

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

IPv6 – A EVOLUÇÃO DO PROTOCOLO IP

WALLACE DE VASCONCELOS VALE

**NATAL/RN
2011**

WALLACE DE VASCONCELOS VALE

IPv6 – A EVOLUÇÃO DO PROTOCOLO IP

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto, M.Sc.

**NATAL/RN
2011**

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

WALLACE DE VASCONCELOS VALE

IPv6 – A EVOLUÇÃO DO PROTOCOLO IP

Monografia apresentada e aprovada em 30 de Setembro de 2011, pela banca examinadora
composta pelos seguintes membros

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Membro examinador

Membro examinador

Natal/RN, 30 de Setembro de 2011.

RESUMO

Este trabalho apresenta os elementos para entendimento da evolução do protocolo de Internet IPv6, seus principais serviços, formato de cabeçalho, tipos de endereçamentos, mobilidade e segurança, o modo das mudanças para a nova versão e como este promete resolver problemas diversificados que surgiram com o crescimento da rede mundial.

Palavras-chave: IPv6, cabeçalho, endereçamento

ABSTRACT

This paper presents elements for understanding the evolution of the Internet protocol IPv6, its main services, header format, types of addresses, mobility and security, so changes to the new version and how it promises to solve diverse problems that arose with the network growth worldwide.

Keywords: IPv6, header, addresses

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS.

TCP	Transmission Control Protocol
IP	Internet Protocol
IANA	Internet Assigned Numbers Authority
NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol
DSL	Assymmetric Subscriber Line
ICMP	Internet Control Message Protocol
SO	Sistemas Operacionais
UDP	User Datagram Protocol
DNS	Domain Name System
ARP/RARP	Address Resolution Protocol/ Reverse Address Resolution Protocol
IGMP	Internet Group Management Protocol
MAC	Media Access Control
IGP	Interior Gateway Protocols
EGP	Exterior Gateway Protocols
BGP	Border Gateway Protocol
LSA	Link State Advertisements
MBGP	Multiprotocol Border Gateway Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
NTP	Network Time Protocol

SUMÁRIO

1	INTRODUÇÃO.....	9
1.1	OBJETIVOS	10
1.2	JUSTIFICATIVA	10
2	REFERENCIAL TEÓRICO.....	11
2.1	INTERNET.....	11
2.2	IPv4.....	11
2.3	IPv6.....	12
2.4	DATAGRAMA IP	13
2.4.1	Cabeçalho IPv4.....	13
2.4.2	Cabeçalho IPv6.....	14
2.4.3	Diferenças entre os cabeçalhos.....	15
2.5	TIPOS DE ENDEREÇOS IPv6	15
2.5.1	<i>Unicast</i>	16
2.5.2	<i>Multicast</i>	16
2.5.3	<i>Anycast</i>	16
2.6	SERVIÇOS IPv6.....	16
2.6.1	ICMPv6	16
2.5.2	Protocolo de Descoberta de Vizinhança (<i>Neighbor Discovery</i>)	17
2.6.2	<i>Statless</i>	18
2.6.3	<i>Stateful</i>	18
2.6.4	Fragmentação.....	19
2.6.5	QoS (<i>Quality Of Service</i>).....	20
2.6.6	Mobilidade.....	20
2.7	SEGURANÇA	20
2.7.1	IPSec.....	21
2.8	ROTEAMENTO E GERENCIAMENTO	22
2.8.1	RIPng.....	22
2.8.2	OSPFv3.....	22
2.8.3	IS-IS.....	23
2.8.4	BGP	23
3	DESENVOLVIMENTO.....	25

3.1	IMPLANTAÇÃO DO IPV6	25
3.1.1	Softwares e Hardwares	25
3.2	COEXISTENCIA E TRANSIÇÃO	26
3.3	IMPACTOS ATUAIS.....	27
3.4	DEVER DE APRENDER.....	27
3.5	MUDANÇA GRADUAL DE VERSÃO	28
4	CONCLUSÕES	30
	REFERÊNCIAS BIBLIOGRAFICAS	31

LISTA DE FIGURAS

Figura 1: Cabeçalho do IPv4.	14
Figura 2: Cabeçalho do IPv6.	14

1 INTRODUÇÃO

A Internet nasceu praticamente sem querer. Foi desenvolvida nos tempos remotos da Guerra Fria com o nome de ArpaNet para manter a comunicação das bases militares dos Estados Unidos, mesmo que o Pentágono fosse riscado do mapa por um ataque nuclear. Quando a ameaça da Guerra Fria passou, a ArpaNet tornou-se tão inútil que os militares já não a consideravam tão importante para mantê-la sob a sua guarda. Foi assim permitido o acesso aos cientistas que, mais tarde, cederam a rede para as universidades as quais, sucessivamente, passaram-na para as universidades de outros países, permitindo que pesquisadores de todo o mundo tivessem acesso. Nos dias de hoje, não é mais um luxo ou simples questão de opção uma pessoa utilizar e dominar o manuseio e serviços disponíveis na Internet, pois é considerada o maior sistema de comunicação desenvolvido pelo homem.

Como é de nosso conhecimento, o avanço da tecnologia promove sempre o desenvolvimento de equipamentos cada vez mais modernos, e para se tornarem competitivos, precisam ser também baratos e de boa qualidade. No mundo da informática não é diferente, as empresas desenvolvedoras produzem computadores pessoais cada vez mais rápidos e baratos, dessa forma, atingem uma gama de clientes maior, que vão desde pessoas com o poder aquisitivo mais simples até os abastados. Conseqüentemente, o número de computadores ligados a rede mundial cresce em um ritmo exponencial e esse crescimento faz surgir diversos problemas.

Há várias formas de estabelecer comunicação entre computadores. No entanto, os protocolos TCP/IP, sigla para *Transmission Control Protocol/Internet Protocol*, são a base para Internet e para a grande maioria das redes locais. O TCP/IP é um conjunto de protocolos, isto é, de padrões de comunicação. É como se fosse uma linguagem, onde todos os computadores "falam" este idioma e respeitam suas regras, conseguem se comunicar e trocar informações. Apesar de a sigla TCP/IP fazer referência a dois protocolos - *Transmission Control Protocol* e *Internet Protocol*, o conjunto conta ainda com vários outros padrões, cada um sendo responsável por uma determinada tarefa.

