Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

IPCalipse - Fim do IPv4 e Surgimento do IPv6

Kátia Gabriele de Ornelas

Americana, SP
2011

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

IPCalipse – Fim do IPv4 e Surgimento do IPv6

Kátia Gabriele de Ornelas

gabrieleornelas@gmail.com

Trabalho de conclusão de curso para obtenção de grau de Técnologo em Segurança da Informação da Faculdade de Tecnologia de Americana, sob orientação do Profº. Alberto Martins Júnior.

Área: Segurança da Informação

Americana, SP
2011

BANCA EXAMINADORA

Profº. Alberto Martins Júnior (Orientador)

Prof. Marcus Lahr (Convidado)

Prof. Antonio Alfredo Lacerda (Presidente da banca)

"Take the Internet where no other Network has been before."
Vint Carf, IPv6 Forum Honorary Chairman

AGRADECIMENTOS

Em primeiro lugar, ao meu orientador Alberto Martins Júnior, que me instruiu em todas as etapas da produção de minha monográfia. Obrigada pelas dicas e por sempre estar disponível se preciso. Agradaço também aos meus colegas de classe Válter Aires Netto e Mauricio Rafael Possari, que sempre me ajudaram quando tinha dúvidas nas matérias e além de ser o grupo de todos os trabalhos, que mesmo sendo feitos na correria ou em cima da hora sempre ficaram excelentes. Obrigada pela assistência durante esses 3 anos de faculdade.

RESUMO

O presente trabalho tem como objetivo apresentar o protocolo IP em sua nova versão mais aprimorada – Versão 6 – especificando os seus benefícios em relação à versão 4 - IPv4 – atualmente utilizada. É aqui apresentado e detalhado todos os novos recursos, protocolos, projetos e estruturas do IPv6, sempre mostrando como era utilizado os mesmos no IPv4. Dentre os grandes benefícios do novo protocolo, está a redução de processamento no roteador em função do novo processo de fragmentação do datagrama, a criação de cabeçalho de tamanho fixo, o conceito de cabeçalhos concatenados e, o mais significativo, o aumento em quase três vezes na capacidade de endereçamento de hosts e redes.

Palavras Chave: Comparação de Estruturas IPs

ABSTRACT

The present paper has the objective of present the next generation of the Internet Protocol (also known as IPv6), focusing on its benefits as compared to the current version 4. It is presented here and in detail all the New features, Protocols, projects and Structures of IPv6, always showing how its where used on IPv4.

Among the great benefits of the new protocol are the load reduction over the router due to the extinguishment of datagram fragmentation, use of fixed length protocol Header, the concept of header concatenation and, the more important one, the expansion of hosts and nets addressing in about three times.

Keywords: Comparison of Structures IPs

LISTA DE SIGLAS

Sigla	Nomenclatura
AFI	*Address Family Identifier*
AH	*Authentication Header*
ALG	*Application Layer Gateway*
ARP	*Address Resolution Protocol*
AS	*Autonomous System*
BGP	*Border Gateway Protocol*
BIA	*Bump in the API*
BIS	*Bump in the Stack*
CGI	Comitê Gestor da Internet no Brasil
CIDR	*Classless Inter-Domain Routing*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoD	*Department of Defense*
DSL	*Digital Subscriber Line*
EGP	*Exterior Gateway Protocols*
ESP	*Encapsulating Security Payload*
FTP	*File Transfer Protocol*
GRE	*Generic Routing Encapsulation*
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocols*

IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPFIX	*Internet Protocol Flow Information Export*
IPng	*Internet Protocol New Generation*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol Version 4*
IPv6	*Internet Protocol Version 6*
ISATAP	*Intra-Site Automatic Tunnel Addressing Protocol*
ISP	*Internet service provider*
LACNIC	Latin American and Caribbean Internet Addresses Registry
LIR	*Local Internet registry*
LSA	*Link State Advertisements*
MAC	*Media Access Control*
MBGP	*Multiprotocol Border Gateway*
MIB	*Management Information Base*
MTU	*Maximum Transmit Unit*
NAT	*Network Address Translation*
NIC	Núcleo de Informação e Coordenação
NIR	*National Internet Registry*
NLPID	*Network Layer Protocol Identifiers*
NTP	*Network Time Protocol*
OMB	*Office of Management and Budget*
OSPFv3	*Open Shortest Path First Version 3*
PTR	*Pointer Record*
QoS	*Quality of Service*
RARP	*Reverse Address Resolution Protocol*
RFC	*Request for Comments*

RIR	*Regional Internet Registries*
RNP	Rede Nacional de Pesquisa
SEND	*Securing Neighbor Discovery*
SIIT	*Stateless IP/ICMP Translation*
SNMP	*Simple Network Management Protocol*
SSH	Secure Shell
Sub-AFI	*Subsequent Address Family Identifier*
TCP	*Transmission Control Protocol*
TFTP	*Trivial File Transfer Protocol*
TLV	*Threshold Limit Value*
TRT	*Transport Relay Translator*
UDP	*User Datagram Protocol*
USAGI	*Universal Playground for* IPv6
VoIP	Voice over Internet Protocol
WWW	*World Wide Web*

LISTA DE FIGURAS, GRÁFICOS E TABELAS

Figuras **Página**

Gráficos **Página**

Tabelas **Página**

SUMÁRIO

1 INTRODUÇÃO

Com a evolução dos computadores houve a necessidade da interconexão.

Existem várias formas de se fazer isso, diferenciando o modo de conexão, velocidades, formas de comunicação, tratamento dos erros, entre outros. Este conjunto de interconexão ficou denominado de rede de computadores. (GASPARINI; BORTOLLI, 1999)

As redes de computadores fizeram com que a utilização dos computadores ficasse mais simplificada, reduzindo custos para as empresas e aumentando a produtividade. Porém, a evolução desses dispositivos eletrônicos é cada vez maior, fazendo com que a área de redes evoluísse ainda mais.

Uma prova desta evolução é que antes dos anos 90, cada aparelho tinha uma função específica, ou seja, aparelho de som era feito só para reprodução de músicas, telefone só para conversação, máquina fotográfica para registro de imagens e computadores para programação, edição de documentos, execução de aplicativos e comunicação de dados.

As redes de informação conquistaram seu espaço desde as atividades mais simples do cotidiano até a interação entre os dispositivos eletrônicos. Um exemplo no qual podemos enxergar isto é na telefonia celular, que atualmente é capaz de trafegar voz, dados, imagem com a utilização de um aparelho telefônico através de redes integradas à Internet. E Computadores também exercem todas as atividades de eletrônicos como conversação, execução de jogos, captura e edição de imagens e vídeos, além da execução de músicas.

Toda esta modificação na estrutura dos eletro-eletrônicos e comunicação entre redes foi possível por causa da existência do protocolo Internet Protocol (IP), pois este permite a comunicação entre hardwares e sistemas de diferentes tecnologias, o que o difundiu de uma maneira fazendo-se necessária a criação de

mecanismos de segmentação entre as redes privadas (Intranet) e a pública (Internet).

Para as redes privadas foi permitido a adoção de endereços IP de escolha própria, onde a administração é feita exclusivamente pela organização. Já a rede

pública possui, em cada país, uma unidade controladora que tem a finalidade de gerenciar a distribuição de IPs, impedindo assim a duplicidade.

Mesmo utilizando-se vários recursos para melhor distribuir e aproveitar os endereços públicos, a quantidade de usuários e empresas que necessitam da Internet cresceu descontroladamente, fazendo com que os profissionais da área percebessem que os mais de 4 bilhões de endereços da Internet iriam se esgotar em

poucos anos.

Foi analisando este cenário que grupos de pesquisa começaram a trabalhar em um novo modelo de endereçamento TCP/IP a fim de atender à demanda mundial. Este modelo recebeu como nome inicial "IPng" (Internet Protocol - next generation). Mais tarde se oficializando como "IPv6", que entra em atividade para substituir o atual IPv4.

O lançamento deste novo Protocolo teve como justificativa o crescimento exponencial Internet, e a escassez de endereços públicos. Sendo que o IPv6 foi totalmente baseado na estrutura IPv4, pode-se dizer que ele é apenas uma melhoria de seu antecessor com uma capacidade de endereços extravagantemente maior.

Hoje em dia somos muito dependentes desses recursos, e um colapso no sistema traria prejuízos incalculáveis, principalmente para os profissionais liberais e empresas que dependem de tal estrutura para manter seus negócios. Isso não significa que a Internet iria parar, mas não seria mais possível a criação de novos aplicativos e muito menos a expansão de serviços. A fim de evitar esta situação crítica, foi desenvolvida a versão 6 do protocolo IP.

Muito mais que a ampliação da faixa de endereçamento oficial, o IPv6 visa a melhorar o desempenho das redes, principalmente nos pontos onde se exige maior processamento para passagem dos datagramas entre redes diferentes (roteadores). Outra questão importante seria o novo conceito de “cabeçalhos concatenados”. Isso permite um melhor gerenciamento de segurança do datagrama desde as atividades mais simples até as mais complexas como, por exemplo, criptografia e Virtual Private Network (VPN).

Levando em consideração essas idéias, já se é oportuno que todas as grandes empresas iniciassem o plano de migração para esta nova tecnologia do protocolo IP. Mudança que poderá ser implementada em longo prazo, uma vez que há serviços de compatibilização que tornam comunicável as duas versões do protocolo.

Até mesmo porque uma migração feita de imediato pode representar alto custo em hardware e software caso os equipamentos da corporação não suportassem IPv6.

Então visando esclarecer sobre este novo protocolo, este trabalho apresenta no decorrer de seus capítulos, quais são suas novas funcionalidades, o que mudou do IPv4 para o IPv6, quais projetos alguns países implantaram para amenizar o impacto da mudança, como está o novo cabeçalho e como funciona o seu endereçamento, os novos serviços criados para a melhoria do Protocolo. E finalmente, e mais importante, como a segurança é tratada neste novo modelo e como está sendo feito para se ter a coexistencia dos dois protocolos até que todos estejam adaptados a receber somente o IPv6.

1.1 Justificativa

O Trabalho de Monográfia tem o objetivo de apresentar um estudo do protocolo IPv6, destacando o que mudou da versão anterior, e resaltando suas inovações em relação ao IPv4. Ao final explicar com está sendo feito o processo de coexistência dos dois protocolos.

1.2 Objetivo

- Mostrar as diferenças entre as versões IPv4 e IPv6, mostrando sempre como é feito o processo no modelo Atual do protocolo e como será para a nova estrutura. E citando também o que foi criado para o IPv6, e as modificações relacionadas com a segurança.

- Explicar como está sendo feito o processo de coexistencia dos dois protocolos.

1.3 Metodologia

Foi realizado um estudo sobre as características da estrutura do protocolo IPv6 em comparação com o IPv4 para melhor compreensão.

Uma bibliográfia de boa qualidade e rica em explicações foi objeto de consulta, bem como bons sites da Internet, com a intenção se obter dados suficientes para um correto entendimento sobre o assunto.

2 O PROTOCOLO IP

Neste primeiro capítulo serão detalhados alguns conceitos sobre Redes, *Internet*, Protocolo *Internet* (IP), que são definições importantes para se entender melhor algumas idéias descritas no decorrer deste trabalho.

2.1 O que são as Redes

Seguindo a idéia de Tanenbaum (2003), uma rede de computadores possui dois ou mais computadores e outros dispositivos interligados entre si por meios físicos e que são capazes de se comunicar e compartilhar recursos físicos e lógicos, os quais podem ser: dados (arquivos, programas e acesso à *Internet*, mensagens) e componentes periféricos (como impressoras, *scanners*, entre outros). Utilizam para isso um conjunto de regras e códigos em comum.

Esse conjunto de Regras é chamado de Protocolo, ele é equivalente a linguagem dos seres humanos só que para computadores.

2.2 Internet

Segundo Tanenbaum (2003) a *Internet* é a Interligação de várias redes de computadores que utiliza como protocolo de comunicação o IP (*Internet Protocol*), que foi especialmente projetado para fazer a interligação de diversas redes.

É preciso prestar atenção quanto a nomenclatura da *Internet*, pois quando ela é escrita com I maiúsculo se refere a grande interligação mundial de redes computadores e com i minúsculo designa apenas uma rede normal, de pequena proporção.

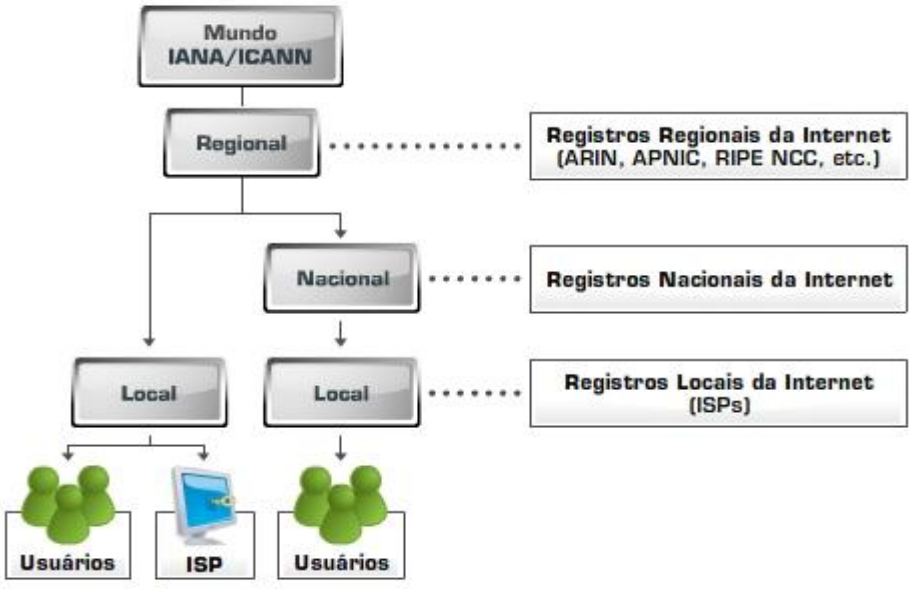
2.3 IP - Internet Protocol

O IP é o protocolo mais importante da *Internet*, basicamente, um endereço que indica o local de um determinado equipamento em uma rede privada ou pública. É ele que define as regras através das quais as informações fluem na rede mundial.

Como observado por Kurose (2006) o IP foi criado para suprir a necessidade de identificar cada computador univocamente na rede, sem nenhuma possibilidade de engano. Então o Endereço IP é este número único que identifica cada dispositivo da rede de modo que não existam na *Internet* dois com o mesmo endereço.

Para evitar os endereços duplicados de IP, sua distribuição é controlada por um conjunto de entidades que dividem a responsabilidade na seguinte estrutura hierárquica:

Figura 1: Estrutura de Distribuição IP



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

A IANA (*Internet Assigned Numbers Authority*) juntamente com a ICANN (*Internet Corporation for Assigned Names and Numbers*) é responsável por controlar todos os números IPs. A responsabilidade sobre alguns IPs a IANA delega para cada um dos Registros Regionais de *Internet* (RIR - *Regional Internet Registries*), que distribuem dentro de suas regiões geográficas. Há ainda, em alguns países, o Registro Nacional de *Internet* (NIR - *Nacional Internet Registry*) responsável pela distribuição Nacional do mesmo. E finalmente, provedores podem ser considerados Registros Locais de Internet (LIR - Local *Internet Registries*) distribuindo os endereços para usuários finais ou para outros provedores.

