FACULDADE DE TECNOLOGIA DO ESTADO DE SÃO PAULO

FAGNER GERALDES BRAGA

A CONTINUIDADE DA INTERNET PASSA PELO IPv6

São Paulo – SP

2011

FACULDADE DE TECNOLOGIA DO ESTADO DE SÃO PAULO

FAGNER GERALDES BRAGA

A CONTINUIDADE DA INTERNET PASSA PELO IPv6

Trabalho apresentado à Faculdade de Tecnologia de São Paulo, para a obtenção do grau de Tecnólogo em Processamento de Dados.

Professor Orientador: Gabriel Issa Jabra Shammas

São Paulo – SP

2011

Dedicatória

Dedico este trabalho à minha mãe e aos meus avós (in memoriam), por serem os pilares da educação que recebi.

Agradecimentos

Aos familiares: pelos valores transmitidos e também pelo incentivo, apoio e confiança ao longo de todos estes anos.

Aos amigos da FATEC-SP: pela troca de conhecimentos, ajuda mútua e também pelos momentos de lazer e diversão vividos durante a vida acadêmica.

Aos amigos de infância: pelos momentos inesquecíveis que passamos e ainda passaremos juntos.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

AH - Authentication Header - Cabeçalho de Autenticação

API - Application Programming Interface – Interface de Aplicação Programável

ARP - Address Resolution Protocol – Protocolo de Resolução de Endereço

ARPA - Advanced Research Projects Agency - Agência de Pesquisas e de Projetos Avançados

AS – Autonomous Systems - Sistemas Autônomos

AT&T - American Telephone and Telegraph

BGP - Border Gateway Protocol – Protocolo de Gateway de Borda

BIA – Bump in the API

BIS – Bump in the Stack

CIDR - Classless Inter-domain Routing – Roteamento entre domínios sem classe

DHCP - Dynamic Host Configuration Protocol – Protocolo de Configuração de Host Dinâmico

DiffServ - Differentiated Services - Serviços Diferenciados

DNS - Domain Name System – Sistema de Nome de Domínio

DoD – Department of Defense - Departamento de Defesa dos Estados Unidos

EGP - Exterior Gateway Protocol – Protocolo de Gateway Externo

E-Mail - Electronic Mail – Correio Eletrônico

ESP - Encapsulating Security Payload - Encapsulamento Seguro de Carga de Dados

EUA - Estados Unidos da América

FTP - File Transfer Protocol – Protocolo de Transferência de Arquivos

GPS – Global Positioning System – Sistema de Posicionamento Global

GRE – Generic Routing Encapsulation – Encapsulamento de Rota Genérica

HP - Hewlett-Packard

HTTP - Hypertext Transfer Protocol – Protocolo de Transferência de hipertexto

IANA - Internet Assigned Numbers Authority – Autoridade Concessora de Números de Internet

IBM - International Business Machines

ICMP - Internet Control Message Protocol – Protocolo de Mensagem de Controle de Internet

IETF - Internet Engineering Task Force – Força Tarefa de Engenharia da Internet

IGMP - Internet Group Management Protocol – Protocolo de Gerenciamento de Grupo de Internet

IGP – Internal Gateway Protocol – Protocolo de Gateway Interno

IKE - Internet Key Exchange - Troca de Chaves de Internet

IntServ - Integrated Services - Serviços Integrados

IPSec - Internet Protocol Security – Segurança do Protocolo de Internet

ISATAP – Infra-Site Automatic Tunnel Addressing Protocol

ISP - Internet Service Provider – Provedor de Serviço de Internet

LAN - Local Area Network - Rede de Área Local

MIB - Management Information Base - Base de Gerenciamento de Informação

MIT - Massachusetts Institute of Technology – Instituto de Tecnologia de Massachusetts

NAT - Network Address Resolution – Resolução de Endereços de Rede

NCP - Network Control Protocol – Protocolo de Controle de Rede

NetBIOS - Network Basic Input/Output Systems – Sistemas de Entrada/Saída Básica de Rede

NTOP - Network Traffic Probe - Sonda de Tráfego de Rede

NTP - Network Time Protocol - Protocolo de Horário da Rede

OSPF - Open Shortest Path First - Caminho Mais Curto Aberto Primeiro

P2P - Peer-to-Peer – Ponto a Ponto

POP3 - Post Office Protocol – Protocolo de Correio

PPPoE - Point-to-Point Protocol over Ethernet - Rede Sobre Protocolo Ponto a Ponto

QoS - Quality of Service - Qualidade de Serviço

RADIUS - Remote Authentication Dial In User Service - Serviço de Autenticação Discada de Usuário Remoto

RFC - Request for Comments – Pedido de Comentários

RIP - Routing Information Protocol – Protocolo de Roteamento de Informação

RIPng – Routing Information Protocol Next Generation – Protocolo de Roteamento de Informação da Próxima Geração

RIR – Regional Internet Registry – Registro Regional de Internet

ROAD - Routing and Addressing – Endereçamento e Roteamento

RSVP - Resource ReserVation Protocol - Protocolo de Reserva de Recursos

SIIT – Stateless IP/ICMP Translation

SMTP - Simple Mail Transfer Protocol – Protocolo de Transferência de Mensagem Simples

SNMP - Simple Network Management Protocol – Protocolo de Gerenciamento de Rede Simples

SRI – Stanford Research Institute – Instituto de Pesquisa de Stanford

SSH - Secure Shell

TCP - Transmission Control Protocol – Protocolo de Controle de Transmissão

TCP/IP - Transmission Control Protocol/Internet Protocol – Protocolo de Controle de Transmissão/Protocolo Internet

TRT – Transport Relay Translator – Tradutor de Agente de Transporte

UCLA – University of California, Los Angeles – Universidade da Califórnia, Los Angeles

UCSB – University of California, Santa Barbara – Universidade da Califórnia, Santa Bárbara

UDP - User Datagram Protocol – Protocolo de Dados de Usuário

VOIP - Voice over Internet Protocol – Voz sobre Protocolo de Internet

VPN - Virtual Private Network – Rede Virtual Privada

WAN - Wide Area Network - Rede de Área Ampla

Curriculum Vitae

Fagner Geraldes Braga nasceu em 25 de Fevereiro de 1984, na cidade de Guarulhos no estado de São Paulo, formou-se em Técnico em Informática no ano de 2003 e atualmente cursa o último semestre de Tecnologia em Processamento de Dados na Faculdade de Tecnologia de São Paulo.

Possui as certificações Microsoft Certified Professional (MCP) e Microsoft Certified Technology Specialist (MCTS): Windows 7, Configuration.

Resumo

O rápido crescimento da Internet nos últimos anos tem criado uma grande necessidade de endereços IP. Além do problema da escassez de endereços, o aumento da tabela de roteamento e falta de segurança, obrigou a criação de um novo protocolo de comunicação que suprisse todas essas necessidades.

O IPv6 é uma solução para este problema de escassez de endereços IP e também é provido de novos recursos, tais como o suporte a novas tecnologias de rede (ATM, Gigabit Ethernet, entre outros), novo formato do cabeçalho, infraestrutura hierárquica e eficiência de roteamento e endereçamento, configuração de endereçamento com ou sem estado, segurança embutida, melhor suporte para a qualidade dos serviços (QoS), novo protocolo para interação entre nós vizinhos e capacidade de extensão.

A transição do protocolo IPv4 para o IPv6 deverá ser de forma gradual para garantir a funcionalidade da rede. Foram criados dispositivos para que se possa fazer uma transição de modo que os dois protocolos de rede possam coexistir.

Palavras-chave: IPv4, IPv6, Internet, Qos, IPSec, DHCP, CIDR, DNS, NAT, RFC, TCP/IP.

Abstract

The Internet has been growing quickly in recent years and it has created a large need for IP addresses. Besides the lack of IP addresses, the routing table has been growing and the security is a big deal nowadays. Because all these problems a new protocol has created for meet all these needs.

IPv6 is a solution for these problems and it is also equipped with new features such as support for new network technologies (ATM, Gigabit Ethernet, etc.), new header format, infrastructure and efficiency of hierarchical addressing and routing, addressing configuration with or without the state, built-in security, better support for quality of service (QoS), a new protocol for interaction between neighboring nodes and extensibility.

The transition from IPv4 to IPv6 will be gradual to ensure network functionality. Devices have been created so you can make a transition so that the two network protocols can coexist.

Keywords: IPv4, IPv6, Internet, Qos, IPSec, DHCP, CIDR, DNS, NAT, RFC, TCP/IP.

1. Introdução

O protocolo IPv6 existe faz um tempo, porém sua implantação ainda está se iniciando por todo o planeta. Com o grande crescimento do número de dispositivos conectados à rede mundial (computadores, notebooks, smartphones, tablets, GPS (Global Positioning System), etc.) e o grande desperdício de endereços causados pela maneira como foram distribuídas as faixas IPv4, o IPv6 está cada vez mais se consolidando como o protocolo padrão da Internet.

De acordo com as companhias que regulam a Internet, a previsão para o esgotamento dos endereços IPv4 é julho de 2011, fazendo com que a implantação do IPv6 seja inevitável num futuro próximo.

Além disso, o IPv6 traz inúmeras vantagens como escalabilidade, segurança, configuração e administração de rede, suporte a QoS, mobilidade e políticas de roteamento.

