MEC – SETEC
SERVIÇO PÚBLICO FEDERAL
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO
CAMPUS CUIABÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

ESTRATÉGIAS DE IMPLEMENTAÇÃO IPV6

BARROS JUNIOR, Jose Carlos

Orientador: Professor André Valente do Couto

RESUMO: Este trabalho apresenta conceitos das técnicas de transição do atual protocolo IPv4 para o protocolo IPv6. A pesquisa baseia-se em conhecer os principais mecanismos de transição descrevendo brevemente a estrutura do atual protocolo IPv4, suas características e os motivos do seu esgotamento e, como as redes IPv4 existentes podem coexistir com a nova geração do protocolo IPv6 através de técnicas como o tunelamento.

Palavras-chave: IPv4, IPv6, Transição, Coexistência, Tunelamento

ABSTRACT: This work presents concepts of the techniques of transition from the current protocol IPv4 to protocol IPv6. The research is based on revealing the main transition mechanisms describing briefly the structure of the current IPv4 protocol, its characteristics and the reasons for its depletion and, as the existing IPv4 networks can coexist with the new generation of IPv6 through techniques such as tunneling.

1 INTRODUÇÃO

A crescente utilização da internet e o aumento de novos hosts conectados a ela, estão ocasionando um esgotamento de endereços, necessitando assim da implementação de um novo protocolo capaz de suportar essa demanda. Esse novo protocolo, chamado Protocolo de Internet versão 6, o IPv6, é a versão aperfeiçoada da atual versão IPv4. Segundo Santos et al., (2010), o aperfeiçoamento do IPv6 abrange os seguintes aspectos: segurança melhorada, aumento na disposição de

endereços, retirada do broadcast, simplificação do cabeçalho, suporte a cabeçalhos de extensão, autenticação e privacidade.

Este trabalho tem como objetivo apresentar os mecanismos de transição utilizados para realizar a comunicação entre a atual versão do protocolo IPv4 com o Ipv6.

1.1 O Esgotamento de Endereços IPv4

A Internet não foi projetada inicialmente para uso comercial. Desde os anos 70 utiliza-se o protocolo IP para a comunicação em rede e a partir do início dos anos 80 o IPv4, versão atual do protocolo, passou a ser um dos protocolos mais utilizados no mundo (Obelheiros, 1999). O IPv4 é um protocolo bastante estável e robusto e é baseado em 32 bits, logo são possíveis $2^{\wedge 32}$ endereços IP únicos na Internet, ou seja, 4.294.967.296 endereços Ipv4. Porém, a estrutura de endereços do IPv4 não é linear, sendo agregados em blocos de classes e domínios de redes.

Embora o intuito dessa agregação tenha sido tornar a distribuição de endereços mais flexível, abrangendo redes de tamanhos variados, esse tipo de classificação mostrou-se ineficiente, pois conforme pode ser identificado, o bloco denominado classe A atenderia a um número muito pequeno de redes que alocaria a metade de todos os endereços disponíveis.

O outro motivo é que a relação de endereços IP para cada pessoa não é de 1-1,mas de n-1. Em outras palavras, o usuário comum utiliza em média 03 IPs. (Artur Rodrigues - da teoria à prática);

Segundo, Vint Cerf (2010), vice-presidente do Google, os endereços de IP podem acabar em até um ano. Conforme a figura 1, podemos observar que a Asia e a Europa já sofrem com a escassez de endereços IP.

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	**110,931,700**	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	**825,094,396**	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	**475,069,448**	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	**63,240,946**	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	**266,224,500**	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	**204,689,836**	34.5 %	1,032.8 %	10.4 %

Oceania / Australia	34,700,201	7,620,480	**21,263,990**	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	**1,966,514,816**	**28.7 %**	444.8 %	100.0 %

Figura 1- Quantidade de usuários na Internet
Fonte: http://www.internetworldstats.com/stats.htm, 15/03/2011

No entanto, esse esgotamento não se concretizou devido ao desenvolvimento de uma série de tecnologias que funcionaram como uma solução paleativa para o problema, adiando assim o esgotamento do Ipv4.