O protocolo IP atual dispõe de aproximadamente 4 milhões de endereços, o que é evidente não ser suficiente para acessos nos dias atuais e a tendência é só piorar. Esta escassez de endereços IP é o maior gargalo atual para continuação da evolução dos dispositivos que farão uso da Internet no futuro.

1.1 OBJETIVOS

A evolução do IP para sua versão 6 promete ser a solução para este problema, como também para diversos outros que apareceram na estrada do avanço na comunicação, especificamente na Internet. Este trabalho propõe mostrar a eficácia do IPv6, alguns dos seus novos serviços que se agregaram à nova versão do protocolo, os serviços já existentes que foram melhorados, assim como este protocolo resolverá o problema da escassez de endereços IPs.

1.2 JUSTIFICATIVA

O que motivou a realização desse trabalho foi simplesmente o fato da evolução do principal meio de comunicação existente atualmente, que teve em algum momento de seu desenvolvimento, sua velocidade de crescimento ameaçada devido um gargalo inevitável no modo como é implementado. Visto isso, a solução desenvolvida mostra-se de grande importância e deve ser difundida no meio, visando atingir o máximo de pessoas possíveis, sendo elas profissionais da área ou simplesmente pessoas que tem curiosidade de saber como os equipamentos se comunicam.

2 REFERENCIAL TEÓRICO

A fim de entender toda a problemática que o protocolo IPv6 irá resolver, há necessidade de conhecer alguns conceitos básicos relacionados às tecnologias de redes de computadores.

2.1 INTERNET

Para entender o que é Internet, é importante saber o que são as redes de computadores. Rede de computadores[1] é um conjunto formado por dois ou mais computadores, interconectados por um meio físico e que são capazes de se comunicar utilizando um conjunto de regras e códigos comum. Essas regras e códigos receberam o nome de protocolo.

A Internet[1] é a interligação dessas várias redes de computadores, formando assim uma nuvem única de computadores, interligados e se comunicando em tempo real, quando necessário. Para que essa interligação fosse possível, criou-se um protocolo específico para o uso na Internet, chamado *Internet Protocol*, ou somente, IP.

O protocolo IP[10] é o mais importante da Internet, é ele quem define todas as regras de como essas redes em todo o planeta irão se comunicar. Dentre os conjuntos de regras que compõem este protocolo, uma delas se destaca. Cada computador deve ser identificado na rede sem a possibilidade de ser confundido. Para isto, a identificação é feita através de uma numeração única, chamada de endereço IP, ou seja, não podem existir dois computadores na rede mundial com o mesmo endereço IP.

Para regulamentação da distribuição desses endereços IP no mundo, entidades são responsáveis por gerir todo esse processo, a mais importante delas é a IANA[2].

A Internet inicialmente, não foi projetada para ser essa grande rede que nós conhecemos hoje, seu propósito inicial era a interligação dos centros de pesquisa relacionados à defesa dos estados unidos, porém logo foi aberta a outros centros e instituições de ensino. Em 1983 a rede possuía aproximadamente 300 computadores interligados e como sempre se mostrou útil e funcionando bem, por volta de 1993 passou a ser utilizada comercialmente, neste momento, foi que seu crescimento se tornou ainda maior e fez surgir problemas antes desconhecidos, como por exemplo, o esgotamento dos endereços IP, despertando assim já a idéia de uma evolução no protocolo de acesso.

2.2 IPv4

A versão do endereço IP[10] utilizado e que permanece até hoje é a versão 4 ou IPv4. Essa versão utiliza um endereço de 32bits para nomear cada computador conectado a rede, o que gera um número limitado e exato de 4.294.967.296 endereços IP. Além do rápido

crescimento da Internet, a forma como esses endereços foram distribuídos colaborou ainda mais para sua rápida escassez.

Os endereços IPv4[10] são divididos em três classes:

- **Classe A** – possui 128 blocos de IP's com aproximadamente 16 milhões de endereços cada um.
- **Classe B** – possui 16 mil blocos de IP's com aproximadamente 65 mil endereços cada um.
- **Classe C** – possui aproximadamente 2 milhões de blocos de IP's com 256 endereços cada um.

Algumas medidas paliativas foram criadas para tentar minimizar o problema com os endereçamento de IP's, entre elas podemos citar o NAT e o DHCP.

- **NAT** – essa tecnologia permite que com apenas um endereço válido de Internet, uma rede de computadores possa se conectar parcialmente utilizando endereços privados.
- **DHCP** – essa tecnologia permite fazer o endereçamento dinâmico dos IP's. Dessa forma conexões que não eram permanentes poderiam passar seus endereços para outras conexões. Essa técnica é bastante difundida em provedores de Internet.

Apesar dessas medidas serem utilizadas nos dias atuais, há necessidade de se chegar a um modelo que acaba definitivamente com o problema de escassez de endereços IP, como também possibilitar que novas redes sejam interligadas, novos usuários sejam conectados e o mais importante, novas tecnologias sejam implementadas.

2.3 IPv6

Desenvolvida ao longo de mais de 10 anos, a versão 6 do protocolo IP, ou ipv6, mantém como base os princípios do ipv4, mas busca suprir todas as carências apresentadas por seu antecessor. Sua principal diferença é a capacidade de endereçamento, que aumentou de 32bits para 128bits, dessa forma, trazendo uma quantidade de endereços IP tão grande, que irá suprir todas as necessidades atuais e futuras.

Além dessa vantagem[11], o novo formato dos endereços permitirá: definir uma arquitetura hierárquica na Internet, possibilitando um encaminhamento mais eficiente dos pacotes de dados; facilitar a distribuição de IP's fixos e válidos para conexões DSL, Cable Modems e telefones móveis; fornecer endereços válidos na Internet para todos os dispositivos conectados a ela; utilizar a arquitetura fim a fim; eliminar os problemas associados ao NAT; entre outros.

Não podendo deixar de citar, outra importante mudança na evolução do protocolo foi o formato do cabeçalho, onde na nova versão esse cabeçalho foi simplificado, tornando-se assim mais eficiente e como consequência diminui o processamento dos roteadores.