2. Histórico sobre a Internet e o protocolo TCP/IP

No ano de 1966, o Departamento de Defesa norte-americano (DoD – Department of Defense) iniciou um projeto chamado ARPANET através de sua Agência de Pesquisas e de Projetos Avançados (ARPA – Advanced Research Projects Agency). Este projeto tinha como objetivo interligar universidades e instituições de pesquisa e militares. Em 1969, este projeto começa a ser implementado com a instalação dos primeiros quatro nós da rede, na Universidade de Los Angeles (UCLA), na Universidade da Califórnia em Santa Bárbara (UCSB), no instituto de pesquisa de Stanford (SRI) e na Universidade de Utah.

A ARPANET foi desenvolvida com o intuito de proteger informações sigilosas do governo norte-americano contra ataques inimigos, já que este período foi marcado pela Guerra Fria.

Por isso, a ARPANET consistia em um modelo de troca e compartilhamento de informações que permitia a descentralização das mesmas.

Em seu início, a ARPANET utilizava diversos protocolos de comunicação, sendo o principal o protocolo NCP (Network Control Protocol) que pouco tempo depois foi visto como inadequado, e a partir de 1/1/1983, o conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) foi adotado e até hoje continua sendo o protocolo base da Internet.

No início, a Internet tinha poucos serviços, sendo o E-mail (Electronic Mail), o serviço mais utilizado. O FTP (File Transfer Protocol) era utilizado para transferência de arquivos e o Telnet para acesso de sessões em hosts.

A Internet que utilizamos hoje foi criada ao longo da década de 80, onde diversas instituições dos EUA (Estados Unidos da América) e de outros países foram se interligando, porém sem cunho comercial. A pressão para que empresas pudessem também participar da rede mundial, fez com que no início dos anos 90 a Internet fosse aberta para o uso comercial e assim alcançasse uma grande quantidade de pessoas ao redor do mundo.

3. Principais características do protocolo IPv4

3.1. Visão geral do conjunto de protocolos TCP/IP

A Internet possui a mais bem sucedida aplicação prática de conectividade de redes de tecnologias distintas. Essa conectividade foi conseguida pelo uso do conjunto de protocolos TCP/IP. O TCP/IP executa essa conectividade em nível de rede, o que permite a comunicação entre aplicações em computadores de redes distintas sem a necessidade de conhecimento da topologia envolvida nesse processo. (Comer, 1998)

Outra característica importante do TCP/IP é a flexibilidade de adaptação às tecnologias de redes existentes e futuras, que é possível porque o TCP/IP foi concebido de forma independente das tecnologias de redes. Os equipamentos que executam a conexão entre redes na Internet baseiam-se no protocolo IP para o encaminhamento (ou roteamento) de informações através das redes envolvidas, e por isso são denominados como Roteadores IP. (Comer, 1998)

O número de serviços que podem estar disponíveis na Internet é ilimitado, dada à transparência que o protocolo TCP/IP dá a essa rede, facilitando assim o desenvolvimento contínuo de novas aplicações e serviços.

O TCP/IP é um conjunto de protocolos padrão do setor que permite a comunicação em ambientes heterogêneos. As tarefas envolvidas no uso do TCP/IP no processo de comunicação são distribuídas em protocolos, organizados em quatro camadas distintas da pilha do TCP/IP.

Esta divisão do protocolo em camadas traz uma série de benefícios ao TCP/IP que facilita o suporte a diversas plataformas de computação.

As quatro camadas da pilha do protocolo TCP/IP são as seguintes:

Camada de Aplicação: Define os protocolos de aplicativos TCP/IP e como os programas host estabelecem uma interface com os serviços de camada de transporte para usar a rede. Além disso, a camada de aplicação fornece serviços e utilitários que permitem que os aplicativos acessem os recursos de rede. Dois serviços proporcionam acesso aos recursos de rede são o Windows Sockets e o NetBIOS (Network Basic

Input/Output Systems). Além destes serviços citados, existe uma série de protocolos que operam na camada de aplicação do modelo TCP/IP, merecendo destaque:

HTTP (Hypertext Transfer Protocol): Especifica os processos de interação cliente/servidor entre navegadores da Web e servidores Web;

FTP (File Transfer Protocol): Responsável pela transferência de arquivos e gerenciamento básico de arquivos em computadores remotos;

SMTP (Simple Mail Transfer Protocol): Realiza envio de mensagens de clientes para servidores e entre servidores;

DNS (Domain Name System): Responsável por resolver nomes de host para endereços TCP/IP;

RIP (Routing Information Protocol): Este protocolo realiza a troca de informações entre roteadores em uma rede;

SNMP (Simple Network Management Protocol): Permite a coleta de informações sobre dispositivos de rede (Hubs, Roteadores, Pontes). Qualquer informação sobre um dispositivo encontra-se definida em uma MIB (Management Information Base);

POP3 (Post Office Protocol): Utilizado no acesso remoto a uma caixa de correio eletrônico. Este protocolo permite que todas as mensagens contidas numa caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local;

DHCP (Dynamic Host Configuration Protocol): Oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede;

Camada de Transporte: Fornece gerenciamento de sessão de comunicação entre computadores host. Define o nível de serviço e o status da conexão usada durante o transporte de dados. São dois os protocolos dessa camada:

TCP (Transmission Control Protocol): Oferece comunicações confiáveis orientadas para conexão aos aplicativos que normalmente transferem grandes volumes de dados de uma só vez ou que exigem confirmação de recebimentos dos dados transmitidos. Este protocolo garante a entrega dos dados na ordem correta;

UDP (User Datagram Protocol): Oferece comunicações sem conexão e não garante a entrega dos pacotes transmitidos. Este passa ser uma responsabilidade do aplicativo. É utilizado para comunicações mais rápidas e com menor sobrecarga que o protocolo TCP. Geralmente transfere-se pequenas quantidades de dados.

De acordo com (Comer, 1998), para que se forneça um transporte confiável, e seja assegurado que os dados cheguem sem erros e em sequência, o protocolo de transporte faz com que sejam enviadas informações do lado receptor e retransmissão de pacotes perdidos, por parte do transmissor. Similar à manipulação de frames pela camada de rede, esta camada agrega pequenas mensagens em um único pacote, e quebra mensagens grandes em vários pacotes, visando otimizar o desempenho na rede.

Camada de Internet: Empacota dados em datagramas IP, que contêm informações de endereço de origem e de destino usadas para encaminhar datagramas entre hosts e redes. Executa o roteamento de datagramas IP. Os quatro protocolos desta camada são:

IP (Internet Protocol): Realiza o endereçamento e roteamento de pacotes entre hosts e redes;

ARP (Address Resolution Protocol): É quem obtém os endereços de hardware de hosts que estão localizados em uma mesma rede física;

IGMP (Internet Group Management Protocol): Gerencia a participação do host em grupos de difusão seletiva de IP;

ICMP (Internet Control Message Protocol): Responsável por enviar mensagens para outros hosts e relatar erros com relação à entrega de um pacote.

Camada de Enlace: Também conhecida como camada rede. Especifica os detalhes de como os dados são enviados fisicamente pela rede, inclusive como os bits são assinalados eletricamente por dispositivos de hardware que estabelecem interface com um meio da rede, como cabo coaxial, fibra óptica ou fio de cobre de par trançado.

Segundo (Comer, 1998), a camada de Interface de Rede interage com o hardware, permitindo que as demais camadas sejam independentes do hardware

utilizado. Essa camada define como o cabo está conectado à placa de rede, como por exemplo, o tipo de conector e quais pinos serão utilizados. Ela também define qual técnica de transmissão será utilizada para enviar os dados para o cabo da rede.

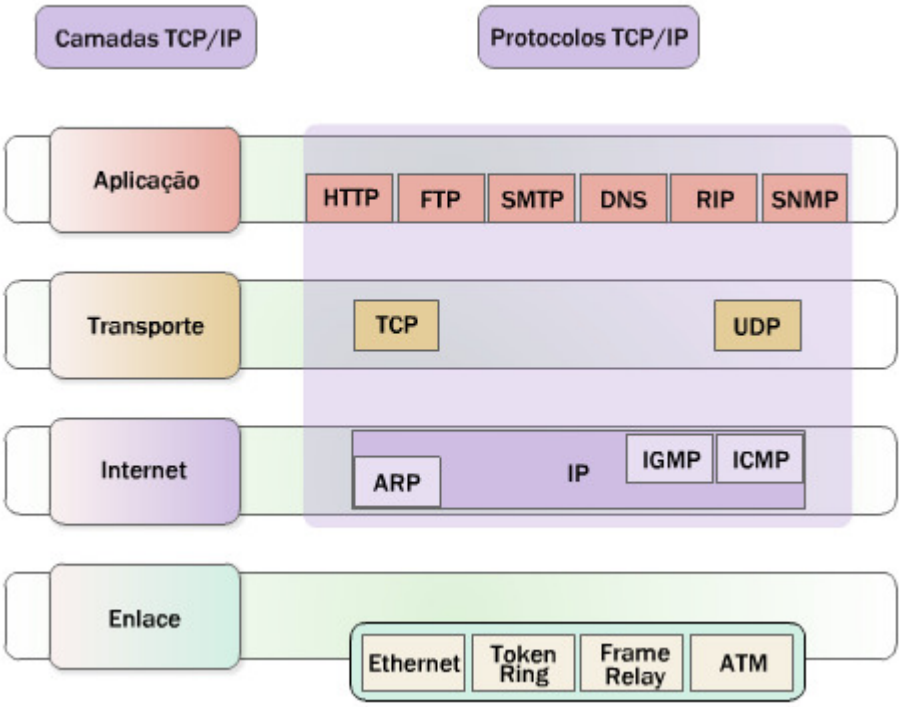

Figura 1 - Arquitetura do conjunto de protocolos TCP/IP
Fonte: (Microsoft, 2003)

O protocolo TCP/IP possui duas funções básicas que foram definidas na RFC (Request For Comments) 791, a fragmentação e o endereçamento.