Dentre essas tecnologias temos: o NAT (Network Address Translation) descrito na RFC 1631; o CIDR (Classless Inter Domain Routing), ou roteamento sem uso de classes que é descrito pela RFC 1519, o uso dos endereços privados não válidos na Internet e nas redes corporativas descrito pela RFC 1918 e o Protocolo de configuração dinâmica de hosts (DHCP) descrito pela RFC 2131.

1.2 Protocolo IPv6

Este protocolo mantém as principais características do IPv4, como o fato de não ser baseado em conexão e deixar a confiabilidade para os protocolos de mais alto nível. Porém, além de ampliar o espaço de endereçamento, dar segurança na conectividade, o IPv6 acrescenta novas funcionalidades ao IPv4 e altera algumas outras características, que são: Simplificação do cabeçalho; Cabeçalhos de extensão; Endereçamento de 128 bits; Novo formato de endereço; Rota definida na origem; Suporte a autoconfiguração; Suporte a endereços *anycast e* Roteamento. (RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification)

2 INTERCONEXÃO ENTRE IPv4 E IPv6

A transição de protocolo é normalmente implantada pela instalação e configuração do novo protocolo em todos os nós da rede e a verificação de que todas as operações e roteamento irão funcionar com êxito. Vários mecanismos de interconexão foram desenvolvidos para disponibilizar a interoperabilidade entre redes Ipv4 e Ipv6. Essas interconexões podem ser classificadas em dois grupos: Tunelamento e Tradução.

O tunelamento ajuda a isolar nós ou sites Ipv6 para se comunicarem através de redes Ipv4 e o mecanismo de tradução permite que nós Ipv4 e Ipv6 possam se comunicar diretamente.

A RFC 1752, determina alguns critérios que devem ser observados para que se possa realizar essa transição: 1- Os hosts Ipv4 existentes possam ser atualizados a qualquer momento independentemente da atualização de outros hosts ou roteadores; 2 - Novos hosts, utilizando apenas Ipv6, possam ser adicionados a qualquer momento sem a dependência de outros hosts ou infraestrutura de roteamento; 3 - Os hosts Ipv4 existentes, com Ipv6 instalado, possam continuar a utilizar seu endereçamento Ipv4 sem precisar de endereçamento adicional.

2.1 Tipos de *Nós*

Os seguintes tipos de nós devem ser compreendidos antes de se começar a análize dos mecanismos de interconexão: (Youngson Mun and Keywon K. Lee, 2005)

- *Nós* apenas Ipv4: Um computador, roteador ou dispositivos de rede tais como impressoras que suportam apenas Ipv4. Estes nós não suportam Ipv6;
- *Nós* Ipv4/Ipv6: Um host ou computador que suporta tanto o Ipv4 como o Ipv6. Estes nós são chamados de nós dual stack (pilha dupla);
- *Nós* apenas Ipv6: Um computador ou roteador que suporta apenas Ipv6. Estes nós não entendem a versão do protocolo Ipv4;
- *Nó* Ipv4: Implementa IPv4 e pode enviar e receber pacotes IPv4. Um nó IPv4 pode ser um nós apenas IPv4 ou um nó IPv4/IPv6;
- *Nó* IPv6: Implementa IPv6 e pode enviar e receber pacotes IPv6. Um nó IPv6 pode ser um nó apenas IPv6 ou um nó IPv4/IPv6.

Para a coexistência ocorrer, o maior número de *nós* IPv4 ou IPv6 devem se comunicar utilizando uma infra-estrutura IPv4, uma infra-estrutura IPv6 ou uma infra-estrutura que é uma combinação do IPv4 com o IPv6.