O quesito segurança não passou despercebido no desenvolvimento da nova versão, como por exemplo, o protocolo IPSec, onde seu suporte passa a ser obrigatório, promovendo assim maior autenticidade, privacidade e integridade dos dados na comunicação. O protocolo ICMP também foi modificado tornando-se mais eficiente, promovendo por vez mecanismos de autoconfiguração de endereços; descoberta de vizinhança e gerenciamento de grupos multicast.

A preocupação com a mobilidade dos dispositivos que farão uso do ipv6 não foi deixada de lado, na nova versão do protocolo o suporte a conexões móveis foi aprimorado e agora passa a fazer parte integrada do protocolo. Esta funcionalidade permite a um usuário se deslocar de uma rede para outra sem necessidade de alterar seu endereço.

2.4 DATAGRAMA IP

O datagrama IP[11] é a unidade básica de dados no nível IP. Um datagrama está dividido em duas áreas, uma área de cabeçalho e outra de dados. O cabeçalho contém toda a informação necessária que identificam o conteúdo do datagrama. Na área de dados está encapsulado o pacote do nível superior, ou seja, um pacote TCP ou UDP.

No cabeçalho encontram-se informações importantes sobre o datagrama como, por exemplo, a versão do protocolo IP utilizado no datagrama, o comprimento do cabeçalho, a qualidade do serviço desejada, tamanho total do datagrama, entre outras informações que são cruciais quando se faz fragmentação de datagramas.

O cabeçalho da nova versão sofreu modificações e nada melhor para identificar essas mudanças do que comparar o cabeçalho das duas versões.

2.4.1 Cabeçalho IPv4

O cabeçalho IPv4[2] é composto por 12 campos fixos, podendo conter ou não opções, fazendo assim com que seu tamanho possa variar entre 20 e 60bytes. A Figura 1 mostra este cabeçalho.

Versão	Comprimento do Cabeçalho	Tipo de Serviço	Comprimento do Datagrama	
Identificador			Flags	Deslocamento de Fragmentação
Tempo de Vida	Protocolo		Bits para verificação da Integridade do Cabeçalho	
Endereço IP da Fonte				
Endereço IP do Destino				
Opções				

Figura 1: Cabeçalho do IPv4.

Estes campos são destinados a transmitir informações sobre: a versão do protocolo; o tamanho do cabeçalho e dos dados; a fragmentação; o tipo de dado; o tempo de vida do pacote; o protocolo da camada seguinte; a integridade dos dados e a origem e o destino do pacote.

2.4.2 Cabeçalho IPv6

O cabeçalho IPv6[3] é composto por oito campos e com tamanho fixo de 40bytes. Abaixo segue um exemplo de um cabeçalho IPv6.

Versão	Classe de Tráfego	Identificação de Fluxo		
Tamanho dos Dados		Próximo Cabeçalho	Limite de Saltos	
Endereço da Fonte (16 bytes)				
Endereço do Destino (16 bytes)				

Figura 2: Cabeçalho do IPv6.

Os cabeçalhos que antes eram obrigatórios se tornaram opcionais. Surgiu uma nova maneira para representação das opções, fazendo com que os roteadores possam ignorá-las caso estas não sejam dirigidas a ele. Dessa forma o roteamento passa a ser mais rápido, visto que o processamento necessário em cada operação no roteador diminui.

As informações transmitidas são: a versão do protocolo; Classe de tráfego; Identificação de Fluxo; Tamanho dos Dados; Próximo Cabeçalho e o Limite de Saltos.

Como informações adicionais podem citar Fragmentação; Roteamento; Opções de Salto a Salto; Autenticação e Opções de Destino. Essas informações são chamadas de Cabeçalhos de Extensão.

Os Cabeçalhos de Extensão localizam-se entre o cabeçalho base e o cabeçalho da camada de transporte.

2.4.3 Diferenças entre os cabeçalhos

No IPv4[10], o campo do cabeçalho reservado para o endereçamento possui um espaço de 32bits. Isso possibilita identificar pouco mais de 4bilhões de dispositivos na Internet. O IPv6 possui em seu cabeçalho um espaço reservado para endereçamento de 128bits, permitindo gerar $3,4 \times 10^{38}$ endereços distintos, equivalente a 56 octilhões de endereços por ser humano na Terra.

Os 32 bits dos endereços IPv4 são divididos em quatro grupos de 8bits cada, separados por “.”, escritos com dígitos decimais. EX.: 192.168.0.1. A representação dos endereços IPv6, divide o endereço em oito grupos de 16bits, separando-os por “:”, escritos com dígitos hexadecimais (2011:ObD8:ad13:2E25:DFA1:F0c4:5311:8C41).

Representando um endereço IPv6 pode-se utilizar caracteres maiúsculos e minúsculos; utilizar regras de abreviação como omitir os zeros à esquerda e representar os zeros contínuos por “::”.

A representação dos prefixos de rede continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR. Esta representação possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

2.5 TIPOS DE ENDEREÇOS IPv6

Os endereços na nova versão do Protocolo IP foram divididos em três categorias: *Unicast*, *Multicast* e *Anycast*.

2.5.1 *Unicast*

Unicast[3] é um endereçamento para um pacote feito a um único destino. A entrega é simples, ponto a ponto. Eles conseguem identificar apenas uma interface. Exemplos de endereços *Unicast* são: *Loopback*, *Unspecified*, *Link-local* e *Unique-local*.

2.5.2 *Multicast*

Multicast[3] é a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções. Diferente do IPv4, onde o suporte a *Multicast* é opcional já que foi introduzido apenas como uma extensão ao protocolo, no IPv6 todos os nós devem ter suporte ao *Multicast*.

2.5.3 *Anycast*

Anycast[3] é uma forma de encaminhamento onde os dados são distribuídos “ao destino o mais próximo” ou “melhores” definidos pelo roteamento da rede. Este tipo de endereçamento é útil para se detectar rapidamente determinados servidores ou serviços, por exemplo, servidores de DNS, ou ainda para identificar um grupo de roteadores pertencentes a um ISP, identificar um conjunto de roteadores conectados a mesma sub-rede, ou identificar os roteadores que provêm a entrada para um domínio específico.