De acordo com (Santos, 2009), a fragmentação permite o envio de pacotes maiores que o limite de tráfego estabelecido de um enlace, dividindo-os em partes menores e o endereçamento permite identificar o destino e a origem dos pacotes a partir do endereço armazenado no cabeçalho do protocolo.

De acordo com as especificações, o IPv4 reserva 32 bits numerados de 0 a 31 para endereçamento, o que resulta em 4.294.967.296 de endereços distintos.

Número de endereços IP disponíveis
2 ^ 32 = 4.294.967.296
Mais de 4 bilhões de endereços

Tabela 1 – Quantidade de Endereços IPv4 disponíveis

3.2. Classes de endereços IPv4

Segundo (Santos, 2009), inicialmente estes endereços foram divididos em três classes de tamanhos fixos da seguinte forma:

Classe A: O bit mais significativo é 0 e utiliza os 7 bits restantes do primeiro octeto para identificar a rede e os 24 bits restantes para identificar o host.

Esta classe possui endereços de 1.0.0.0 até 126.0.0.0;

Classe B: Os dois bits mais significativos são 10 e os 14 bits seguintes identificam a rede e os 16 bits restantes identificam o host.

Esta classe possui endereços de 128.1.0.0 até 191.254.0.0;

Classe C: Os três bits mais significativos são 110 e os 21 bits seguintes identificam a rede e os 8 bits restantes identificam o host.

Esta classe possui endereços de 192.0.1.0 até 223.255.254.0

Classe	Formato	Redes	Hosts
A	7 Bits Rede, 24 Bits Host	128	16.777.216
B	14 Bits Rede, 16 Bits Host	16.384	65.536
C	21 Bits Rede, 8 Bits Host	2.562.097.152	256

Tabela 2 – Classes dos Endereços IPv4
Fonte: (Microsoft, 2003)

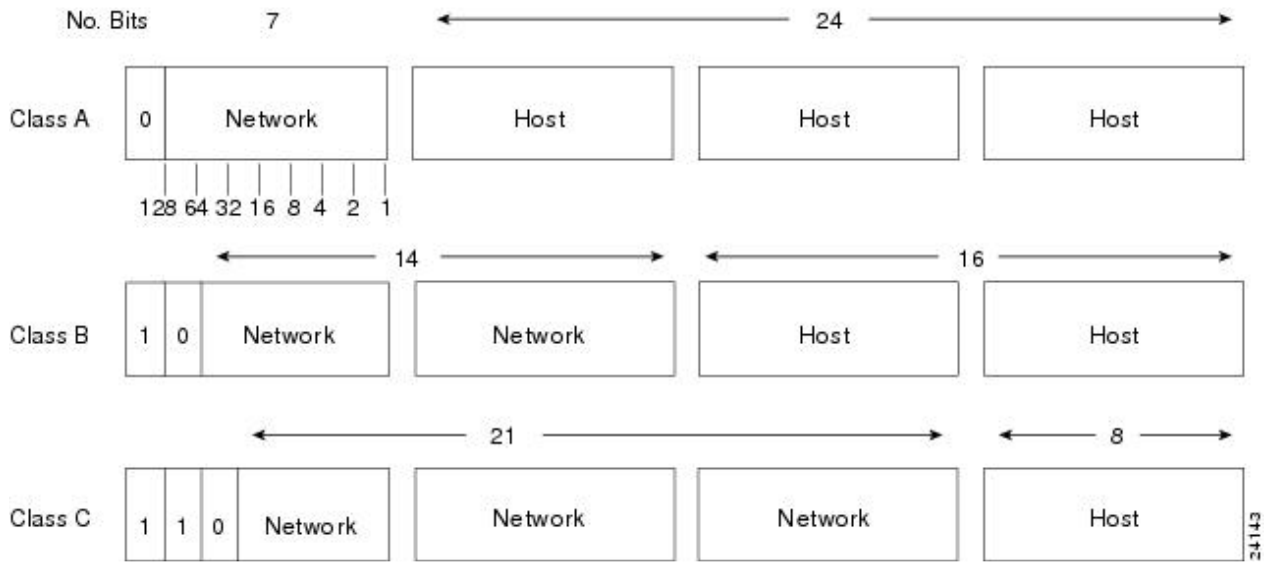

Figura 2 – Classes dos Endereços IPv4
Fonte: (Microsoft, 2003)

A estratégia de divisão dos endereços em classes tinha como objetivo tornar a distribuição de endereços mais flexível, podendo criar redes de tamanhos diferentes, porém com o passar do tempo descobriu-se que esta classificação era ineficiente, pois desperdiça muitos endereços.

Segundo (Santos, 2009), a classe A poderia atender um número muito pequeno de redes, mas ocupava metade de todos os endereços disponíveis; para endereçar 300 dispositivos em uma rede, seria necessário obter um bloco de endereços classe B, desperdiçando assim quase todos os 65.536 endereços; e os 256 endereços da classe C não supriam as necessidades da grande maioria das redes.

Além disso, diversas faixas da classe A foram distribuídas para empresas e instituições como o MIT (Massachusetts Institute of Technology), HP (Hewlett-Packard), Xerox, Apple, IBM (International Business Machines), DoD, AT&T (American Telephone and Telegraph) e Ford. Cada faixa concedida a estas empresas correspondia a 16.777.216 de endereços, sem contar as 35 faixas de endereços reservadas para multicast, loopback e uso futuro.

3.3. Como as máscaras de sub-rede funcionam

Um endereço IP é composto de um identificador de rede e um identificador de host, porém o comprimento destes identificadores varia. Para identificar onde o identificador de rede termina e onde o identificador de host começa foi criada a máscara de sub-rede.

Como exemplo, utilizaremos o endereço IP 192.168.0.10. Este endereço consiste em quatro bytes expressos como números decimais, separados por pontos, e cada um desses números decimais também pode ser expresso em números binários de oito bits.

192	168	0	10
11000000	10101000	0	1010

Tabela 3 – Endereço IP representado em notação decimal e em sua forma binária

255	255	255	0
11111111	11111111	11111111	0

Tabela 4 – Máscara de sub-rede representada em notação decimal e em sua forma binária

Comparando os bits entre si, a primeira parte do endereço IP se alinha com os bits um da máscara de sub-rede. Já a última parte do endereço IP se alinha com os bits zero.

11000000	10101000	0	1010
11111111	11111111	11111111	0

Tabela 5 – Endereço IP e Máscara de sub-rede representados em sua forma binária

3.4. Diretrizes para endereçamento IPv4

Não existem regras para atribuir endereços IP em uma rede, porém, existem diretrizes para atribuir identificadores válidos tanto para a rede quanto para o host.

Estas diretrizes são:

- Não utilizar o número 127 em decimal ou 01111111 em binário para o primeiro octeto do identificador de rede. Este número é utilizado para diagnóstico. Como exemplo vale citar o famoso comando ping 127.0.0.1 que faz o diagnóstico da placa de rede local;

- Utilizar endereços de IP público somente quando necessário;
- Utilizar as faixas de endereços IP privados reservados pela IANA (Internet Assigned Numbers Authority) para endereçamento privado de IP;
- Não utilizar todos os números 1 (binários) para identificar o host em uma rede de classes porque este endereço é interpretado como difusão ou broadcast;
- Não utilizar todos os números 0 (binários) para identificar o host em uma rede de classes porque em algumas implementações TCP/IP este endereço é interpretado como difusão ou broadcast;
- Não duplicar endereços de host dentro de um mesmo segmento de rede para evitar conflitos de endereço IP.

4. Por que o protocolo IPv4 está sendo substituído

4.1. Limitações do protocolo IPv4

Com o crescimento acelerado de dispositivos e usuários que acessam a Internet, os mais de 4 bilhões de endereços IP estão quase todos alocados, o que limita a continuidade do crescimento da Internet.

Para se ter uma idéia, em 1990 existiam 313.000 hosts conectados a rede, em 1992 este número já passava de 1.136.000. Em 1993 com a criação do protocolo HTTP e a liberação da Internet para o uso comercial, este número ultrapassou os 2.056.000 e em 1997 atingiu o números de 26.000.000 de hosts conectados.

Data	Hosts	Domínios	Data	Hosts	Domínios
1981	213	-	1990	313000	9300
1982	235	-	1991	617000	18000
1983	562	-	1992	1136000	17000
1984	1024	-	1993	2056000	26000
1985	1961	-	1994	3212000	46000
1986	5089	-	1995	8200000	120000
1987	28174	-	1996	16729000	488000
1988	56000	1280	1997	26053000	1301000
1989	159000	4800	1997	26053000	1301000

Tabela 6 – Crescimento da Internet ao longo dos anos.
Fonte: (Santos, 2009)

O aumento da tabela de roteamento é outro fator importante para a substituição do protocolo IPv4, já que os roteadores dos backbones devem manter sempre informações completas do roteamento da Internet. Se o número de entradas nas tabelas de roteamento crescerem indiscriminadamente, os núcleos dos roteadores serão forçados a pular rotas e porções da Internet ficarão inalcançáveis.

Além disso, o protocolo não dispõe de nenhum mecanismo de segurança nativo para os dados que são transmitidos pela rede, possibilitando assim que um invasor intercepte uma conexão e tenha acesso aos dados.

4.2. Soluções paliativas (Utilização do CIDR, do DHCP e do NAT)

Com o potencial esgotamento dos endereços IP e também o problema do aumento de tabela de roteamento, em 1991 a IETF (Internet Engineering Task Force) criou um grupo de trabalho batizado com o nome de ROAD (Routing and Addressing). Este grupo apresentou como solução paliativa para estes problemas a utilização do CIDR (Classless Inter-domain Routing).