3 O ESGOTAMENTO DOS ENDEREÇOS IPs

Após a pequena explicação sobre alguns dos principais conceitos na área de Redes, será falado, neste segundo capitulo, o que aconteceu para ocorrer o esgotamento dos endereços IPv4.

Em 1969, quando se deu inicio à *Internet* através de um projeto para interligar os centros de pesquisa relacionados ao departamento de Defesa Estudinense e logo após abrindo à outros centros e Universidades, os seus progenitores não imaginavam que a sua expansão aconteceria de forma tão rápida e alcançasse a popularidade e a importância que esta rede mundial tem hoje em dia.

Foi em 1993, quando a *Internet* começou a ser utilizada comercialmente, que ela teve o seu crescimento acelerado, problemas estruturais apareceram e começaram a ser discutidos. Um deles foi justamente o esgotamento dos endereços IPs.

Esta história sobre o começo da *Internet* é reforçada por Tanenbaum (2003) e Kurose (2006), em seus respectivos livros sobre Redes de Computadores, contando em detalhes todo o ocorrido até a popularização da mesma.

A versão utilizada na época até atualmente é a versão 4, conhecida como IPv4. Cada endereço é representado por um número Binário de 32 bits, possibilitando a existência de 4.294.967.296 endereços IP. Apesar de ser uma quantidade generosa, a forma como eles foram distribuídos inicialmente colaborou para o seu rápido esgotamento.

No inicio os endereços eram divididos em classes e distribuidos da seguinte forma:

- Classe A: Possuía 128 blocos de IPs com aproximandamente 16 milhões de endereços cada um. Desse modo só 128 redes seriam atendidas ocupando metade de todos os endereços disponíveis.
- Classe B: Possuía 16 mil blocos de IPs com aproximadamente 65 mil endereços cada um. Nesse padrão, para atender 300 dispositivos em uma rede seria necessário obter um bloco de endereços dessa classe, desperdiçando quase o seu total.
- Classe C: Possuía 2 milhões de blocos de IPs com 256 endereços cada um.

O Núcleo de Informação e Coordenação do Ponto BR (NIC) apresenta pesquisas que mostram que na década de 90, para retardar o esgotamento de endereços IPs algumas soluções paliativas foram desenvolvidas. Exemplos são:

- CIDR: Reponsável por eliminar o sistema de classes, permitindo o alocamento de blocos de endereços de tamanhos correspondentes a necessidade, possibilitando um uso mais racional do espaço para endereçamento.
- RFC 1918: Especificou três faixas de endereços privados para uso em redes corporativas. Esses endereços não são válidos na *Internet*.
- NAT: É uma tecnologia onde um único endereço válido na *Internet* conecte toda uma rede de computadores, que usem endereços privados.
- DHCP: Protocolo que permite a alocação dinâmica de endereços IP, assim provedores podem reutilizar endereços fornecidos aos clientes para conexão não permanentes.

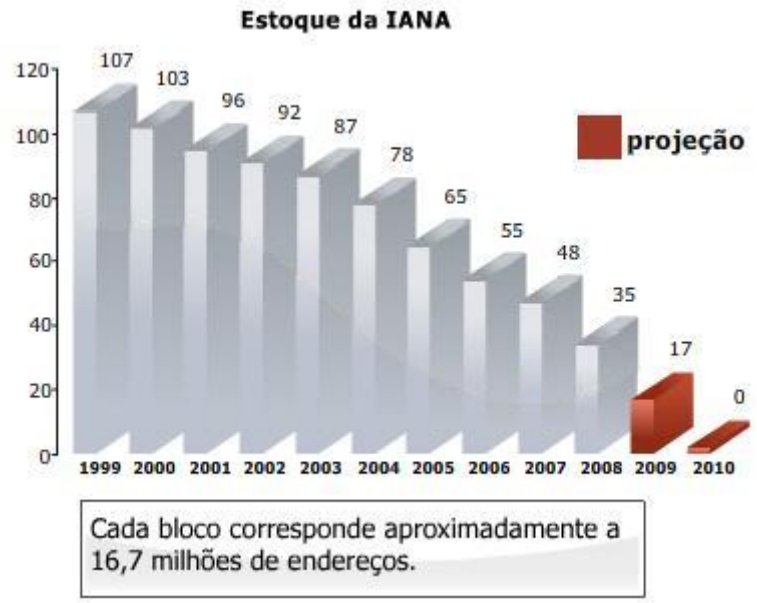
Mas essas eram só soluções provisórias, seu uso visando uma solução definitiva prejudicaria muito o desenvolvimento da *Internet* como um todo. A única solução definitiva que salvaria a *Internet* seria a criação de um novo Protocolo *Internet*. Então, nessa época, iniciou-se o chamado IPng (*Internet Protocol New Generation*), que resultou no IPv6.

O sucesso do IPv6 é de suma importância para se garatir a continuidade da *Internet* e o surgimento de novas redes interligadas, novos usuários e novas aplicações. Entretando é importante frisar que ela continuaria funcionando sem novos endereços IP, mas teria dificuldades para crescer.

A seguir alguns gráficos mostram o Nível de consumo do IPv4:

Este Primeiro gráfico demonstra o Estoque de endereços IPv4 disponíveis desde o ano de 1999 até 2010.

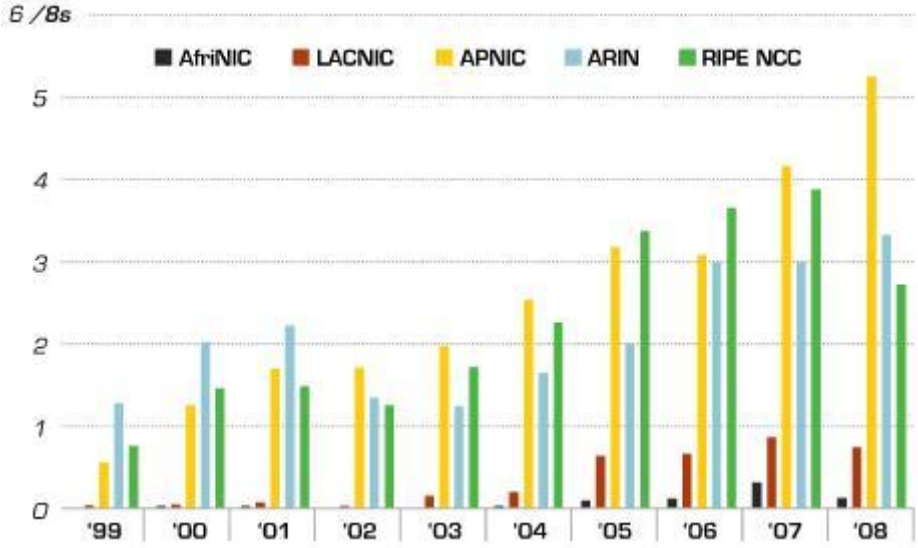
Gráfico 1: Evolução do Estoque de Blocos IP na IANA



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

O segundo gráfico mostra a quantidade de blocos IPs que são solicitados anualmente pelos RIRs, responsáveis por distribuir os Endereços Regionalmente.

Gráfico 2: Quantidade de Blocos IP Solicitados Anualmente pelos RIRs



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

4 O IPv6

O IPv6 foi desenvolvido para solucionar definitivamente o problema de infraestrutura da *Internet* e trazer uma série de avanços.

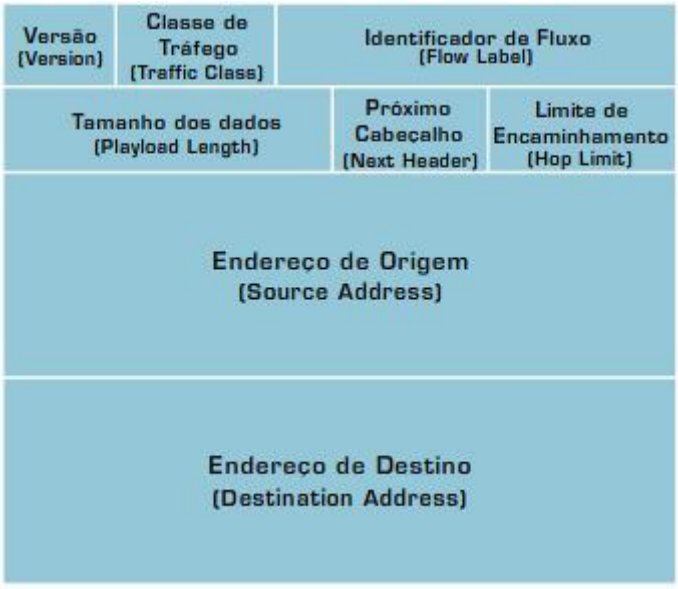
A versão 6 do IP foi desenvolvida ao longo de 10 anos, mantendo como base os príncipios do IPv4 mas suprindo todas as suas carências. A maior diferença entre o IPv4 e o IPv6 é a capacidade de espaço para endereçamento, que passou de 32 bits para 128 bits.

Acreditasse que com isso toda a necessidade atual e futura será cumprida. O novo espaço total para endereçamento fornece 340.282.366.920.938.463.463.374.607.431.768.211.456 de endereços (2128), o que representa 79 trilhões de vezes a quantidade disponível no IPv4.

Com o novo formato de endereços é possível definir uma arquitetura hierárquica na *Internet*, possibilitando um encaminhamento mais eficiente dos pacotes de Dados; Facilitando a distribuição de IPs fixos e válidos para conexões DSL, *Cable Modens*, e telefones móveis; Utiliza a arquitetura fim-a-fim; e eliminando os problemas associados ao NAT.

Outra grande mudança está no formato do cabeçalho, que se tornou mais simples e eficiente, reduzindo o processamento dos roteadores.

Figura 2: Cabeçalho IPv6



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

Na parte de segurança também ocorreram mudanças importantes. O IPSec passou a ser obrigatório, fazendo parte do próprio protocolo IPv6, isso permite que os administradores de redes ativem o IPSec em todos os dispositivos da mesma tornando-a mais segura, pois a função do IPSec é garantir Autenticidade, Privacidade e Integridade.

O protocolo ICMP (*Internet Control Message Protocol*), tornou-se mais eficaz, permitindo a inclusão de novas funcionalidades ao IPv6 e aprimorando o mecanismo de autoconfiguração de endereços e o gerenciamento de grupos *multicast.*

Em geral deve-se entender que o IPv6 não é um upgrade de IP, mas sim um novo Protocolo de IP, então algumas mudanças em equipamentos de redes, como roteadores, *switches* e *firewalls* devem ocorrer e também nos sistemas operacionais e programas de computadores.

Reforçando todo esse novo conceito sobre IPv6, Silvia Hagen escreveu o livro “IPv6 Essentials”, que traz uma sucinta explicação sobre o por quê da sua necessidade, e explica os novos conceitos para as funções e recursos.

5 IMPLANTAÇÃO DO IPv6

Huston (2010) explica em artigos publicados em seu site que a implantação do IPv6 é necessária e inevitável. Embora o esgotamento de endereços IPv4 não faça a *Internet* parar de funcionar, ela prejudica a taxa de crescimento da rede e faz com que algumas aplicações que irião ser criadas não seja mais, resultando no encarecimento das conexões *Internet*. Entretanto a implantação do IPv6 não acontecerá de forma rápida e não haverá uma “data da virada”, todo esse processo acontecerá de forma gradual e com o IPv4 em pleno funcionamento.

Para a eficácia dessa implantação é preciso que:

- As empresas tomem consciência da necessidade de implantar o IPv6;
- Técnicos aprimorem seus conhecimentos sobre o IPv6 e façam experimentos;
- O Suporte ao IPv6 deve ser exigido na compra de novos equipamentos, *softwares* e contratação de serviços;
- Seja feito um planejamento detalhado sobre como será feita a implantação do novo protocolo dentro da empresa/entidade.

Uma das orientações divulgadas para minimizar o impacto da transição é que durante esse período de coexistência entre os IPs, para se manter a compatibilidade entre as versões os profissionais devem se utilizar de mecanismos de transição, tunelamento, tradução e pilha dupla.

Assim como no IPv4, a distribuição de endereços IPv6 será feita de forma hierárquica. Esta divisão dos blocos IPv6 acontecerá da seguinte maneira:

- Cada RIR recebe da IANA um bloco /12;
- Os provedores recebem dos RIRs blocos /32.

Os provedores devem entregar aos seus clientes blocos variando entre /48 e /56, dependendo da necessidade de cada um, pois:

- Um bloco /48 pode ser dividido em até 65.536 redes diferentes, cada uma com 18.446.744.073.709.551.616 endereços diferentes; e

- Um bloco /56 pode ser dividido em até 256 redes diferentes, cada uma com 18.446.744.073.709.551.616 endereços diferentes.

Há ainda a possibilidade de um endereço /64 ser designado a um usuário se houver certeza de que apenas uma rede atende às suas necessidades, um exemplo seriam usuários domesticos.

Todos os RIRs já distribuem endereços IPv6 em suas regiões. O NIC.br é o responsável pela distribuição de bloco IPv6 no Brasil.

Pensando em facilitar a transição entre protocolos, empresas responsáveis pelos principais Sistemas Operacionais e Aplicativos já adaptaram os seus sistemas para suportar o IPv6. Por exemplo:

- O Windows lançou sua versão oficial com suporte ao IPv6 junto com o Service Pack 1 para o Windows XP. E atualmente, as versões XP SP2 e SP3, Vista, 2003 Server, 2008 Server e CE apresentam versões mais aprimoradas.
- O MAC OS X tem suporte para IPv6 desde a versão 10.2 Jaguar e, por padrão, já vem com o IPv6 habilitado.
- O primeiro código relacionado ao IPv6 foi adicionado no Kernel do Linux na versão 2.1.8 e aprimorado a partir da versão 2.2.x
- O FreeBSD apresenta suporte ao IPv6 desde a versão 4.0. Já o NetBSD utiliza esse suporte desde Dezembro de 2000 na versão 1.5 e no OpenBSD desde a versão 2.7.

Tão importante quanto o suporte nos *Softwares*, o suporte em roteadores e *switches* é necessário para que os mesmos estejam aptos a tratar o tamanho do endereçamento, seu impacto na tabela de rotas, além de mudanças no roteamento. Então os principais modelos de equipamentos de redes se adaptaram ao novo protocolo. Como exemplo pode-se citar:

- CISCO *Systems*: proveu suporte ao IPv6 nos roteadores a partir das séries 12000 e 10720;

- Juniper *Networks*: introduziu o suporte ao IPv6 nos seus principais roteadores, T-Series e M-Series, desde a versão 5.1 do sistema operacional JUNOS;
- Alcatel-Lucent: adaptou o seu sistema operacional SR-OS para suportar várias funcionalidades do IPv6, instalando ele nos roteadores 7750SR e 7710SR;
- Hitachi: Desde 2001 os roteadores GR2000 da Familia *Gigabit Router* oferecem entrega de pacotes IPv6 em alto-desempenho, além de QoS, túneis e filtros;
- 3Com *Corporation*: desde 1997 os softwares dos roteadores *NETBuilder* e os *Switches PathBuilder* S500 possuem suporte ao IPv6.