2.6 SERVIÇOS IPv6

Afim de entender melhor os serviços oferecidos pelo IPv6, é importante conhecer o protocolo ICMPv6, pois ele é a base para muitos serviços.

2.6.1 ICMPv6

As principais informações que são obtidas com a troca de mensagens no ICMPv6 são as de informar as características da rede, relatar erros no processamento de pacotes e realizar diagnósticos. Dessa forma, o ICMPv6 está para o IPv6 como o ICMP está para o IPv4. As mensagens do ICMPv6 são classificadas em dois tipos: mensagens de erro e mensagens de informação.

O cabeçalho ICMPv6[10] possui basicamente 4 campos, o campo Tipo indica, como o próprio nome diz, o tipo de mensagem. Seu tamanho é de 8bits. O campo Código oferece algumas informações adicionais para determinados tipos de mensagens. Também possui 8bits de tamanho. O campo Soma de Verificação, é utilizado para detectar dados corrompidos no

cabeçalho ICMPv6 e em parte do cabeçalho IPv6. Seu tamanho é de 16bits. Por fim, o campo Dados, onde são apresentadas as informações de diagnóstico e erro de acordo com o tipo de mensagem. Seu tamanho pode variar de acordo com a mensagem.

Em um pacote comum de dados no IPv6, o cabeçalho ICMPv6 vem precedido pelos cabeçalhos de extensão, se houver, sendo identificado no campo Próximo Cabeçalho pelo valor 58.

Como nesta nova versão o protocolo ICMP incorpora funções que vão além das já conhecidas na sua versão 4, como por exemplo as funções dos protocolos ARP/RARP e IGMP, este possui uma quantidade maior de mensagens.

2.5.2 Protocolo de Descoberta de Vizinhança (*Neighbor Discovery Protocol*)

Este protocolo é bastante utilizado por *hosts* e roteadores para diversas funções, entre as mais importantes podemos citar: encontrar roteadores vizinhos; determinar o endereço MAC dos nós da rede; detectar endereços duplicados; determinar a acessibilidade dos roteadores; redirecionamento de pacotes; autoconfiguração de endereços; entre outras funções.

Este protocolo torna mais dinâmica alguns processos de configuração de rede em relação ao IPv4, combinando as funções de protocolos como ARP, ICMP, Router Discovery e ICMP Redirect, além de adicionar novos métodos não existentes na versão anterior do protocolo IP.

As mensagens do ICMPv6[10] 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, descartando as mensagens com valores diferentes.

A Descoberta de Endereços da Camada de Enlace é utilizada para determinar o endereço MAC dos vizinhos do mesmo enlace, onde um *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* informando seu endereço MAC.

A Descoberta de Roteadores e Prefixos é utilizada para localizar roteadores vizinhos dentro do mesmo enlace, bem como aprender prefixos e parâmetros relacionados à autoconfiguração de endereço. A descoberta de roteadores e prefixos é realizada através da recepção de uma mensagem *Router Advertisement* enviada a partir de um roteador local para o endereço *multicast all-nodes*.

Mensagens *Redirection* são enviadas por roteadores para redirecionar um *host* automaticamente a um roteador mais apropriado ou para informar ao *host* que o destino encontra-se no mesmo enlace. Este mecanismo é igual ao que existe no IPv4.

2.6.2 *Stateless*

Trata-se de um mecanismo que permite aos nós a configuração automática dos endereços em suas interfaces, sem a utilização de servidores DHCP.

O mecanismo de autoconfiguração *stateless*[10] permite que endereços *unicast* sejam atribuídos aos nós sem a necessidade de configurações manuais, sem servidores adicionais, apenas com configurações mínimas 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.

Para cada prefixo informado nas mensagens *Router Advertisement*, é gerado um endereço através do mecanismo de autoconfiguração *stateless*, combinando o prefixo ao identificador da interface. Estas mensagens possuem duas flags: *managed address configuraion* – indica se os *hosts* devem ou não utilizar autoconfiguração *stateful* para obter endereços e *stateful configuration* – indica se os *hosts* devem utilizar a autoconfiguração *stateful* para obter informações adicionais, como endereços de servidores DNS e outros dados sobre a configuração da rede.

2.6.3 *Stateful*

Stateful[10] é uma técnica 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. É utilizado quando não há roteadores em uma rede, ou quando as mensagens *Router Advertisement* apresentam *flags* que habilitam seu uso, a autoconfiguração de endereços *stateful* baseia-se no uso de protocolos, como o DHCPv6, a fim de obter endereços e outras opções de configuração.

O DHCPv6 possibilita a distribuição dinâmica de endereços IP em uma rede, a partir de um servidor DHCP, fornecendo um controle maior na atribuição de endereços ao *host*. No DHCPv6, cliente e servidor trocam mensagens utilizando o protocolo UDP.

A utilização do DHCPv6 provê algumas vantagens em relação a autoconfiguração *stateless*. Ela fornece opções de configurações de rede como endereços de servidores DNS, NTP, etc. Permite também a definição de políticas de controle de acesso.

Existem também a possibilidade de utilizar os dois mecanismos simultaneamente, utilizando a autoconfiguração *stateless* para atribuir os endereços e DHCPv6 para informar o endereço do servidor DNS.

2.6.4 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. O modo como esse processo é tratado no IPv6 difere sensivelmente do modo como este é tratado no IPv4.

No IPv4, a fragmentação ocorre sempre que os pacotes são grandes demais (superiores à *Maximum Transmit Unit*) para serem transmitidos em determinado enlace de um caminho. Este processo ocorre em qualquer ponta de um enlace: fonte ou encaminhadores podem ter de fragmentar os pacotes a enviar. A remontagem é efetuada no destino do pacote, após a recepção correta de todos os segmentos que formam o pacote. Caso haja algum problema na recepção, os segmentos recebidos são descartados. Este processo provoca congestão em enlaces mais "estreitos" e aumenta o tempo de processamento dos pacotes.