CIDR

O CIDR é um método de atribuição e agregação de endereços. Ele combina várias identificações de rede consecutivas e que pertencem à mesma classe de endereço IP em um único bloco.

Esta combinação de redes é bastante utilizada para poupar endereços de classe B através da associação de grupos contíguos de endereços de classe C. Para isso, os endereços de classe C devem ter os mesmos bits de ordem superior e a máscara de sub-rede é reduzida tomando bits emprestados da identificação de rede e atribuindo-os à parte de identificação do host para criar uma máscara de sub-rede personalizada.

Segundo (Santos, 2009), o CIDR acaba com o uso de classes de endereços o que permite a alocação de blocos de endereços IP com tamanho apropriado para a real

necessidade de cada rede, reduz o tamanho da tabela de roteamento já que permite a agregação de rotas. O CIDR é definido na RFC 4632.

Com o CIDR os blocos são referenciados como prefixo de redes.

DHCP

O DHCP é um serviço e um protocolo que trabalham em conjunto para distribuir automaticamente endereço IP, máscara de sub-rede, roteador padrão e endereço de servidor DNS local para os hosts de uma rede. Esta atribuição dinâmica de endereços IP aos seus clientes é feita a partir de um pool de endereços.

Segundo (Santos, 2009), o DHCP tem sido muito utilizado por parte dos ISPs (Internet Service Provider) por permitir a atribuição de endereços IP temporários a seus clientes conectados. Desta forma, torna-se desnecessário obter um endereço para cada cliente, devendo-se apenas designar endereços dinamicamente, através de seu servidor DHCP. Este servidor terá uma lista de endereços disponíveis, e toda vez que um novo cliente se conectar à rede, lhe será designado um desses endereços de forma arbitrária e, no momento que o cliente se desconecta, o endereço é devolvido.

O DHCP possui uma série de benefícios merecendo destaque:

- Não ser necessário configurar manualmente cada cliente com um endereço IP;
- Não ser necessário manter um registro dos endereços IP que foram atribuídos;
- É possível atribuir automaticamente um novo endereço IP ao mover um cliente de uma sub-rede para outra;
- É possível liberar o endereço IP de um computador que esteja off-line por um período específico de tempo e reatribuir o endereço a outro computador;
- Redução da possibilidade de duplicação de endereços.

O processo de funcionamento do DHCP

Um host precisa de dados de configuração TCP/IP para poder acessar a rede, por isso ele envia um pacote de difusão DHCP que solicita informações sobre a disponibilidade de servidores DHCP que podem fornecer configuração TCP/IP.

Quando um servidor DHCP disponível recebe a solicitação, ele seleciona o endereço IP de um pool de endereços definido em seu banco de dados, responde e oferece dados de configuração TCP/IP ao cliente.

Caso o cliente aceite a oferta, as informações sobre o endereçamento IP são concedidas por um tempo especificado de tempo. Enquanto o intervalo de concessão estiver aberto, o cliente renovará a atribuição de endereço toda vez que fizer logon na rede. Se esta concessão expirar e não for realizada a renovação, o endereço IP será devolvido ao pool de endereços e estará disponível para ser atribuído a outro cliente.

NAT (Network Address Resolution)

De acordo com (Santos, 2009), o NAT é mais uma técnica paliativa desenvolvida para resolver o problema do esgotamento dos endereços IPv4. Definida na RFC 3022, tem como idéia básica permitir que, com um único endereço IP, ou um pequeno número deles, vários hosts possam trafegar na Internet. Dentro de uma rede, cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno. Quando um pacote precisa ser roteado para fora da rede, uma tradução do endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.

Isto é possível porque na RFC 1918, existem 3 intervalos de endereços IP que são considerados privados. Estes intervalos de endereços não são roteados pela Internet. As faixas de endereços reservados são as seguintes:

- 10.0.0.0 a 10.255.255.255/8 que pode endereçar 16.777.216 hosts;
- 172.16.0.0 a 172.31.255.255/12 que pode endereçar 1.048.576 hosts e;
- 192.168.0.0 a 192.168.255.255/16 que pode endereçar 65.536 hosts.

A utilização do NAT possui as seguintes vantagens:

- Reduz a necessidade de endereços públicos, contribuindo para diminuir a escassez deste tipo de endereço;
- Facilita a numeração interna das redes;
- Oculta a topologia das redes e;

- Permite apenas a entrada de pacotes gerados em resposta a um pedido de rede.

Apesar de todas estas vantagens o NAT possui também uma série de desvantagens:

- Quebra do modelo fim-a-fim da Internet, já que não permite a conexão direta entre dois hosts;
- Dificulta o funcionamento de uma série de aplicações, como VPNs (Virtual Private Network), VOIP (Voice over Internet Protocol) e P2P (Peer-to-Peer);
- Baixa escalabilidade devido ao baixo número de conexões simultâneas;
- Exige grande poder de processamento do dispositivo tradutor;
- Passa uma falsa sensação de segurança porque não permite a entrada de pacotes não autorizados, mas não realiza nenhum filtro nos pacotes que passam por ele;
- Não permite o rastreamento do caminho do pacote através de ferramentas como traceroute;
- Dificulta a utilização de técnicas de segurança como o IPSec (Internet Protocol Security).

Mesmo com todas estas soluções paliativas, o problema do esgotamento dos endereços IP não foi resolvido, já que a utilização destas técnicas diminuiu em apenas 14% a quantidade de blocos de endereços IP solicitados a IANA.

4.3. Riscos da não implantação do IPv6

Apesar de crescer a cada dia, o IPv6 não possui uma grande representatividade dentro da Internet, sendo o IPv4 o protocolo padrão na maioria das redes. Este cenário precisa ser alterado muito em breve para que a Internet não tenha problemas de crescimento e desenvolvimento.

Hoje, existe uma demanda muito grande por endereços IP e o IPv4 já não conseguirá atender muito em breve a esta necessidade e isto poderá comprometer o crescimento da Internet, impedindo o surgimento de novas redes além de diminuir o

processo de inclusão digital e assim reduzir o números de novos usuários dentro da rede mundial.

A não implantação do IPv6 também dificulta o surgimento de novas aplicações.

Novas tecnologias surgem a todo instante e cada vez mais dispositivos se conectam à rede.

Dentre estas novas tecnologias podemos citar as redes 3G, que hoje é responsável pela conexão da maioria dos dispositivos móveis como notebooks, celulares, smartphones, tablets, etc., no Brasil e no mundo.

A tecnologia 4G também já está sendo testada e logo estará sendo utilizada em larga escala requerendo um grande número de endereços IP.

E caso o IPv6 não seja implantado num curto espaço de tempo, todo este desenvolvimento estará comprometido.

Além disso, a utilização do IPv6 elimina e necessidade de utilização de NATs, que prejudica o funcionamento de várias aplicações e quebra o modelo fim-a-fim que dá uma maior transparência a utilização da Internet, permitindo identificar exatamente de onde vem e para onde vão todos os pacotes transmitidos.

Por esta razão, o custo de não utilizar ou adiar a implantação do protocolo IPv6 será muito maior do que utilizá-lo.

Já para os provedores de serviço, a não utilização do IPv6 fará com os mesmos percam competitividade e assim não consigam manter posição de destaque dentro do mercado, já que os clientes necessitam de novos serviços a cada dia.

5. Visão Geral do protocolo IPv6

De acordo com (Santos, 2009), as especificações do IPv6 apresentadas pela RFC 2460 tinham como principais mudanças com relação ao IPv4:

Maior capacidade de endereçamento: o endereçamento de 128 bits permitiu: alcançar níveis mais específicos de agregação de endereços; identificar uma quantidade maior de dispositivos na rede; e implementar mecanismos de autoconfiguração. A escalabilidade do roteamento multicast foi aprimorada através da adição do campo “escopo”. E o endereço anycast foi definido;

Simplificação do formato do cabeçalho: alguns campos do cabeçalho IPv4 foram removidos ou tornaram-se opcionais para reduzir o custo do processamento dos pacotes nos roteadores;

Suporte a cabeçalhos de extensão: as opções fazem parte do cabeçalho de extensão o que permite um roteamento mais eficaz, limites menos rigorosos em relação ao tamanho e a quantidade de opções, e uma maior flexibilidade para a introdução de novas opções no futuro;

Capacidade de identificar fluxos de dados: adição de recurso que permite identificar pacotes que pertencem a determinados tráfegos de fluxos, para os quais podem ser requeridos tratamentos especiais;

Suporte a autenticação e privacidade: os cabeçalhos de extensão são capazes de fornecer mecanismos de autenticação e garantir a integridade e a confidencialidade dos dados transmitidos.

Para finalizar o IPv6 passou a tratar a fragmentação de pacotes somente na origem, além de permitir o uso de conexões fim-a-fim e utilizar recursos que facilitam a configuração de rede.

5.1. Estrutura e sintaxe do IPv6

Os endereços IPv4 e IPv6 podem ser facilmente diferenciados um do outro. Enquanto o IPv4 possui 32 bits gerando pouco mais de 4 bilhões de endereços, o IPv6 possui 128 bits, o que resulta num total de 340.282.366.920.938.463.463.374.607.431.768.211.756 endereços. Isto representa 54.525.952 endereços para cada metro quadrado da superfície terrestre.

Na prática, o espaço de endereço IPv6 permite múltiplos níveis de sub-redes e alocação de endereços entre o backbone de internet a sub-redes individuais dentro de uma organização (McLean & Thomas, 2010).