3 MECANISMOS DE TRANSIÇÃO

Para coexistir com uma infra-estrutura IPv4 e para disponibilizar uma eventual migração para uma infra-estrutura apenas IPv6, os padrões de transição definem os

seguintes mecanismos: a) Usar conjuntamente os protocolos IPv4 e IPv6; b) Tunelamento IPv6 sobre IPv4; c) Infraestrutura de Nomeação de Dominios (DNS); d) Tradução.

3.1 Utilizando Conjuntamento os Protocolos IPv4 e IPv6

Durante o tempo em que a infraestrutura de roteamento está sendo migrada de *nós* apenas IPv4 para *nós* IPv4/IPv6 e, finalmente para *nós* apenas IPv6, os *nós* devem ser capazes de alcançar o destino utilizando tanto o protocolo IPv4 quanto protocolo IPv6. Por exemplo, durante uma transição, alguns serviços dos servidores serão alcançados utilizando o IPv6. Porém, alguns serviços, que não foram atualizados para suportar IPv4 e IPv6, serão alcançados apenas pelo protocolo IPv4, portanto os hosts devem ser capazes de utilizar tanto o IPv4 quanto o IPv6.

3.1.1 Arquitetura de Pilha Dupla

Uma arquitetura de pilha dupla contém os protocolos IPv4 e IPv6 na camada da internet mas eles estão dentro de pilhas diferentes de protocolos conforme mostra a figura 2.

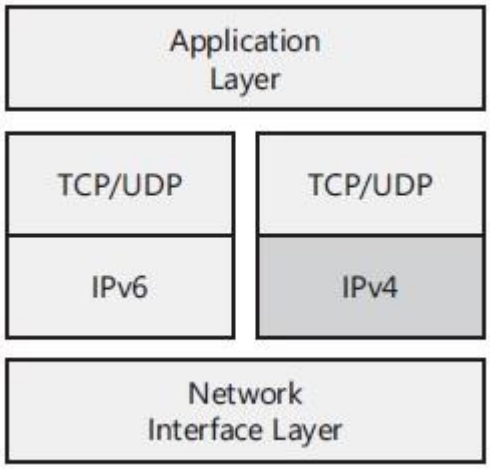

Figura 2 – Arquitetura de pilha dupla
Fonte: (DAVIES, J., 2008, pg. 264)

Os nós IPv6 podem ser compatíveis com nós IPv4 através da implementação da pilha de protocolos e rodando o protocolo apropriado dependendo da capacidade de comunicação dos pares. Um sistema de pilha dupla permite a interoperabilidade

entre nós baseados em IPv4 e nós baseados em IPv6 e a transição gradual do IPv4 para o IPv6. Em sistemas de pilha dupla, qualquer aplicação baseada em apenas um protocolo da pilha (ex. IPv6) pode coexistir e utilizar outras aplicação baseadas em outro protocolo da internet (ex. IPv4).

Apesar dos nós serem implementados com o IPv4 e IPv6, um deles pode ser desabilitado e podem ser operados em um desses três modos: IPv4 habilitado e IPv6 desabilitado; IPv6 habilitado e IPv4 desabilitado; IPv4 e IPv6 habilitados.

Quando ambos os protocolos estão habilitados, os endereços IPv4 e IPv6 devem ser configurados. Para a associação de endereços um mecanismo tal qual o DHCP pode ser empregado para associar um endereço IPv4 e um mecanismo tal qual o DHCPv6 pode ser empregado para associar um endereço IPv6 ao nó.

A figura 3 mostra os tipos de pacotes com a arquitetura de pilha dupla.

