UNIVERSIDADE FEDERAL DO MARANHÃO - UFMA
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA – CCET
COORDENAÇÃO DE CIÊNCIA DA COMPUTAÇÃO - COCOM

SALVIANO LIMA DA SILVA

INTEROPERABILIDADE ENTRE IPv4 E IPv6 :

UMA ANÁLISE DOS ASPECTOS DE SEGURANÇA DAS TÉCNICAS DE TRANSIÇÃO

SÃO LUÍS/MA

2016

SALVIANO LIMA DA SILVA

INTEROPERABILIDADE ENTRE IPv4 E IPv6 :

UMA ANÁLISE DOS ASPECTOS DE SEGURANÇA DAS TÉCNICAS DE TRANSIÇÃO

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Mário Antônio Meireles Teixeira

SÃO LUÍS/MA

2016

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

Silva, Salviano Lima da.
Interoperabilidade entre IPv4 e IPv6 : uma análise dos aspectos de segurança das técnicas de transição. - 2016.
74 f.

Orientador(a): Mário Antônio Meireles Teixeira.
Monografia (Graduação) - Curso de Ciência da Computação, Universidade Federal do Maranhão, São luís, 2016.

1. IPv6. 2. IPv4. 3. Segurança. 4. Transição. 5. Internet. I. Teixeira, Mário Antônio Meireles. II. Título.

SALVIANO LIMA DA SILVA

INTEROPERABILIDADE ENTRE IPv4 E IPv6 :

UMA ANÁLISE DOS ASPECTOS DE SEGURANÇA DAS TÉCNICAS DE TRANSIÇÃO

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Monografia aprovada em: 21 / 06 / 2016

Prof. Dr. Mário Antônio Meireles Teixeira
Orientador

Prof. Me. Carlos Eduardo Portela Serra de Castro
1° Examinador

Prof. Dr. Anselmo Cardoso de Paiva
2° Examinador

A minha mãe Rejane Lima Silva e ao meu pai Francisco das Chagas Silva (*in memorian*), pelo constante incentivo .

AGRADECIMENTOS

Agradeço a minha mãe Rejane Lima Silva e ao meu pai Francisco das Chagas Silva (in memorian) por todo o incentivo e apoio necessário para que meus estudos e esse trabalho fossem possíveis.

Aos professores do curso de Ciência da Computação que sempre acreditaram no meu potencial e me incentivaram a prosseguir nos estudos.

A minha namorada Monia Tainá pelo grande incentivo e pelo paciente trabalho de revisão da redação feito nesta presente monografia e a todos que direta ou indiretamente contribuíram com a execução desse trabalho.

"Não importa quanto a vida possa ser ruim, sempre existe algo que você pode fazer, e triunfar. Enquanto há vida, há esperança."

(Stephen Hawking)

RESUMO

O IPV6 é uma nova versão do protocolo de Internet que visa resolver a falta de endereços do atual protocolo (IPV4). Devido ao esgotamento dos endereços IPV4, a implementação do IPV6 torna-se necessária nas redes atuais, e esta transição necessitará de um período de coexistência e interoperabilidade dos mesmos, devido à incompatibilidade entre ambos os protocolos. Com isso o novo desafio dos administradores de rede será prover essa coexistência e interoperabilidade através de técnicas de transição, e manter a segurança da rede em ambos os protocolos. Ao analisar as técnicas de transição, verificaremos as possíveis vulnerabilidades de segurança das redes que usam cada um dos métodos de transição, fazendo um comparativo entre as técnicas e apresentando possíveis soluções para as vulnerabilidades encontradas.

Palavras-chave: IPV6, segurança de redes, protocolo, *i*nternet, vulnerabilidades.

ABSTRACT

IPV6 is a new version of the Internet Protocol to the resolution of the lack of current protocol addresses (IPV4). Due to the exhaustion of IPV4 addresses, the implementation of IPV6 becomes necessary in today's networks, this transition requires a period of coexistence and interoperability between them , due to incompatibility between the two protocols. Then the new challenge for network administrators will provide this coexistence and interoperability through transition techniques and keeping network security in both protocols. Analyzing the transition techniques, we´ll see the potential security vulnerabilities of networks using each transition methods making a comparison between the technical and presenting possible solutions to the vulnerabilities found.

Keywords: IPV6, network security, protocol, Internet, vulnerabilities, transition.

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

APNIC	*Asia Pacific Network Information Centre*
CIDR	*Classless Inter-domain Routing*
IETF	*Internet Engineering Task Force*
IANA	*Internet Assigned Numbers Authority*
IPng	*Internet protocol next generation*
IPSec	*IP Security Protocol*
ISOC	*Internet Society*
IPv4	*Internet Protocol version* 4
IPv6	*Internet Protocol version* 6
MPLS	*Multi-Protocol Label Switching*
NAT	*Network address translation*
RFC	*Request for Comments*
RIPE-NCC	*Réseaux IP Européens Network Coordination Centre*
RIRs	*Regional Internet Registry*
ROAD	*Routing and Addressing*
TCP	*Transmission Control Protocol*

SUMÁRIO

1 INTRODUÇÃO

Com a insuficiência dos estoques de endereços IPv4, a implantação do protocolo IPv6 tornou-se uma necessidade atual. O estoque central de IPv4 da IANA chegou ao fim em fevereiro de 2011, após a cerimônia de entrega dos últimos blocos /8 para os Regional Internet Registrys (RIRs). Com isso, empresas que utilizam internet, usuários domésticos, provedores de internet e conteúdo, sistemas autônomos e dispositivos que acessam internet deverão passar a operar com o protocolo IPv6, visto que o protocolo IPv4 passa a apresentar limitações geradas pelo grande número de usuários e dispositivos interligados. Como esta transição não pode ser feita de forma imediata, será necessário um período de coexistência do IPV4 com o IPV6, o que requer uma implantação correta, evitando riscos de segurança, inclusive para redes que ainda não estejam usando IPv6 nativo.

1.1 Motivação

Na implantação de novas tecnologias em uma rede de computadores, uma das principais preocupações deve ser a segurança antes, durante e depois da implantação, de forma a evitar que haja pontos de falha ou possibilidade de invasão da rede em questão. Para executar essa implantação é importante o conhecimento dos métodos de transição e seus respectivos impactos para a segurança da rede. É necessário propor meios de defesa a possíveis vulnerabilidades para evitar problemas futuros decorrentes da implantação de IPV6 em todas as redes. Este é o principal foco desta pesquisa.

1.2 Objetivos

1.2.1 Objetivo geral

- Encontrar um método eficiente e seguro de implantação do protocolo IPV6 em redes que utilizam o protocolo IPV4.

1.2.2 Objetivos Específicos

- Descrever as vulnerabilidades, vantagens e desvantagens dos métodos de transição

entre IPV4/IPV6;

• Apresentar meios de solucionar as vulnerabilidades encontradas;

• Simular 3 cenários de redes (apenas IPV4, apenas IPV6 e com suporte nativo aos 2 protocolos), e apresentar a solução mais segura que promova a interoperabilidade entre os 2 protocolos em cada cenário.

1.3 Organização do trabalho

No capítulo 2 será abordada a parte teórica, mostrando as limitações do protocolo IPv4, e explicações sobre o protocolo IPv6, expondo a importância e os problemas decorrentes de sua implantação.

No capitulo 3 serão abordados os métodos de transição e coexistência entre redes IPV4 e IPV6.

No capítulo 4 serão citadas as falhas de segurança, bem como possíveis soluções.

No final do trabalho serão apresentados as possíveis formas de reduzir as vulnerabilidades de uma rede em transição de protocolos IP, através de um *firewall* pilha dupla, sugerindo a forma mais segura de implantar a coexistência entre IPv4 e IPv6 de acordo com a presente pesquisa.

2 PROTOCOLO IPV6/IPV4

2.1 O protocolo IPv6

O IPv6 é uma evolução do protocolo IPv4 , o qual endereça dispositivos conectados a Internet, surgindo como medida a sanar o esgotamento de endereços do protocolo IPv4. Cada endereço possui forma unívoca, ou seja, possui combinação única. No inicio dos anos 90 a IETF iniciou o desenvolvimento de um sucessor do protocolo IPv4, devido a necessidade de obter novos endereços que estavam extinguindo-se com o crescimento de usuários e novas tecnologias. A IETF formou então o IPng, com o objetivo de estabelecer padrões para serem seguidos pelo novo protocolo como segurança e autoconfiguração, suporte a grandes pacotes e encapsulamento (tunelamento) IPv6 sobre IPv4 (GRAZIANI,2012).

Com o esgotamento de endereços IPv4 foram utilizados métodos provisórios para tentar diminuir a grande demanda do protocolo, porém estes não conseguiram resolver os problemas causados pelo crescimento da Internet. Tais métodos, entretanto, serviram como fatores de tempo para que o protocolo IPv6 fosse desenvolvido. A IETF padronizou em 1993 pesquisas para que o protocolo IPv6 pudesse ser aperfeiçoado e ampliado. O IPng formalizou através da RFC 1550 novos projetos , requisitando propostas para o estudo do IPv6. A abordagem do novo projeto envolvia um protocolo que fosse baseado no protocolo IPv4 , porém com a capacidade de fornecer soluções para resolver as falhas do mesmo.

A insuficiência de endereços IPv4 veio com o crescimento excessivo de usuários, e a destinação destes endereços para corporações e instituições, visto que o projeto inicial não foi planejado para o número crescente de computadores . Segundo a *Internet World Statistic (Tabela 1),* no início dos anos 90 haviam cerca de 16 milhões de usuários em todo o mundo. Em 2011 este número subiu para 2 bilhões, aumentando drasticamente devido aos usuários atuais possuírem vários dispositivos conectados (como tablets, smartphones e laptops), conforme a tabela a seguir:

TABELA 1- Crescimento da Internet no mundo

DATE	NUMBER OF USERS	% WORLD POPULATION	INFORMATION SOURCE
December, 1995	16 millions	0.4 %	IDC
December, 1996	36 millions	0.9 %	IDC
December, 1997	70 millions	1.7 %	IDC
December, 1998	147 millions	3.6 %	C.I. Almanac
December, 1999	248 millions	4.1 %	Nua Ltd.
March, 2000	304 millions	5.0 %	Nua Ltd.
July, 2000	359 millions	5.9 %	Nua Ltd.
December, 2000	361 millions	5.8 %	Internet World Stats
March, 2001	458 millions	7.6 %	Nua Ltd.
June, 2001	479 millions	7.9 %	Nua Ltd.
August, 2001	513 millions	8.6 %	Nua Ltd.
Sept, 2010	1,971 millions	28.8 %	Internet World Stats
Mar, 2011	2,095 millions	30.2 %	Internet World Stats
Jun, 2011	2,110 millions	30.4 %	Internet World Stats
Sept, 2011	2,180 millions	31.5 %	Internet World Stats
Dec, 2011	2,267 millions	32.7 %	Internet World Stats
Mar, 2012	2,336 millions	33.3 %	Internet World Stats
June, 2012	2,405 millions	34.3 %	Internet World Stats
Sept, 2012	2,439 millions	34.8 %	Internet World Stats
Dec, 2012	2,497 millions	35.7 %	I.T.U.
Dec, 2013	2,802 millions	39.0 %	Internet World Stats
June, 2014	3,035 millions	42.3 %	Internet World Stats
Dec, 2014	3,079 millions	42.4 %	Internet World Stats
June, 2015	3,270 millions	45.0 %	Internet World Stats
Dec, 2015 (est.)	**3,366 millions**	**46.4 %**	Internet World Stats

fonte: http://www.internetworldstats.com/emarketing.htm(2016)

2.2 O protocolo IPv4 e suas limitações

O IPv4 é o atual protocolo que opera na Internet, descrito pela IETF na publicação RFC 791 em setembro de 1981. Segundo Davies (2012,p.1), "a versão atual não mudou substancialmente desde que foi descrita na RFC, mantendo-se robusta, de fácil interoperabilidade e implementação, porém não previa o grande crescimento de usuários e o esgotamento de endereços". O aumento de usuários e a política de divisão dos endereços a partir dos anos 90 tornou o endereçamento IPv4 escasso, e essa redução tornou-se mais preocupante devido as novas tecnologias que foram sendo implantadas e interligadas a rede.

No protocolo IPv4 existe uma sequência definida por padrão de blocos "x.x.x.x", onde cada bloco x delimita-se a uma sequência de 0 a 255, tendo como disponibilidade 32 bits para endereçamento. Teoricamente essa disponibilidade forneceria a quantidade de 4 bilhões de endereços, número grande para o período de criação do protocolo, porém insuficiente para a quantidade de endereços necessários atualmente, como demonstrado na tabela 2, o Ipv6 resolve esse problema com um numero de endereços bem maior.

TABELA 2- Comparativos entre o Ipv4 e o IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

fonte: http://www.wirelessdesignmag.com/article/2015/10/ipv6-over-bluetooth-smart-lays-iot-foundations(2015)

No modelo técnico do protocolo IPv4 cada endereço recebe uma sequência de 32 bits, sendo que essa sequência é divida em grupos de 8 bits, chamados de octetos. Os primeiros bits do endereço servirão para identificar a rede e os últimos servirão para identificar o computador em

si. Pela quantidade de octetos, qualquer divisão fixa reduziria bastante o número de endereços possíveis, o que seria uma grande limitação no caso da Internet, onde existe um número muito grande de redes diferentes, muitas delas com um número muito grande de micros conectados, como no caso dos grandes provedores de acesso (MORIMOTO,2010). Dependendo da alocação do octeto inicial, seria complicado obter grandes números de endereços. Se a alocação fosse feita com o primeiro octeto, haveriam por exemplo poucos endereços para vários hosts (256 endereços possíveis).

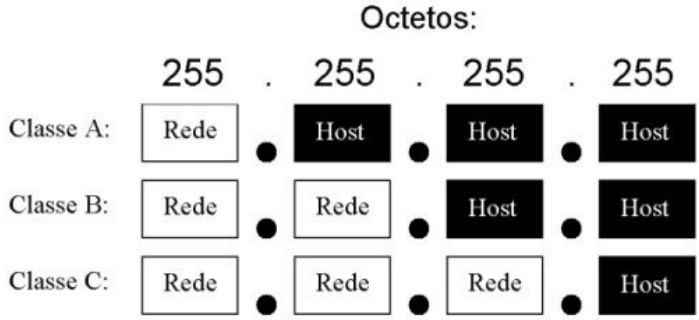
Um endereço Ipv4 é composto de uma determinada sequência de 32 bits, divididos em 4 grupos de 8 bits cada, chamados de octetos e cada octeto permite o uso de 256 combinações diferentes. Conforme visto, cada IP foi identificado pela sua sequência inicial e final (Octeto inicial como identificação e o *host* como octeto final). Com o objetivo de solucionar o esgotamento de endereços pelo principio da alocação fixa dos IP's, foram definidas divisões em grupos de acordo com o intervalo do octeto inicial. Estes grupos foram denominados como classes, sendo que cada classe reserva um determinado número de octetos para definir o endereçamento da rede:

• **Classe A:** A classe A é identificada pelo primeiro octeto do endereço IP. O número do octeto inicial varia do intervalo entre 1 e 126 (como em 114.220.34.57). Em um endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao *host.*

•**Classe B:** A classe B é identificada pelos dois octetos iniciais do endereço IP . O número do octeto inicial varia do intervalo entre 128 a 191. Em um endereço de classe B, a máscara será 255.255.0.0, indicando que os dois primeiros octetos referem-se à rede e os dois últimos ao *host*.

•**Classe C:** A classe C é identificada pelos três octetos iniciais do endereço IP. O número do octeto inicial varia do intervalo entre 192 a 223. Em um endereço de classe C, a máscara será 255.255.255.0, indicando que os três primeiros octetos referem-se à rede e o último ao *host.*

FIGURA 1- Classe de endereços e valores do octeto inicial



fonte: http://www.hardware.com.br/livros/linux-redes/capitulo-entendendo-enderecamento.html(2006)

Embora a subdivisão de classe tivesse como objetivo tornar a distribuição de endereços mais equilibrada, o modelo de classes mostrou-se ineficiente, isso porque determinadas classes atendiam números altos de redes e ocupavam poucos endereços. Outras possuíam muitos endereços, porém atendiam poucas redes. A divisão por classes era desvantajosa já que fazia com que uma grande quantidade de endereços IP fossem desperdiçados. Segundo Graziani(2012,p. 13) "a maioria das redes de classe A e B possuíram um grande número de endereços não utilizados, enquanto a maioria das redes de classe C tiveram grande oferta de endereços, porem muitos destes não foram utilizados". A má distribuição de classes do tipo "A" também foi um dos fatores que colaboraram com o esgotamento de endereços, isso porque tais endereços foram fornecidos e reservados a grandes organizações, sendo que praticamente muitos nem seriam utilizados por completo.

> O problema é que durante a década de 1980 muitos endereços registrados foram alocados para empresas e organizações sem qualquer controle consistente. Como resultado, algumas organizações têm mais endereços do que elas realmente precisam, dando origem a escassez de endereços registráveis. (AMOSS; MINOLI,2007,p. 8)

Amoss e Minoli (2007, p.5) definem que "o protocolo IPv4 tem mostrado-se como sendo um poderoso mecanismo de rede flexível, porém começando a apresentar limitações atuais geradas pelas novas populações de usuários e novas tecnologias de dispositivos conectados a rede, o que diz respeito a necessidade de aumento de espaço para endereços IP". Mesmo o protocolo

IPv4 que manteve-se por 30 anos encontra-se num momento de fragilidade e esgotamento.