Para evitar estes problemas e permitir suporte de serviços em tempo-real, o IPv6 apresenta um novo processo, *Patch MTU Discovery*, onde não há intervenção dos roteadores, é enviada um pacote inicial até ao destino, onde são guardados os tamanhos máximos permitidos em cada enlace do caminho a percorrer. Quando é estabelecido o canal de comunicação, a mensagem é devolvida à fonte que fica assim sabendo qual o tamanho com que pode enviar os pacotes para que eles não tenham de ser fragmentados.

Sendo apenas efetuada na fonte, a fragmentação em IPv6 permite reduzir o tempo de processamento dos pacotes e liberta os roteadores desta tarefa, além de diminuir a possibilidade de perda de pacotes na recepção.

Jumbograms[11], são pacotes enviados pela rede cuja sua forma de envio difere entre a IPv6 e o IPv4. No IPv4 o limite para o tamanho dos pacotes é de 64KB. No entanto, o IPv6 apresenta a opção do Cabeçalho de Extensão *Hop-By-Hop* chamada *Jumbo Payload*. Essa opção permite envio de pacotes IPv6 com cargas úteis entre 65.536 e 4.294.967.295 Bytes de comprimento, os *jumbograms*. Ao enviar estes pacotes, o cabeçalho IPv6 trará os campos Tamanho dos Dados e Próximo Cabeçalho com valor zero. Este último indicará que as opções do Cabeçalho de Extensão *Hop-By-Hop* devem ser processadas pelos nós, o que permitirá o cálculo do tamanho dos *jumbograms*.

2.6.5 QoS (*Quality Of Service*)

É importante garantir a qualidade do transporte do tráfego de determinados tipos de aplicações. Por exemplo: VoIP, Distribuição de vídeos de alta qualidade, jogos online, etc. Para isso, é aplicado a Internet o conceito de QoS, Quality of Service.

O IPv6 busca 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 Tráfego e o Indicador de Fluxo.

2.6.6 Mobilidade

O IPv6 já traz incorporado ao protocolo funcionalidades de suporte à mobilidade. Desta forma, mesmo com a movimentação de um *host* de uma rede a outra, os pacotes enviados ao seu endereço original continuarão sendo recebidos normalmente. Isto se deve porque o dispositivo móvel pode se deslocar de uma rede para outra sem necessidade de alterar seu endereço IP de origem.

Desta forma, quando este dispositivo estiver fora de sua rede, os pacotes continuarão sendo encaminhados a ele usando seu Endereço de Origem. Isso faz com que a movimentação entre as redes fique invisível para protocolos das camadas superiores. Diferente do IPv4, os mecanismos necessários para garantir essa mobilidade já vêm incorporados ao protocolo IPv6.

2.7 SEGURANÇA

Destinado inicialmente a interligar apenas algumas redes de pesquisa acadêmicas, o projeto original do IPv4 não apresentava muita preocupação com a questão da segurança das informações transmitidas. No entanto, com o crescimento da Internet, diversas ameaças à segurança da rede e ao tráfego de dados surgiram, prejudicando, por exemplo, sua utilização em operações bancárias e em transações entre empresas e consumidores.

Com isso, tornou-se necessário acrescentar novos mecanismos ao protocolo original, que garantissem a confiabilidade de tais serviços.

Entre esses novos mecanismos, destaca-se o IPSec (IP Security), um protocolo que implementa criptografia e autenticação de pacotes na camada de rede, fornecendo uma solução de segurança fim-a-fim, garantindo a integridade, confidencialidade e autenticidade dos dados.

2.7.1 IPSec

O IPSec[7] foi criado originalmente para ser usado em conjunto com o IPv4, entretanto, seu mecanismo de autenticação não pode ser utilizado em conexões que estejam atrás de NAT, que “esconde” o endereço IP original do emissor dos pacotes impedindo sua identificação.

Com a implantação do IPv6 o uso do IPSec torna-se mais fácil. Embora seu funcionamento seja praticamente o mesmo nas duas versões do protocolo IP, no IPv6 não há necessidade de se utilizar NAT, permitindo que o IPSec funcione sem restrições. Os mecanismos de autenticação e encapsulamento do IPSec fazem parte do protocolo. Além disso, seu suporte é obrigatório em todos os nós, o que não ocorre no IPv4.

Deste modo, através do IPSec o IPv6 é capaz de garantir 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.

Embora no IPv6 o suporte ao IPSec seja obrigatório, para sua efetiva utilização, ele deve ser habilitado em cada nó pelos administradores de rede ou caberá a cada aplicação definir a utilização ou não do IPSec.

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

O IPSec pode operar em dois modos:

- Modo de Transporte – protege apenas os protocolos das camadas superiores, pois o cabeçalho de segurança aparece imediatamente após o cabeçalho IP e antes dos cabeçalhos das camadas superiores;
- Modo Túnel – protege todo o pacote IP, encapsulando-o dentro de outro pacote IP, deixando visível apenas o cabeçalho IP externo.

Embora as funcionalidades do IPSec sirvam como proteção contra algumas ameaças à segurança, como técnicas de falsificação de endereços, ataques de negação de serviço e análise de tráfego, ainda existem diversas outras ameaças aos dados que trafegam na rede.

2.8 ROTEAMENTO E GERENCIAMENTO

Os protocolos de roteamento são os 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 em suas tabelas de roteamento o prefixo correspondente ao endereço de destino, e a partir desta informação, determinam qual o melhor caminho a percorrer.

Para sincronizar e gerenciar as tabelas de roteamento de forma dinâmica são utilizados os Protocolos de Roteamento. Estes protocolos dividem-se em dois tipos:

- **Interno** – Os protocolos que distribuem as informações dos roteadores dentro de Sistemas Autônomos são chamados de *Interior Gateway Protocols* (IGP).
- **Externo** – Os protocolos que distribuem as informações entre AS distintos são chamados de *Exterior Gateway Protocols* (EGP). No IPv6 normalmente utiliza-se as extensões para multiprotocolos do *Border Gateway Protocol* (BGP).