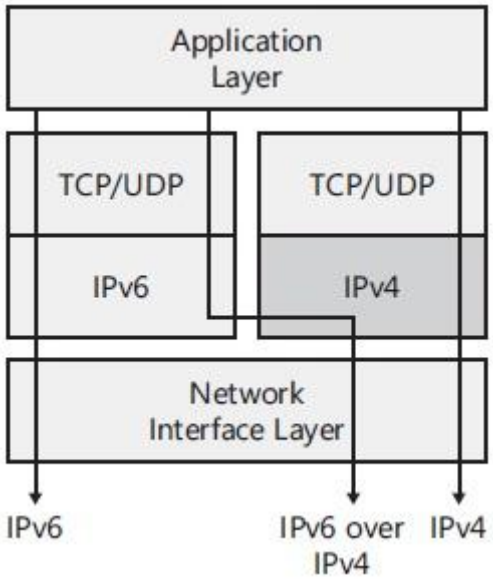

Figura 3 – Tipos de pacotes com a arquitetura de pilha dupla
Fonte: (DAVIES, J., 2008, pg. 264)

A transição disponibilizada pela pilha dupla facilita o gerenciamento da implantação do IPv6 por permitir que este seja feito de uma forma gradual configurando apenas pequenas seções do ambiente de rede. Além disso, caso o IPv4 não seja mais utilizado no futuro basta desabilitar esse protocolo em cada nó da rede.

Alguns aspectos de infraestrutura devem ser observados ao se implemetar essa técnica como a reestruturação do DNS, a configuração dos protocolos de roteamento e dos firewalls.

No caso do DNS é preciso que ele esteja habilitado para resolver nomes e endereços de ambos os protocolos. Já no roteamento é preciso verificar se há a necessidade de se realizar um upgrade na versão que se está utilizando, como por exemplo o OSPFv2 para o OSPFv3 que suporta roteamento para o IPv6.

3.2 Tunelamento IPv6 sobre IPv4

A técnica de tunelamento permite transmitir pacotes IPv6 através da infra-estrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4.

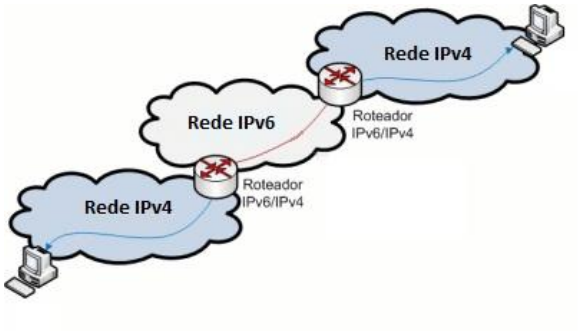

Figura 4: Tunelamento (http://www.ipv6.br, 16/03/2011)

As principais técnicas de tunelamento são: Tunnel Broker; 6to4; ISATAP e Teredo, sendo que cada uma dessas técnicas apresentam dificuldades e diferenças de performance necessitando de uma análise na aplicabilidade de cada uma nos diferentes cenários.

3.2.1 Tunnel Broker

Esta técnica consiste em um túnel IPv6 dentro da rede IPv4, criado do seu computador ou rede até o provedor que irá fornecer a conectividade. Para isso é necessário cadastrar-se em um provedor de acesso Tunnel Broker e realizar o download de um software ou script de configuração.

A conexão do túnel é estabelecida através da solicitação do serviço ao Servidor Web do provedor, que após autenticação, lhe atribui um endereço IPv6. A partir desse ponto, o cliente pode acessar qualquer h*ost* na Internet. (Santos et al, 2010).

3.2.2 6to4

Esta técnica permite a interconexão ponto-a-ponto entre roteadores, sub-redes ou computadores IPv6 através da rede IPv4, fornecendo um endereço IPv6 único formado a partir de endereços IPv4 públicos. Este endereçamento 6to4 utiliza o prefixo de endereço global *2002:wwxx:yyzz::/48 onde wwxx:yyzz* é o endereço IPv4 público do cliente convertido para hexadecimal.