Para tentar então diminuir a grande demanda do IPv4, foram então utilizados métodos "paliativos" para reduzir o esgotamento.

2.3 Métodos paliativos

Com o esgotamento dos endereços IPv4 e a falha de subdivisão por classes, a IETF começou a procurar soluções para sanar a falta dos estoques do protocolo. O protocolo IPv6 era então uma solução a longo prazo, porém como a transição demoraria e o gerenciamento por classes gerava desperdício de IP, era necessário dispor de uma solução a médio prazo para minimizar os esgotamentos. Em 1991, a IETF forma o grupo de trabalho ROAD, cujo objetivo era discutir métodos para evitar a exaustão de espaço do protocolo IPv4. O grupo então define um novo método para utilização dos endereços sem subdivisão de classe: o método CIDR.

2.3.1 O método CIDR

Com o modelo falho de alocação por classes, a *IETF* decidiu modificar o método de subdivisão de endereços, partindo através da RFC 1338 a utilizar o roteamento entre domínio sem classes, definido como CIDR. O CIDR foi citado na RFC 1518, 1519, e 2050, sendo descrito na RFC 4632. A principal proposta do CIDR era dispensar a alocação baseada no uso de classes. Isto permitiria uma alocação mais flexível, baseada na necessidade real de determinada rede. Conforme Amoss e Minoli (2007, p.7), a ideia do CIDR é que blocos de vários endereços (por exemplo, blocos de endereços classe C) podem ser combinados ou agregados para criar um conjunto sem classe maior de endereços IP. O CIDR permite que haja grande versatilidade na hora de gerar novos endereços IP porque possui vários recursos de alocação como a utilização de máscaras de tamanho variável (*Variable-length subnet Mask),* o agrupamento de faixas de endereços em faixas maiores, e a mudança de referencial no octeto inicial.

Na configuração de uma determinada rede não bastaria apenas o fornecimento do

endereço IP. A identificação deste endereço de rede pelo octeto inicial e *host* é definida pela máscara de rede (*subnet mask*). Diferente do IP, a máscara de sub-rede é normalmente formada por apenas dois valores: 0 e 255, que como visto, o valor 255 indica a parte endereço IP referente a rede, e o valor 0 indica a parte endereço IP referente ao *host*. Logo, dependendo do valor inicial da máscara, esta seria alocada e designada a determinada classe de endereçamento. O método CIDR quebra a alocação por classes utilizando máscaras variáveis de uma forma mais refinada, promovendo, portanto, um uso mais eficiente para os endereços IP cada vez mais escassos.

2.3.2 O protocolo NAT

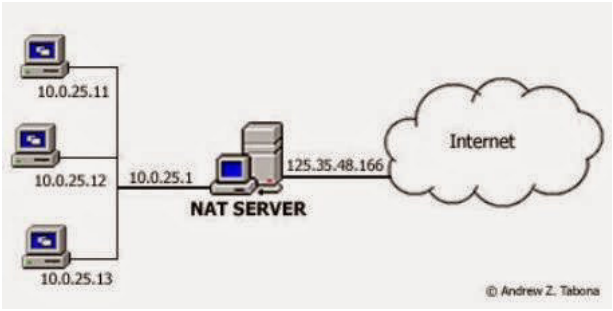
Um outro método provisório que permitiu leve sobrevida ao IPv4 foi o uso do protocolo NAT, que executa a tradução de endereços IP e portas TCP, permitindo que vários computadores de determinada rede possuam acesso a Internet utilizando um único IP, prevenindo esgotamentos do protocolo IPv4. O protocolo foi definido na RFC 3022, como método para quebrar o modelo fim-a-fim da internet, realizando conexões entre os dispositivos e fazendo com que estes passem por um processo de tradução. O funcionamento do NAT tem como principal ideia conceder com que vários *hosts* possam trafegar na rede, com apenas um endereço IP, ou um número pequeno de endereços.

Conforme visto, cada máquina que deseja acessar a Internet deve possuir o protocolo TCP/IP configurado. Para isso, cada computador da rede interna precisaria de um endereço IP válido no ambiente da internet. Por esse motivo o endereçamento do protocolo entraria em escassez. A criação do NAT veio para solucionar este esgotamento, ou pelo menos fornecer uma determinada solução até que o IPv6 esteja em uso.

Com o método NAT, um grande número de computadores podem acessar a rede ao mesmo tempo apenas utilizando um endereço IP ou um número de endereços em quantidade bem pequena em comparação ao número de computadores interligados na rede. O protocolo age diferenciando e otimizando a atribuição de portas de comunicação, associando-as com cada IP de

uma rede.

FIGURA 2-Modelo do protocolo NAT



Fonte: http://infocare4u.blogspot.com.br/2014/12/internet-connection-sharing_30.html(2014)

No acesso a uma determinada rede, um usuário possui um pacote definido como pacote de informações, em que consta um endereço IP da rede interna. Caso o endereço de origem não seja válido (como exemplo um endereço que seja de faixa privada), o pacote não poderá ser enviado para a rede utilizando somente o método NAT, sendo necessário a "substituição" do endereço IP de origem por outro endereço da própria interface do NAT. Define-se este processo como tradução, em que consiste em mudar o endereço interno por um endereço válido na rede. Além da tradução, o NAT associa o endereçamento IP com portas de comunicação em uma tabela, onde determinada porta relaciona-se com um endereço traduzido. O protocolo relaciona então as portas com o usuário do IP modificado. Como as portas estão relacionadas a um endereço interno, o protocolo através de uma consulta na tabela direciona o pacote de informações ao computador cujo IP interno esteja relacionado a porta de comunicação.

Apesar do protocolo NAT ser considerado um bom método para tentar diminuir a escassez do endereçamento IPv4, o mesmo apresenta falhas, o que torna-o inconveniente para algumas conexões. Segundo Davies (2012, p.1), "o esgotamento de espaços do protocolo IPv4, acarretou o uso do protocolo NAT para mapeamentos de pequenos números de endereços públicos para vários endereços privados, violando o principio da neutralidade da rede". Um exemplo é o mecanismo do NAT, que "quebra" o modelo fim-a-fim da Internet, o que acaba não

permitindo conexões diretas entre *hosts.* Este processo dificulta a criação de aplicações estilo Voip, P2P, entre outras, pelo fato dos dispositivos conectados via NAT possuírem um endereço privado e compartilharem o mesmo endereço público. Conforme Graziani (2012, p.16), "a utilização do NAT tem sido fundamental na redução do esgotamento dos endereços IPv4. Entretanto, o NAT tem certas limitações, como a incerteza do endereço de destino e um endereço público que pode ser compartilhado entre vários usuários". O protocolo, portanto, ocasiona dificuldades a gerência da segurança de uma rede, pois para identificar os acessos de um usuário para fins de investigação é necessário guardar logs de acesso dos IPs privados utilizados (Os quesitos de segurança serão melhor abordados no capitulo 4).

Mesmo com a técnica do protocolo NAT que tinha como objetivo reduzir a demanda por endereços IP, e com os outros métodos paliativos utilizados, em 2011, os últimos blocos disponíveis na IANA foram entregues aos RIRs, ou seja , o estoque central de endereços IP mantidos pela IANA acabou, havendo apenas os estoques regionais. Os estoques IPv4 da APNIC e o estoque do RIPE-NCC também chegaram ao fim em 2011. Os métodos acabaram minimizando o esgotamento, porém não foram suficientes para reduzir a grande demanda do IPv4. Logo, "o protocolo NAT funciona melhor para reutilização de endereços privados, porém o mesmo é uma medida improvisada para prolongar a vida útil do espaço de endereço IPv4 público e não é uma solução para o problema do espaço de endereços IPv4". (DAVIES, 2012, p. 5)

Sendo assim, para que a internet permaneça em expansão torna-se necessária a implantação de um protocolo de endereçamento capaz de suprir a demanda de endereços IP: o protocolo IPv6, que possui aproximadamente 79 octilhões de endereços, tornando possível o endereçamento dos dispositivos de rede sem necessidade do NAT.

2.4 Benefícios da implantação do protocolo IPv6

Com o atual esgotamento do protocolo IPv4, a transição para um novo protocolo

tornou-se necessária para suprir a falta de endereços. Porém esta migração não é somente pela escassez de endereçamento, mas também pelas limitações que o IPv4 possui. A internet requer portanto, a disponibilização de serviços novos capazes de otimizar e resolver falhas atuais do IPv4 geradas pela falta de suporte, falta de auto configuração, dentre outras deficiências.

> O protocolo IPv4 tem provado, por meio de sua longa vida ser um protocolo de rede flexível e de mecanismo poderoso. No entanto o IPv4 está começando a apresentar limitações, não apenas com respeito à necessidade de um aumento do espaço de endereços IP, mas também em relação a um lançamento potencial do VoIP.(…) O IPv6 também acrescenta melhorias em áreas como roteamento e rede de autoconfiguração.
> (AMOSS; MINOLI, 2007, p. 5)

Segundo Amoss e Minoli (2007, p.5), os benefícios da implantação do IPv6 são os seguintes:

• **Escalabilidade:** Uma das principais citadas no protocolo**;** O IPv6 possui endereços de 128 bits contra os endereços IPv4 que possuem 32 bits. Com o protocolo IPv4 , o número de endereços IP disponíveis é 2^{32} (aproximadamente 4 bilhões de endereços). No IPv6 a quantidade de endereços aumenta para um espaço de 2^{128} **(** aproximadamente 340 undecilhões);

• **Segurança**: O IPv6 inclui recursos de segurança , como criptografia de carga, autenticação da fonte de comunicação e nas suas especificações. Segundo Davies (2012, p. 2), "a comunicação privada em utilização a uma mídia pública como a internet requer serviços de criptografia que protegem os dados enviados, sejam aqueles para visualização quanto os modificados em trânsito". Embora um padrão de segurança já existisse para pacotes IPv4 que é o IPSec, este padrão é opcional para o mesmo, sendo que apesar de existir a opção do IPSec, são utilizadas preferencialmente soluções proprietárias na maioria das implementações de segurança (O IPSec será melhor abordado no capitulo 4);

• **aplicações em tempo real:** com o objetivo de proporcionar melhor suporte para tráfego em tempo real, o protocolo IPv6 possui o rotulado de fluxos. (pacotes de dados são rotulados e estes reconhecem o fluxo, sendo encaminhados com base no conteúdo desses rótulos, semelhante

ao serviço MPLS;

• **Serviço *Plug-and-play*** : O IPv6 inclui o mecanismo *plug-and-play*, que facilita a conexão de equipamentos à rede . A configuração necessária é automática;

• **Mobilidade**: O IPv6 possui mecanismos de mobilidade mais eficientes e melhoradas particularmente importantes para as redes móveis . Segundo Davies (2012,p. 15), "embora os recursos como segurança e mobilidade estejam disponíveis no IPv4, eles estão disponíveis como "extensões". logo possuem limitações de arquitetura ou de conectividade que não existiriam caso fossem implementadas no projeto inicial do protocolo";

• **Protocolo otimizado**: Na otimização, o IPv6 incorpora melhores práticas do protocolo IPv4 , porém remove características IPv4 consideradas obsoletas . Isto resulta em um protocolo de internet aperfeiçoado;

• **Endereçamento e roteamento**: O IPv6 melhora a hierarquia de endereçamento e roteamento;

• **Extensibilidade**: O protocolo foi projetado para ser extensível e oferece suporte para novas opções e extensões. Segundo Davies (2012, p. 8), "o IPv6 pode ser facilmente estendido para novas funcionalidades , adicionando cabeçalhos de extensão após o cabeçalho. Ao contrário do IPv4 que pode suportar apenas 40 *bytes* de opções, no IPv6 os cabeçalhos são apenas limitados pelo tamanho do pacote IPv6".

3 TRANSIÇÃO

3.1 O cenário da transição IPv6

As soluções paliativas surgiram como métodos para tentar solucionar o impasse do esgotamento de endereços IP. Porém tais métodos não foram suficientes para reduzir a grande demanda do IPv4, que continuou possuindo grande expansão na proporção ao crescimento da internet. Diante tal escassez, a IETF possuía, depois de ter descartado outros projetos incompletos ou falhos o protocolo IPv6, visando uma solução não só de esgotamentos, mas sim de falhas do protocolo antigo. A transição era então vista como algo imediato, porém com o numero exorbitante de aplicações legadas e *hardwares* operando em redes com protocolo IPv4, o grande impasse da implantação do IPv6 é ainda a incompatibilidade entre este e o protocolo atual, o que acaba gerando atraso de transição, necessitando de um período de coexistência entre ambos os protocolos, até que todos os dispositivos e *softwares* legados sejam substituídos por outros similares ou recebam atualizações que permitam a integração com redes IPv6. Para a implantação do protocolo em grandes empresas por exemplo, há um número de exigências aplicáveis como um bom gerenciamento do IPv6, monitoramento ligado a segurança e boa interoperabilidade entre IPv4 e IPv6, como no uso da pilha dupla[1].

Nessa implantação do IPv6 eram necessárias técnicas para facilitar a transição. Foram então desenvolvidos vários mecanismos que visam reduzir os transtornos decorrentes do processo de transição, evitando possíveis erros de compatibilidades. Determinadas técnicas seriam utilizadas de acordo ao propósito e necessidade de um rede.

> A migração é esperada para ser bastante complexa . Inicialmente, a interligação entre dois ambientes serão críticos . Os nós IPv4 existentes terão de executar os nós de pilha dupla ou converter para sistemas IPv6. Felizmente, o novo protocolo suporta endereços IPv6 compatíveis com IPv4, que é um formato de endereço IPv6 que emprega endereços IPv4 incorporados. O Tunelamento irá desempenhar um papel importante

1 6NET. **Final IPv4 to IPv6 Transition Cookbook for Organisational/ISP (NREN) and Backbone Networks.** Disponivel em: <https://www.6net.org/publications/deliverables/D2.2.4.pdf>. Acesso em 22 fev.2016

no início da transição. (AMOSS; MINOLI,2007,p. 17)

No cenário inicial da transição, na qual os provedores de acesso ainda não estão utilizando IPv6, opera ainda a "pilha" simples IPv4. Sem esse suporte nativo ao IPv6, um dispositivo IPv6 pode se comunicar com outro dispositivo IPv6 somente utilizando determinadas técnicas, como a de tunelamento para passar o tráfego IPv6 encapsulado em pacotes IPv4 pela rede IPv4, que vai ser desencapsulado no dispositivo receptor, e este irá ler o cabeçalho IPv6 e enviar o pacote correspondente ao receptor (geralmente um servidor que opera em pilha dupla realiza esse processo).

Como um grande número de serviços atuais utilizam o protocolo IPv4, seria então demorado (ou talvez impossível) realizar tal mudança imediata para o protocolo atual. Logo, deveriam ser abordados métodos que implementassem o protocolo IPv6 de forma simultânea de modo a não causar falhas em equipamentos e outros serviços. Estes métodos seriam mecanismos básicos que não causariam interferências a uma rede implantada.

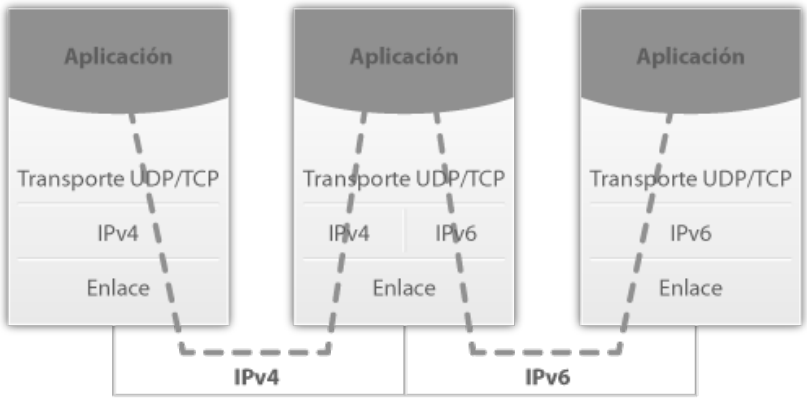
Em uma determinada rede seria escolhido um método de transição, dependendo do suporte de rede e topologia. Como muitos serviços de rede ainda utilizam o protocolo IPv4, no cenário da transição inicial é necessário manter o IPv4 operante e complementá-lo com o IPv6 nativamente, mantendo-o de forma simultânea em uma rede. A esse tipo de método denomina-se pilha dupla.