Buscando incentivar o uso do IPv6 diversas iniciativas, como políticas de estimulos, estão sendo tomadas pelos RIRs nas regiões por eles administradas. No âmbito acadêmico existem diversos grupos que trabalham no desenvolvimento de projetos relacionados ao IPv6, destacando-se os projetos: Rede CLARA (Cooperação Latino-Americana de Redes Avançadas); GÉANT2; Internet2; KAME; USAGI (*Universal Playground for* IPv6). No Brasil é a rede RNP (Rede Nacional de Pesquisa) que tem o destaque com o Projeto Br6Bone. Atualmente toda essa rede RNP está apta a operar e fornecer conexão com o protocolo IPv6 em modo nativo.

Há também um grande incentivo Global por parte dos Governos em prou da utilização do novo protocolo, ocorrendo desde recomendações até ações mandatórias. Em países como Estados Unidos, Brasil, União Européia, China e Japão tiveram as seguintes metas emitidas por seus governos:

- No Estados Unidos o governo publicou, em setembro de 2003, um memorando determinando metas e o planejamento para a realização da transição para o IPv6 de toda a infraestrutura de sua rede, até 2008. Baseados neste memorando, foram criados documentos definindo um conjunto de padrões técnicos e requisitos de interoperabilidade que devem ser seguidos por equipamentos e *softwares* utilizados nas redes do DoD. O Gabinete de Gestão e Orçamento dos Estados Unidos (*OMB - Office of Management and Budget*) também emitiu, em agosto

de 2005, um memorando estabelecendo metas semelhantes às do DoD referentes às redes das Agências Governamentais Federais estadunidenses.

- O Governo do Brasil fez a recomendação da arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico), que define um conjunto de premissas, políticas e especificações técnicas que visam regulamentar a utilização da Tecnologia de Informação e Comunicação no Governo Federal. Esta recomendação expressa que os órgãos das Administrações Públicas Federais deverão se planejar para uma futura migração para IPv6 e prever suporte à coexistência dos protocolos IPv4 e IPv6 em novas contratações, compra de produtos e atualizações de redes.

- Na União Européia já foram investidos, desde 2002, mais de €90 milhões em pesquisas relacionadas ao IPv6, podendo chegar a um total de €300 milhões até 2013. Em 27 de maio de 2008 foi estabelecido como objetivo para a Europa que, em 2010, 25% das empresas, administrações públicas e usuários particulares já utilizem o IPv6. Também foi sugerido que os Estados-Membros exijam a utilização do IPv6 como condição para os contratos públicos e lancem campanhas de incentivo junto as empresas e organizações, além de ajudá-las na transição.

- O Governo da China iniciou a implantação de uma rede IPv6 chamada *China Next Generation Internet,* investindo cerca de US$170 milhões, e envolvendo oito ministérios, cinco grandes companhias nacionais e várias redes nacionais de pesquisa. Também utilizou os Jogos Olímpicos de Pequim 2008 para testar dispositivos móveis e sistemas inteligentes de transporte e de segurança operando sobre IPv6.

- No Japão, o governo oferece, desde 2000, incentivos fiscais para a adoção do IPv6, além de apoiar, criar e financiar projetos como o IPv6 *Promotion Council*, WIDE, KAME, USAGI, entre outros.

- Todas essas ações do Governo, adaptações de sistemas físicos e lógicos, que já vem sendo realizadas pelas empresas, está contribuindo para que a implantação do IPv6 ocorra sem grandes impactos para todos.

Todas estas informações sobre aplicativos já adaptados para suportar o IPv6 e ações tomadas por alguns países para incentivar o uso Global do novo protocolo *Internet*, foram retiradas de listas e artigos do sitio ipv6.org.

6 CABEÇALHO IPv6

No começo do projeto foi falado que a principal mudança ocorreu no cabeçalho. Neste capitulo será detalhado quais foram essas mudanças.

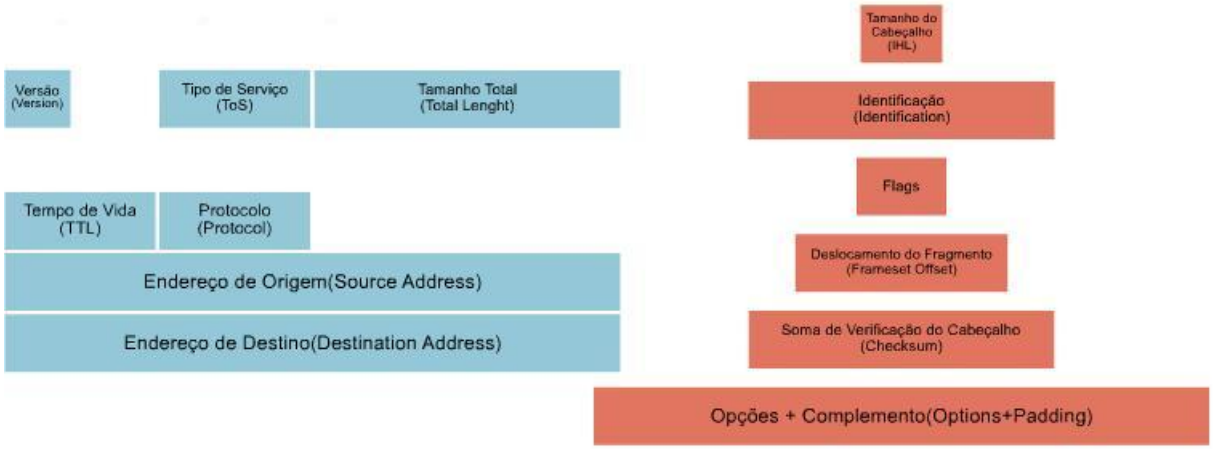
O Cabeçalho IPv4 é composto por 12 campos fixos, que são: Versão, Tamanho do cabeçalho, Tipo de serviço, Tamanho Total, Identificação, Flags, Deslocamento do fragmento, Tempo de vida, Protocolo, Soma de verificação do cabeçalho, Endereço de origem, Endereço de destino, Opções + Complemento. Estes campos podem ou não conter opções, fazendo com que o tamanho varie entre 20 e 60 bytes.

Os campos têm a função de transmitir informações sobre a versão do protocolo, o tamanho do cabeçalho e dos dados, a fragmentação, o tipo de dados, o tempo de vida do pacote, o protocolo da camada seguinte (TCP, UDP, ICMP), a integridade dos dados, a origem e o destino do pacote.

Utilizando os estudos de Tanenbaum (2003), podemos perceber que o cabeçalho do IPv6 foi totalmente baseado no anterior, com algumas mudanças, sendo que uma delas foi a remoção de 6 campos do cabeçalho IPv4 pois suas funçãos não são mais necessárias ou são implementadas pelo cabeçalho de extenção. Assim o novo cabeçalho possui os campos: Versão, Tipo de Serviço, Tamanho Total, Tempo de Vida, Protocolo, Endereço de Origem e Endereço de destino.

A figura abaixo demonstra os campos retirados:

Figura 3: Mudanças da Estrutura IPv4 para IPv6



Fonte: Núcleo de Informação e Coordenação do Ponto BR

Os motivos que levaram a remoção desses campos especificamente foram:

- Tamanho do Cabeçalho: Removido porque no IPv6 este valor é fixo;
- Identificação, *Flags* e Deslocamento do Fragmento: Removidos porque as informações referentes a fragmentação são indicadas em um cabeçalho de extensão apropriado.
- Soma de Verificação do Cabeçalho: Removido pois este cálculo já é realizado pelos protocolos das camadas superiores. Isto melhorou a velocidade no processamento dos roteadores.
- Opções + Complemento: Removidos porque as opções adicionais agora fazem parte dos cabeçalhos de extensão do IPv6.

A segunda modificação foi a alteração dos nomes e posicionamentos de outros quatro campos, isto foi definido para facilitar o processamento dessas informações pelos roteadores. Sendo assim os campos ganharam a seguinte configuração:

Figura 4: Nova Configuração dos Campos do Cabeçalho

Fonte: Núcleo de Informação e Coordenação do Ponto BR

- Classe de Tráfego: Continua provendo as mesmas funcionalidades do campo Tipo de serviço do IPv4;
- Tamanho dos Dados: no IPv4 o campo Tamanho Total indicava o tamanho do cabeçalho mais o tamanho dos dados transmitidos. No IPv6 apenas o tamanho dos dados é indicado, visto que o tamanho do cabeçalho agora é fixo;
- Limite de Encaminhamento: No IPv4 o campo Tempo de Vida deveria indicar em segundos quanto tempo o pacote levaria para ser descartado caso não chegasse ao seu destino. No entanto, ele é apenas decrementado em cada nó que ele percorre, sendo descartado quando esse valor chega a zero. No IPv6 este método foi apenas padronizado;
- Próximo Cabeçalho: este campo foi renomeado refletindo a nova organização dos pacotes IPv6, pois agora este campo não contem apenas valores referentes a protocolos da camada superior, mas também indica os valores dos cabeçalhos de extensão.

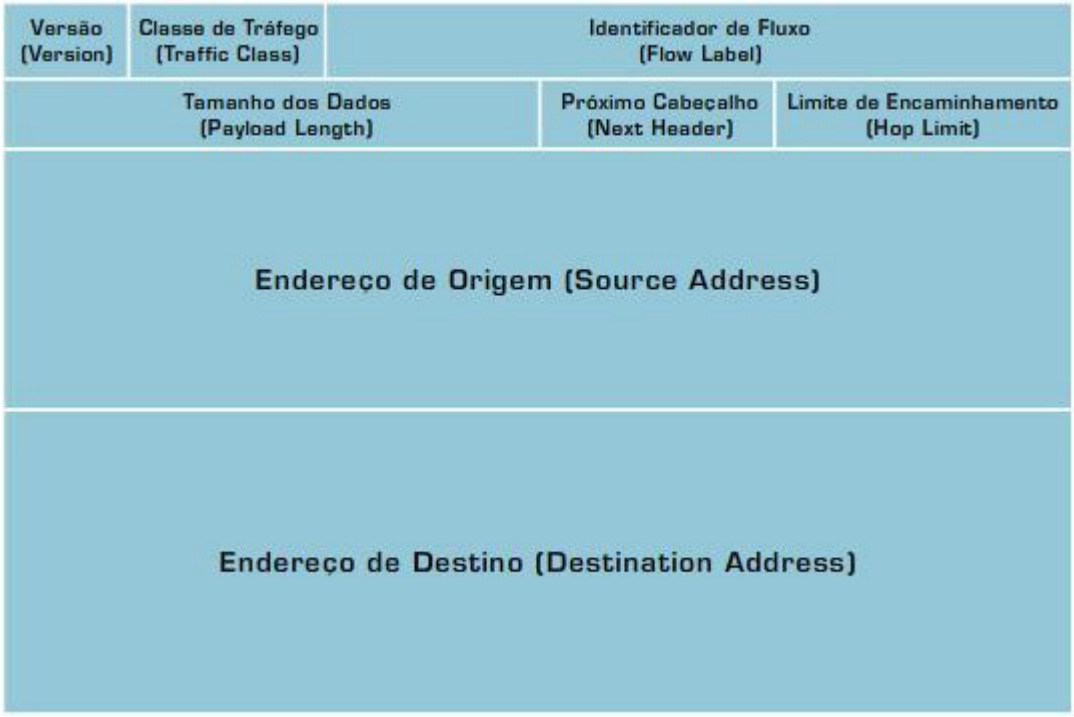
Continuando as modificações o campo “Indetificador de Fluxo” foi acrescentado, adicionando um mecanismo extra de suporte a QoS ao IP. E três campos foram mantidos, alterando apenas o tamanho do espaço reservado para endereçamento que agora passa a ter 128 bits.

Essas mudanças tornaram o cabeçalho IPv6 mais flexível e simples, prevendo sua extensão por meio de cabeçalhos adicionais, e deixando-o com um

tamanho fixo de 40 bytes e apenas 8 campos. Deste modo, mesmo com um espaço de endereçamento de 128 bits, que é quatro vezes maior que os 32 bits do IPv4, o tamanho Total do cabeçalho IPv6 é apenas duas vezes maior que o do IPv4.

A sua versão final ficou com a estrutura baixo:

Figura 5: Estrutura Cabeçalho IPv6



Fonte: Livro Rede de Computadores, 4º Edição, Andrew S. Tanenbaum

6.1 Definições dos campos

- Versão (*Version*)

  Definição: Campo de identificação do Protocolo IP utilizado.

  Tamanho Campo: 4 bits.

- Classe de tráfego (*Traffic class*)

  Definição: é utilizado para definir diferentes classes e prioridades aos pacotes IPv6, facilitando assim, o tratamento dos dados provenientes de aplicações com exigências distintas. Este campo serve de base para o funcionamento do mecanismo de qualidade de serviço (QoS) na rede.

Tamanho Campo: 8 bits.

- Identificador de Fluxo (*Flow Label*)

  Definição: Indentifica e diferencia sequências de pacotes pertencentes ao mesmo fluxo de dados, que necessitem do mesmo tratamento para um processamento mais eficiente nos roteadores.

  Tamanho Campo: 20 bits.

- Tamanho dos Dados (*Payload Length*)

  Definição: Indica o volume de dados, em *bytes*, que o pacote transporta. Tamanho Campo: 16 bits

- Proximo cabeçalho (*Next Header*)

  Definição: indica o tipo de informação que se segue ao cabeçalho IPv6. Poderá ser um pacote da camada de transporte (TCP/UDP) ou um dos cabeçalhos de extensão.

  Tamanho Campo: 8 bits

- Limite de Encaminhamento (*Hop Limit*)

  Definição: Indica o numero máximo de roteadores pelos quais o pacote pode passar antes de ser descartado.

  Tamanho Campo: 8 bits.

- Endereço de Origem (*Source Address*):

  Definição: especifica o endereço de origem do pacote.

  Tamanho Campo: 128 bits.

- Endereço de Destino (*Destination Address*):

  Definição: especifica endereço de destino do pacote.

  Tamanho Campo: 128 bits.

6.2 Cabeçalho de extensão

Outra mudança retratada por Tananbaum (2003) sobre a nova estrutura do IPv6 é que diferentemente do IPv4, que inclui em seu cabeçalho todas as opções adicionais, no IPv6 essas informações são tratadas por meio de cabeçalhos de extensão.

Esses cabeçalhos localizam-se entre o cabeçalho base e o cabeçalho da camada de transporte.

Figura 6: Cabeçalho de Extensão IPv6

Fonte: Núcleo de Informação e Coordenação do Ponto BR

Não existe um limite para a quantidade de cabeçalhos de extensão que podem ser anexados ao cabeçalho base, porém, caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão adicionados em série formando uma “cadeia de cabeçalhos”.

