autenticação, como o uso de certificados digitais e sua validação mediante o procedimento de autenticação via IPSec ou TLS (*Transport Layer Security*).

Alguns ataques são direcionados especificamente para os processos de roteamento e repasse das redes IP, que são vitais para o funcionamento da rede. Dentre eles, se destacam: redirecionamento de tráfego, negação de serviço (DoS – *Denial of Service*) ao roteador e ao processo de roteamento, sequestro de rota BGP (*Border Gateway Protocol*), entre outros. Ambas as redes IPv4 e IPv6 sofrem de forma similar com essas ameaças.

O IPv4 e o IPv6 também sofrem de forma parecida com ataques de inundação, ataques de amplificação e ataques de reflexão, que podem aumentar a magnitude de tráfego malicioso e sobrecarregar o alvo, causando a interrupção do serviço ou do sistema.

1.3.2 Problemas de segurança que o IPv6 endereça melhor que o IPv4

O IPv6, de fato, é uma evolução disruptiva de seu antecessor, o IPv4. Suas melhorias e modificações se estendem muito além do aumento de bits na sua convenção de endereçamento. Destaca-se, entre essas modificações, a maior preocupação quanto a questão da segurança da camada de rede e, portanto, esse item traz alguns pontos em que o IPv6 endereça a segurança cibernética de forma melhor que seu antecessor.

Um dos recursos de segurança mais conhecidos da camada de rede é o *framework* IPSec. Ele oferece serviços de segurança, permitindo que um sistema selecione protocolos de segurança exigidos, determine o(s) algoritmo(s) que deseja usar para o(s) serviço(s) e disponha de quaisquer chaves criptográficas para oferecer os serviços solicitados [39]. Contudo, a partir da RFC 6434 [40], o IPSec passou a ser apenas recomendado para o IPv6, ou seja, conforme é feito para o IPv4. Portanto, não é o IPSec que agregará mais segurança à rede, mas sim, a forma de implementação e a competência das equipes de TI e de segurança que irão influenciar o quão segura é uma rede na prática.

No IPsec, há dois modos de implementação: transporte e túnel. Normalmente, o primeiro é usado para oferecer proteção fim-a-fim entre dois hospedeiros, ou dois dispositivos finais (por exemplo, um cliente e um servidor ou duas estações de trabalho). Ele oferece proteção principalmente para os protocolos da camada superior, pois se estende ao *payload* do pacote. O segundo modo oferece proteção entre dispositivos intermediários e normalmente é usado em VPNs (*Virtual Private Network*). Nele, o pacote inteiro é tratado como payload, e adiciona-se um novo cabeçalho IP externamente. Assim, todo o pacote original viaja por um túnel de um ponto da rede a outro, sem que nenhum roteador ao longo do caminho seja capaz de examinar o cabeçalho IP interno.

No IPv4, o IPsec possui restrições por conta da massiva utilização de NAT nas redes. O NAT não é amigável ao IPSec em modo transporte, impossibilitando a proteção fim-a-fim entre dispositivos. Portanto, no IPv4, na maioria das vezes, o uso do IPSec é limitado à conexão entre as bordas da rede sendo empregado em modo túnel e provendo, assim, apenas uma VPN para proteção entre as conexões. Sem a necessidade de utilização de NAT, em redes IPv6 não há restrição

quanto a implementação do IPsec, sendo possível utilizá-lo em modo transporte, proporcionando a proteção da comunicação fim-a-fim.

Outro aspecto de segurança que o IPv6 endereça melhor que o IPv4 é quanto à varredura (*scan*) e reconhecimento de rede, que consiste no primeiro passo para explorar vulnerabilidades em um sistema. Uma varredura sequencial em uma rede pode ser feita muito mais rápido no IPv4, devido à imensa quantidade de endereços IPv6. Isso, embora não impossibilite, torna essa tarefa muito mais árdua e demorada em redes IPv6. Alguns trabalhos têm proposto formas seguras de atribuição de endereços IPv6, visando dificultar cada vez mais a varredura e o reconhecimento de dispositivos [41] [42] [43].

1.3.3 Novos desafios de segurança que devem ser considerados pelo IPv6

Novas tecnologias trazem consigo novas vulnerabilidades, ou, pelo menos, novos desafios quanto à segurança cibernética. O IPv6, apesar de endereçar alguns aspectos de segurança melhor que o IPv4, traz algumas implementações diferentes e, assim, novas preocupações relacionadas à segurança vêm à tona.

Diferentemente do IPv4, no IPv6, o cabeçalho tem tamanho fixo e, para manter a generalidade e ser amigável a novas funcionalidades, criou-se os cabeçalhos de extensão. Essas extensões devem ser incluídas em um pacote conforme a necessidade, aumentando também a eficiência na utilização da largura de banda. No entanto, esse novo conceito pode permitir novas ameaças e ataques à infraestrutura de uma rede IPv6. Por exemplo, o envio de pacotes IPv6 com combinações erradas de extensões ou com uma infinidade de extensões pode aumentar demasiadamente o consumo de recursos da rede levando a um ataque DoS. Além disso, alguns trabalhos também mostraram que extensões de cabeçalho IPv6 podem ser usadas para contornar a segurança de firewalls [44] [45].

O protocolo de descoberta de vizinhança (NDP – *Neighbor Discovery Protocol*) permite que os dispositivos identifiquem seus vizinhos e os notifiquem de sua presença na rede, entre outras funções. Suas funcionalidades contêm vulnerabilidades que podem ser exploradas em ataques como: inundação de mensagens RA (*Routing Advertisement*), RS (*Routing Solicitation*), NA (*Neighbor Advertisement*) e NS (*Neighbor Solicitation*). Há também ataques de falsificação de vizinhança ou de roteador, em que um atacante se passa por um dispositivo legítimo, redirecionando o tráfego para um destino malicioso ou levando a um ataque MITM. Uma solução descrita como SEND (*Security Neighbor Discovery*), RFC 3971, aliado ao CGA (*Cryptographically Generated Addresses*), RFC 3972, pode mitigar esses problemas. Porém, SEND e CGA não são largamente utilizados por questões de complexidade, reivindicações de propriedade intelectual e termos de licenciamento [46]. Além disso, mesmo o SEND pode sofrer ataques de inundação [47].

Ainda com relação ao NDP, o processo de detecção de endereços duplicados pode ser atacado, impedindo que um usuário acesse uma determinada rede. Isso pode ocorrer quando se utiliza a técnica de autoconfiguração SLAAC. Após configurar um endereço para si, o dispositivo encaminha uma mensagem NS para todo seu grupo *multicast* para verificar se já existe algum elemento utilizando aquele mesmo endereço na rede. Se nenhum dispositivo dentro da rede responder a essa mensagem dentro de um tempo pré-determinado, o primeiro dispositivo poderá utilizar o endereço IPv6 autoconfigurado. Sendo assim, um atacante pode permanecer respondendo as mensagens NS toda vez que alguém fizer uma consulta, impedindo que usuários se associem à rede.

Com relação ao protocolo ICMPv6 (*Internet Control Message Protocol*), pode-se exemplificar o ataque onde um terceiro malicioso envia pacotes contendo a mensagem *Too Big* para um roteador. Isso faz com que a MTU desse enlace seja reduzida ao valor mínimo de 1280 bytes, restringindo sua capacidade. O ataque denominado *Smurf*, também conhecido como ataque de amplificação multicast, também é um ataque direcionado ao ICMPv6. Esse é um ataque de inundação de mensagens ICMPv6 *Echo request* que pode elevar o consumo de recursos, levando à negação de serviço.

Como se sabe, o IPv6 não é compatível com o IPv4. Assim, espera-se que as duas versões coexistem na Internet antes de se finalizar a transição para o IPv6. O uso de pilha dupla aumenta a superfície de ataque pois somam-se as vulnerabilidades das duas versões do protocolo no mesmo dispositivo. Além disso, o tunelamento pode permitir ataques de injeção e ataques de reflexão, enquanto o uso de tradução de endereços pode limitar o uso do IPsec, impossibilitar o uso do DNSSEC (DNS Seguro) e permitir ataques de reflexão.

Além de todos os ataques abordados, o IPv6 pode trazer vulnerabilidades devido à pouca maturidade no desenvolvimento dos sistemas que o implementam, como ocorreu com o uso do IPv4 ao longo do tempo. Era comum os sistemas operacionais apresentarem vulnerabilidades em códigos, que precisaram ser corrigidas após descobertas. Isso pode ocorrer com o IPv6, não só pela baixa maturidade no desenvolvimento de produtos, mas, também, das equipes de O&M das redes, levando a falhas de configuração dos sistemas.

CAPÍTULO 2 - DESENVOLVIMENTO GLOBAL DO IPv6

O setor global e os tomadores de decisão em todos os países estão cada vez mais conscientes do valor do IPv6 e do IPv6 Enhanced para a digitalização da economia e de como podem impactar positivamente diversos setores, tais como manufatura, saúde, entretenimento, varejo, educação, turismo, serviços públicos etc., para citar apenas alguns. Devido a isso, todos os países estão tomando medidas, em maior ou menor grau, para fomentar a implantação e a adoção do IPv6 pelos diversos membros do setor.

Infelizmente, o desenvolvimento do IPv6 em todo o mundo é desigual e o estágio atual de um país depende, em geral, de diversos fatores. As ações passadas tomadas pelas diferentes partes interessadas do país com base em suas prioridades são uma delas mas, em muitos casos, o nível de adesão do IPv6 tem alguma relação com o desenvolvimento econômico do país. Os mais desenvolvidos tendem a ter um nível mais elevado. No entanto, existem exceções significativas, como será visto mais adiante.

Para conhecer a situação atual de cada país, diversas instituições, utilizando diferentes metodologias, medem o nível de implantação do IPv6 e publicam uma classificação global. Na seção seguinte é apresentada uma visão geral da situação atual ao examinar alguns dos relatórios mais notáveis.

2.1 Status global de implantação do IPv6

Não é surpreendente que o desenvolvimento global nos últimos anos tenha ganhado impulso e, ao se observar o número de usuários capazes de usar o IPv6 em todo o mundo, percebe-se um aumento em ritmo constante desde 2017. Com base nas estatísticas do APNIC, que é um dos mais usados no setor e fonte de muitos outros índices compostos, a adesão global do IPv6 em outubro de 2023 alcançou mais de 35%.

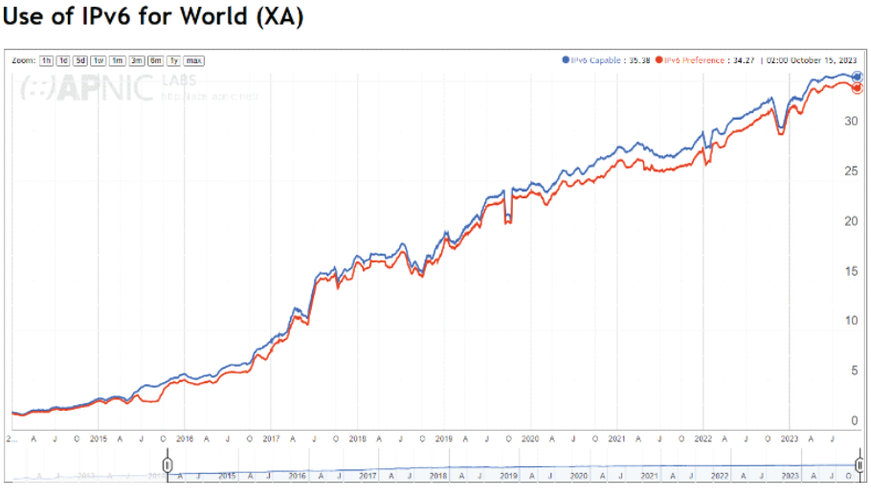

Figura 4 - Usuários habilitados ao IPv6 no mundo

O indicador usado pelo APNIC, que é a porcentagem de usuários capazes de usar o IPv6, é um indicador simples para medir o nível de adoção do IPv6 em cada país e região. O mapa a seguir apresenta uma visão geral da adesão em todo o mundo. No geral, ela é bastante desigual, com países da América do Norte e da Europa Ocidental liderando a lista de classificação, mas com países pioneiros em todos os outros continentes.