3.2 A pilha dupla

A maioria das redes atuais utilizam o protocolo IPv4, logo a transição para o IPv6 deveria ser feita de forma a prover a coexistência entre ambos os protocolos e evitar problemas com dispositivos que utilizem o protocolo antigo. A Pilha dupla (*dual-stack*) consiste em um método para essa implementação simultânea, como suporte ao IPv4 e IPv6, permitindo que equipamentos estejam equipados com "pilhas" para ambos os protocolos, tendo a capacidade de

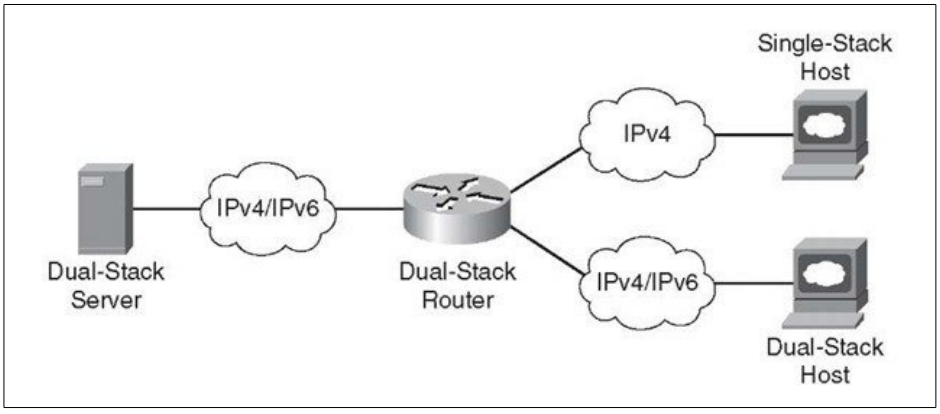
enviar e receber os dois simultaneamente. Conforme Cicileo[1], "neste caso é necessário dispor de uma quantidade suficiente de endereços IPv4 para poder implementar as duas versões do protocolo juntos por toda a rede". Quando for estabelecida uma conexão, cujo destino é apenas IPv4, será utilizada a conectividade IPv4, e quando for estabelecida uma conexão, cujo destino é apenas IPv6 ou pilha dupla, será utilizada a conectividade IPv6. "Os nós de pilha dupla mantém, portanto, dois protocolos operando em paralelo em pilhas, permitindo que o sistema final possa operar através de qualquer protocolo". (AMOSS; MINOLI, 2007, p. 108)

FIGURA 3 -Esquema da pilha dupla



fonte:http://portalipv6.lacnic.net/pt-br/mecanismos-de-transicao

FIGURA 4 – Topologia de uma Pilha dupla



fonte: http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-1/

1CICILEO, Guilherme.Mecanismos de transição. Disponível em: <http://portalipv6.lacnic.net/pt-br/mecanismos-de-transicao/>Acesso em 25 de fev.2016

No funcionamento da pilha dupla, um nó incluirá ambos os endereços (IPv4 e IPv6). Estes nós estarão sendo enviados por equipamentos que possuem "pilhas", que realizam a comunicação e envio simultâneo. Um determinado nó duplo se comunicará, por exemplo com um nó IPv6 , e logo se comportará como um nó IPv6. Caso este nó esteja se comunicando com um nó IPv4 se comportará como nó IPv4.

> Atualmente a Internet continua a ser principalmente sediada pelo IPv4. No entanto , é razoável esperar que este cenário vai mudar em breve, logo que mais e mais redes são migradas para a nova pilha de protocolos. Infelizmente, migrando milhões de redes vai demorar algum tempo. Entretanto, alguma forma de 6to4 / pilha-dupla vai fornecer a funcionalidade desejada. (DAVIES apud SOTILLO,2006, p. 5)

Embora a transição pelo método da pilha dupla fosse uma ótima alternativa para implementação de protocolo simultâneo, nem em todos os casos é possível utilizá-la. Um exemplo é que determinados nós só podem se comunicar com nós iguais. O método também falha quando não existem mais endereços IPv4 , e quando não existem equipamentos capazes de suportar o IPv6. Existe também o foco nas configurações, principalmente no DNS(*Domain Name System*) e outros protocolos de roteamento. O método da pilha dupla não é totalmente a prova de falhas, portanto precisa ser avaliado principalmente no gerenciamento de uma rede e no *Firewall*[1].

3.3 Método de tunelamento (encapsulamento)

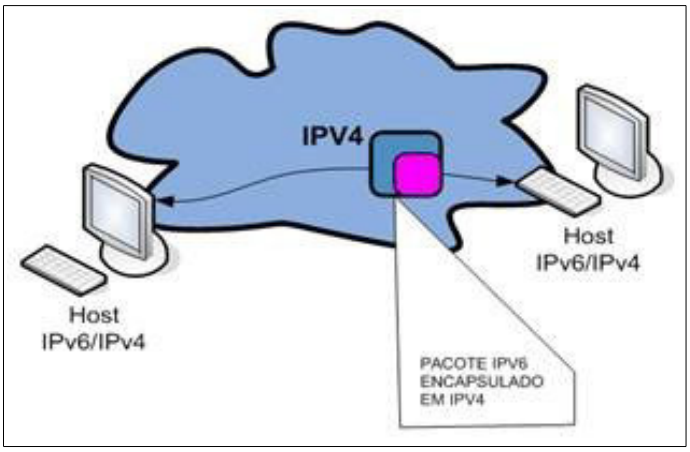
O método do tunelamento (*tunneling*) consiste em encapsulamento de pacotes IPv6 em IPv4. É utilizado para casos onde não houvesse suporte ao IPv6 nativo.

Em um cenário tipico da primeira fase da transição, na qual os provedores de acesso ainda não estão utilizando IPv6 em uma rede IPv4 sem suporte nativo, um dispositivo IPv6 pode se comunicar com outro dispositivo IPv6 usando técnicas de tunelamento para passar o tráfego encapsulado em pacotes IPv4 pela rede que vai ser desencapsulado no dispositivo receptor e este irá ler o cabeçalho IPv6 e enviar o pacote correspondente ao receptor. De maneira geral são

1 IPV6.BR. Transição. Disponivel em < http://ipv6.br/post/transicao/>. Acesso em 26 fev. 2016.

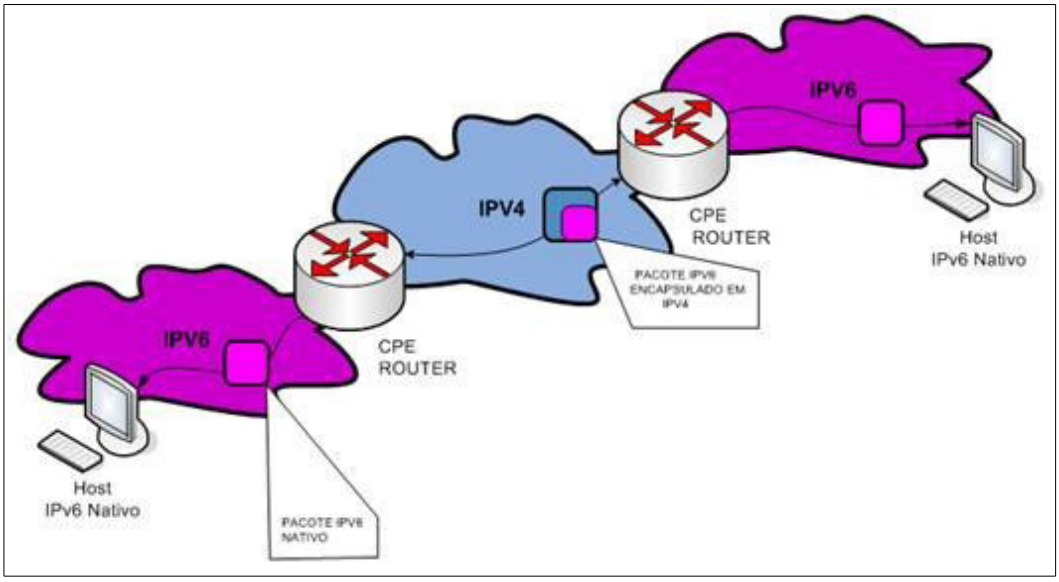
utilizados “túneis” que encapsulam IPv6 dentro do IPv4, o que permite atravessar redes que não possuem o IPv6. Pacotes são encaminhados até determinado ponto de rede, sendo depois encapsulados para poderem atravessar e ser desencapsulados na parte em que a rede o suporta. Por fim os pacotes seguem e são enviados ao destino final.

FIGURA 5 – Tunelamento em Configuração *Host* a *Host*



fonte: http://www.teleco.com.br/tutoriais/tutorialredeipmig1/pagina_3.asp

FIGURA 6 – Tunelamento em Configuração *Host* a Roteador



fonte: http://www.teleco.com.br/tutoriais/tutorialredeipmig1/pagina_3.asp

Existem vários tipos de tunelamento. Segundo Graziani (2012), a IETF estabeleceu várias técnicas para o uso de túneis, entretanto de forma básica toda técnica de tunelamento executa a mesma ideia de encapsulamento. Esse número de opções de encapsulamento são muito grandes, então para evitar confusões, as técnicas seriam utilizadas de acordo com a quantidade e requisitos específicos para esses túneis.

As técnicas *Broker*, 6*over*4, 6*to*4, Teredo, ISATAP e GRE são exemplos de tunelamentos conhecidos, cada uma utilizada de acordo com a necessidade da implantação e transição. Quatro destas serão abordadas. As técnicas 6*to*4, teredo, *broker* e GRE.

3.3.1 6to4

O tunelamento manual é um método de transição muito importante e de boa configuração. Porém torna-se problemático quando a quantidade de túneis aumenta. "A IETF definiu então o mecanismo 6to4 para conexão automática a varias redes IPv6 mais um túnel configurado". (GRAZIANI, 2012, p.341)

O *6to4* é um método de tunelamento, que assim como os outros, encapsula o trafego IPv6 com cabeçalho IPv4, de forma a passar por uma rede IPv4 sem problemas. Descrito na RFC 3056, o método baseia-se no uso de *relays* e *r*oteadores *6to4* para fornecer a uma rede IPv4, conectividade IPv6.

A arquitetura do *6to4 é* dividida em três estruturas:

• ***relays****: Relays* são roteadores que apresentam conexão nativa IPv4 e IPv6, encaminhando trafego 6ťo4 entre roteadores e a internet. Os *relays* ficam na extremidade dos túneis automáticos para os roteadores *6to4* que precisam se comunicar com a rede IPv6[1];

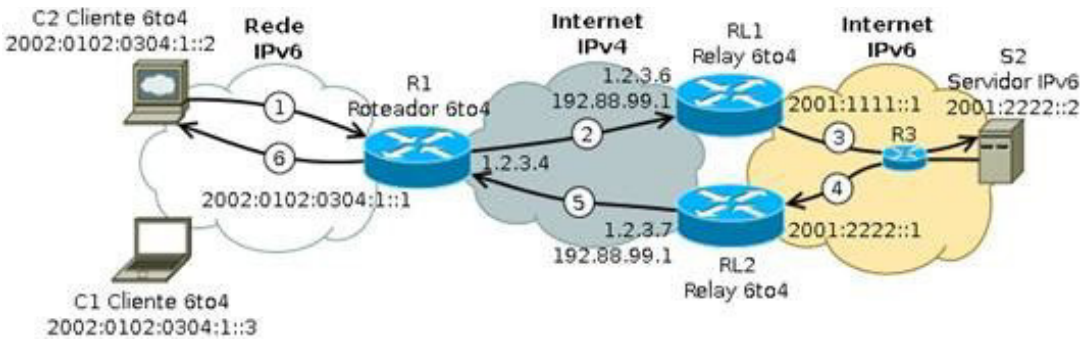
• **Roteador 6to4**: Conforme Amoss e Minoli (2007, p.130), "um roteador IPv6 / IPv4 é um dispositivo que suporta o uso de um túnel 6to4 e é normalmente usado para transmitir endereços

1 TELECO. Redes IP II: técnicas de transição de tunelamento. Disponível em < http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp>. Acesso em 27 fev. 2016.

6to4 de tráfego entre o 6to4 e outros roteadores 6to4 (ou 6to4 *relay*) para a rede IPv4";

• **cliente 6to4:** Clientes são os computadores, ou os equipamentos de rede que utilizam endereços IPv6 do túnel 6to4.

FIGURA 7 - Topologia e funcionamento do túnel 6to4



fonte: <http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp>

No mecanismo 6to4, um pacote de endereço IPv6 segue para o roteador, disponibilizado pelo cliente, sendo encapsulado em IPv4 e transportado ao *relay*. Do *relay*, ele segue para a rede, sendo antes desencapsulado. Depois de desencapsulado, o pacote é enviado (através de outro roteador) para um servidor. O servidor envia outro pacote IPv6 pelo mesmo roteador que enviou o primeiro nó, cujo o destino é o cliente. Chegando ao *relay* próximo, o pacote segue para a interface 6to4 que o empacota como IPv4. Por ultimo, o roteador que recebe o pacote desencapsula o mesmo e este segue para o cliente 6to4. [1]

Conforme Amoss e Minoli (2007, p.130), "O fornecimento de informações e recursos (*host 6to4*), o roteamento IPv6/IPv4 com suporte a túneis e o uso de *relays* com o objetivo de encaminhar tráfego 6to4 entre roteadores 6to4 na Internet e *hosts* na Internet IPv6 são os principais elementos do mecanismo 6to4 para a transição IPv6".

Apesar do método 6to4 ser uma técnica interessante para uso na transição IPv6, o mesmo

1 TELECO. Redes IP II: técnicas de transição de tunelamento. Disponível em < http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp> Acesso em 27 fev. 2016.

apresenta falhas importantes, principalmente na segurança (as falhas de segurança serão abordadas no capitulo 4).

3.3.2 Teredo

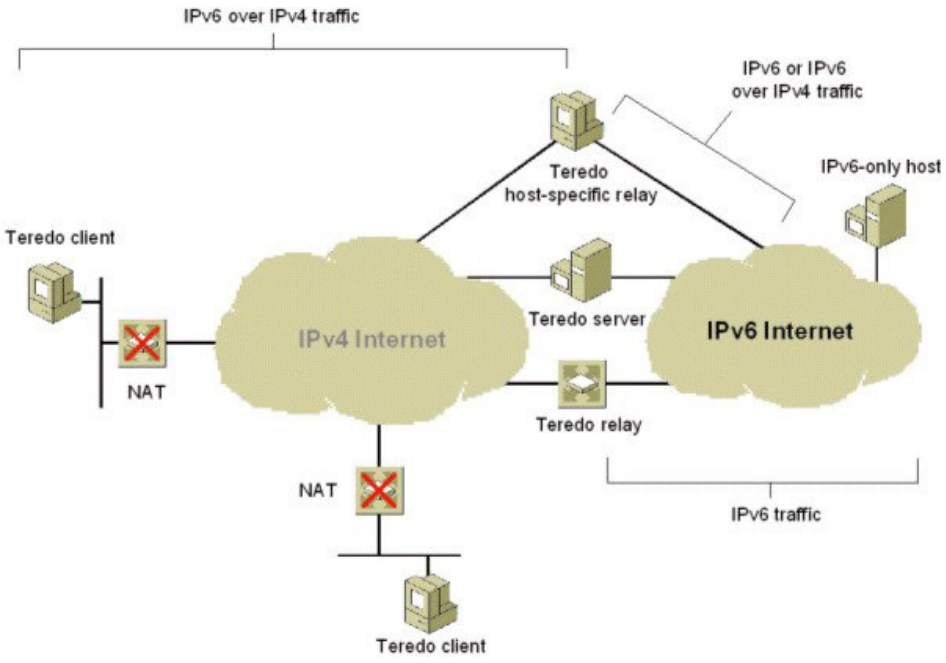
A técnica Teredo, citada e definida na RFC 4380, é um método de tunelamento com atribuição de endereços criada pela *Microsoft*. O mecanismo baseia-se na conectividade de nós localizados atrás de um ou vários tradutores de endereço de rede IPv4 (NAT) utilizando tunelamento em IPv4. A técnica é uma das formas utilizadas para usuários que desejam manusear o IPv6 sem autenticação, permitindo que o tráfego atravesse o NAT. Segundo Amoss e Minoli (2007), assim como o mecanismo 6to4, o método Teredo é uma tecnologia de encapsulamento, mas difere do 6to4 em alguns quesitos, como a tecnologia da sub rede que utiliza IPv4 ao NAT, ao contrário do 6to4 que utiliza IPv6, e o túnel, que origina-se no *host*, e não em um roteador 6to4.

O tunelamento 6to4 atua de boa forma quando existem roteadores 6to4 em sua rede. Conforme descrito, este usa endereços, encaminha-os ao roteador, e o mesmo encapsula e desencapsula os endereços. Logo, com ajuda de *relays* as redes IPv4 poderiam, portanto, possuir acesso ao tráfego IPv6. Porém, segundo Davies (2012, p. 347), "como muitas empresas utilizam nas redes o NAT aliado ao IPv4, e na maioria das configurações do NAT o dispositivo que possui tal serviço não é capaz de agir com um roteador 6to4, então surge a necessidade da utilização do Teredo para tunelamento, associando-se ao NAT". Para uma explicação sobre o uso do Teredo e o comportamento 6to4 em NAT, Amoss e Minoli (2007), citam que o 6to4 requer a atribuição de um endereço IP publico, quando utiliza mecanismos de implementação e em questão de tunelamento, o túnel 6to4 não utiliza protocolos TCP , UDP e ICMP, diferente do NAT. Tais dispositivos, portanto, que utilizam NAT poderiam causar problemas ao método 6to4.