Conforme a figura 5, podemos visualizar a forma de endereçamento utilizada nesta técnica:

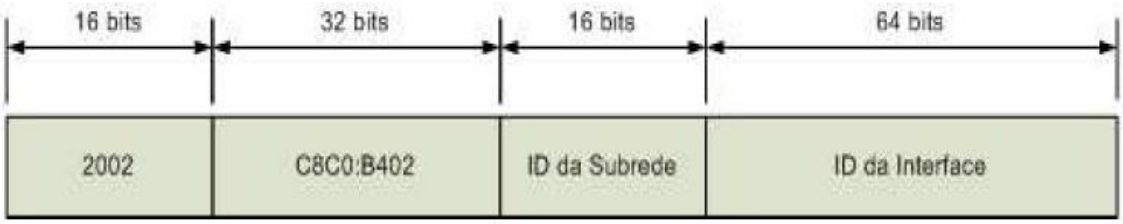

Figura 5 – Endereçamento da técnica 6to4
Fonte: (http://www.ipv6.br/IPV6/ArtigoTuneis6to4, 19/03/2011)

O prefixo 6to4 é sempre **2002;** O próximo campo, IPv4 público do cliente, é criado convertendo-se o endereço para hexadecimal; O ID da subrede pode ser usado para segmentar a rede IPv6 6to4 em até 216 subredes com 264 endereços cada, pode se utilizar por exemplo 0, 1, 2, 3, 4...; O ID da interface pode ser igual ao segundo campo(IPv4 convertido para hexadecimal) no caso da configuração automática do Windows Vista e Server 2008 ou então 1, 2, 3, 4... no caso de configuração manual ou do Linux e BSD. Como o comprimento deste campo é de 64 bits, podemos ter até 264 endereços por subrede.

Como desvantagens o relay roteador não verifica os pacotes IPv6 que estão encapsulados em IPv4, apesar dele os encapsular e desencapsular e não há um sistema de autenticação entre o roteador e o Relay roteador, facilitando assim a exploração de segurança através da utilização de Relays roteadores falsos. Outra

desvantagem é o spoofing de endereço que é um problema grave de túneis 6to4, podendo ser facilmente explorado. (Santos et al, 2010)

3.2.3 ISATAP (Intra-site Automatic Tunnel Addressing Protocol)

Esta técnica é baseada em túneis IPv6 criados automaticamente dentro da rede IPv4 e em endereços IPv6 associados aos clientes de acordo com o prefixo especificado no roteador ISATAP e no IPv4 do cliente. É uma técnica de tunelamento que liga hosts a roteadores o qual não possui um serviço público. Essa técnica é utilizada, por exemplo, quando a organização já tem uma numeração IPv6 válida e conectada na borda, mas a sua infra-estrutura interna não suporta IPv6. Conforme a figura 6, podemos visualizar a forma de endereçamento utilizada nesta técnica:

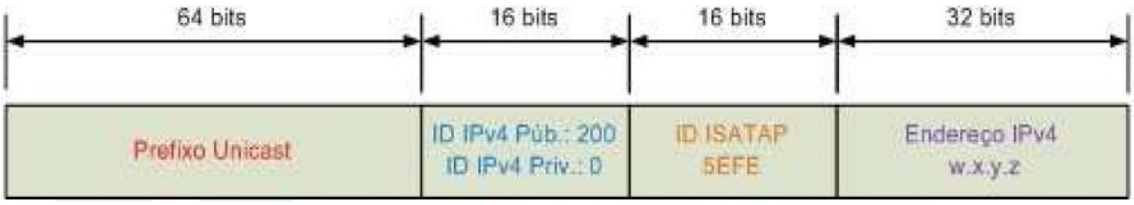

Figura 6 – Endereçamento da técnica ISATAP
Fonte: (http://www.ipv6.br/IPV6/ArtigoTuneisISATAP, 19/03/2011)