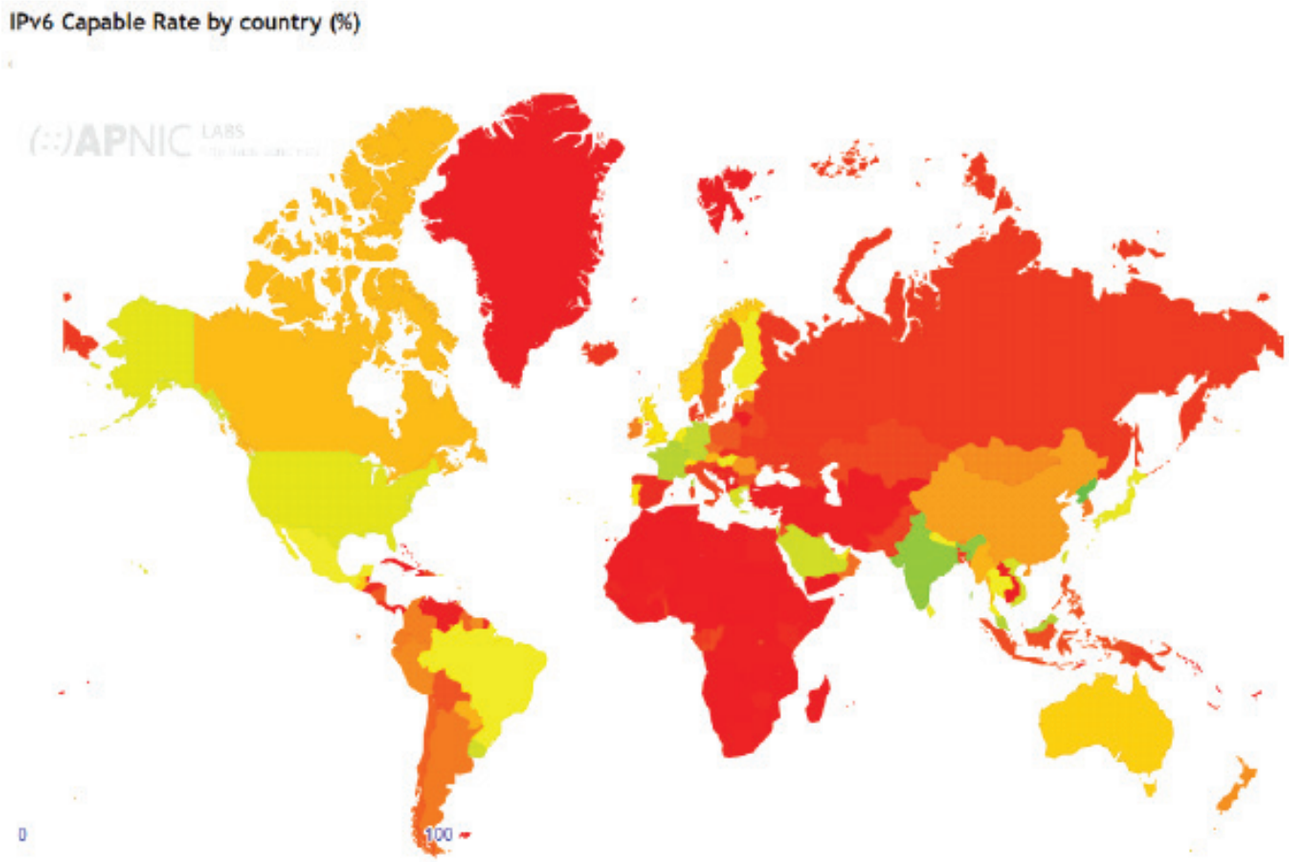

Figura 5 - Mapa de usuários habilitados ao IPv6 por país

Com base neste mapa, pode-se perceber que normalmente os países com maior PIB tendem a ser mais desenvolvidos na adesão do IPv6, mas há exceções notáveis. Por exemplo, Espanha e Itália têm taxas de adesão relativamente baixas, enquanto os países vizinhos da UE têm taxas muito mais altas. Por outro lado, a Índia tem uma taxa de adesão excepcionalmente alta, sendo um país em desenvolvimento. Por regiões, o Sul da Ásia lidera a lista, mas é seguido de perto pela Europa Ocidental e pela América do Norte. Ao fim da lista estão os países da África e da Ásia Central. Por país, Índia e Malásia lideram a lista, com França e Bélgica nas seguintes posições.

2.2 Status de implantação do IPv6 na América Latina

Com base nas mesmas informações do APNIC, é notável que o desenvolvimento na América Latina é bastante discrepante, com o Uruguai na posição de liderança, seguido de perto pelo Brasil e México, quase no mesmo patamar. Todos os outros países da região, com algumas exceções, estão atrasados. O Brasil está na 3ª posição na América Latina com uma adesão de 48%; também está na 22ª posição entre todos os países. Esta excelente taxa de adesão, que se aproxima do limiar de 50%, mostra o esforço de todas as partes interessadas no país e é fruto das políticas relacionadas nos últimos anos.

As estatísticas fornecidas pelo APNIC, embora boas, indicam apenas uma dimensão: estimam a proporção de usuários finais prontos para acessar conteúdo IPv6 ou sistemas finais. A Cisco usa um método mais abrangente para calcular um índice para cada país que, além da métrica do APNIC, também usa outras métricas como prefixos IPv6, disponibilidade de conteúdo IPv6 e outros indicadores, todos baseados em IPv6.

Outro ranking que se destaca e fornece informações abundantes, não apenas sobre a adoção do IPv6, mas também sobre a adoção de soluções de maior valor agregado do IPv6 Enhanced, é o relatório publicado pela consultoria alemã Roland Berger. O último relatório **"Global IPv6 Development Report 2022"** apresenta o Índice de desenvolvimento do IPv6 de 92 países e inclui a maioria dos países da região LATAM.

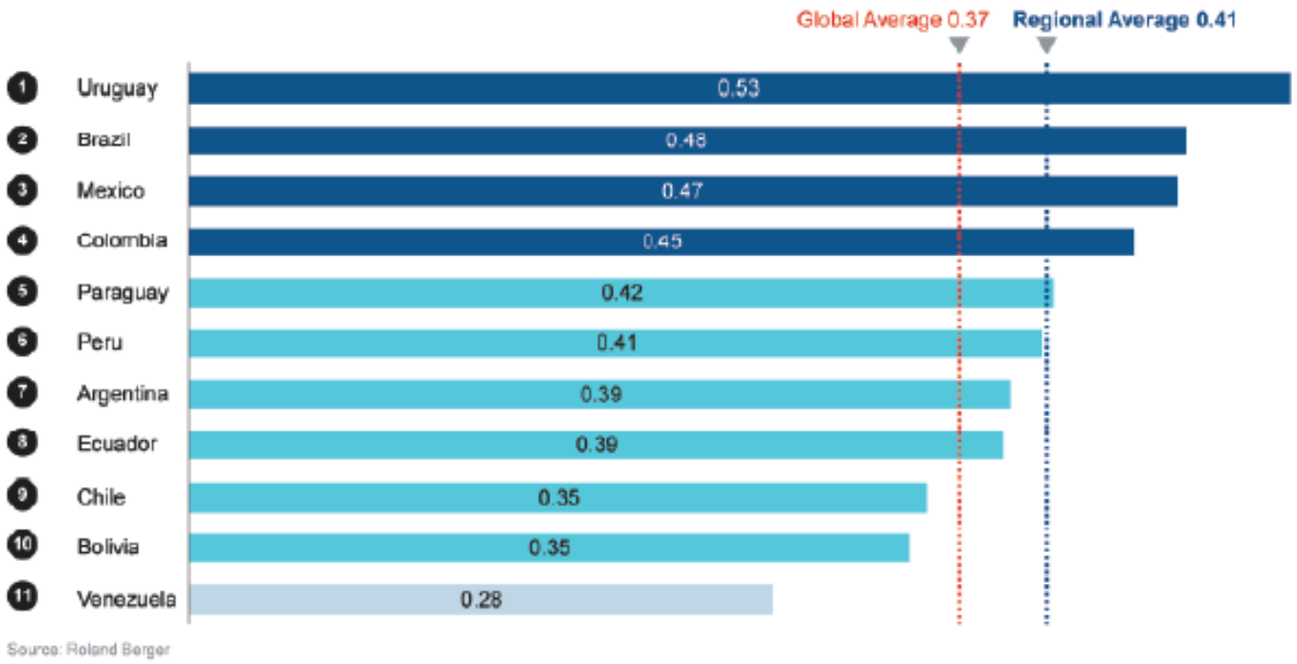

Figura 6 - "Global IPv6 Development Report 2022" da Roland Berger

De acordo com este relatório, o Brasil está classificado em 13º lugar globalmente e na segunda posição na região da América Latina. O índice é calculado com base em três dimensões: inserção, desempenho e inovação do IPv6. Os dois primeiros são puramente baseados em IPv6, mas a dimensão inovação considera também a adesão a tecnologias IPv6 Enhanced. A seguir estão os valores dos diferentes subíndices para o Brasil.

Figura 7 - Detalhamento do índice da Roland Berger no Brasil

Os resultados indicam que a classificação de inserção do IPv6 é boa e está alinhada à classificação do APNIC, mas os valores de desempenho e inovação podem melhorar. Especificamente, um baixo índice de desempenho indica que as redes das operadoras podem ser atualizadas ou ajustadas para fornecer uma melhor qualidade de serviço para tráfego em IPv6. Enquanto um valor baixo no índice de inovação indica uma baixa adesão de tecnologias IPv6 Enhanced e participação em associações padrão e industriais.

2.3 Política global de IPv6 para as indústrias

É evidente que um ambiente industrial favorável, respaldado por políticas adequadas da administração, é a melhor maneira de impulsionar o desenvolvimento do IPv6. As políticas podem adotar diferentes abordagens: implementação, recomendação, subsídio, roteiro e plano estratégico são algumas das práticas comuns. A título de referência, a seguir estão alguns exemplos de políticas adotadas por países importantes.