O Teredo aborda as questões relacionadas com a falta de funcionalidade 6to4 na

> Internet, aos dispositivos e configurações de multicamadas NAT. (...) Mesmo que o mecanismo 6to4 fosse universalmente suportado em dispositivos na Internet, algumas configurações de conectividade contêm vários níveis de NAT. Portanto, para permitir que o tráfego IPv6 flua através de uma ou várias NAT's, o Teredo encapsula o pacote IPv6 como uma mensagem IPv4 UDP, contendo tanto um IPv4 e cabeçalho UDP. Estas mensagens UDP podem ser traduzidas pela maioria dos NATs e podem percorrer várias camadas do mesmo.(DAVIES, 2012, p. 348)

FIGURA 8 – Infraestrutura do Teredo



fonte: <https://technet.microsoft.com/en-us/library/bb457011.aspx>

Os elementos principais da arquitetura do Teredo segundo Davies (2012, p. 352), são divididos nos seguintes componentes:

• **cliente:** O cliente Teredo é um nó que suporta encapsulamento, servindo para outros clientes Teredo ou para nós IPv6 de uma rede. Este nó comunica-se com o servidor Teredo, a fim de obter um endereço para contribuir com a comunicação com outros clientes ou *hosts* na rede IPv6.

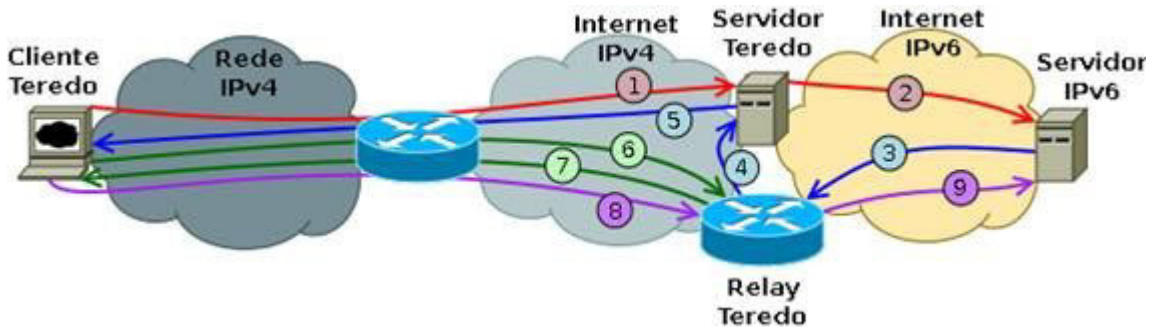
•**Servidor:** O servidor é a estrutura responsável por contribuir para a configuração do endereço de clientes Teredo possuindo suporte ao tunelamento, facilitando assim a comunicação entre

clientes e *hosts* IPv6.

•***Relay:*** O *relay* é um roteador IPv6 e IPv4 que pode encaminhar pacotes entre clientes Teredo na rede IPv4 (usando uma interface de encapsulamento Teredo) e na rede IPv6 (por *hosts* IPv6).

No mecanismo de funcionamento, o servidor inicia a conexão, baseando-se no NAT utilizado pelo cliente Teredo. Caso o nó final seja de IPv6 nativo, o *Relay* Teredo cria a interface que fica localizada entre o cliente e o caminho em que o nó irá seguir. Os servidores Teredo utilizam por convenção a porta UDP 3540 para comunicação. O *Relay* utilizado será sempre o que estiver mais próximo do nó de destino e não o mais próximo do cliente.[1]

FIGURA 9 - Estabelecimento de túnel Teredo



Fonte: <http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp>

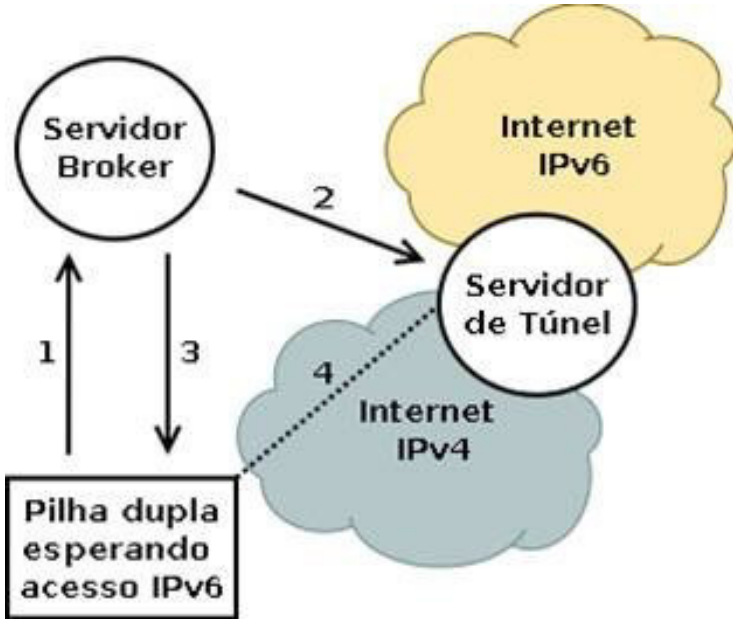
A técnica Teredo atrai, portanto, clientes que utilizam NAT e desejam possuir conexão ao IPv6 sem a autenticação. Porém não é uma técnica recomendada, pois além de não ser eficiente possui muitas falhas, tanto na estrutura quanto em segurança (Falhas de segurança do tunelamento Teredo serão abordadas no capitulo 4). Por padrão, em algumas versões do Windows o Teredo vem habilitado (como no Windows 7), sendo possível desabilita-lo no próprio Windows ou nas portas UDP 3544, que são as portas que fazem a comunicação dos nós.

1 TELECO. Redes IP II:Técnicas de transição de Tunelamento- Teredo. Disponível em <http://www.Teleco.Com.bt/tutoriais/tutorialredeip2/pagina_3.asp>. Acesso em 27 fev. 2016

3.3.3 Túnel Broker

O túnel broker, definido na RFC 3053, consiste em um método de tunelamento que permite a obtenção de conectividade IPv6 por meio de um túnel utilizando um provedor. Conforme a RFC 3053 (2001, p.2), "a ideia do túnel *broker* é uma abordagem alternativa, baseada na prestação de servidores para gerenciar automaticamente solicitações de tuneis vinda de usuários, vindo a ser útil para estimular o crescimento do IPv6".

FIGURA 10 - Topologia lógica do Túnel *Broker*



fonte: <http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp>

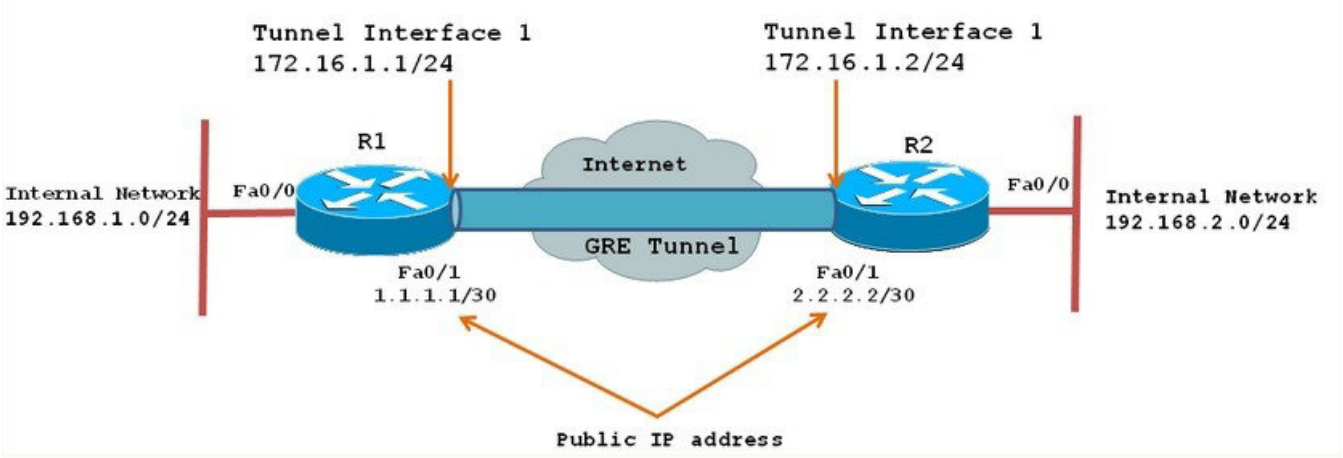
Os tuneis *brokers* são oferecidos por serviços na Internet (provedores). Para utilizá-lo, o usuário se cadastra neste serviço, e depois que o cliente tenha sido autorizado a acessar o serviço, o provedor cadastra-o, informando ao cliente parâmetros para criação do determinado túnel. Por fim o tunelamento é realizado. A utilização de *Tunnel Brokers* é recomendada para usuários domésticos e corporativos que querem testar o IPv6, ou começar um processo de implantação em

suas redes, mas cujos provedores de acesso à internet ainda não oferecem suporte ao novo protocolo.[1]

3.3.4 GRE

Túneis GRE são túneis citados na RFC 2784, que realizam a comunicação entre dois nós, permitindo o encapsulamento de vários tipos diferentes de protocolos. A tecnologia desenvolvida pela CISCO "possui configuração semelhante aos túneis manuais, permitindo que outros protocolos possam ser transportados pela rede, assim como o ISIS (*Intermediate System–to–Intermediate System*)". (GRAZIANI, 2012, p.347).

FIGURA 11 – Configuração do Túnel GRE



fonte: <https://supportforums.cisco.com/document/13576/how-configure-gre-tunnel>

No funcionamento do túnel, os pacotes originais recebem um cabeçalho: o GRE, junto com o cabeçalho IPv4. Os pacotes são então enviados para o IP de destino. Assim que chegam, os cabeçalhos são então removidos, restando apenas o pacote original que é devolvido ao destinatário. O túnel GRE é suportado na maioria dos sistemas operacionais e roteadores, e

1 TELECO. Redes IP II: Técnicas de Transição de Tunelamento-Tunnel Brokers. http ://www.Teleco.com. br/tutoriais/tutorialredeip2/pagina_3.asp. Acesso em 27 fev.2016

possibilita a criação de um link ponto a ponto. Assim como o *6over4,* sua configuração é manual, de modo que pode gerar um esforço na sua manutenção e gerenciamento proporcional à quantidade de túneis. [1]

3.4 Tradução

A tradução, citada na RFC 2765, consiste em um método de transição que permite "traduzir" tráfego IPv6 para o IPv4 ou o contrário. Conforme Amoss e Minoli (2007), o método da tradução tem como objetivo conservar endereços IPv4, isto porque trabalha de forma temporária, atribuindo endereços IPv4 /IPv6. Na tradução, os pacotes são convertidos para o destino, seja IPv4 ou IPv6.

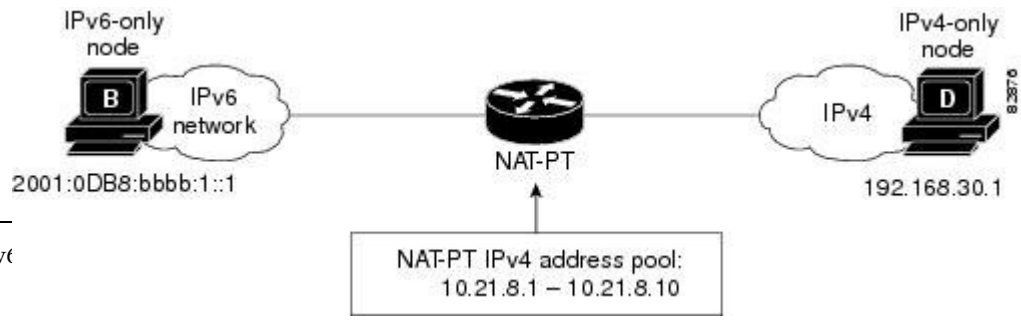
Existem dois métodos de Tradução especifica. NAT-PT E NAT64.

3.4.1 NAT-PT e a transição Ipv6

Conforme visto anteriormente, o protocolo NAT executa a tradução de endereços IP, permitindo que dispositivos se comuniquem com outros através de um endereço IP ou um número de endereços em quantidade bem pequena, diminuindo a escassez do endereçamento IPv4. O NAT modifica o endereço IP de origem por um de interface externa, ou seja, traduz um endereço IP interno não válido, por um válido e aceito na camada de rede.

Associado a transição IPv6, o NAT, agora sendo NAT-PT (*protocol translation*) permite a comunicação *host* IPv6 com *host* IPv4, combinando métodos de tradução.

FIGURA 12 – Estrutura do NAT-PT/Operação Dinâmica NAT -PT



1 IPv6

fonte:<http://www.cisco.com/c/en/us/td/docs/iosxml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

No funcionamento do NAT-PT com objetivo a transição, um determinado *host* de protocolo IPv6 envia o pacote em direção ao *gateway* NAT. Este faz o mapeamento do endereço recebido e o encaminha ao *host* IPv4. Antes de seguir para o *host* IPv4, o h*ost* IPv6 adiciona um prefixo ao endereço de destino IPv4 e o *gateway* realiza a tradução do protocolo IPv6 para o IPv4. Este prefixo que identifica o caminho pelo qual o pacote irá seguir.[1]

3.4.2 NAT64/DNS64

Com o inicio da transição IPv6, muitas vezes era necessário algum método que não "alterasse" os nós, mas sim mantê-los apenas utilizando a tradução. Conforme Davies (2012, p.377), "A IETF buscou métodos que envolvessem a tradução de IPv6 para o IPv4 e vice versa, vindo a definir essa necessidade com a combinação do NAT64 E DNS 64. "

O NAT64 é um método de tradução que utiliza como auxiliar o DNS64. Conforme a RFC 6147 (2011, p. 1), "o DNS64 é um mecanismo para a síntese de registros de recursos AAAA (RRS) de A RRS, utilizado como um conversor IPv6/IPv4 para permitir a comunicação entre o cliente IPv6 e um servidor IPv4, sem a necessidade de qualquer alteração nos dois nós, para a classe de aplicações que funcionam através do NAT". O DNS64 é, portanto, um "método de mapeamento para consultas de registros de endereços IPv6 ao IPv4, facilitando a comunicação entre os nós de ambas as redes (DAVIES, 2012, p. 296). Logo, para a comunicação das redes IPv6 e IPv4, o NAT64 necessita da técnica auxiliar de conversão DNS, que é a DNS64.

Conforme Davies (2012, p. 377), o NAT64 fornece as seguintes funções em uma rede:

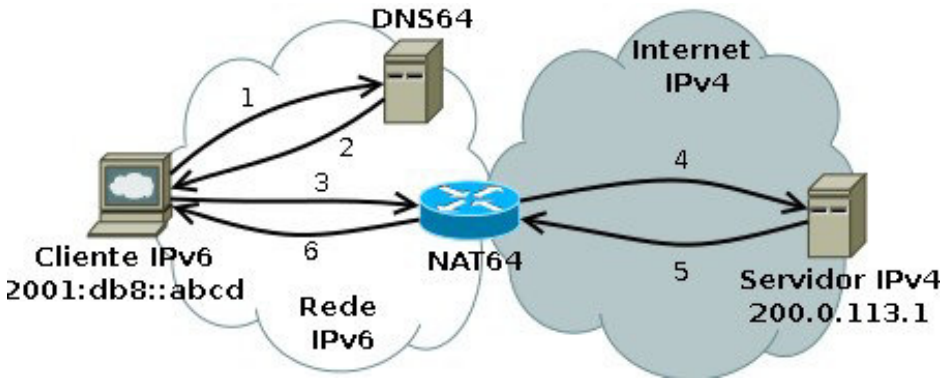
• **Registro de endereços**, para facilitar a comunicação IPv6 e IPv4. Através do mecanismo auxiliar DNS64, acontece a modificação do código de registro a forma AAAA (*host* IPv6) para

1 TELECO. Tradução. Disponível em <http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_4.asp>. Acesso em 28 fev.2016.

facilitar na comunicação do *host* IPv6, no qual manda o pacote "mascarado" ao *host* IPv4;

• **Tradução:** O NAT64 fornece tradução com o tráfego entre IPv6 e IPv4 quando este é iniciado por um nó IPv6. O NAT recebe então pelo tráfego IPv6 o nó e o converte em tráfego IPv4 para o nó IPv4.

FIGURA 13 - Topologia de rede do NAT64 / DNS64



Fonte: <http://ipv6.br/post/transição/>

No funcionamento do NAT64, uma determinada máquina com estrutura IPv6 tenta acessar a rede IPv4. O DNS64 recebe essa solicitação, convertendo o código de registro para o modelo AAAA(tipo de registro de DNS para endereços de *hosts* IPv6). Depois disso, o usuário envia o pacote para o *host* IPv4, que é então convertido pelo NAT64.

3.5 Desafios da transição

No projeto inicial do IPv6, uma vez que o protocolo estivesse pronto seria iniciado o processo da transição de forma gradual na internet, cujo funcionamento fosse em conjunto com o IPv4 em pilha Dupla ou em tunelamento (para casos em que o protocolo IPv6 não estivesse disponível em todos os sistemas autônomos seria necessário este método para prover acesso a conteúdo IPv6 em redes que ainda não suportem o protocolo durante a fase de transição). Com esse projeto, quando o IPv4 esgotasse o IPv6 já estaria em funcionamento na internet, implantado por pilha dupla em todo o mundo. Por fim o IPv4 poderia ser apenas desativado. Entretanto, não

foi dada a devida importância à transição, de forma que ainda são poucos os provedores que fornecem tráfego IPv6. Com o fim do IPv4 nos estoques regionais (RIRs), é provável que o IPV6 ainda não esteja em toda a internet, o que "forçaria" os provedores de acesso a usar CGN (NAT no provedor de acesso), entregando um IP privado para o cliente, ao invés de entregar um publico, como é feito atualmente.