2.8.1 RIPng

O protocolo RIPng[9] é baseado em um algoritmo *distance-vector* conhecido como *Bellman-Ford*. Esse protocolo segue os principais conceitos do RIPv2 utilizado com o IPv4. O RIPng apresenta como uma das principais mudanças em seu funcionamento o suporte aos prefixos e ao tamanho dos endereços IPv6. E por tratar-se de um protocolo específico do IPv6, utiliza o como endereço de destino para mensagens RIP Update o endereço multicast *All RIP Routers* (FF02::9).

2.8.2 OSPFv3

O OSPFv3[9] é um protocolo de roteamento interno do tipo *link-state*. Através do processo de *flooding*, 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 informa todos os estados dos enlaces que conhece aos roteadores vizinhos. Com o conjunto das LSAs, todos os roteadores formam um banco de dados de estado do enlace idêntico.

OSPFv3 é uma versão do protocolo exclusivamente IPv6. Com isso, algumas alterações ocorreram em relação a versão do OSPFv2. Dentre estas, pode-se citar:

- Foram criados novos tipos de LSAs e algumas foram alteradas;

- No OSPFv3 a autenticação foi retirada, contado apenas com a autenticação do IPv6;
- No IPv4, o OSPF conecta interfaces por sub-rede, no OSPFv3 para IPv6 isso é feito por enlace;
- Um único enlace pode ter múltiplas instâncias do OSPFv3 sendo executadas;
- São utilizados endereços multicast *AllSPFRouters* (FF02::5) e *AllDRouters* (FF02::6).

2.8.3 IS-IS

Outro protocolo de roteamento interno, o IS-IS não teve uma nova versão desenvolvida para trabalhar com o IPv6. Apenas adicionaram-se novas funcionalidades à versão já existente, para que pudesse tratar as mudanças no formato do endereçamento IPv6. Foram adicionados dois novos TLV (Tag/Length/Values) para IPv6:

- IPv6 Reachability
- IPv6 Interface Address

E um novo identificador da camada de rede:

- IPv6 NLPID

2.8.4 BGP

O BGP[9] é o protocolo de roteamento externo mais utilizado. Como não há uma versão de BGP específica para o IPv6, a nova versão do Protocol Internet 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 famílias de endereços, IPv4 e IPv6.

Esta capacidade de trabalhar com diversos protocolos de rede, além dos dois Protocolos Internet, é possível pela adoção de identificadores, que atuam na identificação do protocolo a ser suportado;

- *Address Family Identifier* (AFI)
- *Subsequent Address Family Identifier* (Sub-AFI)

E pela utilização de dois novos atributos:

- MP_REACH_NLRI
- MP_UNREACH_NLRI

O primeiro atributo é utilizado no transporte do conjunto de destinos acessíveis junto com o *next hop*. O segundo transporta o conjunto de destinos inacessíveis.

A partir da troca de informações entre dispositivos de rede, é possível gerenciar seu desempenho, detectar e solucionar problemas, controlar equipamentos, além de outras inúmeras atividades que permitam obter o máximo desempenho desta rede.

A troca de informações entre o gerente e o agente SNMP pode ser feita tanto em conexões IPv4 quanto conexões IPv6, mesmo que essas informações sejam sobre IPv6. Porém já existem diversos equipamentos com suporte a SNMP sobre IPv6 que podem ser monitorados em redes com conexões apenas IPv6.

Embora o SNMP seja amplamente utilizado devido a sua simplicidade, quando é necessária uma análise mais detalhada da rede, podemos aplicar uma abordagem alternativa que consiste em recolher informações sobre cada pacote. Neste método, equipamentos de rede, por exemplo, um roteador, 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, também já estão preparados para coletar dados sobre o tráfego IPv6. A versão 9 do NetFlow, protocolo desenvolvido pela Cisco Systems, já apresenta suporte a IPv6. Do mesmo modo, o protocolo IPFIX (*IP Flow Information Export*), também é capaz de exportar e coletar dados sobre o tráfego IPv6.

Outras funções básicas de gestão de rede, como o gerenciamento das configurações dos equipamentos, também são possíveis em redes IPv6. Os principais protocolos utilizados para essa função, seja através da execução remota de comandos ou de transferência de arquivos, já apresentam suporte ao novo protocolo IP. Podemos citar: SSH, TELNET, SCP, FTP E TFTP.

Um quesito muito importante no gerenciamento de redes, a sincronização dos relógios dos computadores pode refletir de forma significativa no funcionamento de diversos softwares e sistemas, além da segurança dos computadores, redes e da própria Internet. Com a utilização do protocolo NTP (*Network Time Protocol*) é possível manter o relógio do computador sempre com a hora certa, com exatidão de alguns milésimos de segundo. Isto pode ser feito sincronizando o relógio do computador com um servidor NTP público.

A sincronização dos relógios de uma rede IPv6 é possível conectando-se a servidores que possuam suporte ao novo protocolo IP.

3 DESENVOLVIMENTO

Existem vários ajustes, extensões e aplicativos de suporte adicionados ao IPv4 que compõem a estrutura de trabalho do IPv6. Fundamentalmente, os computadores se comunicam de IP para IP, usando números, não nomes, e que a maioria das características da comunicação IP não vai mudar. Por exemplo, um cabeçalho de pacote no IPv4 é um cabeçalho de pacote no IPv6, com pequenas modificações de formato. A maior mudança é que, em vez de usar 32 bits para formar um endereço IP, o IPv6 usa 128 bits. É fácil de entender. Entretanto, não vamos memorizar o endereço IP completo de cada máquina. Mesmo assim, algumas pessoas vão memorizar as informações de sub-rede ($2n$) que podem formar $2(128-n)$ bits do endereço IP. Um endereço IP no IPv6 é formado por 128 bits de informação e é escrito em formato binário ou hexadecimal. O endereço IP é feito de 16 partes de 8 bits. Seria mais fácil dizer que os endereços IP são oito endereços de 16 bits, pois a forma hexadecimal terá de ser dividida nas separações de 16 bits. O endereço consiste do prefixo global de roteamento, identificação da sub-rede e da interface.