Estados Unidos

A política dos EUA deixou grande parte da transição do IPv6 para as forças do mercado, mas o governo adotou políticas para direcionar esse processo para as agências federais. Com os provedores de serviços e empresas nos EUA acelerando suas migrações para infraestruturas somente em IPv6, o governo federal dos EUA não quer que suas próprias agências sejam deixadas para trás. O Escritório de Gestão e Orçamento dos EUA (OMB) começou a planejar a transição para o IPv6 em 2005, embora esse processo tenha sido mais lento do que inicialmente previsto. O ritmo de adesão pelas empresas, no entanto, acelerou nos últimos cinco anos, estimulando a OMB a emitir novos requisitos governamentais em novembro de 2020, através de um memorando. Ele exige que as agências federais criem planos para garantir que “pelo menos 80% dos ativos habilitados para IP em redes federais sejam somente IPv6 até o final do ano fiscal de 2025.” Esses planos devem ser apoiados pelo desenvolvimento de “‘um plano de implementação de IPv6 até o final do ano fiscal de 2021.” Além disso, o memorando de novembro de 2020 do OMB determina que as agências federais “identifiquem oportunidades para pilotos IPv6 e concluam pelo menos um piloto de um sistema operacional exclusivamente IPv6 até o final do ano fiscal de 2021”. O Instituto Nacional de Padrões e Tecnologia (NIST) rastreia a adoção do IPv6 pelas agências governamentais. Em agosto de 2020, o NIST estimou que 85% dos serviços DNS do governo dos

EUA, 56% dos serviços da web e 28% dos serviços de e-mail suportavam IPv6 nativamente.

China

O desenvolvimento do IPv6 na China está dividido em quatro etapas. Durante o período de reserva tecnológica de 1999 a 2007, a China lançou o projeto CNGI da rede de demonstração da Internet da próxima geração, que concretizou a interconexão de IPv6 da rede de educação e pesquisa científica. Durante o período de avanço do setor, de 2008 a 2017, foram implementadas a fase comercial de testes de serviços de Internet de próxima geração e a industrialização de equipamentos. Durante o período de aplicação em larga escala de 2017 a 2020, o país lançou o Plano de Ação para Promover a Implantação em Grande Escala do IPv6, e o desenvolvimento do IPv6 se acelerou. De 2021 até agora, o país lançou o Plano de Ação Especial Trienal para Melhoria do Tráfego IPv6 (2021 a 2023), estabelecendo três primeiros objetivos para escala de rede, escala de usuários e escala de tráfego, e liderando o desenvolvimento de redes de próxima geração. Em novembro de 2022, a taxa de implantação integrada de IPv6 na China atingiu 33%. A reconstrução do IPv6 foi basicamente concluída para as operadoras na China. Mais de 95% dos nós CDN na China suportam IPv6. Os 20 principais serviços de 13 grandes empresas de serviços em nuvem na China foram reconstruídos.

A experiência na promoção da implantação de IPv6 em larga escala na China é a seguinte:

- **Diretrizes políticas:** o IPv6 tornou-se uma estratégia nacional. Foram lançados vários documentos de orientação, como o aviso sobre a aceleração da implantação e aplicação em larga escala do IPv6, que define objetivos claros, planos de ação, tarefas principais e medidas de salvaguarda.
- **Coordenação de recursos:** adaptar-se às políticas nacionais e mobilizar recursos dos ministérios nacionais relevantes, incluindo nuvem (infraestrutura de aplicativos), canalização (infraestrutura de rede), dispositivos (móveis e terminais fixos) e usuário. Aplicativos típicos e sites governamentais e empresariais, mídia central e sites empresariais centrais. A supervisão (plataforma de monitoramento) percorre toda a fase de implantação em larga escala do IPv6. Departamentos governamentais em todos os níveis promovem ativamente a implantação do IPv6 em larga escala, incluindo o Ministério da Indústria e Tecnologia da Informação, o Gabinete do Estado, SASAC, o Ministério da Educação e os departamentos políticos e digitais provinciais.
- **Promoção colaborativa:** as instituições de pesquisa são responsáveis por estudar novas tecnologias IPv6 e dar sugestões para planejamento e desenvolvimento do protocolo. A organização de padrões fórmula padrões para o IPv6. Os fabricantes de dispositivos fornecem dispositivos e terminais IPv6 e IPv6 Enhanced para promover a formulação e implementação dos padrões. Operadoras aceleram a implantação de redes IPv6 e participam de discussões sobre requisitos e formulação de padrões. Provedores de conteúdo e setores verticais suportam o acesso IPv6, melhorando a experiência de usuário com o protocolo.
- **Garantia organizacional:** o Comitê de Especialistas em IPv6 foi criado para estudar as estratégias nacionais e questões importantes sobre o protocolo, formular indicadores de desenvolvimento e de monitoramento do IPv6, conduzir supervisão do trabalho e avaliação de suporte do IPv6, estabelecer uma plataforma nacional de monitoramento do desenvolvimento do IPv6 e avaliar o efeito da implementação de documentos políticos. Além disso, organizar a Conferência de Inovação e Desenvolvimento do IPv6 e a Competição de Inovação em Aplicações do IPv6, promover a divulgação e o resumo da experiência.

França

A França é um dos primeiros países do mundo a implantar o IPv6. Já em 2002, o grupo de trabalho nacional sobre IPv6 foi estabelecido. Em junho de 2022, a abrangente taxa de implantação do

IPv6 na França atingiu 63%, classificando o país entre os três primeiros do mundo. Conforme o relatório de evolução do IPv6 na França, divulgado pela Autoridade Reguladora de Distribuição de Comunicações Eletrônicas, Postais e de Mídia Impressa da França (ARCEP) em 2022, a taxa de implantação do IPv6 em redes fixas das operadoras atinge 90% para Free e Orange, 80% para BYT e 40% para SFR. A taxa de implantação do IPv6 nas redes móveis das operadoras atinge mais de 89% pela BYT, 71% pela Orange e 40% pela SFR. 31% dos sites mais populares na França suportam IPv6 e 67% do conteúdo da web suporta IPv6, classificando o país entre os primeiros do mundo. O governo francês implementou diversas medidas regulatórias para incentivar a adesão em larga escala do IPv6 que podem servir de referência para os países. Elas estão descritas a seguir.

• **Lançamento do barômetro de IPv6 anual:** desde 2016, a ARCEP publica anualmente o relatório de progresso do IPv6 na França que mostra o cenário da implantação do IPv6 no país e fornece sugestões para acelerar a transição.

• **Estabelecimento de uma organização de promoção do IPv6:** em março de 2019, foi estabelecida a força-tarefa para o IPv6 na França para desenvolver o roteiro de migração do protocolo e monitorar o progresso de sua implantação.

• **Vinculação entre IPv6 e o espectro 5G:** em dezembro de 2020, a ARCEP lançou uma política para alocar espectros 5G de 3,4 a 3,8 GHz com base no uso em larga escala do IPv6 e exigir que operadoras de redes 5G sejam compatíveis com o IPv6.

• **Promoção da implantação do IPv6 nas empresas:** em março de 2022, a força-tarefa francesa para o IPv6 lançou um whitepaper sobre a implantação do IPv6 nas empresas pela primeira vez para orientar caminhos e práticas corporativas de migração para o IPv6.

• **Construção de uma rede de monitoramento do IPv6:** em junho de 2023, a ARCEP lançou a rede global de monitoramento do IPv6, sendo a França o primeiro país europeu a ter essa iniciativa. Essa rede classifica os 100 principais países quanto ao número de usuários de Internet e rastreia o progresso da implantação do IPv6 de cada um, estimulando a concorrência global e acelerando a implantação do IPv6 em vários países.

Colômbia

Em maio de 2021, o Ministério de ICT atualizou as datas para que suas entidades finalizem a transição do IPv6 (a coexistência com o IPv4 é permitida). Para as entidades nacionais, o prazo foi de junho de 2022, e, para as administrações locais, o prazo foi de dezembro de 2022.

Emirados Árabes Unidos

O governo dos Emirados Árabes Unidos adotou medidas robustas para promover o desenvolvimento do IPv6.

• **Fortalecimento da colaboração internacional:** em 2017, TRA e RIPE NCC assinaram um memorando de entendimento para promover o desenvolvimento do IPv6 nos Emirados Árabes Unidos.

• **Treinamento IPv6 aprimorado:** para acelerar a adoção do IPv6, a TRA estudou as lacunas do mercado e coletou feedback corporativo através dos LIRs dos Registos de Internet dos Emirados Árabes Unidos sobre as principais razões pelas quais as empresas hesitam em mudar para o IPv6. Devido à compreensão limitada do IPv6, à satisfação do cliente com o IPv4 e à cautela do cliente em relação às mudanças, a TRA organiza regularmente workshops e treinamentos em grande escala, o que aumenta muito a confiança das empresas na implantação do IPv6.

• **Prioridade da rede governamental:** em 2018, a rede IPv6 da FedNet foi implementada, garantindo a prontidão de hardware e software IPv6. Em 2019, a FedNet passou a fornecer oficialmente serviços governamentais inteligentes para clientes em todo o país. Projetos governamentais dos Emirados Árabes Unidos, como a plataforma de eLearning, o sistema de informações de saúde eletrônica Wareed e o laboratório de ciência de dados implementaram ativamente o IPv6. Os Emirados Árabes Unidos se tornaram o primeiro país do Oriente Médio a

colocar o protocolo em uso comercial.

• **Prioridade das operadoras:** as operadoras são as pioneiras na implantação do IPv6. Em 2018, ET e du, nos Emirados Árabes Unidos, implantaram o protocolo. Graças aos ganhos da implantação da rede IPv6, a receita anual e o lucro da ET aumentaram constantemente nos últimos cinco anos e as despesas de capital diminuíram em 30%. Após a implantação do IPv6, os serviços da du foram significantemente otimizados, com um crescimento estável do lucro e a proporção de receita para usuários pagantes foi mantida em um nível alto de 80 AED;

• **Padrões do setor publicados:** em 2022, a TDRA lançou o whitepaper 5G 2B dos Emirados Árabes Unidos, o qual define o IPv6 como uma tecnologia obrigatória para a construção de redes 5G, fundamentada na construção da rede 5G e na migração de serviços para a nuvem. Tecnologias IPv6 inovadoras, como SRv6, fatiamento e rede de veículos autônomos, devem ser planejadas e implantadas em cenários-chave para construir uma rede 5G 2B unificada.

CAPÍTULO 3 - VALOR E APLICAÇÕES DO IPv6/IPv6 ENHANCED NOS SETORES

Fomentar a implantação do IPv6 e do IPv6 Enhanced pode aumentar a segurança cibernética e promover o progresso da economia digital no Brasil. A adoção em larga escala do IPv6 estabelece uma base sólida para a Internet dos usuários e contribui para a transformação digital em vários setores. Da mesma forma, o IPv6 Enhanced aprimora ainda mais a infraestrutura de rede e as aplicações das indústrias com suas inovações. Assim, ambos contribuem e são essenciais para o desenvolvimento de um governo digital, de uma sociedade digital e de uma economia digital.

3.1 Operadoras

As operadoras podem se beneficiar muito da construção da infraestrutura de rede e da atualização da Internet baseada em IPv6 e da promoção das inovações tecnológicas do IPv6 Enhanced, como o SRv6, o fatiamento de rede, o IFIT e o APN 6. Além disso, as vantagens de segurança do IPv6 permitem garantir endereços confiáveis, não falsificados e rastreáveis, para uma infraestrutura confiável e segurança integrada de rede em nuvem.

Uma infraestrutura de rede convergente Metro e de backbone com IPv6 Enhanced pode ser construída para suportar novas conexões 10GE de banda ultralarga de forma abundante. Para cenários de serviço completo, pode-se utilizar recursos como SRv6, fatiamento de rede e IFIT para atender aos requisitos de conectividade, tais como flexibilidade na rede, provisionamento rápido de serviços, O&M simplificada da rede, experiência de usuário otimizada e garantia diferenciada. Além disso, esses recursos auxiliam as operadoras a criar serviços de rede privada de IPv6 para governos e empresas, atendendo aos requisitos diferenciados dos setores e aumentando suas receitas.