Para se entender a definição de cada cabeçalho de extensão e saber qual o valor que está associado a eles no campo Próximo Cabeçalho do cabeçalho base, uma analise da tabela a segir deve ser feita:

Tabela 1: Tabela Cabeçalho de Extensão

Valor	Nome do cabeçalho	Definição
0	Hop-By-Hop	Transporta informações opcionais que são processadas em cada nó ao longo do caminho do pacote, incluindo a origem e o destino.
60	Destination Options	Transporta informações opcionais que são processadas apenas pelo destino final do pacote.
43	Routing	Utilizado no suporte a mobilidade do IPv6, ele armazena o endereço original de um nó móvel (Type 2).
44	Fragmentation	Utilizado pela origem para enviar pacotes maiores do que a Maximum Transmit Unit (MTU) de um caminho. Ao contrário do IPv4, a fragmentação no IPv6 não ocorre nos roteadores encontrados ao longo do caminho do pacote, apenas na origem, sendo re-agrupados no destino final.
51	Authentication	Utilizado pelo serviço IPSec (IP Security) para prover autenticação e garantia de integridade aos pacotes IPv6. Esse cabeçalho é idêntico ao utilizado no IPv4.
50	Encapsulating Security Payload	Também utilizado pelo IPSec, provê integridade e confidencialidade para os pacotes.

Fonte: Núcleo de Informação e Coordenação do Ponto BR

A ordem apresentada nessa tabela deve ser respeitada pelo nó de origem quando enviar um pacote contendo mais de um cabeçalho de extensão. No entanto, o nó de destino deve estar preparado para entender os cabeçalhos em qualquer ordem.

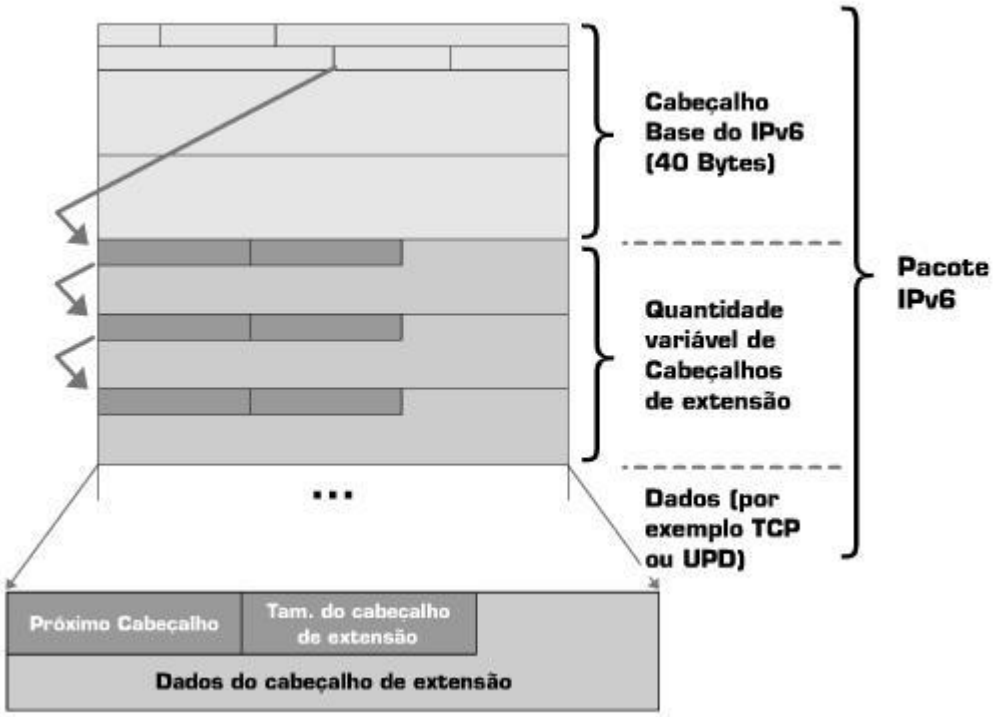
É importante destacar alguns outros aspectos sobre os cabeçalhos de extensão, como:

- Com a utilização desses cabeçalhos o tempo de processamento nos roteadores diminuiu, já que o roteador irá processar um único cabeçalho.
- Em caso de um endereço *multicast* no campo de Endereço de Destino, o cabeçalho de extensão será examinado por todos os pertencentes ao grupo *multicast*
- Um cabeçalho *Mobility* pode ser utlizado pelos nós que possuírem suporte a mobilidade IPv6.

6.3 Analise Final do cabeçalho

Para uma melhor compreensão da estrutura de um pacote IPv6, a próxima imagem permitirá uma observação do posicionamento de cada cabeçalho e a ordem em que eles são dispostos:

Figura 7: Estrutura de um Pacote IPv6



Fonte: Núcleo de Informação e Coordenação do Ponto BR

7 ENDEREÇAMENTO DO IPv6

Embora o tenha ocorrido diversas mudanças em toda a estrutura do IPv6, as principais alterações estão relacionadas ao modo de endereçamento do novo Protocolo. Como destaque houve o aumento no espaço para endereçamento no cabeçalho IPv6 e a sintaxe utilizada para representar os endereços.

O IPv6 possui em seu cabeçalho um espaço reservado para endereçamento de 128 bits, permitindo gerar 3,4 x 1038 endereços distintos, o que equivale à 56 octilhões (5,6 x 1028) de endereços por ser humano na Terra. Enquanto no IPv4 o endereçamento possui um espaço de apenas 32 bits.

No IPv4, os 32 bits dos endereços eram divididos em quatro grupos de 8 bits cada, separados por “.” e escritos com digitos decimais: 192.168.10.1 . Como observado por Tanenbaum (2003) no IPv6 o endereço é dividido em oito grupos de 16 bits, separados por “:” e escritos com digitos hexadecimais: 2001:0DB8:AD1F:25E2:DFA1:F0C4:5311:84C1.

Na apresentação de um endereço IPv6 é permitido utilizar caracteres maiusculos e minusculos, e utilizar regras de abreviação como:

- Omitir os zeros à esquerda;

- Representar os zeros continuos por “::”, esta abreviação só pode ser utilizada uma única vez, caso contrario haverá ambiguidades na representação do endereço.

Exemplo: 2001:0db8:0000:130F:0000:0000:087C:140b

2001:0db8:0:130F::087C:140b

A representação dos prefixos de rede continua sendo escrita do mesmo modo, utilizando a notação CIDR (*Classless Inter-Domain Routing).* Esta notação é representada na forma “endereço-IPv6/tamanho prefixo”, onde “tamanho do prefixo” é um valor decimal que especifica a quantidade de bits continuos à esquerda do endereço que compreendem o prefixo.

Exemplos: 2001:db8:3003::/48 e

2001:db8:3003:2:a:20ff:fe18:4c/64.

Esta representação possibilita a agregação dos endereços de forma hierarquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede. Assim é possivel diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

7.1 Tipos de Endereços

No IPv6 houve a definição de 3 tipos de endereços *Unicast, Multicast e Anycast.* Neste tópico será explicado com um pouco mais de detalhes essas novas funcionalidades. Como apresentado por Huston (2010) em suas pesquisas.

7.1.1 Unicast

Geoff Huston cita que os endereços *unicast* identificam apenas uma única *interface*. Desse modo, um pacote enviado a um endereço *unicast* é entregue a uma única *interface*. Há diversos tipos de endereços *unicast:*

- *Global Unicast*: é globalmente roteável e acessivel na Internet IPv6;
- *Link-local*: são atribuidos automaticamente e válidos apenas dentro do mesmo enlace, utilizando o prefixo FE80::/64, com espaço de 64 bits reservado para a identificação da *interface*;
- *Unique-local*: são globalmente únicos e utilizados apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces, não devendo ser roteáveis na *Internet* global. São identificados pelo prefixo FC00::/7 seguido de um ID global único de 40 bits gerado randomicamente.
- IPv4 mapeado em IPv6: possui o formato 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, onde wxyz é um endereço IPv4 convertido em hexadecimal, é usado para representar um endereço IPv4 como um endereço IPv6 de 128 bits. São utilizados em tecnicas de transição.
- *Loopback*: o endereço especial 0:0:0:0:0:0:0:1 ou ::1 é utilizado para identificar a própria *interface*.
- *Unspecified*: o endereço especial 0:0:0:0:0:0:0:0 ou ::0 é usado apenas para identifcar a ausencia de endereço.

7.1.2 *Multicast*

O *multicast* identifica um grupo de *interfaces* pertencente a diferentes nós, mas um pacote destinado a um endereço *multicast* é enviado para todas as *interfaces* do grupo.

Segundo Huston (2010) o endereço *multicast* deriva do bloco FF00::/8, onde o octeto, que se segue ao prefixo FF contêm quatro *flags*, que determinam o tempo de vida do pacote, e um valor de quatro bits que define o escopo do grupo *multicast*. O restante é utilizado para identificar o grupo *multicast*.

No IPv6 todos os nós devem ter suporte ao *multicast*, isso porque várias funcionalidades do IPv6 dependem dele e ele substituiu o *Broadcast*.

7.1.3 Anycast

É utilizado para identificar um grupo de *interfaces* que pertencem a nós diferentes. Um pacote destinado a um endereço *anycast* é enviado apenas para *interface* deste grupo mais próximo da origem.

Ele é útil para detectar rapidamente determinados servidores, serviços ou ainda para identificar um grupo de roteadores pertecentes a um ISP, um conjunto de roteadores conectados a uma mesma sub-rede ou identificar roteadores que proveêm a entrada para um dominio especifico.

7.2 Atribuições

Huston (2010) afirma que os endereços no IPv6 são atribuidos às *interfaces* físicas e não aos nós, do mesmo modo que era feito com o IPv4. Há a possibilidade de se atribuir a uma única *interface* múltiplos endereços, independente do seu tipo. Com isso, um nó pode ser identificado através de qualquer endereço de sua *interface.*

8 SERVIÇOS BÁSICOS DO IPv6

Este capítulo falará sobre o funcionamento dos novos protocolos e mecanismos IPv6, como ICMPv6, Descoberta de Vizinhança, autoconfiguração *stateless* e *stateful*, fragmentação. E também explicará sobre o suporte à Qualidade de Serviço e como funciona o sistema de nomes de dominio neste novo protocolo.

8.1 ICMP

O ICMP (*Internet Control Message Protocol*) é um protocolo integrante do IP e foi definido pelo RFC 792 com a função de fornecer relatórios de erros à fonte Original.

No IPv6 esse protocolo recebeu o nome de ICMPv6, mas tem basicamente as mesmas funções do protocolo ICMP para IPv4 que são:

- Informar as Características da Rede
- Realizar Diagnósticos
- Relatar erros no processamento de pacotes

Utilizando a RFC 4443 pode-se perceber que o ICMPv6 apresenta uma quantidade maior de mensagens, pois lhe foi incorporado as funções de outros protocolos , como ARP/RARP (*Address Resolution Protocol - Reverse Address Resolution Protocol*) e IGMP (*Internet Group Management Protocol*), sendo assim abrangendo as funções de: Descoberta de Vizinhança; Gerenciamento de Grupos *Multicast*; Mobilidade IPv6 e Descoberta do *Path* MTU, que são funções essenciais no IPv6.

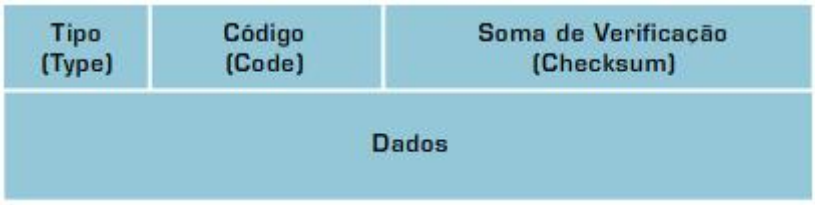
Para se obter as informações é necessário a troca de mensagens ICMIPv6, que são divididas em classes de ‘Mensagem de Erro’ e ‘Mensagem de Informação’.

Em um pacote de dados, o cabeçalho ICMPv6 é precedido pelos cabeçalhos de extensão e pelo cabeçalho base do IPv6. Sua estrutura geral é bem simples e igual nos dois tipos de mensagens:

Figura 8: Ilustração Geral ICMPv6

Fonte: Núcleo de Informação e Coordenação do Ponto BR

Figura 9: Estrutura Cabeçalho ICMPv6



Fonte: Núcleo de Informação e Coordenação do Ponto BR

- Tipo (*Type*): Indica o tipo da mensagem. Seu tamanho é de oito bits.
- Código (*Code*): Oferece informações adicionais para determinados tipos de mensagens. Seu tamanho é de oito bits também.
- Soma de verificação (*Checksum*): é usado para detectar dados corrompidos no cabeçalho ICMPv6 e IPv6. Seu tamanho é de dezesseis bits.
- Dados: São mostradas as informações de diagnóstico e erro de acordo com o tipo de mensagem. Seu tamanho varia de acordo com a mensagem.

As duas tabelas abaixo mostram todas as mensagens ICMPv6, de Erro e de Informação, definidas até o momento.

Nesta primeira trata sobre as mensagens de erro cadastradas até o momento no ICMPv6, que podem ser enviadas.

Tabela 2: Tabela de Mensagens de Erro do ICMPv6

Mensagens de Erro:		
Tipo	Nome	Descrição
1	*Destination Unreachable*	Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	*Packet Too Big*	Indica que o tamanho do pacote é maior que a Unidade Máxima de Transito (MTU) de um enlace.
3	*Time Exceeded*	Indica que o Limite de Roteamento ou o tempo de remontagem do pacote foi excedido.
4	*Parameter Problem*	Indica erro em algum campo do cabeçalho IPv6 ou que o tipo indicado no campo Próximo Cabeçalho não foi reconhecido.
100-101		Uso experimental.
102-126		Não utilizado.
127		Reservado para expansão das mensagens de erro ICMPv6.

Fonte: Núcleo de Informação e Coordenação do Ponto BR

E na tabela abaixo é mostrado quais são as possíveis mensagens de Informação mandadas pelo ICMPv6.