Além dessa grande capacidade de endereçamento o novo formato ainda permitirá:

- Arquitetura hierárquica, possibilitando um encaminhamento mais eficiente dos pacotes;
- Distribuição de IPs fixos e válidos para conexões DSL, Modems, telefones móveis, etc.;
- Fornecer endereços válidos na Internet para todos os dispositivos conectados a ela;
- Utilizar arquitetura fim-a-fim;
- Eliminar problemas associados ao NAT.

Há 3 formas de representação do endereço IPv6:

- A notação mais usual é x:x:x:x:x:x:x:x, onde os "x" são números hexadecimais, ou seja, o endereço é dividido em oito partes de 16 bits, como no seguinte exemplo: 1080:0:0:0:8:800:200C:417;
- Sequências de zeros podem ser substituídas pela string "::". Esta substituição só pode ser feita uma única vez em cada endereço;

Endereço	Forma Completa	Forma Abreviada
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:43	FF01::43
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

Tabela 7- Representações do Endereço IPv6
Fonte: (Nunes, 2005)

Conforme (Bernal Filho, 2005), em ambientes mistos com nodos IPv4 e IPv6, é da forma x:x:x:x:x:x:d.d.d.d, onde:

"x" - são números hexadecimais (16 bits);

"d" - são valores decimais de 8 bits referentes à representação padrão já bem conhecida do IPv4.

Por exemplo: 0:0:0:0:0:0:192.168.20.30 ou, na forma abreviada: ::192.168.20.30.

5.2. Endereçamento IPv6

Um endereço IPv6 é dividido em oito grupos de 16 bits e são escritos com dígitos hexadecimais (0-F), não havendo distinção entre caracteres maiúsculos e minúsculos. O separa cada um destes 8 blocos e o símbolo ":".

Exemplo de um endereço IPv6:
0001:0DB8:AD1E:25E1:CA05:1902:CADE:E04F

Existem também regras de abreviação onde é permitido omitir os zeros a esquerda de cada bloco de 16 bits e também substituir uma sequência muito longas de zeros por "::".

O endereço 2001:0DB8:0000:0000:130F:0000:0000:140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B. Como mostram os exemplos, o símbolo "::" só pode ser utilizado uma vez para evitar ambiguidades.

Outra forma de representação de endereços é a utilização da notação CIDR. Esta notação é representada da forma "endereço-IPv6/tamanho do prefixo".

Exemplo:
Prefixo: 2001:db8:3003:2::/64
Prefixo Global: 2001:db8::/32
ID da sub-rede: 3003:2

Através desta representação consegue-se agregar 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. Isto tudo agiliza o encaminhamento de pacotes porque diminui a tabela de roteamento.

Os endereços IPv6 passam a ter colchetes quando forem destinados para URLs (Uniform Resource Locators) como no exemplo:

http://[2001:12ff:0:4::22]/pagina.html

Existem três tipos de endereços no IPv6:

Unicast: identifica uma única interface.

Anycast: identifica um conjunto de interfaces tais que um pacote enviado a um endereço Anycast seja entregue a qualquer um dos membros desse conjunto.

Multicast: Identifica um grupo de interfaces, tais que um pacote enviado a um endereço Multicast seja entregue a todas as interfaces do grupo.

Não existe nenhum endereço Broadcast no IPv6, sendo sua função substituída por endereços Multicast.

Endereços Unicast: Existem diversos tipos de endereços Unicast alocados no IPv6 como: Provider-based, Neutral-interconnect, NSAP, IPX , Site-local-use, Link-local-use, e IPv4- capable-host.

Provider-based: São endereços utilizados para comunicações globais. Sua utilização é parecida com a do CIDR utilizado no IPv4. Seu formato é:

3	n bits	m bits	o bits	p bits	o-p bits
10	REGISTRY ID	PROVIDER ID	SUBSCRIBER ID	SUBNET ID	INTF. ID

Tabela 8 - Formato endereços Provider-based.
Fonte: (Bernal Filho, 2005)

Local-use: É um endereço que tem escopo local para roteamento, porém pode ter também um escopo global de comunicação.

É dividido em:

Link-local-use: usado num único link ou canal de comunicação. Seu formato é:

10 bits	n bits	118-n bits
1111111010	0	INTERFACE ID

Tabela 9 – Formato endereço Link-local-use.
Fonte: (Bernal Filho, 2005)

Site-local-use: usado em um único site. Seu formato é:

10 bits	n bits	m bits	118-n-m bits
1111111011	0	SUBNET ID	INTERFACE ID

Tabela 10 – Formato endereço Site-local-use.
Fonte: (Bernal Filho, 2005)

IPv4 Encapsulados: Permite o envio dinâmico de pacotes IPv6 através infraestrutura de roteamento do IPv4. Aos nós IPv6 que utilizam esta técnica são atribuídos os endereços Unicast especiais que carregam um endereço IPv4 no 32-bits de menor ordem. Esse tipo de endereço é denominado IPv4-compatible IPv6 address, e seu formato é:

80 bits	16 bits	32 bits
000..... 000	0	ENDEREÇO IPv4

Tabela 11 – Formato de Endereço IPv4-compatible IPv6 address.
Fonte: (Bernal Filho, 2005)

Um segundo tipo de endereço IPv6 que encapsula um endereço IPv4 também é definido. Este endereço é usado para representar os endereços de nós exclusivamente IPv4 como os endereços IPv6. Este tipo de endereço é denominado IPv4-mapped IPv6 address, e seu formato é:

80 bits	16 bits	32 bits
000..... 000	FFFF	ENDEREÇO IPv4

Tabela 12 – Endereços IPv4-mapped IPv6 address.
Fonte: (Bernal Filho, 2005)

Endereços Anycast: É utilizado em comunicações de um-para-um-de-muitos. Ele identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próximo da origem.

Os endereços de Anycast, quando usados como parte de uma seqüência de rota, permitem a um nó selecionar qual dos diversos provedores existentes deve carregar o seu tráfego. Isto seria executado configurando endereços da anycast para identificar o conjunto de roteadores que pertencem aos provedores selecionados (por exemplo, um endereço do anycast por o provedor). Estes endereços anycast podem ser usados como endereços intermediários em um cabeçalho do IPv6, fazendo com que um pacote seja entregue através de um provedor ou de uma seqüência particular de provedores. Outros usos possíveis de endereços anycast seriam identificar um conjunto

de roteadores que fazem parte de uma sub-rede particular, ou o conjunto de roteadores de entrada para um domínio específico. Os endereços Anycast são alocados a partir do espaço de endereço do Unicast, usando alguns dos formatos de endereço definidos para o Unicast. Assim, os endereços Anycast são sinteticamente indistintos dos endereços Unicast. Quando a um endereço Unicast é atribuído uma ou mais interfaces, gerando assim um endereço do Anycast, os nós a que o endereço é atribuído devem explicitamente ser configurados para identificar que é um endereço Anycast.

Endereços Multicast: Um endereço Multicast é um identificador para um grupo de interfaces. Uma interface pode pertencer a qualquer número de grupos Multicast. Seu formato é:

8 bits	4 bits	4 bits	112 bits
11111111	FLAGS	SCOPE	GOUP ID

Tabela 13 – Formato endereços Multicast
Fonte: (Bernal Filho, 2005)

5.3. Políticas de Alocação e Designação

De acordo com (Santos, 2009), na hierarquia das políticas de atribuição, alocação e designação de endereços, cada RIR (Regional Internet Registry) recebe da IANA um bloco /12 IPv6. A alocação mínima para ISPs é um bloco /32.

Existem dois tipos de abordagem referentes a políticas de alocação e designação de endereços. Estas abordagens são a one size fits all e a conservadora.

Abordagem one size fits all

A recomendação da RFC 3177 é que seja seguida a abordagem one size fits all para a alocação e designação de endereços a usuários finais. Suas principais características são:

- As redes /48 são apropriadas para todos os tipos de usuários (domésticos, pequenas ou grandes empresas;

- Poderão receber redes /47, ou prefixos um pouco menores ou redes que são múltiplos de /48 as empresas que são muito grandes;
- Redes /64 deverão ser utilizadas quando uma e apenas uma sub-rede for necessária. Neste caso, usuários 3G são um bom exemplo para esta utilização;
- Redes /128 deverão ser utilizadas para conectar apenas uma interface como em conexões PPPoE (Point-to-Point Protocol over Ethernet).

Como principais vantagens a abordagem one size fits all oferece:

- Facilidade na renumeração da rede se houver a troca de provedor, onde se altera apenas o prefixo da rede;
- Possibilidade de se expandir a rede sem precisar solicitar mais endereços ao provedor;
- Facilidade no mapeamento entre o endereço global e o endereço Unique Local (ULA fc00:xyzw:klmn::/48);
- Possibilidade para a manutenção de regras únicas para zonas reversas de diversos prefixos;
- Facilidade de manutenção.

Abordagem conservadora

Esta abordagem é oposta a abordagem one size fits all. Ela recomenda que endereços de rede /48 não sejam atribuídos a todo tipo de usuário. Para usuários domésticos e pequenas empresas devem ser delegados endereços /56 porque desta forma reduz-se o consumo total de endereços de 6 a 7 bits.

E como uma rede /32 possibilita 65.536 /48, ela não seria suficiente para atender a demanda dos grandes provedores.

6. Principais características do protocolo IPv6

6.1. Escalabilidade

Um dos maiores benefícios da implementação de rede IPv6 é a disponibilidade de um número quase ilimitado de endereços IP. O IPv6 passa possuir um endereço de 128 bits contra os 32 bits do IPv4. Isso totaliza aproximadamente 1030 endereços por pessoa existente no planeta.