Para Graziani (2012), a transição do IPv6 só deve ocorrer com uma serie de fatores que incluem o planejamento estratégico dos departamentos de TI, treinamento de equipes para que os profissionais estejam habilitados a implementar o protocolo; Testes de laboratório com manipulação do protocolo e equipamentos/dispositivos de suporte, como *softwares* de segurança, serviços, roteadores e *switches. O*s departamentos de TI devem começar com a preparação do IPv6 agora , isto porque a medida em que o protocolo IPv4 alcançar o potencial máximo e for se extinguindo, surgirão problemas de desempenho e disponibilidade de endereços.

Atualmente, não existe data prevista para que haja a total implantação do protocolo IPv6. A ISOC, organização de associados profissionais, que visa fortalecer evoluções técnicas na Internet, organiza o dia mundial do IPv6, em que incita provedores a testar implementações e a implantar permanentemente o novo protocolo para os serviços prestados, visto que existem ainda poucos provedores fornecendo o novo protocolo. Graziani (2012) afirma que atualmente não há prazos para a transição total do IPv6, por ser uma migração bastante complexa, e que apesar da transição do protocolo IPv4 para o IPv6 está em andamento, esta mesma provavelmente se prolongará por muitos anos.

> Cada uma dessas tecnologias de transição podem ser aplicadas e adequadas para uma tipo específico de cenário e aplicação. Cada tecnologia envolve compensações. Por exemplo, a implantação de uma rede de pilha dupla fornece a plena interoperabilidade com o protocolo IPv4, mas aumenta a complexidade de uma rede. Por outro lado, a implantação por tunelamento é simples, porem menos flexível e robusta (DUTTA, A et.al, 2006, p.2)

4 ASPECTOS DE SEGURANÇA NA TRANSIÇÃO PARA O IPv6

4.1 Segurança de redes

Um dos aspectos mais importantes do projeto de transição é a segurança da rede. Esta deve ser mantida de forma a evitar que sejam exploradas vulnerabilidades decorrentes do processo de mudança. A preocupação com a segurança em redes IPv6 não se resume apenas a redes que suportam IPv6 nativo, isso porque o tráfego IPv6 pode ser encapsulado em pacotes IPv4, permitindo que haja uma comunicação IPv6 passando pelo *firewall* IPv4, o que é especialmente arriscado em caso de túneis automáticos. O protocolo IPv4, bem como o IPv6 possuem vulnerabilidades conhecidas. Alguns dos mecanismos de transição, como o tunelamento, permitem que haja tráfego de dados sem o controle do *firewall*, por se utilizarem de conexão IPv4 para passar tráfego IPv6 e vice-versa, utilizando servidores *relay. D*essa forma, é importante conhecer os métodos de transição com o objetivo de evitar que esses métodos sejam usados de forma mal intencionada.

> É possível que haja ataques contra os mecanismos de transição para conseguir acesso a qualquer uma das partes do IPv4 ou IPv6. A segurança dos sistemas IPv6 devem ser avaliadas e ativadas em redes e sistemas, atuais ou futuros. Isso porque como os dois protocolos estão relacionados, as semelhanças entre os protocolos podem criar padrões de ataque similares.(HOGG; VYNCKE, 2008, p. 5)

Com o crescimento da Internet, muitos usuários possuem identidade desconhecida e isso acaba iniciando um ambiente onde redes tornam-se vulneráveis a ataques. O protocolo IPv4 possui falhas de segurança bem conhecidas, como a utilização do NAT para a expansão da Internet, o que acaba prejudicando a segurança de uma rede. Porém, o IPv6 também não escapa dos riscos da Internet, isto porque apesar do IPv6 ter corrigido falhas do IPv4, o mesmo possui ainda pouca utilização, podendo possuir novas falhas que poderão ser exploradas . O cenário de implantação dos protocolos também podem apontar determinadas falhas para qualquer um dos

protocolos, dependendo do cenário escolhido.[1] Logo, um dos grandes desafios na transição é aliá-la a uma rede segura, de forma a beneficiar e não expor os usuários que a utilizam.

4.1.1 Vulnerabilidades do IPv6

Como a implantação e implementação do protocolo IPv6 em redes é recente, o seu sistema não foi totalmente testado, necessitando de testes extensivos para avançar na transição. Conforme Hogg e Vyncke (2008, p.7), "Muitos grupos estão realizando testes de IPv6 para encontrar soluções antes de implantá-lo. No entanto os principais fornecedores de equipamentos de informática e *software* publicaram vulnerabilidades nas suas implementações".

As empresas e corporações que pretendem adotar a transição para o novo protocolo devem garantir a segurança com o objetivo a evitar ataques de rede, estando cientes de que existem alguns fatores de risco que podem deixar o sistema IPv6 em risco, como falta de *softwares* de segurança focados em IPv6, dificuldade em detectar acessos IPv6 desconhecidos ou não autorizados em redes IPv4 e a fragilidade de defesa no destino de uma rede, causado pela multiplicação dos tuneis de transição.[1]

> Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores com a finalidade de enviar mensagens e compartilhamento de equipamentos. Sob essas condições, a segurança nunca precisou de maiores cuidados. Porém como milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, arquivar impostos e fazer compras, a segurança das redes está desapontando no horizonte como um problema potencial. (TANENBAUM, 2003, p. 767)

Em redes IPv4, a IETF tinha interesse em definir um padrão de segurança que protegesse o protocolo. Conforme Tanenbaum (2003), a IETF sabia que existiam falhas de segurança na internet e rede IPv4 , logo o argumento para definir um padrão de segurança na rede era de que realizar a codificação em determinada camada não impediria que usuários

1 FTP. Registro.br. Capacitação IPv6 – Segurança em IPv6. Disponível em <ftp :// ftp. Registro .Br/pub/gter/gter 33 / Tutorial-IPv6-Seguranca.pdf. Acesso em 13 mar. 2016.

1 TELECO. Redes IPv6: Desafios para a Implantação. Disponível em: <http ://www.teleco.com.br/tutoriais/tuto rialipv6seg/pagina_4.asp>. Acesso em 14 mar.2016

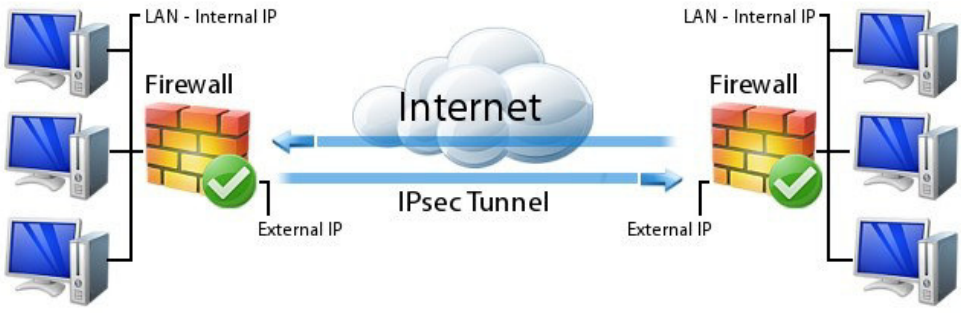
conscientes de segurança a implementassem na camada de aplicação, sendo que esse processo também poderia ajudar outros usuários com poucas preocupações em seguranças de redes.

A extensão dessa preocupação da IETF gerou então um projeto de protocolo para proteção de rede IPv4, que visava a privacidade e proteção do usuário. O projeto também seria altamente importante para o novo protocolo IPv6. Tratava-se do novo protocolo IPSec.

4.2 IPSec

O IPv4 foi criado sem preocupação com a segurança e privacidade. Desta forma os dados trafegam sem criptografia e os pacotes podem ser interceptados e lidos quando utilizando *sniffers* na rede. Para resolver esses problemas, foi definido na RFC 6071 e especificado em RFC 2401, 2402, 2406 e 2408 o protocolo IPSec, descrito como uma suíte de protocolos que fornece segurança à comunicações da Internet na camada IP. "Os principais serviços são sigilo, integridade de dados e proteção contra ataques de reprodução (conversação). Todos esses serviços se baseiam na criptografia de chave simétrica, porque o alto desempenho é importante". (TANENBAUM, 2003, p.821). O IPSec é portanto uma extensão de protocolo IP, que visa garantir segurança as comunicações entre computadores.

FIGURA 14 – Exemplo ilustrativo do túnel IPSec e VPN



fonte:<https://techlib.barracuda.com/display/bngv52/how+to+create+an+ipsec+vpn+tunnel+between+the+barracuda+ng+firewall+and+a+pfsense+firewall>

Com o IPSec é possível garantir a autenticidade dos pacotes recebidos com o uso dos protocolos auxiliares *Autentication Header* (AH), *Encapsulate Security Payload* (ESP) e *Internet key Exchange* (IKE) para prover criptografia, checagem de integridade do pacote, e evitar que o conteúdo do pacote possa ser lido por *sniffers*. Dependendo de qual protocolo IPSec é usado, o pacote original completo pode ser criptografado, encapsulado, ou ambos. O IPSec é utilizado principalmente para criar VPNs (*Virtual Private Networks*), e sua implementação torna-se mais complexa caso seja usada em conjunto com o NAT, pelo fato do endereço usado na comunicação com a internet ser diferente do IP do *host* de destino. Dessa forma, seu uso no IPv4 é bem restrito.

Conforme Tanenbaum(2003, p. 822), o IPSec pode ser utilizado de dois modos:

• **Modo de transporte**: No modo de transporte, o cabeçalho IPSec é inserido depois do cabeçalho IP(para informar que o cabeçalho IPSec foi incluído no IP, o campo *protocol* é alterado). Este cabeçalho contem informações de segurança, identificadores, número de sequência e verificações de integridade.

•**Modo de túnel**: Quando todo o pacote , juntamente com o cabeçalho é encapsulado em um novo pacote IP. Útil para casos do túnel terminar em um local diferente do destino final.

TABELA 3 – Funcionalidade do modo transporte e do modo túnel

	SA do modo túnel	SA do modo transporte
AH	Autentica todo o pacote de IP interno (cabeçalho interno mais payload de IP) mais partes selecionadas do cabeçalho de IP externo e cabeçalhos de extensão IPv6 externos.	Autentica o payload de IP e partes selecionadas do cabeçalho de IP e cabeçalhos de extensão IPv6.
ESP	Criptografa todo o pacote de IP interno.	Criptografa o payload de IP e quaisquer cabeçalhos de extensão IPv6 após o cabeçalho ESP.
ESP com autenticação	Criptografa todo o pacote de IP interno. Autentica o pacote de IP interno.	Criptografa o payload de IP e quaisquer cabeçalhos de extensão IPv6 após o cabeçalho ESP. Autentica o payload de IP, mas não o cabeçalho de IP.

Fonte: STALLINGS, Willian. Criptografia e seguranças de redes- princípios e praticas. São Paulo: Pearson Prentice Hall, 2008, p.354.

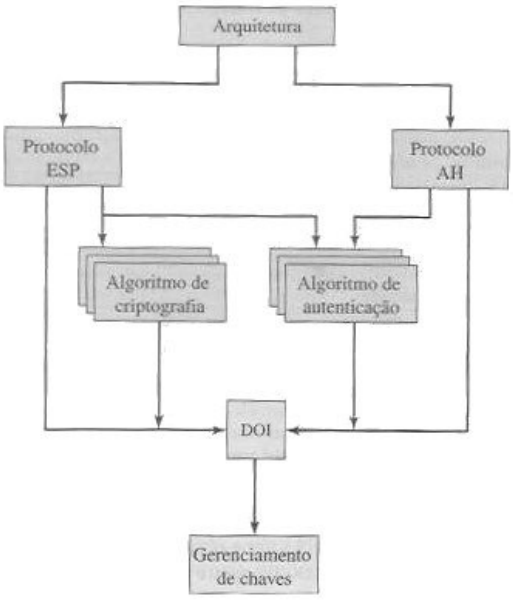
Tanto o cabeçalho de autenticação(AH), quanto o encapsulamento de segurança do

payload (ESP) admitem os dois usos.

Inicialmente a implementação do IPSec seria mandatória no IPv6, se aproveitando do fato de (por ter um espaço de endereçamento muito maior que o IPv4) ter sua implementação facilitada pela ausência do NAT. Porém, a obrigatoriedade do IPSec foi retirada das especificações mínimas de implementação do IPv6 devido ao fato de necessitar muito processamento, o que acabaria dificultando sua implementação em dispositivos embarcados que teriam seu custo de produção aumentado para ter suporte a IPSec.

"As especificações do IPSec aparecem divididas em RFC's e em documentos publicados pela IP *Security Protocol Working Group*, sendo estabelecidas pela IETF. Nesses documentos constam os grupos que caracterizam o suporte ao IPSec".(STALLINGS,2008,p. 351). Esses documentos são divididos em sete grupos, caracterizando a estrutura IPSec. Segundo Stallings são definidos como (2008, p. 351):

FIGURA 15 – Visão geral do documento IPSec



Fonte: STALLINGS,Willian. Criptografia e seguranças de redes- princípios e praticas. São Paulo: Pearson Prentice Hall, 2008.

• **Arquitetura**: onde constam os conceitos gerais, mecanismos e requisitos do IPSec;

• **encapsulamento ESP:** Abrange o formato de pacote e questões relacionadas ao uso do ESP para criptografias de pacote;

• **Autenticação do cabeçalho AH:** abrange o formato de pacote e questões relacionadas ao uso do AH para autenticação de pacotes;

• **Algoritmo de criptografia:** a descrição do funcionamento dos algoritmos de criptografia para a ESP;

•**algoritmos de autenticação:** a descrição do funcionamento dos algoritmos de autenticação utilizados para a AH;

•**Domínio de interpretação**: inclui os identificadores de algoritmo aprovados para criptografia e autenticação, parâmetros operacionais e valores utilizados para a relação dos outros documentos do IPSec.

Há dois protocolos IPSec utilizados como cabeçalhos na segurança: *Authentication Header* e o *Encapsulating Security Payload*.

4.2.1 Authentication Header

O protocolo *Authentication Header* (AH) proporciona a autenticação, integridade da origem dos dados e a proteção de repetição. No entanto, o AH não proporciona a confidencialidade , o que significa que todos os dados são enviados sem proteção.

O AH assegura a integridade dos dados pela soma de verificação gerada pelo código de autenticação de uma mensagem, como por exemplo, o MD5. Para garantir a autenticação da origem dos dados, o AH inclui uma chave partilhada secreta no algoritmo que utiliza para a autenticação. Para garantir a proteção de repetição, é utilizado um campo de número de sequência dentro do cabeçalho. De forma simplista, o AH assegura que nada interfira com os dados em trânsito para o terminal.

> O cabeçalho de autenticação oferece suporte para integridade de dados e autenticação dos pacotes IP. Essa integridade garante que a modificação não detectada do conteúdo

> de um pacote em trânsito não seja possível. A autenticação permite que um sistema final ou dispositivo de rede autentique o usuário ou a aplicação e filtre o tráfego adequadamente.(STALLINGS, 2008, p.355)

Apesar do AH autenticar o maior número possível de datagramas IP, os valores de determinados campos no cabeçalho IP não podem ser previstos pelo destinatário. O AH não protege estes campos, que são conhecidos como campos variáveis. No entanto, o AH protege sempre a carga útil do pacote IP.

4.2.2 *Encapsulating Security Payload*

O ESP fornece autenticação dos dados de origem, integridade de dados, proteção anti-repetição, e a opção de confidencialidade para pacotes IP. O ESP no modo transporte não protege o pacote completo com uma soma de verificação criptográfica. O cabeçalho IP não é protegido. Em modo túnel, encapsula e protege o pacote original completo, incluindo o cabeçalho IP (mas não o cabeçalho IP externo). Conforme a RFC 4303(2005, p.3), "o ESP pode ser usado para garantir a confidencialidade, os dados de autenticação, a integridade sem conexão, e serviços para fluxo de confidencialidade (limitado) de tráfego."

O ESP é o único protocolo que pode ser usado através do NAT. O IKE automaticamente detecta a presença do NAT e propõe encapsulamento UDP-ESP para que o tráfego IPSec passe pelo servidor NAT.