IPv6 e IPv6 Enhanced auxiliam as operadoras a implementar canais convergentes de serviços completos, serviços diferenciados e capacidade de sinergia entre rede e nuvem, transformando-se em novos provedores de serviços de DICT.

3.2 Governo

Big data governamental, governança urbana, rede privada governamental IPv6 e escritórios móveis estão acelerando o surgimento de elementos de transformação em sistemas, tecnologias e cenários, desafiando continuamente os recursos de serviço de rede.

O IPv6 e o IPv6 Enhanced auxiliam o governo digital a concretizar a “Internet + serviços governamentais” que estão interligados vertical e horizontalmente, promovendo colaboração entre departamentos. A tecnologia de fatiamento de rede e os recursos de segurança integrados garantem a confiabilidade e a segurança dos dados governamentais. Com a ampla cobertura de estados e comunidades, os serviços públicos são providenciados e isolados de forma segura. As aplicações são disponibilizadas na nuvem em um único salto da rede. Os serviços de linhas privadas podem ser provisionados rapidamente e ajustados de maneira flexível, atendendo cada estado e região. Pode-se construir um data center integrado de big data e utilizar Ethernet de alto desempenho e tecnologias inteligentes para viabilizar aplicativos inovadores de elementos de

dados. Por fim, pode-se construir uma rede governamental digital integrada, hiperconvergente, hiperconectada e orientada a serviços, com segurança integrada em nuvem.

3.3 Serviços públicos e cidades inteligentes

IPv6 e IPv6 Enhanced melhoram a governança social nas cidades. No nível individual, os protocolos são mais seguros e as opções padrão de criptografia proporcionam uma proteção aprimorada para as atividades online do dia a dia. As pessoas podem ter mais confiança na segurança de seus dados ao realizar negócios, socializar e transferir arquivos importantes online. Em nível nacional, as câmeras de rede IPv6 (criptografia de rede) podem ser usadas em vários setores. O fortalecimento do mecanismo de monitoramento da rede pode não apenas atender aos requisitos de gestão interna do setor, mas também reforçar a segurança pública nacional.

3.4 Instituições financeiras

O IPv6 e o IPv6 Enhanced auxiliam o setor financeiro a realizar a digitalização das filiais de produção e de escritório, o provisionamento rápido de serviços e os serviços baseados em vídeo, além de acelerar a conexão onipresente da IoT financeira. O SRv6 é configurado apenas nas extremidades e suporta conexão direta de um salto, reduzindo em 80% o tempo de provisionamento do serviço. IPv6 e a IA auxiliarão o setor financeiro a superar limites comerciais e permitirão que os clientes expandam seus serviços de maneira oportuna por meio da expansão flexível de redes de IP inteligentes. Eles ultrapassam os limites da experiência, utilizando redes determinísticas para auxiliar os usuários na migração ágil para a nuvem, proporcionando a melhor experiência ao usuário.

3.5 Energia

O IPv6 e o IPv6 Enhanced oferecem suporte a acesso massivo, interligação entre domínios e alcance de ponta a ponta, auxiliando o setor de energia na implementação de redes de energia completas. O IPv6 de ponta a ponta é usado na rede de produção para promover o acesso seguro à IoT das empresas de energia. O SRv6 com IPv6 Enhanced é usado para implementar nuvem para filiais e campi de produção. A rede de backbone de energia oferece largura de banda estável e latência determinística para serviços de controle industrial, implementando otimização de largura de banda em cenários multiníveis de agendamento de vídeo baseados em SRv6. A detecção associada ao IPv6 Enhanced auxilia na rápida identificação de falhas de serviço, melhorando a eficiência da operação e manutenção. O IPv6 e o IPv6 Enhanced estabelecem novas bases de rede, serviços inteligentes e segurança para IoT, contribuindo para atender melhor à transformação digital das empresas de energia.

3.6 Manufatura

O IPv6 e o IPv6 Enhanced auxiliam o setor de manufatura a convergir e inovar em cenários de redes industriais. A Internet industrial visa realizar a conexão abrangente de todos os elementos, cadeia industrial e cadeia de valor por meio da interconexão total de pessoas, máquinas e objetos. A transformação baseada em IP e a modernização das redes internas e externas será acelerada. Será desenvolvida uma infraestrutura avançada de rede para a Internet industrial por meio de tecnologias inovadoras, atendendo às demandas de conexões de terminais em massa e qualidade de conexão confiável no setor. Isso possibilitará a transferência rápida de dados entre fábricas, empresas e setores industriais, promovendo a integração profunda da tecnologia da informação de rede e da manufatura.

3.7 Transportes

O IPv6/IPv6 Enhanced auxilia o sistema de transporte na construção de um sistema de coleta digital, um sistema de transmissão em rede e um sistema de aplicativo inteligente, promovendo assim a transformação digital e a modernização inteligente da infraestrutura de transporte. Com base em endereços IPv6 em larga escala, a rede rodoviária inteligente detecta a infraestrutura de transporte digital e estabelece uma base para a coleta digital. A rede de nuvem inteligente de IPv6 Enhanced auxilia na construção de plataformas de nuvem para o transporte ferroviário urbano, os aeroportos e a logística. Ela promove a implantação rápida e o compartilhamento eficiente de novos aplicativos de serviço, implementa o gerenciamento do ciclo de vida completo da construção, gestão e manutenção do transporte, contribuindo para a melhoria da experiência de viagem. A detecção de fluxo de IPv6 Enhanced auxilia os departamentos de transporte a resolver problemas de operação e manutenção causados pela convergência de dados, localizar falhas com precisão e construir uma rede inteligente de dados de transporte com “condução autônoma”.

3.8 Educação

Com o aprofundamento contínuo da informatização na educação, esse setor concentra-se na convergência, análise e compartilhamento de dados educacionais para alcançar os objetivos de aprendizagem personalizada, educação equitativa e gestão inteligente. Isso exige a interconexão e o compartilhamento de conexões de rede em escolas primárias e secundárias para alcançar a turma, a escola e a comunidade. No campo do ensino superior, observa-se um crescente compartilhamento de plataformas de pesquisa científica e inovação entre as universidades, demandando comunicação inter-regional e níveis de segurança mais elevados. A rede original não consegue atender aos requisitos de conexão rápida, segurança, isolamento e largura de banda.

O SRv6 com IPv6 Enhanced possibilita o provisionamento rápido de serviços sem a necessidade de atualização em toda a rede. Em cenários de educação de modo geral, os dispositivos em nuvem podem provisionar serviços rapidamente para escolas na região. O IPv6 Enhanced utiliza a tecnologia de fatiamento de rede para evitar interferências mútuas entre as redes e isolar os serviços. Além disso, ele oferece flexibilidade, largura de banda ajustável, troca e liberação sob demanda, melhorando significativamente a utilização de recursos. Salas de aula on-line para educação geral fornecem experiência de rede dedicada. A utilização da largura de banda da rede aumenta durante aulas online e videoconferências e os serviços escolares são migrados para a nuvem. Portanto, a experiência desses sistemas deve ser garantida. O IPv6 Enhanced usa a tecnologia SDN para tornar a rede gerenciável, visível e controlável, além de demarcar e localizar falhas automaticamente.

3.9 Agricultura

A tendência de desenvolvimento da agricultura moderna irá possibilitar que mais agricultores tenham acesso à Internet. A promoção e gestão da rede rural baseada em IPv6 irá otimizar e atualizar a estrutura agrícola-industrial. A tecnologia agrícola e a inovação no planejamento terão um impacto profundo no mercado rural, na eficiência da produção agrícola e no valor da utilização dos recursos. A tecnologia IPv6/IPv6 Enhanced pode auxiliar os agricultores a conectarem-se rapidamente ao sistema em nuvem e fornece suporte técnico pragmático para todo o gerenciamento de processos das principais culturas, pecuária e aves, além da piscicultura. Deve-se promover eficazmente a popularização e a aplicação de conhecimentos técnicos avançados na produção agrícola e na gestão científica.

Com base em IPv6/IPE, é proposta uma IoT agrícola eficiente e inteligente. Vários pontos de monitoramento com sensores distribuídos remotamente pela região coletam dados on-line sobre a umidade do solo, nutrientes e condições meteorológicas. Múltiplas tecnologias de IoT são usadas para acessar a rede e promover uma IoT eficiente. Ao mesmo tempo, combinando-se com as características fisiológicas do crescimento das culturas plantadas, realiza-se a previsão das condições do solo e a tomada inteligente de decisões quanto ao momento e à quantidade de irrigação. O gerenciamento inteligente também pode realizar funções como controle remoto automático de equipamentos de irrigação, fertilização precisa, irrigação racional, economia de água, taxa eficiente de uso de água e fertilizantes, além de minimizar a poluição ambiental. Através da Internet das Coisas agrícola, são concretizadas funções de percepção e controle inteligente, possibilitando a informatização, automação e inteligência dos processos de produção. Esse avanço culmina na realização de uma IoT agrícola eficiente e inteligente.

CAPÍTULO 4 - ÍNDICE DE DESENVOLVIMENTO DO IPv6

A implantação do IPv6 e de suas inovações está acontecendo de forma gradual no mundo todo. É importante salientar que ela precisa ocorrer em toda a cadeia de valor da Internet, incluindo usuários, dispositivos, provedores de acesso, provedores de conteúdo e de serviços. Nesse sentido, cada país tem avançado em seu próprio ritmo, refletindo em diferentes estágios e a visão clara do cenário de desenvolvimento do IPv6 é essencial para o direcionamento de esforços estratégicos para promover seu crescimento em cada lugar.

4.1 Panorama de metodologias para construção do índice do IPv6

Atualmente, existem muitas ferramentas para medir o desenvolvimento do IPv6, criadas por diversas organizações com diferentes metodologias, de acordo com suas respectivas finalidades. Elas podem ser diferenciadas, por exemplo, com base no escopo territorial (mundial, nacional etc.), na forma de reportar os resultados (websites ou publicações), na frequência de atualização, nos conjuntos de dados e KPIs, nas fontes de dados (terceiros ou coleta própria) e na inclusão ou não de parâmetros relacionados às inovações tecnológicas do IPv6 Enhanced. A seguir, serão detalhadas duas iniciativas para medir o desenvolvimento do IPv6, os relatórios da ARCEP (França) e da Roland Berger. Ambos são publicados anualmente e possuem diferentes abordagens.

4.1.1 Barômetro IPv6 (ARCEP)

A ARCEP desenvolveu um barômetro que mostra como cada participante da cadeia de valor da Internet na França está se saindo na transição para o IPv6 [48]. Assim, seu estudo provê uma visão mais detalhada dos cenários das operadoras de rede fixa e móvel, dos serviços de hospedagem, dos provedores de conteúdo e das infraestruturas de DNS. Ele é publicado anualmente e usa dados coletados pela própria ARCEP e por fontes terceiras, como APNIC, Cisco, Google e Facebook, entre outras.