Esta disponibilidade de endereços e prefixos de rede, fornece uma flexibilidade na arquitetura de redes que permite uma organização hierárquica e inclusive geográfica, onde um prefixo de rede pode ser usado para endereçar um país ou até mesmo um continente e subdividi-los em diversos níveis.

Desta forma, os grandes provedores podem agregar todos os endereços de seus usuários a um único prefixo de rede e anunciar apenas uma rota para outros provedores. De maneira semelhante, o uso de diversos níveis hierárquicos dentro de um mesmo prefixo permite uma maior flexibilidade e funcionalidades como a utilização do escopo de endereços. Esta hierarquização da estrutura tem como objetivo reduzir o tamanho das tabelas de roteamento.

6.2. Segurança

Quando o IPv4 foi implantado não houve grande preocupação com a questão da segurança da informação, já que o protocolo servia apenas para interligar redes de pesquisa acadêmicas.

Devido ao crescimento da Internet, diversas vulnerabilidades foram exploradas e desta forma o tráfego de informações sigilosas, operações bancárias e transações comerciais ficaram comprometidos.

Sendo assim, criou-se a necessidade de adicionar novos mecanismos ao protocolo para que o mesmo se tornasse mais confiável.

Entre os principais mecanismos destacamos o IPSec que implementa criptografia e autenticação de pacotes na camada de rede, fornecendo uma solução de

segurança fim-a-fim, garantindo a integridade, a confidencialidade e a autenticidade dos dados.

O protocolo IPSec foi criado para ser utilizado com o IPv4, porém o IPv6 tornou sua implantação mais fácil, embora o funcionamento seja semelhante em ambos os protocolos.

Os mecanismos de autenticação e encapsulamento do IPSec são integrados ao IPv6 e seu suporte é obrigatório em todos os nós, já no IPv4 tudo isto é opcional.

O IPSec não pode ser utilizado com conexões que estejam atrás de NAT, porque o mesmo oculta o endereço IP de origem do emissor e isto impede sua identificação. Como não existe a utilidade de utilização de NAT no protocolo IPv6, o IPSec funciona sem nenhum tipo de restrição.

Através do IPSec, o IPv6 garante que a mensagem recebida não seja adulterada, que a mesma não seja entregue diversas vezes e que seu conteúdo seja criptografado, garantindo a confidencialidade da mensagem.

O suporte ao IPSec é obrigatório no IPv6, porém para sua efetiva utilização o mesmo deve ser habilitado em cada nó da rede, senão cada aplicação definirá ou não a sua utilização.

O IPSec é um conjunto de protocolos de segurança que para realizar suas funções, faz o uso de recursos independentes.

O protocolo utiliza dois cabeçalhos de extensão do IPv6: o Authentication Header (AH) que garante a autenticação e o Encapsulating Security Payload (ESP) para garantir a confidencialidade dos pacotes transmitidos. Além disso, para garantir a criação e gerenciamento de chaves de segurança ele utiliza o protocolo Internet Key Exchange (IKE).

6.3. Gerenciamento e Monitoramento

Para que uma rede funcione com qualidade e com o melhor desempenho possível, é necessário utilizar protocolos e ferramentas de gerenciamento e monitoramento de redes.

Entre as funções básicas na gestão de redes, duas das mais importantes são o acesso remoto e a transferência de arquivos.

Os protocolos Telnet e SSH (Secure Shell) utilizados para a realização de conexões remotas já trabalham sobre o IPv6, da mesma forma que os protocolos SCP, TFTP e FTP que são utilizados para a transferência de arquivos também já trabalham sobre o IPv6.

Outro protocolo importante no gerenciamento de redes é o protocolo SNMP. Este protocolo é um dos mais utilizados em rede IPv4 e seu funcionamento baseia-se na utilização de dois dispositivos, um agente e um gerente. Cada dispositivo que é gerenciado na rede precisa possuir um agente e uma base de dados que indica o estado atual deste dispositivo. Esta base de dados pode ser consultada e também alterada pelo dispositivo gerente. O conjunto dos dados dos dispositivos gerenciados é conhecido como MIB, que nada mais é do que uma estrutura de dados que prepara todas estas informações coletadas e que são de vital importância para o gerenciamento da rede.

O agente mantém as informações e as envia ao gerente quando solicitadas para que este monitore o sistema.

Estas informações armazenadas nas MIBs podem ser enviadas em conexões IPv4 ou IPv6 e desde 2002, o SNMP já consegue monitorar redes que só possuem conexões IPv6.

Outra forma de se gerenciar uma rede é através do monitoramento de fluxo. Esta técnica é utilizada em análises mais detalhadas de uma rede, onde cada pacote que trafega na rede é analisado durante um determinado período. Sendo assim, os equipamentos de rede enviam um fluxo de dados para um coletor e este armazena e interpreta os dados

A sincronização dos relógios é um fator importante no gerenciamento de redes e pode refletir no funcionamento de softwares e sistemas, além da segurança dos computadores, das redes e da própria Internet. O protocolo NTP (Network Time Protocol) é o responsável por manter o relógio do computador sincronizado e deste modo com o horário correto. Esta sincronização já ocorre com a utilização do protocolo IPv6 graças a servidores NTP públicos que já possuem suporte ao IPv6.

Além destes inúmeros protocolos que já auxiliam administradores a gerenciarem e monitorarem as redes IPv6, existem diversas ferramentas que auxiliam neste processo valendo destacar:

Argus: aplicativo de monitoramento de redes e sistemas, que permite acompanhar e avaliar dados referentes à conectividade na rede, porta TCP/UDP e de aplicações como HTTP, SMTP, RADIUS (Remote Authentication Dial In User Service);

Nagios: ferramenta versátil e flexível que apresenta inúmeras funcionalidades como monitoramento de serviços de rede; de recursos dos hosts; notificação de erros, etc. Possui a vantagem da possibilidade de adição de novas funcionalidades através de plugins;

NTOP (Network Traffic Probe): capaz de detalhar a utilização da rede por host, protocolo, etc., permitindo a visualização de estatísticas do tráfego, análise do tráfego IP, detecção de violações de segurança na rede, entre outras funções;

MRTG: utiliza o SNMP para obter informações de tráfego dos dispositivos gerenciados. Todos os dados obtidos através do protocolo SNMP podem ser monitorados por esta ferramenta e analisados através de gráficos em HTML;

Pchar: ferramenta de avaliação de performance da rede. Analisa aspectos como largura de banda, latência e perda de conexões;

Wireshark: analisador de tráfego de rede através da captura de pacotes. Possui interface gráfica e apresenta informação sobre a árvore de protocolos do pacote e seu conteúdo;

Looking Glass: permite a obtenção de informações sobre um roteador sem necessidade de acesso direto ao equipamento. Pode ser acessado através de uma interface Web, facilitando o diagnóstico de problemas na rede.

6.4. Suporte a QoS

Como o protocolo IP trata todos os pacotes da mesma forma, não dando a eles nenhum tipo de preferência ao serem encaminhados, o que fazer com aplicações como

VoIP, videoconferência e jogos, que necessitam que seus pacotes trafeguem com o mínimo de atraso, latência ou perda de pacotes?

Esta é a função do QoS, que é empregado em protocolos que necessitam que dados sejam transmitidos com prioridade de entrega e com garantia de qualidade.

Hoje o QoS trabalha principalmente com duas arquiteturas que possuem políticas de tráfego e podem ser combinadas para que o QoS seja utilizado em LANs (Local Area Network) e WANs (Wide Area Network).

Essas arquiteturas são a Differentiated Services (DiffServ) e a Integrated Services (IntServ).

DiffServ

A arquitetura DiffServ utiliza o conceito de classes, onde os pacotes que possuem requisitos QoS similares são agregados e priorizados.

A identificação dos pacotes DiffServ ocorre através dos oito bits do campo Tipo de Serviço do IPv4 e do campo Classe de Tráfego do IPv6 e tem como objetivo identificar e distinguir as diferentes classes ou prioridades de pacotes que necessitem de QoS.

Estes campos mencionados acima possuem as mesmas definições. Já as prioridades atribuídas a cada tipo de pacote podem ser definidas na origem, nos roteadores ou ao longo do caminho em roteadores intermediários.

Quando o campo Classe de Tráfego possui o valor zero significa que o pacote não precisa de QoS.

A arquitetura DiffServ é bastante utilizada porque a sua implantação é simples.

IntServ

A arquitetura IntServ utiliza o conceito de reserva de recursos por fluxo e geralmente é utilizada juntamente com o protocolo RSVP (Resource ReserVation Protocol). Este protocolo é utilizado para reservar o recurso da origem até o destino de um fluxo que requer QoS.

No IPv6, são utilizados os 20 bits do campo Identificador de Fluxo para identificar aqueles que necessitam de QoS. O campo Identificador de Fluxo deve ser preenchido com valores aleatórios entre 00001 e FFFFF. Os pacotes que não

pertencem a este fluxo deverão ter o campo Identificador de Fluxo preenchido com zeros.

Roteadores e hosts que não possuem suporte as funções do campo Identificador de Fluxo deverão preencher este campo com zeros ao enviarem um pacote, além de não alterar este pacote ao encaminhá-lo ou ignorá-lo ao recebê-lo.

Os pacotes que possuem o mesmo fluxo precisam possuir um mesmo endereço tanto de origem quanto de destino, além do mesmo valor no campo Identificador de Campo.

Vale mencionar que o protocolo RSVP utiliza alguns elementos do protocolo IPv6, como o protocolo Identificador de Fluxo e também o cabeçalho de extensão Hop-by-Hop.