Tabela 3: Tabela de Mensagens de Informação do ICMPv6

Mensagens de Informação:		
Tipo	Nome	Descrição
128	*Echo Request*	Utilizadas pelo comando ping.
129	*Echo Reply*	
130	*Multicast Listener Query*	Utilizadas no gerenciamento de grupos multicast.
131	*Multicast Listener Report*	
132	*Multicast Listener Done*	
133	*Router Solicitation*	Utilizadas com o protocolo Descoberta de Vizinhança.
134	*Router Advertisement*	
135	*Neighbor Solicitation*	
136	*Neighbor Advertisement*	
137	*Redirect Message*	
138	*Router Renumbering*	Utilizada no mecanismo de Re-endereçamento (Renumbering) de roteadores.
139	*ICMP Node Information Query*	Utilizadas para descobrir informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de redes.
140	*ICMP Node Information Response*	
141	*Inverse Neighbor Discovery Solicitation Message*	Utilizadas em uma extensão do protocolo de Descoberta de Vizinhança.
142	*Inverse Neighbor Discovery Advertisement Message*	
143	*Version 2 Multicast Listener Report*	Utilizada no gerenciamento de grupos multicast.
144	*Home Agent Address Discovery Request Message*	Utilizadas no mecanismo de Mobilidade IPv6.
145	*Home Agent Address Discovery Reply Message*	
146	*Mobile Prefix Solicitation*	
147	*Mobile Prefix Advertisement*	
148	*Certification Path Solicitation Message*	Utilizadas pelo protocolo SEND.
149	*Certification Path Advertisement Message*	
150		Utilizada experimentalmente com protocolos de mobilidade como o Seamoby.
151	*Multicast Router Advertisement*	Utilizadas pelo mecanismo Multicast Router Discovery.
152	*Multicast Router Solicitation*	
153	*Multicast Router Termination*	
154	*FMIPv6 Messages*	Utilizada pelo protocolo de mobilidade Fast Handovers
200-201		Uso Experimental
255		Reservado para expansão das mensagens de erro ICMPv6

Fonte: Núcleo de Informação e Coordenação do Ponto BR

8.1.1 Descoberta de Vizinhança

No curso sobre IPv6 Básico, feito por Regis, Moreiras, Reis e Rocha, disponivel no site do Nucleo de Informação e Coordenação do ponto BR (NIC) é dito que este protocolo do IPv6 é utilizado por *hosts* e roteadores, tornando mais dinamicos alguns processos de configuração de rede em relação ao IPv4. Possui os seguintes propósitos:

- Determinar o endereço MAC dos nós da rede;
- Encontrar roteadores vizinhos;
- Determinar prefixos e outras informações de configuração da rede;
- Detectar endereços duplicados;
- Determinar as acessibilidades dos roteadores;
- Redirecionar pacotes;
- Autoconfiguração de endereços.

As cincos mensagens do ICMPv6 mais utilizadas pelo protocolo de Descoberta de vizinhança são:

- *Router Solicitation* (Tipo=133): utilizada pelos *hosts* para requisitar aos roteadores mensagens *Router Advertisements* imediatamente;
- *Router Advertisement* (Tipo=134): enviadas automaticamente ou em resposta à uma *Router Solicitation*, são usadas pelos roteadores para anunciar a sua presença em um enlace e na *Internet*;
- *Neighbor Solicitation* (Tipo=135): mensagem *multicast* enviada por um nó para determinar o endereço MAC e a acessibilidade de um vizinho, além de detectar a existência de endereços duplicados;
- *Neighbor Advertisement* (Tipo=136): enviada como resposta a uma *Neighbor Solicitation*, podendo também ser enviada para anunciar a mudança de algum endereço MAC dentro do enlace;

- *Redirect* (Tipo=137): utilizada por roteadores para informar ao *host* um roteador mais indicado para se alcançar um destino.

Esta mensagens são configuradas com o valor 255 no campo Limite de Roteamento do cabeçalho IPv6. Isso garante que as mensagens recebidas serão originadas de um nó do mesmo enlace. Elas podem conter, ou não, opções, conforme tabela abaixo:

Tabela 4: Opções das Mensagens do Protocolo de Descoberta de Vizinhança

Veja as opções:	
Mensagem	Atribuição
Source link-layer address	Utilizada em mensagens *Neighbor Solicitation*, *Router Solicitation*, e *Router Advertisement*. Nele está o endereço do remetente do pacote.
Target link-layer address	Utilizada nas mensagens de *Neighbor Advertisement* e *Redirect*. Contém o endereço de destino do pacote.
Prefix information	Fornece aos hosts os prefixos do enlace e os prefixos para que o endereço seja autoconfigurado. Utilizada em mensagens *Router Advertisement*.
Redirected header	Utilizada nas mensagens *Redirect*. Essa mensagem contém todo ou parte do pacote de redirecionamento.
MTU	Utilizada em mensagens *Router Advertisement*. Essa opção garante que todos os nós em um enlace usem o mesmo valor de *Maximum Transmission Unit* (MTU).

Fonte: Núcleo de Informação e Coordenação do Ponto BR

Com o conhecimento sobre os tipos de mensagens do ICMPv6 utilizadas pelo Protocolo de Descoberta de Vizinhança, será descrito agora algumas de suas funcionalidades, seguindo ainda as idéias demonstradas no curso IPv6 Básico citado acima e disponivel no NIC.br.

1. Descoberta de Endereços da Camada de Enlace

Esta funcionalidade é utilizada para determinar o endereço MAC dos vizinhos de mesmo enlance, onde o *Host* envia uma mensagem *Neighbor Solicitation* informando no campo de Dados seu endereço MAC e também solicitando o endereço MAC do vizinho. Ao receber a mensagem, o vizinho responde enviando uma mensagem *Neighbor Advertisement* com o seu endereço. Esta função é comparada ao protocolo ARP do IPv4, só que em vez de se utilizar um endereço *Broadcast* é utilziado um *Multicast*.

2. Descoberta de Roteadores e Prefixos

Esta funcionalidade é utilizada para localizar roteadores vizinhos dentro do mesmo enlace, e também para aprender prefixos e parâmetros relacionados à autoconfiguração de endereço. Para ser feito a descoberta é enviado uma mensagem de *Router Advertisement* a partir de um roteador local para o endereço *Multicast all-Nodes*. No IPv4, esse mapeamentoo é feito através da mensagem de ARP *Request.*

3. Detecção de Endereços Duplicados

No IPv4, os nós utilizam mensagens de ARP *Request* e um metodo chamado gratuitos ARP para detectar endereços *unicast* duplicados dentro do mesmo enlace.

4. Detecção de Vizinhos Inacessíveis

Para acompanhar o estado dos vizinhos, o nó IPv6 utiliza duas importantes tabelas:

- *Neighbor Cache*: mantem a lista de vizinhos locais para os quais foi enviado tráfego recentemente, com o endereço IP, informações sobre o endereço MAC e um *flag* indicando se o vizinho é um roteador ou *host*. Também é informado se ainda há pacotes na fila para serem enviados, a acessibilidade do vizinho e para quando esta agendada a proxima inacessibilidade. Esta tabela pode ser comparada a tabela ARP do Ipv4.

- *Destination Cache*: mantem as informações sobre destinos para os quais foi enviado tráfego recentemente, incluindo destinos locais e remotos. É atualizado com as informações recebidas pela mensagem *Redirect*.

5. Redirecionamento

Mensagens *Redirection* são enviadas pelos roteadores para redirecionar um host automaticamente a um roteador mais apropriado ou para informar ao host que o destino encontra-se no mesmo enlace. Existe este mesmo mecanismo no IPv4.

6. AutoConfiguração de Endereços *Stateless*

Permite que os nós façam as configurações automatica dos endereços em suas *interfaces*, sem a necessidade de utilizar um servidor DHCP.

8.2 AutoConfiguração de Endreços *Stateless*

Por ser umas das Funcionalidades ICMPv6 mais complexa, neste capitulo será detalhado o seu funcionamento, seguindo o estudo de Carlos Friaças e Pedro Lorga sobre este assunto que foi divulgado no sitio brasileiro do projeto 6Deploy.

Este mecanismo permite que endereços *Unicast* sejam atribuidos aos nós sem a necessidade de configurações manuais, sem servidores adicionais, apenas configurações minimas dos roteadores. A partir de informações enviadas pelos roteadores, em mensagens *Router Advertisement,* e de dados como o endereço MAC das *interfaces*, os nós IPv6 criam automaticamente endereços *Link-Local* únicos.

Esses endereços *Link-Local* são gerados como o prefixo FE80::/64. A esse prefixo é anexado o identificador de 64 bits da *interface* física. O Novo endereço passa então a fazer parte dos grupos *multicast solicited-node e all-node,* após isto, é feito a verificação de unicidade do endereço através do processo de detecção de endereços duplicados. Caso haja duplicidade o processo é interrompido e é necessario fazer a configuração manualmente, caso contrário ele será automaticamente inicializado para a *interface*. Para determinar quais roteadores pertencem ao enlace e quais os prefixos, o *host* envia uma mensagem *Router Solicitation* para o grupo *Multicast all-routers*. Feito tudo isso, todos os roteadores do enlace respondem com uma mensagem *Router Advertisement.*

Estas mensagens são utilizadas para configurar:

- Os roteadores padrão;
- Um valor predefinido para o campo Limite de Encaminhamento do cabeçalho IPv6;
- O valor de MTU do enlace;

- E a lista de prefixos de rede.

Para cada registro informado nas mensagens de *Router Advertisement*, é gerado um endereço através do mecanismo de autoconfiguração *Stateless*. E estas mensagens apresentam duas *flags*:

- *Managed Address Configuration*: indica se os *hosts* devem ou não utilizar autoconfiguração *Stateful* para obter endereços;
- *Stateful Configuration*: indica se os *hosts* devem utilizar a autoconfiguração *stateful* para obter informações adicionais, como endereços de servidores DNS outros dados sobre a configuração da rede.

8.3 Autoconfiguração *Stateful*

As informações abaixo são também encontradas na mesma apresentação do Carlos Friaças e Pedro Lorga sobre o nome de “Autoconfiguração (*Stateless, Stateful*)” comentada no capitulo anterior.

A autoconfiguração *Stateful* é uma tecnica alternativa a *stateless*, onde é necessária a utilização de servidores que informem aos *hosts*, os dados a serem utilizados na obtenção dos endereços, além de outras configurações da rede.

Esta tecnica é utilizada apenas quando não há roteadores na rede, ou quando há flags que habilitam seu uso. A autoconfiguração *Stateful* baseia-se no uso de protocolos, como o DHCPv6, a fim de obter endereços e outras opções de configuração.

O uso do DHCPv6 possibilita a distribuição dinamica de endereços IP em uma rede, fornecendo um controle maior na atribuição de endereços ao *host*. As trocas de mensagens feitas entre cliente e servidor utilizam o protocolo UDP.

Os clientes utilizam um endereço *Link-Local* para transmitir ou receber mensagens DHCP, enquanto os servidores utilizam um endereço *multicast* reservado (FF02::1:2 ou FF05::1:3) para receber mensagens dos clientes.

A utilização do DHCPv6 provê algumas vantagens em relação a autoconfiguração *Stateless*. Algumas são:

- Fornece opções de confgurações de rede, como endereços de servidores DNS, NTP, etc;
- Permite a definição de politicas de controle de acesso.

No entanto, é possivel utilizar os dois mecanismos simultaneamente. Por exemplo, utilizando a autoconfiguração *Stateless* para atribuir os endereços e DHCPv6 para informar o endereço do servidor DNS.

8.4 Fragmentação

O processo de fragmentação de um pacote de dados permite o envio de pacotes maiores que o limite de tráfego estabelecido de um enlace. A diferença de como isso é tratado no IPv6 e no IPv4 é bem sutil.

Numa transmissão de pacote IP, este pode passar por vários enlaces até chegar ao destino. Possivelmente, cada um desses enlaces possuirá uma limitação distinta em relação ao tamanho máximo do pacote que pode trafegar através dele, este tamanho máximo é chamado de MTU (*Maximum Transmit Unit*). Com o IPv4, cada roteador pode fragmentar os pacotes durante o percurso, caso eles sejam maiores que o MTU do enlace. Dependendo do desenho da rede, o pacote IPv4 pode ser fragmentado mais de uma vez no seu trajeto, sendo reagrupado no destino final.

Já no IPv6, o processo de fragmentação começa utilizando o protocolo *Path MTU Discovery* que descobre de forma dinamica qual o tamanho maximo permitido ao pacote, identificando previamente os MTUs e cada enlace no caminho do destino.

O *Path MTU Discovery* assume que o MTU de todo o caminho é igual ao MTU do primeiro salto. Caso haja no caminho algum roteador que não suporte o tamanho do pacote enviado, este irá descartá-lo e retornará uma mensagem de ICMPv6 *packet too big* e após o recebimento desta mensagem, o nó de origem reduzirá o

tamanho dos pacotes de acordo com o MTU do caminho indicado na mensagem *packet too big*. Este procedimento só termina quando o menor MTU é encontrado, e até lá várias mensagens podem ser trocados.

Deste modo, os nós IPv6 realizam a fragmentação dos pacotes apenas na origem, reduzindo o *overhead* do calculo dos cabeçalhos alterados nos roteadores intermediários.

Outro aspecto que o IPv6 se difere do IPv4 na questão do envio de pacotes é em relação aos *jumbograms.* No IPv4, o limite para tamanhos dos pacotes é de 64KB, no entanto, o IPv6 apresenta a opção do cabeçalho de extensão *Hop-by-Hop* chamada *Jumbo Playload.* Esta opção permite que o IPv6 envie pacotes com cargas úteis de 65.536 e 4.294.967.295 Bytes de comprimento, os *jumbograms.*

Reforçando a idéia Huston (2010) fez uma publicação falando sobre fragmentação em seu Website no artigo intitulado “A Tale of Two Protocols: IPv4, IPv6, MTUs and Fragmentation”.

8.5 DNS

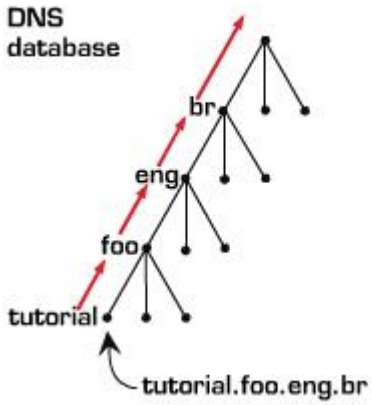
O DNS (*Domain Name System*) é uma imensa base de dados distribuida utilizada para a resolução de nomes de domínios em endereços IP e vise-versa.

Figura 10: Exemplo Resolução DNS

Fonte: Núcleo de Informação e Coordenação do Ponto BR

Sua arquitetura é hierárquica, com os dados dispostos em uma árvore invertida, distribuida eficientemente em um sistema descentralizado e com *cache*.

Figura 11: Hierarquia DNS



Fonte: Núcleo de Informação e Coordenação do Ponto BR

Embora os dados contidos na árvore de DNS sejam independentes da versão IP utilizada pelo servidor de DNS, algumas mudanças foram necessárias para que este servidores pudessem trabalhar com consultas a endereços IPv6.

Essas mudanças, definidas na RFC3596, incluem:

a. Novo Registro para armazenar endereços no formato IPv6:

- O AAA ou quad-A, que traduz nomes em endereços IPv6 (equivalente ao Registro “A”, que traduz nomes para endereços IPv4).

Exemplo: www.ipv6.br IN A 200.160.4.22

IN AAA 201:12ff:0:4::22

b. Uma nova representação textual para o registro PTR, que traduz endereços IPv6 em nomes, o dominio.

Exemplo: 2.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa

PTR www.ipv6.br

Um cliente DNS com suporte a IPv6, ao realizar uma consulta, busca primeiro por registros do tipo AAA, caso não haja resposta, faz uma consulta por registros do tipo A com o mesmo nome.

8.6 QoS

É muito importante garantir a qualidade do transporte do tráfego de aplicações, como VoIP, distribuição de vídeos de alta qualidade, jogos online, etc. Segundo Chow (2010) para garantir essa qualidade, é aplicado a Internet o conceito de QoS (*Quality of Service*).