Nas análises das operadoras de rede fixa, algumas condições são observadas para se considerar que a rede pode operar tráfego IPv6: a rede deve ser compatível com IPv6, os CPEs (*Client Premises Equipment*) devem ser compatíveis com o IPv6, tanto hardware quanto firmware, a operadora precisa configurar o IPv6 remotamente no CPE e os sistemas operacionais dos dispositivos devem ter suporte e estar habilitados ao IPv6.

Da mesma forma, para as operadoras de rede móvel, têm-se as seguintes condições para se considerar que a rede pode transmitir e receber tráfego IPv6: a rede deve ser compatível com IPv6 (*Access Point Name* deve ser capaz de suportar o IPv6), a operadora precisa configurar o IPv6 remotamente no dispositivo do usuário e os sistemas operacionais dos dispositivos devem ser compatíveis e habilitados ao IPv6.

O estudo classifica os usuários das operadoras como “IPv6-ready” ou “IPv6-enabled”. O primeiro significa que eles podem ativar o IPv6 em seus equipamentos. O segundo denota que o dispositivo do usuário já envia e recebe tráfego IPv6.

O relatório então compara a quantidade de usuários “IPv6-enabled” de cada operadora e traz dados sobre a evolução de cada uma nesse aspecto ao longo do tempo. Além disso, ele detalha as estatísticas por tipo de usuário (xDSL, cabo, FTTH e 4G) na rede fixa e apresenta as políticas de ativação do IPv6 nos dispositivos na rede móvel de cada operadora. Ele ainda informa sobre as práticas de compartilhamento de IPv4 e apresenta especificamente o cenário de usuários corporativos de cada operadora.

Nas análises dos serviços de hospedagem, dos provedores de conteúdo e das infraestruturas de DNS, são avaliadas algumas condições para se considerar um serviço “IPv6-enabled”: a rede deve ser compatível com o IPv6, o sistema operacional do servidor deve suportar e estar habilitado ao IPv6, o serviço de hospedagem deve pré-configurar o servidor para utilizar o IPv6, o servidor de aplicação deve ser capaz de gerenciar o IPv6 e o provedor de conteúdo deve configurar o DNS com um registro IPv6.

O relatório apresenta então dados sobre o IPv6 em serviços de hospedagem web e de e-mail e na infraestrutura de DNS. Além disso, ele também traz estatísticas sobre a adoção do IPv6 em websites e serviços online governamentais. Por fim, o estudo apresenta a taxa de adoção do IPv6 na França e a compara com outros países, além de fazer também uma comparação entre as regiões do globo.

4.1.2 Índice de desenvolvimento IPv6 (Roland Berger)

O estudo conduzido pela Roland Berger mede o índice de desenvolvimento do IPv6 em 92 países [49]. Além disso, ele faz uma análise quantitativa do impacto econômico das inovações tecnológicas do IPv6 Enhanced, apresenta informações mais aprofundadas sobre o cenário do protocolo em alguns países e traz recomendações de políticas para os diferentes grupos do estudo. Ele é baseado nas metodologias do LACNIC, da OCDE e da Cisco.

O índice de desenvolvimento do IPv6 utiliza subindicadores agrupados em três categorias para avaliação. O resultado é calculado através da soma ponderada dos subindicadores e posterior normalização dos resultados, resultando em um índice que varia de 0 a 1. Conforme suas pontuações, os países são listados em ordem decrescente e agrupados em três conjuntos: *front-runners, adopters* e *starters*. A seguir estão os indicadores que compõem o índice.

- **Inserção IPv6:** Planejamento de endereços; Implementação na rede; Implementação nos provedores de conteúdo; Implementação nos usuários.
- **Desempenho IPv6.**
- **Inovação IPv6:** Desenvolvimento de padrões; Políticas de suporte; Contribuição acadêmica; Aplicações.

CAPÍTULO 5 - IMPLANTAÇÃO DO IPv6 NO BRASIL

A implantação do protocolo IPv6 começou a ganhar força a nível mundial a partir de 2011, quando a IANA distribuiu os últimos blocos de endereços IPv4. Na região do LACNIC, onde se encontra o Brasil, o estoque de endereços IPv4 acabou em agosto de 2020 [50]. Atualmente, de acordo com o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), estima-se que a fila de espera para novas solicitações de blocos IPv4 chegue a seis anos [51]. Portanto, reitera-se que optar pelo IPv4 não é mais o caminho para novos sistemas autônomos ou para os que desejam expandir sua estrutura e necessitam de novos endereços públicos. O IPv6 é o padrão atual da Internet e sua adoção deve ocorrer em todo o ecossistema da rede, incluindo provedores de acesso e trânsito, provedores de conteúdo e serviços e dispositivos finais.

5.1 Status de desenvolvimento e análise do IPv6

Uma das formas de medir o IPv6 na Internet é pelo medidor do APNIC que realiza testes com rede de anúncio para identificar usuários capazes de se comunicar em IPv6 na rede [52]. No Brasil, a estimativa mostra que o uso do protocolo começou a crescer a partir de 2015, o que coincide com as metas estabelecidas no GT-IPv6, grupo que foi coordenado pela Anatel e contou com a participação do NIC.br e das grandes prestadoras de telecomunicações. Hoje, essa taxa está em torno de 48%, como mostra a Figura 8.

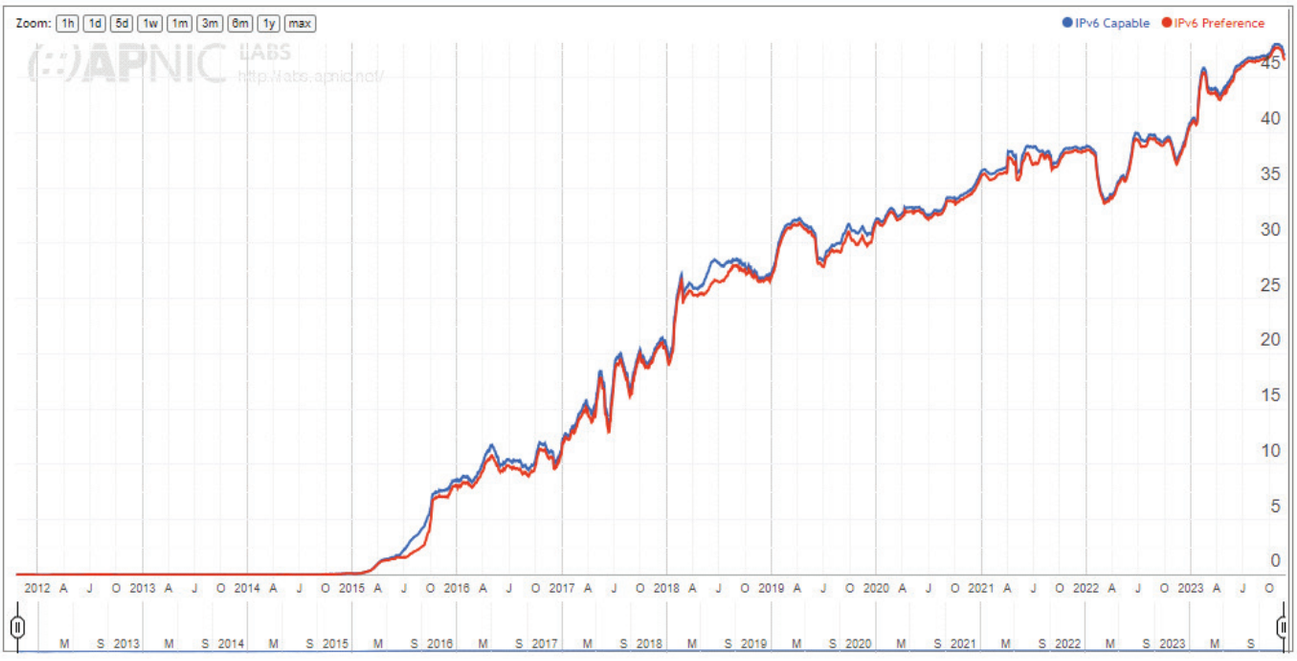

Figura 8 – Usuários habilitados ao IPv6 no Brasil

A ferramenta também consegue mostrar o resultado medido por sistema autônomo que é visível na Internet. De forma geral, aqueles em que há uma maior capacidade de acesso IPv6 somam uma pequena parcela enquanto na grande maioria essa taxa ainda é muito baixa, como detalhado na Tabela 1.

Usuários IPv6	Quant. de AS	% AS
Acima de 90 %	11	0,13%
Entre 70% e 90 %	254	3,11%
Entre 50% e 70 %	631	7,72%
Entre 30% e 50 %	834	10,21%
Entre 10% e 30%	1329	16,26%
Abaixo de 10%	5114	62,57%

Tabela 1 - Usuários habilitados ao IPv6 nos sistemas autônomos visíveis do Brasil

Como resultados dos trabalhos do GT-IPv6 [53], as maiores operadoras de telecomunicações do Brasil já disponibilizam o IPv6 a seus usuários, tanto finais (B2C) quanto na forma de trânsito (B2B), mas o acesso à rede com o protocolo também depende da compatibilidade dos dispositivos finais. Já a compatibilidade dos CPEs foi tratada no GT-IPv6, que definiu requisitos de certificação

para garantir que todos os novos dispositivos certificados tivessem suporte ao Dual Stack.
Em 2023, a Anatel apurou dados referentes a usuários com IPv6 ativo e ao volume de dados do novo protocolo nas redes de algumas operadoras do país. O resultado é apresentado na Tabela 2. As operadoras também reportaram que os principais provedores de conteúdo que utilizam suas redes já funcionam em Dual Stack, ou seja, operam tanto em IPv4 quanto em IPv6.

Operadora	Banda Larga Fixa		Banda Larga Móvel	
	Usuários Dual Stack	Volume de dados IPv6	Usuários Dual Stack	Volume de dados IPv6
Claro	92%	31%	78%	54%
OI	100%	30%	-	-
TIM	N/A	1%	90,6%	66,4%
VIVO	100%	40%	62%	89%
SERCOMTEL	-	11%	-	-
LIGGA	100%	27%	-	-
Horizons	69%	10%	-	-
Nova Fibra	3%	3%	-	-

Tabela 2 - Estatísticas do IPv6 nas redes de banda larga fixa e móvel do Brasil

O volume de dados IPv6 do serviço de banda larga fixa é limitado em grande parte pela baixa adesão ao novo protocolo por parte dos dispositivos finais dos usuários, principalmente daqueles que consomem tráfego de vídeo, como as smart TVs. Sobre os terminais móveis, percebe-se uma grande adoção do IPv6, uma vez que todos os novos terminais móveis são compatíveis com o novo protocolo e os aparelhos são trocados com mais frequência pelos usuários.

Com relação aos provedores de conteúdo, um estudo realizado pelo NIC.br em 2022 mostrou que 24% dos 9.793 domínios avaliados possuíam o IPv6 habilitado e, dentre os serviços de e-mail, esse percentual era de 22% [54] . Em geral, os grandes provedores já fornecem acesso IPv6 em seus conteúdos, mas há uma baixa adesão ao novo protocolo entre os pequenos. Isso é preocupante, especialmente quando se trata de serviços críticos para a sociedade, como internet banking, serviços governamentais (incluindo segurança pública) e serviços de educação e saúde.