3.1 IMPLANTAÇÃO DO IPv6

A implantação do IPv6 é necessária e inevitável. Sabe-se que mesmo os endereços IPv4 acabando, a Internet não pára, continuará funcionando normalmente, porém ocorrerá uma diminuição na taxa de crescimento da rede e de algumas novas aplicações, outras que poderiam ser criadas, não serão. Também se imagina que as conexões Internet ficariam mais caras. No entanto, a implantação do IPv6 não será algo rápido, será feita de forma gradual, com as duas versões do protocolo em funcionamento.

Um cenário que se imagina são ilhas IPv6 conectadas por túneis v4, com a evolução do processo Ilhas IPv4 passariam as estar conectadas por túneis sobre uma Internet IPv6, até o processo ser concluído e se obter uma Internet operando 100% IPv6. O mais importante neste processo é manter a compatibilidade entre as versões do protocolo IP, tornando essencial para o sucesso da transição para o IPv6.

3.1.1 Softwares e Hardwares

Atualmente, os Sistemas Operacionais mais utilizados já trazem suporte à versão mais nova do Protocolo IP. As empresas proprietárias desses SO's montaram suas linhas de pesquisa afim de sair na frente na corrida dessa evolução. Entre eles temos o Windows, Mac OS, Linux e BSD.

As empresas de hardware de rede também seguiram a tendência e já implantaram em seus produtos o suporte necessário para o IPv6. São elas, CISCO Systems, Juniper Networks, Hitachi, 3Com Corporation.

3.2 COEXISTENCIA E TRANSIÇÃO

Hoje em dia, toda a estrutura da Internet está baseada na versão 4 do protocolo IP. Deste modo uma troca imediata de protocolo torna-se inviável, dado o tamanho e a proporção que esta rede possui. Desta forma, haverá nessa fase inicial de transição, um período de coexistência entre os dois protocolos, em que redes IPv4 precisarão comunicar-se com redes IPv6 e vice-versa. E com o intuito de facilitar este processo, foram desenvolvidas 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:

- Pilha Dupla – Provê o suporte a ambos os protocolos no mesmo dispositivo. Com este método hosts e roteadores tornam-se capazes de enviar e receber pacotes tanto para o IPv4, quanto para o IPv6. Esse método permitirá 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.

- Tunelamento – Permite o tráfego de pacotes IPv6 sobre estruturas de rede IPv4, ou o inverso. De uma forma 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. A utilização do protocolo 41 é comum em algumas técnicas de tunelamento, como o 6to4, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) e Tunnel Broker.

- Tradução – Permite a comunicação entre nós com suporte apenas a IPv6 com nós que suportem apenas IPv4 e vice-versa. Elas podem atuar 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 tráfego TCP ou UDP.

Cada uma dessas técnicas apresenta uma característica específica, e pode ser utilizada individualmente ou em conjunto, de modo a atender as necessidades de cada situação, seja a migração para o IPv6 feita passo a passo, iniciando por um único host ou sub-rede, ou até de toda uma rede corporativa.

3.3 IMPACTOS ATUAIS

Esta mudança de protocolo pode impactar o seu dia a dia. De forma muito prática tem que como pessoa física em uma residência, será pouco afetada e sem muito que fazer, a não ser aguardar a evolução dos softwares de uso doméstico e da atualização dos equipamentos dos provedores de acesso. Por outro lado não se deve aceitar maquiagem em equipamentos para receber informações geradas e transmitidas sob protocolo IPv6. De outra forma, não pode permitir o uso de tunelamento em sua máquina. Se houver necessidade o equipamento deve ser migrado todo para o protocolo IPv6. Como responsável de uma pessoa jurídica, deve-se elaborar um diagnóstico de como está sua empresa neste assunto e planejar a migração para o protocolo IPv6. Ação esta que deve ser feita com a urgência possível.

Praticamente todos os sistemas operacionais desenvolvidos na última década estão aptos a se comunicar por IPv6. Se o computador não estiver pronto para o IPv6, é devido a ajustes ou a obstrução do canal de comunicação.

As empresas devem sair na frente. A Internet abriu oportunidades inigualáveis para os negócios em geral e dominar um recurso desconhecido da maioria e permanecerem alguns passos adiante da concorrência é o mais correto para se manter na liderança de mercado. Domínio se adquire quando se experimenta o novo. Algumas novidades podem ser exploradas e revertidas para reforçar a posição da empresa em seus próprios negócios, melhorando aspectos de segurança, evitando fraudes, ocultação de dados e informações e de qualidade de serviços. Outro aspecto da nova Internet é o fator mobilidade e, por representar inovação, trará um diferencial expressivo para a empresa de visão aguçada que incorporá-la em seu negócio.

3.4 DEVER DE APRENDER

A necessidade do IPv6 é premente, e as ferramentas necessárias para sua implementação estão prontamente disponíveis. As iniciativas de utilização surgem a todo o momento: vários provedores de serviços importantes já disponibilizam acesso via IPv6. Alguns poucos provedores de acesso já oferecem acesso IPv6 nativo; não é surpresa isso ocorra em regiões como Japão, Austrália e Europa, menos privilegiadas na distribuição das faixas IPv4. A próxima grande frente de adoção de IPv6 é a América Latina. O grande temor de muitos, e gancho para críticas severas ao IPv6, foi a dificuldade de obtenção de um momento para que a comunidade Internet começasse a efetivamente utilizar esse novo protocolo. Hoje, esse é um problema resolvido. Já existe uma boa massa crítica de

documentação, software e administradores de rede capacitados em IPv6. Resta agora que a necessidade dos recursos disponíveis unicamente em IPv6 aperte um pouco mais, o que vai ocorrer num futuro não muito distante.

E a necessidade não deve tardar. A próxima grande revolução é a substituição massiva do telefone por conexões rápidas à Internet; a comunicação de voz será absorvida pelo uso de VoIP, que é uma tecnologia bem estabelecida. Mas não há como acomodar todos os terminais telefônicos no espaço de endereçamento IP atual. E antes de os endereços IP estarem esgotados, os roteadores NAT já terão infernizado o suficiente os administradores de rede, a ponto de todos considerarem a migração para IPv6. Quem já tentou implementar um esquema de VoIP entre duas corporações, cada uma com seu firewall, conhece bem esses problemas.