> Considerando que a ESP pode fazer tudo que o AH pode fazer e muito mais, além de ser mais eficiente durante a inicialização, surge a questão: afinal, qual é a necessidade do AH? A resposta é principalmente histórica. No inicio, o AH cuidava apenas da integridade, enquanto a ESP tratava do sigilo. Mais tarde, a integridade foi acrescentada a ESP, mas as pessoas que projetaram o AH não queriam deixa-lo morrer depois de tanto trabalho. No entanto, o único argumento real dessas pessoas se baseava no fato de que o AH é capaz de verificar uma parte do cabeçalho IP o que o ESP não faz.
> (TANENBAUM, 2003, p. 825)

4.3 Vulnerabilidades do NAT

Conforme visto, o NAT é uma tecnologia que permite a tradução de endereços IP privados (não roteáveis) para endereços válidos (roteáveis), de forma que um endereço, ou um grupo de endereços IP sejam compartilhados entre inúmeros dispositivos, sendo que um servidor ou dispositivo NAT será o responsável por encaminhar os pacotes para o dispositivo que solicitar cada conexão. Os dispositivos que estão sob um servidor NAT não podem ser identificados individualmente na internet, por isso, pra se saber de qual dispositivo partiu alguma solicitação, é necessário fazer logs de acesso do servidor NAT para ter real controle dos acessos.

A segurança de uma rede usando NAT se resume ao fato do NAT ocultar a topologia da rede, funcionando assim como um *firewall stateful*, pois só aceita a entrada de pacotes solicitados previamente. Porém não é uma segurança confiável, pois não há filtragem de pacotes. Alguns métodos de transição que utilizam tunelamento de IPv6 em redes IPv4 por exemplo, podem permitir que um dos clientes da rede que utilize por exemplo, um cliente Teredo, fique exposto na rede IPv6 ,isso porque caso o *firewall* não esteja configurado pra bloquear túneis Teredo ou 6to4 e mesmo que essa rede não suporte nativamente o IPv6, o cliente corre o risco de ficar fora do controle do *firewall* IPv4.

Servindo como um método de tentar reduzir o consumo de endereços IP, o NAT é utilizado em redes domésticas, redes corporativas e está começando a ser utilizado inclusive em provedores, sendo esse uso chamado de CGN (*Carrier Grade NAT*), que consiste na entrega de IP privado para o cliente do provedor. O uso de NAT possui várias implicações, e portanto é necessário a manutenção de uma tabela de tradução de endereços. No caso do CGN é necessário 2 tabelas de tradução, o que gera o custo adicional de memória e processamento da busca nessa tabela, reduzindo o desempenho da rede.

Como cada IP válido pode usar cerca de 65536 portas, o compartilhamento desse IP entre vários *hosts* da rede privada gera uma série de limitações, como a quantidade de conexões ou até o não funcionamento de alguns serviços. As aplicações *web* precisam de adaptações para

conseguirem se comunicar através do NAT. Por causa dos motivos apresentados a implementação do NAT e CGN só é recomendada como forma de manter os sistemas IPv4 funcionando enquanto é posto em prática e em paralelo o projeto de implantação do IPv6 em pilha dupla, para assim resolver a dificuldade da falta de IP's sem prejudicar o funcionamento das aplicações que porventura estejam sendo utilizadas no ambiente de produção onde será feita a transição de protocolo IP.

4.4 Vulnerabilidade 6to4

O método 6to4 é um técnica muito utilizada na hora da transição. Entretanto, apesar de ser uma técnica utilizada em grande proporção na internet, a mesma apresenta falhas importantes. A característica dos ataques ao 6to4 baseia-se no seu mecanismo de funcionamento, isso porque como o 6to4 recebe trafego IPv4/IPv6 de qualquer lugar, é provável que acabe sofrendo ataques pela falta da verificação de identidade desse tráfego.

Segundo Gadong e Darussalam(2008, p. 8), ” Mesmo que o sistema 6to4 seja adequadamente implementado, ele também representam ameaças à segurança.” Conforme Gadong e Darussalam as ameaças são:

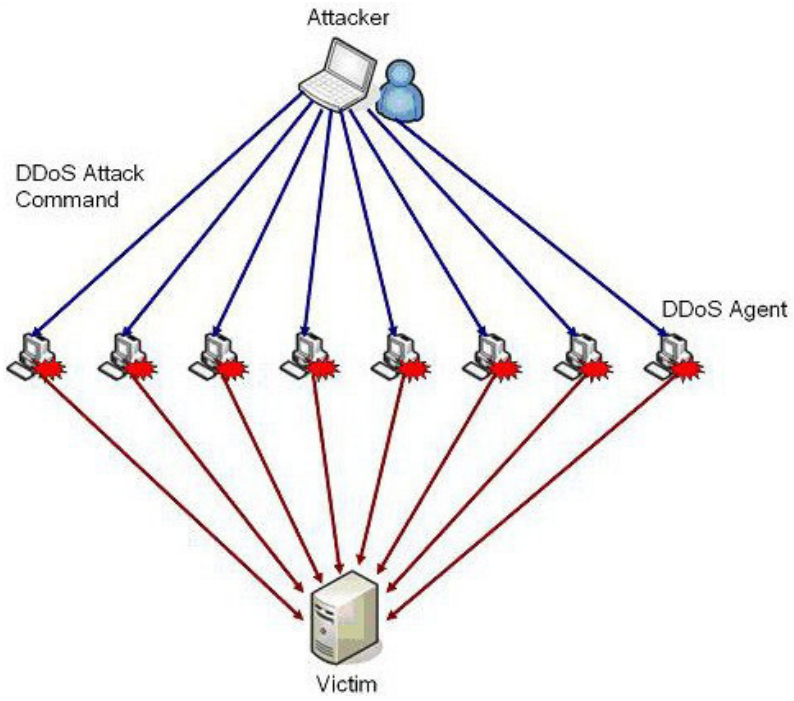
• **DoS *attack:*** O Dos *attack* (ou ataque de negação de serviços) consiste em um tipo de ataque em que uma determinada máquina recebe requisições em uma quantidade tão grande que sobrecarrega. Caracteriza-se em tentativas que impedem computadores comuns ou principalmente servidores de executarem tarefas. Ao contrário do vírus, o DoS *attack* não infecta uma máquina, mas sim visa esgotar o funcionamento da mesma através da sobrecarga de requisições, gerando lentidão em um serviço, até este se tornar indisponível. Isso força o usuário a desligar, ou reduzir os serviços de forma que atrapalha a comunicação entre tarefas.

• **Reflection Denial-of-Service (DoS) attacks:** nesse caso um nó malicioso “reflete” o tráfego dos outros nós para um único nó que deseja atacar. Isso faz com que o nó atacado e os outros nós

tenham falhas para se comunicar pela sobrecarga ao nó atacado.

• **Roubo de serviço**, no qual um nó, site ou usuário mal-intencionado pode fazer uso não autorizado do serviço.

FIGURA 16 – Exemplo do ataque DoS



fonte: <http://omegasecure.com/blog/>.

As grandes vulnerabilidades no 6to4 existem pelo fato que os roteadores não são capazes de identificar se os *relays* são seguros. *Relays* públicos podem então sofrer ataques DoS e ataques de reflexão de nós. Essa utilização dos *relays* não privados também pode ocasionar outras falhas, como mau funcionamento aos serviços, isso porque não existe um controle especifico destes *relays* , o que acaba vulnerabilizando a estrutura 6to4 .

Por recomendação, é necessário desativar o 6to4 de redes corporativas, bloqueando-o com *firewall. O* impasse do 6to4 é que muitos usuários sofrem risco porque utilizam computadores que utilizam tuneis 6to4 sem o conhecimento. Logo estes usuários devem

desativar as funções de tunelamento 6to4 a fim de evitar consequências causadas pelos ataques na rede. Conforme a RFC 3964 - *Security Considerations for 6to4* (*2004*, p.19), " os nós 6to4 e IPv4 podem acessar nós IPv6 nativos através dos *relays* 6to4. Esses *relays* desempenham um papel crucial em qualquer ataque contra nós IPv6 por nós IPv4 ou nós 6to4". Logo, os *relays* minimizam os problemas da rede com mecanismo 6to4.

4.5 Vulnerabilidade Teredo

Como a utilização da técnica Teredo permite que nós atrás do NAT obtenham conectividade IPv6, a grande preocupação é se esses nós irão sofrer ataques em uma rede. Devido a sua arquitetura e diversidade de nós, o Teredo torna-se suscetível a muitos ataques. Conforme a RFC 4380 (2006, p.38), "os nós Teredo podem utilizar os serviços IPSec, como o AH ou ESP. Esses serviços tem um efeito positivo, no entanto a análise de segurança deve ter em vista os efeitos negativos dos serviços Teredo". Esses efeitos negativos , segundo a RFC são o DoS attack, falsificação de servidores Teredo, e outros ataques potenciais destinados a negarem serviços a um cliente. Uma outra preocupação do mecanismo Teredo é que usuários de algumas versões do Windows possuem por padrão o Teredo habilitado. Muitos nem tem o conhecimento da ativação do Teredo, então ficam mais vulneráveis a ataques. Por recomendação, o Teredo deve ser desabilitado de redes, em especial as corporativas. Usuários do Windows podem desabilitá-lo no próprio sistema ou através das portas UDP 3544, que são responsáveis pela comunicação do mecanismo[1].

> O transporte de pacotes IPv6 dentro de IPv4 por túneis tem poucos ou nenhum recurso de segurança. Estes são propensos a injeção de túneis (uma pessoa de fora pode injetar pacotes no túnel, o que poderia levar a um ataque *Reflection DoS*. Alguns desses túneis (Teredo, ISATAP e 6to4) estão habilitados em alguns sistemas, acrescentando ao IPv6 ameaça latente através da ligação com o IPv4. VLAN ACLs (*Virtual lan access control list*) podem aproveitar a rede para bloquear todo o tráfego, e as configurações podem também ser utilizadas para desativar esses túneis .
> (HOGG; VYNCKE, 2008, p. 463)

1 IPv6.net. TRANSIÇÃO. Disponível em <http://ipv6.br/post/transicao/>. Acesso em 19 mar.2016.

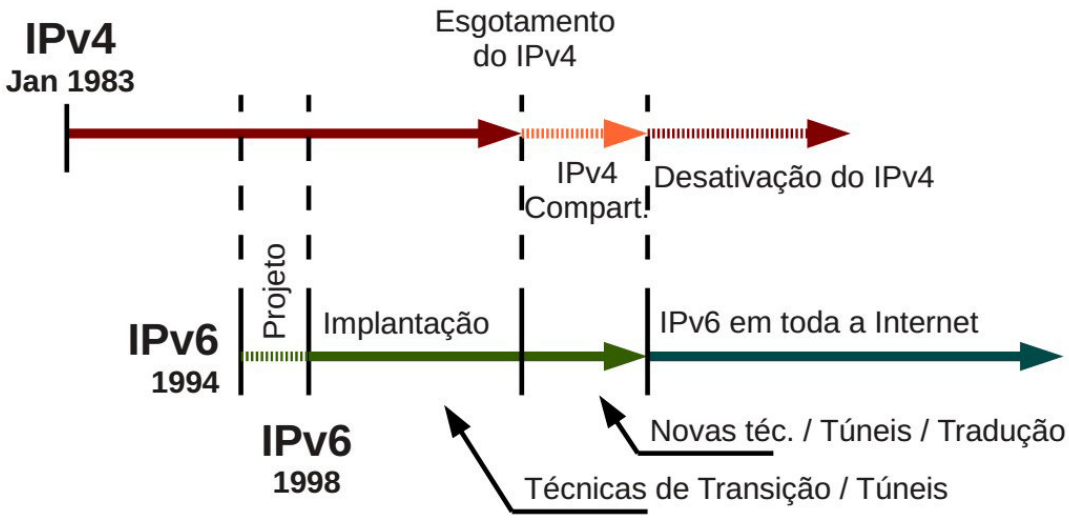
Segundo Hogg e Vyncke(2008), é muito difícil assegurar ameaças do Teredo , devido aos seus *relays* que são dinamicamente selecionados pelos *hosts* IPv6 e poderiam estar fora do domínio Teredo. O problema aumenta principalmente para usuários de algumas versões do Windows, que possuem o Teredo habilitado por padrão. Usuários desses sistemas estão, portanto correndo riscos , através de, por exemplo, livre fluxo de pacotes desconhecidos.

5 ESTUDO DE CASO

5.1 Implementação segura de redes

Para garantir a segurança das redes de computadores, dado as vulnerabilidades causadas pelos métodos de transição, temos que avaliar cada cenário de rede (apenas IPv4, apenas IPv6, e pilha dupla), para através do *firewall* tornar a rede segura contra ataques que se utilizem dos métodos de transição. No caso de pilha dupla, é necessário que o *firewall* suporte IPv4 e IPv6, e tenha as regras para bloquear ataques em ambos os protocolos. O presente estudo visa expor e analisar as vulnerabilidades decorrentes da transição IPv6, bem como listar as suas possíveis soluções. [1]

FIGURA 17 - Processo de implantação atual do IPV6/Novo plano de transição



Fonte:<http://ipv6.br/media/arquivo/ipv6/file/60/ApostilaIPv62012.zip>

1 Na abordagem deste estudo serão vistas as vulnerabilidades geradas pelo protocolo IPv6 e pelos seus métodos de transição. Não serão tratadas, portanto, as vulnerabilidades exclusivas do protocolo IPv4.

5.1.1 Analise e interpretação de dados

Para a seguinte pesquisa será demonstrada a configuração de firewall, e através de *scripts* procede-se a analise e interpretação de dados.

5.1.2 analise das soluções

Cada técnica será exposta com suas respectivas falhas e métodos utilizados para solucionar os impasses ocorridos em cada uma das etapas de implementação do IPv6, a partir da transição de uma rede originalmente IPv4.

5.2 Etapa 1: Garantir a segurança de uma rede IPv4 em relação aos métodos de tunelamento

Devido às técnicas de tunelamento de tráfego IPv6 no IPv4 é necessário que se analise cada técnica de tunelamento e sejam criadas regras de *firewall* para bloquear possíveis ataques. Mesmo em redes em que não hajam planos de implantar IPv6, é necessário garantir a segurança em relação às seguintes vulnerabilidades:

5.2.1 Teredo

Para evitar a abertura de túneis Teredo em uma rede com *firewall* há duas abordagens: O bloqueio de trafego bidirecional, e o bloqueio da porta de conexão Teredo. No bloqueio de tráfego bidirecional para os *relays* teredo, os principais *relays* são: *teredo.ipv6. microsoft.com*, *teredo. remlab. net, teredo2.remlab.net, debian-miredo.progsoc.org, teredo.ginzado.ne.jp e teredo.iks-jena.de.*

No *firewall iptables* há 3 regras de bloqueio de tráfego:

- **INPUT:** utilizada quando o destino final é a própria máquina filtro;
- **OUTPUT:** qualquer pacote gerado na máquina filtro e que deve sair para a rede.
- **FORWARD:** qualquer pacote que atravessa o filtro, oriundo de uma máquina e direcionado a outra.

Sendo assim, para cada servidor serão adicionadas 3 regras no *script* do *firewall*, ficando

da seguinte forma:

```
iptables -A OUTPUT -d teredo.ipv6.microsoft.com -j DROP
iptables -A FORWARD -d teredo.ipv6.microsoft.com -j DROP
iptables -A INPUT -s  teredo.ipv6.microsoft.com -j DROP
iptables -A OUTPUT -d teredo.remlab.net -j DROP
iptables -A FORWARD -d teredo.remlab.net -j DROP
iptables -A INPUT -s  teredo.remlab.net -j DROP
iptables -A OUTPUT -d teredo2.remlab.net -j DROP
iptables -A FORWARD -d teredo2.remlab.net -j DROP
iptables -A INPUT -s  teredo2.remlab.net -j DROP
iptables -A OUTPUT -d debian-miredo.progsoc.org -j DROP
iptables -A FORWARD -d debian-miredo.progsoc.org -j DROP
iptables -A INPUT -s  debian-miredo.progsoc.org -j DROP
iptables -A OUTPUT -d teredo.ginzado.ne.jp -j DROP
iptables -A FORWARD -d teredo.ginzado.ne.jp -j DROP
iptables -A INPUT -s  teredo.ginzado.ne.jp -j DROP
iptables -A OUTPUT -d teredo.iks-jena.de -j DROP
iptables -A FORWARD -d teredo.iks-jena.de -j DROP
iptables -A INPUT -s  teredo.iks-jena.de -j DROP
```

Como é possível criar outros *relays* Teredo, ou mesmo pode ocorrer de algum vírus redirecionar o tráfego teredo para outro servidor (por exemplo, alterando o arquivo *hosts* no sistema), convém bloquear a porta padrão de conexão do Teredo, que é a porta UDP 3544 (método de bloqueio da porta de conexão Teredo).

A porta pode ser então bloqueada com a seguinte regra:

```
iptables -A INPUT -p udp --dport 3544 -j DROP
iptables -A OUTPUT -p udp --dport 3544 -j DROP
iptables -A FORWARD -p udp --dport 3544 -j DROP
```

5.2.2 6to4 e tuneis broker

O 6to4 é outra forma de túnel automático que permite conexão através de um *firewall* IPv4. Para efetuar seu bloqueio, devemos levar em consideração que os pacotes IPv6 encapsulados em pacotes IPv4 transitam com o campo *protocol* do cabeçalho do IPv4, contendo o numero 41, o que é caracterizado como código do protocolo de encapsulamento (o mesmo

utilizado em tuneis *broker).* Basta bloquear, portanto, a entrada, saída e o redirecionamento desses pacotes no *firewall* com as seguintes *chains* no *iptables*:

```
iptables -A INPUT -p 41 -j DROP
iptables -A OUTPUT -p 41 -j DROP
iptables -A FORWARD -p 41 -j DROP
```

5.3 Etapa 2: implantação da segurança IPv6 e coexistência com o protocolo IPv4

Nessa etapa haverá a coexistência entre os protocolos, logo a rede funcionará em pilha dupla com o *firewall* IPv4 aplicando as regras descritas anteriormente, e o *firewall* IPv6 tratará das regras descritas a seguir para garantir a segurança de ambos os protocolos.