O QoS é garantido na rede, através dos componentes e equipamentos utilizados no trafego dos dados. O IPv6 tentou solucionar esta questão através da implementação de especificações que priorizam o fluxo de determinados pacotes. Para isso foram designados dois campos do cabeçalho IPv6: o Classe de Trafego e o Indicador de Fluxo.

Os 20 bits do campo Identificador de fluxo são preenchidos com valores aleatórios entre 00001 e FFFFF. Caso o roteador ou *Host* não tenham suporte às funções do campo Identificador de fluxo, eles devem preencher este campo com zeros ou simplesmente ignorá-lo quando enviarem um pacote. Os pacotes de um mesmo fluxo são identificados quando enviados com o mesmo endereço de origem e destino, e o mesmo valor no campo Identificador de fluxo. Além de que, caso o pacote inclua em seu cabeçalho a opção *Hop-by-Hop*, esta opção também deverá ser incluida nos cabeçalhos dos outros pacotes.

A utilização dos 8 bits do campo Classe de Tráfego permite identificar e distinguir as diferentes classes ou prioridades de pacotes IPv6.

8.7 Suporte à Mobilidade

Davies (2008) defende que o Protocolo IPv6 já traz incorporado esta funcionalidade e este suporte à mobilidade permite, no IPv6, que um dispositivo móvel se desloque de uma rede para a outra sem a necessidade de alteração do

endereço IP de origem. Assim, mesmo que este dispositivo esteja fora de sua rede, os pacotes continuarão sendo encaminhados a ele usando o seu endereço de origem, fazendo com que a movimentação entre as redes fique invisivel para protocolos da camada superior.

Detalhadamente a funcionalidade funciona da seguinte maneira:

Quando o nó Móvel se desloca da sua rede de origem ele obtém um novo endereço IPv6 na rede remota. Para se ter a certeza de que os pacotes chegem a sua rede remota, é necessária a associação entre o endereço remoto e o Endereço de Origem, que é feita pelo Agente de Origem. Este Agente registra o Endereço remoto enviado em uma mensagem *Binding Update* pelo Nó móvel e responde com uma mensagem *Binding Acknowledgement*.

Após esta associação o encaminhamento de pacotes para o Nó Móvel pode acontecer de forma otimizada que é conhecido como:

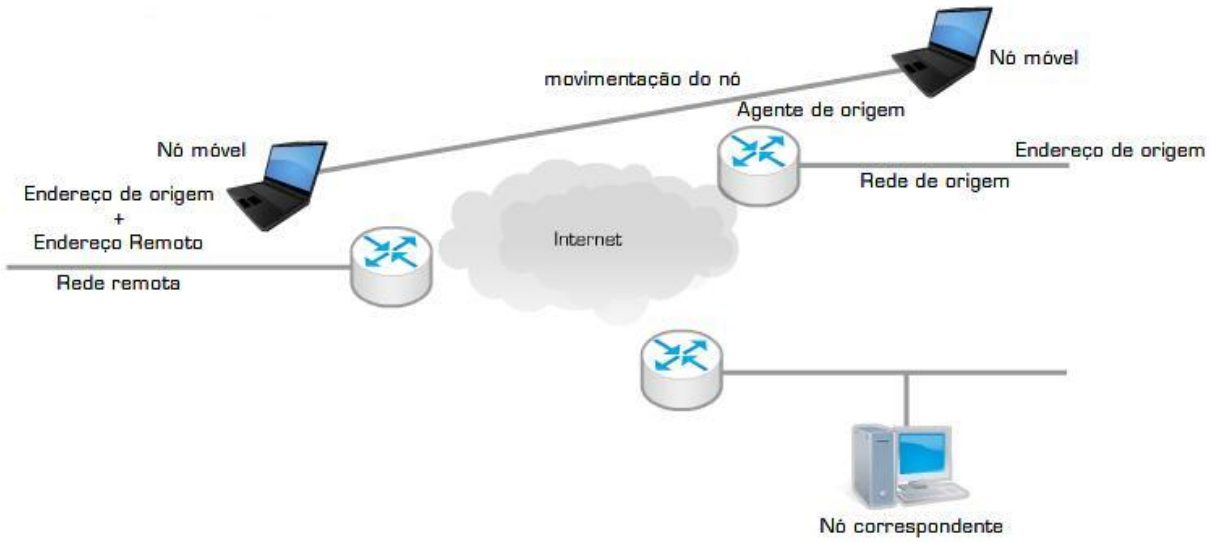
a. Otimização de Rota

Neste modo o nó móvel informa diretamente ao nó correspondente seu endereço Remoto, através do procedimento de *Correspondent Binding*.

O nó correspondente armazena em um *Cache* a associação entre o Endereço de Origem e o Remoto do Nó móvel. A partir dos dados desse *cache*, a comunicação passa a ser direta e sem utilizar um Agente de origem.

A figura a seguir demonstra todos os dispositivos que fazem parte do sistema de mobilidade do IPv6:

Figura 12: Dispositivos de Mobilidade do IPv6



Fonte: Núcleo de Informação e Coordenação do Ponto BR

Para a melhor eficiência da mobilidade do IPv6, este utiliza da estrutura do novo cabeçalho e o novo protocolo ICMPv6, e para isso:

- Um novo cabeçalho de Extensão, o *Mobility*, foi criado;
- Foi adicionado um novo tipo de Cabeçalho *Routing*, o *Type 2*;
- Foram criadas quatro novas mensagens ICMPv6:
    1. *Home Agent Address Discovery Request;*
    2. *Home Agent Address Discovery Reply*;
    3. *Mobile Prefix Solicitation*;
    4. *Mobile Prefix Advertisement*.

Comparando com o IPv4, o suporte a mobilidade IPv6:

- Não necessita implantar roteadores especiais na rede remota;
- Envia pacotes por meio do endereço remoto, evitando os problemas de segurança;

- Garante acessibilidade simétrica entre o nó móvel e o roteador padrão na rede remota por meio do processo de Detecção de Vizinhos Inacessíveis;
- Envia os pacotes por meio do cabeçalho de roteamento em vez de encapsulados;
- Utiliza o protocolo de Descoberta de Vizinhança, em vez de ARP, permitindo que o processo de intercepção dos pacotes não dependa da camada de enlace;
- Faz a busca por agentes utilizando *anycast*, garantindo que o nó móvel receba apenas a resposta de um único Agente de Origem. No IPv4 utiliza-se o *broadcast*, isto implica em uma resposta separada para cada Agente de orgiem existente;
- O uso do IPSec é recomendado para aumentar o nível de segurança neste tipo de comunicação.

9 SEGURANÇA

Tanenbaum (2003) apresenta que no início do Protocolo IPv4 não foi dado muita importância para a questão da segurança das informações, pois ele era usado somente em algumas redes de pesquisa acadêmica. Mas com o crescimento da Internet diversas ameaças à segurança da rede e ao tráfego de dados surgiram prejudicando várias transações entre empresas e consumidores. Com isso, tornou-se necessário acrescentar novos mecanismos ao protocolo original para garantir a confiabilidade do serviço.

9.1 IPSec

Moreiras (2010) observou que dentre esses novos mecanismos, destaca-se o IPSec (*IP Security*), um protocolo que implementa criptografia e autenticação de pacotes na camada de rede, criando uma solução de segurança fim-a-fim, garantindo a Confidencialidade, Integridade e Autenticidade dos dados.

Embora o funcionamento do IPSec seja basicamente o mesmo tanto no IPv4 como no IPv6, no segundo ele se tornou bem mais fácil de se usar:

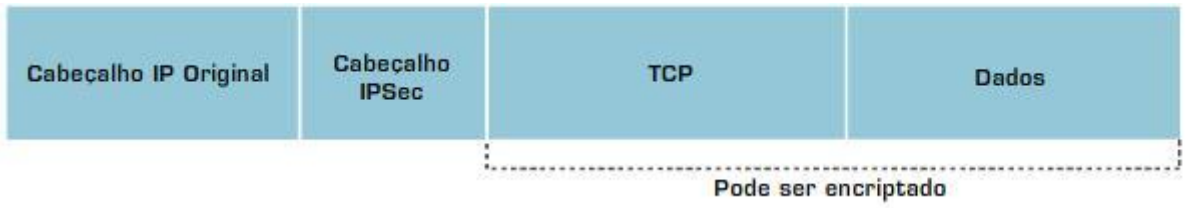
- Não há a necessidade de se utlizar NAT, permitindo que o IPSec funcione sem restrições;
- Os mecanismos de autenticação e encapsulamento do IPSec fazem parte do Protocolo;
- Seu suporte é obrigatorio em todos os nós, o que não ocorre no IPv4. Mas ele deve ser habilitado em cada nó pelos adminitradores de rede.

O IPSec é um *framework* de segurança, pois para realizar suas funções ele faz uso de recursos independentes. Sendo assim, ele utiliza dois cabeçalhos de Extensão do IPv6: o *Authentication Header*(AH), para garantir a autenticação; e o *Encapsulating Security Payload*(ESP) para garantir a confidencialidade dos pacotes transmitidos. Além de gerar e gerenciar chaves de segurança a partir do protocolo *Internet Key Exchange*(IKE).

Ele opera em dois modos:

a. Modo de Transporte: Protege apenas os protocolos das camadas superiores, pois o cabeçalho de segurança aparece logo após o cabeçalho IP e antes dos cabeçalhos dos protocolos das camadas superiores;

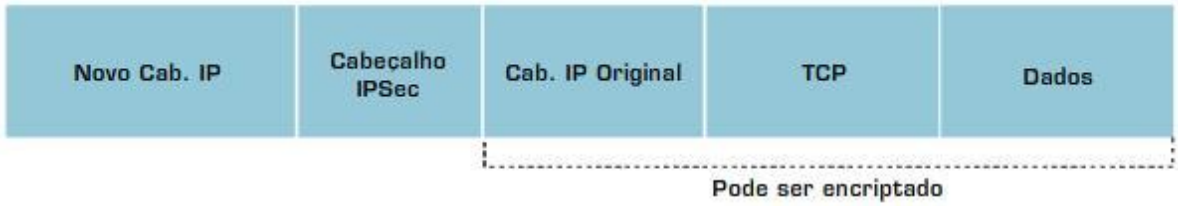
Figura 13: IPSec Modo Transporte



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

b. Modo Túnel: Protege todo o pacote IP, encapsulando-o dentro de outro pacote IP, deixando visível apenas o cabeçalho IP externo.

Figura 14: IPSec Modo Túnel



Fonte: Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações

Assim o IPv6 consegue garantir através do IPSec, que a mensagem recebida não tenha sido adulterada; a identidade do remetente; que a mensagem não seja entregue diversas vezes; e a confidencialidade da mensagem, criptografando seu conteúdo.

9.2 Outras Soluções

Embora o IPSec sirva para como proteção contra muitas ameaças à segurança, há ainda diversas outras ameaças aos dados que trafegam na rede, como:

- Ataques usando ICMPv6;
- Varredura de Endereços (*Scanning*);
- Ataques Físicos;
- Descoberta de Senhas;
- Vírus, Cavalos de Tróia e *Worms;*
- Ataques a aplicações;
- Ataques através de métodos de transição;
- *Man-in-the-middle*;
- Controle de acesso não autorizado;
- Acesso Acidental;
- Engenharia Social;
- Desastres Naturais.

Como exemplo, é possível citar que as mensagens ICMPv6, utilizado pelo protocolo de Descoberta de Vizinhança, não são protegidas pelo Protocolo IPSec, isto ocorre porque para autenticá-las utilizando o cabeçalho AH, é preciso que os nós tenham seu endereços já definidos para ocorrer a negociação de chaves pelo protocolo IKE. No entanto, isso torná-se inviável no processo de autoconfiguração de endereços.

E assim, os problemas de segurança relacionados à configuração de endereços tornam-se similares aos ocorridos com o protocolo ARP no IPv4.

Estas informações podem ser encontradas nos estudos feitos pelo Comitê Gestor da Internet no Brasil (CGI) e no trabalho de John Curran, divulgado pela IETF.

Para solucionar tais problemas o IETF (*Internet Engineering Task Force*) criou o grupo de trabalho chamado *Securing Neighbor Discovery* (SEND). Foi definido por este grupo um suporte para segurança do protocolo de Descoberta de Vizinhança que não exige configuração manual de endereços. Para isso, a proposta de solução contém os seguintes itens:

- A Criação de uma cadeia de certificados;
- A utilização de endereços gerados criptograficamente, assegurando que o transmissor de uma mensagem *Neighbor Advetisement* ou *Router Advertisement* seja o dono do endereço informado;
- Criação de uma nova opção *Neighbor Discovery*, chamada *Signature*, para proteger todas as mensagens relativas ao *Neighbor Discovery* e ao *Router Discovery;*
- Prevenção à ataques de reenvio de mensagens por meio de duas novas opções no *Neighbor Discovery*, que são: *TimeStamp* para endereços *multicast* e *Nonce* para endereços *unicast.*

Para a Segurança da rede, a grande vantagem trazida pela nova estrutura dos endereços IPv6 é que se tornou praticamente impossivel “varrer” (*Scanning*) toda a faixa de endereços de uma rede em busca de computadores para explorar suas falhas de seguranças, pois a quantidade de endereços possiveis com o novo protocolo IP é imensa.

Mas mesmo assim ainda é possivel se encontrar vitimas para esse tipo de ataque, como por exemplo, servidores públicos que divulgam endereços no DNS ou endereços que são atribuidos automaticamente com base no MAC.

Worms costumam utilizar a varredura de endereços para infectar outros dispositivos, mas sua propagação agora será dificultada por causa dessa nova estrutura do IPv6. E em relação aos métodos de proteção contra vírus, cavalos de Tróia e outros *Worms*, não existem mudanças substâncias com a utilização do IPv6.

É recomentado que se dê atenção especial às tecnicas de transição entre IPv4 e IPv6, pois estas podem funcionar como portas de entrada para novos tipos de ataques.

Contudo, assim como no IPv4, práticas simples podem evitar a ocorrência da maioria dos problemas de segurança, como a seguir:

- Programar corretamente o IPSec;
- Filtrar nos roteadores de borda endereços IPv6 internos;
- Filtrar as mensagens ICMPv6 seletivamente;
- Filtrar a entrada de pacotes com endereços de origem *multicast*;
- Utilizar mecanismos tradicionais de autenticação em roteadores de borda e IPSec em roteadores internos;
- Utilizar pilha dupla na migração, protegendo as duas pilhas com *firewall;*
- Dar preferência aos túneis estáticos, no lugar dos automáticos;
- Permitir a entrada de tráfego apenas de túneis autorizados.

10 ROTEAMENTO E GERENCIAMENTO

Será apresentado os principais protocolos de roteamento utilizados com o IPv6 e as diferenças apresentadas em relação ao IPv4. Para isto será utilizado como base o curso sobre IPv6 Básico, feito por Rodrigo Regis, Antônio M. Moreiras, Eduardo Reis e Ailton Soares da Rocha, disponivel no site do Nucleo de Informação e Coordenação do ponto BR (NIC).

10.1 Protocolos de Roteamento

Para Regis (2010), Moreiras (2010), Reis (2010) e Rocha (2010) os protocolos de roteamento são responsáveis por manter atualizadas as informações utilizadas pelos roteadores para encontrar o melhor caminho disponível no encaminhamento de pacotes de dados até o seu destino.