5.2 Política atual para IPv6 no Brasil

No Brasil, algumas políticas foram definidas após os esforços do GT-IPv6, um Grupo de Trabalho para Implantação do Protocolo IPv6 nas redes das prestadoras de telecomunicações, criado em 2014 pela Anatel através da Portaria n.º 152. O grupo, coordenado pela Anatel, teve a participação das principais prestadoras de telecomunicações do Brasil e do NIC.br para discutir as atividades relacionadas à adoção do novo protocolo nas redes brasileiras e da solução temporária para o período de transição entre IPv4 e IPv6. Após os trabalhos, foram tomadas algumas decisões:

Solução de transição – CGNAT-44

• **Disponibilização do CGNAT-44:** prestadoras cujos recursos IPv4 tiverem se esgotado devem implementar o CGNAT-44 como solução paliativa;
• **Incompatibilidades com IPv4 compartilhado:** clientes que não queiram ou não possam trabalhar com IPv4 compartilhado, caso haja disponibilidade, podem receber um IP público dinâmico não oneroso ou um IP fixo de forma onerosa;
• **Quebra de sigilo de dados telemáticos com CGNAT-44:** as prestadoras devem fornecer identificação unívoca de usuário. Para isso, devem ser capazes de informar a porta de origem das conexões, além do endereço IPv4 de origem e do período de tempo do acesso (junto ao fuso horário aplicável).

Disponibilização do IPv6

• **Peering/Trânsito:** as prestadoras devem ofertar Peering/Trânsito em IPv6 nos seus principais pontos de troca de tráfego de interligação e interconexão;
• **Usuário final:** as prestadoras devem ofertar endereços IPv6 públicos a novos usuários e a usuários legados que solicitarem e, nas localidades onde não houver oferta de IPv6, deve ser alocado ao usuário, de forma dinâmica ou fixa, um endereço IPv4 público não compartilhado.

Na época, o grupo também trabalhou na definição de requisitos técnicos para avaliação da conformidade do protocolo IPv6 em produtos para telecomunicações. Recentemente, a Anatel atualizou esses requisitos através do Ato nº 7971, de 22 de junho de 2023. Eles passaram a se basear nas seguintes referências normativas:

• **Terminais fixos (xDSL, xPON e DOCSIS):** RFC 7084, IPv6 READY CE, IPv6 READY Core
• **Terminais móveis (3GPP):** RFC 8200, ETSI TS 102 514, 3GPP TS 36.523-1

5.3 Desafios de desenvolvimento do IPv6 no Brasil

O avanço na adoção do IPv6 é fundamental para que se mantenha o progresso das telecomunicações no Brasil. Até o momento, percebe-se um esforço por parte das grandes operadoras, que já disponibilizam o IPv6 a seus usuários. Além disso, os requisitos técnicos para avaliação da conformidade do protocolo IPv6 em produtos de telecomunicações, que abrangem equipamentos terminais de acesso fixo e móvel, foram recentemente atualizados pela Anatel. No entanto, há muito o que se avançar com relação aos pequenos provedores de acesso, provedores de conteúdo e dispositivos finais legados de usuários. As empresas terão que se empenhar mais na adoção do protocolo e o governo deve exercer ações para conduzir e incentivar esse processo.

Os pequenos provedores de acesso devem priorizar a implementação do IPv6 e sua disponibilização aos usuários. Muitos ainda insistem no IPv4 principalmente devido ao uso de CGNAT-44 para compartilhamento de endereços, embora este recurso conduza a uma piora na experiência do usuário à medida que a rede cresce. O governo pode incentivar e cobrar esforços para a adoção do IPv6 e desestimular o uso do CGNAT-44. O uso de CGNAT-44 também deve ser desencorajado por conta das questões de segurança que ele traz consigo, ao dificultar o rastreamento de atividades maliciosas na rede e a identificação unívoca do usuário, podendo prejudicar a investigação de cibercrimes. Os crimes digitais são uma realidade que deve se intensificar e o uso de CGNAT-44 torna mais complexo o enfrentamento desse problema.

Os dispositivos finais que devem se diversificar cada vez mais com a IoT também precisam ser adequados ao IPv6. Não adianta o provedor de acesso fornecer IPv6 ao usuário se seus dispositivos não forem compatíveis com o protocolo. Por exemplo, é comum encontrar smart TVs sem suporte ao novo protocolo, sendo este um dispositivo com alto consumo de dados. O governo precisa avaliar estratégias para adequação do cenário de dispositivos, como a implementação de Dual Stack se houver viabilidade ou a adoção de técnicas de transição que permitam dispositivos IPv4 acessar conteúdos e serviços disponíveis somente na rede IPv6.

Os pequenos provedores de conteúdo precisam implementar o Dual Stack e tornar seus serviços acessíveis via IPv6. Isso é especialmente importante no caso de serviços críticos para a sociedade, como internet banking, serviços governamentais (incluindo segurança pública) e serviços de educação e saúde. Nesse caso, o governo também pode incentivar e cobrar esforços para a adoção do novo protocolo.

Por fim, é preciso investir em ferramentas que permitam o acompanhamento efetivo da adoção do IPv6 no país. Isso pode ser feito através de um barômetro que mensure dados de todo o ecossistema da rede, como provedores de acesso e trânsito, provedores de conteúdo e serviços e dispositivos finais. Isso é extremamente útil no direcionamento de esforços e avaliação de resultados para aceleração do processo de transição entre os protocolos IPv4 e IPv6.

5.4 Metas, ritmo e sugestões de desenvolvimento do IPv6 para o Brasil

Atualmente, o desenvolvimento do IPv6 no Brasil é caracterizado principalmente pela falta de conteúdo na Internet em sites e aplicativos que utilizam IPv6. Em vários setores, como operadoras, governos e instituições financeiras, a implantação do IPv6 ainda é baixa. Assim, o desempenho do acesso ao conteúdo IPv6 é significativamente inferior ao do IPv4. Ao mesmo tempo, de acordo com um relatório, o Brasil sofreu 7,5 bilhões de ataques de segurança cibernética em 2022 [55], sendo o país mais atacado da América Latina. Os setores financeiro, de saúde, varejo e governamental são os mais vulneráveis a ataques. Os recursos de segurança de rede não possuem a capacidade de construir um sistema de segurança sistemático e detectar ameaças. Como resultado, operadoras e empresas não contam com recursos de segurança e a proteção dos

dados essenciais é insuficiente, deixando as operadoras e empresas mais vulneráveis a ataques de ransomware e DDoS. Do ponto de vista da soberania digital, da infraestrutura crítica da Internet e da segurança de rede, a ausência de um sistema independente e controlável de servidores-raiz resulta na incapacidade de se defender contra ataques de DDoS em larga escala. Atualmente, a tecnologia Anycast é usada para implantar imagens em servidores-raiz, podendo facilmente resultar em ataques às imagens de servidores locais, sem um mecanismo de emergência. Para garantir a segurança da soberania digital, as vantagens do IPv6/IPv6 Enhanced podem ser exploradas para garantir a confiabilidade, a autenticidade e a rastreabilidade dos endereços e fornecer uma infraestrutura segura de rede em nuvem.

5.4.1 Metas e ritmos de desenvolvimento do IPv6

Para impulsionar o desenvolvimento do IPv6/IPv6 Enhanced no Brasil, são sugeridas metas de curto (2024 e 2025), médio (2026 a 2027) e longo prazos (2028 a 2030). Dessa forma, pode-se fortalecer a gestão dos principais indicadores e recursos do IPv6, desenvolver gradualmente o protocolo e aprimorar os recursos digitais nacionais e a segurança cibernética. Essa proposta é apresentada na Tabela 3.

Indicador	Descrição	Curto Prazo	Médio Prazo	Longo Prazo
Percentual de usuários IPv6	Percentual de usuários finais que acessam a internet através de IPv6, incluindo banda larga fixa e móvel	50%	60%	70%
Taxa de suporte ao IPv6 em sites governamentais	Número de sites governamentais que suportam IPv6	20%	30%	50%
Taxa de suporte ao IPv6 dos principais sites comerciais e apps de internet móvel	Número de sites e aplicativos que suportam o acesso ao IPv6 dentre os 500 principais	35%	40%	45%
Taxa de suporte ao IPv6 de CPEs coorporativos	Dispositivos de acesso CPE corporativos que suportam IPv6	30%	50%	70%
Taxa de ativação de IPv6 em dispositivos de rede da operadora	Percentual dos recursos de IPv6 ativados em dispositivos de rede da operadora, incluindo os protocolos IPv6, SRv6, fatiamento e IFIT	20%	30%	40%
Percentual de tecnologias IPv6 Enhanced usadas em redes privadas	Percentual de tecnologias em IPv6 Enhanced (SRv6 ou fatiamento de rede) usados por rede dedicada	5%	10%	15%

Tabela 3 - Sugestões de metas para o desenvolvimento do IPv6 no Brasil

As metas propostas para o percentual de usuários IPv6 baseiam-se em uma previsão conservadora de aumento de 5% a cada ano, conforme observado no Brasil nos últimos 10 anos.

Planejamento de curto prazo (2024 a 2025)

• **Acelerar a promoção e a implantação de conteúdo IPv6:** promover a implementação do IPv6 em plataformas de serviços governamentais e sites do governo, além de impulsionar a atualização para o IPv6 nos principais aplicativos comerciais e sites do setor.

• **Promover a implantação do IPv6 nos dispositivos:** acelerar a habilitação do IPv6 para terminais domésticos de banda larga, fortalecer a implantação e a aplicação do IPv6 em terminais de IoT e atualizar os CPEs corporativos para IPv6.

• **Acelerar a implantação e a inovação do IPv6/IPv6 Enhanced para operadoras e setores:** acelerar a adoção, por parte das operadoras, dos recursos e funcionalidades do IPv6 Enhanced, visando a melhoria do desempenho do IPv6 de ponta a ponta. Otimizar a eficiência de linhas

privadas, banda larga doméstica e serviços 5G usando SRv6, fatiamento, IFIT e monitoramento aprimorado, e aprimorar os recursos IPv6 para redes privadas da indústria.

• **Promover a criação do sistema de segurança para operadoras e empresas:** fortalecer o sistema de proteção em toda a rede com base no reconhecimento situacional de segurança, detectar prontamente ameaças desconhecidas, prever e alertar sobre a tendência de desenvolvimento de ameaças à segurança da rede e alterações no tráfego, além de aprimorar a capacidade de lidar com ameaças avançadas. Criar um sistema de garantia colaborativa que integre redes de infraestrutura IPv6, datacenters, plataformas de nuvem e aplicações.

Planejamento de médio prazo (2026 a 2027)

• **Acelerar a implantação do IPv6 em todos os setores:** promover a ampla aplicação de IPv6/IPv6 Enhanced nos setores governamentais, de finanças, de energia, de transporte, de educação e de manufatura por meio de especificações de construção de rede IPv6, orientação de implantação e treinamento de pessoal, além de definir padrões de referência do setor.

• **Melhorar a inovação da tecnologia de IPv6 Enhanced em larga escala das operadoras:** acelerar a aplicação em larga escala de novos recursos, como SRv6, fatiamento, IFIT e evoluir no longo prazo.

• **Promover a construção de imagens de servidores raiz IPv6 no Brasil:** construir servidores de imagens DNS IPv6 para aumentar o controle da soberania digital nacional e aprimorar a capacidade de garantia de segurança da infraestrutura crítica da Internet.

Planejamento de longo prazo (2028 a 2030)

• **Melhorar significativamente a capacidade de acesso do usuário ao IPv6:** nas operadoras e empresas, a implantação do IPv6 aumentou em mais de 50%, melhorando significativamente o desempenho do IPv6 e superando a capacidade de acesso ao IPv4.