6.5. Mobilidade

O protocolo IPv6 fornece suporte à mobilidade. Desta forma, um dispositivo móvel ao mudar de rede mantém seu endereço IP de Origem. Isto torna a movimentação entre as redes invisível aos protocolos de camadas superiores e todos os pacotes enviados a este dispositivos continuarão sendo encaminhados.

Os elementos responsáveis pelo funcionamento da mobilidade IPv6 são:

- **Nó Móvel:** dispositivo que mantém seu endereço IP de Origem quando muda de uma rede para outra e por isso continua recebendo os pacotes encaminhados a ele;
- **Rede de Origem:** É a rede que atribui o Endereço de Origem ao Nó Móvel;
- **Agente de Origem:** É um roteador localizado na Rede de Origem. Este roteador mantém a associação entre o Endereço de Origem e o Endereço Remoto do Nó Móvel;
- **Endereço de Origem:** É um endereço global unicast que é atribuído pela Rede de Origem ao Nó Móvel. Este endereço é permanente e os pacotes são direcionados para ele;
- **Rede Remota:** É qualquer rede, com exceção feita à Rede de Origem, onde o Nó Móvel se encontra;

- **Endereço Remoto:** É um endereço global unicast que é atribuído ao Nó Móvel através da Rede Remota;
- **Nó Correspondente:** É o novo que realiza a comunicação com o Nó Móvel e pode ser móvel ou estacionário.

Funcionamento da Mobilidade IPv6

A Rede de Origem atribui um endereço de Origem Fixo ao Nó Móvel. Este endereço não é alterado mesmo quando o Nó Móvel se desloca para outra rede qualquer.

O Nó Móvel recebe um ou mais Endereços Remotos ao ingressar em uma Rede Remota através de mecanismos de autoconfiguração. Estes endereços são constituídos de um prefixo válido na Rede Remota.

O nó realiza uma associação entre o Endereço de Origem e o Endereço Remoto para que os pacotes IPv6 destinados ao Endereço de Origem possam ser recebidos. Esta associação é registrada no Agente de Origem após ser enviada uma mensagem Binding Updates. Após receber esta mensagem, o Agente de Origem envia uma resposta Binding Acknowledgement. Outra forma de realizar esta associação é realizá-la diretamente com o Nó Correspondente e assim a comunicação é otimizada.

As comunicações entre Nós Móveis e Nós Correspondentes podem ocorrer através do Tunelamento Bidirecional e da Otimização de Rota.

Tunelamento Bidirecional

O Agente de Origem intercepta os pacotes enviados pelo Nó Correspondente para o Endereço Original do Nó Móvel e os encaminha através de um túnel, para o Nó Móvel utilizando o Endereço Remoto. Após isto, através do túnel, o Nó Móvel responde ao Agente de Origem e este reenvia o pacote ao Nó Correspondente.

Otimização de Rota

O Nó Móvel e o Nó Correspondente realizam a comunicação diretamente. Isto ocorre quando o Nó Móvel registra o seu Endereço Remoto no Nó Correspondente e este realiza a associação entre os Endereços de Origem e Remoto do Nó Móvel.

Diferenças entre suporte à mobilidade IPv6 e IPv4:

- Os roteadores atuando como agentes remotos não são mais necessários;

- Ao invés de fazer parte de um conjunto de extensões opcionais, a otimização da rota passou a ser incorporada ao protocolo;
- A atribuição de Endereços Remotos é facilitada pela configuração stateless;
- O protocolo IPv6 oferece benefícios como Descoberta de Vizinhança, mensagens ICMPv6 e cabeçalhos de extensão que são utilizados pela mobilidade IPv6;
- Através da Descoberta de Vizinhança, a mobilidade IPv6 é facilitada porque antes se necessitava do ARP para interceptar os pacotes destinados ao Nó Móvel e isto gerava dependência da camada de enlace;
- Através da utilização do anycast, o Nó Móvel recebe apenas a resposta de um único agente origem. Já com o IPv4 e a utilização do broadcast, o Nó Móvel recebe uma resposta separada de cada agente de origem.

6.6. Políticas de Roteamento

Os protocolos de roteamento encarregam-se de manter as informações utilizadas pelos roteadores atualizadas. Desta forma, os roteadores podem encontrar o melhor caminho para que os pacotes sejam encaminhados até o seu destino.

O processo de roteamento consiste em encaminhar pacotes através de diversos roteadores até que o mesmo alcance seu destino. 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.

Os protocolos de roteamento são divididos em internos e externos.

Os protocolos de roteamento interno são responsáveis por distribuir as informações dentro de Sistemas Autônomos (AS) e são conhecidos como Protocolos de Gateway Interno (IGP).

Os principais protocolos de roteamento interno utilizados no IPv4 são o RIP e o OSPF (Open Shortest Path First), porém estes protocolos ganharam novas versões para suportarem o IPv6. Estes novos protocolos são o RIPng (Routing Information Protocol Next Generation) e o OSPFv3.

O protocolo RIPng é baseado no algoritmo vetor distância e apresenta como principais mudanças em seu funcionamento o suporte aos prefixos e ao tamanho dos endereços IPv6.

O protocolo OSPFv3 é um protocolo de roteamento interno do tipo estado de link. Os roteadores constroem o mapa da rede com as rotas mais curtas, através do processo de flooding.

As principais diferenças entre o protocolo OSPFv3 e seu antecessor são:

- Criação de novos tipos de LSA´s;
- Retirada da autenticação, contando apenas com a autenticação do IPv6;
- Num único enlace pode ter múltiplas instâncias do OSPFv3 sendo executadas;
- Pacotes OSPF usam um endereço link-local como endereço de origem;
- No IPv4, o OSPF conecta interfaces por sub-rede, no OSPFv3 isso é feito por enlace.

Já os protocolos de roteamento externo se encarregam de distribuir as informações entre sistemas autônomos distintos e são conhecidos como Protocolos de Gateway Externo (EGP).

Nos protocolos de roteamento externo, o BGP (Protocolo de Gateway de Borda) é o mais utilizado. Como não há uma versão de BGP específica para o IPv6, a nova versão do protocolo IP utiliza as extensões multiprotocolo do BGP. Estas extensões suportam as mesmas funcionalidades que o BGP para o IPv4 e trabalham com as duas famílias de endereços.

7. IPv4 x IPv6

7.1. Coexistência e Transição

Como se sabe, o protocolo IPv4 é a base de toda a estrutura da Internet atualmente. Devido ao tamanho e também a proporção da rede mundial de computadores, a troca imediata do protocolo IPv4 pelo IPv6 é inviável. Por isso, o protocolo IPv6 deve substituir o protocolo IPv4 de forma gradual e transparente para que sua implantação seja bem sucedida. Por isso, ambos os protocolo deverão coexistir durante um período para evitar um problema de funcionamento da Internet.

Pensando-se nesta transição, foram elaboradas algumas técnicas para viabilizá-la. Estas técnicas são conhecidas como Pilha Dupla, Tunelamento e Tradução.

Pilha Dupla

Na técnica da pilha dupla, hosts e roteadores possuem suporte tanto ao IPv4 como ao IPv6 e por isso podem enviar e receber ambos os pacotes. Por isso, cada dispositivo é configurado com um endereço IPv4 e um endereço IPv6.

Para que esta técnica seja bem sucedida, alguns aspectos da infra-estrutura devem ser analisados:

- O servidor DNS precisa estar configurado para resolver nomes e endereços de ambos os protocolos;
- A configuração de roteamento IPv6 normalmente é independente da configuração de roteamento IPv4, por isso, ao implementar pilha dupla numa infra-estrutura onde o protocolo de roteamento é o OSPFv2, que só possui suporte ao IPv4, faz-se necessário a migração deste protocolo para outro que suporte ambos os protocolos, como o protocolo IS-IS ou deve-se utilizar o protocolo OSPFv2 em paralelo com outro protocolo que pode ser o IS-IS ou OSPFv3;
- Configurações dos firewalls também podem ser necessárias porque algumas plataformas não realizam a filtragem de pacotes IPv4 e IPv6 de forma integrada.

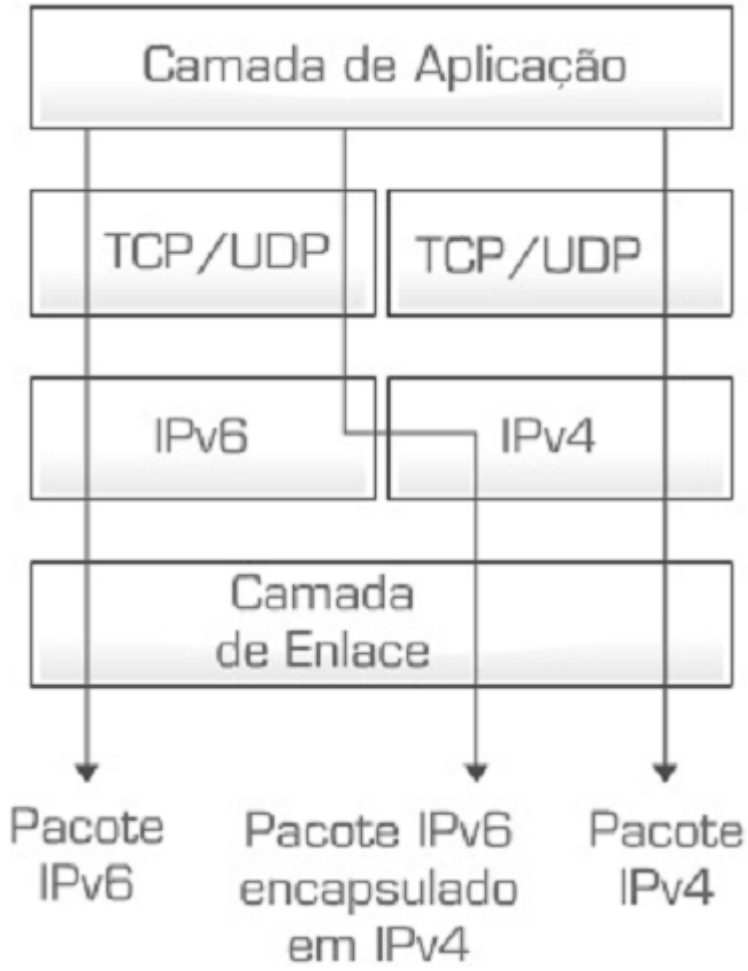

Figura 3: Pilha Dupla
Fonte: HTTP://cgi.br

Tunelamento

Esta técnica permite que pacotes IPv6 trafeguem em estruturas IPv4 já existentes sem precisar realizar qualquer tipo de alteração na forma como os pacotes são roteados, já que o conteúdo do pacote IPv6 é encapsulado em um pacote IPv4.