O processo de roteamento de um pacote de dados consiste em encaminhá-lo através de diversos roteadores até alcançar seu destino final. Estes roteadores buscam nas tabelas de roteamento o prefixo correspondente ao endereço de destino, e a partir da informação, determinam qual o melhor caminho a se percorrer.

Os protocolos de Roteamento são usados para se fazer o gerenciamento e sincronização das tabelas de roteamento de forma dinâmica. Estes protocolos são divididos em dois tipos:

1. Internos

Protocolos que distribuem as informações dos roteadores dentro de Sistemas Autônomos (AS - *Autonomous System*) são chamados de *Interior Gateway Protocols* (IGP).

Como Protocolo de roteamento Interno existe o OSPFv3, que é do tipo *link-state*. É através do processo de *flooding* que os roteadores constroem um mapa da rede, utilizado para definir as rotas mais curtas dentro do enlace. Este processo consiste na propagação de mensagens *Link State Advertisements* (LSA), onde cada roteador irá informar todos os estados dos enlaces que conhece aos roteadores

vizinhos. Assim com o conjunto das LSAs, todos os roteadores formam um banco de dados de estado do enlace idêntico.

Pelo OSPFv3 ser uma versão exclusiva do IPv6, algumas alterações ocorreram em relação a versão do OSPFv2:

- Foram criados novos tipos de LSAs;
- a autenticação foi retirada, contando apenas com a autenticação do IPv6;
- A conexão entre *interfaces* é feito por enlace, enquanto no IPv4 era feita por sub-rede;
- Um único enlace pode ter múltiplas instâncias do OSPFv6 sendo executadas;
- Os pacotes OSPF usam um endereço *link-local* como endereço de origem;
- São utilizados os seguintes endereços *multicast: AllSPFRouter* (FF02::5) e *ALLDRouters* (FF02::6)

É utilizado também no IPv6 como protocolo de roteamento interno, o protocolo IS-IS. Este não teve uma nova versão desenvolvida, apenas foram adicionadas novas funcionalidades à versão já existente. Foram adicionados dois novos TLV (*Tag/Length/Values*) para IPv6:

- IPv6 *Reachability*
- IPv6 *Interface Address*

E um novo identificador da camada de rede, o IPv6 NLPID.

2. Externos

Protocolos que distribuem as informações entre AS distintos são chamados de *Exterior Gateway Protocols* (EGP).

Como protocolo de roteamento externo é utilizado o BGP. Como não se tem uma versão de BGP específica, a nova versão do IP utiliza as extensões multiprotocolo do BGP ou *Multiprotocol Border Gateway Protocol* (MBGP). Essas extensões suportam as mesmas funcionalidades que o BGP para IPv4 e trabalham

com as duas familias de endereços, IPv4 e IPv6.
Esta capacidade de trabalhar com diversos protocolos de rede, é possivel por causa da adoção de identificadores, que atuam na identificação do protocolo a ser suportado, que são o *Address Family Identifier* (AFI) e *Subsequent Address Family Identifier* (Sub-AFI).

Outro protocolo de roteamento é o RIPng, baseado em um algoritmo *distance-vector* conhecido como Bellman-Ford. Este protocolo segue os principais conceitos do RIPv2 utilizado pelo IPv4.

As principais mudanças do RIPng são o suporte aos prefixos e ao tamanho dos endereços IPv6, e por se tratar de um protocolo especifico do IPv6, utiliza como endereço de destino para mensagens RIP *Update* o endereço *multicast ALL RIP Routers* (FF02::9).

10.2 Gerenciamento de Rede

Ainda seguindo as idéias de Regis (2010), Moreiras (2010), Reis (2010) e Rocha (2010), eles afirmam que através da troca de informações entre dispositivos de rede, é possivel detectar e solucionar problemas, gerenciar seu desempenho, controlar equipamentos e outras atividades que permitem melhorar o desempenho da rede.

Umas das principais ferramentas para se fazer esse gerenciamento é o protocolo SNMP (*Simple Network Management Protocol*), utilizada tanto em rede IPv4 quanto em IPv6. Seu funcionamento baseia-se na utilização de um agente e de um gerente. Cada dispositivo gerenciado deve possuir um agente e uma base de dados referente ao seu estado atual, podendo ser consultada e alterada pelo gerente. Esse conjundo de dados é conhecido como MIB (*Management Information Base*) e possui especificações definidas por um padrão próprio.

A troca de informações entre o gerente e o agente SNMP pode ser realizada tanto por conexões IPv4 quanto por conexões IPv6, mesmo que as informações sejam sobre o IPv6. Mas também há diversos equipamentos com suporte a SNMP sobre IPv6 que podem ser monitorados em redes com conexão apenas IPv6. É

também necessário que as MIBs sejam capazes de recolher informação sobre a rede IPv6.

Apesar de o SNMP ser o mais utilizado devido a sua simplicidade, quando se necessita de uma análise mais detalhada da rede, aplica-se uma abordagem alternativa que consiste em recolher informações sobre cada pacote.

Neste método, equipamentos de rede enviam periodicamente informações sobre um determinado fluxo de dados para um dispositivo chamado coletor, que armazena e interpreta esses dados.

Os principais protocolos utilizados para a transmissão de informações sobre um fluxo IP de uma rede, como por exemplo, a versão 9 do *NetFlow* (Cisco *Systems*) e o IPFIX *(IP Flow Information Export)*, já estão preparados para coletar dados sobre o tráfego IPv6.

Os protocolos para gerenciamento das configurações dos equipamentos também já podem ser utilizados em rede IPv6, seja através da execução remota de comandos ou de transferência de arquivos, os protocolos SSH, TELNET, SCP, FTP e TFTP já apresentam suporte ao novo protocolo IP.

Um dos quesitos mais importantes no gerenciamento de redes é a sincronização dos relógios dos computadores, pois isto reflete de forma significativa no funcionamento de *softwares* e sistemas, além da segurança dos computadores, redes e da *Internet*. Então para se evitar problemas de sincronização se utiliza o protocolo NTP (*Network Time Protocol*), com ele é possivel manter o relogio do computador sempre com a hora certa e com exatidão de milesimos de segundo. Esta sincronização pode ser feita através de um servidor NTP público.
Para a rede IPv6 o processo é o mesmo, o único detalhe é que é preciso se conectar a servidores que já possuam suporte ao novo protocolo. No Brasil os servidores NTP públicos que já tem esse suporte são:

- a.ntp.br
- ntp.pop-sc.rnp.br
- ntp.pop-rs.rnp.br
- ntp.cert-rs.tche.br

11 COEXISTÊNCIA E TRANSIÇÃO

Atualmente toda a estrutura da Internet está baseada no protocolo IPv4. Deste Modo, uma troca imediata de protocolo é inviável, dado o tamanho e a proporção que esta rede possui. Com isso, para uma adoção bem sucedida do IPv6, é preciso que ela seja realizada de forma gradual e transparente para a maioria dos usuários.

Então, nesta fase inicial de transição haverá um periodo de coexistência entre os dois protocolos, em que redes IPv4 precisarão comunicar-se com redes IPv6 e vice-versa.

Para que esse coexistencia seja possível, foi necessário o desenvolvimento de algumas técnicas que visam manter a compatibilidade de toda a base das redes instaladas sobre IPv4 com o novo protocolo IPv6. Estas técnicas de transição podem ser classificadas nas seguintes categorias:

1. Pilha Dupla

Provê o suporte a ambos os protocolos no mesmo dispositivo.

2. Tunelamento

Permite o trafego de pacotes IPv6 sobre estruturas de rede IPv4, ou o inverso.

3. Tradução

Possibilita a comunicação entre nós com suporte apenas a IPv6 com nós que suportem apenas IPv4 e vice-versa.

Cada uma das técnias apresenta uma característica específica, podendo ser utilizada individualmente ou em conjunto, de modo a atender as necessidades de cada situação.

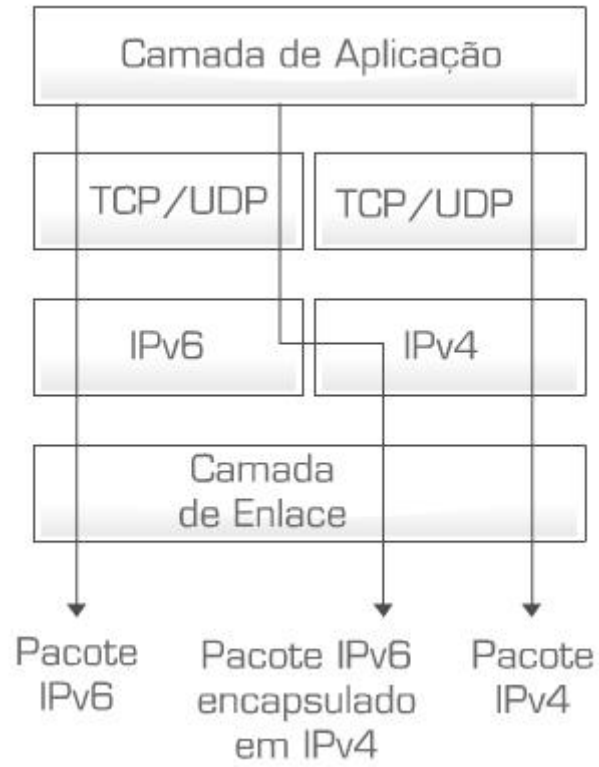
11.1 Pilha Dupla

No método de transição da Pilha Dupla, explicado por Huston (2011), *Hosts* e roteadores tornam-se capazes de enviar e receber pacotes tanto para o IPv4 quanto para o IPv6. Este método permite que um nó Pilha Dupla, ao se comunicar com um

nó IPv6, se comporte como um nó IPv6 e na comunicação com um nó IPv4, como nó IPv4.

Para que isto ocorra, cada nó IPv4/IPv6 é configurado com ambos os endereços, utilizando mecanismos como o DHCP para endereços IPv4 e mecanismos do IPv6 para endereços IPv6.

Figura 15: Pilha Dupla



Fonte: Núcleo de Informação e Coordenação do Ponto BR

Para ser feita a implantação dessa técnica, é exigido a análise de alguns dos seguintes aspectos:

- Configuração dos Servidores de DNS: é recomendado que estes servidores estejam habilitados a resolver nomes e endereços de ambos os protocolos.

- Configuração dos Protocolos de Roteamento: Caso a rede onde será implementada a Pilha Dupla utilize um protocolo de roteamento interno com suporte apenas para um dos Protocolos, por exemplo, o OSPFv2 (só suporta IPv4), será necessário migrar para um protocolo de roteamento que suporte tanto IPv4 quanto IPv6, como IS-IS, ou forçar a execução de um IS-IS ou ISPFv3 em paralelo com o OSPFv2.

- Configuração dos *Firewalls*: A filtragem dos pacotes que trafegam na rede pode depender da plataforma utilizada. Em alguns Sistemas Operacionais, os filtros de pacotes são totalmente independentes, não compartilhando nenhuma configuração, já em outros, as regras são aplicadas a ambos os protocolos, a menos que se restrinja explicitamente a qual família de protocolo as regras se aplicam.

11.2 Tunelamento

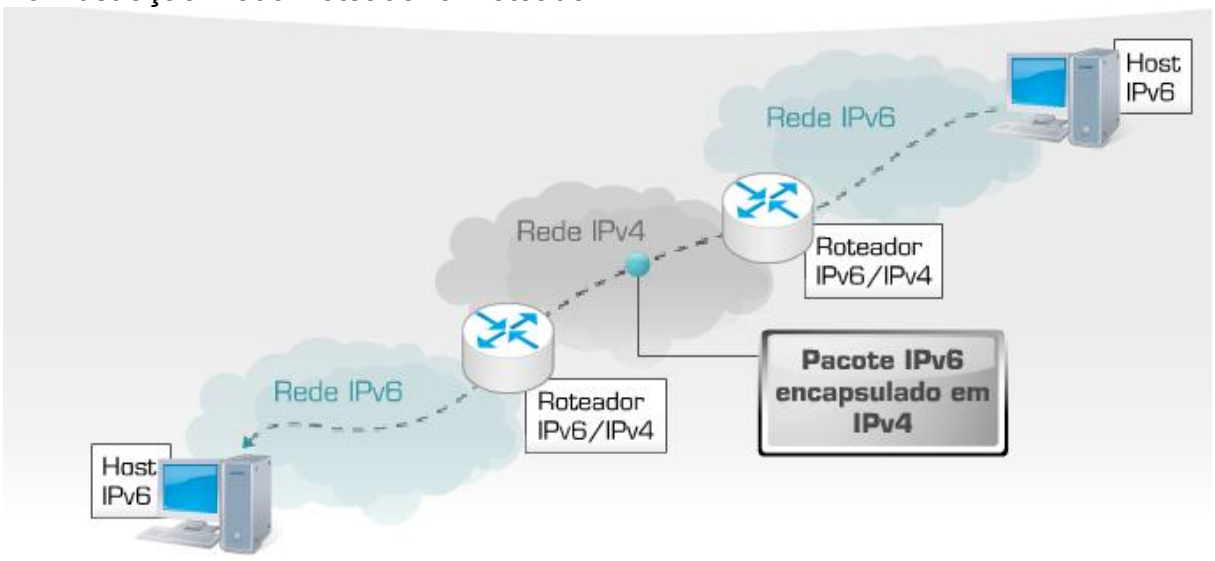
A técnica de Tunelamento permite transmitir pacotes IPv6 através da Infraestrutura IPv4, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, pois encapsula o conteúdo do pacote IPv6 em um pacote IPv4.

De uma maneira geral, o funcionamento de um túnel é bem simples. O nó de entrada do túnel, cria um cabeçalho IPv4 com o pacote IPv6 encapsulado e o transmite através da rede IPv4. Este processo de encapsulamento, conhecido como 6in4, é identificado como protocolo do tipo 41.

Podem-se classificar os Túneis nos modos:

- Roteador-a-Roteador: roteadores IPv4/IPv6, conectados via rede IPv4, trocam pacotes IPv6 entre si, ligando um segmento no caminho entre dois *hosts*.