O endereço IPv4 dos clientes e roteadores são utilizados como parte dos endereços ISATAP. Com isso, um nó ISATAP pode determinar facilmente os pontos de entrada e saída dos túneis IPv6, sem utilizar nenhum protocolo ou recurso auxiliar; **Prefixo unicast :** É qualquer prefixo unicast válido em IPv6, que pode ser link-local (FE80::/64) ou global; **ID IPv4 público ou privado:** Se o endereço IPv4 for público, este campo deve ter o valor "200" e se for privado (192.168.0.0/16, 172.16.0.0/12 e 10.0.0.0/8) o valor do campo é zero; **ID ISATAP:** Sempre tem o valor 5EFE; **Endereço IPv4:** É o IPv4 do cliente ou roteador em formato IPv4;

Como desvantagem, normalmente as interfaces virtuais dos túneis são mais vulneráveis a invasões do que as conexões físicas, visto que um invasor, em qualquer lugar da Internet, pode enviar um pacote IPv6 encapsulado em um pacote IPv4. Essa é a base para as duas formas principais de ataque a túneis ISATAP, onde um nó de fora da rede envia um pacote IPv6 encapsulado com endereço de

origem falso ou onde um invasor que ganhe acesso a rede, injeta pacotes com endereços de origem falsos diretamente na rede. (Santos et al, 2010)

3.2.4 Teredo

Esta técnica permite que nós localizados através da Network Address Translation (NAT) obtenham conectividade IPv6 utilizando o protocolo UDP.

A conexão é realizada através de um Servidor Teredo que a inicializa, e determina o tipo de NAT usado pelo cliente. Em seguida, caso o *host* de destino possua IPv6 nativo, um *Relay Teredo* é utilizado para criar uma interface entre o Cliente e o *host* de destino. O *Relay* utilizado será sempre o que estiver mais próximo *host* de destino, e não o mais próximo ao cliente. Conforme a figura 7, podemos visualizar a forma de endereçamento utilizada nesta técnica:

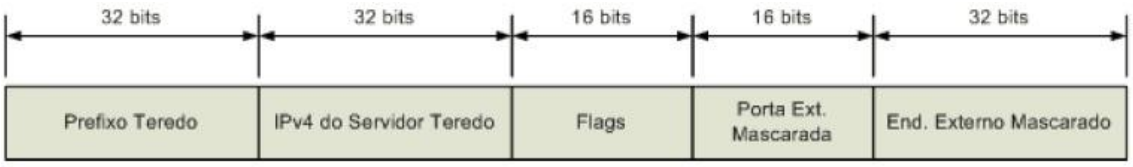

Figura 7 – Endereçamento da técnica Teredo
Fonte: (http://www.ipv6.br/IPV6/ArtigoTuneisTeredo, 20/03/2011)

Utiliza o prefixo **2001:0000::/32**; Os 32 bits seguintes contém o endereço IPv4 do Servidor Teredo; Os 16 bits seguintes são utilizados para definir *flags* que indicam o tipo de NAT utilizado e introduzem uma proteção adicional ao nó contra ataques de *scan*; Os próximos 16 bits indicam a porta UDP de saída do NAT; Os últimos 32 bits representam o endereço IPv4 público do Servidor NAT.

Como desvantagem esta técnica não é muito eficiente devido ao *overhead* e a complexidade de seu funcionamento, e se o seu firewall não estiver devidamente configurado para atuar com essa técnica o seu tráfego pode passar despercebido pelos filtros e *firewalls* se os mesmos não estiverem preparados para interpretá-lo, sendo assim, os computadores e a rede interna ficam totalmente expostos a ataques vindos da Internet IPv6. Entretanto, quando o *host* está atrás de NAT**,** que consiste na utilização de um endereço IP roteável (ou um número limitado deles) para conectar um conjunto de máquinas na rede com endereços IP não rateáveis, ela é uma das únicas opções.