Estes túneis podem ser classificados como roteador-a-roteador, host-a-roteador, roteador-a-host e host-a-host.

Figura 4: Tunelamento
Fonte: HTTP://cgi.br

Existem diversas técnicas de tunelamento. As principais são Tunnel Broker, 6to4, ISATAP, Teredo e GRE.

Tunnel Broker

Através desta técnica, hosts IPv6/IPv4 que estão isolados em uma rede IPv4 podem acessar redes IPv6. Para funcionar o host precisa se cadastrar em um provedor de acesso Tunnel Broker e realizar o download de um software ou de um script de configuração. Após isto, o host realiza a solicitação do serviço ao servidor Web do provedor e ao se autenticar, o provedor verificar se o host utiliza um IPv4 público ou o NAT e lhe atribui um endereço IPv6. De agora em diante, o cliente pode acessar qualquer host na Internet.

6to4

Esta técnica permite a interconexão ponto-a-ponto entre roteadores, sub-redes ou computadores IPv6 através de redes IPv4. Esta técnica fornece um endereço IPv6 único a cada host, que é formado a partir de endereços IPv4 públicos. O endereçamento 6to4 possui um prefixo de endereço global 2002:wwxx:yyzz::/48, onde wwxx:yyzz é o endereço IPv4 público do cliente convertido para hexadecimal.

O prefixo 6to4 sempre será 2002, já que foi definido pela IANA.

ISATAP (Infra-Site Automatic Tunnel Addressing Protocol)

Esta técnica é baseada em túneis IPv6 que são criados de forma automática dentro da rede IPv4. O ISATAP é utilizado dentro das organizações, quando esta já possui numeração IPv6 válida e conectada na borda, mas sua infra-estrutura interna não suporta IPv6.

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 recurso auxiliar.

Teredo

No Teredo, os pacotes IPv6 são encapsulados em pacotes UDP e funciona através do NAT.

Um servidor Teredo inicializa a conexão e determina qual o tipo de NAT utilizada pelo cliente. Se o host de destino possuir IPv6 nativo, utiliza-se um Relay Teredo para criar a interface entre o cliente e o host de destino. O Relay utilizado sempre será aquele mais próximo ao host de destino.

Esta técnica gera overhead e seu funcionamento é complexo, diminuindo sua eficiência, porém é uma das únicas opções para hosts que estão atrás de NAT.

GRE (Generic Routing Encapsulation)

O GRE é um túnel estático entre dois hosts que encapsula diferentes tipos de protocolos. Ele foi desenvolvido pela Cisco e é suportado pela maioria dos sistemas operacionais e roteadores, funcionando como um link ponto a ponto. Sua principal desvantagem é a configuração manual, que pode gerar um grande esforço administrativo e de gerenciamento, caso a quantidade de túneis seja grande.

Seu funcionamento consiste em pegar os pacotes originais, adicionar o cabeçalho GRE e enviá-los ao IP de destino.

Tradução

A técnica da tradução permite que nós IPv6 comuniquem-se apenas com nós IPv4 e vice-versa. Esta tradução é realizada de diversas formas e também nas mais

diversas camadas, onde os cabeçalhos IPv4 são traduzidos para IPv6 e vice-versa, endereços e APIs (Application Programming Interface) são convertidos e a tradução também atua na troca de tráfego TCP ou UDP.

Figura 5: Tradução
Fonte: HTTP://cgi.br

Entre as principais técnicas de tradução estão a SIIT, BIS, BIA e TRT.

SIIT (Stateless IP/ICMP Translation)

Esta técnica permite a comunicação entre nós com suporte apenas ao IPv6 com nós que apresentam suporte apenas ao IPv4. Através de um tradutor localizado na camada de rede da pilha, campos específicos dos cabeçalhos de pacotes IPv6 são convertidos em cabeçalhos de pacotes IPv4 e vice-versa. Geralmente os pacotes TCP e UDP não são traduzidos.

BIS (Bump in the Stack)

Esta técnica funciona entre a camada de aplicação e a camada de rede e é utilizada para suportar aplicações IPv4 em redes IPv6.

O BIS adiciona três módulos à pilha IPv4. O módulo Tradutor realiza a tradução dos cabeçalhos IPv4 em cabeçalhos IPv6 e vice-versa. O módulo Mapeador de Endereços possui uma faixa de endereços IPv4 que são associados a endereços IPv6 quando o Tradutor recebe um pacote IPv6. Já o módulo Resolvedor de Nomes de Extensão é responsável pelas consultas realizadas pelas aplicações IPv4.

Este método funciona apenas na comunicação de aplicações IPv4 com hosts IPv6 e não possui suporte a comunicação do tipo multicast.

BIA (Bump in the API)

Possui funcionamento semelhante ao BIS, porém este mecanismo adiciona uma API de tradução entre o socket API e os módulos TCP/IP dos hosts de pilha dupla. Isto permite a comunicação de aplicações IPv4 com hosts IPv6, já que as funções do socket IPv4 são traduzidas em funções do socket IPv6 e vice-versa. Três módulos são adicionados a esta técnica. Os módulos Resolvedor de Nomes de Extensão e o Mapeador de Endereços funcionam da mesma forma que no BIS. Já o Mapeador de Funções, detecta as chamadas das funções do socket IPv4 e invoca as funções correspondentes do socket IPv6 e vice-versa.

Este mecanismo também utiliza faixas de endereços IPv4 e não suporta comunicações multicast.

TRT (Transport Relay Translator)

Esta técnica atua como tradutor da camada de transporte, o que possibilita a comunicação entre hosts IPv6 e IPv4 através de tráfego TCP/UDP.

Ele funciona em máquinas com pilha dupla que precisam ser inseridas num ponto intermediário dentro da rede.

Quando é realizada a comunicação de um host IPv6 com um host IPv4, um prefixo IPv6 falso é adicionado ao endereço IPv4 de destino. Ao passar pelo TRT, este pacote com prefixo falso é interceptado e enviado ao host IPv4 de destino em um pacote TCP ou UDP.

Este mecanismo só funciona de maneira bidirecional quando um bloco de endereços IPv4 públicos e um servidor DNS-ALG que servirá para mapear endereços IPv4 para IPv6 são adicionados.

8. Conclusão

Ao que tudo indica, o IPv6 será sem dúvida o protocolo padrão da Internet num futuro bem próximo não só pela escassez de endereços IPv4, mas pela demanda de serviços nos quais o IPv4 já não é mais adequado. Porém, a migração para este protocolo deve ocorrer de maneira gradual e transparente aos usuários. Para isto, o protocolo precisa ser de amplo conhecimento aos profissionais que atuam na área de infra-estrutura de Tecnologia da Informação para que esta migração obtenha sucesso.

A mobilidade dá ao protocolo a característica de conectividade a tudo e a todos num ponto em comum de comunicação.

Muitos problemas relacionados à questão de segurança foram melhorados graças ao suporte padrão ao IPSec que agora é obrigatório.

Outro fator importante é que o IPv6 não necessita de NAT e desta forma não quebra o modelo de conexão fim-a-fim da Internet, sem contar no tratamento diferenciado que pode ser dado aos mais variados serviços através do QoS.

Portanto, uma nova era nas comunicações está começando e sem nenhuma dúvida o IPv6 fará parte desta evolução.

Bibliografia

Bernal Filho, H. (21 de 03 de 2005). Teleco Inteligência em Telecomunicações. Acesso em 21 de 08 de 2011, disponível em Teleco Inteligência em Telecomunicações: http://www.teleco.com.br/tutoriais/tutorialipv6/pagina_2.asp

Comer, D. E. (1998). Interligação em rede com TCP/IP – volume 1 Princípios, protocolos e Arquitetura. Rio de Janeiro: Campus.

Karn, P., Metzger, P., & Simpson, W. A. (08 de 2005). The ESP DES-CBC Transform. San Diego, Nova Iorque, Madison Heights, California, Nova Iorque, Michigan, EUA.

McLean, I., & Thomas, O. (2010). MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7. Redmond: Microsoft Press.

Microsoft. (2003). 2180A - Implementação de uma infra-estrutura de rede do Microsoft Windows Server 2003: hosts de rede. Microsoft Press.

Nunes, C. (10 de 08 de 2005). História do Protocolo IPv6. Acesso em 21 de 08 de 2011, disponível em PUC - RS: http://www.inf.pucrs.br/~cnunes/cdt/aulas/IPv63.pdf#search=%22ICMPv6%20%22

Santos, R. R. (2009). Curso de IPv6 básico (1ª ed.). São Paulo.