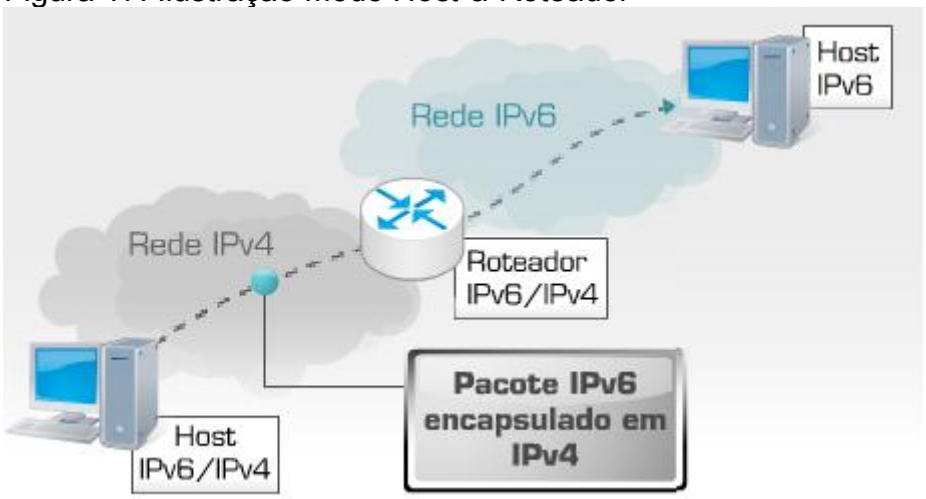
Figura 16: Ilustração Modo Roteador-a-Roteador



Fonte: Núcleo de Informação e Coordenação do Ponto BR

- *Host*-a-Roteador (ou Roteador-a-*Host*): os *hosts* IPv6/IPv4 enviam pacotes IPv6 a um roteador IPv6/IPv4 intermediário via rede IPv4, ligando o primeiro segmento no caminho entre dois *hosts*. No caminho inverso, os roteadores enviam pacotes IPv6 ao destino final IPv6/IPv4, ligando o último segmento do caminho entre dois *hosts.*

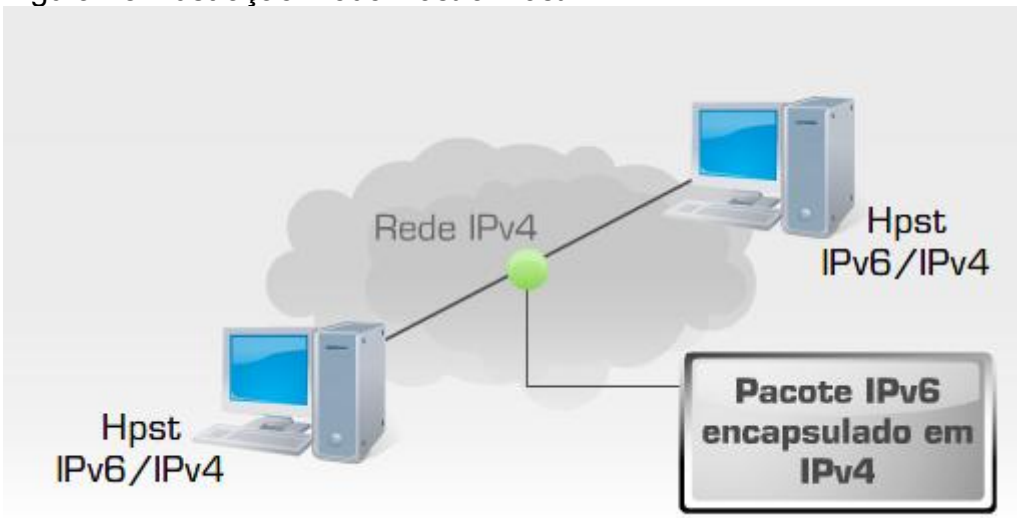
Figura 17: Ilustração Modo *Host*-a-Roteador



Fonte: Núcleo de Informação e Coordenação do Ponto BR

- *Host*-a-*Host: Hosts* IPv6/IPv4, conectados via rede IPv4, trocam pacotes entre si, ligando todo o caminho entre os dois *hosts.*

Figura 18: Ilustração Modo *Host*-a-*Host*



Fonte: Núcleo de Informação e Coordenação do Ponto BR

Há ainda diversas técnicas de tunelamento disponíveis, por este motivo, é necessária uma análise detalhada de cada uma, pois os cenários onde podem ser aplicadas, as dificuldades de implementação e a diferença de desempenho variam significativamente entre cada modelo. A seguir um detalhamento sobre as tecnicas de *Tunnel Broker*, 6to4, ISATAP, Teredo, GRE, seguindo as idéias do artigo "Transitioning Protocols" escrito por Geoff Huston:

- *Tunnel Broker*

Permite que hosts isolados em uma rede IPv4 acessem redes IPv6. Para utilizar é preciso se cadastrar em um provedor de acesso *Tunnel Broker* e realizar *download* de um *software* ou *script* de configuração. A conexão do túnel é feita através da solicitação do serviço ao Servidor *Web* do provedor. Caso o provedor de *Tunnel Broker* utilizado esteja geograficamente distante, isto pode interferir negativamente na velocidade de transmissão dos dados.

- *6to4*

É um tunelamento roteador-a-roteador, que permite a comunicação entre *hosts* IPv6 através de uma infraestrutura IPv4, fornecendo um endereço IPv6 único, formado pelo prefixo de endereço Global 2002:wwxx:yyzz::/48, onde wwxx:yyzz é o endereço IPv4 público do *host* convertido para hexadecimal.

- ISATAP

Possibilita a criação de túneis que ligam *hosts* a roteadores através de uma rede IPv4. O endereço IPv6 que será atribuido aos *hosts* e roteadores é baseado em um prefixo *unicast* de 64 bits, um prefixo 6to4, ou um prefixo global atribuído por um provedor, seguido por ::0:5EFE:w.x.y.z ou ::200:5EFE:w.x.y.z, onde w.x.y.z representa o endereço IPv4 do *host* ou roteador, e os valores 0:5EFE e 200:5EFE indicam se esse endereço IPv4 é privado ou público, respectivamente.

- Teredo

Permite o trafego IPv6 atraves de NAT, encapsulando o pacote IPv6 em pacotes UDP. Para utilizar este tipo de túnel, o cliente deve conectar-se a um Servidor Teredo, que define o endereço IPv6 do cliente e em qual tipo de NAT ele se

encontra. Após isto, o Servidor estabelecerá a conexão inicial com o *host* IPv6 de destino e este *host* manterá a conexão com a origem através de um *Relay* Teredo mais próximo dele.

- GRE

Generic Routing Encapsulation (GRE) é um túnel manual e estático entre dois *hosts*, que foi desenvolvido justamente para encapsular vários tipos diferentes de protocolos. Este tipo de encapsulamento consiste em um *link* ponto a ponto e é suportado pela maioria dos Sistemas Operacionais e roteadores.
O seu funcionamento consiste em pegar os pacotes originais, adicionar o cabeçalho GRE, e enviar ao IP Destino, quando o pacote encapsulado chega na outra ponta do Túnel, é removido dele o cabeçalho GRE, sobrando apenas o pacote original, o qual é encaminhado normalmente ao destinatário.

11.3 Tradução

Rodrigo Regis dos Santos explica em seu artigo “Técnica de Transição”, disponivel no Website ipv6.br, que a Tradução atua de diversas formas e em camadas distintas, traduzindo cabeçalhos IPv4 em cabeçalhos IPv6 e vice-versa, realizando conversões de endereços, de APIs (*Application Program Interface*) de programação, ou atuando na troca de trafego TCP ou UDP.

Figura 19: Mecanismo de Tradução

Fonte: Núcleo de Informação e Coordenação do Ponto BR

Os principais mecanismos de Tradução são:

- SIIT (*Stateless IP/ICMP Translation*)
- BIS (*Bump in the Stack*)
- BIA (*Bump in the API*)

- TRT (*Transport Relay Translator*)
- SOCKS64 (*Socks-Based IPv6/IPv4 Gateway*)
- ALG (*Application Layer Gateway*)

Todos eles possuem basicamente a mesma função, só se diferenciando em poucos detalhes.

12 INFORMAÇÕES ADICIONAIS

A seguir serão apresentados sites e documentos técnicos onde se pode encontrar e ter um aprofundamento maior sobre o IPv6.

12.1 Informações sobre IPv6 em Português

- http://ipv6.br - este *site* faz parte do projeto IPv6.br e tem como objetivo divulgar informações sobre esta nova versão do Protocolo, ajudando a criar condições para sua implantação nas redes e na Internet brasileira.
- http://portalipv6.lacnic.net/pt-br: é o *site* do LACNIC onde se pode encontrar informações relevantes e atualizadas, experiências, apresentações e outros tipos de dados que contribuem à transição e adaptação ao novo protocolo IPv6.
- http://maputo.ip6.fccn.pt: *Site* que apresenta um tutorial sobre IPv6, com material desenvolvido pelo projeto *6deploy*, além de exercicios de laboratorio utilizando o novo Protocolo *Internet.*

12.2 Informações sobre IPv6 em Inglês

- http://www.ipv6.org: *Site* que possui várias informações sobre IPv6, como lista de alguns *softwares* que já estão preparados para IPv6, tutoriais de como instalar o novo protocolo em alguns sistemas, lista de alguns *sites* que já operam em IPv6.
- http://www.ipv6forum.com: Disponibiliza fórum, base de conhecimento e alguns estudos sobre IPv6 e a sua implementação
- http://www.6deploy.com: site do projeto Europeu *6DEPLOY*, que disponibiliza diversos tutoriais e publicações a respeito do IPv6.
- http://www.potaroo.net: Contém diversos artigos sobre IPv6, além de estatisticas e gráficos sobre quantidade de números IPv4 utilizados, restantes e o tempo para sua exaustão.

12.3 RFCs sobre IPv6

- RFC1752: *The Recommendation for the IP Next Generation Protocol*
- RFC2460: *Internet Protocol, Version 6 (IPv6) Specification*
- RFC3315: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC3596: *DNS Extensions to Support IP Version 6*
- RFC4213: *Basic Transition Mechanisms for IPv6 Hosts and Routers*
- RFC4291: *IP Version 6 Addressing Architecture*
- RFC4301: *Security Architecture for the Internet Protocol*
- RFC4302: *IP Authentication Header*
- RFC4303: *IP Encapsulating Security Payload (ESP)*
- RFC4861: *Neighbor Discovery for IP version 6 (IPv6)*

- RFC4862: IPv6 Stateless Address Autoconfiguration

13 CONSIDERAÇÕES FINAIS

A partir da apresentação e análise dos dados, observa-se que, com o decorrer do tempo, e com o grande desenvolvimento Global da área tecnologica, a estrutura de rede Internet e seu atual protocolo, o IPv4, utilizado para a comunicação entre os diferentes tipos de redes e com a função de também possibilitar que novos usuarios, equipamentos e aplicações se conectem a rede, não é mais suficiente, além de que a segurança programada inicialmente para ele já está ultrapassada, o que dá vasão à ataques, caso outros artificios não sejam utilizados em conjunto.

Só que a criação de um novo Protocolo foi necessária, pois no começo o seu antecessor foi muito mal distribuido, ocasionando o seu rápido esgostamento. Quando este fato foi percebido pelos profissionais responsaveis, eles tentaram usar soluções paliativas para retardar o seu esgotamento, até que uma solução permanente fosse criada. Essa solução teve o nome inicial de IPng (Internet Protocol - next generation), que mais tarde se oficializou e tornou-se o IPv6.

Este projeto tomou por base toda a estrutura do IPv4, mas muito foi melhorado e outras funções criadas para se atender os requisitos para este novo mundo globalizado em que estamos vivendo. Por exemplo houve o aumento da capacidade de espaço para endereçamento, que passou de 32 bits para 128 bits. E nesse novo formato de endereços tem-se um encaminhamento mais eficiente dos pacotes de Dados, Facilidade na distribuição de IPs fixos e válidos para conexões DSL, *Cable Modens*, e telefones móveis e eliminação dos problemas associados ao NAT. Outra grande mudança que vale ser citada é o formato do cabeçalho, que se tornou mais simples e eficiente reduzindo o processamento dos roteadores. Além de que, no quesito segurança está bem mais aprimorada, pode-se observar isso no IPSec, por exemplo, que embora o seu funcionamento seja basicamente o mesmo tanto no IPv4 como no IPv6, no segundo ele se tornou bem mais fácil de se usar e é obrigatório.

No entanto, é importante ressaltar que essa transição não vai ocorrer da noite para o dia, o que é até inviavel, tanto financeiramente quanto estruturalmente, no momento está ocorrendo o periodo de coexistencia, onde os dois protocolos estão

sendo usados simultaneamente através de técnicas como pilha dupla, tunelamento e Tradução, para que todos possam se adaptar corretamente para receber esta nova tecnologia de comunicação entre redes, sem prejuizos.

O IPcalipse, como é chamado por alguns autores, ocorreu no dia 02/02/2011 e o ultimo bloco de endereços IPv4 foi dado para os países Asiáticos, segundo informou o IANA.

O Fim do IPv4 não causaria o fim da Internet e nem um *crash* mundial, apenas não seria mais possivel a adessão de novos aplicativos na Internet, o que não se pode deixar acontecer neste mundo globalizado de hoje, onde a cada segundo uma nova conexão é feita na Rede Mundial. Através disto, conclui-se que o IPv6 veio com o principal objetivo de suprir primeiramente esta necessidade de faltas de endereços.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Fernando. **TCP/IP Internet: Protocolos e Tecnologias** 3º Edição. Editora Axcel Books, 2001.

DAVIES, Joseph. **Understanding IPv6** 2º Edição. Editora Microsoft Press, 2008

HAGEN, Silvia. **IPv6 Essentials**. Editora Oreilly & Assoc, 2006.

HUSTON, Geoff. Artigos Disponíveis em:
http://www.potaroo.net. Acesso em 15 Jan. 2011. 10h22.

KUROSE, James F.. **Redes de Computadores e a Internet** 3º Edição. Editora Addison-Wesley, 2006

MALONE, David. **IPv6 Network Administration**. Editora Oreilly & Assoc, 2005

TANENBAUM, Andrew Stuart. **Redes de Computadores** 4º Edição. Editora Campus, 2003

Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil Disponível em:
http://www.cert.br/. Acesso em 20 Mai. 2011. 14h15.

Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações Disponível em:
http://ceptro.br/. Acesso em 21 Mai. 2011. 20h

Centro de Estudos sobre as Tecnologias da Informação e da Comunicação Disponível em:
http://cetic.br/. Acesso em 20 Mai. 2011. 16h30.

Comitê Gestor da Internet no Brasil Disponível em:
http://cgi.br/. Acesso em 10 Dec. 2010. 15h42.

Guia do Hardware Disponível em:
http://www.guiadohardware.net/termos/ipv6. Acesso em 14 Abr. 2011. 16h11.

Info Wester Disponível em:
http://www.infowester.com/internetprotocol.php. Acesso em 10 Mar. 2011. 10h24.

IPv6 Dissemination Disponível em:
http://www.6diss.org. Acesso em 05 Fev. 2011. 11h.

Núcleo de Informação e Coordenação do Ponto BR Disponível em:
http://www.nic.br/index.shtml. Acesso em 16 Dec. 2010. 10h25.

Projeto 6Deploy Disponível em:
http://www.6deploy.com – Acesso em 21 Fev. 2011. 13h45.

Registro de Domínios para Internet no Brasil Disponível em
http://registro.br. Acesso em 14 Mai. 2011. 10h24.

Web Page para IPv6.br Disponível em:
http://www.ipv6.br. Acesso em 12 Mai. 2011. 13h45.

Web Page Disponível em:
http://www.fayerwayer.com.br/2010/11/faltam-cerca-de-100-dias-para-o-ipcalipse/.
Acesso em 14 Abr. 2011. 14h52

Web Page Disponível em:
http://www.kplus.com.br/materia.asp?co=11&rv=Vivencia. Acesso em 10 Mar. 2011.
12h15.