Nem o protocolo IPv4 nem o IPv6 tem como foco a segurança de redes, pois esses protocolos fornecem apenas o endereçamento. Por isso, alguns recursos que podem facilitar a implementação do IPv6 ou formas de implementação do protocolo podem gerar vulnerabilidades na rede. Não existem redes 100% seguras, entretanto algumas boas praticas que serão sugeridas a seguir terão como foco tratar as vulnerabilidades conhecidas do protocolo, já que pelo fato do IPv6 não estar totalmente implementado em todo o mundo, outras vulnerabilidades poderão ser conhecidas no futuro.

5.3.1 Neighbor Discovery Protocol-NDP

O Protocolo de descoberta de vizinhança, serve tanto pra passar informação aos nós sobre os roteadores que estão disponíveis na rede, quanto para checar se algum endereço existe na mesma. Nas redes com autoconfiguração, disponibiliza as informações necessárias para que o nó se configure automaticamente.

Sempre que um nó entra na rede, este envia uma mensagem *Neighbor Solicitation* para saber se o IP a ser configurado já existe na rede. O problema disso é que outro nó pode por exemplo, interceptar esse *neighbor solicitation*, e falsificar o *router advertisement,* fazendo com que o nó que está se conectando a rede não consiga obter IP por detectar que o endereço está duplicado. Sendo assim, um ataque do tipo negação de serviço pode impedir a obtenção de um

endereço IPv6 válido.

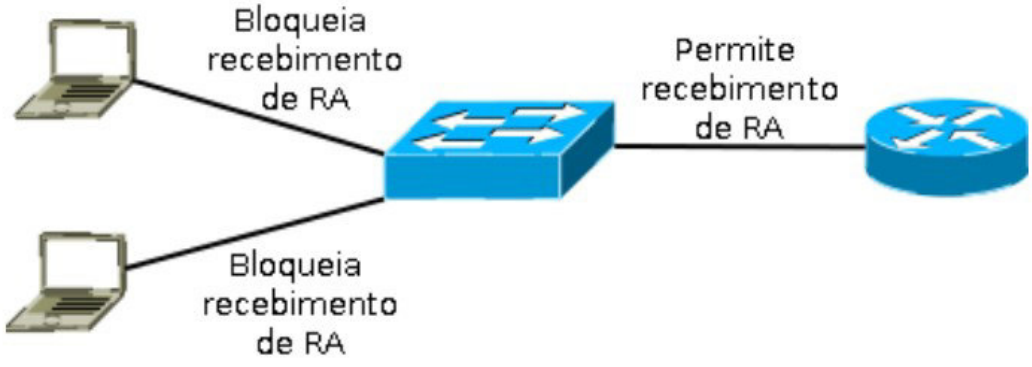
No NDP também há o *Router Advertisement*, sendo uma mensagem enviada automaticamente pelo router, ou mediante solicitação (*router solicitation*). Em uma rede sem implementação de segurança, um nó pode interceptar um *Router Solicitation* e responder com um RA indicando seu endereço como router, fazendo com que o nó fique com uma configuração que possui um *router* falso, o que pode interceptar todas as informações que saírem desse nó.

Para dar mais segurança ao NDP foi criado o SEND (*Secure Neighbor Discovery),* que consiste em obrigar a existência de uma assinatura RSA tanto no Neighbor Advertisement quanto no Router Advertisement, de forma a evitar ataques de negação de serviço no NA e falsificação de RA. Entretanto, para que funcione com segurança é necessário estar implementado em todos os nós da rede.

É possível monitorar e detectar ataques acompanhando as mensagens NDP a partir do *NDPmon*, que é um software de diagnostico que analisa os pacotes icmpv6 e reporta ao administrador. Ou por outras ferramentas como via syslog e *email* para que o administrador possa identificar e tomar providencias em relação aos ataques feitos usando o NA ou o RA.

No caso do *Router Advertisement*, como apenas os roteadores necessitam enviar o RA, então a abordagem para evitar a falsificação da mensagem RA consiste no uso do *RAGuard. O RAGuard* é, então implementado a nível de *switch* gerenciável, bastando bloquear RA em todas as portas, com exceção das portas confiáveis onde os roteadores estão conectados.

FIGURA 18 - Funcionamento do RA Guard



Fonte: <http://ipv6.br/media/arquivo/ipv6/file/58/Slides_Campus.zip>

5.3.2 Segurança do conteúdo trafegado

Em qualquer rede de computadores, o conteúdo trafegado na rede é sujeito a interceptação, e se não estiver criptografado é possível que outro nó da rede tenha acesso a sua informação. Para evitar isso, no caso do IPv6, há o protocolo IPSec que provê a criptografia dos pacotes trafegados na rede, dificultando que o mecanismo de ataque consiga ler as informações trafegadas, já que apenas o nó receptor terá a chave pra descriptografar os dados da conexão.

5.3.3 Varredura de rede

Para ocorrer um ataque a um determinado nó o mecanismo de ataque precisa necessariamente saber o endereço do nó que será vitima do ataque. Nesse ponto, o IPv6 possui uma vantagem em relação ao IPv4, pois uma rede IPv6 pode ter no mínimo 2^{64} endereços IP por subrede (seguindo a proposta do IPv6 de entregar no mínimo uma rede /64 para redes locais pois é o mínimo necessário para que o recurso de autoconfiguração *stateless* funcione), enquanto que no IPv4 o menor espaço de endereçamento entregue pra redes locais é o de /24, o que dá apenas 2^8 endereços IP. Isso faz com que uma varredura numa rede IPv4 possa ser muito mais rápida, enquanto numa rede IPv6 a demora da varredura fará esse ataque ser praticamente inviável caso não se procure um meio de reduzir o espaço de busca.

Na autoconfiguração *stateless,* a principio é utilizado o endereço MAC da placa de rede para geração do endereço IPv6. O problema dessa abordagem é o fato de que o endereço MAC possui seus primeiros 24 *bits* destinados a identificação do fabricante, o que pode ser conhecido facilmente por um mecanismo de ataque, sendo usado pra restringir o espaço de busca a varredura dos 24 *bits* finais, ficando assim equivalente a fazer a varredura de uma rede IPV4 classe A (2^{24} endereços).

Devido a identificação, os endereços gerados automaticamente a partir do MAC facilitam

a rastreabilidade do dispositivo, pois qualquer rede que se conecte por esse método, terão os mesmos 64 bits finais. Entretanto para solucionar a questão da privacidade e também dificultar uma varredura inteligente da rede a partir da autoconfiguração *stateless* é recomendável usar endereços gerados aleatoriamente, ou então usar endereços gerados criptograficamente (no SEND os endereços são gerados a partir de um *hash* da chave publica, e assim os 64 bits finais variam entre redes distintas, variando a cada vez que a chave publica muda).

Outra forma de evitar a varredura de rede é usar apenas endereços do tipo link-local (equivalentes aos endereços privados do IPv4) para o caso de dispositivos que precisam se conectar apenas na intranet. Isso evita que nós fora da intranet consigam acessar o nó pertencente a intranet, por ser um endereço não roteável. Também é possível usar as extensões de privacidade (RFC 4941) para que os endereços *stateless* sejam alterados de acordo com um período de tempo pré determinado.

5.3.4 Segurança em relação a conexões entrantes

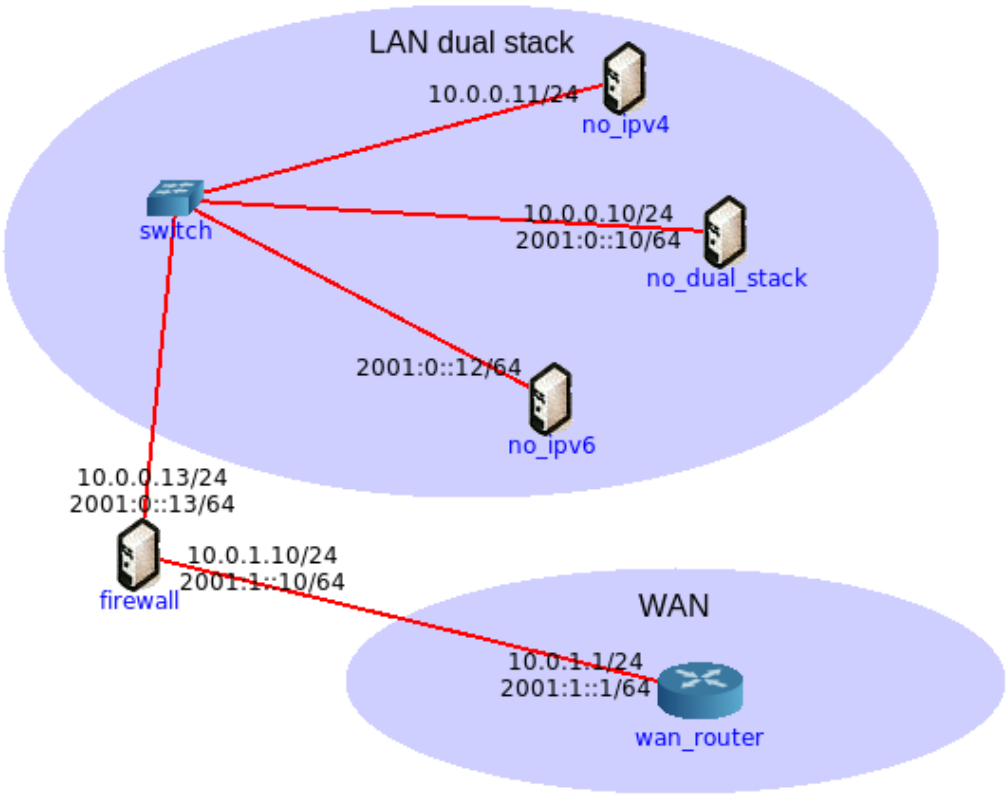
No IPv6 todos os nós conectados a internet terão endereços válidos; Não serão mais mascarados por NAT pois não há necessidade. Apesar do NAT não ser um mecanismo de segurança, muitos administradores de rede se acostumaram a usá-lo para ocultar a topologia da rede e assim, fornecer um nível de segurança maior do que teria se o nó fosse totalmente exposto.

Com esse cenário de existir 1 endereço válido por nó, é necessário um controle de segurança que pode ser feito utilizando *firewall* e sistemas de detecção de intrusão, que serão necessários em toda rede onde a segurança for requerida. A segurança pode ser feita através de bloqueio de conexões e portas que não são necessárias para o nó da rede.

> Na rede IPv4, devido à escassez de endereços válidos na empresa (e no mundo), utiliza-se NAT para endereçar os dispositivos localizados na área de Serviços e Clientes Internos. Já com o protocolo IPv6, todos os dispositivos receberam endereços globais roteáveis na Internet, permitindo conexões entrantes. Contudo, é preciso configurar o *firewall* IPv6 no roteador dessas redes corretamente para que apresente um comportamento semelhante ao NAT em relação às conexões entrantes, ou seja, permitir

apenas o encaminhamento de pacotes que sejam relacionados a requisições internas da rede corporativa. (IPV6.Br..Segurança sem NAT- Parte 2 . 2013, slide 36)

FIGURA 19 - Topologia de uma rede em pilha dupla com *firewall*- Ferramenta CORE



Fonte: SILVA, Salviano Lima (2016)

5.4 Etapa final: Rede apenas IPv6

Nessa etapa todas as regras do *firewall* IPv6 ficarão ativas da forma descrita nesse capítulo. Haverá apenas a desativação do protocolo IPv4 na rede, pois nessa etapa já será desnecessário tanto o IPv4 quanto o *firewall* IPv4.

Com o término dessa fase estará concluído a fase de transição entre IPv4 e IPv6.

6 CONSIDERAÇÕES FINAIS

O protocolo IPv4 manteve-se em utilização na Internet, e este uso, que não foi projetado para resolver grandes limitações no futuro, acabou gerando falhas atuais. O desenvolvimento de soluções, visando diminuir o esgotamento IPv4 incluiu em primeira fase métodos provisórios, que apesar de não resolverem as falhas da grande demanda, conseguiram contribuir como o desenvolvimento do projeto IPv6.

O desenvolvimento IPv6 era então visto como modelo para disponibilizar e aperfeiçoar soluções para as falhas IPv4. O resultado deste desenvolvimento era o surgimento de uma nova tecnologia a se resolver a falta de endereços IP. Entretanto, para a implantação deste novo mecanismo é necessário o estudo de casos, vulnerabilidades e tipagens de uma rede. A união desses modelos de estudos para analise entram nos quesitos de segurança da transição. Afinal, a transição era algo a ser altamente discutido, porém tal mudança deveria ser analisada antes de qualquer implantação.

Diante disso, os métodos de transição possuem o papel fundamental para auxiliar a mudança necessária de protocolos. Em um período de transição inicial de redes, a implantação do IPv6 surgiria com muitos empasses, causados principalmente pela grande utilização de serviços IPv4. A adequação deve, portanto vim de forma a não prejudicar os utilitários de uma rede que se mantêm ao modelo atual de protocolo IPv4.

Além do esgotamento, o crescimento da internet não trouxe só falhas para o IPv4 em falta de endereços, mas sim em segurança. Isso porque, com o aumento de usuários, muitos destes possuem identidade não conhecida, e portanto uma rede acaba correndo riscos. O protocolo IPv4 não possui fortes defesas para ataques, e isso acaba deixando um usuário vulnerável. O IPv6 viria

para resolver determinadas falhas, porém só o protocolo também não é suficiente , e por isso as vulnerabilidades dos métodos transitivos devem ser conhecidas, a fim de proteger aos que utilizam uma rede.

Os mecanismos de transição viriam a sanar a dificuldade do protocolo utilizado atualmente, porém a implantação não poderia ser feita de forma simples, sem conhecer as falhas. É necessário, portanto, conhecer as vulnerabilidades destes mecanismos, o que é um fator decisivo para qualquer transição. A utilização de tais métodos deve ser feita de tal forma a não só priorizar esta transição, mas sim proteger o usuário de qualquer risco a ataques. É disso, portanto, que trata esta obra.

No presente estudo foram demonstradas algumas das vulnerabilidades conhecidas do Ipv4, Ipv6 e nos protocolos relacionados aos métodos de transição, bem como as formas de evitar ataques explorando essas vulnerabilidades e de implementar uma rede de pilha dupla com um nivel aceitável de segurança.

REFERÊNCIAS

GRAZIANI, Rick. **IPv6 Fundamentals:** A Straightforward Approach to Understanding IPv6. 1. ed. Indianapolis: Cisco Press, 2012.

DAVIES, Joseph. **Understanding IPv6.** 3. ed. California: Microsoft Press, 2012.

AMOSS, John J; MINOLI, Daniel. **Handbook of IPv4 to IPv6 transition :** methodologies for institutional and corporate networks. 1. ed. Northwest Florida: Auerbach Publications, 2007.

HOGG, Scott; VYNCKE, Eric. **IPv6 Security.** 1. ed. Indianapolis: Cisco Press, 2008.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003.

STALLINGS, William. **Criptografia e segurança de redes**: Princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

INTERNET WORLD STATS. **History and Growth of the Internet from 1995 till Today**. Disponível em <http://www.internetworldstats.com/emarketing.htm>. Acesso em 23 de fev.2016

MORIMOTO, Carlos E. **Entendendo o CIDR** (máscaras de tamanho variável). Disponível em <http://www.hardware.com.br/dicas/entendendo-cidr.html>. Acesso em 9 de fev.2016.

6NET. **Final IPv4 to IPv6 Transition Cookbook for Organisational/ISP (NREN) and Backbone Networks.** Disponível em: <https://www.6net.org/publications/deliverables/D2.2.4.pdf>. Acesso em 22 fev.2016.

CICILEO, Guilherme. **Mecanismos de transição**. Disponível em:<http://portalipv6.lacnic.net/pt-br/mecanismos-de-transicao/>Acesso em 25 de fev.2016

SOTILLO, Samuel. **IPv6 Security Issues**. Disponível em <http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf> Acesso em 26 de fev. 2016.

IPV6.BR. **Transição**. Disponível em < http://ipv6.br/post/transicao/>. Acesso em 26 fev. 2016.

TELECO. **Tutoriais banda larga**: Redes IP II : técnicas de transição de tunelamento. Disponível em < http://www.teleco.com.br/tutoriais/ tutorialredeip2/pagina_3.asp>. Acesso em 27 fev. 2016.

TELECO. **Tradução**. Disponível em <http://www.teleco.com.br/ tutoriais/tutorialredeip2/

pagina_4.asp>. Acesso em 28 fev. 2016.

TELECO. **Redes IPv6**: Desafios para a Implantação. Disponível em: <http://www.teleco. com.br/tutoriais/tuto rialipv6seg/pagina_4.asp>. Acesso em 14 mar. 2016

DUTTA, A et al. **IPv6 Transition Techniques for Legacy Application.** Disponível em <https://www.researchgate.net/publication/232616697_IPv6_Transition_Techniques_for_Legacy_Application>. Acesso em 27 fev. 2016.