Das ferramentas de implementação IPv6, a mais importante é sem dúvida a interface de programação de aplicações (API). As duas famílias de sistemas operacionais mais importantes do mercado atual, Windows e UNIX, já possuem APIs implementadas e funcionais. A API Sockets BSD para IPv6 é uma interface bem definida, bem resolvida, suficientemente independente de plataforma para que qualquer software de rede IPv6 seja portátil entre os UNIX modernos.

Mais que isso, a concepção permite criar aplicativos prontos para IPv6, e que trabalham unicamente em IPv6, mas funcionam corretamente numa rede puramente IPv4 ou mista IPv4/IPv6. Os softwares novos prevêem apenas IPv6, os softwares antigos podem ser modificados para isso mas tudo continua funcionando na Internet atual. Assim, é perfeitamente factível que, quando os provedores passarem a oferecer acesso IPv6 corriqueiramente, os usuários finais nem notem a diferença.

3.5 MUDANÇA GRADUAL DE VERSÃO

A implantação do IPv6 não implica na criação de uma nova Internet, tampouco significa que o IPv4 será imediatamente descontinuado e substituído pelo IPv6 de forma abrupta. Ambos os protocolos coexistirão na Internet por um longo período, mesmo após o esgotamento dos endereços IPv4. Tanto as previsões para o esgotamento dos endereços IPv4, quanto para sua total substituição pelo IPv6, são bastante imprecisas e variam de acordo com o método utilizado e fontes de pesquisa.

Atualmente já existe uma considerável quantidade de equipamentos de rede que são compatíveis com IPv4 e IPv6 simultaneamente. Da mesma forma, as versões mais recentes de diversos sistemas operacionais já trazem embutidas funcionalidades que os tornam compatíveis com os dois protocolos em questão. Destaquem-se o Windows Vista e várias

distribuições Linux, além do Windows XP, que conta com mecanismos opcionais para ativação de suporte ao IPv6.

Na criação do IPv6 já foram também concebidos mecanismos de transição. Outros mecanismos específicos estão em fase de desenvolvimento e testes, como o “Ipv6-to-IPv4 HTTP Proxy”, por exemplo, usado para dispositivos móveis.

A tecnologia de IP móvel já estava disponível com uso do IPv4, porém o IPv6 traz características embutidas que melhoram esta modalidade de serviço. Em Parziale[19] é dito que o 3GPP (3rd Generation Partnership Project) tem conduzido discussões para fazer melhor uso das capacidades nativas do IPv6 em redes sem fio e serviços 3G. Como resultado da adoção do IPv6 nativo, eles asseguram que telefones são compatíveis com computadores móveis no compartilhamento de drivers e programas referentes à mobilidade.

4 CONCLUSÕES

Conforme o uso do IPv6 na Internet cresce, o conceito básico de configuração e uso de endereços IP torna-se crítico para todas as organizações. As companhias precisam criar e implementar uma estratégia eficaz de migração. Não só os endereços IP externos terão de ser atualizados, mas também os endereços internos que conectam-se aos parceiros por meio de túneis IPSec e conexões secundárias. Já os usuários domésticos estão mais tranquilos, visto que na sua grande maioria são usuários de SO's que suportam tal avanço.

A implantação do IPv6 na Internet não é uma tendência, é uma necessidade e realidade em curso já há alguns anos. A tendência é a intensificação do uso, devido ao iminente esgotamento de endereços IPv4, determinado por uma série de fatores e pelas vantagens técnicas que o novo protocolo traz desde a sua origem, pois foi concebido como uma evolução do IPv4 e para corrigir deficiências identificadas neste último.

Para vencer os desafios da transição dos protocolos IPv4 para IPv6, que inevitavelmente coexistirão por longo tempo, as instituições provedoras de serviços de Internet, bem como instituições governamentais ou privadas que têm estes serviços como um de seus insumos, deverão fazer inevitáveis investimentos tempestivos na boa capacitação do pessoal técnico, atualização ou substituição de alguns elementos de suas redes internas (equipamentos, programas, sistemas operacionais, etc.) e, principalmente, ficarem atentas para as ameaças e oportunidades decorrentes de seus planos e ações para esta transição.

Afirma-se que IPv6 é uma realidade que ninguém pode mais dar-se ao luxo de ignorar. Porque as implementações e aplicações já existem; porque a necessidade é premente; porque bem ou mal já está sendo usado; porque é suportado pelos fabricantes; porque após um processo que já foi excessivamente demorado, foi a saída apontada pelo IETF, e não consta alternativa melhor; porque foi desenhado de modo a causar o menor impacto possível na Internet em funcionamento.

REFERÊNCIAS BIBLIOGRAFICAS

1. Enciclopédia Livre, Wikipedia: História da Internet. Disponível em (http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet). Acessado em 22/09/2011.
2. Enciclopédia Livre, Wikipédia: Protocolo de Internet. Disponível em (http://pt.wikipedia.org/wiki/Protocolo_de_Internet) . Acessado em 20-06-2011.
3. Enciclopédia Livre, Wikipedia: IPv6. Disponível em (<http://pt.wikipedia.org/wiki/IPv6>). Acessado em 20-06-2011.
4. Comunidade Infowester: O que é IPv6. Disponível em (<http://www.infowester.com/ipv6.php>). Acessado em 18-06-2011.
5. Comunidade Ipv6 Forum: Desenvolvimento do IPv6. Disponível em (<http://www.ipv6forum.com/>). Acessado em 02-05-2011.
6. Comunidade 6diss: Programa de apoio ao desenvolvimento do IPv6. Disponível em (<http://www.6diss.org/>). Acessado em 23-07-2011.
7. HAGEN, Silvia. IPv6 Essentials. O'Reilly Media, 1st edition. July 2002.
8. DAVIES, Joseph. Understanding IPv6. Microsoft. November 2002.
9. BEIJNUM, Iljitsch. Running IPv6. Apress; 1 edition. November 2005.
10. Comunidade IPv6: IPv6. Disponível em (<http://ipv6.br/>). Acessado em 10-06-2011.
11. Núcleo de Informação e Coordenação do Ponto BR: Comitê Gestor de Internet no Brasil. Disponível em (<http://nic.br/>). Acessado em 10-06-2011.