4 CONCLUSÃO

Atualmente a grande maioria das redes usam IPv4 com equipamentos e hosts com suporte a IPv6 (Windows 7 e Linux) o que possibilita a sua migração dependendo das particularidades de cada uma. A técnica 6t04 é a mais adequada para o caso de uma infra-estrutura interna ser migrada toda para o IPv6, permitindo, assim, que rotadores, sub-redes ou computadores comuniquem-se com a infra-estrutura IPv4 existente da internet. Já o Tunnel Broker é uma alternativa mais viável para um único host ou uma pequena rede que utiliza o IPv4, pois com essa técnica basta se cadastrar em um provedor de acesso Tunnel Broker e realizar o download de um software para poder ter acesso à rede IPv6. Porém, se você já possui um endereço IPv6 público mas sua infra-estrutura interna ainda é IPv4 e não utiliza NAT, a técnica ISATAP é a mais indicada por permitir a criação de um túnel IPv4-IPv6. Para o caso de redes que estão atrás de NAT a técnica Teredo é a mais indicada para que os hosts obtenham conectividade IPv6 através do protocolo UDP.

Esses mecanismos possibilitam uma migração segura dependendo, como mencionado, da necessidade e complexidade da técnica utilizada, mas a tradução também pode ser utilizada para tal finalidade. A tradução é uma técnica que possibilita um roteamento transparente entre nós que possuem suporte a apenas um tipo de versão do protocolo IP, traduzindo cabeçalhos IPv4 em cabeçalhos IPv6 e vice-versa, realizando conversões de endereços, de APIs, ou atuando na troca de tráfego TCP ou UDP. Ficam como sugestões para trabalhos futuros, os mecanismos de tradução: SIIT(Stateless IP/ICMP Translation Algorithm*);* NAT-PT (Network Address Translation with Protocol Translation*);* NAPT-PT (Network Address Port Translation and Packet 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).

5 REFERÊNCIAS

CERF, Vint. 2010. *Google vice-presidente de questões relacionadas a avisos da internet*: Disponível em: <http://www.guardian.co.uk/technology/2010/nov/11/google-vint-cerf-internet>. Acesso em 11 de março de 2011.

Cristina, Kellen Bogo, A História da Internet – Como tudo Começou. Disponível em: <http://www.kplus.com.br/materia.asp?co=11&rv=Vivencia>. Acesso em 08 de fevereiro de 2011.

H´obbes, Robert Zakon, Hobbes' Internet Timeline, Disponível em: <http://www.zakon.org/robert/internet/timeline/>. Acesso em 08 de fevereiro de 2011.

IANA – Internet Assigned Numbers Authority. Disponível em: <http://www.iana.org>. Acesso em 11 de março de 2011.

Moreiras, Antonio M. Entenda o Esgotamento do IPv4, Disponível em: <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4>. Acesso em 14 de fevereiro de 2011.

Rodrigues, Artur , da teoria à prática: disponível em: <http://blogs.technet.com/b/arturlr/archive/2009/04/21/a-exaust-o-de-endere-os-ipv4-na-internet-e-a-solu-o-ipv6.aspx>. Acesso em 11 de Março de 2011.

JOSEPH, Daveis, **Undertanding IPv6**, 2º Edição, 2008, Microsoft Press.

OBELHEIRO, Rafael Rodrigues**, Intodução e Histórico do IPv6**, 1999.

PETE, Loshin, **IPv6 Theory, Protocol and Pratice**, 2º Edição, 2003, Morgan Kaufmann.

Regis, Rodrigo dos Santos; Moreiras, Antonio M.; Ascenço, Eduardo Reis; Soares, Ailton da Rocha, **Curso IPv6 Básico**, São Paulo, 2010, Núcleo de Informação e Coordenação do ponto BR.

Request For Comments 1631 - The IP Network Address Translator (NAT)

Request For Comments 1918 – Address Allocation for Private Internets

Request For Comments 2131 – Dynamic Host Configuration Protocol (DHCP)

Request For Comments 1752 – The Recommendation for the IP Next Generation Protocol

Request For Comments 4213 – Basic Transition Mechanisms for IPv6 Hosts and Routers

Youngsong Mun and Hyewon K. Lee, **Understanding Ipv6**, Springer, 2005.