FTP.REGISTRO.BR. **Capacitação IPv6 :** Segurança em IPv6. Disponível em <ftp://ftp.Registro. Br/pub/gter/g ter33 / Tutorial-IPv6-Seguranca.pdf>. Acesso em 13 mar. 2016.

GADONG, Jalan; DARUSSALAN, Brunei. **IPv6-to-IPv4 Transition And Security Issues.** Disponível em <http://www.brucert.org.bn/files/IPv6-to-IPv4%20Transition%20&%20Security %20Issues.pdf>.Acesso em 18 mar.2016

THE INTERNET ENGINEERING TASK FORCE(IETF). **RFC 3053: IPv6 Tunnel Broker.** Disponível em: <https://tools.ietf.org/html/rfc3053>. Acesso em 26 fev. 2016.

THE INTERNET ENGINEERING TASK FORCE(IETF). **RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers.** Disponível em: <https: //tools.ietf.org/html/rfc6147>. Acesso em 27 fev.2016.

THE INTERNET ENGINEERING TASK FORCE(IETF). **RFC 4303: IP Encapsulating Security Payload (ESP).** Disponível em: <https://www.ietf.org/rfc/rfc4303.txt>. Acesso em 11 mar. 2016.

THE INTERNET ENGINEERING TASK FORCE(IETF). **RFC 3964: Security Considerations for 6to4.** Disponível em: <https://www.ietf.org/rfc/rfc3964.txt>. Acesso em 13 mar. 2016.

THE INTERNET ENGINEERING TASK FORCE(IETF). **RFC 4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).** Disponível em: <https://www. Ietf.org/rfc/rfc4380.txt>. Acesso em 14 mar. 2016.

ANEXOS

ANEXO A – COMPARAÇÕES ENTRE IPV4 E IPV6

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec header support is optional.	IPsec header support is required.
No identification of packet flow for prioritized delivery handling by routers is present within the IPv4 header.	Packet flow identification for prioritized delivery handling by routers is present within the IPv6 header using the Flow Label field.
Fragmentation is performed by the sending host and at routers, slowing router performance.	Fragmentation is performed only by the sending host.
Has no link-layer packet-size requirements and must be able to reassemble a 576-byte packet.	Link layer must support a 1,280-byte packet and be able to reassemble a 1,500-byte packet.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
ARP uses broadcast ARP Request frames to resolve an IPv4 address to a link-layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMPv4 Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages, and it is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP for IPv4.	Does not require manual configuration or DHCP for IPv6.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses AAAA records in the DNS to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.

Fonte: DAVIES, Joseph.**Understanding IPv6.** 3. ed. EUA: Microsoft Corporation,2012, p. 8)

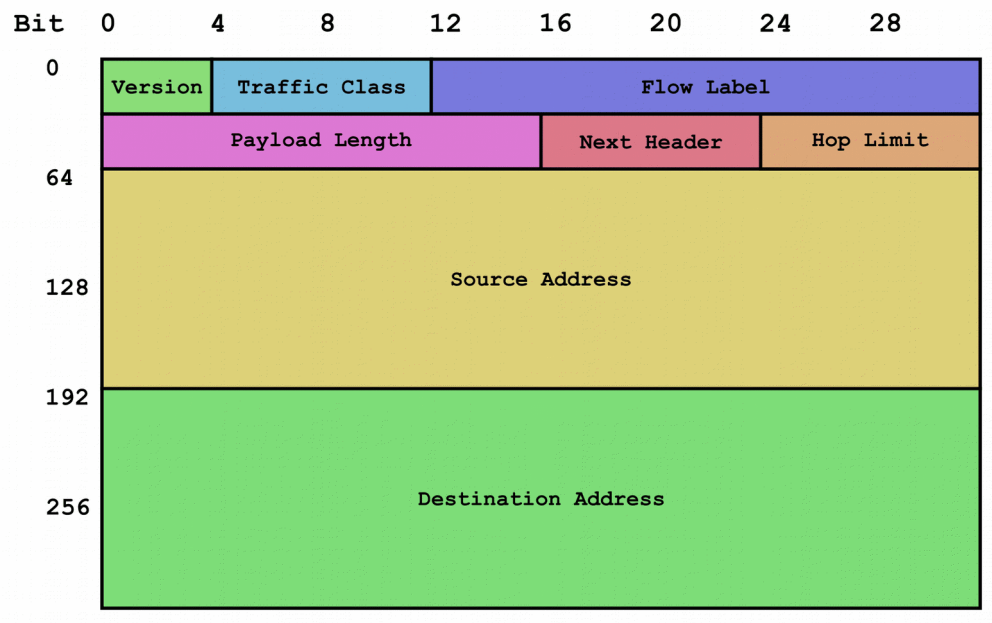
ANEXO B – VANTAGENS E DESVANTAGENS DAS TÉCNICAS DE MIGRAÇÃO

Tabela 1: Vantagem e Desvantagem das técnicas de migração

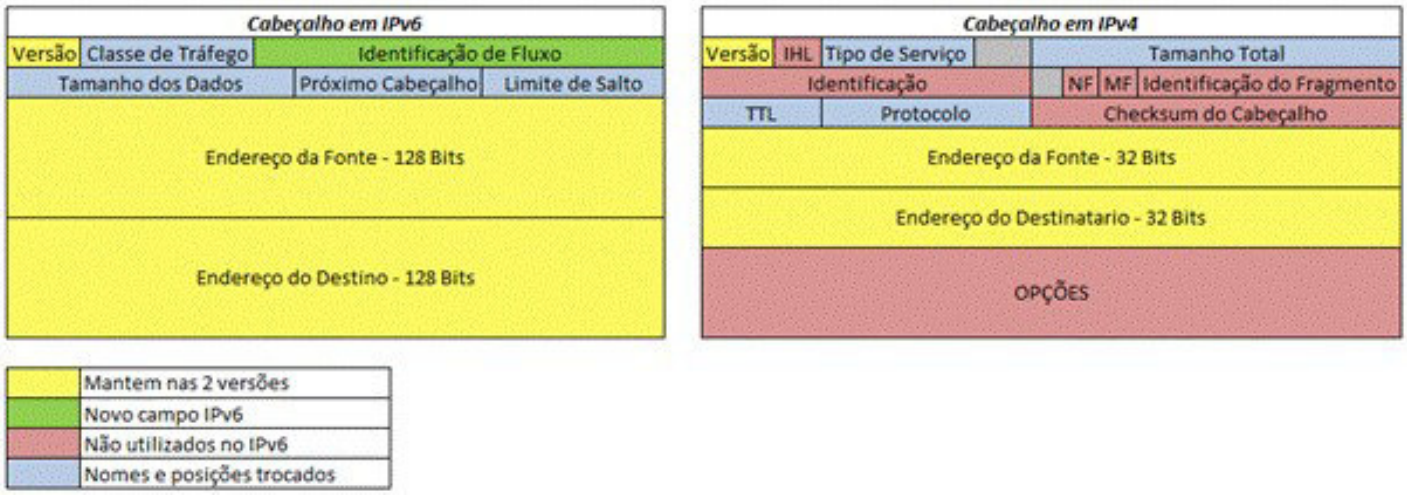
TÉCNICAS	VANTAGEM	DESVANTAGEM
Pilha Dupla	Utiliza técnicas *stateless* baseadas em uma dupla tradução de pacotes	Cada *Host* precisa ter as duas pilhas rodando separadamente, o que demanda o poder de processamento adicional e memória.
Tunnel Brokers	Baixa complexidade de funcionamento	Alta latência
6to4	Cria túneis automaticamente para outros endereços 6to4.	Segurança, sendo vulneráveis a ataques do tipo *Man-in-the-Middle* e DoS.
6rd	Rápida adoção do IPv6 para usuários domésticos	Deve sempre existir um protocolo IPv4 público operando em paralelo para seu funcionamento
NAT444	Não e necessário conhecimento em IPv6	Quebra do modelo fim-a-fim da Internet
ISATAP	Suporta a maior parte dos sistemas operacionais e roteadores e de fácil implantação	Não provê nenhuma economia de endereços IPv4, pois todos os hosts envolvidos na comunicação precisam de um endereço IPv4 público.
Teredo	Fácil implementação para usuários domésticos, devido a configuração automática.	Segurança por utilizar o protocolo UDP
NAT-PT	Tem uma eficiência mais elevada do que as técnicas utilizadas na camada de aplicação.	É muito complicado para criar entradas estáticas para múltiplas fontes de comunicação com vários destinos.
NAT64/DNS64	Infraestrutura de IPv4 permanece inalterado	Incompatibilidade com balanceamento de carga em servidores ou algo do gênero.

Fonte: <http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_5.asp>Acesso em 13 mar.2016.

ANEXO C – DATAGRAMAS IPv6/IPv4

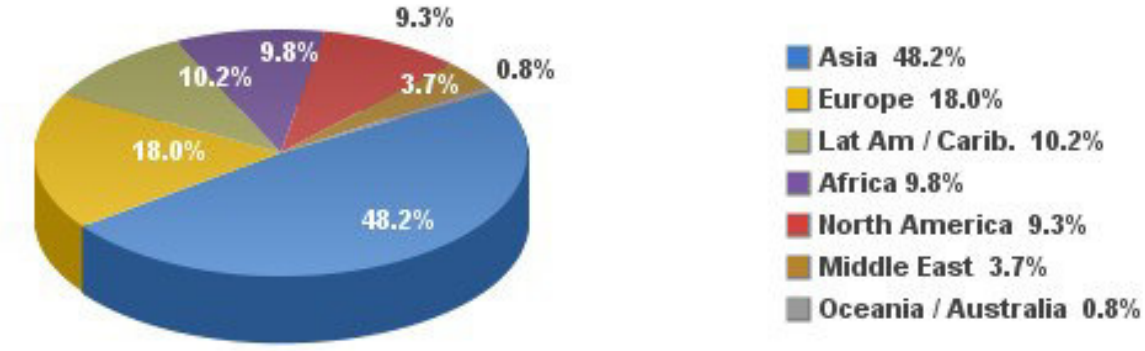


Fonte:< http://www.tass.com.br/imprensa2.asp?C%C3%B3digo=16>. Acesso em 01 abr.2016.

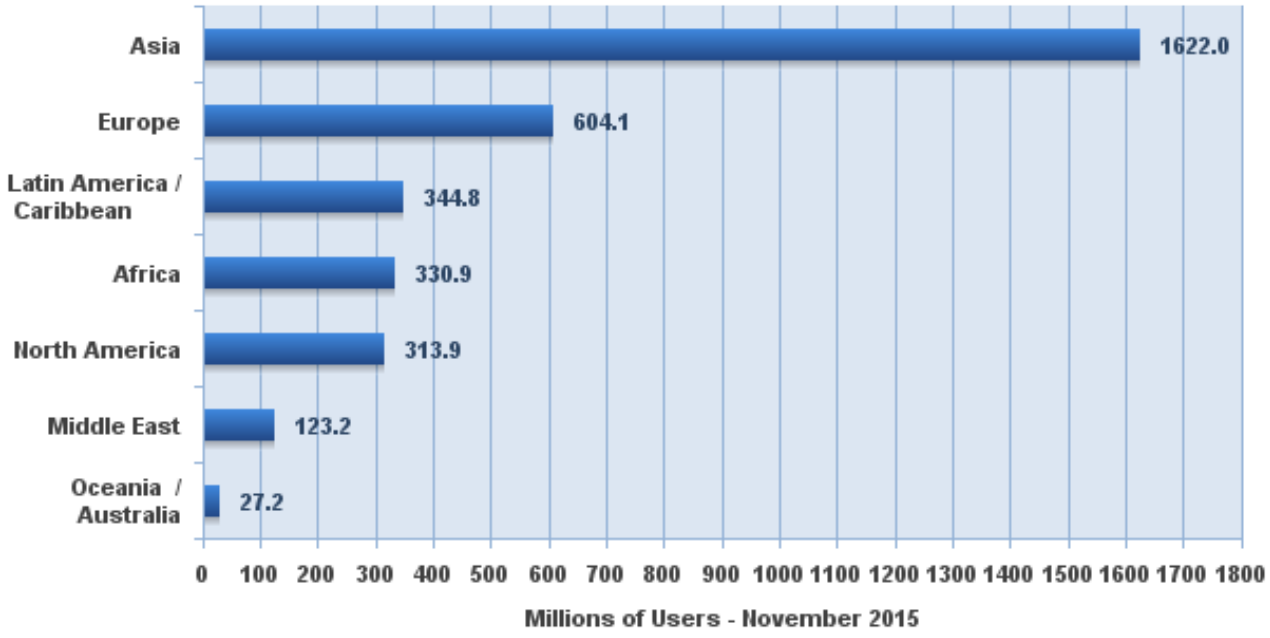


Fonte:< https://rafaelantunesavila.wordpress.com/2011/03/28/ipv6-o-que-e-isto/>.Acesso em 1 abr.2016.

ANEXO D – CRESCIMENTO MUNDIAL DA INTERNET- 2015

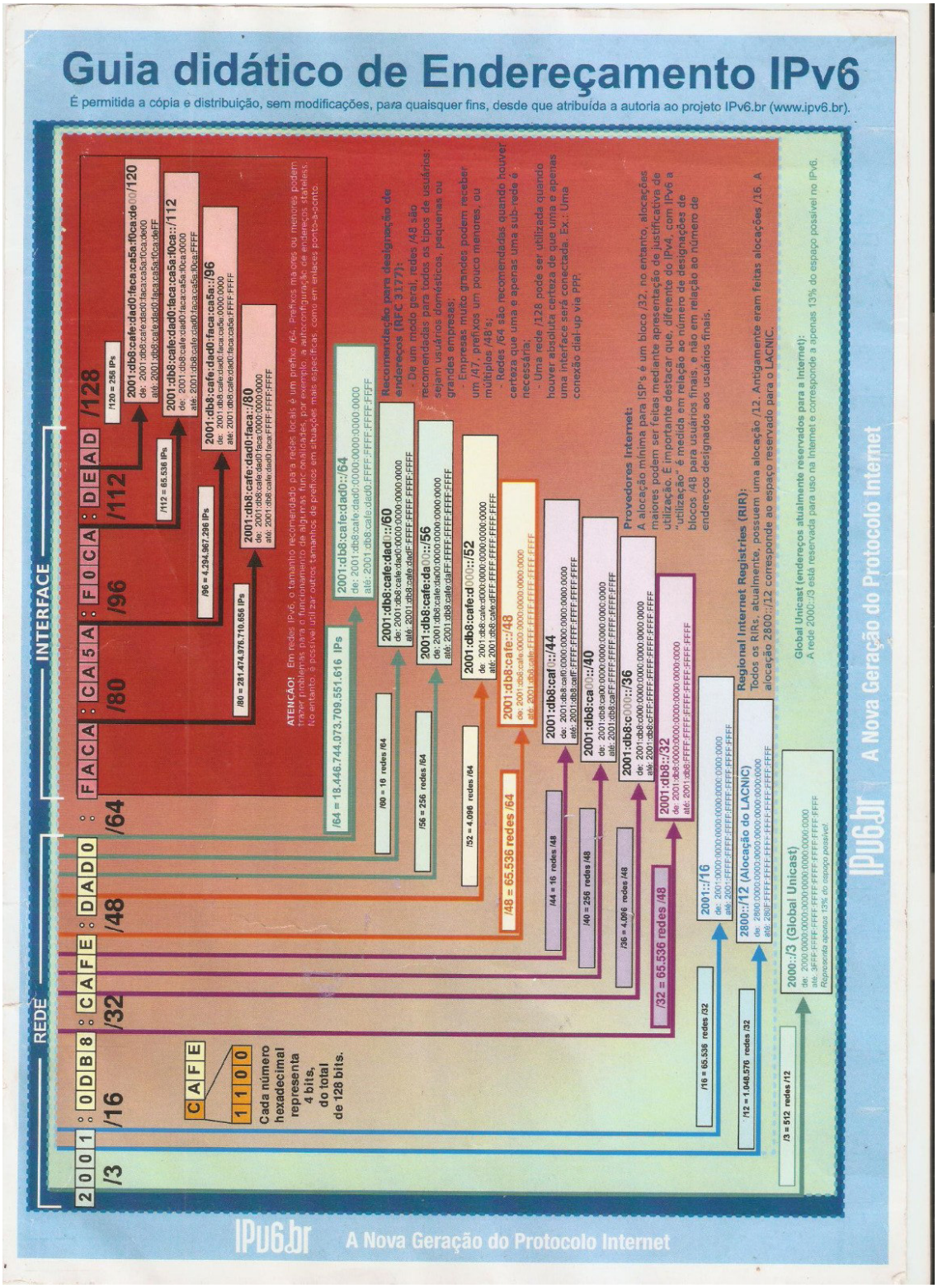


Fonte:<http://www.internetworldstats.com/stats.htm>.Acesso em 30 mar.2016.



Fonte:<http://www.internetworldstats.com/stats.htm>.Acesso em 30 mar.2016.

ANEXO E – GUIA DIDÁTICO DE ENDEREÇAMENTO IPv6



Fonte: <http://ipv6.br>. Acesso em 2 abr. 2016.