• **Melhorar os recursos de segurança das operadoras e dos setores:** implementar monitoramento de segurança para todo o tráfego na rede ativa para detectar e defender-se rapidamente contra vários ataques.

5.4.2 Principais recomendações de desenvolvimento

1. Construindo uma plataforma de monitoramento de IPv6

Estabelecer uma plataforma nacional de monitoramento do desenvolvimento do IPv6, publicar regularmente relatórios de evolução do IPv6 com base em vários indicadores da plataforma, identificar pontos fracos no desenvolvimento do IPv6 e fornecer sugestões sobre melhorias e estratégias para promover operadoras e empresas, acelerando assim a implantação do IPv6 e do IPv6 Enhanced.

2. Práticas de inovação das operadoras relacionadas ao IPv6 Enhanced

Incentivar as operadoras a acelerar a inovação e a aplicação dos novos recursos do IPv6 Enhanced, aplicando novas tecnologias às redes. Isso visa atender aos requisitos de conectividade em cenários de sinergia de redes 5G e nuvem, tais como rede flexível, provisão rápida de serviços, operação e manutenção simplificadas, experiência de usuário otimizada, serviços sob demanda e garantia diferenciada.

Com base em suas próprias características e requisitos, cada setor impõe requisitos diferentes às redes, como segurança e confidencialidade, isolamento rígido de dados, altíssima largura de banda, baixíssima latência, fatiamento massivo e latência determinística. As redes tradicionais de setores privados terão dificuldade em atender a esses novos e diversificados requisitos. As operadoras são incentivadas a construir redes privadas em IPv6 com funções poderosas.

3. Inovação, especificações e orientações sobre o IPv6 dos setores

Promover a atualização da rede IPv6 em diversos setores: governo, finanças, energia, educação, transporte e saúde. A rede privada IPv6 usa tecnologias-chave como SRv6, fatiamento e detecção de fluxo para fornecer provisionamento rápido, alta qualidade, baixo custo, segurança e redes fáceis de manter para os setores de governo inteligente, telemedicina, educação on-line, cidade inteligente e títulos financeiros. Redes privadas IPv6 usam SRv6 para fornecer recursos de provisionamento rápido. O fatiamento de rede fornece múltiplos planos em uma rede para atender a diferentes setores e serviços, implementando isolamento seguro e de baixo custo, além de recursos de garantia de serviços diferenciados de alta qualidade. A detecção baseada em tráfego e a operação e manutenção inteligentes oferecem detecção e localização inteligentes de falhas, além de recursos operacionais de baixo custo.

4. Construindo uma arquitetura segura

Deve-se reforçar, de maneira abrangente, a segurança cibernética, promovendo a atualização dos recursos das operadoras e empresas em setores-chave, impulsionando o desenvolvimento conjunto de segurança cibernética e informatização e aprimorando o sistema de gestão e garantia técnica da segurança cibernética. Além disso, reforçar a avaliação de riscos de segurança cibernética e as simulações de emergência, aprimorar a prevenção de ameaças e as capacidades de resposta a emergências, e melhorar continuamente a maturidade do sistema de proteção de segurança.

Promover a implementação de segurança cibernética para infraestrutura em setores estratégicos, como governo, finanças, energia, transporte, saúde e educação. Fortalecer o desenvolvimento de múltiplas soluções de segurança para ativos, dispositivos, identidades, dados e aplicativos, e aperfeiçoar os recursos de proteção de segurança. Estabelecer mecanismos de segurança e sistemas de proteção aprofundados, tais como consciência situacional, notificação e alerta, resposta a emergências e operação segura, e aperfeiçoar continuamente as capacidades de prevenção de riscos e resposta a incidentes.

CAPÍTULO 6 - CASOS DE USO DO IPv6 E DO IPv6 ENHANCED

6.1 Operadora

Atualmente, algumas operadoras no Brasil já começaram a testar laboratórios e redes ativas com IPv6 Enhanced. Os serviços tradicionais de linha privada MPLS precisam ser configurados manualmente, salto por salto, e o provisionamento leva muito tempo. Especialmente, o provisionamento de serviços entre domínios exige interconexão manual de diferentes segmentos, levando até semanas. Normalmente, não há métodos para visualizar falhas, o que demanda um longo tempo para detecção. Algumas operadoras têm planejado implantar recursos de SRv6 e de IFIT com IPv6 Enhanced para atualizar os recursos de linha privada, acelerar a implantação de linha privada IPv6, fornecer rapidamente recursos de linha privada para clientes do setor e auxiliar as operadoras a aumentar a receita para serviços B2B.

A rede de suporte 5G de uma operadora sul-africana está congestionada devido ao aumento do tráfego, e a taxa de perda de pacotes continua alta. À medida que a taxa de perda de pacotes aumenta, a qualidade do vídeo dos usuários móveis se deteriora e o congelamento de quadros ocorre com frequência. A experiência de usuário se deteriora e a supressão do tráfego atinge o nível de terabytes todos os dias. A receita das operadoras é afetada. A qualidade da rede tradicional não é claramente perceptível e a otimização manual é complexa. As rotas precisam ser restauradas manualmente, salto a salto, e recalculadas. A otimização leva dias e a qualidade da otimização não pode ser garantida. A experiência de usuário não pode ser restaurada em tempo hábil, resultando em muitas reclamações. Após a implantação de um novo sistema de gerenciamento de rede que utiliza SRv6 e a telemetria com IFIT, a taxa de perda de pacotes no link é detectada em segundos. Quando há aumento da perda de pacotes, a otimização automática é acionada. A computação inteligente do percurso, baseado em atraso e largura de banda, reduz significativamente a perda de pacotes em toda a rede. Este recurso libera a supressão de tráfego, aprimora a experiência do usuário e auxilia as operadoras a aumentar o DOU em mais de 20%.

6.2 Governo digital

Uma província na África do Sul iniciou a construção de um governo digital. O governo digital disponibiliza infraestrutura de rede para órgãos governamentais, incluindo escolas, hospitais, escritórios do governo e zonas de desenvolvimento econômico. Ele constrói e habilita plataformas de serviços e oferece diversos serviços de suporte em TIC. O objetivo do governo digital é fornecer serviços de conectividade para pequenas e médias empresas e reduzir os custos empresariais, oferecer vários serviços digitais governamentais aos cidadãos e estabelecer uma plataforma de big data para apoiar a governança urbana e prover conexões de banda larga e filiais para 200 hospitais e 2.000 escolas públicas, visando apoiar o alcance das metas de saúde e educação digitais.

A infraestrutura de rede tradicional está desatualizada e defasada, resultando em desenvolvimento econômico insuficiente. Os serviços tradicionais de governo, educação e saúde coexistem em diversas redes, tornando o compartilhamento de informações difícil e a eficiência baixa. Além disso, com o desenvolvimento dos serviços digitais, há uma grande demanda por conexões,

e a largura de banda na rede ativa é insuficiente. Portanto, uma grande rede de banda larga é urgentemente necessária. Os links de rede ativos são alugados, resultando em deficiências de segurança e confiabilidade, bem como riscos de dados. A capacidade geral de operação e manutenção é fraca, mas os requisitos de suporte continuam a crescer rapidamente.

Uma rede governamental de banda ultralarga é construída com base em recursos de IPv6 Enhanced. A rede governamental de banda ultralarga permite o acesso à rede e a troca de informações entre governos e instituições públicas, como o Ministério da Educação e o Ministério do Interior. A eficiência no atendimento do governo aos cidadãos foi melhorada em 20% e a taxa de processamento da rede governamental atingiu 15%. Além disso, agências governamentais, 200 instituições médicas e 2.300 instituições educacionais estão interligadas por meio da rede IPv6, reduzindo o TCO em 30% e impulsionando a educação e os cuidados de saúde digitais. O isolamento de dados e o balanceamento de carga de serviços baseados em fatiamento melhoram a confiabilidade da rede e a utilização do link. A tecnologia de isolamento na rede portadora garante 100% de segurança dos dados do serviço. E o mecanismo diferenciado de garantia de SLA, baseado no IPv6 Enhanced, atende aos requisitos de QoS de diversos serviços, como telefones IP, vigilância por vídeo e serviços de dados. Ao mesmo tempo, os avanços na rede e em sua operação geram mais oportunidades de emprego de maior qualificação na área de TIC.

6.3 Energia

Uma grande empresa de energia no Brasil, dedicada à exploração, refino, derivados, armazenamento, transporte, vendas, importação e exportação, necessita de plataformas amplas de TIC para suportar suas operações. Os cenários envolvem atividades no campus empresarial, monitoramento de oleodutos e gasodutos, vigilância de áreas de alto risco, interconexão de filiais de postos de gasolina e armazenamento de dados nos escritórios de produção de petróleo.

O estágio das redes de backbone limita significativamente a digitalização empresarial. A rede de backbone possibilita a interconexão entre os centros de dados empresariais, o acesso à Internet e a conexão entre os campi empresariais e as filiais de oleodutos na rede de produção. Atualmente, a infraestrutura da rede de backbone está desatualizada, e a largura de banda dos links é limitada, o que não satisfaz as exigências de desenvolvimento de serviços. Além disso, a capacidade de operação e manutenção é baixa. O SNMP é usado para gerenciamento simples e operação e manutenção manuais. Mais de 10 falhas ocorrem a cada semana, sendo necessário mais de quatro horas para identificar cada uma.

Com base em novos recursos, como IPv6/IPv6 Enhanced, SRv6 e operação e manutenção inteligentes, a empresa de energia planeja construir uma rede que pode ser orientada para os próximos 5 a 10 anos. Links de alta capacidade são usados para interconectar data centers para suportar serviços massivos. Além disso, a solução de SRv6 com IPv6 Enhanced é utilizada para implementar o acesso E2E IPv6 aos data centers, simplificando a implantação e a operação e manutenção. Utilizando IFIT baseado em IPv6, um sistema de gerenciamento e controle é implementado com visualização multidimensional, gestão entre domínios e capacidade de localização de falhas em minutos.

6.4 Educação

Uma rede educacional privada com IPv6 está sendo construída em Xangai, China. As redes educacionais tradicionais estão sendo construídas com foco na otimização estrutural, eficiência intensiva, segurança e confiabilidade. Com base nas instalações de rede maduras e nos recursos profissionais de operação e manutenção das operadoras de telecomunicações e ISPs, aproveita-

se ao máximo as vantagens da construção e manutenção unificadas para otimizar os custos de construção da rede e a eficiência de operação e manutenção. Conforme os requisitos do Departamento de Educação, focaliza-se no compartilhamento de dados e na interligação de recursos, coordenando conjuntos intensivos de recursos em nuvem e serviços de informatização geral da rede privada de educação para construir uma rede privada de educação baseada em IPv6 Enhanced.

A rede privada de educação suporta o tráfego da Internet e dos serviços de educação. Para garantir a qualidade dos serviços educacionais, os serviços relacionados à educação, como testes e gestão financeira, são realizados em fatias de rede separadas, e estão verdadeiramente isolados dos serviços de Internet em termos de largura de banda. Dessa forma, vários serviços são realizados em uma rede. Para resolver os problemas de implantação de serviços de fatiamento complexos e demorados, a plataforma de gerenciamento de operação de integração de rede em nuvem pode ser construída para calcular de forma inteligente e implantar rotas com base nos requisitos de largura de banda do serviço a qualquer momento.

O protocolo SRv6 com IPv6 Enhanced é implantado na rede privada de educação E2E para os serviços IPv4 e IPv6. O SRv6 simplifica significativamente o número de protocolos de rede. Juntamente com a nuvem inteligente habilitada para SRv6 implantada em mais de 800 escolas e instituições educacionais, o SRv6 estabelece a base para uma transferência do SRv6 de ponta a ponta para a nuvem na rede. Com base na plataforma de gerenciamento de operações de integração entre nuvem e rede, o controlador de rede e a plataforma híbrida de gerenciamento de nuvem são otimizados para proporcionar o rápido provisionamento, em minutos, de serviços em nuvem para a educação.

A rede inteligente sempre foi o objetivo na construção de redes privadas de educação. Requer que o sistema implemente um gerenciamento preditivo ou proativo em ciclo fechado, guiado pela experiência do cliente em um ambiente complexo de múltiplas redes. A plataforma de gerenciamento de operações de integração entre nuvem e rede incorpora a função de monitoramento de rede e realiza um gerenciamento visualizado por meio da detecção de fluxo para acompanhar em tempo real o status de integridade da rede e a qualidade do serviço. Além disso, os caminhos de serviço podem ser otimizados automaticamente. A rede privada de educação como um todo possui o recurso de auto inteligência de serviço de ponta a ponta.

Com base nos recursos IPv6 e IPv6 Enhanced, a largura de banda geral da rede é aumentada em mais de 10 vezes, atendendo de forma mais eficaz aos requisitos de suporte de largura de banda da base digital de educação. A rede privada de educação utiliza tecnologias avançadas, como fatiamento, SRv6 e mapa digital. Destaca-se pelo provisionamento simples, operação e manutenção fáceis, alta qualidade e elevada segurança, incorporando plenamente as vantagens das redes privadas industriais.

[1] “Digital 2023: Global Overview Report”. DataReportal – Global Digital Insights. Jan. 2023. Disponível em: <https://datareportal.com/reports/digital-2023-global-overview-report>.
[2] “IoT Connected Devices Worldwide 2019-2030”. Statista. Jul. 2023. Disponível em: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide>.
[3] “A Brief History of the Internet”. Internet Society. 1997. Disponível em: <https://www.Internetsociety.org/Internet/history-Internet/brief-history-Internet>.
[4] Postel, J. “Internet Protocol”, RFC 791. IETF. Set. 1981.
[5] “IPv6 – Google”. Disponível em: <https://www.google.com/intl/pt-BR/ipv6/statistics.html>.
[6] “Number Resources”. IANA. Disponível em <https://www.iana.org/numbers>.
[7] Clark, D.; Chapin, L.; Cerf, V.; Braden, R.; Hobby, R. “Towards the Future Internet Architecture”, RFC 1287. IETF. Dez. 1991.
[8] Fuller, V.; Li T. “Classless Inter-domain Routing (CIDR)”, RFC 4632. IETF. Ago. 2006.
[9] Droms, R. “Dynamic Host Configuration Protocol”, RFC 2131. IETF. Mar. 1997.
[10] Egevang, K.; Srisuresh, P. “Traditional IP Network Address Translator (Traditional NAT)”, RFC 3022. IETF. Jan. 2001.
[11] Rekhter, Y.; Moskowitz, R.; Karrenberg, D.; Groot, G. “Address Allocation for Private Internets”, RFC 1918. IETF. Fev. 1996.
[12] Deering, S.; Hinden, B. “Internet Protocol, Version 6 (IPv6) Specification”, RFC 8200. IETF. Jul. 2017
[13] Narten, T.; Thomson S.; Jinmei, T. “IPv6 Stateless Address Autoconfiguration”, RFC 4862. IETF. Set. 2007.
[14] Seo, K.; Kent, S. “Security Architecture for the Internet Protocol”, RFC 4301. IETF. Dez. 2005.
[15] Amante, S.; Carpenter. B.; Jiang, S.; Rajahalme, J. “IPv6 Flow Label Specification”, RFC 6437. IETF, Nov. 2011.
[16] NIC.br, “Transição”. Abr. 2012. Disponível em: <https://ipv6.br/post/transicao>.
[17] “IPv4 Address Report”. Dez. 2023. Disponível em <https://ipv4.potaroo.net>.
[18] Jiang, S.; Carpenter, B. “An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition”, RFC 6264. IETF. Jun. 2011.
[19] Weil, J.; Kuarsingh, V.; Donley, C.; Liljenstolpe, C.; Azinger, M. “IANA-Reserved IPv4 Prefix for Shared Address Space”, RFC 6598. IETF. Abr. 2012.
[20] Liljenstolpe, C.; George, W.; Donley, C.; Howard, L. “IPv6 Support Required for All IP-Capable Nodes”, RFC 6540. IETF. Abr. 2012.
[21] “5G System Overview”. 3GPP. Ago. 2022. Disponível em: <https://www.3gpp.org/technologies/5g-system-overview>.
[22] “Overview of the Internet of things”. ITU-T. Jun. 2012.
[23] Simmon, E. “Evaluation of Cloud Computing Services Based on NIST SP 800-145”. NIST Special Publication 500-322. Feb. 2018.
[24] “IPv6 Enhanced Innovation (IPE); IPv6 based Data Centers, Network and Cloud Integration”. ETSI. Abr. 2022.
[25] “IPv6 Enhanced Innovation (IPE); Gap Analysis”. ETSI. Ago. 2021.
[26] “IPv6 Enhanced Innovation (IPE); 5G Transport over IPv6 and SRv6”. ETSI. Mai. 2022.
[27] Barr, J. “New – AWS Public IPv4 Address Charge + Public IP Insights”. AWS News blog. Jul. 2023. Disponível em: <https://aws.amazon.com/pt/blogs/aws/new-aws-public-ipv4-address-charge-public-ip-insights>.
[28] Donley, C.; Howard, L.; Kuarsingh, V.; Berg, J.; Doshi, J. “Assessing the Impact of Carrier-Grade NAT on Network Applications”, RFC 7021. IETF. Set. 2013.
[29] Ford, M.; Boucadair.; Durand, A.; Levis, P.; Roberts, P. “Issues with IP Address Sharing”, RFC 6269. IETF. Jun. 2011.
[30] Hain, L. “Architectural Implications of NAT”, RFC 2993. IETF. Nov. 2000.
[31] “IP Resource Distribution Reports”. Disponível em: <https://bgp.potaroo.net/iso3166/v4cc.html>.

[32] “IPv6 Enhanced Council”. Disponível em: <https://ipv6Enhanced.ipv6forum.com>.
[33] Filsfils, C.; Dukes, D.; Previdi, S.; Leddy, J.; Matsushima, S.; Voyer, D. “IPv6 Segment Routing Header (SRH)”, RFC 8754. IETF. Mar. 2020.
[34] Filsfils, Clarence, Leddy, J.; Matsushima, S.; Voyer, D.; Camarillo, P.; Li, Z. “Segment Routing over IPv6 (SRv6) Network Programming”, RFC 8986. IETF. Fev. 2021.
[35] Luo, L. “SRv6”, IP Network eBook series. Huawei. Ago. 2023.
[36] Rokui, R.; Homma, S.; Makhijani, K.; Contreras, L.; Tantsura, J. “A Framework for Network Slices in Networks Built from IETF Technologies”, Internet-Draft: draft-ietf-teas-ietf-network-slices-25. IETF. Set. 2023.
[37] Song, H.; Qin, F.; Chen, H.; Jin, J.; Shin, J. “Framework for In-situ Flow Information Telemetry”, Internet-Draft: draft-song-opsawg-ifit-framework-21. IETF. Out. 2023.
[38] Li, Z.; Peng, S.; Xie, C. “Application-aware IPv6 Networking (APN6) Encapsulation”, Internet-Draft: draft-li-apn-ipv6-encap-07. IETF. Jul. 2023.
[39] J. A. Loughney, “IPv6 Node Requirements,” RFC 4294, RFC Editor, Apr. 2006. DOI: 10.17487/RFC4294.
[40] E. Jankiewicz, T. Narten, and J. A. Loughney, “IPv6 Node Requirements,” RFC 6434, RFC Editor, Dec. 2011. DOI: 10.17487/RFC6434.
[41] T. Narten, R. P. Draves, and S. Krishnan, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” RFC 4941, RFC Editor, Sep. 2007. DOI: 10.17487/RFC4941.
[42] F. Gont, “A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC),” RFC 7217, RFC Editor, Apr. 2014. DOI: 10.17487/RFC7217.
[43] T. Aura, “Cryptographically Generated Addresses (CGA),” RFC 3972, RFC Editor, Mar. 2005. DOI: 10.17487/RFC3972.
[44] M. Heuse, “IPv6 Insecurity Revolutions,” presented at Hack in the Box, Oct. 8-11, 2012, Kuala Lumpur, Malaysia.
[45] F. Gont and M. Heuse, “Security Assessments of IPv6 Networks and Firewalls,” presented at IPv6 Congress 2013, June 6-7, Frankfurt, Germany.
[46] F. Najjar, Q. Bsoul, and H. Al-Refai, “An Analysis of Neighbor Discovery Protocol Attacks,” Computers, vol. 12, no. 6, p. 125, Jun. 2023, doi: 10.3390/computers12060125.
[47] P. Fojtu, “Vulnerabilities and Threats in IPv6 Environment,” Master’s thesis, Dept. of computer science na engineering, Univ. Of West Bohemia, Pilsen, Czech Republic, 2013.
[48] “Annual barometer of the transition to IPv6 in France”. Arcep. Nov. 2021. Disponível em: <https://en.arcep.fr/maps-data/our-facts-figures-publications/the-transition-to-ipv6/annual-barometer-of-the-transition-to-ipv6-in-france.html>.
[49] Li, B. “Global IPv6 Development Report 2022”. Roland Berger. Jan. 2023. Disponível em: <https://www.rolandberger.com/en/Insights/Publications/Global-IPv6-Development-Report-2022.html>.
[50] “Esgotamento do IPv4: O LACNIC designou o último bloco”. LACNIC. Ago 2020. Disponível em: <https://www.lacnic.net/4849/3/lacnic/esgotamento-do-ipv4:-o-lacnic-designou-o-ultimo-bloco>.
[51] “NIC.Br Reforça Necessidade de Adesão Ao IPv6”. TeleSíntese. Abr. 2023. Disponível em: < https://www.telesintese.com.br/fila-de-espera-por-ipv4-chega-a-6-anos-e-nic-br-reforca-necessidade-de-adesao-do-ipv6>.
[52] “IPv6 Capability Metrics”. APNIC. Disponível em: <https://stats.labs.apnic.net/ipv6/BR>.
[53] “GT-IPv6 - Relatório final de atividades”. Anatel. Dez. 2014. Disponível em: <https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/a11c833a13469d0d13a0aa2f489b5c0a>.
[54] “IPv6 Como está sua implantação?”. IX Forum 16. Out. 2023.
[55] “Brasil é o segundo país mais vulnerável a ataques cibernéticos, segundo relatório da Trend Micro”. ABES. Out. 2023. Disponível em: <https://abes.com.br/brasil-e-o-segundo-pais-mais-vulneravel-a-ataques-ciberneticos-segundo-relatorio-da-trend-micro>.

HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P. R. China
Tel: +86-755-28780808
www.huawei.com